KPMG

Protecting your customers and business operations

KPMG in Bahrain Cyber Security service offering and capabilities

kpmg.com/bh

Cyber attacks are an inevitable part of the digital world

The advent of digital innovation has improved connectivity and created significant value across business models, customer experience and operations.

However, this greater connectivity brings increasing cyber vulnerability. According to KPMG's 2018 Global CEO Outlook Survey , about half of all CEOs (49 percent) say that a cyber attack is now a case of 'when', instead of 'if'.

How much vulnerability?

Many CEOs are concerned about the robustness of their lines of defence. Only about half of CEOs (51 percent) believe they are well-prepared for a cyber attack.

Given the importance of energy and power to countries' economy and society, it is perhaps not surprising that CEOs from the infrastructure sector consider themselves to be the most well-prepared against cyber aggressors compared with their counterparts in other sectors.

> “It [cyber risk] is a very big issue because as the technology changes, it opens up more loopholes. We have manufacturing systems that control things, so if they are hacked or frozen or lock-up, it could obviously have a major impact on us.”
>
> **Tim Murray**
> CEO, Aluminium Bahrain (a manufacturing company).

KPMG can help you protect your customers and business operations

KPMG looks at the digital world from your perspective, bringing a business context to cyber security for all levels of your organisation — from the boardroom to the back office.

This begins with helping you understand, prioritise, and manage your cyber risks from strategy through implementation.

Cyber penetration testing

Incident response training

Cyber framework compliance

Cyber staff augmentation

Cyber penetration testing

Testing your network to simulate the organisation readiness for a variety of cyber attack scenarios.

External attack simulation

Our black box approach starts from an external attacker perspective as we attempt to gain internal network access. We test the full range of your external attack surfaces, including your public-facing websites, online applications, employee email and employee remote access.

Internal attack simulation

We simulate the steps a hacker would take after gaining an initial foothold into your network. Your defence, detection and response capabilities are tested as we demonstrate whether an attacker could stealthily move through your network, shut down your business and steal confidential data.

Incident response training

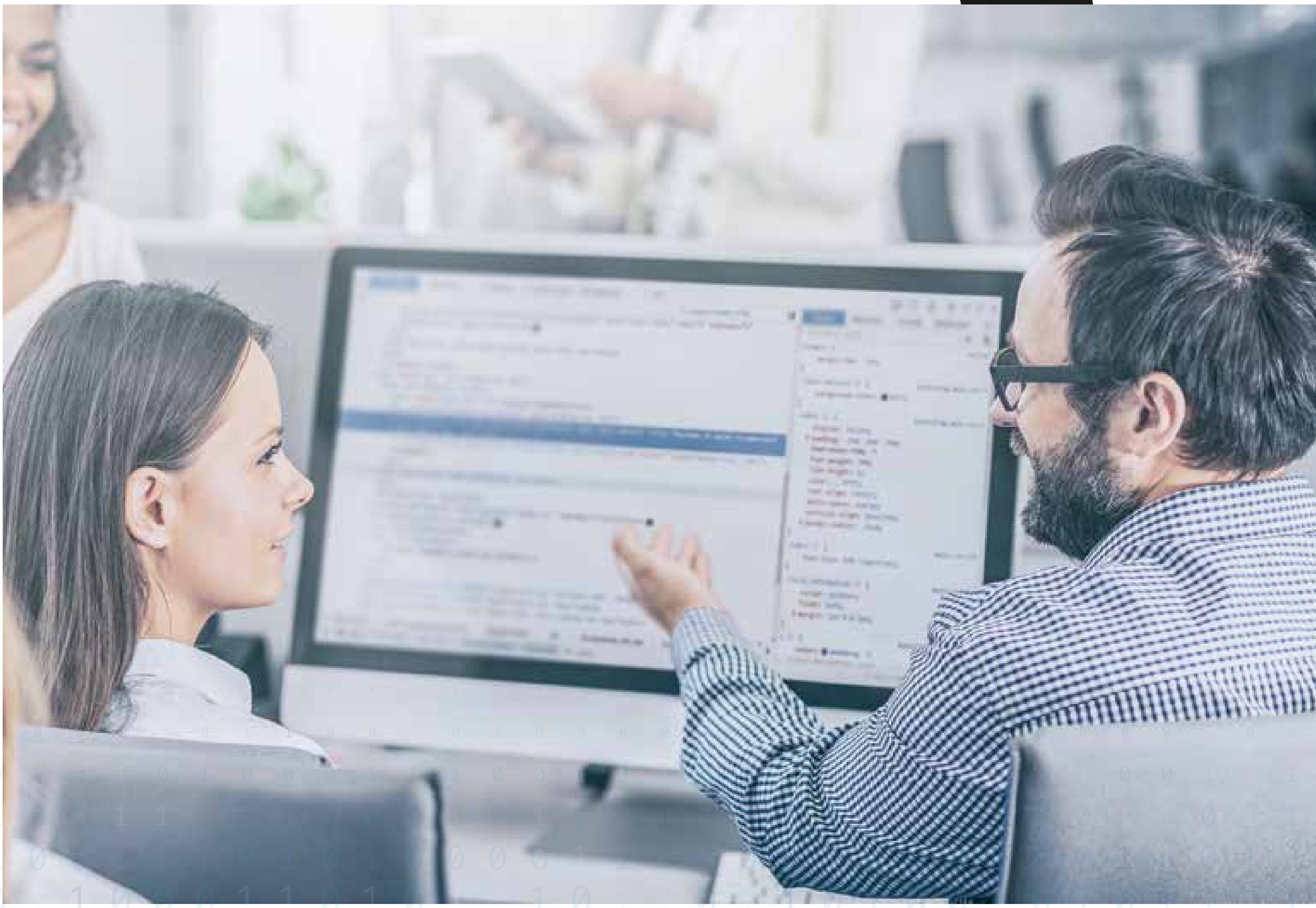
Preparing your staff to proactively defend and quickly respond to cyber incidents.

