MLPS 2.0 Insights and Strategies

Management Consulting

KPMG China

—

May 2019

Preface

Henry Shek
KPMG China
Cybersecurity Advisory
Head of IT Advisory Risk Consulting

Richard Zhang
KPMG China
Cybersecurity Advisory
Partner

With cybercrimes and cyber events occurring more and more frequently around the world, cybersecurity issues are drawing an unprecedented amount of attention. This area is particularly important for the Chinese economy and for Chinese people's livelihoods, as the country has more than 800 million Internet users.

In 2016, China released its first National Cybersecurity Strategy, which states, "There is no national security without cybersecurity." This strategy also highlights the importance of cybersecurity legislation. As a result, the *Cybersecurity Law of the People's Republic of China* ("CSL") was adopted in November 2016 and became effective in June 2017.

As the first fundamental cybersecurity law in China, the CSL made clear the cybersecurity obligations and responsibilities of network operators, individuals and the State. It also consolidated scattered regulations into a unified national law and specified the duties and responsibilities of various stakeholders. Article 21 of the CSL states that China has initiated a cybersecurity multi-level protection scheme ("MLPS"), building it as a basic national cybersecurity system.

In fact, the MLPS is derived from the *Administrative Measures for the Multi-level Protection of Information Security* ("MLPS Administrative Measures"), which has been under implementation by the Ministry of Public Security for years. Based on the MLPS Administrative Measures, the Ministry of Public Security, in conjunction with other related government agencies, drafted the *Regulations on Multi-level Protection for Cybersecurity (Exposure Draft)* ("MLPS Regulation") to support the implementation of CSL and the MLPS. The MLPS Regulation marked the beginning of MLPS 2.0.

Recently, Technical Management Department of the State Administration for Market Regulation (SAMR) held a national standard press conference to officially issue core MLPS 2.0 series of national standards ("MLPS 2.0 series of standards"), including <GB/T 22239-2019 Information Security Technology–Baseline for Classified Protection of Cybersecurity>, <GB/T 25070-2019 Information Security Technology–Technical Requirements of Security Design for Classified Protection of Cybersecurity> and <GB/T 28448-2019 Information Security Technology–Evaluation Requirements for Classified Protection of Cybersecurity>, which can effectively guide network operators, network security enterprises and network security service providers to carry out the multi-level protection implementation work and comprehensively improve the security protection capability of network operators.

Content

MLPS History

1994

Regulations of the People's Republic of China for Safety Protection of Computer Information Systems issued by the State Council

2007

Administrative Measures for the Multi-level Protection of Information Security (GongTongZi [2007] No. 43)

2008-2012

MLPS 1.0 series of national standards released

2014

Symposium on Cybersecurity and Informatisation (19 April Speech)

2017

Cybersecurity Law of the People's Republic of China enacted; MLPS 2.0 series of national standards (draft) released

2018

Regulations on Multi-level Protection for Cybersecurity (Exposure Draft) solicited public opinion; exposure draft of Multi-level Protection 2.0 series of national standards released; and *Regulations for Internet Security Supervision and Inspection by Public Security Organs* (Decree No. 151 of the Ministry of Public Security) officially enacted

2019

Core MLPS 2.0 national standards officially released on May 13th , 2019 and will enact on December 1st, 2019

CSL Article 21: The State has implemented a cybersecurity multi-level protection scheme. Network operators must perform the following security protection duties according to the requirements of the cybersecurity multi-level protection scheme to ensure the network is free from interference, damage, or unauthorised access, and to prevent network data leaks, theft, or falsification…

MLPS 2.0 Challenges

What is MLPS 2.0?

> **As a normative document, the MLPS Administrative Measures primarily apply to government departments and key industries, while the MLPS Regulation is a legal regulation that apply to the supervision of the development, operation, maintenance and use of networks in China.**

CSL connection: As an administrative regulation based on CSL Article 21, the *Regulations on Multi-level Protection for Cybersecurity (Exposure Draft)* ("MLPS Regulation") is an important supporting regulation—along with the MLPS 2.0 series of national standards ("MLPS 2.0 series of standards")—for the establishment of the cybersecurity multi-level protection scheme. According to the MLPS Regulation, network operators are required to classify their network and information systems into different levels and implement security protections accordingly in order to safeguard national cyberspace, ensure the public interest, and protect the rights and interests of citizens and legal persons. These network operators are also required to address security risks presented by new technologies and applications. MLPS 2.0 emphasises the importance of security protection capability, that is, the ability to prevent threats, detect security incidents and recover after damage. Network operators shall ensure that objects of different protection levels have the corresponding levels of security protection ability.

