

The eGuide to
Data Movement and Governance:

Helping Business Professionals
Stay Up to Speed



If you find this eGuide helpful, please share it with colleagues.

Table of Contents

Introduction	3	Integration with Common Security Infrastructure	23	Chapter 5: Making Capabilities Work for You	41
Chapter 1: Building on Basics	4	Active Directory, LDAP	24	Use What you Learn	41
Data Movement	5	Key and Certificate Store.....	25	About Sterling Commerce	42
Managed File Transfer.....	6	Key Points to Remember.....	26	Appendix: Regulations You Should Know	43
Governance.....	7	Chapter 3: Governance for Outbound Data Movement	27		
Key Points to Remember.....	8	Encryption	28		
Chapter 2: Governance for Inbound Data Movement	9	Ad hoc Transfer Support	29		
Defense In Depth	10	Data Loss Prevention.....	30		
Multi-Factor Authentication.....	11	Key Points to Remember.....	31		
Multi-Zone DMV	12	Chapter 4: Visibility for Data Movement Inside and Outside	32		
Session Break.....	13	Centralized Provisioning.....	33		
Protocol Inspection.....	14	Notifications	34		
Audit Controls	15	Policy Enforcements	35		
Reporting.....	16	SLA Based Monitoring.....	36		
Monitoring	17	Integration Into Other Systems Management Tools	37		
Delivery Receipt.....	18	Centralized Provisioning for All New Connections	38		
Smart Automation Processes	19	Outsourcing and Third Party Managed Services	39		
Virus Scanning	20	Key Points to Remember.....	40		
Deleting of Processed Files	21				
Checkpoint/Restart.....	22				

Knowledge of data movement and governance principles can help you help your business stay competitive.

Introduction

You think you know all you need to know about data movement—after all, it's just about sending files, something you do routinely every single day. Really, how critical can it possibly be? And then it happens.

You fail an audit. Or customer information is compromised. Or you are called on the carpet for failing to meet a critical customer SLA. At that point you realize just how important it is to your organization and to your career. How do you prepare for that moment? More importantly, how do you prevent it from happening in the first place?

It is absolutely critical that you understand the possible consequences of a failure to properly monitor, control, and protect the movement of data. Missed opportunities and lost revenue might be the least of your worries. In some cases, poor practices can lead to lawsuits, fines, and even the failure of the business itself.

The purpose of this eGuide is to help you grasp the measures that can keep your organization on track to meet objectives and in line with regulations. What's more, it's your chance to become more effective in your job and build the confidence to bring valuable suggestions to your security department. You have a lot to gain.

Ready to get moving?

Chapter 1: The Basics



Since many who are reading this eGuide regularly work with managed file transfers, we can keep this chapter short and sweet. For those of you who are completely new to the subject matter, we'll start with three basic terms:

- **Data Movement**
- **Managed File Transfer**
- **Governance**

Data Movement

Data Movement is more than just file transfer, and it is vitally important to every organization. That's why it is targeted for tighter governance.

Data Movement refers to the transfer of files or information that can be critically important to all stakeholders in your organization: employees, suppliers and everyone you do business with.

Business professionals handle all types of data. And depending on your particular role, you might have a different idea of what it's all about. For example, an employee in data transmission might view it simply as a batch transfer. People in business-to-business integration could view it in terms of EDI. And the average knowledge worker might think only of huge e-mail files. All of these tasks are important—and all of them, to one degree or another, should be subject to **governance**.

Chapter 1: The Basics **Managed File Transfer**

Managed File Transfer, or MFT, is a category of solutions to securely and reliably facilitate data movement.

MFT solutions provide a single framework for taking care of all corporate file transfers, no matter the protocol. They can handle FTP (File Transfer Protocol), FTPS (FTP over SSL), SFTP (Secure File Transfer via SSH), SCP (Secure Copy via SSH), HTTP/S and specialized protocols like PeSIT and Connect:Direct.

What's more, MFT solutions support auditing, reporting, and policy features that are needed to comply with a growing array of government regulations.

Governance

Industry, state and federal regulatory requirements have a strong impact on corporate governance ... the right solutions can help you stay in compliance and reduce cost.

Corporate governance is the set of policies and processes that comply with regulations and laws. All of these affect the way an organization is administered or controlled. In terms of Information Technology, governance relates to the structure, oversight, process and controls that help ensure that data is handled properly.

