



# Achieving end-to-end information security: five critical steps.



August 2008

## Contents

- 2 Introduction**
- 3 Helping increase availability and decrease risk**
- 4 Achieving security balance, step by step**
- 5 Step 1: Define controls**
- 6 Step 2: Discover and classify**
- 6 Step 3: Enforce controls**
- 7 Step 4: Address data retention**
- 8 Step 5: Monitor, audit and report**
- 8 IBM: a trusted advisor**
- 11 Summary**
- 12 For more information**
- 12 About IBM Service Management**

### Introduction

Information is one of the greatest sources of value creation for organizations today, with nearly every aspect of an enterprise dependent on a continuous flow of data. Think of it as currency – freely traded across and beyond the organization, it can yield a significant return on investment, including increased collaboration and innovation, shortened time to market and better decision making.

At the same time, information is one of the greatest sources of risk for organizations today. Whether through intentional or inadvertent means, breaches of data security can expose organizations to regulatory fines or legal actions, reduce a company's competitive advantage and undermine customer confidence. In recent years, lawmakers worldwide have responded to data security breaches with more rigorous data privacy laws.

As data privacy mandates continue to multiply, so too can the risk. Eliminating the risk altogether, however, is not the goal. Were that the case, the solution would be easy: simply lock down both the data and access to it – thus also shutting down the vital link to employees, customers, business partners and suppliers that makes innovation and collaboration possible.

A more sophisticated information security strategy takes a risk management approach that balances risk and reward – availability vs. the confidentiality and integrity of data. This strategy requires the ability to identify and classify sensitive data and mission-critical information within the enterprise and determine the various points of access to this information and the security posture of those access points – all while tracking who has accessed that data and understanding what they have done with it.

## Highlights

Organizations also should protect their own intellectual property from internal threats and ensure data security for the stakeholders' benefit

This paper discusses the challenges of safeguarding critical data while maintaining a continuous flow of information, and describes five key steps organizations can take to help determine their information risk tolerance, better understand potential security issues, and help minimize the breadth and potential impact of those issues.

### **Helping increase availability and decrease risk**

As organizations become more interconnected, they are steadily increasing access to a wide range of information sources. Where availability was once limited by technology constraints, an expanding volume of data is now making its way to growing numbers of employees, suppliers, business partners and customers. This increased availability can present considerable security and compliance challenges. Not only must organizations protect their own intellectual property from internal threats such as supply chain partners and employees who accidentally mishandle information, organizations also should ensure data security for the stakeholders' benefit, including private customer data, as well as financial data where the stakeholders include investors.

As with any strategic asset, information must be backed by a resilient and secure infrastructure that supports compliance measures. Traditionally, however, information has been secured primarily through a perimeter-based approach that relied on firewalls and other point products. These solutions are no longer viable for today's environment. Web-based technology has both enabled and extended the need to collaborate beyond perimeter borders. Security also should be focused on the data itself, safeguarding it wherever it is, from creation to end point, whether it's at rest or in transit.

Ultimately, information security boils down to these questions:

- Who has access to what data?
- What critical/sensitive data do I have?
- What are the points of access to it?
- When is it being accessed?
- Where is the data located?
- How are those access points protected?
- How do I monitor and report on who accesses my critical data?

A holistic, business-driven approach to information security can help provide answers. Through the ability to define, classify and enforce policies and controls based on best practices, organizations can unify who, what, when, where and how to protect data through every step of the information lifecycle.

#### **Achieving security balance, step by step**

Reaching a desired security posture that can meet business and compliance requirements requires an enterprise-wide approach that directly maps to the business needs of the organization. Information security can't be accomplished in a silo; it should be aligned with the entire business continuum, including people, processes and technology, and balanced against acceptable levels of risk.

Applying the right controls can help organizations proactively and responsibly manage information-based risk. The challenge is to find the right balance of controls – rigid enough to secure data throughout its lifecycle but not so rigid that they stifle collaboration. It requires not only examining the current security posture and the processes around it, but also identifying the correct level of security to match identified and potential risks, and the steps needed to get there.

