



IT-OT Cyber Security Convergence Framework

Bridging IT and OT:
Enhancing Security and Efficiency through Convergence

March 2025



A worker in a blue uniform and yellow hard hat is operating a robotic arm in a factory setting. The worker is holding a white control panel. The background is a blurred industrial environment with various machinery and equipment. The overall scene is lit with a blue and purple hue.

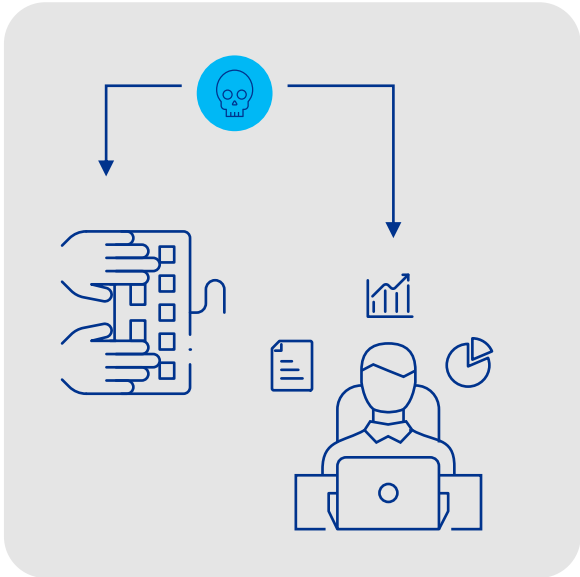
01

Introduction - topic derivation

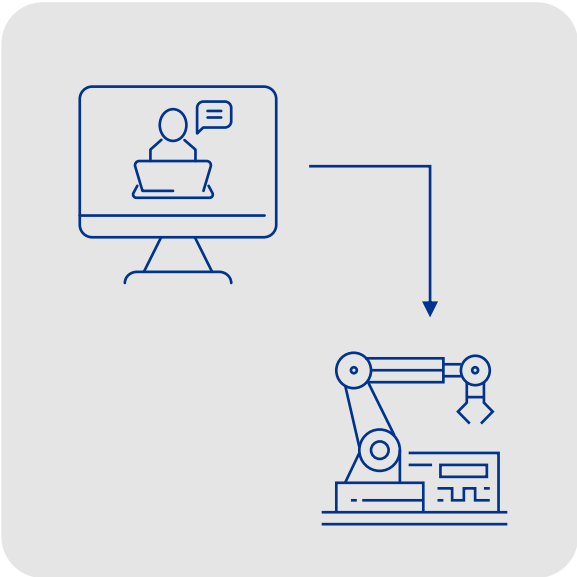
IT/OT – Yesterday

Yesterday

IT



OT

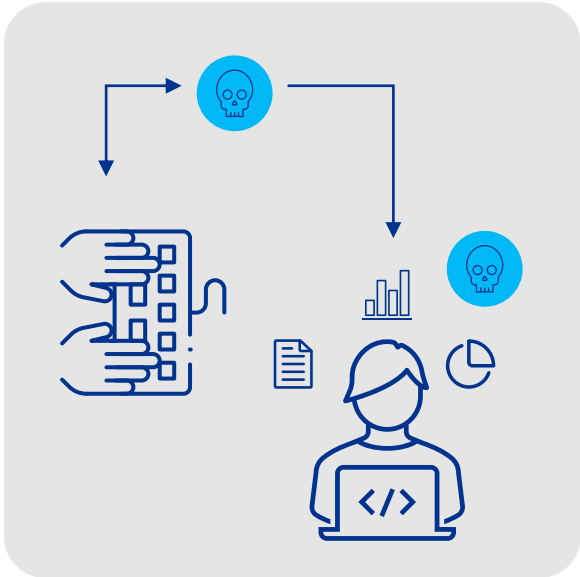


“ Due to the complete separation of production areas, the attack surface was significantly smaller in the past. ”