State and Federal regulations related to customer data privacy and audit-ability of data movement include the following:

- **Graham Leach Bliley Act (GLBA)**
<http://www.glba-guide.com/index.htm>
- **Sarbanes-Oxley (SOX)**
<http://www.soxlaw.com/>
- **Federal Financial Institutions Examination Council (FFIEC)**
<http://www.ffiec.gov/>
- **Payment Card Industry Data Security Standards (PCI DSS)**
<https://www.pcisecuritystandards.org/index.shtml>
- **Personal Information Protection and Electronic Documents Act**
http://www.priv.gc.ca/legislation/02_06_07_e.cf
- **Massachusetts Privacy Law 201 CMR 17.00**
<http://www.mass.gov/Eoca/docs/idtheft/201CMR1700reg.pdf>

Key Points to Remember

Data Movement

Data Movement is a critical consideration for all stakeholders, one which is subject to increasing regulation by government at all levels.

Managed File Transfer

Managed File Transfer solutions handle all types of file transfers and can help users comply with corporate and government rules.

Governance

Governance relates to the structure, oversight, process, and controls that help ensure that data is handled properly.



Chapter 2: Governance for Inbound Data Movement

This chapter looks at the factors to be considered with the movement of data that is inbound to your organization.

The main topics covered are:

- **Defense in Depth**
- **Audit Controls**
- **Smart Automation Processes**
- **Virus Scanning**
- **Integrity Checking**
- **Deleting of Processed Files**
- **Integration with Common Security Structure**

Defense In Depth

Different security products may be deployed to defend a variety of potential threats within the network. Defense in Depth is also known as a “layered approach.”

It’s not surprising that so many IT terms have derived from the military, and Defense in Depth is a perfect example.

Defense in Depth, also called a “layered approach,” is the use of multiple layers and diverse types of security measures to protect both the individual system components and the system as a whole.

An example would be the anti-virus software installed on individual workstations, when there is already virus protection on the firewalls and servers within the same environment.

We will look at four specific components that are used in providing Defense in Depth for managed file transfer:

- **Multi-Factor Authentication**
- **Multi-Zone DMZ**
- **Session Break**
- **Protocol Inspection**

Learn how a proxy can help [here](#).

Multi-Factor Authentication

“By definition, true multifactor authentication requires the use of solutions from two or more of the three categories of factors.”

– American Federal Financial Institutions
Examination Council (FFIEC)

Multi-factor authentication is a way of protecting access to something, such as a bank account or a building, by requiring a user to produce more than one means of identification. The more factors required, the more secure the access.

True multi-factor authentication involves different methods of identifying a user. For example, to get money from an ATM the user must: 1) insert a card and 2) enter a PIN. The user is authenticated in two distinct ways.

In a system-to-system use case, such as you’d find at work, examples of authentication would include a certificate, a username/password and a USB token generated pin.

Two of the three authentication factors recognized and recommended by the [U.S. Federal Financial Institutions Examination Council \(FFIEC\)](#) are:

- **Data** such as a password or a PIN, something the user knows
- **Objects** such as a key or a magnetized card, something the user has

The third type of authentication, biometric characteristics, such as fingerprint or retina scan (something the user is), is not used in system-to-system applications, so we will not address it here.

Multi-Zone DMZ

A DMZ, in military terms, is an unprotected or semi-protected area between opposing military forces.

In computer terms, a DMZ is a buffer zone that enhances security between a trusted computer network and outside influences such as Internet hackers.

The DMZ itself protects the internal computer network from being compromised by attacks from outside, and the existence of multiple zones within the DMZ means that if one DMZ zone is compromised, the others are not.

In a multi-zone DMZ, each of the zones has its own unique security measures, such as credentials being stored in a different DMZ from the servers.

Learn more about DMZ issues [here](#).

Does your organization deploy multi-zone DMZ protection?

Session Break

A computer network security system will force a session break between a targeted user and an attacker immediately upon the discovery of an attempted hostile intrusion.

For security purposes, a session break is the intentional and automatic disconnection between a user's network and an attacker. It is a way to check credentials before the actual contact is made with the server.

Think of it as the activity where passports are examined at security checkpoints before passengers board a plane.

Many companies do not yet deploy some type of DMZ-based security application, so their sessions are at risk. Companies that recognize the threat are taking an additional step to prevent that from happening in first place. They do this by deploying a DMZ- based proxy application that doesn't even establish a session until it authenticates the credentials of the sender.

Learn more about Session Break issues [here](#).

At what point does your network security system force a session break?

Chapter 2: Governance for
Inbound Data Movement

“As the name implies, a protocol, regardless of the context, is a set of rules or ways to do things ... There are applications that do not conform to the protocols as the designers intended. This non-conformity may be a mistake, or it could be an attempt to attack the protocol and produce undesirable results.”

