WHITE PAPER

MANAGED FILE TRANSFER:

10 STEPS TO SECURITY AND COMPLIANCE

01 | OVERVIEW

Do you want to design a file transfer process that is secure? Or one that is compliant? Of course, the answer is “both”. But it’s not always easy to meet that objective.

Good business practice dictates data protection for you, your customers, and your business partners – including data-in-motion. But, even the best security practices do not alleviate the need to demonstrate compliance with a variety of regulations and standards that can carry high contractual, civil, and criminal penalties. Plus, the indirect loss of faith of your customers or business partners can have an incalculable impact on your bottom line.

Most organizations require that all file transfers are secured. In addition, they may need to comply with mandates, such as SOX (Sarbanes-Oxley Act), HIPAA (Healthcare Insurance Portability and Accountability Act)/HITECH (Health Information Technology for Economic and Clinical Health Act), and PCI DSS (Payment Card Industry Data Security Standard).

Often popular secure protocols, such as SSL or SSH, are used when data is transmitted outside the corporate firewall to customers, business partners, or other departments. Although secure protocols support a secure and compliant file transfer process, they are only one component in ensuring that your security goals are met. Delivering security and compliance with your file transfer process requires a Managed File Transfer solution to ensure that your data is protected at all times.

Coviant Software offers Diplomat MFT, a suite of Managed File Transfer products that secure data-in-motion and improve compliance with industry and government mandates. Diplomat MFT brings together the security and workflow management features that IT and security professionals need in an easy to implement, costeffective Managed File Transfer solution for automating your secure file transfer process.

Knowing whether your file transfer process complies with regulations and standards can be difficult. Many regulations are based on objectives. You need to interpret these objectives and create an action plan to design a secure file transfer solution that meets them.

This white paper helps IT and security professionals who need to successfully implement and manage file transfer processes that meet both compliance and security mandates. First, the 10 practical steps to automate your secure file transfer process are detailed. The paper then reviews the sections of SOX (based on the COBIT framework), HIPAA/HITECH, and PCI DSS that relate to secure file transfer processes and how the 10 steps can meet the control objectives in each security standard and regulation.

Although secure protocols support a secure and compliant file transfer process, they are only one component in ensuring your security goals are met.

02 | 10 STEPS TO SECURE FILE TRANSFER

STEP 1: CREATE A SECURE CONFIGURATION

Secure file transfer requires a solution that spans the corporate firewall. One part of the solution, such as a secure FTP or web server, is located outside the firewall and acts as a temporary repository for files being transferred between business partners or other entities. Another part of the solution, such as a Managed File Transfer solution, resides in a secure location inside the corporate firewall and manages file transfers to and from the FTP server. Secure FTP servers are popular among business partners that want to standardize on non-proprietary solutions. To ensure file transfer security, only the secure FTP server should be outside the internal firewall and a Managed File Transfer solution, such as Diplomat Transaction Manager, must be safely inside the internal firewall.