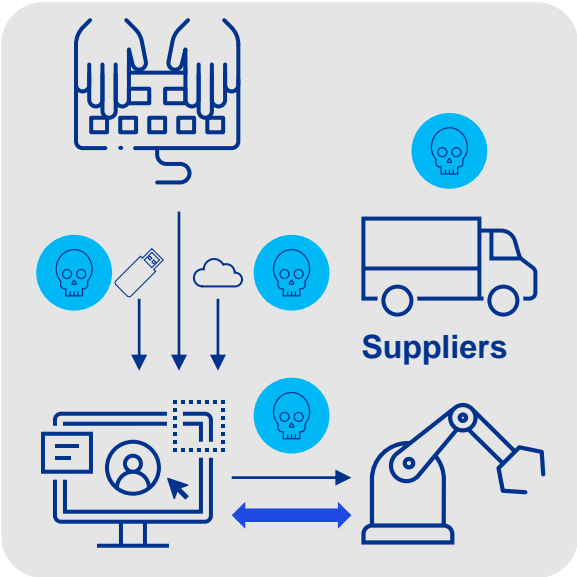
IT/OT – Today

Today

IT



OT

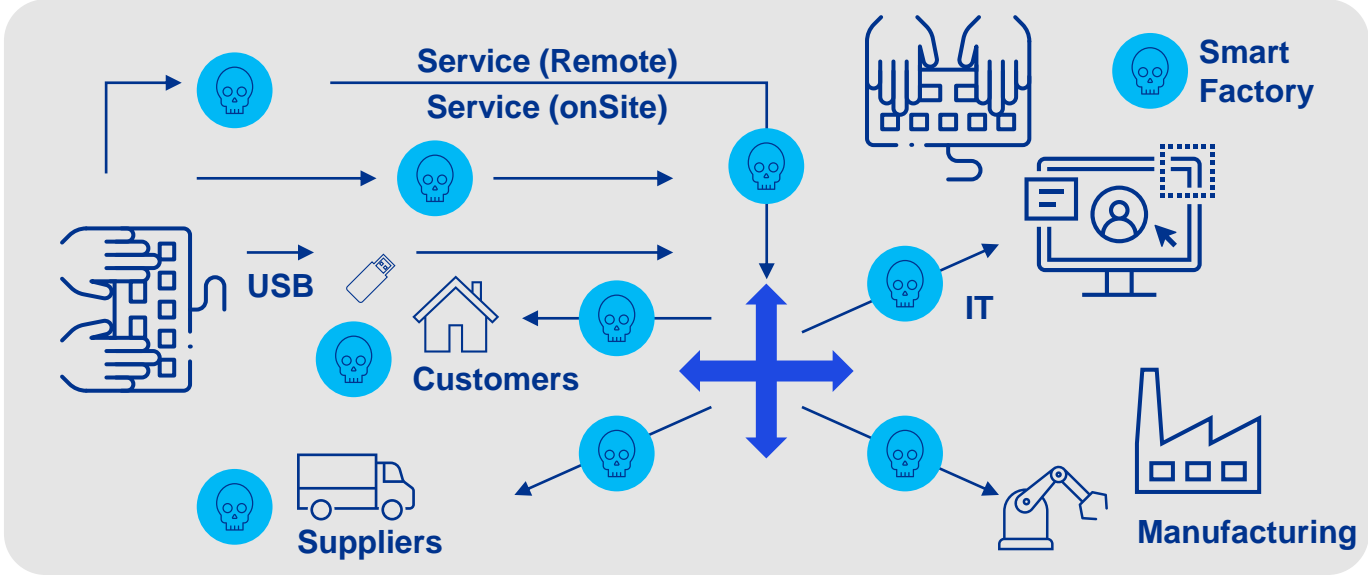


“ ... this leads to an enormous increase in the attack surface – cyber attacks and their effects will increase enormously. ”

IT/OT – Today

Today

IT/OT



“ ... the merging of IT, OT, suppliers and customers leads to an enormous increase in the attack surface. ”

Key messages



Importance of KPMG IT/OT Convergence framework

- Provides guidance and best practices for measuring and evaluating the level of convergence of OT and IT environments with a focus on cybersecurity to break through the silos.
- Ensures that OT and IT environment are aligned to operate seamlessly and securely.
- Emphasizes the need for a well-defined convergence strategy to reduce cyber-attack risks and ensure business continuity.



Reasons to embrace KPMG's Convergence strategy

- Addresses the growing demand for OT and IT integration and promotes technology-driven business strategies, including the integration of emerging technologies, to stay competitive in a rapidly evolving landscape.
- Helps organizations leverage their data effectively to gain a competitive advantage and maximize value.
- Supports the integration of technology and processes to improve organizational efficiency and effectiveness, tested and evaluated based on industry experience.



Benefits of IT/OT Convergence framework

- Provides a controls catalogue for OT systems to ensure robust cybersecurity measures.
- Enhances operational efficiency and business continuity through the seamless integration of OT and IT environment, incorporating resilience to ensure robust and continuous operations.
- Full visibility of processes, people, Technology, and governance models through the convergence of IT and OT environment.



Broader integration of IT and OT

- Facilitates the proliferation of devices, data, and applications within the organization.
- Provides a roadmap for organizations to achieve more operational efficiency through the convergence of OT and IT environments, including governance and guidelines on how people will operate it.

Key challenges for IT/OT convergence



The convergence of IT and OT is becoming a business imperative due to its potential to unlock significant productivity gains and cost reductions. However, achieving successful IT/OT convergence presents several challenges:



Organizational

Challenge

In manufacturing, OT systems, including machines, devices, and control mechanisms, often operate in isolation, using niche communication protocols. As well as limited resources for Cybersecurity and the absence of a central cybersecurity project management.

Convergence advantage

Achieving true convergence requires breaking down these silos to establish a common taxonomy and information architecture, facilitating the seamless flow of data and knowledge. Exceeded through a centralized Cybersecurity Project Management.



Data incompatibilities

Challenge

Data incompatibilities and organizational silos create blind spots that hinder the IT/OT convergence process (e.g. inconsistent data formats).

Convergence advantage

Overcoming these challenges requires both formal and informal communication among system owners to ensure accurate data extraction and transformation.



Cyber Security

Challenge

OT systems were not initially designed for networked environments, making them vulnerable to modern cyber threats. The integration of IP-connected devices and cloud platforms introduces new vulnerabilities.

Convergence advantage

A multi-pronged cybersecurity approach is necessary to continuously manage and mitigate these risks.



Legacy systems

Challenge

Industrial plants often rely on legacy systems that are customized or unsupported. Challenges related to data quality and digitalization persist.

Convergence advantage

To harness the benefits of IT/OT convergence, strategies such as using wrappers or containerization can help integrate these systems without disrupting operations.



IT and OT skill sets

Challenge

The convergence of IT and OT is reshaping the skills required in manufacturing. Management and IT departments aim for process and manufacturing engineers to gain IT proficiency, while OT departments face the retirement of experienced veterans.

Convergence advantage

Successful convergence relies on developing multi-disciplinary engineers with expertise in both IT and OT domains.

More challenges with further risks for large organizations



Large organizations adopting IT/OT convergence face increased challenges and risks, yet KPMG's IT/OT Convergence Framework helps navigate these complexities.

Procedural variation:

Security requirements inevitably interpreted and actioned differently at individual plant level causing inconsistencies.

OT Role career obscurity:

Compared with IT, the prioritization and support of OT cybersecurity personnel for career aspiration is insufficient leading to disengagement and demotivation.

Vendor fragmentation:

Mix of critical vendors with different versions, and different instances across different sites.

Lifecycle range:

Mix of state-of-the-art and legacy systems and applications across different architectures supported by the same people.

Geographical distribution:

Impossible for an OT engineer(s) to cover an incident in a related Plant due to sheer distance and journey time.

