WHITE PAPER

Meeting Compliance and Privacy Requirements

Distributing paper documents electronically in an age of increased regulatory pressures

NUANCE

Contents

Product overview 1

The changing business environment 1

Using technology to meet compliance and information management issues 3

Records and document management 3

Small volume, highly valuable paper-based documents 4

Information security: E-mail 6

Information security: Fax 7

Information security: Activity tracking 7

Tracking disclosures 8

Purging temporary files 8

Information availability 9

Handling information requests… 10

Summary 10

By electing to deploy a scanning solution, you recognize the unique return on investment an integrated scanning solution can offer. You understand that the office copier has emerged as a networked device with many functions: copy, print, fax, and scan. The benefits of scanning are not as obvious as copy, print, and fax, but can have the greatest impact on productivity by enabling you to integrate paper into your digital enterprise applications. Not only will your company realize an immediate increase in productivity but, you will also directly, positively impact your bottom line.

Product overview

Distributed document scanning and the case for electronic distribution Electronic scanning, distribution, and storage of paper documents offers enormous opportunities for cost savings, productivity improvements, and increased business effectiveness.

Here are just a few examples.

- Deliver original-quality documents immediately and at virtually no cost using your existing network infrastructure instead of sending them by fax or overnight mail.
- Scan incoming paper documents into your existing electronic workflows, eliminating costly delays and ensuring accuracy.
- Convert existing paper records into digital files and store them in computerized databases for fast, easy retrieval from any location.
- Back up your scanned documents to off site data storage facilities to ensure business continuance in the event of a disaster.

The changing business environment

While this transformation in the way organizations handle paper has been taking place, changes in the business environment have forced companies and public agencies worldwide to examine and modify their business processes, particularly those related to information management

- A slew of high profile corporate accounting scandals (Enron, Arthur Andersen, WorldCom, etc.) have resulted in calls for greater corporate oversight and demands for executive accountability. Businesses today must be extra vigilant in ensuring that all business-related transactions and communications are documented and retained for subsequent examination.
- The exponential growth in the acquisition and storage of personal information by governments and businesses, as well as an increasing number of cases of identity theft, has led to heightened concerns for personal privacy by consumer advocacy groups and individuals, particularly when information is transmitted across the Internet. Organizations handling confidential or personal information must take proactive measures to ensure information is safeguarded and is not disclosed to unauthorized persons.
- Increased expectations for openness and accountability have ushered in a new era of transparency in governments around the world. Agencies must respond rapidly to citizen requests for records relating to public health, environmental hazards, consumer product safety, government spending, taxes, and foreign policy, to name

just a few. By making information available over the Internet, requestors can conduct their own searches, and providers can eliminate the laborious and expensive process of locating and retrieving information often stored in dusty basements or inconvenient paper archives.

These new standards and expectations have brought about a tidal wave of new laws and regulations worldwide, designed to protect consumers and investors, and empower individual citizens. A sampling of recent legislation is shown in the table on the next page.

Varied in their range and complexity, these laws boil down to three key information management issues.

- **Records management** — the need to document all business transactions and retain records.
- **Privacy protection** — the need to protect confidential personal information.
- **Information availability** — the need to make information available to the general public and respond quickly to requests from individuals.

Law/Regulation	Country	Requirements
Sarbanes-Oxley Act	United States (including overseas subsidiaries of US companies)	Requires public companies to retain all documentation related to financial reports, audits, business transactions, and meetings for a period of five years in such a way that documents can be recovered quickly.
SEC Exchange Act 13-a-15(f)	United States	Requires companies to "provide reasonable assurance that transactions are recorded as necessary to permit preparation of financial statements in accordance with generally accepted accounting principles."
Gramm-Leach-Bliley Act	United States	Requires financial institutions to ensure the security of customers' private information.
Privacy and Electronic Communications Regulations	European Union (EU)	Protects the right to privacy with respect to the processing of personal information in the telecommunications sector.
Health Insurance Portability and Accountability Act	United States	Protects individuals' personal health information from unauthorized access. Requires appropriate administrative and technical safeguards, including data encryption, to ensure the privacy of patient health information.
Data Protection Act	UK and other European Union (EU) nations	Provides individuals with access to any records containing their own personal information, and establishes mechanisms to ensure that personal information is accurate, relevant, and subject to appropriate security.
Personal Information Protection and Electronic Documents Act	Canada	Requires consent before disclosing personal information and measures to ensure that personal information is subject to appropriate security
California Senate Bill 1386	United States	Requires disclosure of any security breach in which unencrypted personal information might have been acquired by an unauthorized person and due diligence in protecting customer information from unauthorized access. Applies to any company doing business in the state of California.
Freedom of Information Act	Enacted in various forms by governments worldwide	Gives individuals the right to request information from government agencies and obligates those agencies to deliver information promptly. It is intended to promote openness and accountability, and facilitate better public access to government information. Advanced integration into backend applications.

