



Vertical Brief – Financial

Security and trust.

The banking industry - large international investment firms or a small local credit union is built on these two cornerstones. Institutions have concentrated on building secure data centers. But, the hard truth is that regulations like Basel II and Sarbanes-Oxley apply enterprise-wide—there is no exclusion for your small branch. So even if you've spent millions of dollars and countless weeks securing your data center, it may not be enough to pass a compliance audit. You also need to secure remote and branch office (ROBO) data—or it could turn out to be a costly area of vulnerability in an otherwise compliant organization. Failure to produce all relevant documents in an audit or court proceeding can lead to disastrous consequences including fines and imprisonment.

Industry analysts such as Gartner Group estimate the cost of service interruptions for banks range from \$60,000 to \$250,000 per hour.

Recent news has shown legacy tape backup to be susceptible to lost and misdirected financial and personal records. Obviously, unencrypted data is even more vulnerable to abuse than encrypted data. In a recent survey, Enterprise Strategy Group found that two-thirds of the financial firms never encrypted the data that they were backing up to tape. The majority of larger firms also failed to encrypt their backup data, with about 56 percent of companies with revenues greater than \$5 billion never having encrypted their data before putting it on tape.

Meeting the security compliance challenge.

Asigra specializes in providing a scalable and cost-effective an agentless, online backup software that complies with financial regulations to protect data in an encrypted format and at an offsite, secure location. Asigra Televaulting is designed to schedule and automatically backup distributed environments such as branch offices of major financial institutions to small community banks or credit union offices that do not have onsite trained IT resources to the secure centralized data center.

Asigra Televaulting encrypts (up to 256 AES) all data at the source and maintains encryption throughout the transfer and storage process, which protects the privacy and integrity of data during the entire backup process. (If stored at a third-party vault, only individuals authorized by the financial institution are able to access the backups.) Clear audit trails are generated when the data is accessed.

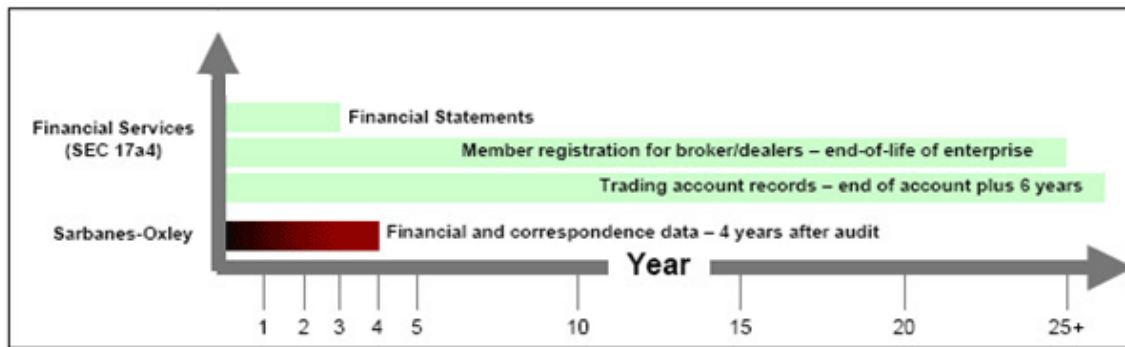
Data is transferred over a secure WAN to a central data center or vault thus ensuring offsite protection. In the event of a server crash, human error, or natural disaster, or audit, data is immediately available for restore and recovery.

Personal privacy is further ensured by the automated processes. There is no handling or transporting of tapes that can be misplaced or misdirected.

Key Benefits:

- Automated compliance with storage and privacy regulations
- Local and offsite storage ensure redundancy
- Data is fully encrypted at all times while in-flight and at-rest
- Easy, efficient backups and restores
- Fully scalable and capacity-based licensing ensures complete backup coverage as data grows
- Instant access and recovery of all backup files in the event of data loss or corruption
- Date and time-stamped access log that fulfills auditing standards. Clear time and date-stamped audit trail.
- Ability to coordinate data backup between multiple office locations.

Records retention periods mandated by various regulations in the United States



Source: Enterprise Storage Group

Additional Information:

Sarbanes Oxley <http://www.sarbanes-oxley.com/>

Sarbanes Oxley FAQs <http://www.sarbanes-oxley-101.com/sarbanes-oxley-faq.htm>

Basel II <http://www.federalreserve.gov/generalinfo/basel2/>

The Gramm-Leach-Bliley Act

<http://www.ftc.gov/privacy/privacyinitiatives/glbact.html>