



**Tivoli** software

# Address the key implications for compliance management.



## Contents

- 2 Introduction
- 3 Rely on best practices
- 5 Establish a central IT governance and compliance platform to efficiently manage policies and requirements
- 6 Explore a common controls example
- 8 Drive value through IT governance and compliance management solutions
- 9 Enforce policies and track changes across the organization
- 10 Restrict unauthorized access through defined policies and data disclosure requirements
- 12 Preserve and retain key business data
- 12 Help optimize system utilization through controlled policies
  - 13 *Simplify system optimization with change and release management*
  - 13 *Leverage a centralized view with availability management*
  - 13 *Manage resource performance with business service management*
- 14 Manage software inventory and use
- 14 Summary
- 15 For more information
- 15 About Tivoli software from IBM

## Introduction

In today's increasingly competitive environment, enterprises must simultaneously be flexible enough to exploit new opportunities, ensure that their organizations are functioning as effectively and efficiently as possible, and minimize risks. One of the biggest challenges IT organizations face in achieving their business goals is managing compliance activities. These challenges can drive up the demand for IT projects, straining resources that are needed to satisfy service level agreements while still managing the complexity of business processes. Furthermore, since IT operations are supporting these business processes, they are often responsible for providing the business with a view of its risk and regularly monitoring and documenting compliance status. The rising costs of managing IT processes and addressing these challenges have made it more important than ever to align IT with business objectives.

As a result, enterprises are becoming more systematic about the strategies and frameworks they have in place to optimize resources, reduce risk and gain more business value from compliance spending. *Governance* is that systematic process. While not a new concept, governance provides the oversight that can help ensure that the appropriate people are involved, that they are involved at the right time and that they can make informed decisions to achieve optimal outcomes. Because effective governance can help organizations weigh performance against objectives – whether they're prescribed by external factors or internal control – compliance management efforts are integral to governance.

As enterprises drive toward effective governance, they are looking for process models and frameworks to lead them on this journey. There are many governance frameworks available, but in most cases these frameworks recommend a continual process consisting of the following common steps, such as:

## Highlights

The IBM Service Management initiative provides an infrastructure on which IT processes can perform consistently, reliably and predictably to support the delivery of services to the business

- Collecting information.
- Analyzing this information and associated risks.
- Making policy decisions.
- Creating procedures and controls, including security, based on policy.
- Testing those controls to determine outcomes against policy, including business performance, value and compliance measures.

The IBM Service Management initiative provides an infrastructure on which IT processes can perform consistently, reliably and predictably to support the delivery of services to the business. IBM Service Management relies on best practices – such as those outlined in the IT Infrastructure Library® (ITIL®) and Control Objectives for Information and related Technology (COBIT) – in order to build a management infrastructure that delivers business-critical IT services. When organizations treat compliance as a set of formally managed IT processes, it can ultimately become a business enabler, helping organizations streamline operations, minimize total cost of ownership and obtain the agility needed to proactively stay ahead of new initiatives.

This paper describes how IBM Service Management can help an organization address compliance issues by providing an integrated, sustainable strategy for IT governance and compliance management. It also offers details on the wide-ranging approach that IBM delivers – including hardware, software and business consulting – to help tackle service management.

### **Rely on best practices**

Proactively measuring IT governance and compliance depends on effectively managing relevant IT process controls. An organization must define, assess and monitor the status of IT processes to maintain desired levels of IT service, security, availability and performance. A process controls framework – based on best practices – can help effectively implement policies while providing a link to business controls, including controls over financial reporting. An IT process controls framework should help address elements such as:

- **Confidentiality.** Protect sensitive information from unauthorized disclosure or intelligible interception.
- **Integrity.** Safeguard the accuracy and completeness of information and software.
- **Availability.** Make information and vital IT services available when required.
- **Performance.** Provide information and services with a high level of efficiency.

There are many different process controls frameworks and guidelines regarding which controls are important and measurable in an organization. Some of the best-known controls frameworks include:

- Committee of Sponsoring Organizations of the Treadway Commission (COSO) — key financial controls framework.
- International Standards Organization (ISO) 9001 — quality controls framework.
- COBIT — IT controls framework.
- ITIL — IT service support framework.
- ISO 17799/ISO 27001 — IT security framework.

Each of these frameworks plays a particular role in the overall governance objectives, helps maximize business integrity in the execution of IT services and corporate governance and provides IT services to help protect against unauthorized access and unforeseen risks.

