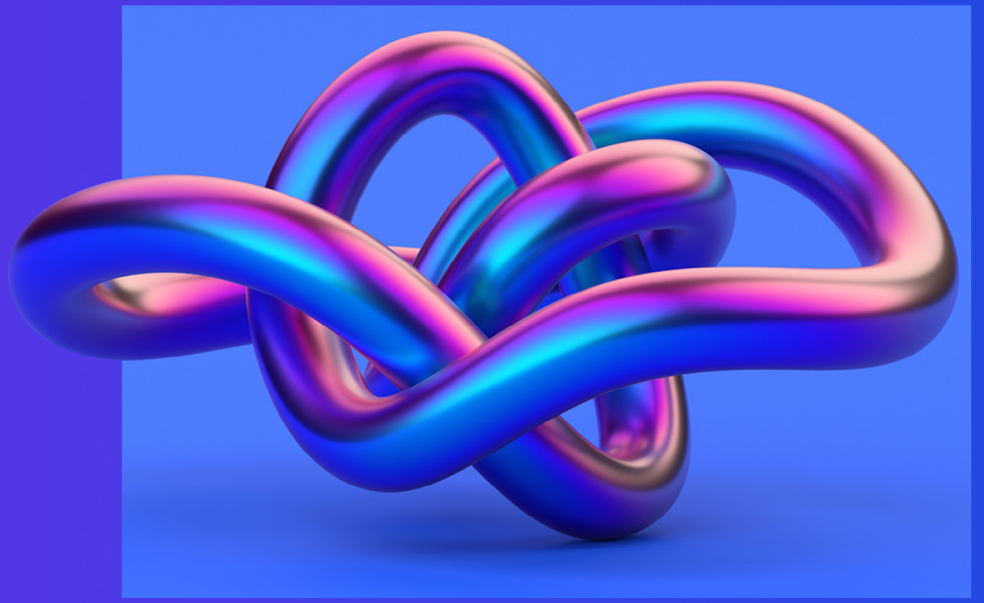
KPMG

Cybersecurity considerations 2023

Industrial Manufacturing



Foreword

Industrial manufacturing (IM) depends on the governance of data and the digital infrastructure behind operational technology (OT). The pandemic accelerated a shift to digital channels bringing these issues into sharp focus. As global economies and supply chains were disrupted, organizations had to rethink their dependencies on goods, services and the evolving digital infrastructure underpinning them.

Breakthrough technologies—artificial intelligence, blockchain, biometrics, hyperconnected systems, and virtual reality, to name just a few—are shaping the future. And all can pose new security, privacy and ethical challenges and raise fundamental questions about our trust in digital systems. However, for IM, these technologies will cause further disparity between IT and OT environments.

While consensus on how to best tackle these issues can be difficult, global commerce must work together to thrive, and we need to address the concerns now as we work to innovate, not retrospectively when it's too late.

The list of industries we consider systemically important is also changing. In the past, we focused on utilities, telecommunications and financial services.

Now we have a complex tapestry of public-private partnerships, connected ecosystems and information infrastructures. One look at a new manufacturing plant shows a hyperconnected network of "smart" relays, remote terminal units, data lakes and managed services—all of which are now systemically critical to the creation of high-quality products.

As the degree of interconnectedness and dependency increases, so too does the interest from those looking to attack and exploit these infrastructures.

With these changes comes a global drive toward greater cybersecurity oversight. This increases concern among organizations over the growing burden of regulation and the diversity of various reporting requirements. As a result, manufacturers are putting more and more emphasis on consolidating security governance into risk management and embedding technical controls into operations, both in response to the changing threats and as a need to comply with transborder regulatory requirements.

Cybersecurity should be integral to every business line, function and service. Organizations must aim to break down siloes to ensure that cybersecurity is ubiquitous across the enterprise and woven into strategy and your floor-level operating procedures. As Lisa Heneghan, chief global digital officer, KPMG International, says:

"Organizations need to start thinking about cybersecurity as the golden thread that runs throughout their organization. It should be put at the heart of business and used as a foundation to build digital trust. But the chief information security officer (CISO) and their teams cannot do this alone; it should be the responsibility of everyone. This isn't easy—first, people should understand how it relates to them—and then you must think about how you can integrate security into existing processes. Treating every business function as a customer and designing security controls with experience in mind can encourage responsible and secure behaviors and can benefit the business hugely."

CISOs will likely also play a major role in activating and shaping a broader dialogue around the resilience of business to digital disruption, helping companies better understand the evolving nature of the assets and digital services companies need to protect and providing the basis for trust in those systems.

This report explores the actions CISOs, specifically, and the broader business, generally, can take in the year ahead to demonstrate to boards and senior management that digital trust can and should be a competitive advantage.

Michael Gomez

Industrial Manufacturing Leader
Cyber Security Services
KPMG in the US

© 2023 Copyright owned by one or more of the KPMG International entities. KPMG International entities provide no services to clients. All rights reserved. USCS001113-1A

Key cybersecurity considerations for IM in 2023

Click on each consideration to learn more.

01

Digital trust: A shared responsibility

Are organizations thinking broadly enough about how to protect the interests of employees, customers, suppliers, and partners?

02

Unobtrusive security drives secure behaviors

How do security teams effectively integrate security into business processes, agile development programs, and disparate operating models?

03

Securing a smart world

What are the implications for security and privacy teams as companies shift toward a smart, hyperconnected product mindset?

© 2023 Copyright owned by one or more of the KPMG International entities. KPMG International entities provide no services to clients. All rights reserved. USCS001113-1A

Consideration 1

Digital trust: A shared responsibility

Digital trust is finding its way onto Board agendas as privacy, security and ethics debates gain momentum—partly driven by regulation and partly by public opinion. The future success of any digitally enabled business is built on digital trust—cybersecurity and privacy are vital foundations for that trust. CISOs must be prepared to help the board and C-suite create and maintain the trust of their stakeholders if they are to create a competitive advantage. Realizing this potential requires a collective commitment from all stakeholders.

Globalization has made the world borderless and interconnected—a reality made only too evident by the disruption to global supply chains brought on by the pandemic. To create lasting relationships with customers (whether B2B or B2C), organizations must establish and maintain digital trust.

Value and trust

Trust is key to success—and is not just about reputation. Boosting trust can create competitive advantage and can add to the bottom line.

More than 1/3 of organizations recognize that increased trust leads to improved profitability.

But 65% report that information security requirements are shaped by compliance needs rather than long-term strategic ambitions.

65% of executives continue to view information security as a risk-reduction activity rather than a business enabler.

49% believe that the board of directors sees security as a necessary cost rather than a way to gain competitive advantage.

Source: KPMG Cyber trust insights 2022.

© 2023 Copyright owned by one or more of the KPMG International entities. KPMG International entities provide no services to clients. All rights reserved. USCS001113-1A

Businesses are starting to care

Growing numbers of senior leaders recognize the benefits of digital trust, with 37 percent seeing improved profitability as the top commercial advantage of increased trust.[1] Digital trust encompasses a wide range of disciplines. Cybersecurity is a major part of that broad spectrum of closely linked digital trust–related issues—reliability, safety, privacy and transparency. These areas impact how companies conduct business and pursue values; the products and services provided; the technology used; how to collect and use data; and how to protect the interests of customers, employees, suppliers, and all other third-party partners and stakeholders.

By contrast, 65 percent continue to view information security as a risk-reduction activity rather than a business enabler.[2] Many organizations still view cybersecurity primarily as a cost and not necessarily as an investment in the future, which is misguided. CISOs should embrace the concept of digital trust and demonstrate how security as an enabler for the business will securely support an organization's digital growth agenda.

CISOs have a significant role in helping their organizations build digital trust, but they cannot do it alone. They should invest sufficient time in encouraging other critical internal and external stakeholders with respect to their respective roles on the digital trust journey. Indeed, CISOs must demonstrate to the C-suite and board why this is such an important topic and how digital trust depends on clearly articulated, business-focused strategies.

As the World Economic Forum (WEF) suggests, companies are beginning to acknowledge that cybersecurity is as much a strategic business element as enterprise risk, product development and data management. In its report, *Earning Digital Trust: Decision-Making for Trustworthy Technologies*, the WEF writes, "Digital trust requires a holistic approach, where cybersecurity is one dimension of trust among many."[3]

What digital trust means to customers

While the typical retail consumer may not care about the nuts and bolts of a company's formal data protection program, the moment customers learn of a breach, they want to know what action is being taken and that their interests are at the heart of the response. The organization can reestablish trust over time by responding to the incident expeditiously and transparently.

Today's consumers understand that breaches happen, and, gradually, most come back if the company offers solid products and services at a competitive price point, there is a consistently positive customer experience, and the details around the response to and recovery from a cyber event are clearly communicated and reassuring.

[1] KPMG International, KPMG Cyber trust insights survey, "Building trust through cybersecurity and privacy," 2022
[2] Ibid
[3] World Economic Forum, Earning Digital Trust: Decision-Making for Trustworthy Technologies," November 2022

© 2023 Copyright owned by one or more of the KPMG International entities. KPMG International entities provide no services to clients. All rights reserved. USCS001113-1A

Digital trust strategies that work

It's vital to embed the concept of digital trust into corporate strategy, product development, and the company's overall market presence and relationship with corporate and retail customers. Thinking broadly about what digital trust means across different stakeholder groups can help underline the importance of cybersecurity and the other disciplines that contribute to establishing and maintaining digital trust, as well as encourage a holistic approach across disciplines.

Trust is a function of specific technologies developed or deployed and the decisions leadership makes. CISOs must continually support a narrative for the board and C-suite to clarify why and how cybersecurity is an integral building block for digital trust.

CISOs must help drive decisions around the right partners and suppliers. Qualifying criteria must be established covering transparency regarding information protection practices and the organization's ability to demonstrate adequate recovery and response resilience.

Make no mistake, regulatory obligations are expected to grow regarding the components of digital trust and so can expectations over the levels of transparency and accountability regulators expect from companies in this regard. A principle-based and holistic approach to meeting the diverse and increasingly complex regulatory landscape can pay dividends and avoid creating costly compliance-driven silos.

It starts at the top and filters down—if leadership accepts and lives this narrative, so should the rest of the organization. That means making it a tangible feature of the company's annual report, in which the company's philosophy and strategy around digital trust by design are outlined in detail. With 34 percent of corporate leaders concerned about their businesses' ability to satisfy reporting requirements for greater transparency over cybersecurity and privacy, KPMG professionals advocate a proactive approach.[4]

Industrial manufacturing considerations

Are manufacturing organizations thinking broadly enough about how to protect the interests of employees, customers, suppliers, and partners?

Many of the largest security breaches have traced the initial attack vector back to a vendor or third party. In turn, multiple cybersecurity regulations and industry frameworks have added third-party security controls to their requirements list.

Unfortunately, industrial manufacturing may have one of the largest attack surfaces when it comes to the sheer number of upstream and downstream vendors involved in business operations. Every day, we work to iteratively improve our own security requirements without affecting the manufacturing plants' productivity. Yet, now, we must worry about our vendors meeting a minimum set of security standards as well.

In an industry where protective relays and remote terminal units are just now joining IP connectivity, it is important to start with engineering-first principles. While it is easy to discuss all the buzzwords regarding automation in third-party security (e.g. AI chat–driven vendor assessments), establishing a solid set of security controls is essential to long-term success.

As such, manufacturers should look at vendor security like they do product creation and simplify the process. A documented core set of security controls for all vendors to confirm compliance with is a strong place to start.

Manufacturers need to establish a foundational checklist of security expectations and would greatly benefit from keeping it simple before transitioning fully into the world of automation.

[4] KPMG Cyber trust insights survey. Op cit.

© 2023 Copyright owned by one or more of the KPMG International entities. KPMG International entities provide no services to clients. All rights reserved. USCS001113-1A

Consideration 2

Unobtrusive security drives secure behaviors

Embedding security within the business in a way that helps people work confidently, make productive choices, and play their part in protecting the organization must be a key, albeit often elusive, CISO objective. It's all too easy for people to see security as an impediment, and only by considering security from both human and business-centric perspectives can CISOs hope to change this mindset.

Perhaps the most essential point is to be attentive to where and when security matters most and where additional security measures will likely impact the business justifiably. There is no absolute security, and if CISOs try to protect everything at every moment, they risk protecting nothing as users find ways around intrusive security measures. CISOs need to be pragmatic around the extent of security controls that are warranted and commensurate with the criticality of the specific business process and the related risk profile.

Confidence in the CISO

Organizations display high levels of confidence and strong belief in the CISO's ability to deliver on crucial tasks.