### Highlights

IBM offers adaptable security solutions to help organizations take the necessary steps to reach their desired state of information security

Drawing on a deep understanding of today's threats to data security from within and beyond the organization, IBM offers adaptable security solutions based on robust methodologies to help organizations take the necessary steps to reach their desired state of information security. These steps encompass the information security lifecycle that requires you to:

- Define controls.
- Discover and classify.
- Enforce controls.
- Address data retention.
- Monitor, audit and report.

The following sections of this paper describe the five steps in greater detail.

#### Step 1: Define controls

Creating an effective information security infrastructure starts with defining appropriate controls and related processes based on relevant standards, data security requirements and business needs. This step includes comparing your current security posture against risk assessment results to determine gaps and identifying both strengths and weaknesses of your current security practices.

As you uncover potential exposures, you should be able to prioritize them based on a risk assessment. By putting a repeatable methodology in place, you can address risk in a comprehensive and integrated way, allowing you to rank the level of risk based on the business need. For example, classified customer data would be assessed as high risk and thus require higher security measures. In turn, you can then create appropriate security policies that help set the stage for how processes and procedures can achieve the controls you establish, with the ability to proactively address risk before problems occur.

## Highlights

Applying a consistent, efficient way to find and handle information can help organizations stay ahead of threats, increase the availability of information and reduce the risk of financial loss, liability and compliance issues

### Step 2: Discover and classify

To protect information effectively, organizations should be able to identify sensitive data, determine where it resides and who can access it. These decisions must take into account the need to protect data and applications across the entire infrastructure, including network, end points and physical security. Compliance requirements must also be taken into consideration, many of which mandate storing documents for a specified amount of time, classifying data by sensitivity and ensuring proper controls such as encryption are in place for those assets.

The sheer volume of ever-expanding data necessitates an efficient way to find and classify important data, and make consistent decisions regarding the handling of it. Automation tools can help organizations automatically discover, classify, apply retention policies and store electronic records according to fiscal and compliance requirements. Applying a consistent and efficient means of finding and handling information can help organizations stay ahead of threats, increase the availability of information and reduce the risk of financial loss, liability and compliance issues.

### Step 3: Enforce controls

Protecting the confidentiality, security and availability of information requires organizations to validate the authenticity of all users who access resources, define what they are entitled to access, and monitor to help ensure that access controls are consistently enforced. Access to data should be controlled at the point of use, including the potential to be shared through authorized parties or intercepted in transit, and while connected or disconnected from the network. This level of security requires effective identity and access management capabilities that enable organizations to centrally manage user identities and authorizations, along with the ability to audit and report on policy compliance.

In order to manage the demands on IT staff in this environment of increasing complexity, it is imperative that these capabilities should help reduce burdensome tasks for both IT staff and end users through the ability to automate user provisioning, as well as providing single sign-on (SSO), self-help and secure audit reporting. A cross-boundary federated identity management platform can help extend user authentication and credentials across enterprises to promote more effective, secure collaboration among partners, suppliers and customers.

**Step 4: Address data retention**

As the number of specific information storage requirements continues to escalate due to data growth, organizations need secure, scalable and integrated archiving solutions that can be used to carry out established retention policies and reporting. These solutions should provide index and search capabilities to make it easier to locate data when it is needed. Storage-tier environments can help reduce costs for data that needs to be held for longer periods of time. By allocating lower-value or inactive data to lower-cost storage resources, more space can be freed for high-priority data in the most cost-effective and time-efficient manner. In addition, progressive incremental backup and restore capabilities can back up only new or changed versions of files to help reduce data redundancy and storage consumption.

