



# Cybersecurity: KPMG at your side

**Our Cybersecurity offer**

October 2021

[kpmg.fr](https://www.kpmg.fr)

# The fundamentals of our offer



## **CYBER IN THE BOARDROOM**

Assist top management in putting Cyber risks under control.



## **TRANSFORMING THE CYBER FUNCTION**

Assist top management in putting Cyber risks under control.



## **TRANSFORMING THE CYBER FUNCTION**

Assist organizations and business lines in securing, and therefore accelerating, digital transformation.



## **CYBER RESILIENCE**

Assist organizations with their operational defense through preventive, detective and curative controls, in addition to continuous testing of controls.

# Our Cybersecurity offer

## 01 CLIENT CHALLENGE

Technology makes many things possible, but possible doesn't always mean safe.

## 02 KPMG RESPONSE

KPMG can help you anticipate tomorrow, move faster and get an edge with technology that is secured and trusted.

## 03 WHY KPMG?

KPMG's professionals are at your side, bringing you a combination of technological expertise, in-depth business and industry knowledge to help you protect and grow your business by addressing potentially divergent issues:

- Resilience and agility
- Serenity despite the risk
- Opportunities despite threats

## 04 OUR SHARED VALUE

Together, we're creating a trusted digital world, so you can push the limits of what's possible.



# Cyber in the boardroom

## YOUR ISSUES

Given the potential critical impacts of Cyber risks on organizations, top management needs to be assisted in:

- Identifying and understanding the most critical Cyber risks ;
- Defining Cyber risk management strategies ;
- Implementing programs in order to reduce or transfer Cyber risks and comply with Cyber laws and regulations.

## OUR SERVICES

- Overall assessment / benchmark of the organization Cybersecurity maturity
- Provision of Cybersecurity expertise and awareness to the Board of Directors
- Global mapping of Cybersecurity threats, regulations and risks, identification of the organization "Crown Jewels"
- Audit of Cybersecurity function
- Development of the Cybersecurity roadmap
- Definition of a world class Cybersecurity function
- Implementation of Cyber insurance
- Design and monitoring of regulatory compliance programs (e.g. GDPR, LPM / OIV, SWIFT, NIS, HDS, PSD2, PCI-DSS)
- Quality and reliability improvement on regulators reporting on Cyber
- Assessment of the integration of Cyber within the organization
- Securing top management use of digital tools
- Cyber crisis simulations, Cyber stress-tests
- Cybersecurity due-diligence during mergers / acquisitions





## YOUR ISSUES

The Cybersecurity function is now recognized as a critical element in organizations' ability to protect their core business from Cyber risks.

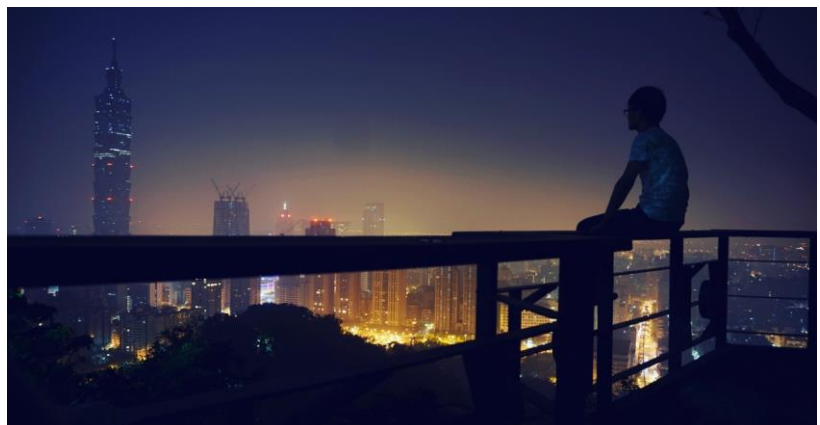
In today's world, it must provide high quality and efficient security services and solutions to business lines and the overall organization.

It must also enable the Board to ensure that Cyber risks are under control, based on factual elements.

# Transforming the Cyber function

## OUR SERVICES

- Cybersecurity risk analysis (organization / IT / project)
- Assessment of the IT Cybersecurity Level (ISO27002)
- Cyber Audit and penetration tests, Red Teaming, mapping of Internet access points
- Development and implementation of Cybersecurity programs
- Assistance to ISMS implementation and ISO27001 certification
- Definition or improvement of Cybersecurity governance, policies, processes, procedures and guidelines
- Integration of Cybersecurity in project management methodologies (including Agile / DevOps)
- Cybersecurity awareness and training (VIP, IT, business, developers)
- Assistance to the selection and deployment of Cybersecurity tools / services / solutions (Internet architectures, DRP, SOC, SIEM, IAM, IDS / IPS, DLP, anti-APT, anti-DDoS, Bug Bounty, SIRP)
- Optimization of management and reporting on Cybersecurity (KPI, dashboards)
- Regulatory compliance programs implementation (GDPR, LPM / OIV, SWIFT, NIS, HDS, PSD2, PCI-DSS)
- Third-party Cybersecurity reviews (vendors, suppliers, service providers, including cloud service providers)