— Thomas W. Shinder and Thorsten Behrens.
The Best Damn Firewall Book Period, 2nd
ed., 2008 Syngress Publishing

Protocol Inspection

Protocol inspection maintains security by ensuring that data conforms with pre-established rules when it travels to a computer or a network.

A protocol is the prescribed format for data and the rules about communicating that data.

Sometimes the data does not comply with the required format or rules. This may be harmless and accidental. On the other hand, it might be evidence of an attack on the network.

An effective security system inspects incoming data for protocol compliance. Harmless data is occasionally protocol-noncompliant, and so many systems allow it to enter because enforcing compliance might block legitimate incoming information. However, attackers can exploit this situation by creating malicious code with noncompliance characteristics typical of harmless, legitimate data. Effective protocol inspection differentiates between legitimate data and malicious data.

[Is your file transfer DMZ doing protocol inspection?](#)

Chapter 2: Governance for
Inbound Data Movement

Audit Controls

In computer security, an audit is the gathering and analysis of information (done either manually or through an automated function) about an application or system to determine its protection against threats and attacks.

A variety of audit controls can be used to ensure that a system is configured and running properly. These include:

- **Reporting**
- **Monitoring**
- **Delivery Receipts**

Chapter 2: Governance for
Inbound Data Movement

Reporting is becoming more demanding ... more than simply collecting logs.

Reporting

Reporting, also called audit event reporting, is typically done on an ad hoc basis, meaning the user asks for and receives specific and customized reports. But reporting is no longer an optional activity. Today, companies are being required to follow a growing list of government requirements.

In addition to Sarbanes-Oxley, corporations are subject to new regulations such as PCI, DSS and HIPPA that require audit logging. These requirements, which always specified logs, are now saying that users must review the activity in logs and identify areas with potentially anomalous activity.

How are you reviewing event reporting for irregular activity?

Chapter 2: Governance for
Inbound Data Movement

Monitoring

Monitoring, also called continuous monitoring or event monitoring, is an automated function that analyzes and describes computer or network events. The purpose is to immediately inform users about potentially risky situations and enable them to take action fast.

*Keep looking for things that
fall outside the norm.*

The positive aspect of event monitoring is that helps ensure that you address important exceptions in a timely manner to keep key processes running, and continue searching for signs of intrusion.



Delivery Receipt

A delivery receipt, also called a delivery confirmation or delivery receipt notification, is an automated message returned in response to transmitted data.

It confirms that data has been received.

In reference to digital security, non-repudiation is one tool used to prove that a transferred message has been sent and received by two parties.

Nonrepudiation is a method to make sure that senders of messages cannot later deny having sent the message; it also proves that the recipient has received the message.

Today, more and more companies are moving data using AS2 (Applicability Statement 2) protocol, which expedites the sending and receiving of data via a secure connection. It functions as a type of envelope where important information is embedded.

So, whether you turn to a different protocol, or a log file record, you have to have a strategy to legally prove that you sent the data and that it was received.

How can you legally prove that data was not only sent,
but received?

Chapter 2: Governance for
Inbound Data Movement

Smart Automation Processes

In smart automation processes, advanced workflow capabilities are used in tandem with industry best practices, so that procedures are triggered automatically.

The issue, in terms of governance, is that you have a standard way of dealing with errors that do not have to be hand coded in a script for every transfer. Events are managed by exception, not inspection, and designated users are alerted in real time about important issues.

In short, it's about working smarter at every turn. Four of the most often used automated processes are:

- **Virus Scanning**
- **Integrity Checking**
- **Deleting of Processed files**
- **Checkpoint/Restart**

Chapter 2: Governance for
Inbound Data Movement

If virus scanning is not being done automatically, you are in danger of letting it slide.

Virus Scanning

A virus is malicious and self-propagating computer code (or malware) that compromises performance of your system. And as you already know, you've got to be on the lookout constantly. One way is virus scanning, which identifies and removes the monsters, ideally, before any harm is done.

And while viruses might be a low threat for system generated files, they still remain a high threat for person to person transfers like e-mail.

Typically, virus scanning deals with additional malware threats, such as Trojan horses and worms. The best virus scanning is done without weakening the performance of an application. What's more, superior virus scanning includes alerts and prompts for correct decision-making. Because new viruses are constantly being invented by hackers, a virus scanning tool is always in danger of being outdated and must be updated regularly.

Chapter 2: Governance for
Inbound Data Movement

Deleting of Processed Files

Deleting of processed files is a best practice for system security. A file might contain critical information that could be accessed by unauthorized users, such as Internet hackers. That's why, after files have been processed, they should be deleted so that the information they contain is no longer available to unauthorized parties.