79% of organizations are confident CISOs can accurately map where critical data is across the enterprise.

3/4 are confident CISOs can identify what their crown data jewels are.

78% are confident CISOs know how much of their sensitive data is with third parties and that it's appropriately secured.

Source: KPMG Cyber trust insights 2022

© 2023 Copyright owned by one or more of the KPMG International entities. KPMG International entities provide no services to clients. All rights reserved. USCS001113-1A

Companies should move away from thinking about enterprise security in binary terms. In today's environment, it's a moving target, and the concept of 'secure' versus 'not secure' is transitory. Instead, CISOs should work to raise the organizational IQ around cybersecurity through awareness; simple, intuitive processes engineered with users in mind; and a better-informed employee base and executive team.

Customer experience applies to security too

It's crucial to focus on building realistic processes for responsible users while still having the means to detect and quickly counter malicious activity. It boils down to ease of use, customer experience and planning around cybersecurity within the context of enterprise-wide priorities—the commercial needs of the broader business—as opposed to thinking of it purely as a regulatory imperative.

Advances in technology can help. From defensive AI, machine learning and chatbots to cloud encryption, blockchain and extended detection and response applications, all are vital parts of the puzzle. So too is creating a more security-aware workforce, guided by consistent IT governance, to inspire people to approach digital communications with appropriate caution. CISOs should consider how they can help employees do the right thing instinctively and design security controls that support them in doing so.

As an ongoing, ever-evolving endeavor, cybersecurity presents many opportunities to 'bolt on' new tools and controls. Still, we encourage organizations to build it in from the beginning, considering the human element. Major transformational initiatives have many components—one should be security. Building security into broad process-oriented initiatives, such as DevSecOps, operational technology and procurement, can be an effective and unobtrusive way to motivate people to behave securely and function as human firewalls without seeming overbearing.

Security teams can learn much from the way organizations enhance the customer experience. Internal security controls should be easy to use, or employees may be motivated to bypass these processes; consider including customer experience specialists in the design of controls.

Security processes should also be personal for internal users. Require the individual to make judgment calls, explain the context, draw a parallel between the value of cautious, secure behavior in their personal and professional lives and make them 'edutaining.' People can then play their part in the security and not be seen as the weakest link.

Industrial manufacturing considerations

How do security teams effectively integrate security into business processes, agile development programs and disparate operating models?

Often, the greatest threats come from inside and are not driven by malicious intent. At a time when manufacturing plant uptime is so critical, different teams in the same company sometimes simply get in each other's way and cause operational issues.

Over time and acquisitions, fiefdoms can form between operations and the business, creating siloes in which team members can inadvertently work against each other. Like it or not, security is a cross-organizational function that provides services to both constituencies often in an attempt to connect the disparate functions.

To operate most effectively, security cannot be seen as an 'ivory tower' organization, disconnected from operations and simply dictating new requirements that floor engineers see as nothing more than roadblocks.

The most secure manufacturers have multiple themes in common:

- A clear three-lines-of-defense model in which roles and responsibilities establish that the second line of defense sets the security requirements with input from the first line, and the first line operates with security always in mind
- Security is built into the operational culture from the beginning, just as safety and line-production efficiency are.
- Security checks are integrated into the natural quality check processes, so they do not end up being an end-of-process barrier that seems bolted on, rather than part of the design.

KPMG © 2023 Copyright owned by one or more of the KPMG International entities. KPMG International entities provide no services to clients. All rights reserved. USCS001113-1A

Consideration 3

Securing a smart world

Businesses across almost every industry are shifting to a product mindset—focusing on developing network-enabled services and managing their supporting devices. CISOs and their teams are getting pulled into discussions with engineering, development and product support teams as organizations realize product security matters too.

In today's smart-product-focused environment, some emerging drivers or enablers dominate:

5G
Offers speed, hyperconnectivity and reduced latency

Quantum computing
Massively cuts processing and calculation time

Trust architectures
Help to ensure that data and identities are secure and trusted from one connected device to another

Software 2.0
Rapid, AI-written code that can reduce complexity while increasing development speed from months to weeks

Applied AI
Real-world fundamental application of artificial intelligence as a developmental wrapper around smart products

CEO cyber outlook

Growing experience of the challenges of cybersecurity is also giving CEOs a clearer picture of how prepared—or underprepared—they may be.

24% of CEOs recognize they're underprepared for a cyberattack, compared to 13 percent in 2021.

56% say they're prepared.

3/4 say their organization has a plan in place to deal with ransomware attacks.

3 in 4 CEOs say that protecting their partner ecosystem and supply chain is just as important as building their organization's cyber defenses.

Source: KPMG 2022 CEO Outlook

© 2023 Copyright owned by one or more of the KPMG International entities. KPMG International entities provide no services to clients. All rights reserved. USCS001113-1A

There are many smart device risks, such as weak default passwords, poor or absent encryption, failure to provide timely secure software updates, malware and lack of denial-of-service protection, to name just a few. CISOs must realize that, with these devices, security is not just based on the CIA triad (confidentiality, integrity and availability). Safety is also a key consideration because hyperconnected, tangible real- world systems are involved. Cyber professionals must apply those risks to a CIAS framework because targeted attacks at scale are a distinct possibility.

As we move to a world of ecosystems, products, devices and sensors and they increasingly become the target of sophisticated cyberattacks, regulators are placing heightened scrutiny on how organizations embed security across the product lifecycle.

Applying the CIAS framework in a hyperconnected world

CISOs should consider smart device–related risks across four main components spanning the lifecycle, each with specific DevSecOps-related priorities: product development, from design implementation to release; managing the expanding supply chain; maintenance and ongoing software updates; and the end user, whether it's another business or an individual consumer. These four areas help CISOs determine how to organize a security plan and gain confidence that the product is as secure as possible. It has become essential that CISOs have a line of sight in all areas of the business.

Software embedded in smart devices has the added complexity of not being easily updated, which is attributable to various factors, such as connectivity and the inability to patch while in use. It depends on the criticality of the device. This poses an additional challenge to builders: having to embed early assurance mechanisms, as well as having a well-organized software bill of materials, which enables companies to detect, and eventually recall, devices in the event critical vulnerabilities are discovered once devices are in use.

Cybersecurity has become a market differentiator. Perhaps it sounds obvious, but it's important for current and prospective customers, and the broad marketplace, to know that the organization's cybersecurity program and device controls, in particular, are ever-evolving, never static, and managed with device lifecycles in mind. Expect regulators worldwide to take a growing interest in the security of these systems and the minimum standards required.

Industrial manufacturing considerations

What are the implications for security and privacy teams as manufacturers shift toward a smart, hyperconnected product mindset?

Industrial manufacturing is uniquely positioned in the market as having more options than many other industries due to the lagging nature of technological upgrades at plants. While other industries may have made iterative technological upgrades over the past 10 to 15 years, many of the operations technology (OT) devices have generally remained the same. Many factories still have mostly serially connected relays and terminals, while IP connection is just now starting to become standardized.

The industry has more options because it can decide the best uses for hyperconnectivity versus simply iterating on the current architecture. Regardless of the technological architecture decision, it is imperative that the security strategy appropriately scales in a parallel manner. Cyber controls need to be established, balancing technical capability of these OT assets while still providing the risk reduction that aligns with the company's risk appetite. For example, while 14- to 16-character passwords are quickly being normalized in the IT world, many OT devices have a 4- to 8-character maximum.

Additionally, as more devices become 'smart,' asset inventories are going to significantly increase in size. Some organizations are seeing a 3x to 6x jump in IT asset inventory as more devices join company networks and can have some security controls applied. As such, it is imperative that security, IT asset management, and operations are in lockstep from the beginning of an asset's life through decommissioning to prevent company devices from going rogue to the point they are unrecognizable by the security team.

KPMG © 2023 Copyright owned by one or more of the KPMG International entities. KPMG International entities provide no services to clients. All rights reserved. USCS001113-1A

Cyber strategies for 2023

What actions can CISOs and the broader business lines take in the year ahead to help ensure security is the organization's golden thread? Following is a short list of tangible steps CISOs should consider as they seek to accelerate recovery times; reduce the impact of incidents on employees, customers, and partners; and aim to ensure their security plans enable—rather than expose—the business.