"Network" instead of system: The term "network" as defined in the MLPS Regulation refers to a system comprised of computers, other information terminals and related equipment that follows certain rules and procedures for gathering, storing, transmitting, exchanging and processing information. The MLPS Regulation focuses on three aspects of cybersecurity: infrastructure security, operational security and data security. These three aspects can be further defined by their different equities with security responsibility, different business and system operation models, and different security protection measures.

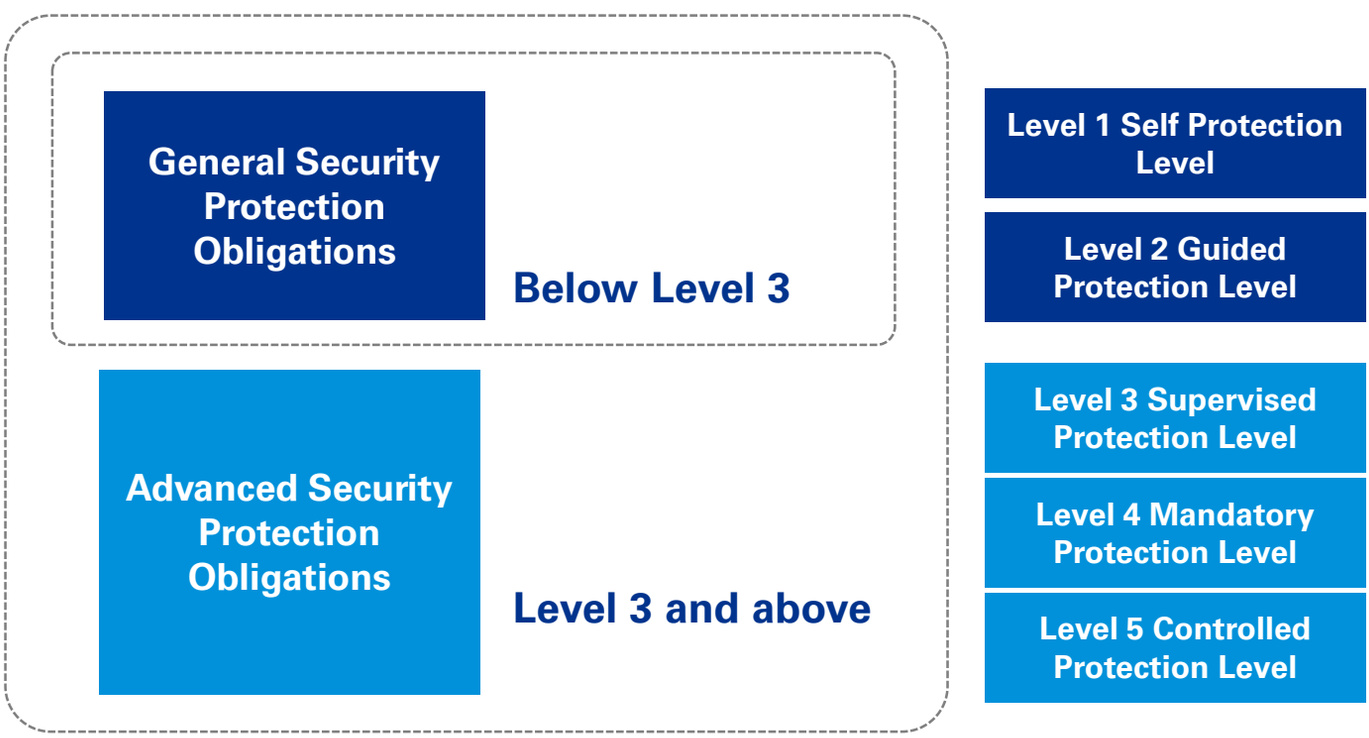
Enhanced enforcement: According the MLPS Regulation, the national cyberspace administration are responsible for comprehensively planning and coordinating cybersecurity efforts, while public security organs are responsible for supervision and management of the cybersecurity multi-level protection scheme. For network operators, the relevant cybersecurity authority is the public security organs where the legal entity is located. Network operators shall follow the requirements of the MLPS 2.0 series of standards: 1) identify the grading objects, reasonably determine their security protection levels, and appoint the responsible security department and personnel; 2) carry out network grading and filing, implementation and remediation of security measures, self-assessments and self-reviews, etc.; 3) implement relevant management and technical measures to fulfil the relevant security protection obligations.

