

# The Top Five Things Every IT Manager Needs to Know About Compliance

How replacing your fax machines with fax server software reduces risk

## Overview

The number one driver for replacing fax machines with fax server software is most often regulatory compliance. Cost savings efforts and productivity gains run a close second with environmental awareness gaining in the standings. Regardless of the space your organization plays, the need to become regulatory compliant remains top priority.

What are some of the regulatory standards you may be required to maintain? For example, Section 404 of Sarbanes-Oxley (SOX) requires that large companies prove that their internal processes can provide certifiably correct accounting data and noncompliance can result in a fine of up to \$1 million and a jail term of up to ten years for any corporate officer who doesn't follow the rules, even if mistakenly. All healthcare organizations must comply with the Health Insurance Portability and Accountability Act (HIPAA). HIPAA restricts releasing protected patient information no matter their size or their ownership. There's the Graham-Leach Billey Act that states that enterprises must identify reasonable and foreseeable internal and external threats that could result in unauthorized disclosure, misuse, alteration, or destruction of customer information—to name a few. The list goes on depending on your geographic location or industry.

*"The Securities and Exchange Commission (SEC) is becoming strict on information that leaves or enters the company. Fax Server is more secure and provides granular control of all faxes."*

– Weiss Research (Financial Services)

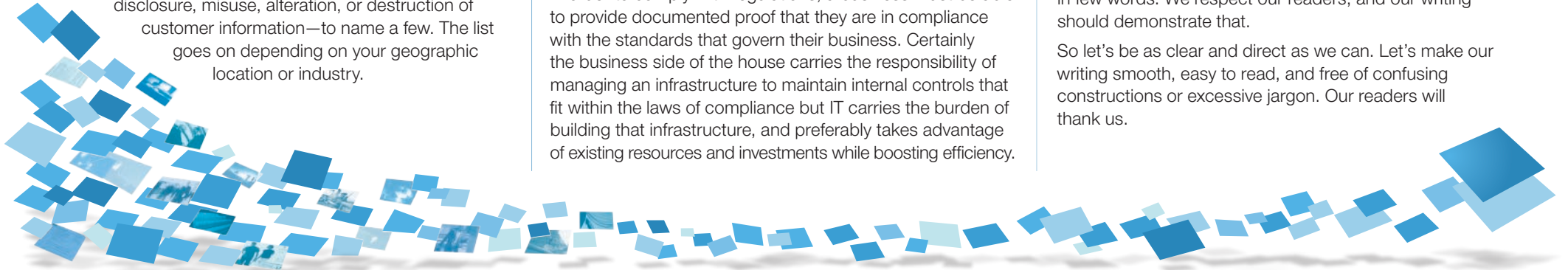
Each of these regulations requires enterprises to protect and control their flow of information. Some of these regulations hold not only the corporation, but individuals such as the CEO and CFO, personally responsible for compliance; they in turn are looking to their IT professionals for compliance planning and implementation. Failure to comply with the regulations can lead to stock price declines which marginalize the value of a company, can quickly lay waste to an organization's hard earned credibility, and can even lead to jail sentences.

In order to comply with regulations, a business must be able to provide documented proof that they are in compliance with the standards that govern their business. Certainly the business side of the house carries the responsibility of managing an infrastructure to maintain internal controls that fit within the laws of compliance but IT carries the burden of building that infrastructure, and preferably takes advantage of existing resources and investments while boosting efficiency.

## 1. Process control

Do you have control of the information in your documents when you manually send them through a fax machine? Think about control over who sees them, how they got there, and where documents are being delivered. Are you confident that information is being received by the right people? Fax server software acts as a centralized document delivery hub that integrates with CRM, document management, email, ERP, workflow, and other software applications you use to operate your business. Each step of the document delivery process is managed electronically with dialing and routing rules that control how and where faxes are sent and received. Information can be exchanged electronically, in real-time directly from your applications without manual intervention. This makes it easier for IT to manage, track, and control how information is disseminated within your organization and beyond your corporate walls. Voice is confident, friendly, informal, and to the point. We know we're busy, and our readers are just as busy. They're also mobile, connected, on the go. For those reasons, they appreciate it when we can say what we need to say quickly, in few words. We respect our readers, and our writing should demonstrate that.

So let's be as clear and direct as we can. Let's make our writing smooth, easy to read, and free of confusing constructions or excessive jargon. Our readers will thank us.



The information technology framework must include secure document delivery and receipt, document control, long-term storage, and auditing. So what are the top five considerations?

