KPMG

CyberSAFE

Cyber Security & Forensic

Determination of maturity level and advice on optimisation of cyber security plus incident response for insurance policyholders and potential customers

The challenge

Cyber security doesn't just mean protection against hackers – it requires a comprehensive overview including the structure of cyber security management and organisational controls. As well as it being in companies' own interests to protect themselves as extensively and efficiently as possible from potential threats, there are also increasing regulatory requirements relating to information security.

At the same time, it is also an immense challenge to keep abreast of the state of the art, the threat level and your company's own capabilities. An information security management system – with or without a formalised framework like ISO/IEC 27001 – is intended to be continually enhanced and adapted to changes in the organisation.

Our Cyber Maturity Assessment (CMA), "KPMG CyberSAFE", allows you – in collaboration with our experienced team – to find a structured and targeted approach to the issue of cyber security. This gives you the opportunity to take control of any uncertainties and develop your digital landscape into a strategic advantage.

You benefit from our experience:

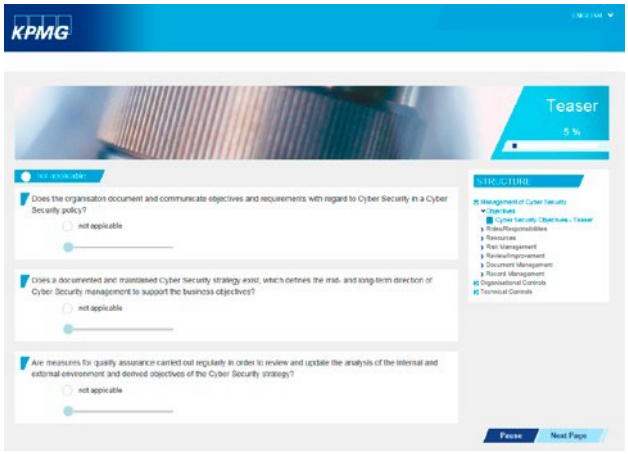
- KPMG knows and audits the processes, structures and systems of a wide range of companies of all sizes and industries – not least in terms of IT and cyber security.
- Our forensic experts investigate all kinds of IT incidents, provide on-site support where necessary (incident response) and assist in crisis management.
- KPMG supports organisations in the determination of their maturity level and advises on the optimisation of processes and structures.

KPMG CyberSAFE

We developed CyberSAFE specifically for two reasons: to gain a comparable overview in an effective and time-efficient manner, and to identify the areas which require deeper examination. CyberSAFE covers the areas relevant for cyber security:

Management	Organisational measures	Technical measures
Objectives	HR	Physical security IT
Roles and responsibilities	Service providers	systems Network
Resources Risk	Classification and handling	security
management	Incident response	Monitoring and logging
Review and optimisation	Crisis management	Vulnerability management
Document management	Compliance	Cryptography
Records management		Mobile systems
		Change management
		Identity and access management
		System life cycle IT
		forensics

Determining maturity level with CyberSAFE



The requirements of recognised standards such as ISO/IEC 27001, the NIST Framework and SANS Critical Controls are incorporated in the assessment. Through benchmarking, CyberSAFE also makes it possible to draw a comparison over time and with other organisations.

CyberSAFE package solutions

In two different packages, we offer you a status summary and specially tailored optimisation recommendations for your cyber security and your incident response capabilities. You should decide which of these options is most suitable for your company based on your size, dependency on IT and general and specific threat level. We are happy to assist you in making this decision.

CyberSAFE Standard

With a standard assessment, we request relevant information from you and process this information. We then conduct a two-day workshop with you as a joint assessment of the current status quo at your organisation. This allows us to conduct a risk dialogue, address any questions and enrich the assessment with our practical experience. In addition, you and your colleagues have the opportunity to tackle the issue in a constructive atmosphere with external experts – in many cases, the workshop already produces ideas for optimisation.

Once we have addressed any follow-up questions to the workshop, you will receive a detailed report from us on the current situation at your organisation and potential optimisation measures. On request, we can also prepare an overview of the relevant infrastructure, the most important data and interfaces with external parties.

CyberSAFE Enhanced

The enhanced assessment is particularly recommended for organisations with a greater reliance on IT and larger IT structures and/or at higher risk. In addition to the contents of the standard assessment, in the enhanced option there is the possibility of a more detailed inspection of relevant documents. Moreover, the workshop is planned over a minimum of four days to match the greater complexity and necessary level of detail.

As and when required, CyberSAFE can be supplemented with further services such as penetration tests, incident readiness assessments, awareness tests and system audits.

Well equipped to meet your needs

KPMG is one of the leading providers of cyber security and forensics. In Germany alone, there are over 150 specialists at your disposal – that's not including our international network.

Contact

KPMG Germany
Michael Sauermann
Partner
+49 30 2068-4624
msauermann@kpmg.com
www.kpmg.de/cyber