Network Operators' Security Protection Obligations

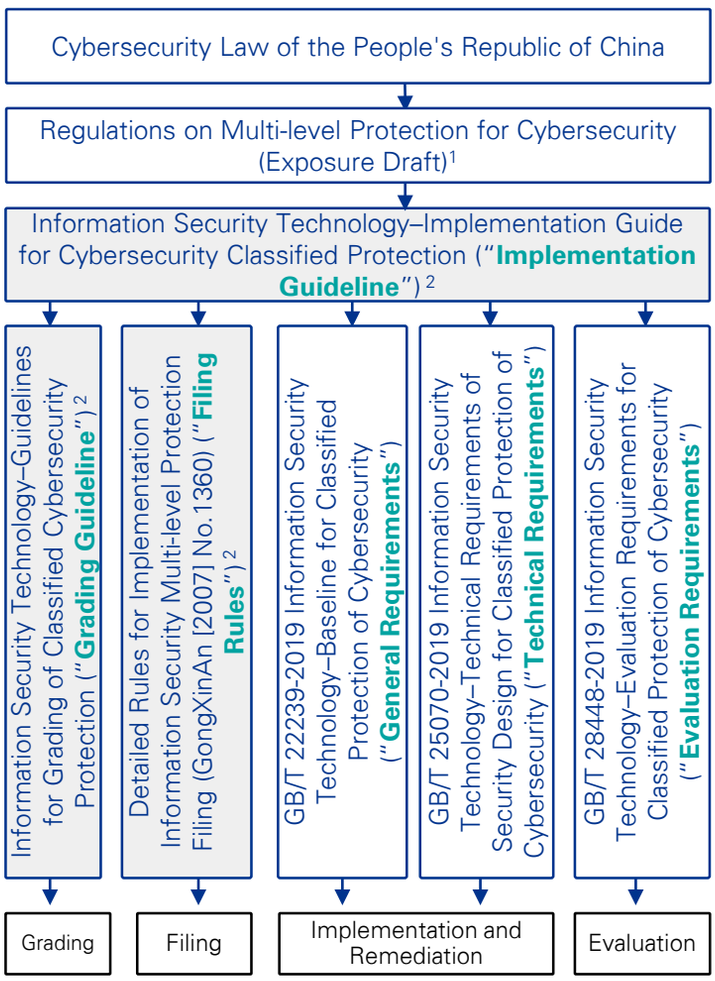
Based on the security protection obligations required of network operators by the CSL, the MLPS Regulation provides more detailed requirements regarding the different levels of security obligations for network operators. This change in the MLPS Regulation provides for the supervisory function of the public security organs and will be conducive to the successful implementation and assessment of the MLPS for network operations.

MLPS Regulation Article 20 specifies eleven general security protection obligations that network operators shall meet, including focusing on compliance and regulation-related matters such as assigning personnel to be responsible for security, establishing and implementing security policies and technical security measures, cybersecurity monitoring and cybersecurity incident management, data classification and protection, personal information protection, network filing, and real-name registration, in addition to more fundamental tasks.

MLPS Regulation Article 21 specifies eight advanced security protection obligations that network operators should comply with for networks graded level 3 or above, including obligations related to security protection elements, cybersecurity strategy planning and implementation, background checks on responsible security personnel and key security personnel, implementation of cybersecurity monitoring and of a management platform, implementation of backup and recovery measures, periodic MLPS assessments, and other areas.



MLPS 2.0 System



Note 1: Based on the MLPS Administrative Measures, the Ministry of Public Security, together with other relevant departments, has drafted the MLPS Regulation. Currently MLPS Administrative Measure is still active, while MLPS Regulation is in draft inviting public reviews and comments.
Note 2: Other MLPS 2.0 series of national standards are still being revised and will be released soon.

Implementation Guideline – Specify the roles and responsibilities of relevant parties, basic processes and implementation requirements across the multi-level protection implementation efforts. The basic processes of multi-level protection include: grading and filing, security planning, security design and implementation, security operations and maintenance, emergency response and protection, and termination of grading objects.

Grading Guideline – Specify the grading method and process for cybersecurity multi-level protection. In addition to the updated grading matrix and process, the new standard adds grading instructions for specific grading objects such as cloud computing platforms, mobile Internet, the Internet of things, big data and industrial control systems.

Filing Rules – Specify processes for filing acceptance, filing review and filing management in order to guide and strengthen multi-level protection filings.