For example, COBIT is a process model that offers a comprehensive view of IT organized by planning, building, deploying and monitoring functions. The control objectives mentioned in COBIT describe the types of criteria an IT organization should be judged against. They represent a set of metrics that help ensure an IT organization is aligning its work with business objectives. ITIL and information security standards, such as ISO 17799 and ISO 27001, represent industry best practices for how to achieve those control objectives. COBIT describes what to do, while ITIL and ISO give more detail on how to do it.

## Highlights

Integrating and automating an IT process controls framework is central to effective IT governance and compliance

Similarly, the IT Governance Institute's new IT value framework (Val IT) extends COBIT by focusing on the investment decisions and realization of benefits. The framework is also consistent with the CIO Executive Board's eight steps for the strategic management of IT.

IBM Tivoli® Unified Process, which defines a series of IBM Service Management processes that are consistent with the guidance in ITIL, provides further guidance and can be deployed to and integrated with an existing IT environment.

### **Establish a central IT governance and compliance platform to efficiently manage policies and requirements**

Integrating and automating an IT process controls framework is central to effective IT governance and compliance. When necessary information is spread across multiple systems and applications, it can be difficult to consistently deploy the controls to help maximize business integrity. A compliance strategy designed to address each of these various domains is important. IT organizations should also take a life-cycle approach, including:

- Defining compliance policies.
- Designing and implementing those policies into systems and applications.
- Monitoring and reporting on compliance within systems and applications.
- Taking action to address noncompliance issues.

An integrated IT governance and compliance management system helps enforce policies consistently across all domains and helps optimize operational costs and efficiencies. For instance, when an organization automatically applies established policies to control user access, it can simultaneously identify and report on noncompliant settings.

### **Explore a common controls example**

To better understand how an integrated IT governance and compliance management system helps enforce policies across the enterprise, we will examine a common controls example in which a business wants to provide a closed-loop system for automating the management of sensitive business information.

The CIO sets a policy to store a particular set of critical business data for at least five years and prevent unauthorized disclosure of and access to it. The IT managers establish IT process controls – data retention windows, access controls, mandatory baseline server configurations and more – to support this policy.

But because most firms deploy these controls manually, three key problems can arise:

1. **The controls are deployed inefficiently.** Fully provisioning user access across heterogeneous resources demands significant resources and time. Often, it takes more than a week to:

- Determine which resources must be modified.
- Determine who owns the resources.
- Gather required approvals.
- Implement changes.
- Verify on a repeatable basis that these and subsequent changes are valid.

2. **The controls are deployed ineffectively.** Manually implementing policies across multiple, heterogeneous resources can increase the likelihood of implementation disparities. Additionally, a heterogeneous environment can make it difficult to gain the comprehensive view needed to monitor controls.

### Highlights

The ability to log and manage events and incidents relevant to compliance is a critical part of the information-gathering process

**3. Compliance-related events are not monitored.** The ability to log and manage events and incidents relevant to compliance is a critical part of the information-gathering process. Regular review of relevant log and audit trails, along with documentation showing proof of these reviews, is an important step in creating an effective control environment.

Moreover, ongoing maintenance is usually handled by a variety of local administrators, who inadvertently or purposefully can cause noncompliance by:

- Trying to manage available storage resources by setting much shorter data retention windows than required by policy.
- Neglecting to update underlying systems with the latest application and security patch levels.
- Satisfying localized requests to allow additional users to access restricted data.
- Subverting password reset, access control or change management policies.

To avoid these potential threats to the availability of restricted data, the organization is faced with the following challenges:

1. Detecting policy violations without manually checking the settings of every system, user and user attribute on an ongoing basis.
2. Discovering policy violations prior to the next audit event.
3. Remediating policy violations automatically, in a closed-loop manner.
4. Documenting and auditing policy violations without relying on spreadsheets that are updated by local administrators.
5. Notifying all relevant parties when hardware and software contracts and licenses are due to expire, to enable effective analysis of product use and facilitate effective renewal negotiation.

A key to addressing these issues is to automate these processes in a repeatable and auditable manner. When an organization uses IBM Tivoli software to automate these processes, it can capture best practices – by creating, customizing and storing workflows – to help minimize the costs of maintaining effective controls. These workflows facilitate business agility by helping an organization act quickly in response to change.