Using technology to meet compliance and information management issues

A carefully considered electronic document distribution and storage policy can go a long way to increasing competitiveness while helping with regulatory compliance. On the other hand, a poorly considered policy can expose an organization to unnecessary or unacceptable risk..

- Important steps in the business transaction cycle may be left undocumented if audit trails are not maintained and complete.
- Confidential information once kept under lock and key may become visible to unauthorized individuals.
- A mountain of paper may be transformed into a sea of unstructured electronic files, making it impossible to locate needed information.

It is vital, therefore, that organizations move cautiously when implementing an electronic document distribution and storage solution.

The remainder of this paper examines the benefits and potential pitfalls of electronic document distribution in this challenging regulatory environment.

Records and document management

Records management governs the creation, availability, retention, and ultimate destruction of documents relating to business activities and transactions.

These information assets, which may include orders, receipts, financial statements, policy statements, legal disclosures, and so on, are vital to the organization's existence—loss of these records could seriously compromise the company's ability to function or could put the company at risk of violating the law. Many companies have run into problems because they failed to retain information about business transactions, or because they purposely altered or destroyed such documents. Records Management, then, is the control and maintenance of these various assets over the course of their lifecycle.

Records Management does not mean keeping everything forever. In fact, there are many reasons not to keep everything beyond its required retention period, including:

- The costs of storage and maintenance, especially if older information must be migrated to newer storage media to ensure continued access.
- The additional time and expense involved in retrieving the information you want from a larger volume of data.
- Possible exposure to litigation based on outdated documents.
- The potential illegality of holding personal information longer than necessary.

The retention period for documents vary. But, in all cases, the employer is responsible for ensuring that employees are aware of the company's document retention policy and understand how to comply with the requirements. Numerous court cases involving employees who have not followed company procedures have exonerated the employee and held the employer liable for failing to provide appropriate guidelines or training.

In the post-Enron/Sarbanes-Oxley era, a wider definition of records management has emerged – one that places emphasis not only on traditional business documents, but also on the peripheral supporting communications, including e-mails, instant messages, voicemails, and other exchanges, regardless of media. Such communications are admissible as evidence in most courts of law and may be subject to the same rules of document retention. When questions about transactions or business practices arise, organizations must be able to retrieve all relevant information within a reasonable time frame.

For any organization that has invested in an electronic document management system, scanning becomes an obvious way to integrate paper-based documents with the company's other information assets. Imaging solutions that scan and file large volumes of incoming paper and file them electronically have been available for many years.

Frequently, the volume of documents handled by an office, department, or small business, does not justify such a specialized solution, or the paper-based information varies in content and format so it must be handled on a piece-by-piece basis. In these cases, a copier-based scanning solution that integrates with a back end document management system for "ad hoc" scanning provides an appropriate solution.

Several copier vendors now offer integration with various document management systems, but most simply deliver the scanned image file, plus perhaps some associated metadata describing the document, into a network folder, where it is processed by a release script and deposited into the back end system.

Risk: For organizations handling confidential or personal information, such a simple solution doesn't meet the requirements of limited access and secure handling. What is needed is a solution that supports authentication at the scanning device and allows the authenticated user to deliver the scanned document directly into a specific target folder that he or she is authorized to access. This way the existing security restrictions applied by the document management system to files in that folder ensure that only authorized users can access the data.

Mitigation: Look for a solution that offers integration into your document management system directly from the copier. While the precise implementation will vary, depending on the back end system, users typically log on using their existing system credentials. Once logged into the network, they select the target folder from a list of folders with authorized access, enter the required metadata, and then store the document. A built-in OCR engine can optionally create a text version of the image to support full text searching during the document retrieval process. Only with this level of integration can organizations handle personal information in a way that sures confidentiality.

Small volume, highly valuable paper-based documents

Businesses with regulatory and legal requirements need to follow specific guidelines for processing, protecting, retaining, and producing information.

