# Enabling Regulatory Compliance with Your IT Infrastructure Platform

From the Experts at
Scale Computing

Technical White Paper

## Table of Contents

# Introduction

Organizations strive to minimize operational interruptions in the event of unexpected business disruptions. A crucial component of a company's comprehensive risk management strategy is an IT business continuity plan. The primary objective of that plan is to swiftly reinstate critical business activities, ensuring that customers, partners, and employees remain unaffected while safeguarding data integrity.

Various events can undermine business continuity, ranging from local power outages and hardware failures to user errors. Disaster recovery focuses on more severe and widespread disruptions like natural or man-made disasters and significant cybersecurity incidents. It is a subset of business continuity.

To instill confidence in end users, prevent revenue loss, and maintain a competitive edge, it is imperative for organizations to establish a resilient business continuity/disaster recovery (BCDR) program. In addition to sound business reasons, today's regulatory frameworks imposed by governments and industries mandate BCDR activities and information security. These regulations demand a robust security posture in general and the protection of sensitive data assets in particular.

The global compliance ecosystem is highly complex:

- National and state data protection laws (all of which reference BCDR) such as those of the EU (GDPR), UK, Canada, and California (CCPA), to name but a few.
- Data privacy laws that cover specific domains such as HIPAA/HITECH for the US healthcare industry, the Gramm-Leach-Bliley Act (GLBA) for U.S. financial institutions, and the Sarbanes-Oxley (SOX) Act for public companies traded on U.S. exchanges.
- Industry-specific, self-regulating frameworks such as the global Payment Card Industry Data Security Standard (PCI-DSS) or the Basel Accords of the worldwide Basel Committee on Banking Supervision.
- Government agencies that develop and enforce compliance standards and best practices, such as FedRAMP and NIST Cybersecurity Framework in the U.S. or FINTRAC in Canada.
- Global IT communities such as the Center for Internet Security (CIS), whose benchmarks and best practices carry great weight in the compliance world.

Navigating regulatory compliance requires a thorough understanding of various requirements. This white paper aims to provide clarity by outlining some of the business continuity and disaster recovery (BCDR) and information security requirements within specific regulatory frameworks, namely HIPAA, PCI-DSS, and SOX. Additionally, it presents recommended BCDR best practices that support and facilitate compliance with these regulations. By following these guidelines, organizations can enhance their adherence to regulatory standards while ensuring effective implementation.

**Note:** This document and any other related documentation on compliance produced by Scale Computing do not offer legal advice. Customers are solely responsible for evaluating and fulfilling their own legal and compliance obligations.

## Regulatory Frameworks Overview

This section offers a brief overview of three regulatory frameworks for information security compliance: the Health Insurance Portability and Accountability Act (HIPAA), the Sarbanes-Oxley Act (SOX), and the Payment Card Industry Data Security Standard (PCI-DSS). It focuses on the essential BCDR-related requirements within each framework. Separate from this, a dedicated section discusses the consequences of non-compliance with these regulations.

### HIPAA

Enacted on August 21, 1996, the Health Insurance Portability and Accountability Act (HIPAA) was established to enhance the portability, security, and privacy of electronic Protected Health Information (ePHI). HIPAA applies to Covered Entities and their Business Associates. Covered Entities encompass health plans (such as health insurance companies and HMOs), clearinghouses involved in processing nonstandard health information, and providers (including doctors, clinics, nursing homes, and pharmacies) that submit electronic HIPAA claims.

HIPAA regulations are structured around three main rules: Privacy, Security, and Breach Notification. BCDR-related and information security matters are addressed primarily within the Security Rule. This rule outlines administrative, technical, and physical safeguards intended to:

- Preserve the confidentiality, integrity, and availability of all received, stored, or transmitted ePHI
- Reasonably protect against anticipated threats to the security or integrity of ePHI
- Implement measures to prevent unauthorized use or disclosure of ePHI

HIPAA adopts a flexible approach, where only a subset of rules is mandatory (“Required”), while the rest are considered recommendations (“Addressable”). Following is a summary of the essential safeguards that impact BCDR and information security activities:

#### Administrative Requirements

- Conduct a comprehensive and accurate risk analysis
- Implement ongoing risk management practices
- Clearly designate the individual(s) responsible for HIPAA security compliance
- Establish sanctions for non-compliance by the workforce
- Regularly review information system activity

**Security Implementations**

- Develop a data backup plan that includes processes for creating and maintaining retrievable and exact copies of ePHI
- Establish a disaster recovery plan with procedures for restoring any lost data
- Create an emergency mode operation plan, including procedures to ensure uninterrupted ePHI security activities

**High Availability**

As a final point, high availability refers to the ability of an organization to maintain its hardware and software systems, making sure that authorized individuals have access to electronic protected health information (ePHI). Achieving this involves implementing the proper technical and physical safeguards.

By adhering to these mandatory safeguards and implementing the recommended practices, organizations can enhance their BCDR and security capabilities while complying with HIPAA requirements.

## Sarbanes-Oxley (SOX)

The Sarbanes-Oxley Act (SOX), passed in 2002, was enacted in response to accounting scandals that eroded investor confidence in major corporations like Enron and WorldCom. Its primary objective is to combat fraud. SOX controls primarily apply to publicly traded companies or those considering an initial public offering (IPO). The Securities and Exchange Commission (SEC) enforces SOX regulations.

While many SOX provisions pertain to financial and accounting practices, effective management of corporate data is integral to achieving compliance. Generally, data must be accurate, protected against internal and external threats, and readily available to auditors and investors in near-real time. Specifically, the source data used for generating financial reports must be traceable, and any revisions to the source data must be documented. Similarly, any modifications made to financial or accounting software must be thoroughly documented.

By adhering to these rules and requirements, organizations can strengthen their BCDR capabilities, enhance data security, and maintain compliance with applicable regulations, particularly those outlined by SOX.

**Access Control.** Grant access to electronic data on a need-to-know basis, and track and verify access activities.

**Data Protection Safeguards.** Implement demonstrable safeguards to protect data from breaches, ensuring that appropriate security measures are in place.

**Data Security Strategy and Policies.** Maintain a formal, written data security strategy and consistently enforce data security policies throughout the organization.

**Offsite Backup.** Back up and store financial records at an offsite location to ensure their availability and protection in the event of a disruption.

**Compliance Documentation.** Record and document compliance activities to demonstrate adherence to regulatory requirements.

**Incident Disclosure.** Promptly disclose any detected data breaches or security control failures to relevant parties as required by regulations.

**Executive Responsibility.** Hold CEOs and CFOs personally responsible for the accuracy and integrity of financial reports and the implementation of internal controls audited to meet SOX requirements.

## PCI-DSS

The Payment Card Industry Data Security Standard (PCI-DSS) was developed to safeguard the security of credit/debit card transactions and cardholder data. It applies to various entities involved in card transactions, including banks, merchants, clearinghouses, and service providers. The initial version, PCI-DSS 1.0, was introduced in December 2004, and compliance is enforced by the major card brands through the Payment Card Industry Security Standards Council (PCI SSC), comprising American Express, Discover Financial Services, JCB International, MasterCard Worldwide, and Visa Inc.

PCI-DSS Requirement 12 emphasizes the establishment, publication, maintenance, and deployment of an information security policy. This includes implementing a risk assessment process. Section 12.10 mandates the creation and implementation of an incident response plan to ensure a swift and coordinated response in the event of a data breach. The incident response plan should encompass business recovery and continuity procedures, as well as data backup processes. It is essential to review and test the incident response plan at least once a year to ensure its effectiveness.

**Note:** The PA (Payment Application) DSS extends PCI-DSS requirements to new digital payment platforms and introduces specific requirements for solution vendors.

## Keep Your Organization Aligned with BCDR Regulatory Requirements

### Organizational

To effectively implement an information security or BCDR strategy, organizations must begin with a comprehensive plan that aligns with their goals and environment. This involves conducting analyses to identify critical business activities and assess the associated risk levels. These analyses not only provide valuable insights for setting focused objectives but also elevate the importance of information security and BCDR within the corporate agenda.