It's simply a matter of good security.

How safe are you if your processed files
are *not* automatically deleted?

*Old files can give rise to a host of
new problems.*



Chapter 2: Governance for
Inbound Data Movement

Checkpoint/Restart

Checkpoint/Restart is a method of recovering from a line glitch or related system failure. For file transfer, a checkpoint involves saving at regular intervals during the transmission of a file. In the event of any failure, the last checkpoint serves as a recovery point, from which transfers can continue. This saves you from starting over at the beginning. If you've got Checkpoint/Restart, errors do not slow you down.

A Checkpoint/Restart will ensure that a transfer continues after an error condition.

If your system fails, will you be able to recover your data without starting the transfer over again?

Chapter 2: Governance for
Inbound Data Movement

Integration with Common Security Infrastructure

Integration with common security infrastructure allows all the different systems you use to facilitate data movement to share a single credential store.

By leveraging a single place to store user data, we don't have user credentials being stored in multiple servers that have to be touched every time something changes.

This greatly simplifies user maintenance and, at the same time, gives IT professionals the governance they need for security audits.

We'll take a look at two aspects:

- **Active Directory**
- **Key and Certificate Store**

*Technology that keeps you
moving in the right direction.*

Active Directory and LDAP

Active Directory is a Microsoft® technology.

Companies use Active Directory to store and arrange information about network components such as computers, devices, or users. In short, it makes it simpler to assign policies, deploy software, and apply critical updates to a computer system.

Active Directory includes Lightweight Directory Access Protocol (LDAP). LDAP is the industry standard for accessing a directory. LDAP means that Active Directory is very accessible to users who want to perform functions such as management applications or queries.

Learn more about Active Directory [here](#).

Learn more about LDAP [here](#).

**Chapter 2: Governance for
Inbound Data Movement**

Key and Certificate Store

In information security, a key (also called a data key or an encryption key) is used to encrypt or decrypt data. A certificate is encrypted information, such as the name of a user or an organization, establishing who “owns” a particular data key.

A certificate store is a central database of certificates maintained by a trusted third party called a certificate authority. When someone tries to access encrypted information, the certificate authority is contacted automatically and the certificate is accessed in the certificate store to confirm ownership of the data key.

By having a common key and certificate store, you can reduce maintenance of these important security artifacts that are used for encrypted protocols in file transfer.

Key Points to Remember

Defense in Depth

Defense in Depth uses multiple layers and different types of security to protect the system.

Multi-Factor Authentication

Multi-Factor Authentication employs at least two types of authentication, such as a USB token and an IP Address Change, to identify a user.

Session Break

Session Break is an automatic disruption to check a user's credentials. There are DMZ-based applications that will ensure security before there is a need to disrupt the communication.

Protocol Inspection

Protocol Inspection ensures that the data conforms to rules. To be maximally effective you should deploy a multi-protocol DMZ solution.

Chapter 3: Governance for Outbound Data Movement

This chapter looks at the factors to be considered with the movement of all data that is outbound from your organization.

The main topics to be covered are:

- **Encryption**
- **Ad hoc Transfer Support**
- **Data Loss Prevention Scanning**



**Chapter 3: Governance for
Outbound Data Movement**

Encryption

Encryption is a means of assuring the confidentiality of messages by transforming data to make it readable only to those who hold the “key” to how the encryption system works.

The use of encryption, or a cipher, suggests decryption, or deciphering, so that the encrypted information returns to a readable form. You have a wide array of encryption protocols to choose from, it’s simply a matter of deciding which encryption key you and the partner want to use.

Most IT professionals are familiar with the different encryption options—the problem is, not all organizations are diligent in applying the solutions that are available.

Does your organization have a classification policy,
and is it followed for all external file transfers?



**Chapter 3: Governance for
Outbound Data Movement**

Ad Hoc Transfer

Ad hoc refers to actions that are spontaneous as opposed to predefined or scheduled.

In the context of managed file transfers, ad hoc relates to person-centric transfer versus system-centric transfers. They are usually unscheduled, outside the company, and involve e-mail attachments, ftp servers, hosted service, or physical media.

With ad hoc transfer, you can exchange large file attachments with external parties through a secure portal, and without IT setup.

The best options today for ad hoc support will provide a Web mail-like user interface, and will deliver notifications on key activities. You'll also have both security and audit ability.

If ad hoc transfers are being made in your organization—and they probably are—what governance and control do you have over these activities?

E-mail servers clogged? Concerned about security?
Under pressure to cut costs?

