Realtime
publishers

Controlling Costs, Improving Compliance, and Streamlining Integration with Managed File Transfer

The Essentials Series

sponsored by
Attachmate®

Dan Sullivan

Managing File Transfer and Improving Compliance 1

The Role of File Transfers in Compliance 1

Regulations that Impact File Transfer Operations 2

Common Requirements Across Regulations 3

Challenges to Complying with Regulations When Using Ad Hoc Custom Scripts 3

Efficiency Tips for Complying with Regulations 4

Advantages of a Using a Company-Wide File Transfer Solution 5

Summary 6

Copyright Statement

Managing File Transfer and Improving Compliance

Complying with regulations is a necessary part of business operations. Managing file transfers is also a necessary part of business operations. Not surprisingly, these two requirements intersect. In order to comply with regulations in an efficient manner, you have to understand different aspects of file transfer:

- The role of file transfers in compliance
- Efficient ways for managing file transfers
- Advantages of using a company-wide file transfer solution

The objective is to understand how you can leverage a managed file transfer solution to improve compliance while controlling costs associated with compliance.

The Role of File Transfers in Compliance

Compliance brings to mind several considerations: protecting the confidentiality of data, ensuring critical information is not tampered with, and demonstrating that you have proper controls in place. These are fairly high-level business process characteristics that can appear distant from the implementation details of file transfers. The way you manage file transfers can directly impact your ability to achieve and maintain compliance. To clearly outline the link between compliance and file transfer, it helps to consider:

- Regulations that might govern file transfer operations
- Common requirements across regulations
- Challenges to complying with regulations when using ad hoc custom scripts

Once these points have been elucidated, you can move on to considering how to meet compliance requirements with regards to file transfers.

Regulations that Impact File Transfer Operations

Many organizations are subject to government and industry regulations. Confidentiality, integrity, and availability of data and information are common themes in regulations. File transfer operations can directly impact the ability to ensure the confidentiality, integrity, and availability of data. Some of the best-known regulations require publically-traded companies, retail businesses, financial services companies, and healthcare providers to deliver specified levels of protection to their data. These regulations include:

- Sarbanes Oxley (SOX) Act
- Basel III
- Payment Card Industry Data Security Standard (PCI DSS)
- Gramm-Leach-Bliley Act (GLBA)
- Health Insurance Portability and Accountability Act (HIPAA)

SOX requires businesses to protect the integrity of data related to business performance. There are other requirements as well, but from a file transfer perspective, the key requirements relate to controls designed to prevent and detect fraud and control reporting procedures. Without proper controls on file transfer operations, for example, an unscrupulous employee could change a file transfer script to replace a legitimate data file with one that had been changed to misrepresent some aspect of business performance. Controls must be in place to mitigate the risk of this kind of tampering from succeeding.

Basel III governs risk management within the banking sector. In order to meet the direct requirements of this industry regulation, banks must be able to ensure the quality and integrity of their performance and risk data. As with SOX, Basel III regulations can impact how you implement file transfer operations.

PCI DSS establishes rules for businesses that process payment card data to ensure that personal and confidential data is not exposed to unauthorized individuals and to protect the integrity of payment card data. For example, one of the PCI DSS requirements is that payment card data must be encrypted when transferred over public networks such as the Internet.

The GBLA and HIPAA regulations both include rules governing the protection of private information. In the case of GBLA, this rule applies to financial services customers, and in the case of HIPAA, it applies to patients in healthcare settings. One of the recognized ways of protecting confidential data during transfers is to encrypt the data using strong encryption.

It is important to point out that not all encryption algorithms provide the same level of protection. Older algorithms, such as the Digital Encryption Standard (DES), were once accepted as standard but are no longer used because they are easily cracked today. Be sure to use strong encryption algorithms, such as the Advanced Encryption Standard (AES), in your file transfer operations in order to comply with today's standards.

Common Requirements Across Regulations

Regulations govern aspects of many kinds of businesses in a wide range of industries. At first, compliance across regulations might seem the start of an intractable problem: so many different regulations that it would be difficult to meet them with a reasonable set of controls and applications. Fortunately, such is not the case. There is substantial overlap between regulations because they frequently require similar best practices designed to:

- Preserve the integrity of data
- Protect the confidentiality of data
- Maintain the availability of data
- Provide audit history of the movement of protected data

You need to trust your data. Imagine if bank customers did not trust their statements, investors questioned quarterly reports, and doctors were not sure about the accuracy of medical records. Basic businesses and services we take for granted would be hampered. It should not be surprising to see data integrity requirements are common across so many regulations governing information technologies.

Confidentiality controls are designed to limit access to private data. The goal is to make sure data is not accessed by those that do not have a legitimate business reason to view or alter the data. Again, this type of requirement is common across regulations.

The availability of data is also an important factor in the areas subject to regulation. For example, when public companies file public reports about performance, it is important the financial officers who developed those reports have access to data needed to compile accurate reports.