While an organization may opt for a unified plan or separate plans for different units and functions, a clear framework for governance is essential. It is necessary to determine who holds overall management accountability and whether they have the necessary authority to enforce compliance. Adequate resources, including budgetary and personnel allocations, should be dedicated to the design, implementation, and management of these plans.

For organizations subject to regulatory frameworks like HIPAA, SOX, and PCI-DSS, periodic external audits are required to ensure compliance. In addition to external audits, conducting regular internal audits and reviews is crucial to test and assess the effectiveness of policies, procedures, and controls. Any weaknesses identified through these internal audits should be promptly addressed, and the plans updated accordingly.

**Note:** In addition to data backups, it is crucial for organizations to maintain current and readily accessible repositories of critical software and their configuration settings. This includes operating systems (OSes), applications, databases, and other important components. Storing and regularly updating these repositories ensures that the organization can efficiently restore software and its associated configurations in the event of a disruption or data loss scenario.

### Disaster Recovery (DR)

A robust disaster recovery (DR) plan is essential for maintaining resilience in the face of a significant disaster and serves as the ultimate test of a business continuity program. DR plans revolve around recovery point objectives (RPO) and recovery time objectives (RTO), where RPO defines the maximum acceptable data loss and RTO signifies the maximum acceptable downtime before business continuity is compromised.

To achieve ambitious RPO and RTO metrics, implement the following best practices:

**Comprehensive documentation.** Maintain a fully documented plan that is regularly updated and accessible to all stakeholders. The plan should outline roles and responsibilities, contact information, triggering events, and criteria for returning to normal procedures.

**Data mirroring.** Implement a data-synchronization/mirroring solution, often based on snapshots, to ensure high availability. This involves continuously replicating data to minimize the risk of loss.

**Complete replication of the production environment.** It is not only data that needs to be mirrored, but the entire infrastructure as well. Prepare a DR site that can seamlessly transition into a production environment. Perform regular maintenance, including software licenses, patching, and upgrades, to keep it up to date.

**Selecting DR location.** Choose a DR site that is sufficiently distant from the primary facility to ensure it remains unaffected by local disaster conditions. However, it should still be accessible for IT personnel.

**Testing.** Regular testing is vital to ensure the effectiveness of the DR plan. Develop a system for periodic testing of all functionalities, such as data recovery, failover and failback processes, remote data access, and stress testing. Establish clear success criteria, including RTO and RPO targets.

By following these best practices, organizations can minimize data loss and downtime during critical situations. Compliance with regulatory frameworks requires the establishment of comprehensive DR plans that are regularly reviewed and tested to ensure their effectiveness.

## Penalties for Non-Compliance

### HIPAA Penalties

Following the implementation of the Omnibus Rule, HIPAA violations can result in penalties for healthcare providers, health plans, healthcare clearinghouses, covered entities, and business associates (BAs) of covered entities. The purpose of these penalties is to hold entities accountable for safeguarding patient privacy, maintaining data confidentiality, and providing patients with access to their health records.

Penalties for HIPAA violations depend on the level of knowledge the covered entity had regarding the violation. The Office for Civil Rights (OCR) determines the penalty based on general factors and the severity of the violation.

It's important to note that ignorance of HIPAA rules is not a valid excuse for noncompliance. Covered entities are responsible for understanding and adhering to HIPAA rules. For willful violations of HIPAA laws, the maximum fines may apply.

A HIPAA violation occurs when a covered entity or business associate fails to comply with the provisions of the HIPAA Privacy, Security, or Breach Notification Rules. Violations can be deliberate or unintentional. Unintentional violations may include disclosing more protected health information (PHI) than necessary. Deliberate violations may involve delayed breach notifications.

### Civil Penalties

Many HIPAA violations stem from negligence, such as the failure to conduct an organization-wide risk assessment. OCR aims to resolve violations through voluntary compliance and technical guidance and reserves financial penalties for serious violations or to emphasize specific violation types.

The penalty structure for HIPAA violations consists of four tiers:
**Tier 1:** Violations that the covered entity was unaware of and could not have reasonably avoided with proper care.

**Tier 2:** Violations that the covered entity should have been aware of but couldn't have avoided even with reasonable care (short of willful neglect).