Baseline – Specify general security requirements and extended security requirements for grading objects of levels 1 – 4. It is a security baseline composed of detailed security control requirements, which are applicable to the security implementation and supervision of non-secret grading objects.

Technical Requirements – Specify technical requirements for multi-level protection security design for grading objects of levels 1 – 4, and act as guidance for system operation organisations, information security companies and information security service providers to carry out the design and implementation of technical security for multi-level protection. These requirements can also be used as the basis for information security departments to supervise, inspect and instruct regarding multi-level protection.

Evaluation Requirements – Specify general security evaluation requirements for grading objects of levels 1 – 4, and extended security evaluation requirements for grading objects related to new technologies and applications such as mobile Internet, big data, cloud computing platforms, the Internet of things and industrial control systems.

Relationship with existing regulations from Public Security Organs

Regulations for Internet Security Supervision and Inspection by Public Security Organs and *Administrative Measures on Security Protection for International Connections to Computer Information Networks* have been released by the public security organs to strengthen Internet security, prevent network crimes and maintain public order and social stability. MLPS 2.0, together with existing regulations, aims to safeguard national cybersecurity and must be followed by network operators.

Relationship with Critical Information Infrastructure protection

The MLPS Regulation and *Regulations for the Security Protection of Critical Information Infrastructure (Exposure Draft)* ("CII Regulations") are the most important supporting regulations for the CSL, and serve as a supplement to CSL Article 21 and Article 31 respectively. All network operators must comply with the MLPS Regulation and their relevant standards, and critical information infrastructure operators must meet further MLPS requirements to achieve more extensive protection. As a fundamental and comprehensive cybersecurity regulation, the MLPS Regulation also serves as the basis for critical information infrastructure protection. Although "critical information infrastructure" is not directly mentioned in the MLPS Regulation, the security protection grading of critical information infrastructure is recommended to be level 3 or above.

MLPS 2.0 Highlights

Compared to MLPS 1.0, MLPS 2.0 features significantly **extended** and **strengthened** supervision and implementation processes.

Extended scope and measures

The regulatory scope of MLPS 2.0 has been broadly extended from traditional information systems to network infrastructure, critical information systems, websites, big data centres, cloud computing platforms, the Internet of things, industrial control systems, public service platforms, mobile Internet, and other areas. In addition to grading, filing and evaluation, MLPS 2.0 includes more regulatory enforcement measures such as remote monitoring, on-site inspection, incident investigation, compliance inquiries with responsible personnel, remediation instruction, penalty notifications, emergency network cutoff, and other measures.

Strengthened content and intensity of supervision

Compared with MLPS 1.0, MLPS 2.0 has made major improvements to processes and requirements. Especially for level 2 networks, MLPS 2.0 provides more detailed implementation requirements (e.g. regarding personal information protection). It also integrates specific requirements regarding network product and service security and domestic system maintenance from the CSL and CII Regulations for networks that are level 3 and above.

MLPS 2.0's key updates:

01/ Grading Confirmation

- In MLPS 2.0's information system security protection grading matrix table and business information security protection grading matrix table, the protection level of "causing especially extreme damage to the legitimate rights and interests of citizens, legal persons and other organisations" has been revised from level 2 to level 3. Network operators should objectively evaluate the affected grading objects and their potential damage level (i.e. impacting business availability, legal disputes, property losses, adverse social effects, etc.).
- Under MLPS 1.0, expert reviews only needed to be performed for systems of level 3 or above. However, under MLPS 2.0 such reviews should be performed for networks of level 2 or above.

02/ Risk Control for New Technologies and Applications

- The general requirements and extended requirements of the MLPS 2.0 series of standards require network operators to fully evaluate the security risks presented by new technologies and applications such as cloud computing, big data, artificial intelligence, the internet of things, industrial control systems and mobile Internet, in order to implement security control measures to protect new technologies and applications.

03/ Personal Information Protection

- MLPS 1.0 provided general requirements for data security. In accordance with the CSL, MLPS 2.0 specifies management requirements on personal information protection and states that network operators should establish and implement personal information security protection policies and procedures and security protection measures at all stages across the data lifecycle. In addition, national standards such as the *Personal Information Security Specifications* and the *Security Impact Assessment Guide for Personal Information (Exposure Draft)* may be referred to for specific requirements on personal information protection.

