



Highlights:

- Identifies risk exposure by mapping security levels against business objectives and industry best practices
 - Creates a plan and prioritized roadmap for ensuring that the enterprise's people, data, applications and infrastructure are adequately and cost effectively protected
 - Implements risk based predictive cyber threat analytics to optimize security controls and facilitate continuous improvement
-

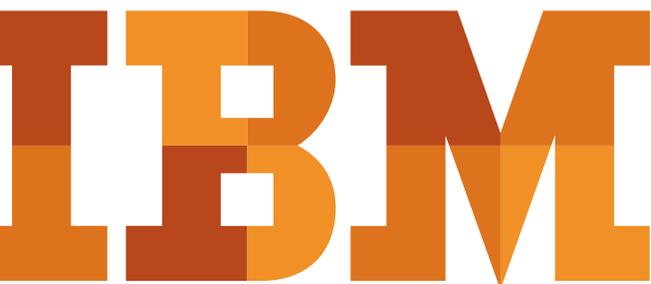
IBM Enterprise IT Security Risk Assessment

Optimizing risk management using an analytics-based approach

Managing threats in the digital age has never been more difficult. Security has moved from an IT issue to an ongoing business concern where increased threats and compliance requirements require more automated, proactive approaches to security and must take a balanced approach to managing physical, technological and human assets. The Enterprise IT Security Risk Assessment helps enterprises evaluate threats, risk and compliance in the context of an increasingly complex world driven by new levels of cyber incidents and more onerous regulatory requirements. It consists of a robust yet rapid assessment and set of actionable recommendations that can help you more effectively manage resource allocation and risk.

Begin to overcome complex and inefficient security management by examining and improving existing security policies, procedures and technology for your enterprise with the IBM Enterprise IT Security Risk Assessment. With this assessment, you can achieve the right balance of security and privacy to effectively help reduce risk while providing consistent policy enforcement. This assessment helps answer these critical questions:

- What is your plan to assess your security risks?
- How are you able to detect threats and report compliance?
- Which processes do you use to handle incident response and disaster recovery?
- To what extent have you rolled out an identity program?
- How do you know what authorized users are doing?
- How do you know if sensitive data leaves your network?
- How do you monitor access to data, including privileged access?



- How is security built into your application development process?
- What is your approach to test web and legacy applications for potential exposures?
- How do you promptly patch connected devices?
- In what ways do you monitor in- and out-bound network traffic?
- How are you building security into new initiatives (such as cloud and mobile)?

In a world where the proliferation of data continues to accelerate, the need for security, risk and compliance has increased as a key enterprise priority. And with continually changing regulations that govern data security and privacy, you can't afford to be unsure whether your existing policies, procedures and technology help support regulatory compliance for information protection.

How is the new economic environment affecting your business?

In a turbulent economic environment, many organizations may find it challenging to put the appropriate level of focus and resources on security, risk and compliance. Hence, it is critical that the right amount of investment is made to adequately address needed people, data, applications and infrastructure safeguards.

Did you know?

- The cost of a data breach continues to rise and is now over \$200 per customer record, and customer turnover, in direct response to breaches, remains the main driver of data breach costs.¹
- CEOs believe that data protection and security can enhance brand and customer loyalty.²

What should you do?

Enterprises should have a clear and comprehensive understanding of their existing organizational requirements for IT security in the context of business imperatives, and determine to what extent they are meeting those requirements and areas for improvement.

IBM is a leader in security, risk and compliance and can apply a proven approach to helping you achieve the right balance of cost effective controls to drive efficiency while providing consistent policy enforcement.

IBM Enterprise IT Security Risk Assessment

The IBM Enterprise IT Security Risk Assessment is focused on ensuring that the enterprise's people, data, applications and infrastructure are adequately and cost effectively protected and that compliance mandates are being effectively met in a timely manner.

The assessment identifies and documents the existing organizational requirements for security, privacy and compliance. With these requirements as context, the enterprise's current security, risk and compliance program are analyzed to determine the adequacy and effectiveness of the program and the program resources.

IBM performs a gap analysis of existing enterprise practices against industry standards of good practice and companies of a similar size, complexity, and industry. Based on the gap analysis, a written report is provided that summarizes the results of the analysis along with recommendations for mitigation of identified risks and the associated business benefits.

We work closely with our clients to tailor a customized report that addresses their key objectives, such as:

- Recommended improvements to security management to improve efficiency and reduce costs
- Access controls for systems and sensitive application data
- Improved visibility and monitoring of sensitive data access
- Adherence to industry and regulatory requirements

What could the Enterprise IT Security Risk Assessment be worth to you?

If you are like most enterprises, balancing the cost and effort to implement and maintain security and privacy with other priorities is a continual challenge. Knowing where your most critical gaps are helps ensure you direct the optimal amount of cost and time to security, risk and compliance to help manage your data and systems in a fast-paced business environment.

Why IBM

- We have performed thousands of successful client engagements
- Cooperating with IBM research, we have received over 1000 security patents and built unique assets in cyber security, cloud security, mobile processing and security analytics.
- Our consultants are recognized internationally as thought leaders
- IBM can provide a broad range of holistic solutions to protect against threats to IP, brand, reputation and customer trust
- IBM can enable clients to confidently pursue new business models enabled by a security-infused infrastructure

IBM brings a commitment to IT security that is second to none. For over thirty years, our extensive background and expertise in security and privacy has been used to help protect our clients' most important data and system assets.

For more information

Please contact your IBM representative or visit:
ibm.com/services/security

Source

¹ Ponemon Institute "Fifth Annual Cost of a Data Breach, January 2012"

² Ponemon Institute "The Business Case for Data Protection, July 2009".



© Copyright IBM Corporation 2012

IBM Global Services
Route 100
Somers, NY 10589
U.S.A.

Produced in the United States of America
May 2012
All Rights Reserved

IBM, the IBM logo and ibm.com 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 product, company or 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.



Please Recycle