Heterogeneity of OT systems:

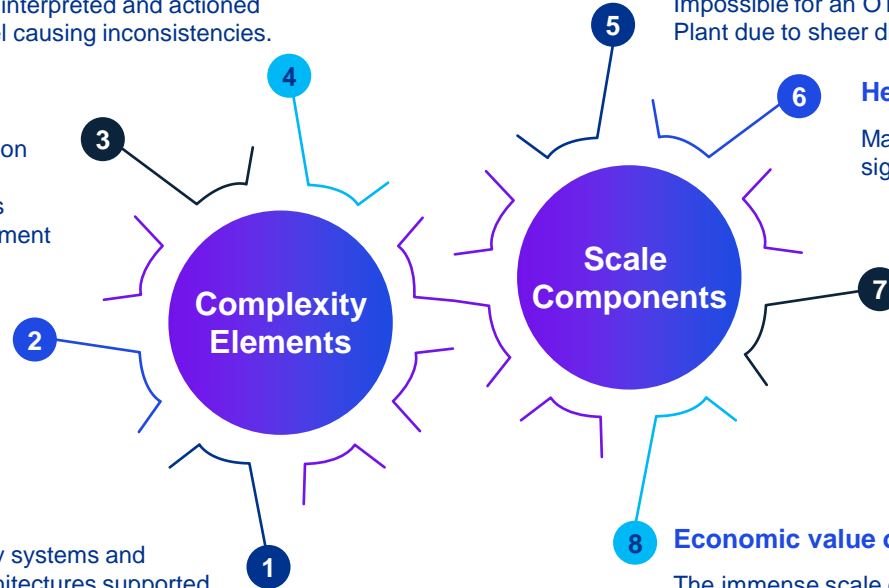
Many unique systems per site creates significant loads on OT engineer(s).

Scope of cybersecurity capabilities:

The range of skills demanded of many distinct capabilities is too great for the inherent skills range of just one OT engineer.

Economic value of production:

The immense scale of production operations creates pressure on OT systems to be kept running at all cost.



Risks

1 Protection gaps:

Sheer volume of sites, people and systems makes management of role based access controls (RBAC) difficult, leading to access compliance violations.

2 Response times:

Geographic range, OT engineer lack of incident response skills and plant organizational structure leads to major business continuity risk.

3 Detection limitations:

Advanced anomaly detection solution, that handles massive data sets in real-time to evaluate the risk of fraudulent actions does not exist and nor do the required skills to operate such a system effectively.

4 People attrition:








Loss of knowledge, and risk to protection continuity as a result of resource gaps caused by employee turnover.

Cybersecurity key stakeholders and influencers



A variety of stakeholders within the organization are relevant for the implementation of the framework. These represent a subset of those who are relevant, depending on the size of the company.

Overseeing CTO/CIO

C*	 <p>CISO</p> <ul style="list-style-type: none"> • Develop and lead the organization's overall information security strategy. • Oversee risk management processes and ensure compliance with security regulations and standards. • Lead the response to security incidents and manage crisis situations effectively. 	C*	
OT	 <p>OT Architect</p> <ul style="list-style-type: none"> • Develop and implement OT system architectures. • Establish security protocols and ensure regulatory compliance. • Work with cross-functional teams to integrate OT and IT systems. 	 <p>OT Policy Governance Manager</p> <ul style="list-style-type: none"> • Develop and implement policies and procedures for OT governance. • Ensure compliance with regulatory requirements and manage risks associated with OT systems. • Coordinate with stakeholders to align OT policies with organizational goals and standards. 	OT
	 <p>OT Engineer</p> <ul style="list-style-type: none"> • Oversee the installation, configuration, and upkeep of OT systems. • Monitor system performance and implement improvements. • Ensure OT systems are secure and compliant with industry standards. 	 <p>OT Security Officer</p> <ul style="list-style-type: none"> • Develop and implement security strategies for OT systems. • Monitor for security threats and respond to incidents. • Ensure OT systems comply with security regulations and conduct regular audits. 	
IT	 <p>IT Architect</p> <ul style="list-style-type: none"> • Develop and implement IT system architectures. • Establish security measures and ensure compliance with industry standards. • Coordinate with various teams to integrate new technologies and systems. 	 <p>IT Policy Governance Manager</p> <ul style="list-style-type: none"> • Develop and implement IT policies and governance frameworks. • Ensure compliance with regulatory requirements and manage IT-related risks. • Coordinate with stakeholders to align IT policies with organizational objectives and standards. 	IT
	 <p>IT Engineer</p> <ul style="list-style-type: none"> • Install, configure, and maintain IT systems and infrastructure. • Monitor system performance and implement optimizations. • Ensure IT systems are secure and compliant with industry standards. 	 <p>Information Security Officer</p> <ul style="list-style-type: none"> • Develop and implement information security strategies and policies. • Monitor for security threats and respond to security incidents. • Ensure compliance with security regulations and conduct regular security audits. 	

Uniting engineering and cybersecurity for enhanced resilience



Breaking down silos between engineering and cybersecurity is crucial for developing mutual understanding and effective collaboration. By fostering relationships and understanding each other's expertise, both can tailor defensive controls and design more resilient systems, ultimately enhancing overall security and operational efficiency.



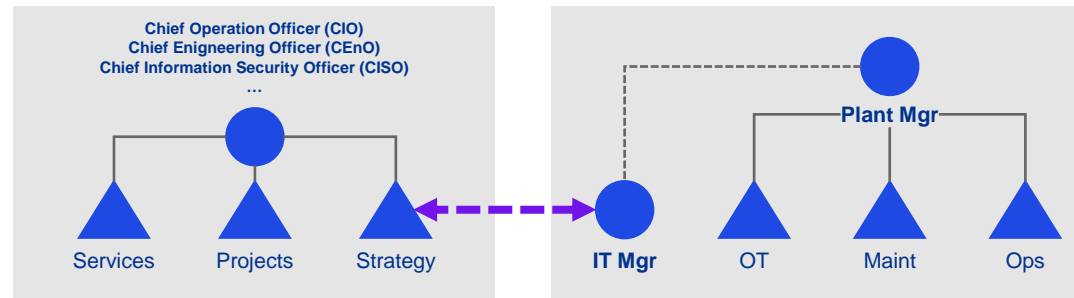
IT-OT Silo experience:

- IT Specialists believe that the OT team isn't knowledgeable about IT best practices.
- The OT team believes that the IT team doesn't know anything about practical engineering and operations.
- Often leads to miscommunication and lowered morale when needing to work in conjunction with each other.
- Will also lead to a break in the ability to work together towards a common goal.

