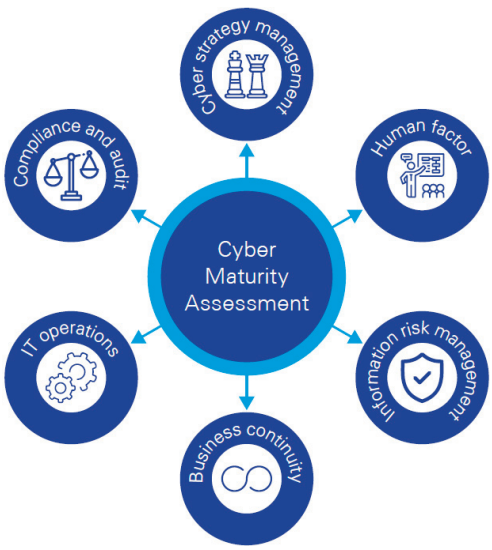
Cyber Maturity Assessment

IT Risk Advisory Services

It could cost you up to EUR 1 million. That's the price of systems recovery and data restoration following a cyber attack. What's more, due to a recently introduced EU data protection regulation, organizations may face more severe fines for security breaches to data privacy. Is your enterprise prepared for managing such cyber security risks?

Cyber security risks are not new but they continue to evolve at an ever-quicker pace. Companies and public sector organizations now need to comply with an increasing number of requirements set out in legal regulations, with internal policies and with those set by authorities in the fields of data protection and privacy. According to the general data protection regulation introduced by the EU, from 2018 regulatory fines of 2-4% of an organization's yearly revenue may be meted out to those found to be not in compliance. Meanwhile, threats from cyber criminals and hacktivists are growing in scale and in sophistication every year. Thus, on a continuous basis, organizations need to develop their cyber defence competencies, and adapt them to the changing digital environment. These days, it is not enough to respond to individual cyber security incidents; a proactive and comprehensive approach is needed that covers each dimension of security across the entire organization.



Do the following issues sound familiar to you?

- You would like to enhance the efficiency of your organization's information risk management system. While you receive numerous tips and recommendations for development, you have no clear picture on the maturity of your enterprise's current cyber security system. Without knowing where you start from, it is difficult to set development goals and determine the desired level of protection.
- You lack a quick and effective diagnostic tool for measuring the pace of your cyber development program's progress. Consequently, you have to rely on feedback that is only available once or twice a year.
- Your co-workers are often careless and do not adhere to information security rules. Up to now, security awareness trainings and campaigns have not shown satisfying results.
- Your organization needs to comply with numerous information security rules, but it is difficult and time consuming to produce high level assessments on how effectively your processes ensure compliance with those rules. As a result, specifying development points to avoid eventual fines from authorities is only possible via increased expenses.

– You wish to compare your organization's level of cyber maturity to requirements of international information security standards (e.g. ISO 27001, NIST) or with that of your competitors, but you lack the benchmark data to rely on.

How can we help?

With KPMG's Cyber Maturity Assessment methodology, we can quickly and effectively evaluate commercial, state-owned and non-profit enterprises' ability to protect their sensitive data and manage cyber attacks. We look beyond pure technical preparedness for cyber threats and consider further dimensions of security: the people fulfilling securityrelated tasks and the processes supporting cyber defence. We present vulnerabilities—as well as remedial IT and organizational developments—in a new context. We also help you to achieve a clear view of data protection-related legal and corporate requirements and compliance.

In developing our Cyber Maturity Assessment methodology, KPMG combines international information security standards with experience gained in global cyber security, risk management, governance and organizational development engagements. Our approach addresses the following six key dimensions:

– Information security governance We examine processes which support management in fulfilling its role as a responsible and proactive actor in strengthening the organization's cyber security.

– Human factors We evaluate how effectively your corporate culture combines up-to-date cyber security knowledge with appropriate practical skills and with security awareness.

– Information risk management We evaluate whether the applied risk management system provides effective protection for sensitive business information throughout the organization and at supply partners.

– Business continuity We assess whether processes implemented for handling cyber security incidents support effective crisis management and damage mitigation.

– Technology and operations We review whether the level of controls integrated into the design and operation of the IT system is in line with the security requirements mandated by the identified risks.

– Compliance and audit We show you whether your organization's cyber security framework ensures compliance with legal requirements and standards.

Advantages for your organization

Cyber Maturity Assessment is a unique diagnostic tool, which enables quick, effective and comprehensive measurement of an organization's preparedness for cyber security threats and helps identify associated areas in need of development. KPMG's IT Risk Advisory Services practice is ready to help you manage deficiencies uncovered during such an assessment in each area of cyber security. Our professionals support you with the design and implementation of your enterprise's cyber protection system at strategic, process and technology levels, with internal and external vulnerability assessments and penetration tests, as well as through improvement of incident response skills and the foundation of proactive and risk-based security management.

If our service offering has aroused your interest, you can contact us for further details via the following contact information.

Contact:

Tamás Kórász
Partner
T.: +(36) 70 333 1507
E.: Tamas.Korasz@kpmg.hu

KPMG.hu

Péter Konrád
Manager
T.: +(36) 1 887 7343
E.: peter.konrad@kpmg.hu

KPMG.hu