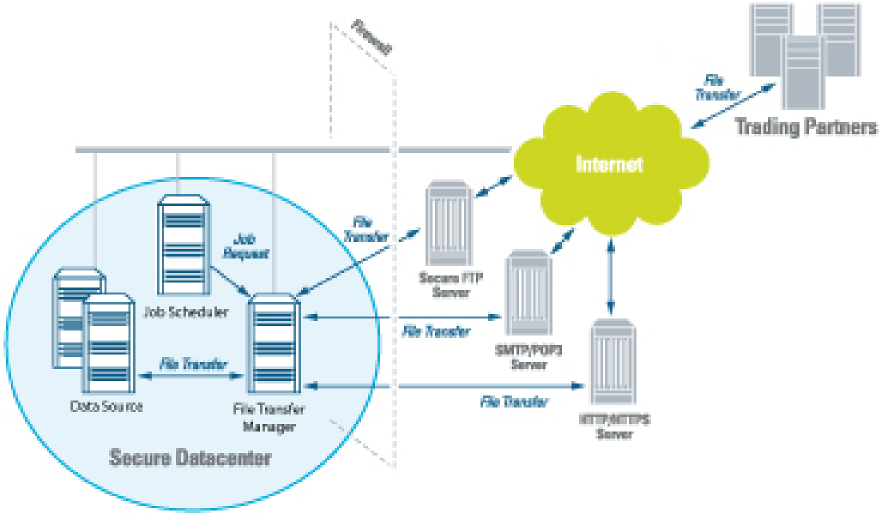

FIG. 1 – SECURE FILE TRANSFER CONFIGURATION

STEP 2: CONTROL ACCESS

Control access to your file transfer solution. Both the FTP or web server and the Managed File Transfer software must be designed and implemented to limit and monitor access when setting up file transfers and when file transfer jobs are run. Limiting users, tasks, and data accessibility prevents unintended errors and makes it more difficult for outsiders to successfully breach your file transfer solution.

Set up access controls during the implementation of your Managed File Transfer solution to:

Protect internal communications. Most administrative consoles for FTP or web servers and Managed File Transfer software use client connections to communicate when setting up file transfer tasks. These client connections should be encrypted with SSL or other secure protocol.

Encrypt access data. File transfer solutions should always encrypt sensitive data at rest and only decrypt it as needed, such as when the application is started or when file transfer jobs are executed. Encryption of user IDs, accounts, passwords, and encryption pass phrases prevents unintended use of the access information. Be careful to avoid file transfer applications that store data in plaintext, such as batch files or registry entries.

Create unique user accounts. Any user uploading or downloading files from your FTP or web server needs to be uniquely identifiable with a user ID and password. Disable anonymous connections. Require complex alphanumeric passwords that must be updated at least every 90 days. Having individual accounts for each of your business partners or other internal groups means you can swiftly shut down accounts in the event of a possible security breach.

Limit privileges on accounts. Each new FTP or web server account creates a potential point of access to your secure file transfer solution. When setting up new accounts, strictly limit privileges based on the precise needs of each user. Restrict access to only one default directory for each account. Restrict read, write, and delete privileges based on whether the user will be sending or receiving files from your server. If possible, restrict access to a limited set of IP addresses.

Terminate inactive sessions. Each unattended administrative logon and each FTP or web session can create easy access to secure file transfer management software, as well as to data on FTP servers. Each logon should be set to automatically terminate after a specified period of time.

STEP 3: AUTOMATE TRANSFERS

Automate file transfers to reduce errors and limit access to sensitive information. A file transfer solution must allow you to run jobs on an automated schedule using the job scheduler of your choice. You need the flexibility to use an internal scheduler that comes with the file transfer solution, a system scheduler (e.g., Windows Scheduler), or a scheduler in a separate application to kick off file transfer jobs that integrate with your business workflow.

Running jobs automatically means that you can eliminate the hit-and miss execution of file transfer jobs using a manual process. Jobs run on time. Plus, the correct encryption key and logon information eliminate the possible introduction of a variety of security errors into the file transfer process.

Automated job execution means that users do not need to know sensitive access information, such as user names, passwords, and pass-phrases. Each manual intervention required to complete a secure file transfer creates an opportunity for user error and for capture of sensitive passwords or pass-phrases. Look for file transfer solutions where access information can be entered once and used as needed at run-time.

Automate file transfers to reduce errors and limit access to sensitive information.

STEP 4: AUTHENTICATE USERS AND PROCESSES

Require user authentication. User authentication ensures that only a limited number of known users with unique privileges can access your file transfer solution. Linking authentication to each user's network or local logon identity both simplifies user authentication with a single sign-on and strengthens security by ensuring that only named users have access to file transfer set-up tasks.

