Delivering information you can trust

Information Management

Smart data governance solutions

Information protection and compliance with IBM System z

Do you ever wonder who accesses, views and uses your data—and for what purpose? You should. The collection, storage, use, sharing and processing of electronic data continues to rapidly increase as global communications create a "geographic transparency" that enables more organizations to interact and share information. While this increases the opportunity for new business and the chances of reaching many more customers, it also increases the risk of breaching ever-increasing sets of regulatory and compliance legislation.

Much of today's compliance regulation requires companies to retain their data for longer amounts of time, and both active and historic data must often be held securely with strict access controls. Privacy controls must be adhered to throughout the entire data life cycle—from development and testing to production and archiving. Data must be accurate and readily available for scrutiny by auditors and authorities. Failure to comply can result in heavy financial penalties, legal actions and, in some cases, prison sentences.

However, organizations must demonstrate their accountability by complying with industry, financial and regulatory guidelines and be able to answer the "who, what, when, where and how" questions about data access. Regulations exist at the worldwide level, in addition to the country- and state-specific laws and regulations that must be followed. Research shows that the perceived quality of a company's corporate governance can influence its share price, as well as the cost of raising capital.[1]

Compliance: A smart way to start your System z data governance journey

Even beyond the impact of global, country or state regulations, compliance makes business sense. The media is filled with stories of high-profile incidents where improper controls and misinterpretation of data have lead to nightmarish consequences, such as potentially life-threatening situations for healthcare patients, or massive fraud and theft in financial, retail and government organizations. The common criteria that caused all these organizations to suffer was lack of end-to-end data governance. No industry is immune from the fact that how you manage your business data directly impacts your business outcomes.

Compliance is a good place to start. It focuses on the *who*, *what*, *when*, *where* and *how*. It is one element of a wider data governance strategy built around the IBM Data Governance Framework created by the IBM Data Governance Council.

Data governance entry points

In 2005, IBM founded the IBM Data Governance Council with almost 50 other industry-leading companies and organizations to address the increasing risks and data exposures faced by businesses worldwide. The Council designed a data governance framework to help businesses understand the supporting and core disciplines and enablers of data governance. They also produced a maturity model to help assess and progress data governance within an organization.

Based on the governance framework and maturity model, three data governance entry points, namely *information quality*, *information lifecycle management* and *information protection* help organizations address their most pressing needs. Each is designed in support of lowering risks and costs, increasing revenue opportunities and delivering competitive differential, while at the same time enabling an organization to take a more holistic approach to a data governance strategy supported through workshops and assessments.

The information protection entry point

Information protection is a common entry point for organizations getting started with data governance. Protecting sensitive data serves a clear business need, and as previously discussed, protecting data is the goal of many current regulations. However, many organizations try to build their own compliance solutions, only to realize that they must to prove to auditors and legal authorities that their system is unbiased in its construction, operation and reporting. Organizations also often underestimate the cost of keeping their compliance systems up to date with frequent changes in regulations and legislation.

The business-focused capabilities of IBM® System z®—including advanced business continuity features; security, transaction integrity, scalability and dynamic workload balancing capabilities; and powerful tools for access control and protection—make it an excellent platform to store and process mission-critical data and information. It's estimated that 95 percent of Fortune 1000 companies store their business data on System z.[2]

IBM provides a set of System z tools for compliance that help secure access, encrypt your data and ensure privacy controls are in place throughout the information life cycle, combined with powerful but flexible analysis and reporting tools (see chart below).

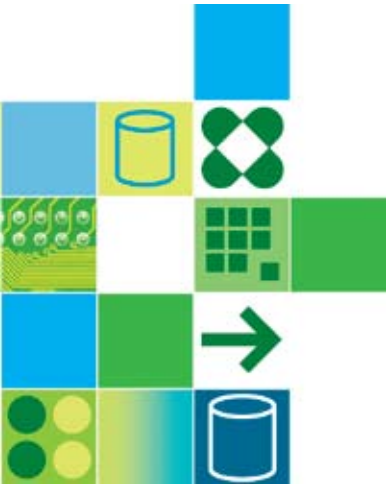
S Security	• Administration of users and passwords is independent of OS and IBM DB2® or IBM IMS™ users • Does not require auditors to be DB2- or IMS-defined users within the monitored system(s), to log on to the OS where the monitored system is running or have extensive interaction with system support personnel (database administrators/system administrators) • Auditor is unable to directly manipulate DB2 or IMS resources, presenting no security conflict between the gathering of auditing data and the users being audited
A Audit	• Centralized auditing of DB2 and IMS brings together information from many different sources into a correlated, coherent view • Enables auditors to collect, view, analyze and report on data, save it into an audit repository, automatically generate their own reports and export the data into other applications • Separation of roles • Low-cost audit data gathering
F Flexible reporting	• User interface reporting options enable auditors to view and report on data in a variety of ways: overview, subsystem, detail (with filters), graphical or tabular • Thresholds can be set to flag data that may need further investigation • Batch reporting
E Encryption	• Low-overhead encryption using cryptographic services on the System z platform • No application changes required • Supports IBM data encryption for DB2 and IMS databases
R Reliable privacy	• Contextual, application-aware test data de-identification enables organizations to substitute realistic, fully functional masked data for sensitive data • Helps ensures sensitive information does not end up in the wrong hands • Helps protects the organization from privacy-related fines and penalties

Start today with compliance as part of your System z data governance solution

Regardless of where you are in your data governance cycle, IBM can help make it easier to take the next step. For example, IBM can help you justify a compliance solution using the IBM Data Governance ROI calculator. Whether you have concerns with security, auditing and privacy, or whether you are not getting enough value from your data due to architectural, quality or general information management issues, IBM has the software, hardware, services and expertise to help you create and deliver a complete data governance strategy for System z and beyond.

For more information

For more information about IBM compliance and data governance resources, please contact your IBM representative or IBM Business Partner, or visit: **ibm.com**/software/data/system-z/data-governance/index.html



© Copyright IBM Corporation 2009

IBM Software Group
Route 100
Somers, NY 10589

Produced in the United States of America
October 2009
All Rights Reserved

[1] O'Donovan, Gabrielle. "A Board Culture of Corporate Governance." Corporate Governance International Journal, Vol. 6, Issue 3, 2003.

[2] Moutsos, Kim. "IMS at 40: Stronger than Ever." IBM Database Magazine. October 2008. www.dbmag.intelligententerprise.com/story/showArticle.jhtml?articleID=211300235

IBM, the IBM logo, ibm.com, and System z are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries or both. If these and other IBM trademarked terms are marked on their first occurrence in this information with a trademark symbol (® or ™), these symbols indicate U.S. registered or common law trademarks owned by IBM at the time this information was published. Such trademarks may also be registered or common law trademarks in other countries. A current list of IBM trademarks is available on the Web at "Copyright and trademark information" at **ibm.com**/legal/copytrade.shtml

Other company, product or service names may be trademarks or service marks of others.

Each IBM customer is responsible for ensuring its own compliance with legal requirements. It is the customer's sole responsibility to obtain advice of competent legal counsel as to the identification and interpretation of any relevant laws and regulatory requirements that may affect the customer's business and any actions the customer may need to take to comply with such laws. IBM does not provide legal advice or represent or warrant that its services or products will ensure that the customer is in compliance with any law.

References in this publication to IBM products or services do not imply that IBM intends to make them available in all countries in which IBM operates. Offerings are subject to change, extension or withdrawal without notice.

All statements regarding IBM future direction or intent are subject to change or withdrawal without notice and represent goals and objectives only.

IMB14059-USEN-00