People

- Prioritize a robust cybersecurity culture that is interesting, engaging and, where appropriate, fun to inspire employees to do the right thing and function as human firewalls.
- Build a security team with the skills mix needed to manage a perimeterless organization, including cloud and third-party dependencies.
- Communicate broadly and clearly. Ask leaders in other organizational functions about their pain points and how automated processes might help.
- Take a multidisciplinary, cross-culture approach. Establish a security ecosystem comprising internal business line specialists, security professionals, data scientists, privacy-oriented attorneys and external policy and industry professionals.
- Embed yourself in the organization and act as a peer, a sounding board and an advisor.

Process

- Build consistent approaches to cyber risk management with an understanding of threat scenarios and attack paths to help inform attack surface reduction and prioritize control improvements.
- Focus on fit-for-purpose security processes that feature consistent user experiences.
- Establish strict identity controls and work to achieve a mature state of identity governance and services.
- Segment legacy environments to limit the attack surface and help contain any breaches.
- Have a proactive recovery plan focusing on the organization's most critical workflows with a communication structure and stress test it often.
- Consider subscription support models with predictable costs, any-shore delivery, and strategic results.

Data and technology

- Embrace the inevitable automation of the security function—trust the latest tools, from robotic processes and security orchestration, automation and response (SOAR) to extended detection and response (XDR) systems.
- Work with cloud providers to help ensure broad visibility into how products and services are configured to avoid inadvertent vulnerabilities.
- Consider cybersecurity and privacy issues up front when exploring emerging technologies, including the evolving risks associated with adopting AI systems.
- Assign responsibilities and establish accountability around how critical data is processed and managed and how it supports critical business processes.
- In the interest of speed, scalability, and trust, a transition to identity as a service in the cloud needs to happen sooner than later.

Regulatory

- Be aware of changing regulatory trends and drivers and what they could mean for the company's future technology strategy, product development and operations.
- Consider the regulatory impacts vis-à-vis AI and automation—establish a clear concept of what the business can and can't do in these arenas and be alive to public concerns and changing expectations.
- Explore automating compliance monitoring and reporting and task a team member to serve as a regulatory monitor to stay on top of privacy and security regulatory trends.
- Align security and privacy compliance strategy with the company's broad business strategy to help ensure stakeholders from across the organization are on the same page.
- Look beyond the letter of the regulation—and be prepared to ask yourself more fundamental questions about digital trust and how you make that central to your strategic thinking.

KPMG

© 2023 Copyright owned by one or more of the KPMG International entities. KPMG International entities provide no services to clients. All rights reserved. USCS001113-1A

How KPMG professionals can help

KPMG firms have experience across the continuum—from the boardroom to the data center. In addition to assessing your cybersecurity and aligning it to your business priorities, KPMG professionals can help you develop advanced digital solutions, implement them, monitor ongoing risks and help you respond effectively to cyber incidents. No matter where you are in your cybersecurity journey, KPMG firms can help you reach your destination.

As a leading provider and implementer of cybersecurity, KPMG professionals know how to apply leading security practices and build new ones that are fit for purpose. Their progressive approach to cybersecurity also includes how they can deliver services, so no matter how you engage, you can expect to work with people who understand your business and your technology.

Whether you're entering a new market, launching products and services or interacting with customers in a new way, KPMG professionals can help you anticipate tomorrow, move faster and get an edge with secure and trusted technology. That's because they can bring an uncommon combination of technological experience, deep business knowledge and creative professionals passionate about helping you protect and build stakeholder trust.

KPMG. The Difference Makers

© 2023 Copyright owned by one or more of the KPMG International entities. KPMG International entities provide no services to clients. All rights reserved. USCS001113-1A

Contact us

Michael Gomez
Principal and Industrial Manufacturing Leader
Cyber Security Services
KPMG in the US
michaelgomez@kpmg.com

Claudia Saran
National Sector Leader and Advisory Industry Leader
Industrial Manufacturing
KPMG in the US
csaran@kpmg.com

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.

kpmg.com/socialmedia

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 upon such information without appropriate professional advice after a thorough examination of the particular situation.

KPMG refers to the global organization or to one or more of the member firms of KPMG International Limited ("KPMG International"), each of which is a separate legal entity. KPMG International Limited is a private English company limited by guarantee and does not provide services to clients. For more detail about our structure, please visit kpmg.com/governance.

© 2023 Copyright owned by one or more of the KPMG International entities. KPMG International entities provide no services to clients. All rights reserved.

The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organization. USCS001113-1A