Track all user activity. A file transfer solution must capture user activity data each time file transfer set-up data is changed. Knowing when file transfer set-up data was changed and who changed it provides an audit trail that simplifies the tracking and correction of problems.

Authenticate all processes making file transfer requests. When an automated process initiates a file transfer job, the process must be authenticated much like a user might need to log into an application to manually encrypt, sign, and transfer a file. Any file transfer solution needs to authenticate job processes that attempt to initiate file transfer jobs. A process that requests a file transfer job be run can be authenticated with a password, user ID of the process making the request, or other authentication methods.

User authentication ensures only a limited number of known users have access to your managed file transfer solution.

STEP 5: ENCRYPT FILES

Encrypt all files before they leave the corporate firewall. Data files should be encrypted in a secure area before transfer to an FTP or web server in the DMZ. Using secure transmission protocols only protects data in transit. As soon as files are at rest on a server in the DMZ, they are vulnerable to attack. Some FTP servers offer data encryption, but these solutions can create a security loophole by waiting until files are in an internet-accessible location before encryption.

Select a solid, widely-used encryption standard, such as OpenPGP. OpenPGP is one of the oldest public key encryption technologies. Because of its popularity, many users spend time attempting to find vulnerabilities in it. And, when vulnerabilities are found, they are rapidly addressed.

Use good encryption practices. Strong encryption algorithms are important, but good encryption practices are equally valuable in decreasing the possibility of a file being breached. Create the minimum number of keys required to meet your business needs. If you select OpenPGP for file encryption, you have the option of using multiple encryption sub-keys with consecutive validity periods. Each new encryption sub-key provides the same security as creating a new key pair without the administrative hassle of sending a new public key to your business partners. When you create a new OpenPGP key pair set up multiple encryption sub-keys that are valid for short intervals, such as a year or less.

STEP 6: SIGN AND VERIFY FILES

Sign and verify files to ensure integrity and non-repudiation. Sign all outbound data files and check for valid signatures on all inbound files. Signing and verification are the best way to guarantee non-repudiation of origin and to ensure decrypted files are safe to process. Verifying signatures on every file ensures that the files you receive have not been altered during transit and confirms the identity of the sender. With an encryption standard like OpenPGP, a signature is created and affixed to a file before it is encrypted in preparation for outbound transmission. The private key of the sender is used to create the signature.

Without a signature, a recipient has no way to determine the sender of the file. When the file is received, the file is decrypted and the signature can be examined before the file is processed. Signatures are used to determine the sender of the file – as only the public key of the sender can successfully verify a signature. If the signature verification fails, then the file should not be processed.

Signatures verify the integrity of files. Part of the signature contains a hash of the original file. As part of the signature verification process, the hash is recalculated using the decrypted file and compared to the hash in the original signature attached to the file. Matching hashes mean that the file has not been altered since the signature was attached. In other words, the integrity of the decrypted file has been confirmed and it is safe to be processed.

Sign and verify files to ensure data integrity and non-repudiation of origin.

STEP 7: USE SECURE PROTOCOLS

Use secure transmission protocols to protect logon data and add an extra layer of protection to encrypted files being transferred.

Secure protocols protect logon data during each user access. File encryption protects your data, but does not protect the logon data used to access an FTP or web server. Secure protocols establish a secure connection with an FTP or web server before sending the logon data used to authenticate a user, such as usernames, passwords, and keys. If attackers capture logon data, they can initiate other file transfer jobs and potentially transmit files with malicious content.

Without secure transmission protocols, an encrypted file can be captured intact during transit. Once the encrypted file is in their possession, attackers can work on decrypting the file at their leisure. Using a secure protocol provides an additional layer of encryption that must be penetrated before a file is compromised.

STEP 8: ARCHIVE ENCRYPTED FILES

Encrypt data files with your own master key before archiving. Archived files can be essential component in providing the business a record of information that has been transferred. These archived files need to be equally as secure as the files that were transferred. Archival of encrypted files provides protection in case of an internal security breach, but you must be able to decrypt the archived files when they are needed. Encrypting archival copies of files to your own master key before storing in a secure location creates a repository of secure files that are safe and meet your business needs.