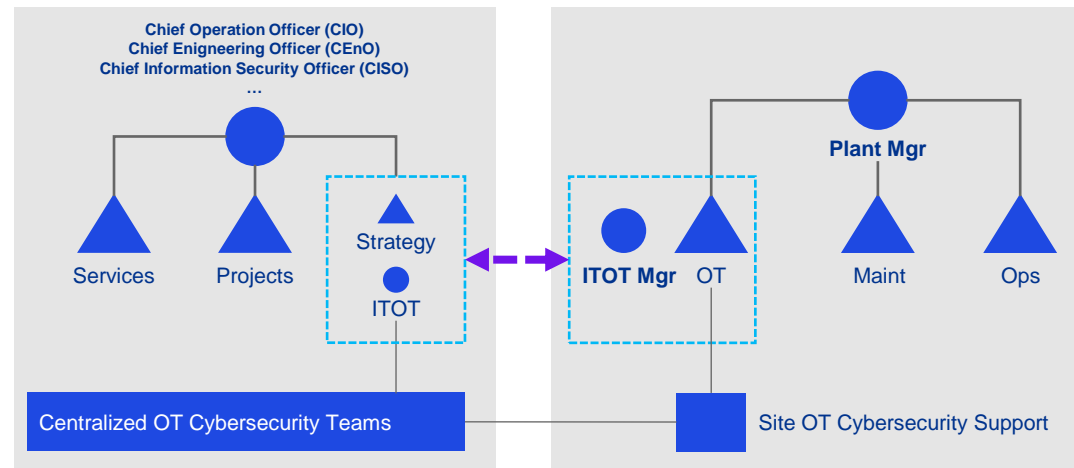


Industry practice:

- Pursuing a combined and centralized IT-OT organization model.
- Establish centralized OT cybersecurity teams to serve as the primary point of contact for individual sites and the IT department.
- Deploy site-specific cybersecurity support teams to address location-specific cybersecurity needs and provide localized support.
- Enable off-site OT experts to reduce the operational burden on plant managers and improve efficiency.



Illustrates the typical communication flow in IT/OT-related companies, where the IT manager communicates through the plant manager.



Demonstrates the recommended approach, where IT and OT teams communicate directly for more effective collaboration.

Current security at scale is a challenge

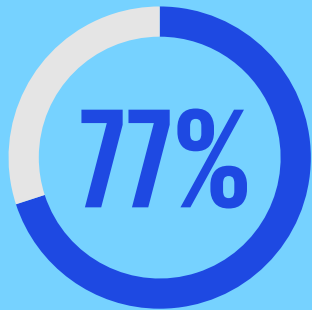
95%



Of organizations indicated that OT security is part of the CISO's responsibilities.

Source

Document: "2023-State-of-Operational-Technology-and-Cybersecurity-Report-DE-WP"

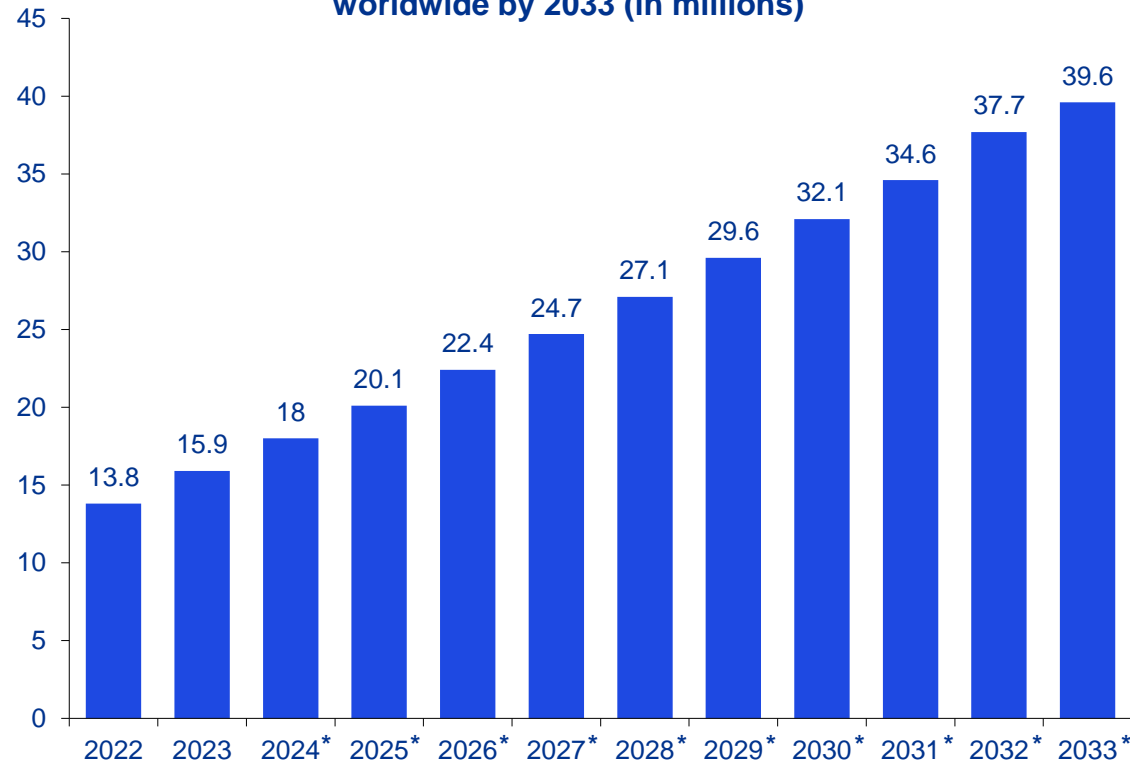


Of organizations view ransomware as a larger concern than other threats to the OT environment.