#### **Drive value through IT governance and compliance management solutions**

IBM offers solutions that define, automate and monitor IT governance and compliance management in a repeatable manner across businesses of any size. The solutions span a range of IT processes – such as availability, configuration, security and storage management – that address IT governance and compliance projects. Based on the IBM Service Management model and executed through best practices such as COBIT and ITIL, these solutions seamlessly integrate with each other to help an organization achieve an end-to-end view of IT governance and compliance measures.

IBM Service Management is comprised of:

- **IT Process Management Products** — integrate and automate IT management processes across organizational silos for rapid responsiveness and greater flexibility.
- **IT Service Management Platform** — streamline team workflow and improve auditability and control over software delivery assets to provide portfolio management and support for today's globally distributed development teams.
- **IT Operational Management Products** — automate tasks to address application or business service operational management challenges.
- **Best Practices** — worldwide practical experience from proven consulting services to help maximize current investments and make IBM Service Management and ITIL actionable.

With IBM IT governance and compliance management solutions, an organization can efficiently and effectively manage assets across organizations, provision and update resources appropriately, and track resource usage. All of these

capabilities feed back into an IT governance and compliance management process framework. Using an integrated yet highly modular approach, an organization can address the process areas that generate the greatest value first, and then build out other process areas as requirements evolve and change.

- IBM Tivoli Change and Configuration Management Database (CCMDB) is the IBM Service Management platform that helps standardize and share information through an open, federated change and configuration management database.
- IBM Tivoli identity and access management solutions help maximize the effectiveness and efficiency of internal controls for provisioning, enforcing, managing and auditing user access to IT systems.
- IBM Tivoli threat management solutions help companies minimize technical risk factors such as security threats.
- IBM Tivoli availability and release management solutions help mitigate risks to availability by implementing processes to support automated change management across systems.
- IBM Tivoli storage and information life-cycle management solutions help companies meet data retention and change management requirements.
- IBM Tivoli asset management solutions help enterprises optimize their asset investments by tracking assets and their usage, then integrating this information with contract and license information. Consequently, an organization can make good decisions and take informed actions about how to best use the assets and asset expenses to respond to the needs of the enterprise.
- IBM Tivoli security information and event management solutions help effectively and efficiently monitor the health of the security environment, monitor and enforce security policies, and detect and respond to security-related incidents whether from external attackers or insider threats.

#### **Enforce policies and track changes across the organization**

An IT infrastructure with good compliance management practices requires strong management of change on all resources – from servers and storage devices to networks – as well as the middleware, applications and data that reside on these resources. Effective change management enables:

- Change tracking.
- Prioritization of changes based on application importance.
- Anticipation of the impact of changes, to lower risk of service interruptions and failures.

## Highlights

Tivoli CCMDB maps IT resources to an application; tracks configuration changes to the application and its supporting resources; and helps automatically discover and federate IT information spread across the enterprise, including details about servers, storage devices, networks, middleware, applications and data. By integrating, automating and optimizing data, workflows and policies, Tivoli CCMDB can help an organization:

- Align the ongoing management of its IT infrastructure with its business priorities.
- Manage and interpret architectural complexity.
- Reduce incident and problem management costs.

### **Restrict unauthorized access through defined policies and data disclosure requirements**

To achieve compliance, IT staff should work to effectively and efficiently eliminate the presence of invalid accounts, remove network and system vulnerabilities so that the infrastructure is not compromised and provide ongoing monitoring of the security posture of the IT environment so that when incidents occur, they can be managed expeditiously.

Manually monitoring and auditing production systems, network devices and applications in today's distributed, heterogeneous IT environments is neither efficient nor effective

However, manually monitoring and auditing production systems, network devices and applications in today's distributed, heterogeneous IT environments is neither efficient nor effective. There is too much data, too much change and too much room for human error.

- IBM Tivoli security management applications provide integrated and automated capabilities to assist IT staff with implementation, management and real-time monitoring of security policies.
- IBM Tivoli identity and access management software for security provides self-managing capabilities to manage access, giving users simplified access to critical applications in compliance with security policies. These solutions also generate audit trails to report on the effectiveness of IT security controls.
  - IBM Tivoli Access Manager products help control IT resource and application access privileges across the enterprise — according to corporate policy and privacy requirements. Using a consolidated, policy-based approach to access control helps reduce the need to manually code security into each application, and helps minimize deployment and administration costs.

