IDERA® | SQL Compliance Whitepaper

HOW COMPLIANCE IMPACTS BACKUP STRATEGY

THE INTERSECTION OF COMPLIANCE AND DIGITAL DATA

Organizations of all sizes and shapes must comply with government and industry regulations. Some regulations are limited to public companies, while others are relevant only to certain verticals. Many regulations cut across type, size, and industry in their impact. In addition to legally mandated requirements, many organizations voluntarily adopt quality and process standards (such as Six Sigma or ITIL) or establish performance guidelines that impact employees and customer agreements. Adhering to these standards brings with it additional (and not always overlapping) sets of rules. In compliance with these standards, regulations, and rules - or just to maintain best practices - most organizations are implementing some degree of business continuity or disaster recovery plan.

While most information can (at least in theory) be recorded on paper, virtually all organizations now keep personnel, customer, financial, transactional and other records in digital format. Indeed, in this day and age, most organizations operate at the intersection of compliance and digital data. After all, compliance and digital data have become inextricably intermingled. Compliance is only manageable when information is digitized, and the proliferation of digital data makes compliance more essential. Organizations need to be following a set of rules about how to manage the growing stores of digital information they are accruing.

The bottom line: Whether legal requirements are in place, whether the rules and regulations are self-imposed, or whether there is a combination of factors in play, prudent business practice calls for backing up and securely housing digital data.

Sarbanes-Oxley Act (SOX)

Gramm-Leach-Bliley Act (GLBA) or Financial Services Modernization Act

Payment Card Industry Data Security Standard (PCI DSS)

Health Insurance Portability and Accountability Act (HIPAA)

Health Information Technology for Economic and Clinical Health Act (HITECH Act)

U.S. Securities and Exchange Commission (SEC)

Basel II

Red Flags Rule

Statement on Standards for Attestation Engagements (SSAE) 16

THE INTERSECTION OF COMPLIANCE AND BACKUP

Compliance-related requirements need to drive the backup strategy, and the backup strategy needs to support whatever compliance-related requirements an organization has in place.

What does having and enforcing a backup strategy accomplish for an organization? For one, it demonstrates to regulators and auditors the capability of protecting and restoring critical data. It can also get databases quickly back in business after a disaster occurs - whether from terrorist attack or hacker intrusion, hurricanes or a burst pipe, or just plain human error. Further, it can help protect and defend organizations when litigation arises from employees, customers, competitors, or regulators.

WHY ANY OLD BACKUP WILL NOT DO

It is not just a matter of backing up. It is also important how databases are backed up. There is a set of technical requirements that must be satisfied to use a backup solution for compliance purposes. These are:

- Encryption in transit
- Encryption at rest
- Access controls
- Audit trails
- Where backed up data is kept (for example, off-premises, in country)
- The ability to determine what types of data get backed up
- The ability to set frequency of backup
- The ability to satisfy restoration time requirement

Any company that maintains personally identifiable information on employees (for example, Social Security numbers, proof of citizenship) has obligations attached to the maintenance of this data. The same holds true for organizations holding confidential customer information (for example, credit card numbers, banking information). These obligations revolve around keeping information private and confidential, keeping information secure from unauthorized access, and just plain keeping information for whatever the requisite retention period is.

There is no need to delve into much (if any) detail on why these requirements make the list. They are all more or less self-explanatory. Two not-so-self-evident issues are worth pointing out here:

1. Tape-based backup, which requires manual intervention, is an inherently insecure process and will fail to meet the compliance threshold for regulations regarding data privacy. Tape-based backup may further fail the test when it comes to satisfying time-to-restoration requirements.
2. All automated software backup solutions are not created equal. When choosing a solution, do so with full awareness of what the compliance needs are of an organization.

IDERA SQL SAFE BACKUP

IDERA Safe Backup is well-suited to meet the compliance needs of so many organizations.

Separation from Actual Data

- **SOX** financial reporting data
- **Basel II** financial reporting data
- **GLBA** nonpublic personal information
- **PCI** personal account number

SQL Safe Backup does not look at any data within the database. Instead, it asks SQL Server to perform backup and restore operations. Consequently, SQL Server is the only application that interacts with the data.

Encryption at Rest

- **SOX** financial reporting data
- **Basel II** financial reporting data
- **GLBA** nonpublic personal information
- **PCI** personal account number

With SQL Safe Backup, encrypt using AES 256 encryption the data as it is written to disk.

Audit Trails

- **HIPAA** for information systems containing protected health information
- **SOX**
- **PCI**

With SQL Safe Backup, each time a task (backup, restore, or merge) is performed, log information on (for example) what database and database files were involved, and where data was backed up or restored to.

Determine What Types of Data to Back Up

- **SOX** financial reporting data
- **HIPAA** electronic protected health information

With SQL Safe Backup, select any combination of files and folders to be excluded from the continuous data protection policy and add advanced rules using patterns to exclude only certain file types.

Set Backup Frequency and Retention Times

- **SOX** sets minimum number of periods for retaining data and audit trails
- **HIPAA** sets varying length requirements for the health records of adults and children

With SQL Safe Backup, schedule server backups as frequently as every 15 minutes and set how many recovery points to retain. Also, configure how much history to retain in the repository database. Moreover, configure the frequency at which backups created through policies are kept on disk (that is, automatically purge backup files).

Satisfy Restoration Time Requirements

- Regulations vary broadly by industry and individual, organizational needs.

With SQL Safe Backup perform restores as fast as possible, and faster than virtually any competitive offering.

There is a final way in which IDERA Safe Backup is compliance-ready. The best-intentioned compliance and backup strategy will live only on paper if it is difficult to implement and time-consuming to deploy on a regular basis. Unlike solutions that may take hours to install and configure, IDERA Safe Backup is built for download and go, with no professional services required. Once IDERA Safe Backup is up and running, tasks are automated, saving administrative time, eliminating the possibility of forgetting about it, and decreasing the likelihood of human error.

Given the simultaneous explosion of digital information and compliance requirements, having a sound, workable backup and restore policy is essential. So is the ability to carry through on that policy. IDERA Safe Backup stands at the intersection of compliance and backup with a solution that lets organizations of all shapes and sizes put compliance into practice, cost efficiently and time effectively.

SQL SAFE BACKUP

AUTOMATE SQL SERVER BACKUP ACROSS YOUR ENTERPRISE

- Backup faster and save space via dynamic compression with encryption
- Choose from multiple options for recovery
- Ensure organizational compliance via policy-based management
- Reduce failures due to temporary network problems
- Receive alerts and create reports with centralized web console

Start for FREE