IBM Global Services
IBM Security and Privacy Services

Guiding you toward secure e-business.
Increasing use of the Internet offers fundamental business advantages—new markets, new relationships and new ways to gain a competitive advantage. E-business technology has become vital to hundreds of thousands of businesses and millions of consumers. Realizing that information technology (IT) is enabling business, not just supporting it, organizations are changing the way they operate to capitalize on this trend. Today, IT is an investment to boost productivity, improve customer service and facilitate seamless working with suppliers, buyers and customers. Consequently, the evolution toward e-business and wireless technology is contributing to the growing complexity of IT environments.

As the number of business partnerships, alliances and mergers and acquisitions escalates, so does the need for shared applications, networks and data. Business-to-business, business-to-consumer and business-to-employee activities are introducing new user groups to business systems and shifting the focus from personal communication to virtual-fronted models. You need to protect the privacy of the people with whom you do business and safeguard your IT and other information assets.
“Organizations that want to survive in the coming years need to develop a comprehensive approach to information security, embracing both the human and technical dimensions. They also need to properly fund, train, staff and empower those tasked with enterprisewide information security.”  

Along with the possibilities brought about by networked systems, there are new dangers. If your company is doing certain types of network computing, your groundbreaking business strategy could end up in the hands of a competitor. Your server could be “attacked” by an unauthorized user. Your confidential merger information could be on its way to the media. And cyberspace is teeming with powerful viruses, as well as pranksters and professional criminals just waiting for hacking opportunities. You need to avoid the financial impacts of these risks and protect your brand image and reputation.

The convergence of IT and business, the increase in global reach with e-business and consumer interaction with corporate information systems all present burgeoning risks and a mounting need for industry-leading security, privacy and trust solutions from IBM Security and Privacy Services.

- **Security**—protecting assets through security-rich business solutions
- **Privacy**—handling and protecting personal information
- **Trust**—having confidence in your business partners

Evolving and thriving as an e-business not only entails keeping pace with the latest best practices for building, monitoring and maintaining a security-rich infrastructure, but also managing and responding to security-related vulnerabilities. You need to determine the best way to protect critical assets and manage risk.

**Establishing your line of defense**

New threats and risks driven by technology and open networks have pushed security to the top of many companies’ priority lists. A constantly changing environment and evolving business requirements present a number of challenges for companies:

- How do you know if your existing security controls are appropriate to mitigate risk?
- How can you justify the cost of security?
- What security controls do you need to implement to achieve a security-enhanced network infrastructure?
- How can you increase awareness and make security a priority within your business?
- How can you implement comprehensive solutions that cover business and IT?
- How can you securely leverage new technologies?
- How can you be confident that over time your security will remain at the appropriate level?
- Where do you find the skills to manage your business?
- How can you best prepare for business continuity?

Understanding and balancing security risks with business needs and implementing solutions that reduce the impact of security exposures can enable companies to conduct business with confidence. IBM Security and Privacy Services is designed to deliver the solutions and services necessary to help build trusted
electronic relationships among customers, employees, business and trading partners and shareholders. We can work with you to address the challenges of security, privacy and trust with a simple, structured approach that includes three phases.

**Enterprise Risk Assessment—identify your security strengths and weaknesses**

Enterprise risk assessment focuses on assessing the current state of information security within your organization. Using a combination of interviews, document reviews (strategies, policies and guidelines), physical security reviews and technical reviews (host and application reviews and ethical hacking), certain threats, vulnerabilities and risks to which your organization is exposed are identified. Based on these analyses, short-term “quick wins” as well as longer-term strategic recommendations and plans for improvement are proposed. Issues are discussed in detail at a concluding workshop, and an action plan is created for effective implementation of the recommendations.

By providing direct links between IT and the effects on your business process, an enterprise risk assessment can help strengthen the alignment between business and IT within your organization. It can also help you establish business justification for addressing security issues and create information security awareness. Designed to help you understand the business risks that are introduced by information security weaknesses in processes, organization and IT, our enterprise risk assessment can also help you define security and privacy requirements in the context of your future business plans.

An enterprise risk assessment can be composed of any of the following IBM Security and Privacy Services components:

- **Security health check**—determines the effectiveness of your current security plan through a broad assessment that includes the review and identification of strengths and weaknesses in your security controls.
- **Site security assessment**—provides an in-depth review of your enterprisewide physical site security controls relating to processes and compliance with your policies.
- **Security process assessment**—examines how people in your organization interface with business-critical information; recommends new processes to reduce risk; and prioritizes areas on which your organization should focus for optimum security improvements.
- **System security assessment**—provides a review of your current operating system security controls to identify vulnerabilities associated with your business-critical internal operating systems.
- **Network security assessment**—involves a review of the design, configuration and deployment of your network to assess how well information assets are protected from outside and inside unauthorized access.
- **Internet security assessment**—examines the configuration and management of your overall topology and design to determine how effectively your internal networks are protected from external intrusion.
- **Application security assessment**—provides an independent review of the architecture, design and function of your critical networked business applications to identify vulnerable stress points.
- **Wireless risk assessment**—identifies threats and vulnerabilities introduced by the implementation of new wireless e-business solutions or by the extension of current IT infrastructure into the wireless space.

IBM Security and Privacy Services can help you determine the best way to protect critical assets and manage risk.
**Ethical hacking**—provides a stress test of your network by simulating a real break-in in which our ethical hackers try to gain unauthorized access to your internal network.

**Enterprise Security Solutions—build up your defenses**
Enterprise security solutions involve the development and implementation of the strategic solutions recommended in the enterprise risk assessment phase. A structured approach is developed for achieving secure solutions by addressing areas including security strategy, policies and guidelines, organization, processes, architecture, risk management, logging, implementation and management.