Source

Document: "2024-control-system-cybersecurity-annual-report"

Number of Internet of Things (IoT) connected devices worldwide by 2033 (in millions)



Note: (*) YEAR = forecast

Source

Document: "statistic_id1420315_anzahl-der-mit-dem-internet-der-dinge-verbundenen-geraete-weltweit-bis-2033"

13%



Increase in the number of connected IoT devices from 2023 to 2024.

Source

Document: "INSIGHTS-RELEASE-Number-of-connected-IoT-devices-vf"

80%



Increase in the monitoring of network activity of the control system from 2023 to 2024

Source

Document: "2024-control-system-cybersecurity-annual-report"

02

Introduction - IT/OT
Convergence



Why converge IT/OT?


IT and OT operate in separate silos with minimal interaction.

Limited collaboration leads to inefficiencies and missed opportunities for optimization.

Integration efforts are sporadic and uncoordinated.

Security protocols are not uniformly applied across IT and OT domains.

Difficulty in identifying and mitigating risks due to fragmented data and processes.



Before IT-OT Convergence




IT/OT Cyber Convergence Framework measures the cyber capabilities of an organization.



IT-OT Convergence Framework assesses the integration and alignment of IT and OT systems.



Enhance the convergence of OT and IT functions.



After IT-OT Convergence

IT and OT operate seamlessly together with integrated processes and frequent collaboration, with cyber resilience as one key element.

Enhanced collaboration drives efficiency and capitalizes on opportunities for optimization.

Integration efforts are strategic and well-coordinated.

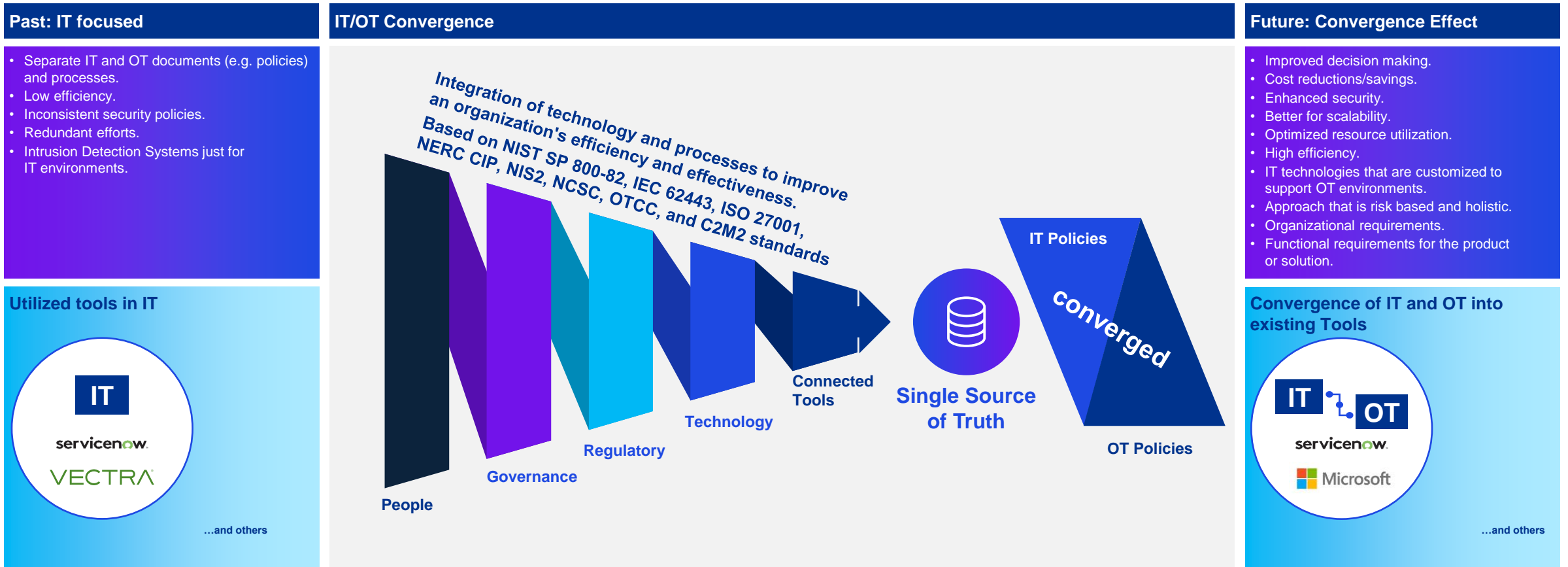
Security protocols are consistently and uniformly applied across IT and OT domains.

Improved risk identification and mitigation through integrated data and streamlined processes.

Migration from IT-based to IT/OT-based approach



Organizations should review their current reference security architecture to develop a new one that is adaptable to emerging technologies such as 5G, robotics, AI machine learning, the Internet of Things, and the Industrial Internet of Things. This will maximize the value of data and enable IT/OT convergence. KPMG's IT/OT Convergence Framework will guide you in maximizing value.

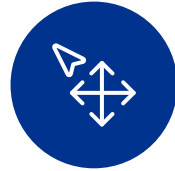


Key Characteristics of the IT-OT Convergence Framework



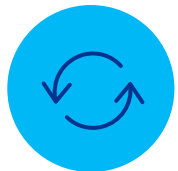
Guidance and Best Practices

Provides detailed guidelines and best practices for measuring and evaluating the level of convergence of IT and OT.



Integration for Efficiency

Promotes the integration of technology and processes to enhance organizational efficiency and effectiveness, ensuring seamless and secure operations, and driving value realization.



Risk Reduction and Business Continuity

Emphasises the importance of a well-defined convergence strategy to reduce the risk of cyber-attacks and ensure business continuity.



Comprehensive Framework

Offers a structured approach for evaluating, measuring, and enhancing IT-OT convergence to guide organizations in leveraging their data and achieving operational efficiency.

If this operating model is the destination for future IT, the implications for cybersecurity are significant.