## YOUR ISSUES

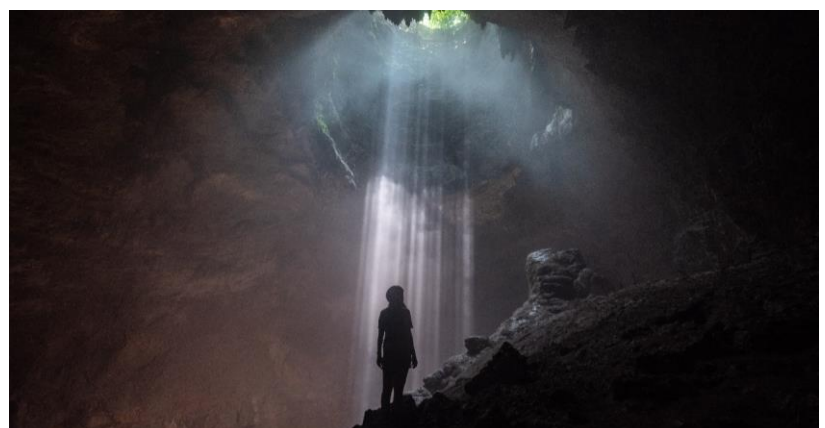
Businesses have embraced digital transformation and are very active in the field of new online services, connected devices as well as in solutions based on innovative technologies such as blockchain.

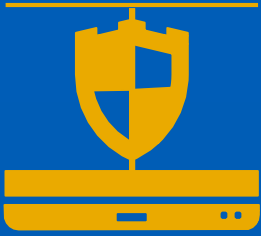
In this context, it is vital that organizations take Cyber risks into account at the very start of projects. Otherwise, they might face security breaches in their systems or in products sold to customers, with consequences that could significantly impact them or their clients.

# Securing digital transformation

## OUR SERVICES

- Awareness on Cyber for business
- Cybersecurity risk analysis related to online applications and services / mobile apps / Internet of Things (IoT) / infrastructure
- Test of security and resilience of business systems / applications / online services / Internet of Things (IoT) / infrastructures through penetration tests / configuration reviews / source code audits / architecture audits
- Assistance on GDPR, LPM / OIV, SWIFT CSP, NIS, PCI-DSS, PSD2 compliance programs on specific business perimeter (risk analysis, customization of business/IT processes, implementation of security measures, testing, reporting)
- Assistance on improving cyber-resilience of business processes or B2B / B2C services (BIA, BCP/DRP, anti-DDoS systems, threat intel, SOC, crisis management, forensic, etc.)
- Assistance on securing industrial information systems / SCADA / IIoT (e.g. risk analysis, diagnostics, security plans, governance, change management)
- Integration of business solutions (including cloud) into the organization security systems and policies
- Assistance on securing business applications (SAP, Oracle)
- Vulnerability research in new technologies (e.g. blockchain, 3D printing, IoT, AI, ZigBee)
- Cybersecurity audit of third parties (vendors, suppliers, service providers)





# Cyber resilience

## YOUR ISSUES

Cyber threats have transformed, becoming more and more innovative, shifting and agile. Attackers evolve at the pace of technology and business. They can lurk in your network for months and strike in a matter of minutes.

To remain ahead of such professional, creative and efficient attackers, Cybersecurity measures must continuously adapt and be more responsive.

Moreover, they must ensure the resilience of business processes beyond the mere protection of IT.

## OUR SERVICES

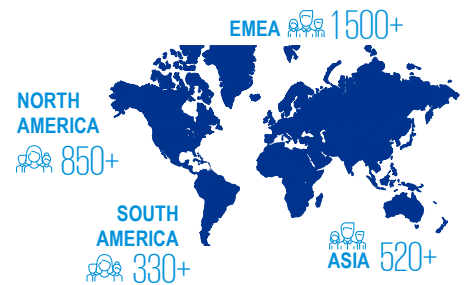
- Assessment of the Cyber-resilience of the organization or of a business process
- Testing of infrastructures, networks, applications, web services through penetration tests (black/grey/white box), source code audits, architecture audits, configuration reviews and physical security audits
- "Red" and "Purple team" penetration tests, phishing campaigns and social engineering
- Hands-on testing of security measures: SOC, anti-DDoS devices, anti-APT systems
- Access control reviews, including the analysis of Active Directory compromise paths
- Assistance in defining test strategies (e.g. penetration tests, vulnerability scans, bug bounty)
- Design of technical architectures and business processes resilient to identified Cyber threats
- Cybersecurity incident response, crisis management, forensic and reverse-engineering
- Hardening of technologies and IT components, drafting of related security hardening guides
- Cyber threat evolution analysis, Threat Intelligence