- IBM Tivoli Federated Identity Manager facilitates collaboration between enterprises, customers and partners to provide security for a service oriented architecture (SOA). It extends management of access privileges to IT resources and applications across enterprise boundaries or security domains.
- IBM Tivoli Federated Identity Manager Business Gateway provides small-to-midsize organizations with an ideal entry point for establishing federated Web single sign-on (SSO) capabilities that bring together customers, partners and suppliers.
- IBM Tivoli Identity Manager provides a single point for creating and managing user accounts across resources. Through a robust workflow engine, Tivoli Identity Manager enables an organization to automate the user provisioning process — including approvals and account creation — as well as the user deprovisioning process, to mitigate the risk of invalid accounts and privileges.
- IBM Tivoli security information and event management software analyzes system event data to determine policy infractions, internal misuse and external attacks. It also enables IT staff to quickly detect, investigate, isolate or mitigate security-related incidents before they impact system availability and performance or allow for damage, theft or misuse of critical data.
  - IBM Tivoli Compliance Insight Manager offers an easy-to-use security compliance management dashboard that summarizes billions of log files in one overview graphic to help you detect insider actions on sensitive or confidential information assets. Through this dashboard, you can gain an overview of your security compliance management posture, understand user activities and security events in comparison to requirements and acceptable-use frameworks, and monitor privileged users and exceptions to change management policies. A library of compliance-oriented reports and an intuitive custom reporting engine allow you to provide audit documentation quickly and easily to help you ensure that your controls are operating as planned.
  - IBM Tivoli Security Operations Manager provides a security operations-focused dashboard from which to monitor the security posture of the IT infrastructure. It correlates and analyzes heterogeneous security data throughout the IT environment to detect security-related incidents. The dashboard can then be used to track, investigate and mitigate incidents related to malicious attacks, malware, network and system misconfigurations, and internal misuse.
  - IBM Tivoli Security Compliance Manager can help an organization detect security risks quickly and deal with them proactively by scanning servers and workstations to verify that IT security controls are in place and that systems comply with security policy.

### Highlights

By managing information from creation to disposal, an organization can eliminate unneeded points of management and help minimize the number of physical devices in the infrastructure

#### Preserve and retain key business data

Information life-cycle management (ILM) helps an organization maximize the business value of storage. By managing information from creation to disposal, an organization can eliminate unneeded points of management and help minimize the number of physical devices in the infrastructure. IBM storage management solutions help an organization take into account its corporate governance policies, business processes and compliance guidelines as it establishes its ILM policies.

- IBM Tivoli Storage Manager can help automatically back up or archive key files to nonrewritable, nonerasable storage when unprotected data or illegal files are detected. These capabilities help administrators identify key corporate data at risk of not being backed up or archived. An organization can also define policies that enable it to keep files for a specified amount of time, then automatically expire them from its tiered storage.
- IBM TotalStorage® Productivity Center can help proactively monitor the storage infrastructure, enabling an organization to predict potential outages and rapidly resolve problems if and when they occur.
- IBM System Storage™ Archive Manager can help facilitate compliance with policy requirements in a flexible and function-rich manner. It helps manage and simplify the storage and retrieval of the ever-increasing amount of data that organizations retain.
- IBM System Storage Data Retention 550 (DR550) is a preconfigured, integrated offering to help store, retrieve, manage, share and retain.

#### Help optimize system utilization through controlled policies

Maintaining availability means that an organization needs to rapidly deploy software releases and patches, as well as frequently make PC and server configuration changes across complex IT environments. Organizations need a way to monitor the business impact of an IT outage and have real-time data to assess service level compliance. In the absence of controls, it can be difficult to link and define compliance processes to IT.

***Simplify system optimization with change and release management***

IBM Tivoli change and release management solutions offer automated capabilities to help simplify the continued optimization of systems.

- IBM Tivoli Configuration Manager enables an organization to capture and store workflows that represent best practices for distributing software and patches throughout the enterprise. By subscribing users, groups of users, end points, pervasive devices, profile managers or inventory query results to a particular reference model, an organization can drive automated compliance through standards and requirements.
- IBM Tivoli Provisioning Manager enables the automation of key data center tasks in accordance with enterprise or industry best practices. This strategy helps operators consistently effect changes that are compliant with predefined policies. It can also help deploy and maintain software elements — including operating systems, patches, middleware and applications — at desired configuration levels.

***Leverage a centralized view with availability management***

IBM Tivoli availability management solutions leverage a centralized view that lets an organization monitor and manage linkages between IT systems and business processes.