Frequently, one of the guidelines that must be followed is that all appropriate information must be managed in a consistent manner. This can be a challenge when some of the required information is stored electronically and some is on paper.

Organizations can convert certain types of high volume paper-based information to a digital format and include it in standard electronic business process workflow applications using centralized, "production" scanning. Establishing documented, consistent policies and procedures for this type of document capture is common and software and vendor support is widely available.

Risk: The greater risk to businesses with regulatory and legal information lies in the "small volume" but "highly valuable" paper-based documents that information workers work with in their daily office/work environment. It is often impossible or impractical to take this paper information out of use, send it to a centralized scanning location, and capture it electronically before making it, once again, available to knowledge workers.

Case law over the past several years has upheld the principle that consistency in the application of practices for regulatory and legal information management across the business is key to demonstrating compliance. However, this can be difficult with large numbers of office workers. Reasonableness Standards for "good corporate citizenship" have now merged as a measure which the courts use to evaluate whether an organization entity has "done enough" to ensure information management requirements are being met. The important question is: has the organization created a process where every employee is capable and equipped to consistently handle required information in the required manner?

Mitigation: The solution is a program that aligns all office employees to act in a manner that is compliant, and is supported by the ubiquitous availability of implementation support – in this case office scanning equipment with software that makes it easy for employees to behave as required.

An effective program, based on consistency and reasonableness, for the compliant management of both paper-based and electronic information, follows these principles.

- Provides a clear policy that identifies "who, what, where, when, and how" for identifying, capturing and managing all (paper-based and electronic) information with regulatory and legal requirements.
- Makes it easy for employees to access the policy.
- Considers requiring annual written acknowledgement (accompanied with a privacy policy reaffirmation) by employees.
- Provides employees with the capability (including the necessary equipment) to easily and conveniently follow the policy and procedures, all of the time.
- Whenever possible, avoids procedures that require employee training.
- Considers requiring training logs when training is required. Logs will protect organizations by documenting the fact that requisite training was available.

A key element of meeting regulatory and legal compliance requirements is ensuring consistent procedures. Document capture software solutions that work with networked copiers allow individual office workers to scan documents the same way that they would make a copy. This technology offers the promise of enabling front office information workers to manage the capture and manipulation of paper- based information themselves. As a result, it can be consistently managed by the organization in a manner that meets regulatory and legal requirements in the same way that electronic documents are managed.

However, there are important considerations that office equipment and software buyers need to consider when evaluating the scanning software.

Look for a single, easy-to-use interface that is consistent across all office scanning devices. This will decrease the likelihood that training will be required. Office employees will quickly and consistently adopt the policy and follow the documented procedures.

- When using multiple brands of network copiers or scanners in conjunction with network copiers, look for a software interface employees can use across all brands
- Many copiers are available with scanning software from the copier equipment manufacturer. This is less desirable for businesses with compliance requirements. Reliance upon this software may require office workers to know how to use multiple procedures (for multiple brands of devices within the business). Remember: consistency is the goal.

Information security: E-mail

The "scan and mail" systems offered by copier vendors today make it very easy to send electronic copies of paper documents—including important business documents—to customers, vendors, business partners, regulatory agencies, etc..

Given the importance of records management, it is vital to track and manage these communications. Transmitting information over any public network requires special considerations.

Risk: Unfortunately, tracking these e-mail communications is not possible with many of the scanning solutions available today. Most of these systems require the use of an SMTP relay for the delivery of e-mail. As its name suggests, SMTP (Simple Mail Transfer Protocol) provides a "simple" way to deliver e-mail messages over the Internet. In fact, its simplicity and lack of any built in authentication makes it a 6perfect mechanism for spammers and virus spreaders, who can broadcast literally thousands of untraceable messages per second using fictitious sender names. Its simplicity also means there is generally no record of outgoing communications.

You can configure any PC with an Internet connection as an SMTP relay. All that is required is some SMTP server software, like Microsoft IIS (included with most versions of Windows) or any of the free SMTP applications available on the internet. To demonstrate just how simple SMTP actually is, here is an SMTP message you can create using any text editor.

> From: cfo@mycompany.com
> To: cfo@yourcompany.com
> Subject: Asset transfer authorization
>
> I have authorized the transfer of $100,000 to your holding account. A copy of the wire transfer authorization is attached.

You then place this file in your SMTP server's "pickup" directory and the message is delivered to the recipient—no authentication, no tracking, no encryption, no confirmation of delivery or receipt.