Don’t keep archive files that you can't decrypt. When you are encrypting files to be sent to your business partners, you use their public key. You will not be able to decrypt these encrypted files unless you also encrypt them with your own master key.

Use audit data strategically to demonstrate comprehensive data security and regulatory compliance.

STEP 9: CAPTURE AUDIT DATA

Capture audit data to demonstrate regulatory and internal audit compliance. Audit data can be used strategically to demonstrate regulatory compliance or tactically to confirm to a business partner the encryption key and destination location used by a specific file transfer job.

Proving that you have a secure file transfer process can be an arduous task. Audit data needs to be both comprehensive and easy to analyze. Your file transfer solution needs to capture extensive data in a standard format, such as a SQL database. Two types of audit data are critical:

Job and file data. Detailed information on each file transfer job and each file transferred can demonstrate that secure procedures, such as encrypting files before transfer and use of secure transmission protocols, were used for each file transferred.

User activity data. Data on who accessed your file transfer solution is equally as important. If files were transferred incorrectly, questions of who may have set up or updated the file transfers may become critical.

The integrity of audit data must also be ensured. If you capture audit data into files, limit the user identities that are allowed to write, alter, or delete audit files. If you use database technology, such as SQL, limit write access to the audit tables to the identity used by the file transfer management software.

03 | SECURITY STANDARDS AND REGULATIONSX

Creating a secure file transfer process does not always guarantee that all regulations and standards will be met. Mandates, like SOX, HIPAA/HITECH, and PCI DSS, are intended to protect the privacy and security of data. Each covers a wide range of control objectives. Only some of which are pertinent when designing and implementing a managed file transfer solution. The next sections identify the portions of each mandate that affect file transfer security and how the 10 Steps to Managed File Transfer can meet those mandates.

STEP 10: MONITOR FILE TRANSFERS

Monitor file transfer jobs to rapidly identify potential security problems. Automating file transfer jobs does not guarantee that no issues will arise at run-time. Your file transfer solution needs to provide real-time information. A job not running on schedule or taking too long to complete may signal a security problem.

When a file transfer job fails, the support person responsible for the job needs to be alerted as soon as possible. Email and/or paging notifications need to be sent, including the information (e.g., log entries) needed to diagnose and correct the problem.

If a security breach occurs unrelated to a file transfer (e.g., an FTP server or encryption key has been compromised), the specific file transfer jobs affected may need to be suspended until the security breach has been corrected.

Creating a secure file transfer process does not always guarantee that all regulations and standards will be met.

DS5 ENSURES SYSTEMS SECURITY

FIG. 2 – COBIT DELIVERY AND SUPPORT CONTROL OBJECTIVES

	DS5.3 Identity Management	**DS5.5 Security Testing, Surveillance**	**DS5.6 Security Incident Definition**	**DS5.7 Protection of Security Technology**	**DS5.8 Cryptographic Key Management**	**DS5.10 Network Security**	**DS5.11 Exchange of Sensitive Data**
	Ensure that all users and their activity on IT systems are uniquely identifiable. Enable user identities via authentication mechanisms … Maintain user identities and access rights in a central repository … Establish user identification, implement authentication and enforce access rights.	Test and monitor the IT security implementation in a proactive way …A logging and monitoring function will enable the early prevention and/ or detection and subsequent timely reporting of unusual and/or abnormal activities that may need to be addressed.	Clearly define and communicate the characteristics of potential security incidents so they can be properly classified and treated by the incident and problem management process.	Make security related technology resistant to tampering, and do not disclose security documentation unnecessarily.	Determine that policies and procedures are in place to organize the generation, change, revocation, destruction, distribution, certification, storage, entry, use and archiving of cryptographic keys to ensure the protection of keys against modification and unauthorized disclosure.	Use security techniques and related management procedures (e.g., firewalls, security appliances, network segmentation, intrusion detection) to authorize access and control information flows from and to networks.	Exchange sensitive transaction data only over a trusted path or medium with controls to provide authenticity of content, proof of submission, proof of receipt and non-repudiation of origin.
10 STEPS TO SECURE FILE TRANSFER IMPLEMENTATION							
1. Secure configuration	●					●	
2. Control access	●					●	
3. Automate transfers				●		●	
4. Authenticate users/ processes	●			●			
5. Encrypt files					●		●
6. Sign and verify files							●
7. Use secure protocols							●
8. Archive encrypted files							
9. Capture audit data		●					
10. Monitor file transfers		●	●				