**Tier 3:** Violations resulting from willful neglect, but with efforts made to correct them.

**Tier 4:** Violations constituting willful neglect without any attempt to correct them within 30 days.

Each tier carries a separate penalty, and OCR determines the specific financial penalty within the applicable range. Factors considered include the duration of the violation, the number of affected individuals, the nature of the exposed data, the organization's cooperation with the investigation, prior history, financial condition, and the level of harm caused.

The penalty amounts for each tier are as follows (adjusted for inflation annually):
**Tier 1:** Minimum fine of $100 per violation up to $50,000

**Tier 2:** Minimum fine of $1,000 per violation up to $50,000

**Tier 3:** Minimum fine of $10,000 per violation up to $50,000

**Tier 4:** Minimum fine of $50,000 per violation

---

**Note:** It's important to note that these penalties are subject to annual adjustments for inflation. The multiplier for 2023 is 1.07745, but official updates for 2023 penalties are pending.

### Criminal Penalties for HIPAA Violations

Criminal penalties for HIPAA violations are categorized into three tiers, and the specific term of imprisonment and accompanying fines are determined by a judge based on the circumstances of each case. Similar to OCR, several general factors are taken into account to determine the penalty. In cases where an individual has profited from the theft, access, or disclosure of protected health information (PHI), the court may require the individual to refund any money received in addition to imposing a fine.

The tiers of criminal penalties for HIPAA violations are as follows:
**Tier 1:** Violation due to reasonable cause or lack of knowledge - Up to 1 year in jail

**Tier 2:** Obtaining PHI under false pretenses - Up to 5 years in jail

**Tier 3:** Obtaining PHI for personal gain or with malicious intent - Up to 10 years in jail

In recent years, there has been an increase in cases involving employees accessing or stealing PHI for various reasons. The black market value of PHI is substantial, making it a strong temptation for some individuals. It is crucial to implement controls that limit opportunities for data theft and establish systems and policies to promptly identify improper access and theft of PHI.

Educate all staff members who may handle PHI as part of their job responsibilities about the criminal penalties under HIPAA. They should understand that violations can not only result in termination of employment but also potentially lead to a significant jail sentence and heavy fines.

## SOX Penalties

Non-compliance with the Sarbanes-Oxley Act (SOX) can have severe consequences, including substantial corporate fines and penalties such as delisting from public stock exchanges. It is important to note that violations are not the only triggers for penalties; failure to rectify disclosed noncompliant internal controls over financial reporting has also led to charges and settlements by the Securities and Exchange Commission (SEC).

Under SOX Section 906, corporate officers bear direct liability for violations. For instance, a CEO/CFO who knowingly approves a non-compliant financial report can be fined up to $5 million or sentenced to up to 20 years in prison. Additionally, even individuals who unintentionally violate the Act can face imprisonment of up to 10 years and a fine of $1 million.

While it is uncommon, SOX can also enforce the clawback clause, which requires non-compliant corporate officers to return incentive-based compensation.

Importantly, SOX safeguards employees who report violations, commonly known as whistleblowers, from retaliation such as termination of employment. Whistleblowers who can demonstrate that their employers violated SOX provisions in this regard have been awarded significant compensation by the courts.

## PCI-DSS Penalties

The PCI Security Standards Council (PCI SSC) has the authority to impose fines on acquiring banks for non-compliance with the Payment Card Industry Data Security Standard (PCI-DSS). These fines can range from $5,000 to $100,000 per month. In turn, the acquiring bank may pass the fine on to the merchant, sometimes indirectly through increased transaction fees. The fines are assessed on a monthly basis, and if the merchant remains non-compliant, the penalty may be escalated. For small and medium-sized businesses (SMBs), a three-month period with a $100,000 monthly penalty could have devastating financial consequences.

Moreover, in the event of an actual data breach suffered by a non-compliant merchant, there can be additional fines imposed. These fines can range from $50 to $90 per affected consumer, with a maximum penalty of $500,000 per incident. The affected consumers must also be notified, which adds to the costs incurred by the merchant.

