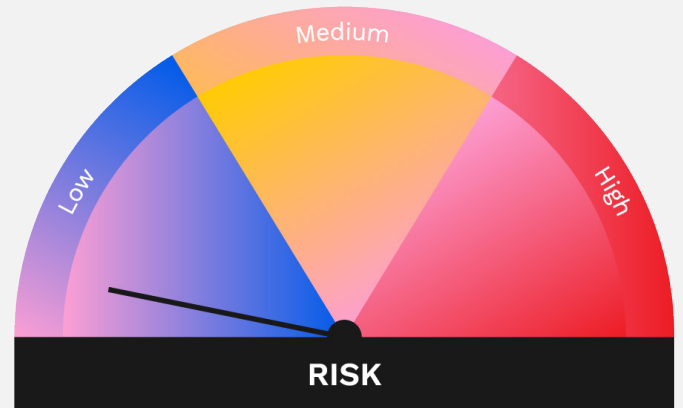SOLUTION BRIEF

Governance and Compliance

Automating corporate governance and compliance with Panzura Symphony.

RISK

Data is one of the most valuable assets for any organization. Whether it's customer information, financial records, or proprietary business data, the integrity, confidentiality, and accessibility of data are essential to a company's success. However, as organizations generate more data and the regulatory environment surrounding data management becomes more complex, the need for effective corporate governance and compliance in data storage has never been more critical.

It has historically been a difficult and manual task to scan for personal identifiable information (PII), protected health information (PHI), social security numbers (SSN), and other private data, tag it and secure it.

Panzura Symphony, along with our partnerships with IBM and GRAU DATA, can enable a full suite of solutions to automate the scanning and tagging of target data, and the appropriate action to take — significantly reducing the cost and complexity of compliance and governance burdens.

The Growing Need for Data Governance and Compliance

Data governance refers to the framework, policies, and procedures that ensure data is properly managed, secured, and utilized within an organization. Compliance, on the other hand, relates to adhering to external regulations, standards, and laws that dictate how data should be stored, protected, and handled. Together, these two components are essential in ensuring that data storage practices align with both internal business objectives and external legal requirements.

As businesses rely more heavily on data, the risks associated with poor data governance and non-compliance have escalated. Data breaches, unauthorized access, and non-compliance penalties are just a few of the potential consequences of not applying proper governance and compliance measures. The importance of these elements cannot be overstated.

Getting your hands around the command and control of these tasks can be daunting given that data now sits on-premises across many storage systems, but also potentially in multiple clouds in both file and object format, in databases, and in proprietary systems in the case of life sciences, engineering, geological (oil and gas) and other industry specific applications.

There is a lot to scan, review, audit and report. Finding a way to automate these tasks within the below examples will save time and money. This is where Panzura Symphony, in some cases in conjunction with IBM's Storage Fusion Data Catalog, as well as GRAU DATA's MetadataHub can assist, offering a single interface to your expansive compliance and governance data set.

Below are some key reasons why organizations should prioritize corporate governance and compliance in their data storage strategies, and how Panzura Symphony, along with our integrated partners, can help automate these arduous tasks.

01 Protecting Sensitive Information

Data storage systems often contain sensitive information such as personal identifiable information (PII), financial data, and intellectual property. If mishandled, this information can be vulnerable to theft, cyber-attacks, or accidental exposure. Effective data governance ensures that data is categorized, encrypted, and stored according to best practices to minimize these risks. For instance, compliance with regulations such as the General Data Protection Regulation (GDPR) or Health Insurance Portability and Accountability Act (HIPAA) requires organizations to put stringent measures in place to protect data privacy and security.

While companies may initially put access control measures in place to protect sensitive information, things tend to change over time. People flow in and out of the company, and access to files gets murky. Mergers and acquisitions often involve the inheritance of datasets and entire storage estates. Some files end up orphaned with no ownership, and others become exposed to too many people. Motion is constant within any organization, and things will always get dirty. Automating such tasks as constant scans for sensitive data, and flagging files or objects which may contain sensitive data is crucial to maintaining compliance with these strict regulations.

Having robust corporate governance over data storage means that access to sensitive data is controlled and logged, reducing the risk of unauthorized access. This also helps organizations quickly identify and respond to any potential breaches, minimizing damage and ensuring the privacy of customers and clients.

Panzura Symphony can scan any source storage metadata to find and flag sensitive information, improper access, orphaned files, and myriad other governance and compliance related issues. This flag acts as a trigger to custom Symphony automations — policies and tasks — which can be set up by either the governing body (required actions) or the company (voluntary actions), which means that your organization can stay compliant at all times, with no human interaction required. Moreover, all actions may be stored in a database for external auditing.

02 Meeting Legal and Regulatory Requirements

Data-related regulations are constantly evolving, with new laws introduced to address emerging risks and technological advancements. These regulations vary by country, industry, and the type of data being stored. For example, the General Data Protection Regulation (GDPR) mandates strict data protection requirements for businesses operating in the European Union, while the California Consumer Privacy Act (CCPA) governs data privacy rights for residents of California.

Looking within all data, across every environment, including on-premises and cloud can be time consuming and virtually impossible. Data covered under GDPR and CCPA includes all data stored within the confines of the region, no matter where. This data may also be in any format (PDF, Word, Excel, database, and proprietary). Looking within the data is where Panzura Symphony leverages IBM's Storage Fusion Data Catalog, a standalone product with native integration for Symphony to provide a single pane of glass view of your data. Data Catalog brings IBM's ability to parse the contents of the majority of file types and tag the file as sensitive.

Data Catalog's deep search capabilities can parse your content, and flag it within the metadata as containing PII, PHI, SSN, etc. After sensitive data is flagged within the metadata, this will trigger Panzura Symphony to run automated tasks to enact the data management policies that have been established.