- > Is security truly integrated into cross-functional teams and flexible in its approach?
- > Can the IT-OT Convergence Framework protect investments and improve operations?
- > Do your customers or stakeholders feel intrinsically secure using your products?
- > Does the security team have the right skills today and a development plan for the future?

Convergence rating levels



The convergence rating levels provide an indication of the current degree of convergence between an organization's IT and OT domains. The standard used within the KPMG IT-OT Convergence Framework differentiates between five convergence rating levels: Minimal Convergence, Partial Convergence, Moderate Convergence, Significant Convergence, and Complete Convergence.

01

Complete Convergence

IT and OT have fully integrated, seamless interaction with multidisciplinary teams using advanced technologies like IoT, AI, and Machine Learning. This enables real-time responses to business changes, threats, and opportunities, leveraging adaptive, resilient, and secure processes.

02

Significant Convergence

IT and OT are highly integrated, with formal collaboration programs and multidisciplinary teams. They share objectives and performance metrics, including security and risk management, using standards-based architectures and technologies for cohesive operation.

03

Moderate Convergence

IT and OT have formalized collaboration with standardized processes and a common framework. They operate with shared objectives, goals, and metrics, and have identified areas for integration. A comprehensive roadmap for IT-OT convergence is still in progress.

04

Partial Convergence

IT and OT collaboration initiatives are evident but limited. There is awareness of the need for integration, and some initial steps have been taken to share information and align processes. However, there are no formalized programs, and integration remains inconsistent.

05

Minimal Convergence(*)

IT and OT operate as separate domains with no collaboration, standardization, or coordination between the two. No integration of IT and OT processes, technologies, or systems exists.

(*) Note: A low convergence rating doesn't necessarily indicate low maturity. Sometimes, keeping IT and OT functions separate is essential for risk management. Recommendations should be based on the assessed convergence rating and industry benchmarks or target ratings for that capability.

03

Our Approach



Domains of Convergence Framework



The IT/OT Convergence Framework is a KPMG proprietary methodology based on leading cyber security measures, such as NIST SP 800-82, IEC 62443, ISO 27001, NERC CIP, NIS2, OTCC, and C2M2 standards. This, combined with our global insight into leading practices regarding cybersecurity, especially in the IT/OT area, informs the framework's nine key topics/security domains. These domains are leveraged to provide a comprehensive measure of the level of convergence of the IT and OT environments in alignment with KPMG CMA domains:

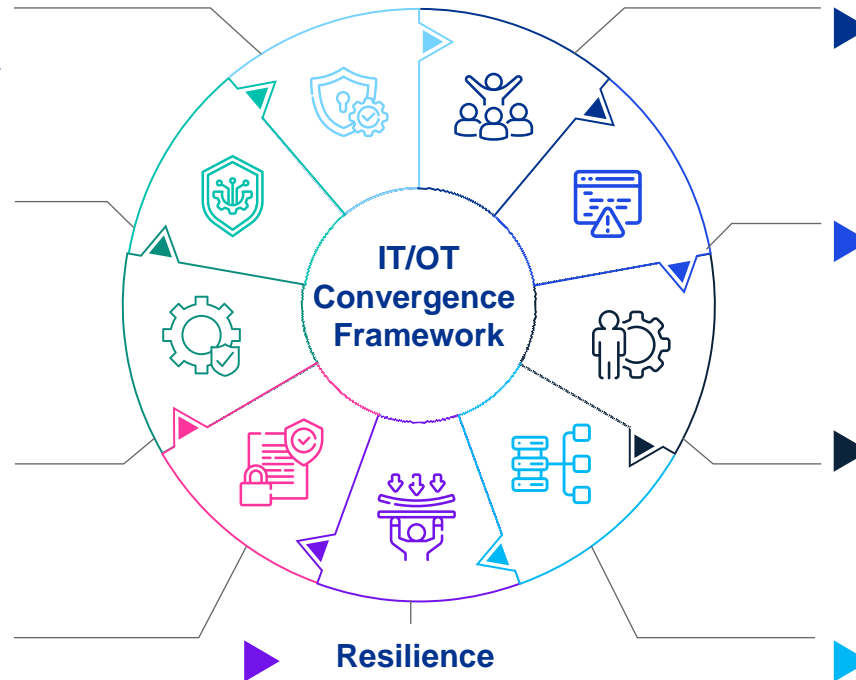
- Security Operations**

Security operations are in place to identify and proactively prevent the compromise of sensitive information and computer systems.
- Security Architecture**

Information systems are designed in alignment with the defined security objectives, to address potential risks to the cyber environment.
- Technical Security**

Technical security solutions are implemented to address identified cyber risks and protect against the theft of sensitive data and/or information.
- Compliance**

Ability to demonstrate compliance against relevant regulatory and international certification standards.



- Leadership & Governance**

Management demonstrate the ability to take ownership and effectively manage risk. Governance mechanisms are in place to demonstrate due diligence.
- Information Risk Management**

An approach to thoroughly and effectively assess, manage and monitor risks associated to sensitive/confidential information exchanged across an organization and its third parties.
- Human Factors**

A security culture exists that empowers and helps ensures the right people, skills, culture and knowledge to protect against cyber security threats.
- Third Parties**

Identify and manage the risk to information throughout the lifecycle of a supplier by defining information security requirements to protect against potential cyber risks.

Opportunities for improvement across the governance model



Opportunities for improvement across the governance model to better address the scale, complexity and risk factors.

Elevating Security

OT security must be prioritized with the same cultural importance and intensity as operational safety and engineering priorities.

Controlled Convergence

Ensure that the path to convergence is systematically managed rather than left to organic evolution.

Resilience Enhancement

Team restructuring allows Plants and Central resources to more effectively cover and monitor the extensive geographical distribution and the broad range of cybersecurity functions.

Team Synergizing

Focus on enhancing collaboration, communication, and connectivity between teams, technologies, and knowledge management.

Capability

Capabilities such as advanced anomaly detection and rapid patch management are identified as weaknesses in the current model.