- IBM Tivoli Monitoring links IT services to processes, data, skills and tools through a single-user workspace, allowing organizations to view consistent data across technology domains and align IT services with business goals to deliver immediate value.

***Manage resource performance with business service management***

IBM business service management solutions help an organization understand how the performance and availability of IT resources affect applications, processes and services. The solutions help prioritize systems around processes that carry the highest business values.

- IBM Tivoli Business Systems Manager lets an organization monitor and manage IT resources in the context of business priorities. Through an executive dashboard, organizations can easily view the availability of their most critical business services and any associated service level agreements. With this real-time information, they can make IT resource decisions to help minimize the high cost of application downtime and optimize business impact.

### **Manage software inventory and use**

Managing the hundreds or thousands of software applications running within an environment – and the contracts related to these applications – remains a complex undertaking. Few IT organizations possess the resources to manually track software inventory and use, or maximize related compliance – for both the distributed and mainframe platforms – to quickly adjust to business needs. Many IT professionals struggle to retrieve contract details stored across multiple departments prior to contract renegotiations. As a result, they often have difficulty reporting software inventory and use activity links to contract terms to prove compliance, which can lead to failed audits.

- IBM Tivoli Contract Compliance Manager provides end-to-end software asset management to help simplify these tasks by storing contracts in a central database. It helps organizations validate invoice information; report on financials enterprise wide; validate product installation, removal and unauthorized use; and facilitate disaster recovery planning. It also enables planning for upgrades and consolidations.
- IBM Tivoli License Compliance Manager for z/OS® and IBM Tivoli License Manager combine with Tivoli Contract Compliance Manager to automate the collection of end-to-end measurements of installed software and use, and facilitate compliance reporting on hosted and distributed platforms. In Tivoli Contract Compliance Manager, this critical data can be linked to existing contracts and license entitlements to support internal and external audit processes. The data can also be used to facilitate decision making about the best use of the assets and asset expenses to respond to the needs of the enterprise.

### **Summary**

Taking a proactive approach to compliance management and governance can give an organization the agility it needs to respond to a variety of challenges it faces – both today and in the future. A centralized, automated approach not only enables organizations to effectively control information and rapidly make it available to meet audit requirements, but also facilitates enforcement that helps protect the integrity of the entire IT infrastructure – and can enhance customer, business partner and employee relationships.

IBM compliance management solutions help enterprises maximize their existing and future technology investments through IBM Service Management. These solutions complement other IBM products (including IBM Lotus® and IBM DB2® software and IBM Business Consulting Services) to support a wealth of other IBM hardware and software offerings. Establishing a robust compliance management infrastructure can help provide the flexibility and integration required to quickly adapt to changing market requirements and capitalize on new opportunities.

**For more information**

To learn more about IBM compliance management solutions or to find out how IBM can help you develop a compliance strategy to meet your unique business requirements, contact your IBM representative or IBM Business Partner, or visit [ibm.com/tivoli/solutions](http://ibm.com/tivoli/solutions)

**About Tivoli software from IBM**

Tivoli software provides a set of offerings and capabilities in support of IBM Service Management, a scalable, modular approach used to deliver more efficient and effective services to your business. Helping meet the needs of any size business, Tivoli software enables you to deliver service excellence in support of your business objectives through integration and automation of processes, workflows and tasks. The security-rich, open standards-based Tivoli service management platform is complemented by proactive operational management solutions that provide end-to-end visibility and control. It is also backed by world-class IBM Services, IBM Support and an active ecosystem of IBM Business Partners. Tivoli customers and business partners can also leverage each other's best practices by participating in independently run IBM Tivoli User Groups around the world – visit [www.tivoli-ug.org](http://www.tivoli-ug.org)



© Copyright IBM Corporation 2007

IBM Corporation  
Software Group  
Route 100  
Somers, NY 10589  
U.S.A.

Produced in the United States of America  
6-07  
All Rights Reserved

DB2, IBM, the IBM logo, Lotus, System Storage, Tivoli, TotalStorage and z/OS are trademarks of International Business Machines Corporation in the United States, other countries or both.

IT Infrastructure Library is a registered trademark of the Central Computer and Telecommunications Agency which is now part of the Office of Government Commerce.

ITIL is a registered trademark, and a registered community trademark of the Office of Government Commerce, and is registered in the U.S. Patent and Trademark Office.

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

**Disclaimer:** The customer is responsible for ensuring 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 reader may have 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 or regulation.

**TAKE BACK CONTROL WITH** 