

Achieving Regulatory Compliance

symform

AUTHOR:

Praerit Garg

6/17/2009

ABOUT THE AUTHOR

Praerit Garg, President and Co-founder

Praerit Garg is the President and Co-founder of Symform. Prior to Symform, Praerit was a Senior Director in Microsoft's Server and Tools division where he built and managed the Dynamic Systems Platform & Tools team. Under his leadership, the team grew from 0 to over 70 people and drove a broad industry initiative to expand W3C's XML standards to incorporate modeling enhancements called Service Modeling Language (SML). The team also delivered technology and solutions across several Microsoft products, including the distributed modeling system in Visual Studio 2007, Group Policy tools in Windows Vista/Server 2008, Server Manager in Windows Server 2008, and Desired Configuration Management in System Center Configuration Manager 2007. Praerit also led an acquisition and integration of a software company developing Group Policy tools.

Earlier in his 12+ year tenure at Microsoft he held various engineering leadership positions in Windows, ranging from a software developer driving US and European security certifications of Windows NT 3.51/4.0 products, to Group Program Manager for Windows Security delivering security infrastructure, such as Active Directory, Kerberos, PKI, EFS and Group Policy in Windows 2000, XP and 2003 releases.

Praerit is a co-inventor on 14 U.S. and international patents and a co-author of IETF RFC 3645, Web Services WS-Trust and WS-Secure Conversation specifications. He holds an M.S. in Computer Science from Purdue University and a B.E. (with Honors) from Birla Institute of Technology & Science, Pilani, India.

Achieving Regulatory Compliance

HIPAA, SOX, GLB and SEC/NASD

As information storage makes a dramatic shift from paper to digital form, federal and other governing agency are starting to mandate industry-specific regulations on organizations to ensure confidentiality, privacy, retention, and traceability.

The Health Insurance Portability and Accountability Act (HIPAA) requires organizations in healthcare industry to provide appropriate administrative, physical, and technical safeguards for patient information.

Sarbanes-Oxley (SOX) Act places specific requirements on an organization around length and mechanisms for retention of its financial records. Created in the wake of Enron and WorldCom corporate frauds, the SOX Act is designed to safeguard against illegal financial activities and other accounting errors.

Gramm-Leach-Bliley (GLB) ensures consumer privacy at financial institutions such as banks, thrifts, credit unions, insurance firms, brokerages, tax and accounting services, investment services, etc.

The Securities and Exchange Commission (SEC) and the National Association of Securities Dealers (NASD) has also defined compliance regulations for storage of financial records and electronic communications.

The **Symform Cooperative Storage Cloud** can be a secure, reliable and affordable data protection tool for organizations burdened with these regulatory requirements to achieve various data retention and recovery objectives stipulated in these regulations.

By implementing the best practices for onsite data backup using a mature, 3rd party local backup application of your choice and combining it with automatic mirroring of the local backups into the secure, redundant, geo-distributed Symform Cooperative Storage Cloud, customers are able to meet the various compliance requirements as follows.

- Backup files are encrypted locally using federally certified **256-bit AES encryption** before any transmission of the data.
- Encrypted data is redundantly geo-distributed using RAID 96™ technology to prevent data loss, tampering, alteration, or unauthorized access.
- Data is available 24x7 via a broadband connection.
- When needed, data is recoverable by authorized personnel only at authorized locations – customer premises or an authorized service provider premises using secure, randomly generated security credentials.

Achieving HIPAA Compliance

HIPAA requires the organizations to establish and maintain reasonable and appropriate administrative, technical and physical safeguards to ensure integrity, confidentiality, and availability of the information. Healthcare organizations are required to individually assess their security and privacy requirements and take suitable measures to implement electronic data protection (both in transit and in storage). As proposed, a HIPAA-compliant information system will need to include combination of administrative procedures, physical safeguards and technical measures to protect patient information while it is stored and transmitted across communication networks.

The **Symform Cooperative Storage Cloud** enables a secure and reliable online storage and disaster recovery service that helps customers achieve HIPAA compliance with respect to backups and archives as follows:

- Customer's backup and archive files are encrypted using federally certified 256-bit AES encryption prior to getting transmitted into the storage cloud.
- The Storage Cloud provides better security than a physical data center by ensuring that no customer file gets stored in one physical location. Instead, files are fragments and distributed over hundreds of locations.
 - The encrypted data is redundantly geo-distributed to hundreds of nodes in the storage cloud using RAID 96™.
 - RAID 96™ divides each 64MB block of data into 64 1MB fragments and then adds 32 1MB parity fragments using Reed Solomon erasure coding.
 - These 96 fragments are then geo-distributed to different participating nodes.