04/ Network Products and Services (Level 3 and above)

- According to the *Measures on Security Examination for Online Products and Services (Trial)* and the *Catalogue of Critical Network Equipment and Dedicated Cybersecurity Products*, the MLPS Regulation requires networks of level 3 and above to adopt network products and services appropriate to their security protection levels. The Regulations also state that important products used in the network must pass testing or certification by professional agencies. Additionally, the MLPS 2.0 series of standards propose that the procurement and use of information security products and encryption products and services follow the requirements of relevant national regulations. Therefore, network operators should ensure that the products they purchase, use and rent are compliant; and they should also vet the qualifications of external security service providers to identify any potential security risks.

05/ Security Management Center

- According to MLPS 2.0, the "security management center" domain is one of the five MLPS technical domains, reflecting the concept of "one center (security management center) and three lines of defense (secure communication network, secure network boundary and secure computer environment). The "security management center" domain for level 2 includes "system management" and "audit management" requirements, while for level 3 it includes "system management", "audit management" and "security management" related requirements.

MLPS 2.0's key updates (cont'd):

06/ Trustable authentication

- According to the MLPS 2.0 Baseline, trustable authentication related requirements have been added into the "secure communication network" domain, "secure network boundary" domain and "secure computer environment" domain of levels 1 – 4. It suggests network operators could perform dynamic trustable authentication for key implementation sessions, and take follow-up actions and records effectively.

07/ System Go-Live Test

- According to the MLPS Regulation, networks classified as level 2 and above must be tested before launching. For newly-built networks classified as level 2, security tests should be performed before operations commence in accordance with the relevant MLPS 2.0 series of standards. Additionally, public security organs are entitled to request testing reports from network operators.

08/ Technical maintenance (Level 3 and above)

- Under the MLPS Regulation, networks of level 3 or above must be technically maintained in China rather than remotely maintained from overseas. When technical maintenance remotely from overseas is needed for business reasons, network operators are required to assess the network's cybersecurity condition and take necessary measures to manage and control risks. Technical maintenance should be recorded, logged and provided for public security organs inspections. Therefore, for network operators the protection intensity for networks of level 3 and above is similar to that for critical information infrastructure.

09/ Security Self-Assessment

- According to the MLPS Regulation, network operators are required to perform self-assessments at least once a year on their implementation of the MLPS procedures and cybersecurity conditions, and they must submit filings to the relevant public security organs regarding any potential risks identified and remediation measures taken. Self-assessment efforts thus become part of the daily work of network operators. Additionally, public security organs will carry out security inspections on networks of level 3 and above at least once a year.

10/ Detection, Early-Warning and Incident Notification (Level 3 and above)

- According to the MLPS Regulation, network operators with networks of level 3 and above must put in place policies and procedures for cybersecurity monitoring, early-warning and incident notification, and report to the relevant public security organs about information regarding cybersecurity monitoring, cybersecurity detection and cybersecurity incidents. Therefore, network operators should establish appropriate incident categorisation and classification procedures, and should put in place procedures for addressing incidents that are based on cybersecurity emergency plans. Additionally, enterprises should establish paths for reporting information to the relevant public security organs.

Proposed Compliance Path for MLPS 2.0

The MLPS is China's fundamental national cybersecurity system, which is the primary method for ensuring cybersecurity compliance and for conducting supervisory activities, and which aims to promote informatisation and cybersecurity maintenance. Enterprises must appoint an eligible testing agency to conduct multi-level protection implementation, assessment and filing in order to effectively manage cybersecurity risks.

KPMG recommends the path below for achieving compliance with the MLPS:

Multi-level Protection Compliance Path

01 System Identification and Grading

- Enterprises should identify systems and generate a system inventory based on the enterprises' operations and plans.
- According to MLPS requirements, enterprises should define network and system boundaries; determine the personnel in charge of information security and grading objects; and perform preliminary grading of internal systems, based on business importance, external service availability for the systems, data type and volume, and other factors.

02 Self-assessment and Remediation

- Based on the identified grading objects and their levels, enterprises should perform gap analysis with reference to the MLPS requirements and produce self-assessment reports.
- For the unfulfilled items, determine the remediation plan and take remedial actions by implementing technical measures, improving management policies, etc.
- Perform compliance assessment, risk assessment and technical testing according to the CSL related requirements as needed to complement MLPS compliance.

03 Third-party Assessment and Filing

- Prepare grading documentation, arrange external expert reviews (level 2 or above), obtain approvals from authorities (where applicable), and submit filings to the relevant public security organs.
- Undergo testing conducted by agencies qualified by the Ministry of Public Security, implement security measures based on the preliminary findings, and obtain the filing certification through the follow-up assessment (level 3 or above).
- Systems of level 3 or above must be tested once a year, and level 2 systems are recommended to be tested once every 2 years.

