Implement and enforce security policies and report on your compliance efforts.

Organizations face ever-growing pressures that continue to increase in number and complexity every year. Today’s enterprises must protect the confidentiality of data and maintain the integrity of the data while continuing to make it highly available for the trusted users, applications and services that require it. Leading companies realize that the information and discipline associated with compliance initiatives can be linked with performance management efforts to help:

- Improve information management and operational understanding.
- Increase efficiency by standardizing processes and eliminating manual activities.
- Focus their resources toward forward-looking, innovative projects.

### Highlights

- Establish a foundation for compliance that helps meet your requirements
- Leverage leading process control frameworks to identify and achieve compliance objectives
- Track and enforce security policy on the activities of privileged users
- Centrally collect and rapidly analyze enterprise-wide security event information to help prevent intrusions
- Streamline enforcement of server and desktop-system configuration policy
- Centralize audit trail and log file collection to facilitate analysis and investigation
- Use an innovative compliance dashboard, patent-pending plain-language translation of collected data into compliance information and best practices–derived reports to authoritatively demonstrate the effectiveness of compliance efforts to auditors
- Centralize audit trail and log file collection to facilitate analysis and investigation
- Use an innovative compliance dashboard, patent-pending plain-language translation of collected data into compliance information and best practices–derived reports to authoritatively demonstrate the effectiveness of compliance efforts to auditors
Because IBM understands that a strong foundation can address compliance requirements while improving business health, we offer a broad portfolio of compliance management, security auditing and reporting solutions to help you meet these needs. IBM software, professional and managed services, systems and financing options help an organization to implement, enforce and demonstrate the effectiveness of its privacy and security controls. Compliance management, security auditing and reporting are a few of IBM security solutions that help customers establish effective risk management strategies to manage and secure business information and technology assets, anticipate vulnerabilities and risk, and maintain timely access to information. IBM security solutions help organizations align technology with business priorities — redirecting resources that might otherwise be dedicated to resolving security problems toward innovative initiatives that deliver substantial value to the business.

The following pages describe ways that organizations can leverage strategic thinking and IBM offerings to help establish a robust platform for compliance initiatives.
Use a best-practice framework to determine corporate security policy

Creating a comprehensive policy framework is the foundation for a sound information security program. Generally speaking, only written policies and procedures can be enforced. Consequently, an industry best practice for the policy framework is to include policy statements, technical standards, specific detailed procedures and technologies to enforce them.

IBM Security Governance Services can help you develop a strategy to improve compliance efforts and then maintain your compliance posture. These services use industry-leading frameworks and standards, including the IBM security solutions framework that has aided numerous clients. IBM Security Governance Services cover broad capabilities that range from risk management to security program design to regulatory and standards compliance.

Additionally, IBM Internet Security Systems Professional Security Services can assist with gap assessments, policy development and remediation of security issues related to regulations.

Implement and enforce security policy in an integrated, automated fashion

Once your organization has derived its information security policies from best practices and its specific needs, it must implement and enforce these policies. To do so most effectively, your organization should automate its process controls wherever possible — not only to drive consistency but also to help minimize errors and the burden of manual enforcement and reporting on your IT staff. IBM offerings for compliance management, security auditing and reporting help you translate your process controls into well-defined, enforceable policies; monitor and report on compliance; and even initiate remediation when noncompliance is identified.

One area that is particularly challenging and important is controlling and tracking the actions of privileged users. Consul InSight Security Manager enables you to monitor security policy compliance for users who might otherwise escape notice as a result of the privileges they need to perform their important responsibilities. With it, you can log the activities of system administrators and system operators as well as access to sensitive data — even from root administration and database administrator (DBA) accounts. Additionally, Consul InSight Security Manager helps you automate and regularly review these logs as well as those for applications, database operating systems and devices. All the while, the software helps you build a record of how you analyze, investigate and remediate security incidents and suspicious activity, to help you respond quickly and authoritatively to auditor requests.

To help you address threats rapidly, IBM Tivoli® Security Operations Manager offers a security information and event management (SIEM) platform from which you can quickly analyze disparate network-level information from across the enterprise. Manual collection and analysis of security data across intrusion detection systems, firewalls, virtual private networks, antivirus applications and more represents an impractically large and expensive task. Tivoli Security Operations Manager automates and centralizes information collection, analyzes the information using complementary correlation techniques and prioritizes the security incidents it
identifies according to your business priorities. By providing a holistic view of your security posture and enabling you to drill down and investigate attacks quickly, Tivoli Security Operations Manager helps prevent intrusions that would hamper your ability to comply with regulations and SLAs.