This inherently eliminates the risk of unauthorized access or malicious data center personnel.

- The fragments are redundant which enables highly reliable restore capability using only a subset of those fragments. This ensures that even multiple failures (as many as 32 simultaneous failures for each block of data) can be sustained without any potential data loss.
 - The system dynamically and automatically replenishes lost fragments due to node failures by regenerating them and placing them on other functioning nodes.
- The data is restored only through Symform Node software installed at a customer-authorized location using secure, randomly generated node security credentials.
- The data is retained in the storage cloud as long as the customer wishes it to remain.

Achieving SOX Compliance

SOX Act states that electronic records must be saved for five years to ensure that the auditors and regulators can obtain requested documents. The organizations regulated under SOX must look to storage format that will ensure their ability to satisfy this legal requirement.

It is important to note that customer's data is encrypted on site before getting spread into the storage cloud. Therefore, Symform has no knowledge of the contents of the files being mirrored into the storage cloud. It is customer's responsibility to ensure that the backups being mirrored to the storage cloud contain the information necessary to stay in compliance and who is authorized to access the

information. Symform's responsibility is limited to security and availability of the information being stored in the storage cloud.

The **Symform Cooperative Storage Cloud** enables a secure and reliable online storage and disaster recovery service that helps customers achieve SOX compliance with respect to backups and archives as follows:

- Customer's backup and archive files are encrypted using federally certified 256-bit AES encryption prior to getting transmitted into the storage cloud.
- The Storage Cloud provides better security than a physical data center by ensuring that no customer file gets stored in one physical location. Instead, files are fragments and distributed over hundreds of locations.
 - The encrypted data is redundantly geo-distributed to hundreds of nodes in the storage cloud using RAID 96™.
 - RAID 96™ divides each 64MB block of data into 64 1MB fragments and then adds 32 1MB parity fragments using Reed Solomon erasure coding.
 - These 96 fragments are then geo-distributed to different participating nodes.

This inherently eliminates the risk of unauthorized access or malicious data center personnel.

- The fragments are redundant which enables highly reliable restore capability using only a subset of those fragments. This ensures that even multiple failures (as many as 32 simultaneous failures for each block of data) can be sustained without any potential data loss.
 - The system dynamically and automatically replenishes lost fragments due to node failures by regenerating them and placing them on other functioning nodes.
- The data is restored only through Symform Node software installed at a customer-authorized location using secure, randomly generated node security credentials.
- The data is retained in the storage cloud as long as the customer wishes it to remain.

Achieving GLBA Compliance

All customers of financial institutions who maintain a relationship or obtain products and services from the institution are protected under GLBA. The products and services may range from mortgages, credit card accounts, brokerage/investment accounts, insurance services, accounting and tax services and others.

Financial institutions are required to keep variety of non-public personal information and personally identifiable financial information is subject to privacy controls under GLBA.

Symform ensures security of backups and archives mirrored into the storage cloud as follows:

- Customer's backup and archive files are encrypted using federally certified 256-bit AES encryption prior to getting transmitted into the storage cloud.
- Storage Cloud provides better security than a physical data center by ensuring that no customer file gets stored in one physical location and instead is spread into pieces over hundreds of locations.

- The encrypted data is redundantly geo-distributed to hundreds of nodes in the storage cloud using RAID 96™.
 - RAID 96™ divides each 64MB block of data into 64 1MB fragments and then adds 32 1MB parity fragments using Reed Solomon erasure coding.
 - These 96 fragments are then geo-distributed to different participating nodes.
- This inherently eliminates the risk of unauthorized access or malicious data center personnel.
- The data is restored only through Symform Node software installed at a customer authorized premises using secure, randomly generated node credentials.

Achieving SEC/NASD Compliance

SEC and NASD have instituted specific regulations that demand compliance to storage practices for financial records and electronic communications.

Symform enables its customers with SEC/NAD regulations as follows:

- Data is backed up and verified using a 3rd party backup software application that is mature and accepted by the IT Service industry.
- The backups are mirrored to the storage cloud for disaster recovery situations.
- The online mirror is available 24x7 for restores.
- The data is stored redundantly and geo-distributed using RAID 96™. RAID 96™ technology can ensure failures of as many as 32 nodes instantly for each block of data stored in the storage cloud. By comparison, RAID 5, regarded as highly reliable storage technology, is able to sustain failure of one disk before data loss may occur.