## Highlights

### Step 5: Monitor, audit and report

To help ensure existing controls and policies are adequately protecting sensitive or regulated information, organizations should constantly monitor their security posture relative to their end goal. This final step closes the loop on the information security lifecycle, enabling organizations to monitor, audit and report on activities related to information security. Continual monitoring can provide greater visibility into security operations with an enterprise-wide view of who is accessing data and the effectiveness of existing security policies. At the same time, it can help organizations quickly identify abnormal data access patterns to more proactively detect threats and take action to respond to incidents. Automation capabilities can generate efficiencies through the ability to collect, analyze and respond to threats and events. Automation can also streamline compliance auditing and reporting by automatically tracking events and generating reports, helping to create cost-efficiencies throughout the organization.

### IBM: a trusted advisor

As you're considering strategies to help safeguard business-critical information, look for a trusted advisor that can help take you through the specific control or security objectives you want to address or the entire lifecycle of information security. Through thousands of customer engagements, IBM has gained deep industry and security expertise to help organizations identify and classify security risks and preemptively protect critical data. No matter where you are in the process, IBM can work with you to help ensure you have a better understanding of what type of information you have, how to control access to it, and how to report on and manage how it's being used.

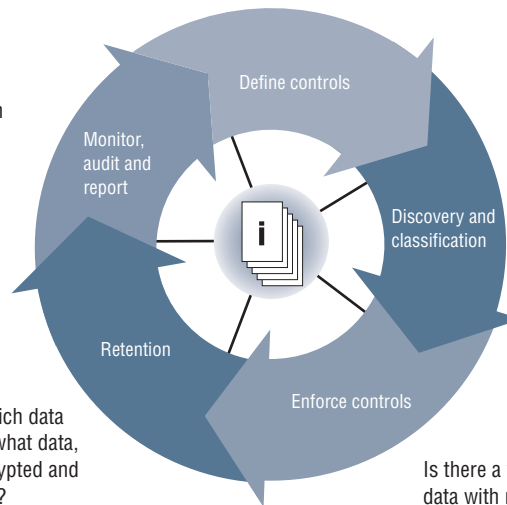
IBM can work with you to help ensure you have a better understanding of what type of information you have, how to control access to it, and how to report on and manage how it's being used

Through initial planning to ongoing monitoring and any of the steps in between, IBM solutions can help you close the gaps where you need to make modifications to reach your desired security posture, with automation capabilities to help you realize cost-efficiencies. Furthermore, the modular and integrated nature of the solutions makes it easy to focus efforts on the most urgent challenges first, as well as using technology already in place. As business needs evolve, you can extend the focus to other areas.

### Data and Information Security — a continuous process

Over 80% of enterprise information is unstructured — requiring classification, protection and monitoring

Is there a way to streamline reporting and tracking information so I can easily sift through the false positives to target the real violations?



Do I have intellectual property, confidential records or personally identifiable information that violates policy or government regulations and/or is on the verge of being compromised?

Are there sophisticated ways to categorize my data, standardize my policies and manage my data protection issues?

How can I keep track of which data retention policy applies to what data, what data needs to be encrypted and how long I need to retain it?

Is there a way to share and guard critical data with manageable policies to mitigate against increasing internal threats?

Key offerings include:

***Steps 1 and 2***

- IBM Internet Security Systems (ISS) Professional Security Services (Information Security Assessment, Application Assessment, Penetration Testing and Policy Development) deliver expert security consulting to help address compliance concerns and maintain business continuity.
- IBM ISS Managed Security Services can help you assess your current security and privacy posture, and design, implement and manage measures that address both internal and external threats.
- IBM Security Risk Management offers a series of solutions (Security Risk Assessment, Security HealthCheck, Security Workshop and Information Security Framework) delivered by IBM ISS security professionals that help you address the challenges of business requirements for information security measured against industry standards.
- IBM Security Program Design and Management includes solutions (Security Process Assessment, Security Policy Definition, Enterprise Security Architecture, Security Standards Definition and Security Process Development) delivered by security services professionals that help you examine IT strategy processes, develop policies, and deploy controls across the enterprise.
- IBM Privacy Services (Workshop, Controls Assessment and Strategy and Implementation) help you identify effective information-privacy practices, and recognize security risks associated with third-party connections and outsourcing.