3.1| MEETING SOX ANDATES (USING COBIT FRAMEWORK)

The Sarbanes-Oxley Act mandates that all publicly-traded organizations demonstrate due diligence in the disclosure of financial information. Each organization must also implement internal controls and procedures to protect financial data from unauthorized access, including access that could occur through file transfers. Developed by the IT Governance Institute, the COBIT (Control Objectives for Information and related Technology) control objectives is an open framework that is often used to design IT controls to comply with the Sarbanes-Oxley Act.

The COBIT framework is based on four domains containing 34 IT processes and over 300 detailed control objectives. The primary processes of interest to IT organizations selecting and implementing secure file transfer solutions are in the Delivery and Support (DS) domain. The pertinent control objectives for secure file transfer are primarily under DS5 Ensure Systems Security. Control objectives that are most relevant to secure file transfer are shown above in **FIG. 2**. Complete documentation on the COBIT framework and process can be found at http://www.itgi.org.

FIG. 2 – HIPAA §164.312 TECHNICAL SAFEGUARDS

	a)(1) Access Control	a)(2)(i) Unique User Identification	(a)(2)(iii) Automatic Logoff	(a)(2)(iv) Encryption And Decryption	(b)(1) Audit Controls	c)(1) Integrity	(c)(2) Authenticate Electronic Protected Health Information	(d) Person or Entity Authentication	(e)(1) Transmission Security	(e)(2)(i) Integrity Controls	(e)(2)(ii) Encryption
	Allow access only to those persons or software programs that have been granted access rights.	Assign a unique name and/or number for identifying and tracking user identity.	Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.	Implement a mechanism to encrypt and decrypt electronic protected health information.	Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.	Property that data or information have not been altered or destroyed in an unauthorized manner.	Implement electronic mechanisms to corroborate that electronic protected health information has not been altered or destroyed in an unauthorized manner.	Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed.	Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network.	Implement security measures to ensure that electronically transmitted electronic protected health information is not improperly modified without detection until disposed of.	Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate.
10 STEPS TO SECURE FILE TRANSFER IMPLEMENTATION											
1. Secure configuration	●										
2. Control access	●	●	●								
3. Automate transfers	●										
4. Authenticate users/ processes	●							●			
5. Encrypt files				●							●
6. Sign and verify files						●	●			●	
7. Use secure protocols									●	●	
8. Archive encrypted files	●			●							
9. Capture audit data					●						
10. Monitor file transfers					●						

3.2 | MEETING HIPAA/HITECH TECHNICAL SAFEGUARDS

The Health Insurance Portability and Accountability Act of 1996 established national standards for the security of electronic health care information with both civil and criminal penalties for noncompliance by covered entities, such as hospitals or physician practices. The HITECH Act of 2009 extended these penalties beyond covered entities to their business associates and established more rigorous enforcement policies.

The HIPAA Security Rule in §164.312 defines the technical safeguards required to protect and control access to patient data. **FIG. 3**. above identifies the relevant security standards in HIPAA §164.312 and the related specifications that are necessary to protect data-in-motion. You can find out more about HIPAA technical safeguards at http://www.cms.hhs.gov/HIPAAGenInfo.