**Chapter 3: Governance for
Outbound Data Movement**

Data Loss Prevention

Data Loss Prevention (also called data leak prevention and DLP) involves stopping the movement of sensitive, data-based on pattern matching. For example, it might identify social security numbers, based on xxx-xx-xxxx number format, in a file and stop the transmission of it in an e-mail attachment.

To do this, DLP software is invoked as a part of the transmission process where it performs functions such as data content inspection, context examination, and remediation.

Key Points to Remember

Important issues

Important issues related to outbound data movement include encryption, ad hoc transfers, and data loss prevention.

Governance

To avoid disruptions, fines—and worse—organizations must have effective governance and control policies in-place and in-use.

Chapter 4: Visibility for Data Movement Inside and Outside

This chapter looks at factors related to the visibility of data movement inside and outside your organization.

The main topics to be covered are:

- **Centralized Monitoring**
- **Centralized Provisioning for All New Connections**
- **Choices for Outsourcing and Third-Party Managed Services**



Centralized Monitoring

Centralized monitoring refers to a solution that provides monitoring of systems, applications, and networks from a single centralized point. We will have a look at these four aspects:

- **Notifications**
- **Policy Enforcements**
- **SLA Based Monitoring**
- **Integration Into Other System Management Tools**

Chapter 4: Visibility for
Data Movement Inside and Outside

Notifications

We are all aware of alarms, flashing lights and annoying beeps that try and get our attention to take a needed action. No longer do you have to sit in front of a console to be informed of a critical file transfer event or exception.

Today companies are using mobile devices to be notified and even deal with file transfer events from wherever they are.

How are you being notified when there is a problem?

Chapter 4: Visibility for
Data Movement Inside and Outside

Policy Enforcements

Policies are functional rules established to deal with situations that are likely to occur. They help maintain security for systems or applications.

For example, a common corporate policy is that no personal identifying information should be sent unencrypted, or that it must have at least 128 bit encryption.

The use of policy enforcements for configurations assures consistency and standardization across a system or network. It blocks “loose cannon” activities by individuals or solution providers who might want to implement unique ways of doing things.

How are you certain that key corporate policies are being enforced for data movement?



Chapter 4: Visibility for
Data Movement Inside and Outside

Effective monitoring can help ensure that requirements spelled out in the SLA are being met, and penalties are being avoided.

SLA Based Monitoring

A service level agreement (SLA) is a service contract in which aspects of the service such as the system uptime or the file delivery windows are very specifically described.

Most importantly, SLAs require a way to measure performance so that guarantees such as 99.999%, or clearing within one hour of receipt, can be achieved and validated.

Today, more and more critical data transfers are failing under SLAs. To meet these promises, you need a way of tracking your SLA performance and figuring out which exceptions need to be addressed first, to keep you within compliance.

Do you have a means of making sure that service levels are being met?

**Chapter 4: Visibility for
Data Movement Inside and Outside**

Integration Into Other System Management Tools

Every large firm uses system management tools such as HP Openview, IBM Tivoli, CA ControlM/Patrol. These are assembled in 24/7 operations centers and monitor the applications, servers, and network health for an entire enterprise.

File transfer has special monitoring requirements, and it is critical that it share alerts and notifications with existing system management tools, as well as provide you the specialized capabilities of SLA management and notification.

Are you leveraging the corporate resources as well as supplementing their standard services with what you need?

Chapter 4: Visibility for
Data Movement Inside and Outside

Centralized provisioning delivers better security, more efficient processes, and faster operation.

Centralized Provisioning for All New Connections

Provisioning involves configuring the system, giving access to users, establishing compliance with rules, and so on.

Centralized provisioning for all new connections provides a single, central point where connections are set up, tested, activated, and deactivated. It can bring structure and control to the ad hoc processes that spring up around the organization.

Centralized provisioning brings better security, more efficient processes, and faster operation versus creating one-off connections by each application or department.

How much control do you have over your current provisioning process?

Outsourcing and Third Party Managed Services

Going outside can help deliver higher levels of service at a lower cost.

The trend in business today is to take select IT functions—ones that are not differentiating to an organization—and turn them over to companies that can deliver higher levels of service at a lower cost. Managed File Transfer as-a-Service is an option that many companies are investigating.

Organizations can choose to outsource, or go with a third-party managed service.

Given the fast changing nature of technology—and growing government requirements—these are options that companies can no longer ignore, especially in B2B environments where there are a large number of connections

Are there elements of your data movement operation that could be outsourced so you could work on more differentiating processes?

