ISO/IEC 27001

KPMG Cybersecurity

KPMG China

kpmg.com/cn

Gartner 2018-2019 Top security trends conference

More and more enterprise managers have realized that information security is an important factor, affecting the company's business development, brand image and reputation.

Cyber security challenges faced by enterprises:

- Security work is unbale to handle?
- Security compliance requirements emerge in endlessly?
- Various security audits, tired of dealing with ?
- Security violation is difficult to prohibit ?
- Does IT department become the "back pot man" of security incidents?
- Business department: security? Looking for IT?
- How is security exactly doing? How to evaluate it?
- We deployed so many security products, and why still the security incidents keep happening ?

Through the implementation of ISO27001 information security management system standard, On the basis of fully identifying the security risks, by deployment of relevant security control measures and achieved continuous improvement on the security management.

KPMG ISO27001 Implementation procedure

	Gap analysis and maturity assessment	Information security risk assessment and response	Establishment of ISMS	ISMS operation and internal inspection	Assist with certification preparation
	Project management and quality assurance				
	Project plan				
	Information and communication				
Project management	As-Is understanding and diagnosis	Consolidation information assets	Security policy define	ISMS operation	System fine tuning / corrective prevention
Organization and Personnel	Gap analysis and Assessment	Risk assessment	Security management and control define	Establishment of review system	Communication with certification authority
Project implementation	Improvement of security organization structure	Acceptable risk level confirmation	Establishment of ISMS	Trial review conducted	Be certified
Technical support	KPMG's ISMS reference model	KPMG's information security risk assessment model	KPMG's information security control system and	KPMG's information audit methodology change model	
	ISO27001 IT risk management gap analysis and maturity assessment tool	ISO27001 Risk assessment method	ISO27001	ISO27001	

© 2020 KPMG Huazhen LLP, a People's Republic of China partnership and KPMG Advisory (China) Limited, a limited liability company in China, are member firms of the KPMG global organisation of independent member firms affiliated with KPMG International Limited("KPMG International"), a private English company limited by guarantee. All rights reserved. Printed in China.

Key Point1: Formation of security culture

KPMG believes that the core of ISMS is its PDCA mechanism, and how to form information security culture within the enterprise through implementation ISMS. Therefore, in the process of ISMS implementation, we should seize the pain point of current information security management, and focus on the formation of security culture and PDCA mechanism.

Key Point2: Security governance development

Information security work is often be defined as a work of security management personnel or the responsibility of IT department. This leads to the lack of cooperation from other business departments and operation support departments during regular security management, and the security work cannot be carried out smoothly. Through the in-depth analysis of the current information security responsibility assignment; identify existing problems at current organizational level; combined with actual information security management needs of client, clarify related departments, teams and their responsibilities at the decision-making, management and implementation level; clarify responsibility boundaries of each team, KPMG could assist client to optimize their current security management and make it more efficiently.

Key Point3: Security management implementation

An ISMS that is not fully implemented is just a castle in the air. Based on the previous rich experience of information security management system design and implementation, KPMG summarized a set of practical and effective mechanisms to ensure the implementation of ISMS. Enterprises should ensure the full implementation of the system through the establishment of a team with full participation, clear control and implementation requirements, regular communication and reporting mechanism supplemented by automatic process control design, diversified publicity and mobilization, and closely tracking mechanism. At the same time, it also ensures the monitoring, audit and performance appraisal of the whole management system.

Our ISO27001 can provide services:

- Information security governance
- ISMS Advisory
- ISO27001 certification assistance Advisory
- Cyber security risk assessment
- Cyber security planning advisory
- Cyber security architecture advisory
- Cyber security transformation advisory
- Cyber security training
- Cyber security audit
- Cyber security maturity evaluation
- Cyber security compliance advisory
- Cyber security exercise
- Cyber security technical testing

© 2020 KPMG Huazhen LLP, a People's Republic of China partnership and KPMG Advisory (China) Limited, a limited liability company in China, are member firms of the KPMG global organisation of independent member firms affiliated with KPMG International Limited("KPMG International"), a private English company limited by guarantee. All rights reserved. Printed in China.

Contact us

Henry Shek
KPMG China
Cybersecurity
Partner
Tel: +852 2143 8799
henry.shek@kpmg.com

Richard Zhang
KPMG China
Cybersecurity
Partner
Tel: +86 (21) 2212 3637
richard.zhang@kpmg.com

Quin Huang
KPMG China
Cybersecurity
Director
Tel: +86 (21) 2212 2355
quin.huang@kpmg.com

Danny Hao
KPMG China
Cybersecurity
Director
Tel: +86 (10) 8508 5498
danny.hao@kpmg.com

Brian Cheung
KPMG China
Cybersecurity
Director
Tel: +852 2847 5062
brian.cheung@kpmg.com

Frank Wu
KPMG China
Cybersecurity
Associate Director
Tel: +86 (21) 2212 3180
fm.wu@kpmg.com

Jason Song
KPMG China
Cybersecurity
Associate Director
Tel: +86 (21) 2212 3306
jason.song@kpmg.com

Jason Li
KPMG China
Cybersecurity
Associate Director
Tel: +86 (10) 8508 5497
jz.li@kpmg.com

John Chiu
KPMG China
Cybersecurity
Associate Director
Tel: +852 2847 5096
john.chiu@kpmg.com

Kevin Zhou
KPMG China
Cybersecurity
Associate Director
Tel: +86 (21) 2212 3149
kevin.wt.zhou@kpmg.com

Kevin Fan
KPMG China
Cybersecurity
Associate Director
Tel: +86 (21) 2212 2200
kc.fan@kpmg.com

Olive Wang
KPMG China
Cybersecurity
Associate Director
Tel: +86 (10) 8553 3630
oh.wang@kpmg.com

Andy Yuen
KPMG China
Cybersecurity
Associate Director
Tel: +852 3927 4697
andy.yuen@kpmg.com

William Xu
KPMG China
Cybersecurity
Associate Director
Tel: +86 (21) 2212 4633
william.q.xu@kpmg.com

kpmg.com/cn/socialmedia

For a list of KPMG China offices, please scan the QR code or visit our website:
https://home.kpmg.com/cn/en/home/about/offices.html

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.

© 2020 KPMG Huazhen LLP, a People's Republic of China partnership and KPMG Advisory (China) Limited, a limited liability company in China, are member firms of the KPMG global organisation of independent member firms affiliated with KPMG International Limited("KPMG International"), a private English company limited by guarantee. All rights reserved. Printed in China.

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