FIG. 4 – PCI DSS REQUIREMENTS (CONTINUED NEXT PAGE)

	1: Install and maintain a firewall configuration to protect cardholder data.	**2: Do not use vendor-supplied defaults for system passwords and other security parameters**	**3: Protect stored cardholder data.**
	1.1 Require firewall between DMZ and internal network **1.2** Restrict connections between untrusted networks and internal network **1.3** Prohibit public access between internet and internal network **1.3.7** Place cardholder data in internal network, segregated from DMZ	**2.2.2** Enable only necessary and secure services, protocols.... **2.3** Encrypt all non-console administrative access using strong cryptography	**3.4** Render PAN (Primary Account Number)) unreadable when stored **3.5** Protect cryptographic keys **3.6** Fully implement key-management procedures, including....Generation of strong keys. Periodic changing of keys.
10 STEPS TO SECURE FILE TRANSFER IMPLEMENTATION			
1. Secure configuration	●		
2. Control access		●	
3. Automate transfers			
4. Authenticate users/ processes			
5. Encrypt files			●
6. Sign and verify files			
7. Use secure protocols			
8. Archive encrypted files			●
9. Capture audit data			
10. Monitor file transfers			

3.3 | MEETING PCI DSS REQUIREMENTS

The PCI DSS (Payment Card Industry Data Security Standard) is an assessment tool for use during compliance audits. It is intended to enhance payment account data security and help organizations proactively protect customer account data. It was developed and is maintained by the major credit card companies through the PCI Security Standards Council and helps facilitate the broad adoption of consistent data security for credit card data. Each entity that has a contractual relationship with credit card companies, financial institutions, and their agents must provide appropriate compliance validation documentation.

The original PCI Data Security Standard became effective in September 2008. An updated PCI DSS Version 2.0 was released in November 2010. The updated version provides additional guidance to explain the intent of the 12 major requirements. The complete PCI DSS can be found at https://www.pcisecuritystandards.org,, including a summary of the changes in Version 2.0.

4: Encrypt transmission of cardholder data across open, public networks.	**7: Restrict access to cardholder data by business need-to-know.**	**8: Assign a unique ID to each person with computer access.**	**10: Track and monitor all access to network resources and cardholder data.**	**12: Maintain a policy that addresses information security for all personnel**
4.1 Use strong cryptography and security protocols		**8.1** Assign all users unique ID **8.2** Authenticate all users **8.4** Render stored passwords unreadable **8.5.3** Change passwords at first use **8.5.9** Change passwords every 90 days **8.5.11** Use passwords with numeric and alpha characters **8.5.15** Require re-authentication if idle more than15 minutes	**10.1** Establish process for access to system components for each user **10.2** Implement automated audit trails **10.3** Record at least user ID, event type, date, time....for each event	**12.5.2** Monitor and analyze security alerts **12.9** Implement an incident response plan
		●		
	●			
		●		
●				
●				
			●	
				●

The PCI DSS is multifaceted security standard that includes requirements for security management, policies, procedures, network architecture, software design and other critical protective measures. These security requirements apply to all system components, including file transfer applications that handle credit card data. **FIG. 4**, above, illustrates the major requirements and the specific implementation standards for each requirement that pertain to a Managed File Transfer solution.