Key Points to Remember

Visibility solutions

Visibility solutions include applications for both centralized monitoring and provisioning.

Trusted third parties

Managed services from a trusted third party can help you keep pace with new technology and government requirements.

Chapter 5: Making Capabilities Work for You

Use What You Learn

As infrastructures become more complex, there is an ever-greater need for data to follow strict guidelines as it moves in and out of the enterprise. Falling behind in these efforts can result in lost revenue, government fines, security breaches or even failed businesses.

Fortunately, there are a growing number of tools and strategies to control and protect corporate data. People involved in managed file transfer have a lot to gain by keeping up to speed on the latest capabilities.

You can help your organization stay competitive by learning about—and helping to implement—the governance capabilities that we have identified.

Don't wait for your corporate security department to ask what you are doing to ensure that data meets all governance requirements—step up and make recommendations, or share what can be done.

Now that you have learned about key issues related to data movement and governance, you are well positioned to meet the challenges head on. When you need support, look to Sterling Commerce solutions that can help you succeed. We are ready to move.

- ***Defense in Depth***
- ***Smart Automation Processes***
- ***Integration with Common Security Infrastructure***
- ***Encryption***
- ***Ad Hoc Transfer Support***
- ***Data Loss Protection***
- ***Centralized Monitoring***
- ***Centralized Provisioning***
- ***Outsourcing***

Chapter 5: Making Capabilities
Work for You

About Sterling Commerce

At Sterling Commerce, we're dedicated to developing innovative solutions for optimizing and transforming our customers' dynamic business networks.

We are one of the few companies that help organizations seamlessly and securely integrate both internal and external business processes to optimize performance.

Extensive business experience, recognition from analysts, and the financial resources of our parent company, IBM, are all sound reasons why you can depend on us. Headquartered in Columbus, Ohio, we have employees worldwide, and operations around the globe. Learn more at www.sterlingcommerce.com

- ***Defense in Depth***
- ***Smart Automation Processes***
- ***Integration with Common Security Infrastructure***
- ***Encryption***
- ***Ad Hoc Transfer Support***
- ***Data Loss Protection***
- ***Centralized Monitoring***
- ***Centralized Provisioning***
- ***Outsourcing***

Appendix: Regulations You Should Know About

Helping Financial Services

Companies Address Regulatory and Industry Security Requirements

Sterling Commerce is at the forefront of government and industry regulations enabling financial services companies to achieve regulatory compliance around data security, customer data privacy and audit-ability of data movement. For all regulations, financial services firms need to establish appropriate controls throughout the enterprise. No one control or solution is adequate for all situations or requirements. Sterling Commerce solutions provide core security capabilities to help financial services firms achieve regulatory compliance and provide the flexibility and extensibility for financial institutions to incorporate their own security policy above and beyond what is called for by the regulations.

Regulation

- Graham Leach Bliley Act (GLBA) – Data Privacy
- Sarbanes Oxley(SOX) – Audit-ability of data movement and data access
- Federal Financial Institutions Examination Council (FFIEC) – online banking authentication
- Payment Card Industry Data Security Standards (PCI DSS) – data security
- Personal Information Protection and Electronic Documents Act (Canada) – data privacy

Sterling Commerce solutions provide:




- Encryption for data in motion and at rest internally or externally
- Role-based access to data and system functions
- Multifactor authentication
- Best practice perimeter security architecture and functionality
- Capabilities to help meet 7 of 12 PCI DSS Requirements
- Detailed audit activity logging and consolidated activity database

**Appendix: Regulations You
Should Know About**

The Sterling Managed File Transfer solution helps exceed security requirements through:

- Authentication best practices by supporting multi-factor authentication, CRL checking, user ID mapping, security layering, LDAP integration and by providing flexibility and extensibility allowing a financial institution to build in additional internal organizational controls.
- Data privacy best practices through capabilities securing customer data such as encryption for data in motion and at rest. Role-based access to data and system functions, multifactor authentication and perimeter security features to prevent unauthorized access to the environment.
- Audit file transfer activity and system access as data moves from system to system internally or with external partners and customers.
- The peer-to-peer file transfer solution reduces data propagation risk by limiting the movement of data to just the producer and consumer. No intermediate infrastructure required to store and forward data thus limiting a data access point and eliminating a data archive location in the infrastructure.