Apart from financial penalties, another significant consequence of non-compliance is the potential freezing of a merchant account or being added to the Terminated Merchant List. Banks may refuse to conduct business with merchants on this list for an extended period, usually at least five years. While this sanction is typically reserved for cases of fraud and serious violations, persistent non-compliance can also be a reason for being included on this list.

It is important to note that as a self-regulating body, the PCI SSC is not obligated to publicize fines and sanctions. This lack of transparency can make it challenging for merchants to contest imposed penalties.

## How Scale Computing Can Support Your Regulatory Compliance Efforts

Scale Computing offers solutions that can assist organizations in remaining compliant with regulatory standards such as HIPAA, SOX, and PCI-DSS. With its innovative technology and features, Scale Computing provides the necessary infrastructure and tools to help organizations meet their compliance requirements effectively.

- **Security and Data Protection.** Scale Computing's hyperconverged infrastructure (HCI) solutions are designed with robust security features to protect sensitive data. Workload data can be encrypted and access to the clusters can be controlled with granular role-based access to ensure the confidentiality and integrity of data. This is crucial for organizations dealing with healthcare data (HIPAA), financial information (SOX), and cardholder data (PCI-DSS).

- **High Availability and Disaster Recovery.** Scale Computing's solutions are designed for high availability and disaster recovery, which are essential for meeting compliance requirements. The built-in failover and replication capabilities ensure that critical applications and data are continuously available, minimizing downtime and data loss. This is particularly important for organizations under HIPAA, SOX, and PCI-DSS, as they need to demonstrate the ability to restore operations quickly and minimize data loss in the event of an IT disruption.

- **Simplified Management and Compliance Reporting.** Scale Computing Platform offers centralized management and monitoring, simplifying the administration of IT infrastructure. This includes features such as automated monitoring, alerts, and data gathering, which can assist organizations in meeting compliance reporting requirements. With comprehensive visibility into their infrastructure, organizations can easily generate the necessary reports to demonstrate compliance with regulatory agencies.

- **Scalability and Flexibility.** Scale Computing's solutions are scalable, allowing organizations to easily expand their infrastructure as needed. This is beneficial for organizations subject to compliance requirements as they can accommodate growing data volumes and changing business needs without sacrificing security or performance.

- **Services and Support.** Scale Computing Services provides expert guidance to help organizations navigate the complexities of compliance regulations. The SC//Services team can assist with numerous services to support customers with Scale Computing Platform:

  - Health Check & Audit Service
  - SC//Platform Cloud Unity DRaaS Service

Ensuring the ability to effectively respond to IT disruptions has become a key performance indicator (KPI) critical to business success. Whether these disruptions are localized and short-lived or extensive and highly impactful, stakeholders such as customers, employees, partners, and regulators expect organizations to swiftly restore normal IT operations with minimal data loss. Regulatory frameworks like HIPAA, PCI-DSS, and SOX outline expectations, mandatory requirements of security laws and regulations, and recommended best practices for BCDR and information security. Each company is responsible for understanding the relevant regulations and maintaining compliance with them.

Implementing compliance best practices involves various organizational activities, such as strategic planning, obtaining cross-organization buy-in, and establishing clear governance guidelines. It also includes regular data and critical software backups stored in secure offsite locations, frequent data integrity checks, and tested procedures for data restoration. Additionally, maintaining a synchronized mirror failover site that can take over if the primary site goes down is essential, supported by a comprehensive and documented disaster recovery plan that has been thoroughly tested.

Non-compliance carries significant direct costs, including penalties, fines, and sanctions. Additionally, there are indirect costs such as revenue loss, damage to reputation, and loss of trust. Therefore, companies have a strong motivation to achieve and maintain compliance with their obligations.

With its focus on security, data protection, high availability, simplified management, scalability, and expert support, Scale Computing provides the necessary tools and infrastructure to support compliance efforts effectively.

Corporate Headquarters
525 S. Meridian Street - 3E
Indianapolis, IN 46225
P. +1 317-856-9959

**scalecomputing.com**

EMEA B.V.
Europalaan 28-D
5232BC Den Bosch
The Netherlands

**+1 877-722-5359**

SCALE COMPUTING