By implementing a strong governance framework and ensuring compliance with relevant laws, businesses can avoid costly fines, penalties, and legal disputes. Additionally, staying compliant helps maintain a good reputation, which is increasingly important for customers who are concerned about how their data is being handled. Non-compliance, on the other hand, can result in significant legal exposure and reputational damage, which may require years to recover from.

03 Enhancing Data Integrity and Quality

Good data governance not only focuses on security but also ensures the quality and integrity of data. Businesses often rely on large amounts of data for decision-making, and if this data is inaccurate, incomplete, or inconsistent, it can lead to poor decisions and lost opportunities.

Life Sciences is a perfect example of the dire need for fast access to quality data. Ensuring the integrity and provenance of research data is vital for guaranteeing that the data is reliable, accurate, and has not been tampered with. This includes proper documentation and audit trails of data storage, access, and modification.

FDA 21 CFR Part 11 (Electronic Records and Electronic Signatures)

This regulation applies to the storage of electronic records in clinical trials and mandates that data storage systems for clinical records must maintain the integrity and authenticity of the records over time. Systems must ensure the data is secure and that there are controls in place to prevent unauthorized access, modification, or deletion of data. There must be provisions for data audit trails and version control.

Clinical Trial Data Retention (FDA and EMA Requirements)

Clinical trial data typically must be stored for a minimum of 2 years after the last marketing application for a drug, as per FDA and EMA guidelines. Some research may require longer retention periods depending on the research type e.g., long-term follow-up studies.

Archival of Biological Data

In some cases, biological data (e.g., DNA sequences, biological samples) may need to be stored for a much longer period, especially if they are linked to clinical studies or have potential for future reanalysis.

Good Clinical Practice (GCP)
GCP guidelines emphasize the need for accurate data collection, storage, and retention to ensure the reliability of clinical trial data. Researchers must establish an audit trail for data to ensure transparency and traceability of data changes, especially when storing clinical trial data.

Good Laboratory Practice (GLP)
Similar to GCP, GLP standards apply to preclinical and laboratory studies and require that all data be stored in a manner that ensures integrity, traceability, and long-term access.

Life Sciences applications leave behind massive artifacts. Their size makes very difficult to parse and scan, and they may take hours to download, depending on their location. Having accurate and up-to-date metadata — data about the data — is crucial. Metadata is a fraction of the size of the data itself and contains much, if not all, of the intelligence that data stewards need to query.

Panzura partners with GRAU DATA, whose MetadataHub product is capable of scanning and creating a metadata catalog of 400+ different file formats. MetadataHub will scan through all the artifacts, and create a unique metadata set that's specific to the company's needs. This metadata is easier and much faster to parse when searching for specific results, or just auditing the progress of a project.

Having instant access to all the metadata also enables the automated migration of these large artifacts from expensive local storage to archive and long-term archive storage until they are needed, complying with GCP and GCP. This data movement is managed by Symphony, following the policies created for treatment of data based on its characteristics. Long term archive would meet the requirements of FDA 21 CFR Part 11 and any long-term retention, at the lowest possible cost.

Corporate governance practices around data storage emphasize accurate data entry, validation, and periodic audits to ensure that data remains reliable over time. By aligning with compliance standards, organizations can ensure that their data storage practices adhere to industry standards for accuracy, accessibility, and consistency, ultimately improving business intelligence and decision-making processes.

04 Mitigating Risks of Data Loss and Downtime

Data loss or prolonged system downtime can be devastating for any organization. Whether it's caused by a natural disaster, system failure, or cyber-attack, the consequences of losing access to critical data can range from financial losses to reputational damage.

Corporate governance practices related to data storage should include disaster recovery and business continuity planning. Data backup procedures, redundant systems, and secure off-site storage can help ensure that in the event of an unexpected incident, the organization can recover quickly without significant loss. Compliance requirements, such as those outlined in ISO 27001 or SOC 2, often dictate specific measures for data backup, archiving, and disaster recovery, helping businesses prepare for and mitigate the risk of data loss.

Panzura's CloudFS platform is designed to mitigate the risks of data loss and downtime via high availability, redundancy, and immutability. You can read more about CloudFS [here](#).

Symphony can also be used to migrate data between storage tiers, utilizing immutable storage to protect against ransomware and malware. Learn more about Symphony data migrations and storage tiering [here](#).

05 Reducing Operational Costs

Although implementing data governance and compliance frameworks requires an upfront investment of time, resources, and effort, the long-term benefits often outweigh the costs. By centralizing data management within a platform like Panzura Symphony, and ensuring proper data storage practices, businesses can reduce inefficiencies, streamline operations, and prevent costly mistakes caused by poor data management.

A Strategic Imperative That Can Be Automated

As data becomes an increasingly important business asset, applying corporate governance and compliance principles to data storage is not just a regulatory requirement but a strategic necessity.

Organizations that prioritize data governance and compliance can better protect sensitive information, mitigate risks, meet legal requirements, and maintain operational efficiency.

When data breaches and privacy violations are headline news, a strong governance and compliance framework not only safeguards your data but also builds trust with customers and stakeholders. For organizations looking to remain competitive and compliant in a data-driven world, integrating and automating governance and compliance into their data storage strategy is essential for long-term success. By taking proactive steps to implement data governance and adhere to compliance standards, businesses can ensure that their data remains secure, accessible, and aligned with both internal policies and external regulations — creating a strong foundation for growth.

Panzura empowers today's digital-first organizations to do impossible things with file data, making them more agile, efficient, and productive. They trust Panzura to help them consolidate dispersed data, see and manage data in and out of the cloud, make it more cyber-resilient and AI-ready, and ensure it is available to people and processes where and when it's needed.

Discover how Panzura can fuel your success at **panzura.com.**