In many ways, confidentiality, integrity, and availability of data are at the core of many regulations. Meeting these three requirements is not sufficient to meet certain regulations, however. In addition to protecting data as required, businesses must be able to *demonstrate* that they are in compliance. To do so, important operations, such as changes to data and data movements, are logged in audit trails.

Consider the depth of controls that must be in place for file transfer programs to comply with these typical types of requirements. Can your custom file transfer scripts meet compliance requirements?

Challenges to Complying with Regulations When Using Ad Hoc Custom Scripts

The fundamental difficulty with using ad hoc custom scripts for file transfers is that the cost and time required to develop a compliant script can be prohibitive. It is difficult to justify the investment required to make a file transfer script compliant with security best practices if it is used for a single file transfer operation or within a single department. A sufficient return on investment is realized only when such as file transfer solution can be used for multiple operations.

If you already have file transfer scripts in place and you want to assess how well they comply, consider whether these solutions:

- Use insecure protocols, such as ftp
- Use insecure authentication methods, such as hard-coded username and passwords mechanisms with passwords stored insecurely
- Fail to check file integrity after a transfer
- Fail to log sufficient details about transfers, so you cannot demonstrate the program performed checks to ensure integrity or used strong encryption to protect confidentiality of data

If you find your file transfer solutions lacking in one or more of these areas, you might want to revise these programs or replace them with a managed file transfer solution. If you choose to continue with custom scripts, you will assume responsibility to continue to maintain these scripts. This includes keeping up to date with vulnerabilities that might be discovered with programs and libraries used to implement the scripts. Developing file transfer solutions that comply with regulations is an area where there are clear economies of scale. In such situations, it might be to your advantage to consider a solution that can be applied throughout your organization.

Efficiency Tips for Complying with Regulations

A managed file transfer solution that has been designed and developed to comply with security best practices might be the most efficient way to meet your file transfer needs while achieving compliance in a cost-effective manner. Of course, not all managed file transfer solutions might fit your needs, so evaluate your options using a range of criteria:

- Security
- Reporting and logging
- Access controls

Security is a complex subject. For file transfer solutions, a sufficiently secure solution will provide protections for the confidentiality, integrity, and availability of your data. Look for solutions that support strong encryption. Also look for consistent levels of secure communication across multiple platforms, with particular attention to minimizing exposure of sensitive files in the DMZ.

Reporting and logging are essential for compliance. Evaluate the kinds of reports and alerts you can set up. You will want to be notified when a significant event occurs, such as a failure to confirm the integrity of a transferred file or the inability to transfer a critical file. The last thing you want is to babysit your file transfers because your file transfer solution does not provide adequate reporting about problematic events.

Consider how you will control access to file transfer jobs. If a file transfer solution allows you to create and configure jobs with an easy-to-use interface, virtually anyone in the business would have the skills to modify such configurations. Job configuration files should be protected with access controls so that only authorized individuals can change them.

Realize efficiencies from standardization. In particular, get the most from your file transfer solution by implementing company-wide standards for all transfers subject to regulation. This implementation could call for employing a set of standards that mirror the most stringent requirements among all those you are subject to. Balance the benefits of having a single strong set of requirements with the need to relax some requirements in some cases.

Part of the standardization effort should be defining policies and procedures governing key areas:

- Access to file transfer programs
- Logging and auditing
- Approvals for outbound transfers

When file transfer programs are written by in-house developers, there is a natural barrier to altering these scripts. If you don’t have the programming skills, you won’t be able to modify the scripts. Easy-to-use managed file transfer solutions lower the barrier to tampering and thus require well-established access controls.

Logging and auditing standards should be sufficient to meet requirements dictated by regulations. Standardizing on a single set of logging parameters might be more efficient than having multiple levels of logging for different applications.

As part of your policies and procedures, do not forget approval procedures. Who will decide whether it is acceptable to transfer data between departments or to outside business partners? The data transfer process might be trivial to implement but might also raise legal and regulatory issues that should be reviewed and approved in compliance with regulations.

Advantages of a Using a Company-Wide File Transfer Solution

There are clearly economies of scale for using a company-wide file transfer solution:

- Standardizing methods for implementing policies governing file transfer
- Reducing the number of programs that must be reviewed and audited to ensure compliance
- Improving return on investment for error handling, exception processing, logging, and reporting

A business can use a variety of ad hoc scripts for their file transfer needs. These various scripts can be brought into compliance. The only question is, at what cost? In addition to the initial development costs, there is ongoing maintenance, vulnerability assessments, and internal audits to ensure each of these solutions complies with regulations.

Summary

Compliance is a necessary part of business. File transfers might be far removed from the high-level strategic concerns of C-level executives, except when compliance is involved. Complying with multiple regulations is difficult. Implementing robust, scalable, and dependable file transfer solutions is difficult. The addition of *compliant* to that list of features increases the cost of implementing custom solutions. A managed file transfer solution might be a better option, but you need to evaluate such a solution based on the criteria outlined here. In addition, keep in mind the benefits of implementing an organization-wide solution.