Scaling Acceleration

IT provides robust and transferable capabilities in areas that are currently underdeveloped in OT but can be quickly adopted. These capabilities, such as offsite backup, may require some modifications to be fit for purpose in OT.

IT-OT Convergence framework approach

01

Planning

- Define clear objectives and goals for the IT-OT convergence initiative, and clearly outline the scope of the project, including the domains and areas to be analyzed, while considering potential risks and looking forward in regard of emerging technologies.
- Identify and engage key stakeholders who will be involved in the assessment of the level of convergence, ensuring their active participation throughout the process to accelerate the engagement efforts.

02

Information Gathering and Measuring Convergence Level

- Collect relevant data from various sources, including the KPMG requirements list for each domain, to ensure comprehensive and insightful information is available.
- Conduct interviews with key stakeholders to gather insights and perspectives on the current level of IT/OT convergence for each domain.

03

Analysis

- Evaluate the current level of convergence for each domain and the overall IT-OT convergence and identify the root causes of inefficiencies and ineffective areas within the IT/OT environment.
- Leverage industry best practices, standards, and KPMG's extensive industrial experience to benchmark the current state, identify areas for improvement, and formulate actionable recommendations for enhancing IT-OT convergence and addressing identified observations.

04

Report

- Provide a high-level overview of key findings, conclusions, and recommendations. Present detailed observations from data collection and analysis. Define the future governance framework and Target Operating Model (TOM) to support IT-OT convergence.
- Outline specific recommendations for improving IT-OT convergence, including technology and process integration. Develop an implementation plan with timelines, resource requirements, and key milestones, incorporating the future governance framework and TOM for long-term success.

What does the IT-OT Convergence Framework deliver?



The IT-OT Convergence Framework provides a comprehensive understanding of the integration and alignment of IT and OT environment, identifying control weaknesses and areas for improvement. This enables organizations to prioritize remediation efforts and enhance both corporate and operational compliance.

Identify

- Identify stakeholders for analyzing the domains on current convergence level.
- Identify inefficient and ineffective areas within the IT/OT environment.

Assess

- Conduct interviews with key stakeholders to gather valuable insights and perspectives.
- Perform a comprehensive analysis of the documents requested for the specific domains to extract pertinent information.
- Document observations and findings derived from both the document analysis and stakeholder interviews in a structured manner.

Evaluate

- Assess the current level of convergence for each domain as well as the overall convergence of IT and OT.
- Provide recommendations for integrating technology and processes to enhance organizational efficiency and effectiveness.

Prioritize

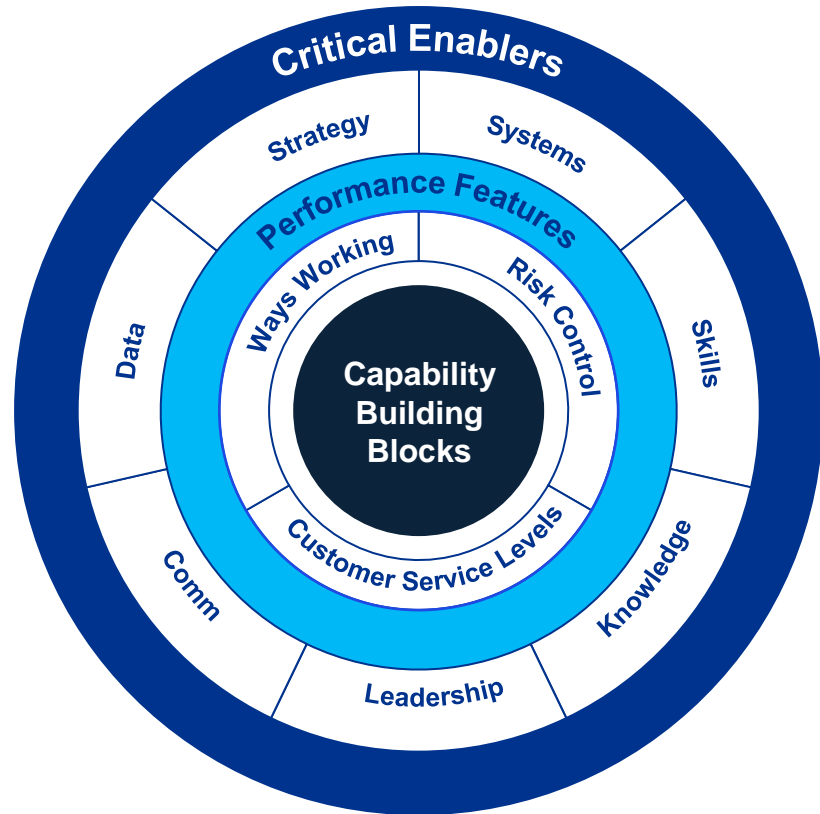
- Key areas for improvement initiatives.
- Evaluate and rank short-term opportunities that can provide rapid benefits and serve as a foundation for more extensive, future projects.

Align

- Develop a comprehensive report detailing the current level of IT/OT convergence for each domain as well as the overall integration status.
- Define improvement initiatives based on the current convergence levels and aligned with industry best practices.
- Benchmark and evaluate technologies that are suitable for integration to enhance convergence.
- Definition of the future Governance and a Target Operating Model (TOM) to support sustained IT/OT convergence.

Compare against industry peers

Key features of transformed Governance Model



Governance Model Improvement Areas



Key Features

- 1 **Address the unsustainable issues in OT engineer roles** by restructuring work, increasing numbers in role and provide career paths under the guidance of a dedicated talent management oriented by the CISO.
- 2 **Leverage the underlying strengths and assets of IT** to accelerate uplift in OT service provision e.g. OT Shared Services through a dedicated department and team for OT.
- 3 **Strengthen ability of CISO** to connect strategy to risk resilience to OT Cyber standards and capability through a dedicated ICS/OT department that takes care of the ICS/OT scope.
- 4 **Broaden the responsibilities** to leverage their collective knowledge of engineering architectures and production processes to strengthen vendor management controls and enforce necessary architecture changes.
- 5 **Increase strategic, advisory and operational responsiveness** through the creation of OT Business Partners, as an extension of existing OT engineers, supporting plant's objectives and a Rapid Response team on standby to support incident response.
- 6 **Promote a strengthened hub** to cope with centralized co-ordination and creation of a risk intelligence umbrella, supported by an enhanced master data management capability to drive protection and pre-emption activities.

