

# IT risk advisory services

## Information security advisory

### Identity and access management

KPMG's identity and access management (IAM) services help you collect all in-use user accounts of your in-scope systems; we assist you with developing the strategy and the business processes that ensure efficient consolidation and management of these user accounts and the efficient management of access to information. Furthermore, our services include the design and implementation of IAM-supporting IT systems.

### Information security policy development and assessment

With our methodology founded on international standards and recommendations (ISO 27000 series of standards, COBIT), we help your company to develop and implement information security policies and processes which create a modern regulatory and documentation framework for information security purposes.

### Business continuity management

KPMG's business continuity management solution is a proactive, risk-based approach that reduces the risks of unavailability of services and information and helps quick recovery or replacement of resources after incidents and disasters. Our methodology is based on international standards and the experience of our professionals, who support our clients with developing, implementing and maintaining a framework, policies and plans for business continuity.

### Log management

With the help of our log management services the time and money your company invests in log management, even at the lowest possible level, can constantly create real value for the enterprise. Furthermore, we assist you to make your log management solution compliant with legal regulations, which are getting stricter and we give you support so that you can uncover all atypical activities in your business.

### Data loss prevention (DLP)

KPMG's data loss prevention services give you assistance with identifying and fulfilling your data protection related needs. By assembling the data inventory of your company we identify the scope of the data to be protected. We assess the channels that may pose a risk of data leakage and we determine the current data loss protection level of the firm. Based on the results of our review we highlight the development points. We can also assist you with choosing and implementing a DLP solution which best fits your company's needs.

### Data privacy advisory

KPMG's data management and data protection services help you to manage and protect sensitive employee and client data effectively and in compliance with legal regulations. Our professionals support you with the enhancement of your data classification system, review your data management solution from legal compliance and information security perspectives and they help you with implementing an efficient solution for data leakage management and with the cost-effective management of incidents that have already occurred.

### Software asset management and license metering

Software asset management is a crucial point in the implementation of a modern IT environment. An appropriate strategy can contribute to the reduction of IT costs and to the reduction of risks related to software ownership and usage; furthermore it can increase the efficiency of the IT department and of end users. KPMG helps to determine the maturity level of your company's software asset management and to optimise the involved processes, policies and assets.

### **Implementation and support of ITIL-compliant operation**

KPMG's services related to ITIL-compliant operation create the foundation for the transparent and measurable operation of IT services. With our contribution your organisation can operate more efficiently, the co-operation between different departments can be increased and contractors' performance can be supervised and brought to account. With an effective asset and configuration management we reconcile internal and external services. With the developed system financial resources spent on IT operation and IT development can be optimised.

### **Information security risk assessment**

Our comprehensive information security risk assessment helps to understand, treat and enhance protection against security risks. After we have taken an assessment of the company's asset and information inventory, we determine the characteristic threats and prepare a business impact analysis to forecast damages which occur in case the threats become reality. On the basis of historical events, our prior experience and employee interviews at your enterprise we also estimate the likelihood of a threat becoming reality. Finally, we rank all information security risks relevant to your firm and prepare an action plan.

## **IT audit related services**

### **Data migration validation and support**

KPMG's migration quality assurance and migration validation services support clients with planning and carrying out data migrations, as well as with their retrospective testing. The validation – the comparison of data gathered from the source and from the target systems – is carried out with analysis software, so that we can process large amount of data without hindrance. If required, we issue a certificate of positive assurance.

### **General IT audit**

General and focused IT audits are examinations based on standard processes, guidelines and methodologies (COBIT, ISO27001). They include review of the IT security management and regulation, and of the general controls of the IT environment. We help our clients to identify and assess IT security risks and to develop a control environment which complies with Hungarian legislation and with international standards as well.

### **IT due diligence**

IT due diligence is an IT audit that covers an organisation's entire IT infrastructure, but focuses only on the main risk areas. This audit is typically requested by investors to gain information on the information technology infrastructure of a company to be acquired. It includes the audit of the designated company's IT organisation, processes, and business-critical IT infrastructure and control environment.

### **IT internal audit support**

Via supporting the operation and development of IT internal audit systems, as well as through auditing them, KPMG helps clients to secure their corporate values. Our services, among others, include optimising IT internal audit processes, developing IT internal audit supporting tool sets, professional support with specific tasks such as mass data analysis or uncovering fraudulent activities. Furthermore, we provide a training programme tailored to our client's needs to prepare the company's employees for the use of IT internal audit systems.

### **Compliance review of assurance over outsourced controls (ISAE 3402, SSAE)**

ISAE 3402 and SSAE 16 are audit standards which evaluate in a formal report the design, implementation and operating effectiveness of IT controls at service organisations. The SAS 70 standard has been replaced by SSAE 16 in the United States and by ISAE 3402 in other countries.

### **Security audit and functional audit of business systems**

Within the framework of a security audit we review the security settings of business systems, reveal data security threats, control weaknesses and, if necessary, we propose implementation of appropriate security measures. During a functional audit we examine, whether the company's IT systems operate according to predefined business logic and identify areas which do not comply with either efficiency or business requirements.