Cyber incident resilience training

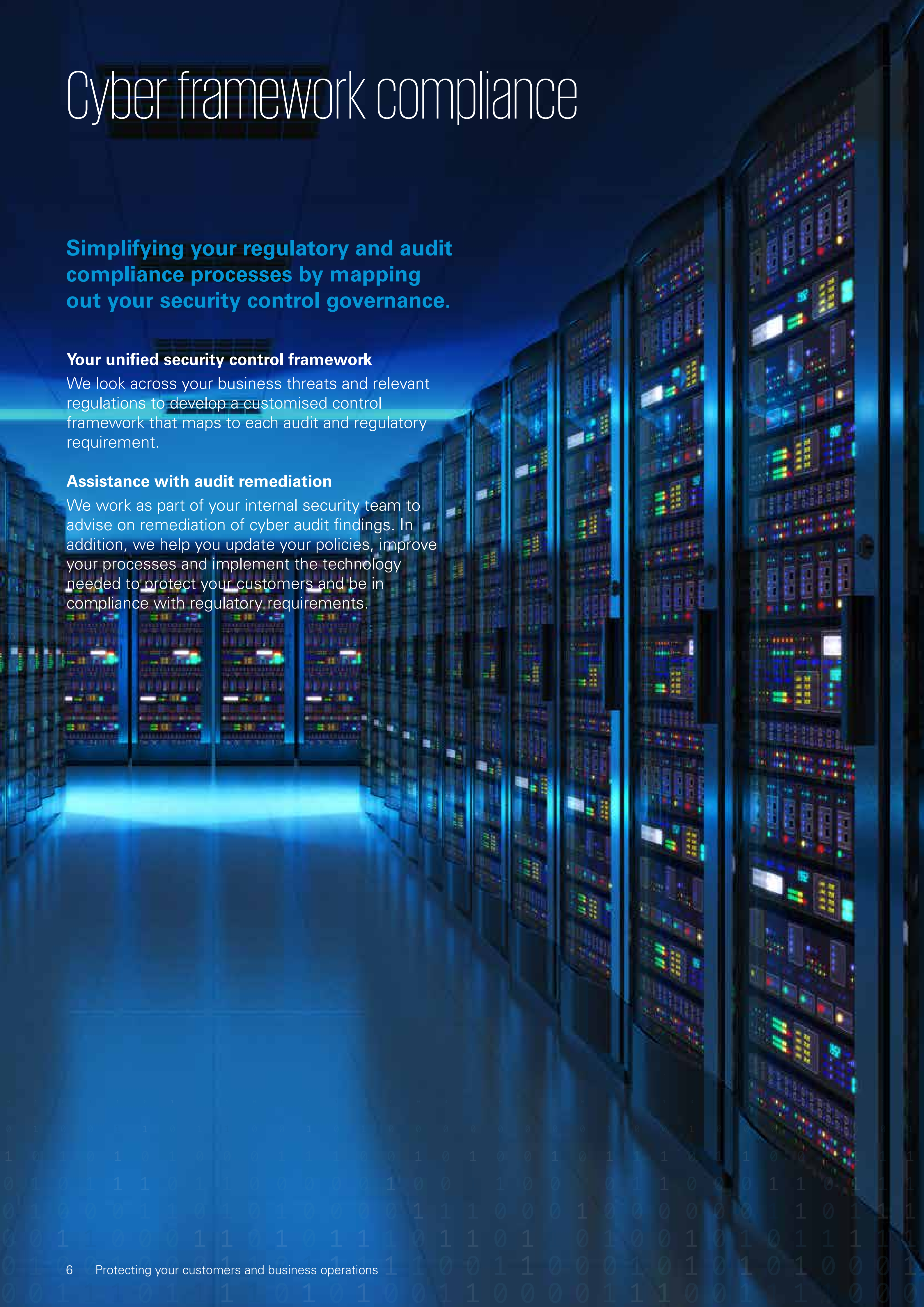
We prepare your cyber-defence staff to respond to real-life scenarios in a way that reduces customer impact and financial loss.

We provide all levels of incident response training, from computer log forensics to advanced malware analysis.

In addition, we facilitate cyber response table-top exercises with representatives from each business unit to practice internal coordination based on recent cyber attack scenarios in your industry.



Cyber framework compliance



Simplifying your regulatory and audit compliance processes by mapping out your security control governance.

Your unified security control framework

We look across your business threats and relevant regulations to develop a customised control framework that maps to each audit and regulatory requirement.

Assistance with audit remediation

We work as part of your internal security team to advise on remediation of cyber audit findings. In addition, we help you update your policies, improve your processes and implement the technology needed to protect your customers and be in compliance with regulatory requirements.

Cyber staff augmentation

Our cyber security professionals join your organisation and fill in the gaps to allow your broader business and technology programmes to safely evolve and mature.

Advanced technical skillsets

Our team has advanced cyber attack and defence skills. We perform solution-specific technical implementations and operate alongside you as part of your defence team.

Mature cyber governance skillsets
We have subject matter expertise in each compliance framework and audit domain. We help you develop and operate mature cyber governance processes, including metrics and board reporting.

For further information, please contact:

Logan Simpson
Lead Cyber Security
Management Consulting
E : jlsimpson@kpmg.com

Padmanabhan Nurani
Digital Advisory
Management Consulting
E : pnurani@kpmg.com

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.