Payment Card Industry Data Security Standards (PCI DSS):

Build and maintain a secure network	
Requirement 1	Install and maintain a firewall to protect cardholder data
Requirement 2	Do not use vendor-supplied defaults for system passwords and other parameters 
Protect cardholder data	
Requirement 3	Protect stored cardholder data
Requirement 4	Encrypt transmission of cardholder data across open, public networks 
Maintain a vulnerability management program	
Requirement 5	Use and regularly update anti-virus software 
Requirement 6	Develop and maintain secure systems and applications

Appendix: Regulations You
Should Know About

Implement strong access control measures	
Requirement 7	Restrict access to cardholder data by business need-to-know
Requirement 8	Assign a unique ID to each person with computer access
Requirement 9	Restrict physical access to cardholder data
Regularly monitor and test networks	
Requirement 10	Track and monitor all access to network resources and cardholder data
Requirement 11	Regularly test security system and processes
Maintain an information security policy	
Requirement 12	Maintain a policy that addresses information security

Using a point-to-point file transfer architecture (for example, Connect:Direct), data is not stored in intermediate file systems exposing the data to potential access by infrastructure or operational staff.

→ **PCI Requirement #3, #7 and #9** (by not requiring infrastructure that would require PCI compliancy)

External File Gateways use a Store and Forward architecture, and as such have the potential for unauthorized access.

a) Sterling File Gateway provides data at rest encryption and role based access providing the security components to meet PCI requirements.

→ **PCI Requirement #3, #7 and #9**

b) Sterling File Gateway supports unique user IDs and has extensive activity logging providing the ability to monitor access and file movement activities through its audit trail and reporting.

→ **PCI Requirement #8 and #10**

Appendix: Regulations You Should Know About

Secure firewall navigation is also a requirement and Sterling Secure Proxy provides a number of capabilities to address the PCI requirements

➔ **PCI Requirement #1**

The entire Sterling Managed File Transfer architecture provides encryption of data transmissions whether internal or external to an organization

➔ **PCI Requirement #4**

Sarbanes Oxley (SOX):

For SOX Compliance, the best practice is adhering to COSO (Treadway Commission) recommendations. And, to the IT practices established in COBIT. Sterling Managed File Transfer suite of products helps organizations achieve compliance. See key items in the table below.

COBIT	Description	Sterling Managed File Transfer Suite
DS1.5	Monitoring and reporting	<p>Sterling Control Center consolidates log files from multiple file transfer solutions used throughout the enterprise into a central database and provides over 50 standard reports and provides custom reporting through Crystal Reports.</p> <p>Sterling Integrator/Sterling File Gateway as the edge solution also provides online monitoring as well as reporting capabilities for operations, internal business users and external trading partners. SNMP can be used to integrate with Enterprise monitoring systems.</p> <p>Sterling Secure Proxy, the DMZ resident security component of the solution provides a consolidated log of activity for all sessions and separate logs. Log messages can also be routed to a syslog daemon which in turn can route messages to interested parties for appropriate action.</p>

Appendix: Regulations You
Should Know About

COBIT	Description	Sterling Managed File Transfer Suite
DS5.1	Remote management	<p>Sterling Control Center provides comprehensive monitoring, notification and Service Level Agreement management of all file transfer activity from any location.</p> <p>Through the MyFileGateway Web interface, end users of Sterling Integrator/Sterling File Gateway (internal or external) have remote self service capabilities to view status, run reports, upload and download files as well as subscribe to e-mail alerts.</p> <p>The DMZ resident security component of the solution, Sterling Secure Proxy can be accessed by administrators through a browser-based user interface. Sterling Secure Proxy can be accessed from the trusted zone via HTTPS for configuration and operations management.</p>
DS5.3	Identity management	<p>Sterling Commerce offers the user flexibility to use inbuilt, operating system, or external authentication (i.e. LDAP). Sterling Integrator/Sterling File Gateway also supports single sign-on.</p> <p>The DMZ resident component of the solution, Sterling Secure Proxy, supports authenticating users through queries to one or more LDAP servers. Certificates are validated including CRL checking. Sterling Secure Proxy also supports multi-factor authentication. Sterling Secure Proxy will terminate sessions with Sterling Integrator/Sterling File Gateway if authentication fails.</p>
DS5.4	User account management	<p>Sterling Commerce offers full capabilities for defining and managing user accounts, including a platform-appropriate interface. These capabilities include defining user IDs and passwords, ability to activate and deactivate access and the ability to define role-based permissions and access rights.</p>