***Step 3***

- IBM Tivoli® Access Manager provides users role-based access to the resources they need and SSO capabilities to help optimize productivity — and minimize the administrative burden on IT staff who can support high-value initiatives.
- IBM Tivoli Identity Manager provides a security-rich, automated and policy-based user management solution to help effectively manage user accounts — along with access permissions and passwords — from creation to termination across the IT environment.
- IBM Tivoli Federated Identity Manager helps enable customers, suppliers and business partners to conduct business across disparate environments and multiple security domains in a protected, flexible and efficient manner.
- IBM Tivoli Key Lifecycle Manager is designed to help automate the management of encryption keys throughout their lifecycle to help ensure that encrypted data on storage devices cannot be compromised if lost or stolen.
- IBM ISS Proventia® Intrusion Prevention Systems for Networks and Servers offer transparent, inline network protection that is designed to help block attacks while allowing legitimate traffic to flow unhindered. IBM Proventia Server offers multilayered protection for Microsoft® Windows® and Linux® servers, to help customers keep their data and applications reliable, available and confidential.

***Step 4***

- IBM Tivoli Storage Manager offers centralized, automated data protection to help reduce the risks of data loss while helping manage costs and address compliance with corporate and regulatory data retention and availability requirements.
- IBM FileNet® Records Manager can streamline records-based activities to help enforce compliance without user participation. Enterprises can use it to classify and apply retention policies and store electronic records.

***Step 5***

- IBM Tivoli Security Information and Event Manager provides an enterprise security compliance dashboard with in-depth privileged user monitoring capabilities, powered by comprehensive log and audit trail collection capabilities, to help organizations more efficiently monitor user behavior across their entire infrastructure.



## Summary

Business demands to make information more accessible have challenged organizations to ensure sensitive data remains secure. Security requires multiple components all functioning in concert to provide end-to-end protection. Backed by more than 40 years of leadership in the IT security field, IBM provides a breadth and depth of services, software and hardware security expertise that can help organizations effectively address information security.

Through a business-driven, holistic lifecycle approach, IBM can help organizations of all sizes safeguard information assets, while empowering dynamic collaboration and supporting compliance efforts. This approach helps assist organizations to find the balance between availability and risk, bringing the proper focus to the potential exposures and vulnerabilities most relevant to an organization's unique business and industry needs.

## For more information

To learn more about IBM information security solutions, contact your IBM representative or IBM Business Partner, or visit [ibm.com/itsolutions/servicemanagement](http://ibm.com/itsolutions/servicemanagement)

## About IBM Service Management

IBM Service Management helps organizations deliver quality service that is effectively managed, continuous and secure for users, customers and partners. Organizations of every size can leverage IBM services, software and hardware to plan, execute and manage initiatives for service and asset management, security and business resilience. Flexible, modular offerings span business management, IT development and IT operations and draw on extensive customer experience, best practices and open standards-based technology. IBM acts as a strategic partner to help customers implement the right solutions to achieve rapid business results and accelerate business growth.

© Copyright IBM Corporation 2008

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

Produced in the United States of America  
August 2008  
All Rights Reserved

IBM, the IBM logo, [ibm.com](http://ibm.com), FileNet, Proventia, Tivoli and Visibility. Control. Automation. 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](http://ibm.com/legal/copytrade.shtml)

Linux is a trademark of Linus Torvalds in the United States, other countries or both.

Microsoft and Windows are trademarks of Microsoft Corporation in the United States, other countries or both.

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

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.

IBM assumes no responsibility regarding the accuracy of the information provided herein and use of such information is at the recipient's own risk. Information herein may be changed or updated without notice. IBM may also make improvements and/or changes in the products and/or the programs described herein at any time without notice.

**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 customer 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.