Remarkably, this is exactly how most copier-based scan and mail systems work—the copier prompts the user to enter the sender and recipient information, formats the message as shown above, attaches the scanned document, and delivers it to the SMTP server's "pickup" directory, where it gets processed and sent out over the Internet. Clearly, such systems expose organizations to untold risks.

Mitigation: The solution is to select a scanning system that integrates directly with your company's corporate e-mail system and delivers documents as if they were sent from the user's desktop. To do this requires an e-mail client that supports authentication and integrates with your mail server at the API level. This way the transaction is captured and retained along with all of the organization's other e-mail communications using whatever e-mail archiving solution has been selected.

In order to safely transmit information over a public network, the information must first be encrypted. This means that any organization planning to send confidential information should make sure any scanning solution they consider includes an encryption capability. Most copier solutions do not encrypt scanned documents.

It is important the solution you choose includes 128-bit document encryption that lets you securely encrypt confidential or personal information and deliver it by e-mail or network file transfer. When configured, the sender enters an encryption password at the scanning device. This password is used to generate the encryption key which is used to encrypt the scanned image file, making it unreadable to any unauthorized person who may

intercept the document. Upon opening the file, the authorized recipient enters the password to reverse the encryption algorithm and read the document.

Information security: Fax

There are similar problems with the fax capabilities of many copier-based scanning solutions as there are with e-mail.

Risk: Many of these systems provide faxing capabilities that are no more sophisticated than a standalone fax machine, with no record of outgoing faxes that can be retained as part of the company's records management policy.

Mitigation: Look for a scanning solution that offers integration with most network fax servers, including Captaris RightFax and Microsoft Exchange or Lotus Notes-based systems. These server-based systems maintain a record of all outgoing faxes, including what was sent, who sent it, when it was sent, and to who, making it easy to track or audit fax-based communications.

Information security: Activity tracking

Another useful feature provided by some copier-based scanning solutions is the ability to capture a record of scanning activities.

The purpose behind this is two-fold.

- To bill costs back to a department or an account ("cost recovery")
- To maintain a log of outgoing communications for audit purposes

To create a useful audit trail, a system must capture at least the following information.

- What was scanned
- Who scanned it
- When it was scanned
- How it was sent (e-mail, fax, network file transfer, etc.)
- Who it was sent to

Ask these critical questions when considering a scanning solution.

- Does the system you are considering ensure that all outgoing scanned e-mail can be traced back to the individual who sent it?
- Does the system you are considering save a copy of all outgoing scanned e-mail on the central mail server?
- Can Microsoft Outlook users view a copy of scanned documents they e-mailed from the copier by clicking "Sent Items" in Outlook?
- Can the system you are considering maintain a record of outgoing faxes?
- What tracking and audit trail capabilities does the system you are considering offer?
- Is your system sufficiently easy-to-use so that staff can comply with document retention policy requirements without affecting overall productivity?

Risk: Many systems lack even the most basic activity logging capabilities, while others simply log the number of pages scanned, with perhaps the ability to capture a billing or department code.

Mitigation: Look for a solution that offers comprehensive activity logging that captures basic information about the sender and recipient, and lets the system administrator configure custom fields to capture information about the document being sent.

Tracking disclosures

Organizations may be required to retain records of all information disclosures. For example, the Health Insurance Portability and Accountability Act (HIPAA) in the United States requires health providers to retain records documenting situations where personal information was released to a third party.

Patients have a legal right to request this disclosure information, and organizations must be able to demonstrate satisfactorily that personal information was disclosed only on a "need to know" basis.

In busy offices, under the pressure of time constraints, it becomes easy to "forget" what may seem like a burdensome detail. Best, then, is to make the tracking of disclosures an integral part of the document transfer process.

Few of the copier-based scanning solutions available today make it possible to track personal information disclosures. Most simply prompt the sender for the recipient's address and deliver the scanned document image via SMTP, providing no record of the transaction (see "E-mailing" on page 6). Look for a solution that provides tracking at two levels.

- Direct integration (API-level) with Microsoft Exchange and Lotus Notes mail servers ensures that a copy of the transaction is stored on the central e-mail server
- Activity tracking with custom fields ensures that a record of the transaction is entered into the transaction log file (see "Activity tracking" on page 8)

Together, these two mechanisms help organizations comply with disclosure tracking requirements with minimal additional effort.

Purging temporary files

Whenever documents are scanned, the scanning system creates temporary image files during the process.

