1. 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 transit. 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), 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 careful design to ensure that your data is protected at all times.

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

Coviant® Software offers Diplomat® Transaction Manager, a suite of file transfer management products that secure data in transit and improve compliance with industry and government mandates. Diplomat Transaction Manager brings together the security and workflow management features that IT and security professionals need in an easy to implement, cost effective 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, 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, 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.