### **Segregation of duties (SoD) support and audit**

We identify issues arising from complex access right structures and settings in business systems, particularly the inappropriate segregation of duties, conflicting roles which enable fraudulent activities that may cause serious financial losses. Modern ERP systems cannot be analysed via simple methods, due to their complex nature. Therefore, we utilise various analysis tools in our audit. We possess outstanding expertise and tools for auditing SAP access rights and SoD.

### **System interface audit**

Interfaces between systems have serious inherent risk. The data can be lost, altered or even duplicated; such incidents can significantly affect the operation of systems or even the general ledger data of the company. With the help of our audit techniques we can reveal functional errors, interface security issues and make suggestions for improvements.

### **Pre- and post-implementation reviews**

For pre-implementation system audits we use a comprehensive approach to ensure that the company performs all necessary preparatory activities. Our aim is to ensure that the new system meets the stakeholders' expectations, and that necessary controls are developed. During a post-implementation review, besides examining whether the data has been migrated appropriately, we also verify that the developed system's functionality meets specification and business requirements.

### **IT related legal compliance review**

Design and operation of the IT control environment are subject to increasingly strict regulation with respect to the telecommunication, financial (bank, insurance, management companies) and public sectors. Furthermore, for some industries the legislator also discusses the criteria of functional compliance of the in-scope systems. Within the framework of our IT related legal compliance services we identify, which laws affect your company and audit whether your firm complies with the legal regulations. Finally, we make suggestions for the actions to be taken in order to remedy deficiencies and ensure compliance.

### **Social engineering audit and security awareness programme**

Employees who can be misled are one of the most serious non-technical information security threats to an organisation. Using agreed rules and methodologies, we execute social engineering attacks and prepare action plans for the company based on our results, in order to avoid similar incidents. Our audit can be paired with a security awareness training, so that employees become more aware of attackers' techniques and of the importance of safety measures to be complied with.

### **Compliance audit**

During a compliance review we examine, whether the requirements of a given international standard (e.g. ISO 27001, ISO 20000, ISO 22301, ISAE 3402, PCI DSS) are met. Based on our findings we can prepare your company for the certification or renewal audit. Such certifications can strengthen trust in your company and provide business advantages over your competitors.

## **Technical security reviews**

### **Penetration testing**

KPMG penetration tests simulate real attacks and threats that could emanate from dissatisfied employees, outside attackers or industrial spies. We identify vulnerabilities and share the details of the attack scenarios with our clients, proposing mitigation measures. We prepare our recommendations in a way that enables them to be interpreted and utilised by both management and technical professionals.

### **System vulnerability assessment**

Vulnerability tests identify technical system weaknesses in a systematic audit of available services, searching for known deficiencies in the network, operating system, database, transport and application layers. We identify the vulnerabilities and share the details of attack scenarios with our clients and suggest corrective procedures. We prepare our recommendations in a way that enables them to be interpreted and utilised by both management and technical professionals.

### Configuration review

A configuration review performed by KPMG professionals helps to effectively enhance your company's IT infrastructure via identification of critical servers and through independent and objective evaluation of server settings. In co-operation with your co-workers we detect, which servers are crucial for business processes. Then, based on KPMG methodologies and industry standards, we assess the servers' settings on operation system level (e.g. access management, system updates) and beyond that (e.g. virus protection).

### Cybersecurity

With the help of KPMG's cybersecurity services you can make well-grounded decisions regarding what you should spend money on – besides IT security solutions suggested by the compliance based approach – in order to make your company's crucial data secure against well-prepared attackers. Our professionals assist you with implementing a solution, which is based on the complex evaluation of results of penetration tests, vulnerability scans and on a review of the risk environment.

### Mobile application assessment

Besides general application security reviews, KPMG provides specific help with the security testing of smart phone applications. We pay special attention to client side security of the mobile platform in question and of crucial smart phone applications. We evaluate, whether the authenticity and integrity of data provided by individual hardware components (e.g. GPS co-ordinates) are ensured in the application. We also examine, whether it is ensured that cryptographic keys used by the application are stored and distributed securely.

### ISO 27002 health check

Based on the requirements set out in the ISO 27002 standard, we assess the condition of your company from the aspect of information security, in order to identify deficiencies in your control environment and to help you create or enhance your information security strategy. In co-operation with your company's co-workers we determine, which processes are relevant from information security point of view and we evaluate the design and operating effectiveness of the controls related to them. We support you with the implementation of a solution which ensures compliance with the ISO 27002 standard.

### Privacy policy framework review

KPMG performs a comprehensive review of all privacy-related internal rules and regulations that are applied in different departments of your company in order to help you ensure legal compliance. We inspect your privacy policy, related declarations, manuals, the IT security policy, the incident management procedures and the data classification process. Our professionals assist you with remediating the deficiencies that may be uncovered.

### Privacy governance structure design

KPMG's comprehensive IT supporting solutions help you to integrate privacy requirements into your company's governance structure. Besides elaborating the legally compliant criteria of access to personal information, we also contribute to the design of IT-tool-supported processes which enable real-time monitoring of the fulfilment of privacy requirements.

---

## Contact:

**György Sallai**

**Director**

**T.:** +(36) 1 887 6620

**E.:** gyorgy.sallai@kpmg.hu

**KPMG.hu**



The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavour to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

The KPMG name and logo are registered trademarks or trademarks of KPMG International.

© 2016 KPMG Tanácsadó Kft., a Hungarian limited liability company and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved.