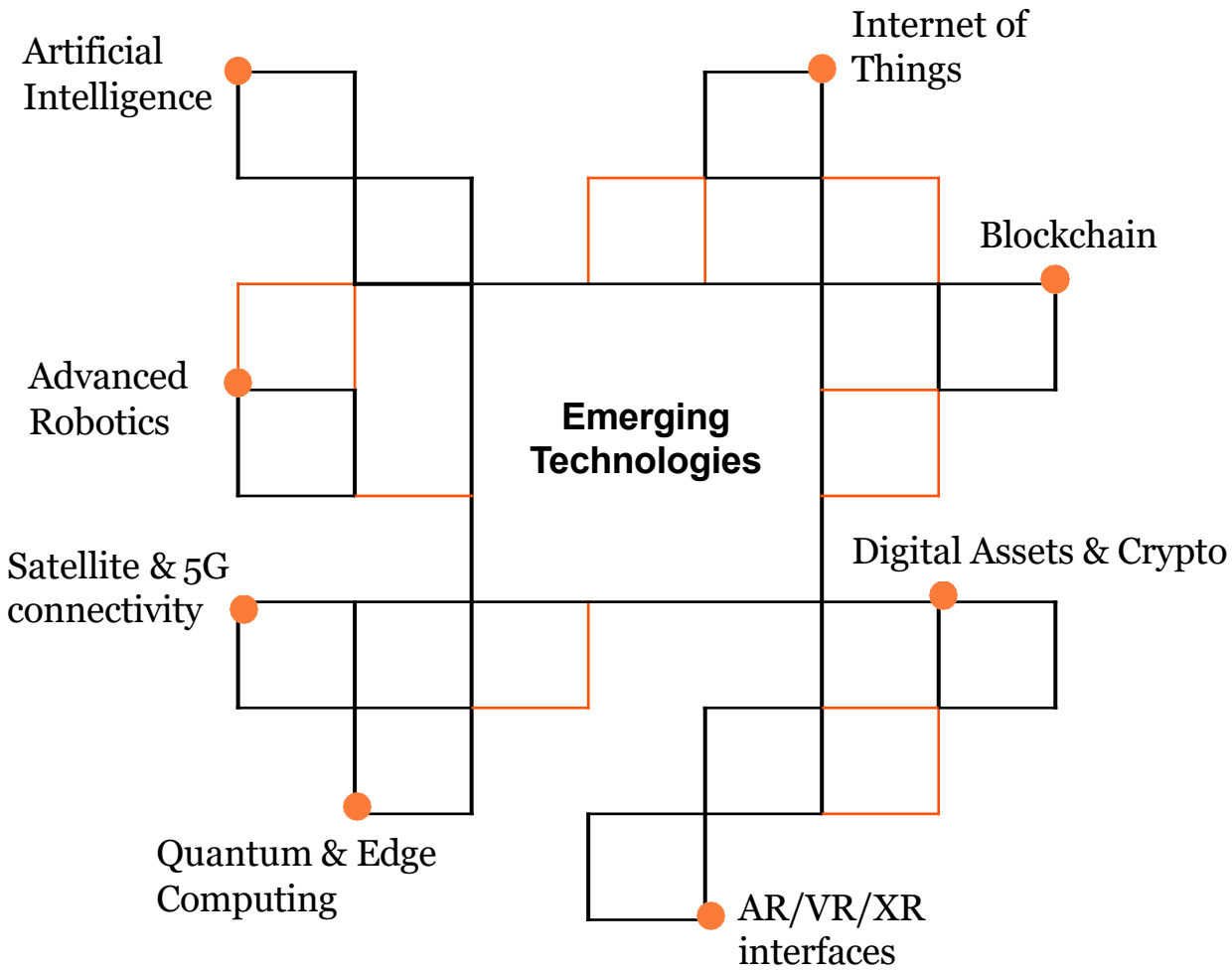
Cyber Emerging Technologies

Building Trust in Emerging Technologies

November 2025



Unlock the transformative power of **Emerging Technologies** with **PwC Cyber**. We partner with you to implement them securely, privately, and resiliently, fostering the **trust** that drives tangible business outcomes and sustainable growth.

Innovation that protects and empowers

Only 2%

have implemented cyber resilience actions across their organisation in all areas surveyed

< 50%

of CISOs are involved to a large extent in key business activities

13% point

gap in confidence between CISOs/CSOs and CEOs in their AI and resilience compliance

Innovation fuels growth but introduces new challenges that require careful navigation. With the attack surface continuing to expand through advances in AI, connected devices and cloud technologies and the regulatory environment in constant flux, achieving cyber resilience at an enterprise level is critical.

Yet despite widespread awareness of the challenges, significant gaps persist. To safeguard their organisations, executives should treat cybersecurity as a standing item on the business agenda, embedding it into every strategic decision and demanding C-suite collaboration.

PwC's **2025 Global Digital Trust Insights survey** revealed significant gaps companies must bridge.

Gaps In implementation of cyber resilience: Despite heightened concerns about cyber risk, only 2% of executives say their company has implemented cyber resilience actions across their organisation in all areas surveyed.

Gaps in preparedness: Organisations feel least prepared to address the cyber threats they find most concerning, such as cloud-related risks and third-party breaches.

Gaps in CISO involvement: Fewer than half of executives say their CISOs are involved to a large extent with strategic planning, board reporting and overseeing tech deployments.

Gaps in regulatory compliance confidence: CEOs and CISOs/CSOs have differing levels of confidence in their ability to comply with regulations, particularly regarding AI, resilience and critical infrastructure.

Gaps in measuring cyber risk: Although executives acknowledge the importance of measuring cyber risk, fewer than half do so effectively, with only 15% measuring the financial impact of cyber risks to a significant extent.

Cyber in Emerging Technologies End to End Benefits

Effectively managing Emerging Technologies has enterprise-wide advantages. It enables you to engage with customers in new ways across multiple locations and devices. Adopting leading edge cybersecurity practices through a clear understanding of compliance, regulatory and threat exposure in the emerging technologies help organisations to tap into its immense potential. All while you reduce operation risk, create new efficiencies and build trust.

So, you can evolve to support your changing digital needs. Whatever business you are in.

- Financial Services
- TMT
- Health & Pharma
- Infrastructure
- Retail & Consumer
- Manufacturing

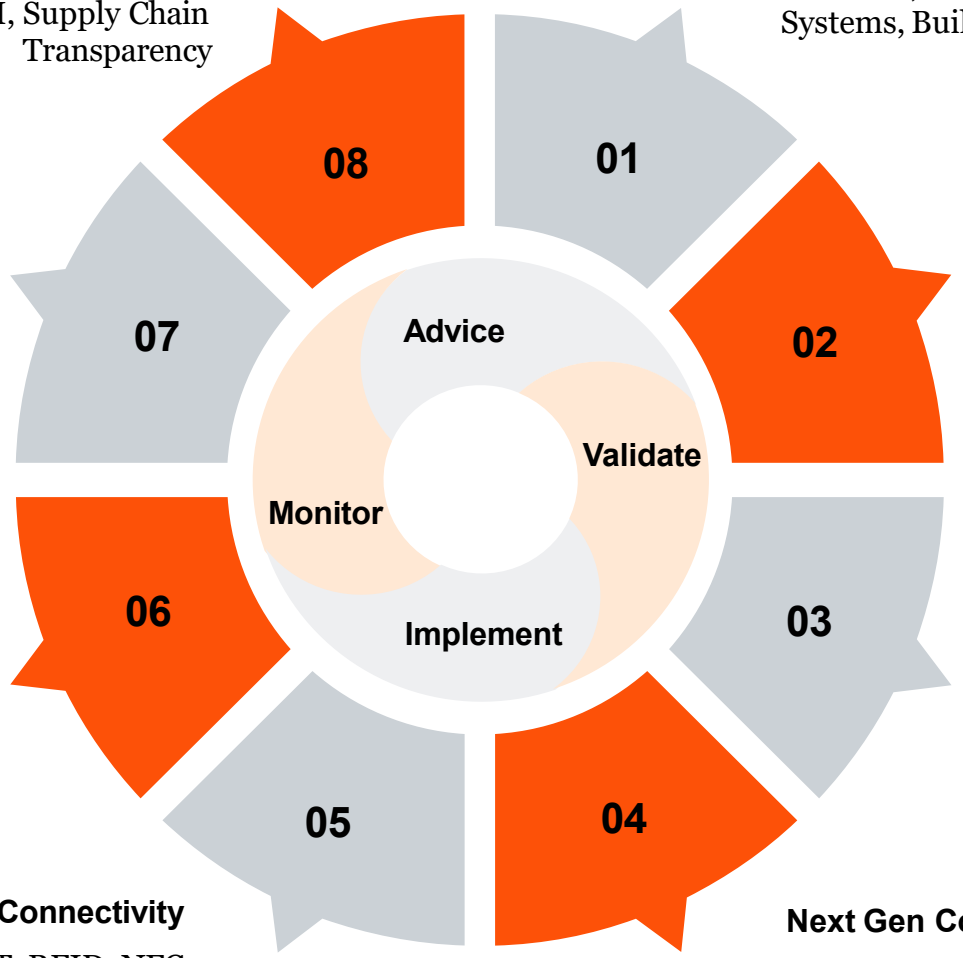
Cyber in Emerging Technologies

Supply Chain Integrity

Product Integrity, SBOM, HBOM, Supply Chain Transparency

Connected Factories

Factories, Industrial IoT, Smart City, Industrial Control Systems, Building Management Systems, Power Grids, Oil rigs



Next Gen Visual Technologies

AR/VR/XR, Metaverse, Digital Twin

Connected Products

Industrial products like Commercial vehicles, Ships, Robotics, CCTV's and

Consumer products like Cars, TV, Medical devices

Digital Assets & Cryptography

Blockchain, NFT, PKI, Utility Tokens

Artificial Intelligence

AI, Gen AI, Agentic AI, Machine learning, Deep Learning

Next Gen Connectivity

5G, LORA, Satellite, NBIoT, RFID, NFC

Next Gen Computing

Quantum and Edge Computing

Read More

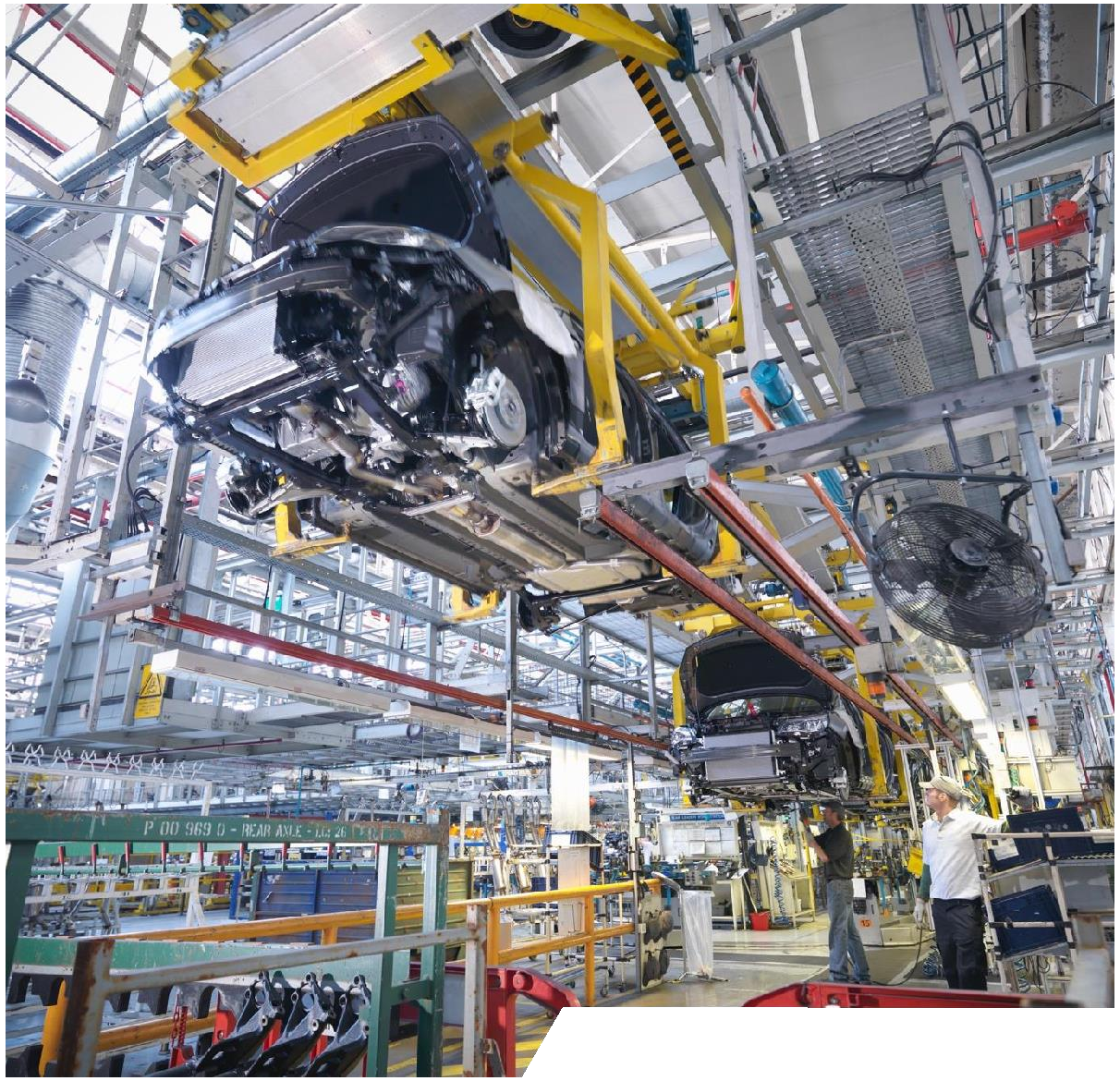
Connected Factories

Connected factories unlock immense opportunities for operational excellence and innovation. Realizing this potential, however, is critically dependent on robust cybersecurity measures that defend against disruption and protect valuable assets.

Whether it is Industrial Control Systems (ICS), Industrial IoT, Network connectivity or Artificial Intelligence or cloud in connected factory environment, Smart cities or BMS, PwC can help build trust, safety, security, privacy and resiliency in these environments.

Our range of services allows you to realise the value by avoiding disruptions, protect your data, communicate across your factories across the globe.

- Security strategy & roadmap
- Secure assessment & validation
- Security tool deployment & configurations
- Monitoring & threat intelligence
- Governance, standards & compliance
- Risk assessments, architecture review and design
- Vulnerability assessments & Pen Testing
- Incident handling



Read More

Connected Products

While connected products revolutionize our daily lives with smart features, their digital nature makes strong cybersecurity an imperative.

The expansive attack surface necessitates comprehensive cybersecurity strategies to prevent data breaches, privacy violations, and device compromise.

PwC cyber team works with your R&D, design, production and after sales team to ensure the products are secure, resilient and private in the hands of your customers or employees and they trust and feel safe while using them.

- Cyber advisory across product lifecycle and certifications
- Product identity, access and device management
- Embedded hardware and firmware security
- Product Monitoring & threat intelligence
- Product Software quality, SUMS, FOTA and OTA
- Risk assessments, Architecture review and design
- Product verification and validation
- Incident handling & recall

Read More

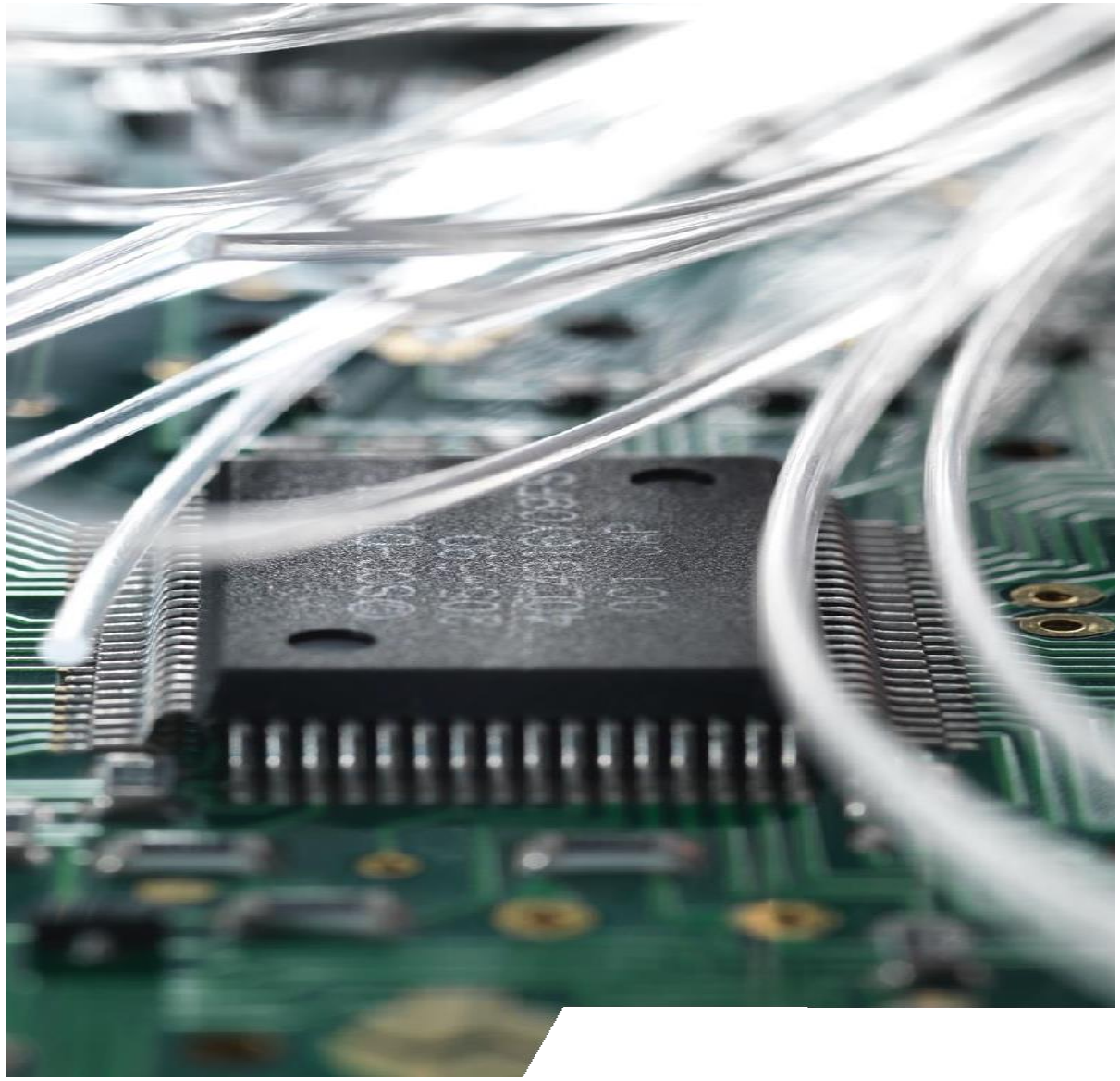
Cyber – Artificial Intelligence

Artificial intelligence is a revolution which is going to be used increasingly in all facets of life whether it is IT, Factories or Products like cars or mobile. Whether it is AI, GenAI, Agentic AI or NI. AI can help bolster defenses and simultaneously pose risk. PwC understands there are three facets to securing AI.

1. **Cybersecurity BY AI:** Use of AI tools and techniques to enhance AI powered cybersecurity defences like leveraging machine learning for advanced threat detection, automated response, and predictive analytics to combat evolving cyber threats more effectively.
2. **Cybersecurity OF AI:** Inherent security risks and biases within AI systems, which could be on how AI's decision-making can be influenced by flawed data or adversarial attacks, potentially leading to incorrect or harmful security outcomes.
3. **Cybersecurity FOR AI:** Protecting AI systems themselves from attacks like addressing vulnerabilities in AI models, training data, and the infrastructure that hosts AI, safeguarding against manipulation, data poisoning, or unauthorized access.

PwC leverages its knowledge, it's tools & accelerators and alliance ecosystems to bring the latest thoughts and solutions.

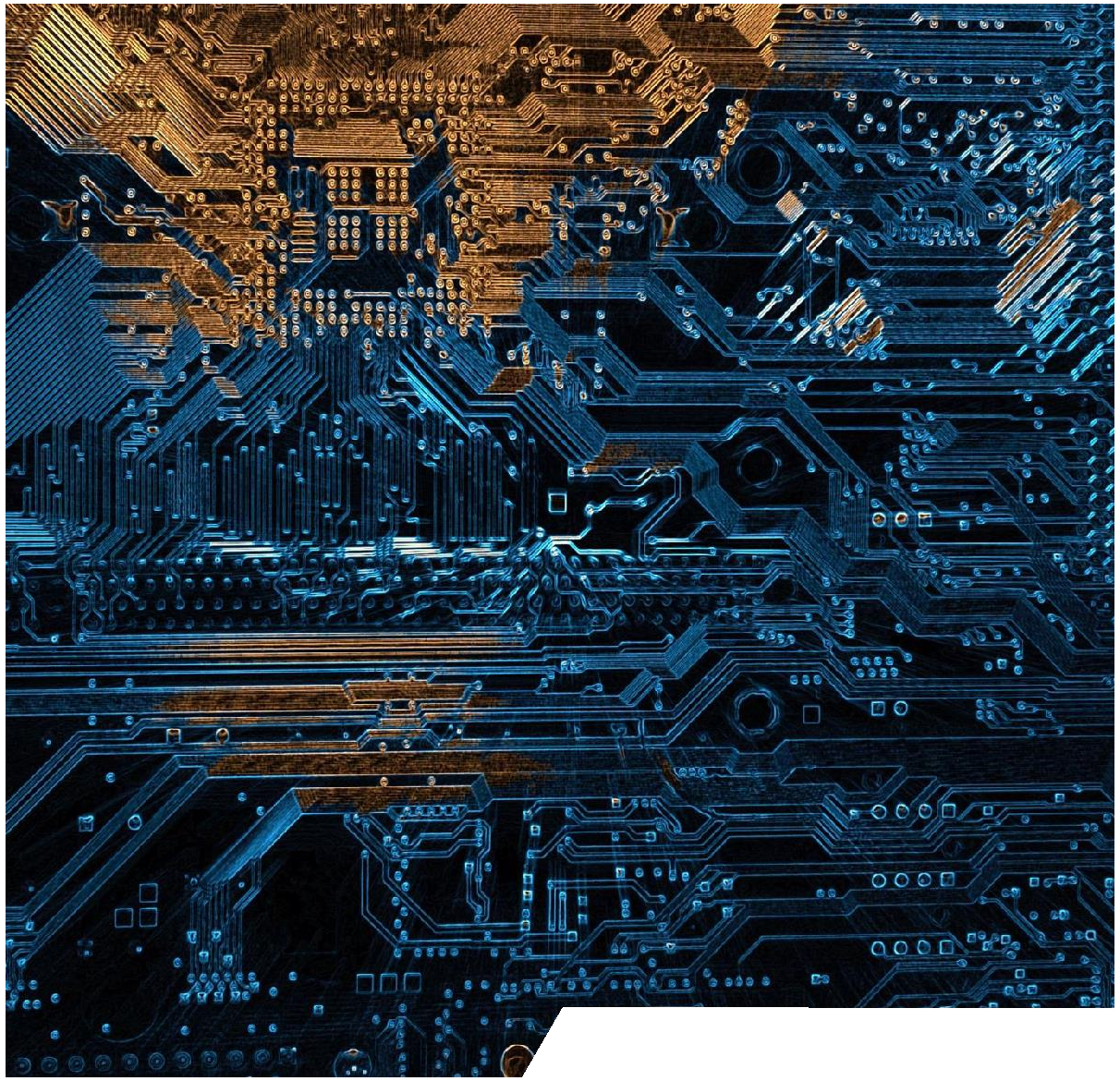
- AI strategy & roadmap
- Compliance and regulations
- Adversarial ML validation and testing
- Threat modelling
- Design, framework review and architecture
- Policy, code practice and ethical validation
- Risk assessment and validation
- Certification and SoP's



Read More

Next-Gen Computing

Next gen computing like Quantum and Edge are revolutionizing the world with its capabilities, while introducing unique challenges. Quantum computing power demands a re-evaluation of cryptographic standards while securing the highly distributed and diverse edge environments require innovative, adaptable protection at every node.



Quantum Computing

- Cryptographic asset discovery and inventory
- Quantum vulnerability risk assessment for cryptographic assets
- Data loss risk assessment: Harvest now, decrypt later threats
- Establishment of post quantum cryptography strategy
- Testing and validation
- Awareness and Education

Edge Computing

- Strategy and advisory
- Risk assessment, Architecture review and design
- Device and identity management
- Vulnerability assessment and Penetration Testing
- Monitoring and threat intelligence
- Incident handling

Read More

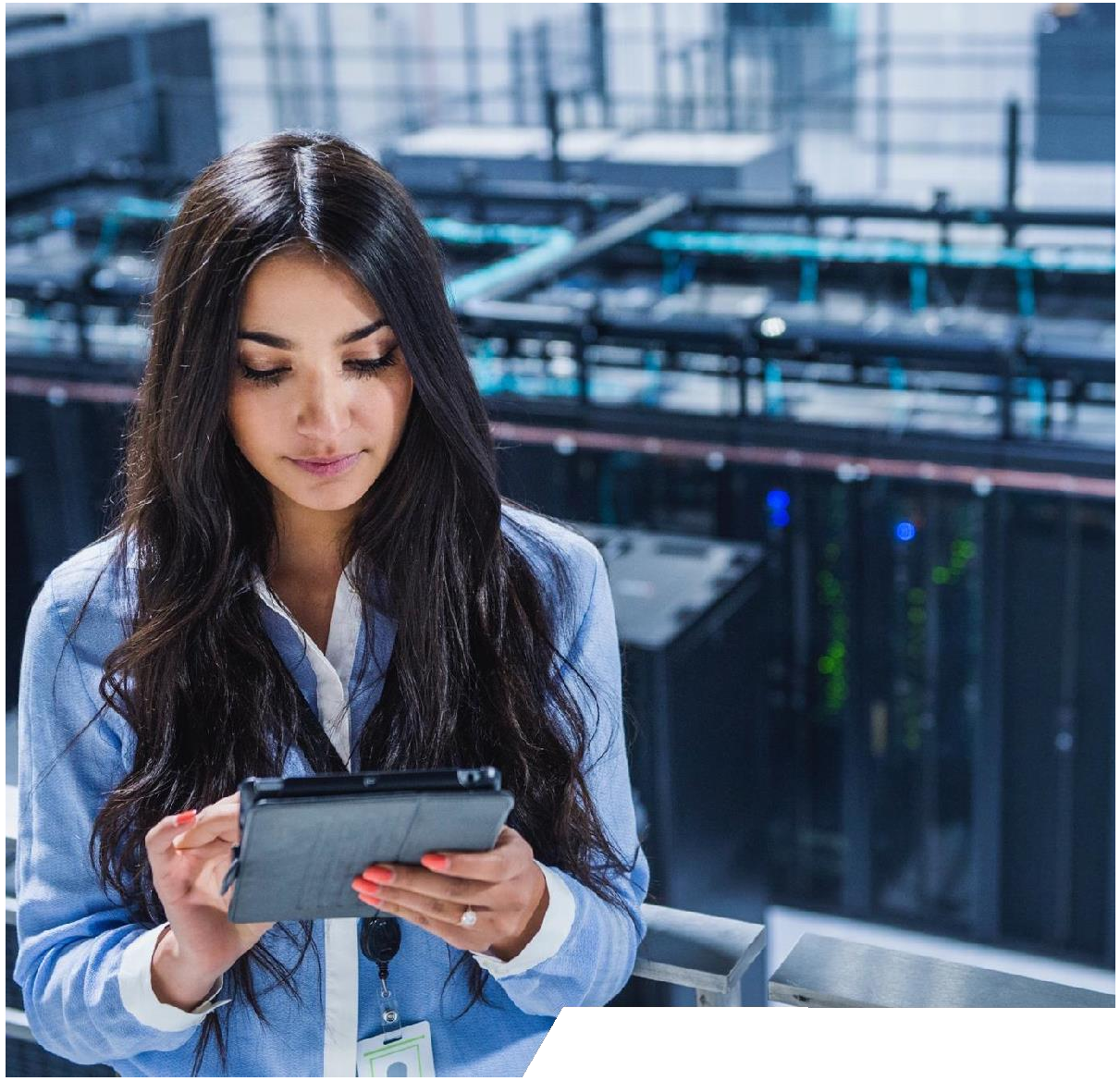
Next-Gen Connectivity

Securing next-generation connectivity solutions like 5G, satellite, and LPWAN (LoRa, NB-IoT) is crucial due to their expanded attack surfaces and diverse device ecosystems.

Robust cybersecurity demands novel approaches, including enhanced authentication, network slicing, and continuous threat monitoring, to protect critical data and ensure reliable service across these complex, interconnected environments

Our range of services allows you to realise the value by avoiding disruptions and protect your critical connectivity channels.

- Connectivity Security strategy development
- Regulatory compliance and policy advisory
- Digital trust frameworks
- Supply chain security for hardware and firmware
- Monitoring and threat intelligence
- Risk assessment and threat modelling
- Security by design
- Risk assessment, testing and hardening
- Vulnerability assessments and penetration testing
- Incident Handling



Read More

Next-Gen Visual technologies

Next-generation visual technologies like AR/VR/XR, computer vision, and digital twins introduce significant cybersecurity challenges by generating and processing vast amounts of highly sensitive data. Protecting these immersive and data-rich environments requires safeguarding privacy, ensuring data integrity, and defending against new attack vectors that could manipulate perception or compromise physical systems through their digital counterparts.

- Strategy and governance for immersive tech
- Privacy impact assessments & privacy by design
- Compliance and regulatory advisory
- Device and endpoint security
- Monitoring and threat intelligence
- Risk assessment and threat modelling
- Secure architecture design
- SDL for applications and content
- Identity and access management
- Vulnerability assessment and penetration testing

Read More

Digital Assets and Cryptography

Securing blockchain, NFTs, and cryptocurrencies demands mitigation of risks like smart contract vulnerabilities and private key theft, safeguarding the integrity of digital ownership and transactions. Public Key Infrastructure (PKI) forms a cornerstone of digital trust, providing the foundational cryptographic framework for secure identity, authentication, and encrypted communication essential across all digital interactions.

- Web3 strategy and governance
- Regulatory and compliance
- Smart contract auditing
- Cryptography implementation review
- Key management System implementation and review
- Risk assessment and threat modelling
- Asset custody and wallet security advisory
- Protocol security assessment
- PKI deployment and hardening

Read More

Supply Chain Integrity

Ensuring supply chain product integrity by protecting against tampering, counterfeiting, and unauthorized alterations at every stage is critical to ensure the final product security and privacy. This involves ensuring the software, hardware, and data flow from design to delivery is ensured, building trust that products are genuine and uncompromised.

The complexity of attacks and threats require a deep look into what goes inside the product to ensure the final product produces the outcome for which it was designed.

- Product integrity testing
- Risk assessments and supplier reviews
- SBOM & HBOM
- Hardware and firmware security specification requirement definition
- Hardware and firmware integrity testing
- Supply chain transparency

Read More

Emerging Tech CoE – Tools & Accelerators and Innovation Hub

AI Based Solutions | **Remote & Virtual Reality Experience for Clients** | **Customer Experience Center** | **Co-Creation and development with Partners**

Connected Factory Lab
Multiple production devices and sensors from different OEM's, 3D Printers, 5G, Extended Reality and Artificial intelligence all under one roof to answer your questions and concerns.

Smart Factory Shield
Experience Smart Factory Shield toolkit can help your organization to secure your shopfloor, converge IT –OT in the shortest time and secure your factories.

Operational Analytics
How operational data can be leveraged to make the best use of the data in a secure, private and resilient way within your organizations.

Cyber Range
Bring your clients, stakeholders and employees for a hands-on experience and go back with Education, Awareness & Training

Connected Product Lab
Vehicle, Medical devices, consumer products, ECU's, IIoT, PKI infrastructure, SUMS, OTA and FOTA and device identity management use cases.

Connectivity Framework
Learn, understand and use the latest in connectivity technologies like 5G, Satellite, LPWAN, LoRA, NBIoT, RFID, Bluetooth and NFC can be securely used in an efficient and connected way

IoT & OT Monitoring
Technologies and use cases to monitor factories, smart cities, utilities, power grids and products like cars, medical devices and consumer products

PwC India – Cyber Service Offerings

Cyber Risk and Regulations

Align with business, prioritize investments and align security capabilities to navigate cyber security risks & compliance requirements leveraging robust strategy & governance frameworks

Security Architecture & Automation

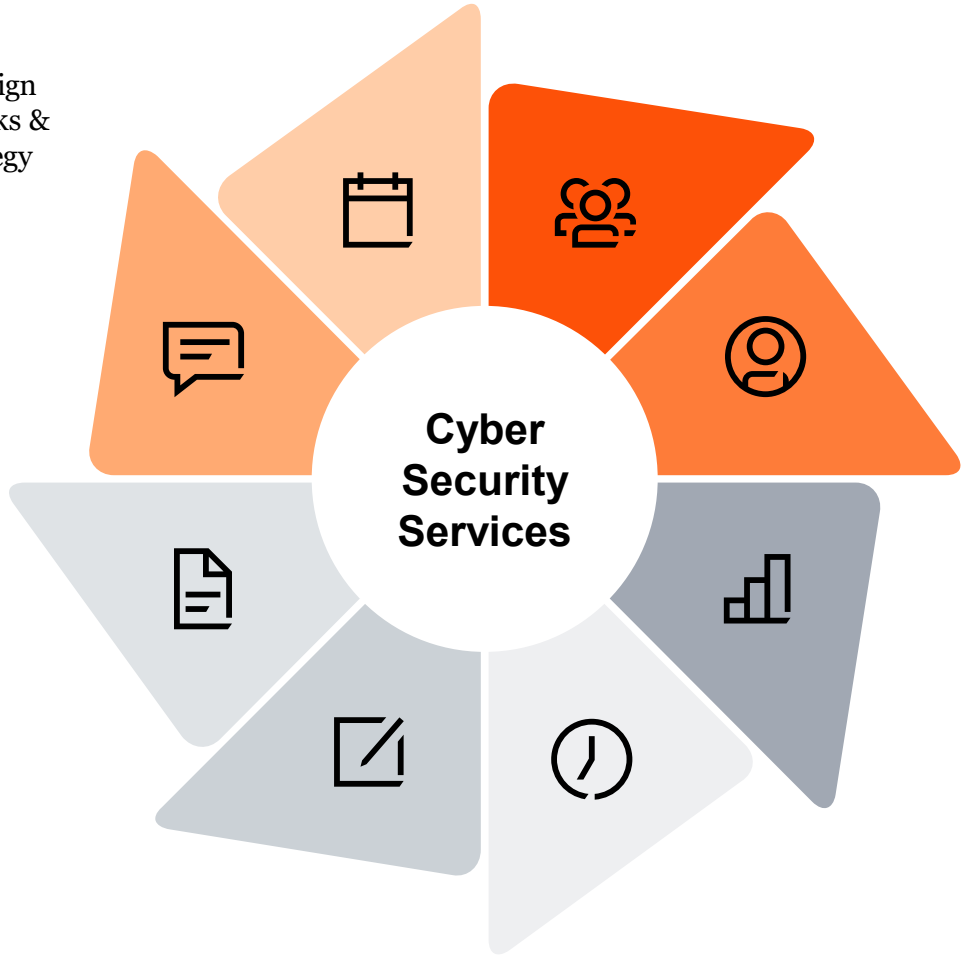
Select, architect and implement security products to discover value of optimal solutions and to secure business ecosystem

Identity Management

Maintain secure access to applications and infrastructure, with risk based intelligent authentication and authorization processes and technology, including privilege identities

Data Trust

Know your data, the handlers of data, protect exfiltration and penalties by complying to geographical, sectoral, business and regulatory mandates



Security Testing

Manage digital infrastructure attack surface, by identifying gaps, exploiting design flaws and assisting you in remedial actions to secure your ecosystem

Cyber in Emerging Technology

Our strategic focus spans across key innovation pillars of Connected Factory, Connected Products, Cybersecurity for AI, Next-Gen Computing, Next-Gen Connectivity, Advanced Visual Technologies, Digital Assets & Cryptocurrencies, and Supply Chain Integrity

Cyber-as-a-service

Ability to detect, manage and respond to security incidents by leveraging our 24x7x365 Cyber Protection Centre (CPC) and active Threat monitoring services, Endpoint Detection Response, etc.

Incident Response

Identify the root cause, nature, means and source of an incident to support as evidence for any legal action & breach support, through our forensic services

Read More

...in partnership with the product ecosystem (Global & India)...

Technology-powered partnerships

Unlock future potential through strategic partnerships, where advanced technology converges with security interventions.

Over time, we have curated strategic alliances with the world's leading technology and security companies to drive accelerated innovations, inform on risk and power business transformations.

PwC integrates deep industry knowledge with our alliance partners' technological capabilities and implementation proficiency, creating a synergy that not only multiplies value but positions organisations for sustained success.

Explore the areas where we collaborate with our alliance partners to power and protect

Security monitoring and operations
- Microsoft
- Google
- OpenText
- Securonix

Identity management
- Microsoft
- SailPoint
- Saviynt
- CyberArk
- Okta
- Tuebora
- Cross Identity
- Cymmetri

System security management
- Microsoft
- Palo Alto
- Sentinel One
- TrendMicro
- Tenable

Application security management
- Automox
- Fortify
- BlueYonder
- Applan
- MuleSoft

Network security
- Microsoft
- Palo Alto
- Fortinet

Cloud security
- Microsoft
- Palo-Alto
- Wiz.IO
- Google
- HTCD
- AWS

Operational technology
- Microsoft Tenable
- Honeywell

Data security management
- Microsoft
- OneTrust
- TrendMicro
- Netskope
- Klassify
- Seqrite
- Varonis
- Securiti.AI

Vehicle security operations center (V-SOC)
- Securethings
- Karamba

Governance, risk and compliance
- Workiva
- MetricStream
- SAP GRC
- ServiceNow
- RSA Archer

Artificial Intelligence
- OpenAI
- Salesforce
- Google
- Harvey
- Oracle

Others
- SAP
- Adobe
- Anaplan
- Jacobs
- Workday

...powered by our digital tools and accelerators...

1 End-to-end platforms

Software supply chain security

Performs continuous third-party software security assessments across development, build and runtime platforms, including COTS, open-source, and in-house software

Automated data discovery and classification

Automates data discovery and classification, significantly reducing effort in data flow assessment exercises

Penetration test automation

Automates triggering of penetration tools like Burp Suite, Nessus and Nmap, consolidates reports, and provides a unified dashboard

Risk Strategy Evaluator (RiSE)

An interactive tool that helps you practice making quick, high-stakes decisions with limited information. It uses a competitive approach to test its ability to respond effectively to cyber attacks.

Privileged users' discovery - OS, DB and mainframes plugin

Discovers privileged users across OS, DB and mainframes, and integrates with the privileged access certification process

Vulnerability management automation

Automates vulnerability scoring based on customer's business risk acceptance and asset priority

SAP-ITSM

Automates assessment of security logs and S4HanaDB transactions against security and business controls

DevSecOps

Automates security scanning within CI/CD pipelines

2 GenAI based Solutions

GenAI-based firewall request review - MSS Automation

Automates firewall rule reviews using GenAI, customised to the client's context

GenAI-based security compliance assessment

Automates NIST, ISO, threat modeling and security compliance assessments

GenAI policy to code

Transforms policy documents into Open Policy Agent code.

Leveraging GenAI in the Cyber Threat Intelligence (CTI) service delivery

GenAI tools like ChatPwC speed up cyber threat advisories and YARA rule creation, cutting manual work from hours to minutes while ensuring accuracy through validation.

Agentic AI automates L0/L1 SOC analyst tasks

Enhances SIEM alerts with context, filters false positives, links related alerts, classifies threats, runs playbooks, creates incident tickets, escalates issues, and refines decisions with analyst feedback

OT security GenAI controls

Generates sector-specific OT security controls and assessment domains

SOC chat bot for L1 investigation

Teams-based chatbot for incident investigation and enrichment

3 SharePoint/ Excel accelerators

SharePoint dynamic application threat modelling-PASTA

Automates threat modeling assessments with dynamic questionnaires and reusable forms

SharePoint-based SailPoint application onboarding factory

Enables self-service onboarding by app owners, accelerating the process across the organisation

Cyber risk quantification toolkit based on FAIR

MS Excel-based cyber risk quantification toolkit providing annualised loss exposure estimates, based on ISF QIRA and FAIR frameworks

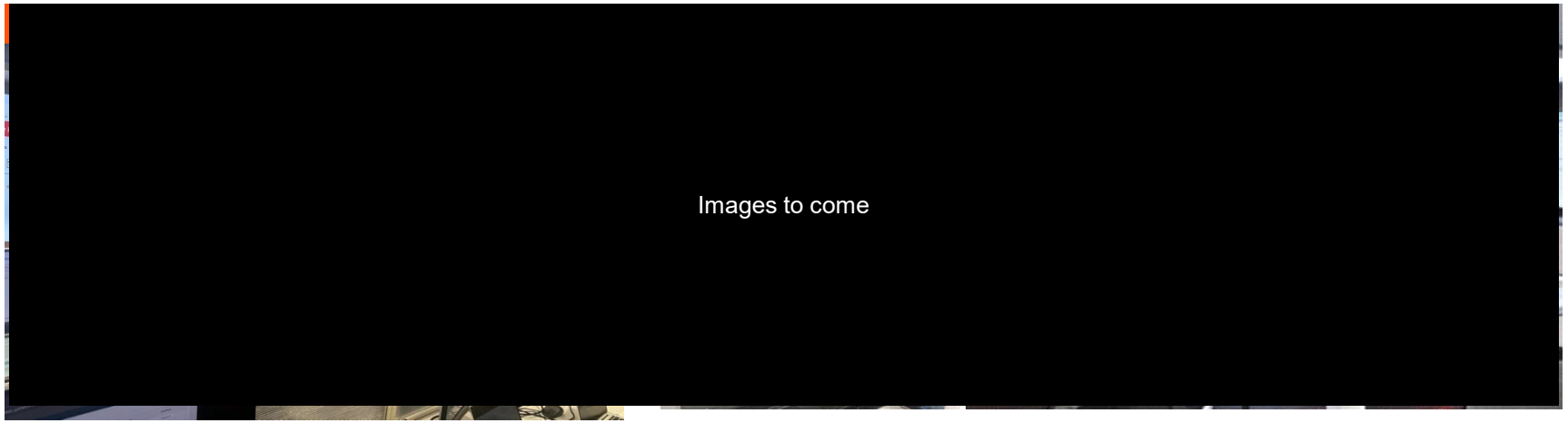
Desktop application security assessments

ISO 27001 estimation template

Reusable Excel toolkit to categorise efforts for ISO 27001 certification, enabling a factory-based certification model

…delivered through our India Cyber Protection Centre (CPC) and Global Delivery Center in India (1/2)

Our state-of-the-art CPC features a 200+ seater facility equipped with video walls for eyes-on-glass monitoring.



PwC's CPC is a state-of-the-art 350+ seat facility in Kolkata, Gurugram and Navi Mumbai. Equipped with the latest technology, our team of highly skilled security analysts work tirelessly to safeguard your digital assets.

Multi-level security

- Dedicated floor for CPC
- Multi-level perimeter security
- Biometric access controls on all doors
- 24x7 IP camera monitoring and feed streaming
- Dedicated facilities (ODC) for high security operations
- On-demand workspace for visiting/stationed client personnel
- Dedicated client contact helpline
- Video conferencing facilities
- Enhanced security for data centre with water seepage detection, FM200 firefighting and rodent protection

Services offered

- Security operations
- Incident management
- Engineering services
- Attack surface management
- Threat intelligence
- Compromise assessment
- Malware analysis
- Forensics and countermeasures
- Network management
- Device management
- Patch management
- Dark web and brand monitoring

CPC Kolkata is ISO 27001 certified

DNV·GL

MANAGEMENT SYSTEM CERTIFICATE

This is to certify that the management system of

PricewaterhouseCoopers Pvt Ltd
Plot # Y-14, Block # EP, Sector V, Salt Lake, Kolkata - 700 091, West Bengal, India

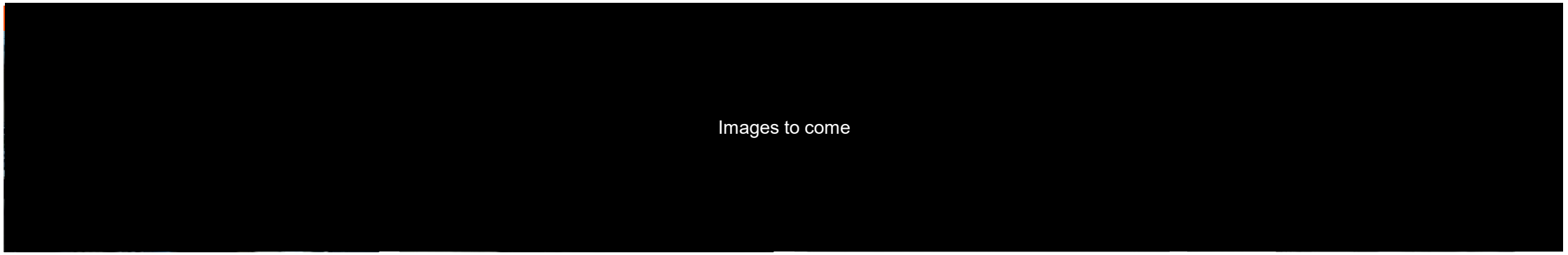
has been found to conform to the Information Security Management System standard:
ISO/IEC 27001:2013

This certificate is valid for the following scope:
Management of information security and support required in terms of cyber protection centre (CPC) facility to provide managed security services (MSS) covering threat detection, response, security engineering & operations and threat & vulnerability management services under the advisory-consulting services in accordance with the statement of applicability ver. no. 3.2 dated 20-Aug-2018

…where clients can experience futuristic cyber risks associated with IoT, devices, vehicles and more (2/2)

PwC India's **Vehicle Security Operations Centre (V-SOC)** serves as a centralised hub for **real-time monitoring** and **rapid response** to security incidents related to connected vehicles. It offers real-time **visibility and proactive threat mediation** ensuring connected vehicles are cybersecure.

PwC's approach to vehicle security also includes building a **security culture, developing cyber strategies and implementing security tools.**



Services:

CSMS homologation

Assess, develop and rollout CSMS inline to AIS 189, BIS and UNR155

Verification and validation

TARA, vehicle, hardware and firmware penetration testing inline with ISO21434, ISO 26262 and others

SUMS and OTA

Assess, develop and rollout inline with AIS190, BIS and UNR156

Training and awareness

Vehicle security awareness about risk assessment, vehicle penetration testing to V-SOC – covering everything from technical to boardroom-level awareness.

Vehicle DevSecOps

AutoSAR, ASPICE, MISRA etc., integrated with agile methodology

Technical Compliance Management System

Technical Compliance Management System (TCMS) covering SBOM, HBOM, supplier transparency, supplier product integrity testing

Vehicle – SOC

- Ingest, correlate and real-time detection
- AI-integrated analytics
- Mobility playbook
- 24 x 7 x 365 operations with build, own, operate and transfer capability

Global service, locally delivered

Whether your organization operate in India or at a global level, we at PwC, we bring the full power of our worldwide network directly to your doorstep. We operate in over 150 countries with a vast array of specialized experts, cutting-edge tools, and proven methodologies, every solution we provide is precisely tailored to your unique context, right here where you do business.

Our global network helps us to tap into our global intelligence – the collective experience of thousands of professionals who have tackled similar issues in diverse markets worldwide. This "global service" ensures that you benefit from the best practices, innovative thinking, and deep industry knowledge that PwC has cultivated across its international footprint.

This global expertise is always filtered through the lens of your local market. Our local teams understand your specific regulatory environment, cultural nuances, competitive landscape, and unique operational realities.

This "locally delivered" approach ensures that the solutions we co-create with you are not just theoretically sound but are practical, actionable, and seamlessly integrate with your existing operations, ultimately driving tangible and sustainable outcomes for your business.

India

- Across 16 locations
- More than 150 Years in India
- 50,000 professionals
- Top 50 Best companies to work for and India Best workplaces in professional services, 2024
- PwC was recognized as Best Employer
- Brand in LinkedIn Talent awards, 2023

PwC – A recognised Leader

- Leader in Worldwide Manufacturing Service Provider Vendor Assessment – IDC Marketspace
- Leader in European Cybersecurity Consulting Providers by Independent Research Firm
- Leader for Global Cybersecurity Consulting - Forrester
- Leader in Cybersecurity Consulting - ALM Intelligence
- Leader in the EMEA Industry Cloud Professional Services - IDC MarketSpace:
- Global Leader in Enterprise Risk Management Consulting Services
- Leader Worldwide SAP implementation Services - IDC MarketScape:
- Leader in the Worldwide Medical Devices Data Driven Transformation Consulting

Read More

Thank you

KA/November 2025/M&C 49843