04 Continuous Improvement

- Formulate security plans and determine cybersecurity tasks and their priorities, costs and resources based on cybersecurity governance goals and findings from the MLPS assessment.
- With reference to MLPS 2.0 and industry best practices, improve the cybersecurity technical protection system (identification, protection, detection, response, recovery, etc.) and perform assessments on a regular basis.
- Stay up to date on cyber security laws, policies and standards, and address new regulations in a timely manner.

KPMG MLPS Compliance Services

KPMG Cybersecurity Services Overview

Strategy and governance	Transformation	Cyber defense	Cyber response
Helping YOU understand how best to align YOUR cyber agenda with YOUR dynamic business and compliance priorities.	Helping YOU build and improve YOUR programs and processes, supported by the right organization and technology, to improve YOUR	Helping YOU maintain YOUR cyber agenda as YOUR business and technology programs evolve by providing greater visibility and understanding of changing risks.	Helping YOU effectively and efficiently response to cyber incidents and conduct forensic analysis and detailed investigations.

Pre Breach → **Post**

KPMG Cyber sees the world from the YOUR perspective, bringing a business context to cyber security for all levels of the organization from the boardroom to the back office.

Helps organizations in transforming YOUR security function into business – enabling platforms so YOU can understand, prioritize and manage YOUR cyber security risks, take control of uncertainty, increase agility and convert risk into advantage

KPMG MLPS Compliance Services

As-is analysis and gap assessment	With regard to the compliance requirements of MLPS 2.0, KPMG can help companies analyse their current state, formulate materials and inputs for grading and filing, and carry out further gap assessment and risk analysis. KPMG can also help develop remediation strategies and action plans based on risk assessments and requirements for security management, business and technology operations.
System optimisation and technical improvement	Based on MLPS 2.0, companies' business and technology status and development strategies, applicable sector standards and best practices, KPMG can help streamline existing cybersecurity systems and improve technical measures; assist companies in developing cybersecurity systems that meet compliance regulations and are practicable; and produce and file policies, procedures, operational manuals and executive records required for assessment and filing purposes.
Project management and coaching	KPMG can provide companies with full lifecycle support throughout the MLPS compliance journey; assist companies in coordinating and communicating with internal and external stakeholders; and prepare materials for grading, filing and assessment, in order to support companies in effectively achieving their compliance goals.

WHY KPMG

Global Network and Collaboration

KPMG's global network of firms has the resources necessary to support you in either localising into China or expanding your operations abroad. Our team can offer steadfast support by helping you establish a cybersecurity management system that takes into account both your global management requirements and local compliance requirements in order to simplify management complexity and ensure feasibility.

Achievements, Credentials and Experience

KPMG has rich experience in implementing cyber compliance measures, specifically with regard to CSL compliance, MLPS compliance, information security management system establishment, data security compliance and other areas. KPMG has assisted a number of organisations in successfully completing MLPS level 3 implementation, assessment and filing.

Active Player in China's Cyber Ecosystem

KPMG maintains close relationships with national and local cybersecurity regulatory authorities, industry authorities, third-party testing companies, certification agencies, and other related institutions. As a member of TC260, KPMG has a history of participation in national and industry information security and informatisation policy discussions and formulation. After decades of practice in local markets, KPMG has managed to establish an ecosystem that covers network security products, security services providers, and industry and sector experts. For these reasons, KPMG is capable of offering a range of value-added services to assist you in your cyber compliance journey in China.

Contact

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

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

Jason He
KPMG China
Cybersecurity Advisory
Partner
Tel: +86 (755) 2547 1129
jason.rk.he@kpmg.com

Patrick Wong
KPMG China
Cybersecurity Advisory
Director
Tel: +852 2140 2823
patrick.c.wong@kpmg.com

Bhagya Perera
KPMG China
Cybersecurity Advisory
Director
Tel: +852 2140 2825
bhagya.perera@kpmg.com

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

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

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

Darryl Sim
KPMG China
Cybersecurity Advisory
Associate Director
Tel: +852 2847 5044
darryl.sim@kpmg.com

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

Stuart Luo
KPMG China
Cybersecurity Advisory
Associate Director
Tel: +86 (755) 2547 3421
stuart.luo@kpmg.com

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

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

kpmg.com/cn