<b>Compliance Concern</b>	<b>Traditional Document Delivery Methods<sup>1</sup></b>	<b>Fax Server and Electronic Document Delivery Software</b>
<b>Process control</b>	Manual decentralized processes and paper-handling; limited ability to control and manage who, how, and where documents are sent	Centralized document delivery hub; each step of the document delivery process is managed electronically.
<b>Information integrity</b>	Paper-based documents are easy to alter as is standard email.	Electronic documents are delivered as unalterable image-based PDF or TIF documents via a secure PSTN.
<b>Privacy</b>	Manual paper-based routines expose documents to view by unauthorized people.	Outbound documents sent electronically directly from business applications to the intended recipient with confirmed delivery; inbound documents can be routed directly to the intended recipient.  Encrypted and certified delivery options offer an added layer of security.
<b>Tracking, reporting and audit trail</b>	Paper-based documents are easy to alter as is standard email.	Paper-based documents are easy to alter as is standard email.
<b>Storage</b>	Physical documents stored in filing cabinets, storage facilities, or not at all.	Electronic documents and metadata can be stored in secure fax repositories, databases, or document management systems.

<sup>1</sup> Traditional document delivery methods include: manual fax, postal delivery, overnight service and standard email

## 2. Information integrity

Determine what documents are outside the control of your computer systems and could raise your risk of noncompliance. Some examples include the following:

- Accounting documents such as purchase orders, purchase requisitions, proofs of delivery, order confirmations, and invoices
- All contracts such as customers, employees and vendors
- Employee paper-work such as nondisclosure agreements, insurance claims receipts, health claims and health records, human resource paperwork, and expense accounts
- Corporate documents such as stock trade confirmations, account statements, and bank statements

All of these documents are potential areas of security threat and pose a risk to your compliance, while a fax server can deliver documents as unalterable PDF or TIF images over a secure Public Switched Telephone Network (PSTN).

## 3. Privacy

Are you sure that your confidential information is kept private and do you have safeguards in place to prevent information tampering? One regulation requires businesses to obscure customer data which at its most basic level means keeping people from seeing what they're not supposed to see. Paper faxes are outside the control of your computer system and can be seen by anyone. Fax servers by design enhance security because they eliminate nonsecure, stand-alone fax machines and deliver documents in tamper-resistant formats. You know exactly who received the information with confirmed delivery and you can take advantage of your network's established Microsoft® Windows security system.



*“Desktop fax capabilities have been instrumental in helping us meet HIPAA guidelines. Faxes are delivered directly to the planned recipient’s computer which has built-in security policies, so we avoided the costly process of analyzing and securing all the stand-alone fax machines.”*

– MagnaCare (Healthcare)

For an added layer of protection some fax server software even offers encrypted and certified email delivery options that require passwords to access information, as well as provide electronic verification of receipt for better authentication. These features help diminish the risk of confidential information falling into the wrong hands.

#### 4. Audit trail

Do you have an audit trail of your corporate communications? Regulations dictate that businesses physically protect information and provide a history of what has happened

to the information and which people have had access to it. Among other functions, fax server software can track fax history, provide verification of fax delivery, assign access passwords, and route incoming faxes to individuals’ fax or email inboxes and be the on-ramp to automated workflows. Such features provide a deeper audit trail for protected documents to help satisfy tracking and reporting requirements. When a company uses fax server software, faxes are received directly to end-user mailboxes so paper doesn’t sit out in the open—a crucial requirement of HIPAA. Plus, once a fax has arrived in your inbox via a fax server, the document is tamper resistant and cannot be edited without that event showing up in the audit trail so there is no question of who accessed a document. This is especially important in industries that must undergo surprise inspections or audits.

And what about your MFPs? One of the biggest advantages of connecting a fax server to your MFP environment is the ability to track and keep history logs of documents scanned and routed from various capture devices. Also, bringing secure document routing technologies to the MFP allows users to scan and send images knowing that their communications are being logged and tracked.

#### 5. Storage

Physical documents are generally stored in file folders and filing cabinets. The problem with this type of storage is evident knowing what we do about control, privacy and audit trails. Fax Server software digitizes your documents and the associated metadata can be stored along with your documents in a secure repository. Do you use a document management system or database for long-term document storage? Fax server software can also integrate with these systems to meet your electronic document retention requirements.

#### [FaxSolutions.OpenText.com](http://FaxSolutions.OpenText.com)

**Sales** captaris.sales@opentext.com  
(800) 304-2727

**Support** support@opentext.com  
(800) 540-7292

[www.opentext.com](http://www.opentext.com)