Enforcing your policies for the configuration of various servers and desktop systems throughout your enterprise is another key part of compliance that can be overwhelming and inconsistently handled if not done in an automated, centralized manner. IBM Tivoli Security Compliance Manager helps you quickly build highly tuned and meaningful security policies, detect security violations and provide steps for remediation. For example, you can enforce password requirements, up-to-date antivirus installations, prohibitions on unnecessary or potentially dangerous services, and much more. The software also performs follow-up checks that verify how and where violations have been corrected, to help you demonstrate that your policies are being followed.

Other IBM offerings that help you implement and consistently enforce security policy include Tivoli identity and access management software. These products help you create and manage the life cycle of user identities (including prompt deletion for expired identities), consolidate access control across applications and extend access management across enterprise boundaries or security domains.

IBM Internet Security Systems designed the Virtual Security Operations Center to help you cost-effectively optimize resources, enhance profitability, improve flexibility and responsiveness, and address compliance requirements. From a high-impact, Web-based portal, you can view and manage in real time your entire security operation, including managed and unmanaged devices (from both IBM and other vendors), security intelligence, reporting, archiving, remediation, escalation and collaboration with IBM Managed Security Services analysts. The Virtual Security Operations Center helps you minimize the complexity and burden of manual data analysis while improving the accuracy of security event identification, incident escalation and remediation.

Prove the effectiveness of compliance efforts using a centralized approach

The offerings described in this document and many others from IBM collect information from across the enterprise that is of interest to auditors. Many of them can format that information into report templates to help you respond quickly and accurately to audit requests. But when these solutions and security monitoring products from other vendors deliver policy violation data to Consul InSight Security Manager, your organization can:

- Automate and centralize the collection of audit logs and log files to make the process more efficient.
- Reliably store and retrieve logs across the enterprise to facilitate compliance efforts.
- Leverage easy-to-use search capabilities to optimize analysis and forensic investigation of potential security incidents contained in the stored logs.

Consul InSight Security Manager can capture application audit logs, in-depth operating system logs and detailed database logs. It also offers a log continuity report so that you can rapidly demonstrate the completeness and continuity of your program for collecting and managing logs.
Once you have captured all the relevant logs throughout your organization, you also need a way to make sense of the massive amount of information. The Consul InSight Security Manager compliance dashboard summarizes log files on one overview graphic, enabling users to quickly view the organization’s compliance posture and easily understand how user activities and security events compare to acceptable-use frameworks.

What’s more, the patent-pending Consul InSight W7 methodology translates native log formats into easily understood language so that you can plainly understand Who did What, When, Where, Where from, Where to and on What.

Consul InSight Security Manager also allows you to produce reports that address specific reporting needs. And customizable templates help you jump-start monitoring and reporting activities for your organization’s specific needs.

For those looking to outsource their security operations, highly cost-efficient security event and log management services are available from IBM Internet Security Systems Managed Security Services. Enabled by the Virtual Security Operations Center, these services can deliver detailed reports in real time, and thereby facilitate in-depth operational analysis that streamlines the process of documenting compliance. IBM Internet Security Systems Managed Security Services can store logs for up to seven years to give you complete access to archived data through ad hoc and customized queries and reports.

For more information
IBM provides a full range of solutions to help you address your compliance management, security auditing and reporting requirements. Whether you need to implement a best-practice framework for your organization’s security policy, integrate and automate your enforcement processes, or demonstrate compliance effectiveness to auditors, IBM can help. When you want to leverage compliance initiatives to not only address regulatory and SLA requirements but also drive business efficiency and performance, turn to IBM.

For more information about how your organization can use IBM security solutions to implement, enforce and report on compliance efforts — or to find the IBM security solutions entry point that is right for your organization — contact your IBM representative or IBM Business Partner, or visit ibm.com/itsolutions/security

About IBM solutions for enabling IT governance and risk management
IBM enables IT organizations to support governance and risk management by aligning IT policies, processes and projects with business goals. Organizations can leverage IBM services, software and hardware to plan, execute and manage initiatives for IT service management, business resilience and security across the enterprise. Organizations of every size can benefit from flexible, modular IBM offerings that span business management, IT development and IT operations and draw on extensive customer experience, best practices and open standards–based technology. IBM helps clients implement the right IT solutions to achieve rapid business results and become a strategic partner in business growth. For more information about IBM Governance and Risk Management, visit ibm.com/itsolutions/governance