Information Security Services

Risk Advisory Services

ADVISORY

The complexity of modern businesses, their reliance on technology, and the heightened interconnectivity among organizations that is both a result and a driver of e-business — these are rapidly evolving developments that create widespread opportunities for theft, fraud, and other forms of exploitation by offenders both outside and inside an organization. With the growth of e-business, perpetrators can exploit traditional vulnerabilities in seconds. They can also take advantage of new weaknesses — in the software and hardware architectures that now form the backbone of most organizations. In a networked environment, such crimes can be committed on a global basis from almost any location in the world, and they can significantly affect an organization's overall well-being.

- 25% of the organizations questioned have been confronted with hacking, viruses and/or worms more than 10 times during the past 12 months
- 25% of the organizations questioned are confronted daily with more than 100 spam incidents
- 72% of the organizations questioned do not use performance indicators for information security.

KPMG Information Security Survey 2006

KPMG Services

KPMG assists organizations to develop an enterprise wide approach to managing security. Our security professionals have an in-depth and up to date understanding of security issues facing companies. Our suite of security products is grouped under three headings:

- Security Design and Integration
- Security Testing
- Security Management

Security Design and Integration

KPMG's Security team can provide advice on the design of security controls, enterprise security architecture, and also advise on the selection and implementation of security software or hardware.

Security Testing

Over the years, the demand for security testing has increased substantially as businesses have recognized the need to provide assurance that they are protected from internal or external threats. Our security testing services include:

- Penetration Testing Services
- System and Infrastructure Configuration Testing
- Wireless Security Testing

Security Management

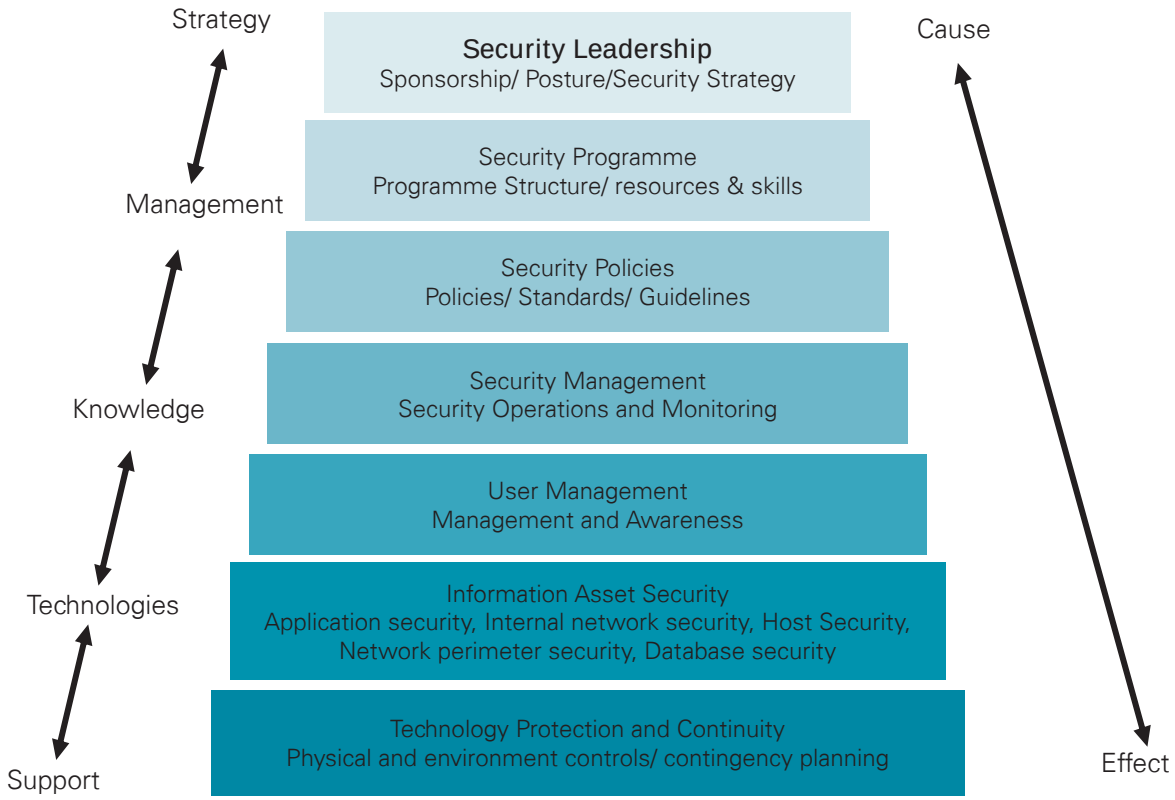
KPMG's Security Management Services provide support across all aspects of security management from review and appraisal to security management co-sourcing. Services include:

- Security Strategy and Policy
- Total Managed Security
- Security Reviews

Enterprise Security Architecture (ESA)	KPMG's proprietary ESA methodology is based on traditional architectural services such as enterprise technology strategy development, information security engineering and design, and business process reengineering. We follow the ACE principle: automate low-value procedures, consolidate redundant technologies, and eliminate ineffective and inefficient security management processes. Through a collaborative design process, we facilitate the design of a client-specific enterprise architecture to meet enterprise objectives.
Security Training	Ongoing security testing is paramount within today's corporate IT infrastructure. It is therefore imperative that security skills are held within the organization to maintain a regular security assessment regime. The 'Security Training' provides an informative and entertaining three day training course covering the subject of IT security by giving an insight into current security threats and countermeasures. In essence the aim of the boot camp is twofold: • Raising awareness to delegates of the types of security threats which exist to a corporate network • Demonstrating techniques for detection and prevention of security intrusion.
Penetration Testing Services	We base our approach on the proposition that an information asset's value, threats, and vulnerabilities represent the level of risk associated with that asset. As the significance of any of these factors increases, the relevant risk also increases. Conversely, reducing any of these factors reduces the risk. All three factors must be understood before it is possible to assess risk in a reliable manner. Our penetration studies assess and quantify threats and vulnerabilities associated with specific target environments.
System and Infrastructure Configuration Testing	Even with a fully tested network infrastructure in place, significant security vulnerabilities are likely to still exist at the application level. Web applications tend to be very bespoke, and thus require equally bespoke testing in order to identify risks. Developers often overlook important security controls to meet imposing release deadlines. This means that weaknesses may exist in areas such as user authentication and transaction processing. KPMG has developed a unified methodology that seeks to address the significant application security risks that typically result in system intrusion. Testing includes: • detailed review of the design and implementation of the application • simulated external attack based upon scenarios of unauthorised and permitted users • reviews of critical and sensitive code
Wireless Security Testing	Organizations are increasingly implementing wireless technology to reduce network infrastructure costs. Unfortunately, this is often done without a full understanding of the security implications. Wireless networks can extend your corporate network outside your physical perimeter, thereby giving hackers the same access as if they were located directly on your network. Our wireless security testing identifies, assesses and addresses wireless network risks through three distinct steps: • Identification of wireless network leakage • Review of wireless security controls • Testing of network clients and infrastructure
Security Strategy and Policy	As with any business function, the development and implementation of a sound strategy is key to achieving clear direction and consistency in approach. Within a security department, development of a successful strategy facilitates buy-in from the executives and assists in increasing security awareness amongst senior management. KPMG can provide assistance in developing your security strategy and policies at any stage in their lifecycle and also assist in their maintenance in an ever changing environment. Our primary focus for strategy and policy development includes: • Information Security Policy • Data classification and data protection registration • Technical security standards (e.g. network, encryption, authentication)

Total Managed Security	Many clients wish to minimize the overhead of managing security infrastructure. KPMG can help reduce this resource cost by providing a range of services designed to help clients experience a minimum overhead in terms of time and resources needed. Our service management covers: • Planning and prioritization • Resource Management • Monitoring and Escalation • Quality and service levels
Security Reviews: Information Security Assessment	KPMG's Information Security Assessment (ISA) Services can help clients make informed choices about their information security needs. Possessing information assets within an information technology environment poses risks, and we assist our clients in recognizing and mitigating these risks. We provide detailed technical assessments of their information systems infrastructure, enterprise applications, and security management policies and procedures. We help clients identify security vulnerabilities, evaluate security controls, and understand business impacts. And we deliver practical improvement recommendations.
Security Reviews: Internet Security Assessment	Internet Security Assessment is designed to: • assist you in identifying and assessing the IT risks introduced by connecting your business to the Internet; • evaluating the effectiveness of your existing controls; and • identifying where key security controls need to be strengthened. We test the security measures your business has in place to manage Internet connections and evaluate whether these security mechanisms are working at an acceptable level. Our tests are intended to mimic the actions of a hacker on the Internet who is attempting to gain unauthorized access.

Information Security Capabilities Model



KPMG takes a complete view of your information security arrangements using our Security Capability Model.

KPMG's security advisors come from a wide range of technical backgrounds. This gives them the insight and experience to identify security weaknesses which otherwise go unnoticed. Their experience also enables them to provide highly relevant recommendations to help you to improve security.

Organizations commonly perform a degree of testing internally, but this is usually automated and only skims the surface. Also, internal testing is usually conducted by teams who actually manage the systems.

KPMG Security Testing and Assessment is independent, delves deeper and address the factors that cannot be addressed using automated tools.

Clients benefit from an increased awareness of the technical and business risks facing the organization, as well identifying and prioritizing the technical security related issues. The detailed recommendations form the basis of an action plan that can be implemented by developers. In addition, KPMG provides security recommendations that are appropriate to manage the risks to an acceptable level in your industry.

Security testing is focused on providing a point in time assessment of the security controls applied to an organization's infrastructure or application. By performing this testing on a periodic basis, security can be reaffirmed not only with senior management and the Board but more importantly, with clients and regulators.

KPMG's modular approach to security allows you to request the type of security assessment or advice that you require without implementing a full-scale strategy. Where necessary, our security offerings can be combined with components of standard software testing, for example unit or system acceptance. This provides a detailed featured testing service to support project management and system development teams.

Our client can gain improved confidence that comes from knowing the best use is being made of the control and security features of your systems and IT environment.

KPMG Risk Advisory Services
Risk Advisory Services assists clients to focus on fundamental business issues that help increase revenues, control costs, and identify and manage risks, including the risks inherent in the technology systems used to support business objectives. Risk Advisory Services also provides information to clients to help them meet their strategic and financial goals.

Other related KPMG IT Advisory Services:

- Business Continuity Services
- IT Project Advisory
- IT Attestation Services
- IS Governance
- Business System Controls

Contact us

Paul Bahnisch
Executive Director
pbahnisch@kpmg.com.my

Mohd Arif Ibrahim
Executive Director
arifibrahim@kpmg.com.my

Mohd Muazzam Mohamed
Executive Director
mmohamed@kpmg.com.my

KPMG Business Advisory Sdn Bhd
Level 10, KPMG Tower
8, First Avenue
Bandar Utama
47800 Petaling Jaya
Selangor, Malaysia.
Phone: +60 (3) 7721 3388
Fax: +60 (3) 7721 3399