# Our strengths

## A worldwide presence

An international presence, with a network of 110 partners and more than 3,200 specialists in Cyber and Privacy in 50 countries



For the third consecutive year, KPMG is an international leader in Cybersecurity

*According to the Forrester 2019 Survey*



KPMG ranked among the world leaders in Cyber Security for ALM Intelligence





# Our capabilities

## Cybersecurity Lab

KPMG has built a dedicated Cybersecurity Lab based in Paris. This collaborative workspace promotes the sharing of knowledge and enables our consultants perform cyber defense engagements for our clients, to simulate specific environments for testing, to learn new technologies, and to improve their technical expertise.



## PASSI\* qualification

KPMG has obtained the PASSI\* qualification from the French government Information Systems Security Agency (ANSSI), which attests:



- The expertise and integrity of our auditors
- The adequate protection of data, reports and documents collected and exchanged during the cybersecurity assessments
- The quality of our security assessment methodology

## Insights Center

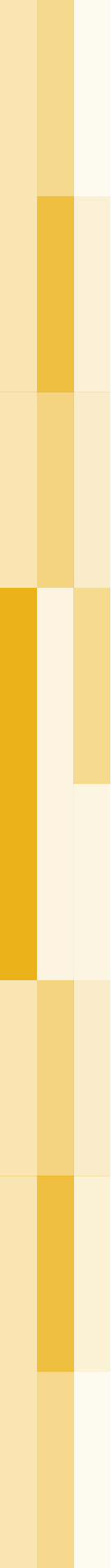
The Insights Center, a unique collaborative workspace dedicated for our clients, with three paths on Cybersecurity topics :

- Cyber Awareness,
- Cyber risks cartography
- and Cyber Crisis Simulation.

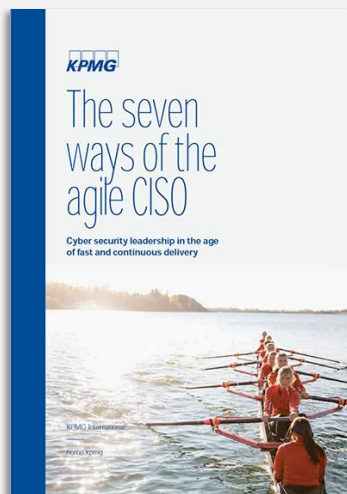
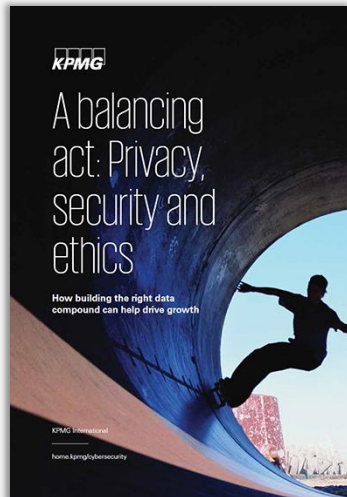


*\* Qualified activities are intrusion testing, configuration assessments, organizational assessments, architecture assessments and source code assessments. Not all of our IT Security Assessments activities are PASSI qualified.*

Qualification attestation N° : 20118. Effective date : Monday 23th November 2020.  
Expiration date : Sunday 24th September 2023. Version : 3



# Our latest publications



# Contacts

**Vincent Maret**  
**Partner**  
**Head of Cybersecurity and Data Privacy services**

Mob: +33 6 17 12 22 13  
Email: [vmaret@kpmg.fr](mailto:vmaret@kpmg.fr)

**Faycal El Belghami**  
**Partner**  
**Cybersecurity Banking and Financial services**

Mob: +33 7 77 31 21 60  
Email: [felbelghami@kpmg.fr](mailto:felbelghami@kpmg.fr)

**Guillaume Rablat**  
**Director**  
**CyberDefense services**

Mob: +33 6 61 57 21 43  
Email: [grablat@kpmg.fr](mailto:grablat@kpmg.fr)

**kpmg.fr**

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 endeavor 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. KPMG S.A. is the member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a Private English company limited by guarantee. KPMG International and its related entities provide no services to clients. No member firm has any authority to obligate or bind KPMG International or any other member firm vis-à-vis third parties, nor does KPMG International have any such authority to obligate or bind any member firm.

© 2021 KPMG S.A., a French limited liability entity and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a Private English company limited by guarantee. All rights reserved. The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organization.

Crédit photos : Shutterstock, iStock, GettyImages, freepik, Unsplash