Appendix: Regulations You
Should Know About

COBIT	Description	Sterling Managed File Transfer Suite
DS5.5	Abnormal activity detection	<p>Sterling Control Center includes blocks for max incorrect login attempts. Sterling Integrator/Sterling File Gateway provide detailed logging to track user and transmission activities.</p> <p>The DMZ resident component of the solution, Sterling Secure Proxy, logs all occurrences of errors. It also verifies the Connect:Direct protocol for correctness and inspects Connect:Direct control messages for proper content. If Sterling Secure Proxy detects any abnormalities, it will terminate the connection if so configured or log a warning message. For the FTP and HTTP protocols, Sterling Secure Proxy can be configured to disallow various commands and operations that are possible in these protocols.</p>
DS5.7	Protection of security technology	<p>Sterling Integrator/Sterling File Gateway's detailed logging and access controls ensure that secure areas within the system are restricted and changes are logged.</p> <p>The DMZ resident component of the solution, Sterling Secure Proxy, secures connections with SSL and TLS, its essential function is to provide a secure boundary for incoming connections so that only those authorized are forwarded into the internal network. No user credentials are stored in the DMZ and only outbound ports are open on the firewalls to protect the trusted zone.</p>
DS5.8	Cryptographic key management	<p>Sterling Commerce will integrate to your standard certificate and key management system.</p> <p>Sterling Secure Proxy provides management of certificates and keys in the various formats that Sterling Secure Proxy requires to implement its security capabilities.</p>

Appendix: Regulations You
Should Know About

COBIT	Description	Sterling Managed File Transfer Suite
DS5.10	Network security	<p>Sterling Commerce solutions provide encryption for transmissions so that data is protected as it traverses the network. No network security components are required (e.g., IPSEC)</p> <p>The DMZ resident component of the solution, Sterling Secure Proxy, provides application proxy services, including SSL session breaks, trading partner validation, protocol validation, certificate validation, session limits and multi-factor authentication. By providing the latest in perimeter security it allows you to safely use the Internet for reliable, low-cost, high speed, standards-based file transfers. It also enables only outbound ports on the firewalls ensuring secure navigation from zone to zone in the DMZ.</p>
DS5.11	Exchange of sensitive data	<p>Sterling Integrator/Sterling File Gateway provides a number of secure protocols and encryption technologies to protect sensitive data exchanges including TLS, SSL, SSH and PGP. Additionally, Sterling Secure Proxy can leverage Sterling Commerce Secure+ functionality in order to securely exchange information with Connect:Direct and protect the perimeter of an organization's network.</p>
DS11.5	Backup and restoration	<p>Data for all Sterling Commerce solutions is stored in standard database and config files. Standard best practice includes regular backup processes and documented recovery processes. Built in archiving function can be regularly scheduled.</p>
DS11.6	Data security	<p>Sterling File Gateway does not store data in the DMZ and provides data at rest encryption as well as role based access to ensure data is only accessible to those with appropriate access.</p> <p>The DMZ resident component of the solution, Sterling Secure Proxy, does not store user data being exchanged using the Connect:Direct, FTP, or HTTP protocols. After validation, the information is passed through from the sending entity to the receiving one.</p>
DS13.2	Job scheduling	<p>Sterling Integrator/Sterling File Gateway has a built in scheduler to automate file transfer processes</p>

**Appendix: Regulations You
Should Know About**

Federal Financial Institutions Examination Council (FFIEC):

The Sterling Commerce Managed File Transfer solution helps a financial institution meet the requirements set forth by the FFIEC with regard to authentication best practices by supporting multi-factor authentication, by offering security layering, LDAP integration and by providing flexibility and extensibility allowing a financial institution to build in other controls. See the SOX Compliance table above for more details.

Graham Leach Bliley Act (GLBA)

The Sterling Commerce Managed File Transfer solution (Note: multiple products make up the solution) helps a financial institution meet the requirements set forth by the GLBA with regard to protecting customer private information by providing best practice capabilities securing customer data such as encryption for data in motion and at rest. Role-based access to data and system functions, multifactor authentication and perimeter security features to prevent unauthorized access to the environment. See the table above under SOX compliance for more details.

**Appendix: Regulations You
Should Know About**

Corporate Security Standards

For all regulations, firms need to establish appropriate controls across the enterprise. No one control is adequate for all situations. Sterling Commerce solutions can help with data security around encryption, both for data in motion and at rest. We can help with auditing activity and access, securing the perimeter to ensure only authorized customers and systems can connect and finally, keeping and maintaining control of the data while within the solution.

Sterling Commerce is at the forefront of government and industry regulations and ensuring companies can comply. Our solution also provides the flexibility and extensibility for a financial institution to incorporate its own security measures above and beyond the regulations. For example, password policies can be configured to your security policy. The solution can integrate your own security functions into the file transfer process as well. Sterling Commerce DMZ security solution provides secure firewall navigation and has flexible deployment schemes to meet network and security architects' requirements.