04

Our capabilities –
Why KPMG?



What can KPMG firms offer across the framework?



How KPMG can help throughout the Framework:



Design the KPIs/KRIs
(KPI Drivers)



Help out Convergence via
Programs (e.g. in ME: Programm
Management Consultancy (PMC))



Designing Processes and Policies



Implementation of Tools

Quick wins & service re-design
Re-imagining & Re-structuring Capabilities

- Role allocation.
- Service definitions.
- KPI development.
- Governance processes.
- Service management philosophy.
- Accountability framework.
- Service crosswalks.
- Enable the IT/OT secure convergence roadmaps.

Skills, talent, governance & measurement
Resourcing & Rigour

- Advanced OT Training set up.
- Hiring and mobility.
- Knowledge driven communities of practice.
- Data model set up and signals management.
- Skills framework adoption.
- Communication channel improvement.
- Cross-team service visioning & engagement.
- Career development.
- Strategic workforce planning.

Continuous improvement
Realization & Resilience

- Service management frameworks.
- Service performance monitoring linked to resilience.
- Future innovation scouting.
- Enterprise risk alignment.
- KPI threat and tolerance setting.
- Predictive scenarios based on threat gaming.
- Maturity re-assessment.
- Benefit realization model.

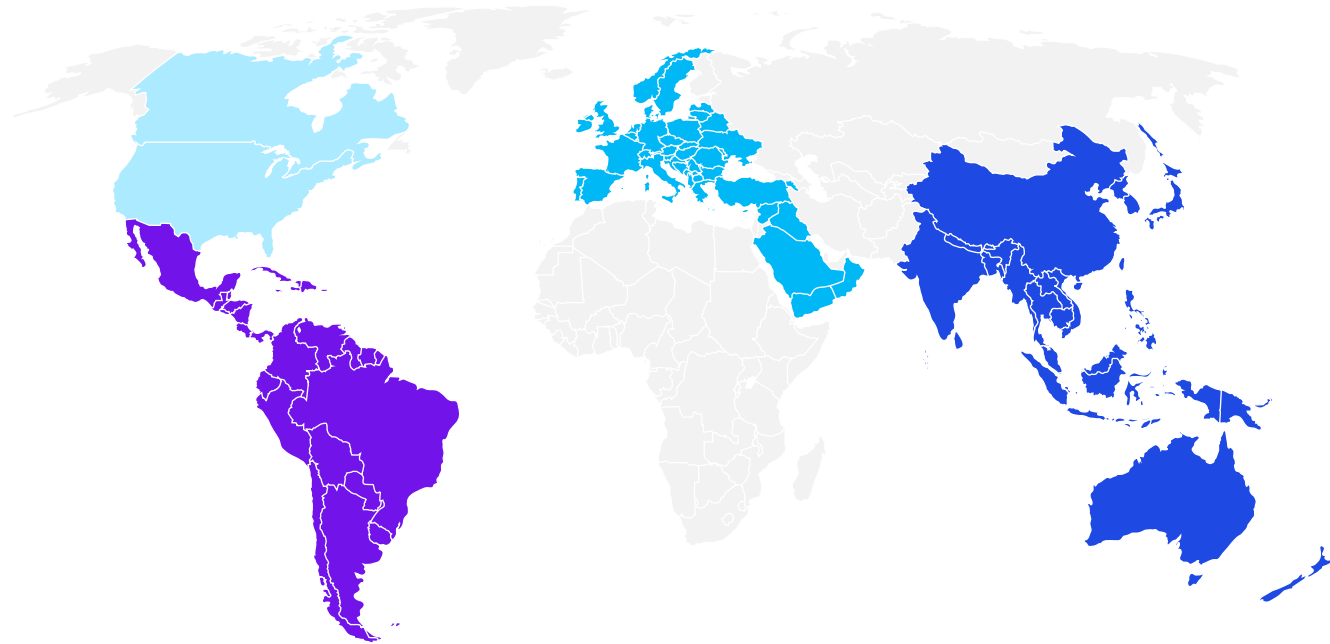
Goal



Continuous Self-Optimizing Cyberrisk Control Capability

Why KPMG firms?

We are a global firm with more than **200+ specialized OT cybersecurity professionals around the world**, combining professionals with complementary specialties both in technical and industry specific topics. **Our Global IOT Nexus Community brings together our most experienced cyber leaders**, who operate as a network, cooperating and combining capabilities as our clients require.



+80

ASPAC

+60

EMA

+40

US & CANADA

+20

LATAM

Our Global IOT Cybersecurity Nexus



Our Global IOT Cybersecurity Nexus reunites our global capabilities in IOT Cybersecurity around the globe, keeping an international community of practitioners along our network of member firms.

Through our Global Nexus we share experiences, develop capabilities, alliances, thought leadership and other assets that our professionals leverage globally in our services.



Contacts



Hossain Alshedoki

Global IOT Lead &
Head of Emerging Tech & OT Security
KPMG Middle East
halshedoki@kpmg.com



Walter Ariel Risi

Partner & Head of Consulting,
KPMG Argentina
wrisi@kpmg.com.ar



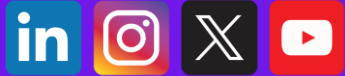
Ashish Ghai

Manager, Cyber Strategy & Governance,
KPMG Global Services
ashishghai1@kpmg.com



Samir Hajdari

Assistant Manager, Cyber Security & Resilience,
KPMG Germany
shajdari@kpmg.com



kpmg.com/uk

© 2025 Copyright owned by one or more of the KPMG International entities. KPMG International entities provide no services to clients. All rights reserved.

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 home.kpmg/governance.

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

Document Classification: KPMG Public

CREATE: CRT158593B | February 2025