When confidential data is involved, it is important to make sure temporary files are not left on the device's hard drive. Doing so could make this data vulnerable to theft or access by unauthorized individuals.

The way these temporary files are handled varies from copier vendor to copier vendor, but some solutions simply leave the files on the system's hard drive or remove them using standard (and easily reversible) file deletion functions.

Choose a solution that provides secure deletion of temporary files by overwriting the disk locations with multiple layers of random characters. This ensures that the data is properly purged and cannot be retrieved using data recovery tools.

Ask these critical questions when considering a scanning solution.

- Does the system you are considering support scanning documents directly into a document management system from the copier?
- Can the system you are considering save documents to a document management system in a way that ensures that only authorized individuals can access the information?
- Can the system you are considering encrypt personal information before sending it by e-mail?
- How does the system that you are considering help document disclosures of personal information?
- Does the system that you are considering ensure that temporary files containing confidential or personal information are purged from the system's hard drive after use?

Information availability

While businesses have an obvious economic incentive to make information about products and services available to the general public, the same is not necessarily true of government agencies. It is only recently that governments have enacted laws requiring public agencies to make information available to their constituents.

Under the United States' Freedom of Information Act (FOIA), you can get information about how an agency operates, actions it has taken, how it spends its money, and what information it has collected. Although FOIA predates the Internet, it is still relevant because it specifies the type of information that must be available, exclusions, rules for compliance, appeals processes, etc., rather than specifying access mechanisms or technologies. It has, however, lost some practical significance today because of its formal and time consuming operation. While written requests and 10-day waiting periods were once acceptable, the Internet has transformed people's ideas about access to information.

FOIA remains, though, an important legal minimum standard for accessing public information. More recent "freedom of information" acts, like the UK's version, specifically require public authorities to adopt and maintain publication schemes, guides to the type of information that the authority publishes, the format in which the information is available, and fees for access, if applicable. The UK's act was created as part of the government's "e-Government" program, which aims to make all public services accessible via the Internet, so much of the language is geared towards the use of technology as an enabler. As a result of a large advertising campaign by the government, the public has become well informed about their rights of access to information, so public agencies have been preparing for an anticipated deluge of requests.

Copier-based scanning solutions are well suited to scanning and archiving small to moderate volumes of documents on an ongoing basis ("ad hoc scanning"). By selecting a scanning solution that integrates with an existing document management system, agencies can efficiently store paper- based documents along with other electronic files, making them instantly available to those with appropriate access.

Many of the copier-based solutions that offer document management system integration, however, lack key features, such as support for full text searching or metadata entry

at the time of storage. Without these features, a scanning solution that was supposed to facilitate document retrieval may do exactly the opposite, if the end result is a folder of unstructured image files that must be searched manually for relevant content.

What is needed, then, is a system that makes indexing an integral part of the scanning process, ensuring that documents are entered according to the filing specifications laid down by the archive administrator.

A few companies offer direct integration with major document management systems directly from the copier and provide support for PDF, full text searching, and metadata entry, making them well suited for information that is available for download via the Internet.

Handling information requests

Most "freedom of information" acts specify how an individual must submit a request and how much time is permitted to comply with the request

In the United States, for example, requests submitted in writing must receive an initial response within 10 days. The agency then has an additional 10 days to provide the information requested. The agency is permitted to charge appropriate fees to cover retrieval and duplication costs.

By making information available over the Internet, agencies can fulfill requests through their Web site. For information that is not appropriate for public access via the Internet, agencies that store records electronically can minimize or eliminate time and costs by providing requested information by e-mail.

- Does the system you are considering allow the scanning of paper documents directly into a document management system?
- What image formats does the system you are considering support, and are these formats viewable using standard Web browser software?

Ask these critical questions when considering a scanning solution.

- Can the system you are considering convert document images into fully searchable text?
- Can the system you are considering add metadata describing the document's content so it can be retrieved easily?

Summary

This document outlines the many benefits of electronic scanning and document distribution, and highlights the important compliance issues to consider when selecting a scanning solution. There are scanning solutions that offer all of these benefits and more. You can build your own personalized solution, with integration into "home grown" document management systems and native integration to existing e-mail systems, to suit the needs of your own company.

The experience speaks for itself™

NUANCE COMMUNICATIONS, INC.
ONE WAYSIDE ROAD
BURLINGTON, MA 01803
781 565 5000
NUANCE.COM

NUANCE