To guide your security decisions, enterprise security solutions address security requirements by providing policies, standards and management architecture principles, and help implement your policies and standards by defining formal security processes and designing specific security-rich solutions. Our professionals assist you in selecting security products and services that best fit your unique requirements. We also offer services to help implement your chosen technology solutions with security management processes that help ensure an appropriate fit with your current and strategic business needs.

An enterprise security solution can be composed of any of the following IBM Security and Privacy Services components:

**Security workshop**—helps you understand the ramifications of new e-business activities and how to protect vital information assets.

**Privacy workshop**—educates you on current privacy issues that impact your industry, as well as multinational companies, and identifies the business activities and systems that collect, store, access and use personal information.

**Public key infrastructure business workshop**—helps you understand the benefits of a public key infrastructure (PKI) and formulate a preliminary plan for incorporating PKI into your business and IT strategies.

**Wireless workshop**—describes new security challenges created by wireless technology and helps enable a fast start of new, secure wireless e-business initiatives.

**Information asset profile**—identifies security gaps and helps you understand which information assets are most critical and how they are protected.

**Privacy strategy and implementation**—examines your policies and processes to help determine the most effective way to implement sound privacy practices that are consistent with customer requirements.

**Public key infrastructure planning and design**—assists in the design of a secure PKI solution for your e-business environment through comprehensive consulting and integration activities.

**Security policy definition**—delivers a customized security policy document that defines and explains your organization’s security policies and helps ensure they meet your business objectives.

**Security standards definition**—investigates the requirements for information security and associated priorities, creates custom security standards that are consistent with organizational business goals and helps you implement enterprise security policies.

**Security process development**—analyzes your organization’s security objectives to help ensure consistent, effective security processes and defines processes and procedures to meet those goals.
Enterprise security architecture—analyzes your enterprisewide business and IT strategies and provides security architecture principles to enable management and technology decisions that are consistent with your organization’s security objectives.

Internet security architecture—analyzes your Internet connections, Internet business strategy and the Web services you provide that link to internal systems. Technology and business aspects are reviewed to determine if your security measures can meet the increased demands of establishing Internet or extranet connections.

Secure solution design—helps design a secure e-business solution and provides a roadmap to your solution objectives that addresses simple access, external publishing, private publishing, production access, e-commerce, collaboration and hosting.

Secure wireless solution design—assists you in planning, architecting, designing and building wireless e-business solutions that satisfy your unique business and security requirements.

Security product selection—identifies your short- and long-term needs, matches those requirements to available products, provides a detailed analysis of each product’s strengths and weaknesses and assists you with implementation.

Implementation services—assists you in implementing the products (IBM and non-IBM) you have selected to build the operational environment defined by the preceding phases.

Managed security services—maintain continuous, adequate security levels

Designed for enterprises that want to outsource security elements of their IT operations, our managed security services help ensure the provision of a state-of-the-art security environment. Industry-leading tools and people help provide security protection for your critical assets. In addition to securing resources for outsourcing, we provide services for business continuity.

Managed security services can be composed of any of the following components:

Intrusion detection—monitors your networks around the clock using industry-leading detection tools. Trained professionals at our network operations centers monitor, investigate and alert security professionals of suspicious activity, as well as work with you to define and coordinate appropriate responses.

Vulnerability scanning—uses a variety of tool-based scanning techniques to enhance your existing security posture and help prevent unwanted intrusions on your network perimeter.

Firewall management—helps ensure your firewall is correctly configured and maintained to help preserve a secure environment.

Incident management—provides around-the-clock response to certain incidents including virus attacks, external and internal hacker attacks, denial-of-service and Web site vandalism via the IBM Computer Emergency Response Team. Assistance includes technical phone consultation and/or onsite coverage at your location, as well as working with your technical staff to resolve the incident.

Our unique methodologies help you integrate security into your enterprise, from start to finish. Assess, plan, design, implement and run phases—part of the IBM security architecture—provide consistency, interoperability and integration across multivendor platforms and environments.
IBM—your security and privacy watchtower

Whether you are interested in a simple security engagement or need to implement comprehensive security, privacy or trust measures, time-tested IBM security methods available throughout IBM Global Services can help ensure smooth integration. We know that security is a cross-industry concern. IBM has the skills, specialists and solutions to address specific security requirements unique to your industry, and the system integration skills to design and implement security solutions that are designed to protect your IT infrastructure. We have a proven track record of implementing successful security projects worldwide in the public, health, travel, distribution and finance industries.

With IBM, you gain timely access to knowledgeable security, privacy and trust consultants, allowing you to concentrate on your core business. For decades, our professionals have helped safeguard IBM and other businesses’ assets and data centers from intrusion. We have real-world experience in integrating information security solutions into current infrastructures and processes, and our global, consistent delivery is based on proven methodologies and best practices. Through systematic development and the use and reuse of intellectual capital worldwide, the people of IBM Global Services can deliver effective security, privacy and trust solutions. We embrace innovative technologies such as PKI, wireless and biometrics, and our IBM Security Research Centers—including the Global Security Analysis Laboratories—and competency centers provide state-of-the-art security tools, techniques and applications.

Our comprehensive offerings—which can be selected individually or in combination—enable secure e-business and help you effectively manage risk. Capitalize on the extensive portfolio of IBM Security and Privacy Services to conduct business more securely.

Get started
To learn more about IBM Global Services, please contact your IBM sales representative, or visit:

ibm.com/services

To learn more about IBM Security and Privacy Services, please visit:

ibm.com/services/security