Secure File Transfer Implementation	SOX (CobiT Delivery and Support Control Objectives)	HIPAA Technical Safeguards	PCI DSS Major Requirements
1. Secure configuration	DS5.3 Identity Management DS5.10 Network Security	a)(1) Access Control	REQ 1: Install and maintain a firewall configuration (1.1.3, 1.2, 1.3, 1.3.7)
2. Control access	DS5.3 Identity Management DS5.7 Protection of Security Technology DS5.10 Network Security	(a)(1) Access Control (a)(2)(i) Unique User Identification (a)(2)(iii) Automatic Logoff	REQ 2: Do not use vendor-supplied defaults (2.2.2, 2.3) REQ 8: Assign a unique ID to each person with computer access (8.1, 8.4, 8.5.3, 8.5,11, 8.5.15)
3. Automate transfers	DS5.10 Network Security	(a)(1) Access Control	REQ 7: Restrict access to cardholder data by business need-to-know
4. Authenticate users/ processes	DS5.3 Identity Management	(a)(1) Access Control (d) Person or Entity Authentication	REQ 8: Assign a unique ID to each person with computer access (8.2)
5. Encrypt files	DS5.8 Cryptographic Key Management DS5.11 Exchange of Sensitive Data	(a)(2)(iv) Encryption And Decryption (e)(2)(ii) Encryption	REQ 3: Protect stored cardholder data (3.5, 3.6)
6. Sign and verify files	DS5.11 Exchange of Sensitive Data	(c)(1) Integrity (c)(2) Authenticate Electronic Protected Health Information (e)(2)(i) Integrity Controls	REQ 4: Encrypt transmission of cardholder data across open, public networks (4.1)
7. Use secure protocols	DS5.11 Exchange of Sensitive Data	(e)(1) Transmission Security (e)(2)(i) Integrity Controls	REQ 4: Encrypt transmission of cardholder data across open, public networks (4.1)
8. Archive encrypted files		(a)(1) Access Control (a)(2)(iv) Encryption And Decryption	REQ 3: Protect stored cardholder data (3.4)
9. Capture audit data	DS5.5 Security Testing, Surveillance and Monitoring	(b)(1) Audit Controls	REQ 10: Track and monitor all access to network resources and cardholder data (10.1, 10.2, 10.3)
10. Monitor file transfers	DS5.5 Security Testing, Surveillance and Monitoring DS5.6 Security Incident Definition	(b)(1) Audit Controls	REQ 12: Maintain a policy that addresses information security for all personnel (12.5.2, 12.9)

04 | BRIDGING SECURITY AND COMPLIANCE

Security drives compliance. When you automate a secure file transfer process using the 10 Steps to Managed File Transfer, you can also demonstrate compliance with the objectives in SOX, HIPAA/HITECH, and PCI DSS. Although each regulation and standard may emphasize different aspects of security, implementation of the practical steps outlined above ensures coverage of the pertinent objectives in each mandate.

FIG. 5, above, summarizes the relationships between the steps to automate a secure file transfer process and SOX, HIPAA/HITECH, and PCI DSS.

05 | SUMMARY

Both security and compliance are essential to smooth operations and business continuity. Developing a Managed File Transfer implementation can also meet the key objectives that are critical for compliance with industry mandates, such as SOX, HIPAA/HITECH, and PCI DSS. Focus on **10 PRACTICAL STEPS** to meet your security and compliance needs:

STEP 1: Secure configuration

STEP 2: Control access

STEP 3: Automate transfers

STEP 4: Authenticate users and processes

STEP 5: Encrypt files

STEP 6: Sign and verify files

STEP 7: Use secure protocols

STEP 8: Archive encrypted files

STEP 9: Capture audit data

STEP 10: Monitor file transfers

Coviant Software offers Diplomat Transaction Manager, a suite of Managed File Transfer products that secure data in transit and improve compliance with industry and government mandates.

WHITE PAPER

ABOUT COVIANT SOFTWARE

Coviant Software delivers secure file transfer management products that secure data in transit and improve compliance with industry and government mandates. Built on open technologies, such as OpenPGP encryption, SFTP, and SQL, Coviant's Diplomat MFT platform is an easy-to-implement, cost-effective solution for automating your secure file transfer process.

5804 Babcock Rd / Suite 151 / San Antonio, TX 78240 /
210.985.0985 / info@coviantsoftware.com/
www.coviantsoftware.com