Cybersecurity Capability Overview

Transforming the security landscape for organisations

November 2025

What are the challenges you are facing today?

Emerging technologies and GenAI

Advancement of Gen AI presents new opportunities but poses cybersecurity risks – advanced threats, integration challenges, and dual-use in defense and attack.

Complexity of compliance

Strict regulations like Digital Personal Data Protection (DPDP) Act, 2023, Reserve Bank of India (RBI)'s Cybersecurity Framework, Securities and Exchange Board of India (SEBI) Cybersecurity and Cyber Resilience Framework (CSCRF), CERT-In Guidelines, Telecom Cyber Security Rules, 2024, demand rapid compliance, challenging existing security practices.

Cyber Risk Quantification

Cyber risk is widely acknowledged as critical, yet many still face challenges in quantifying its financial impact.

Cyber investment and priorities

Cybersecurity is a key differentiator, strengthening brand integrity, trust and competitive advantage amid rising threats.

Cyber resiliency

As businesses grow, they struggle with resilience, leaving them exposed to growing threats.

Securing the cloud and security in the cloud

With the evolving digital landscape, cloud security continues to remain a top priority, requiring recurring investments.

The rollout of DPDP Act,2023 has made end-to-end data lifecycle management essential requiring cloud security to redefine itself with unification of infrastructure and integration across systems.

Harness unmatched scalability: Our comprehensive suite of services synchronise security effortlessly to multiply business value

01. Cyber risk and regulations

Align with business, prioritise investments and security capabilities to navigate cybersecurity risks and compliance requirements, leveraging robust strategy and governance frameworks.

02. Security architecture and implementation

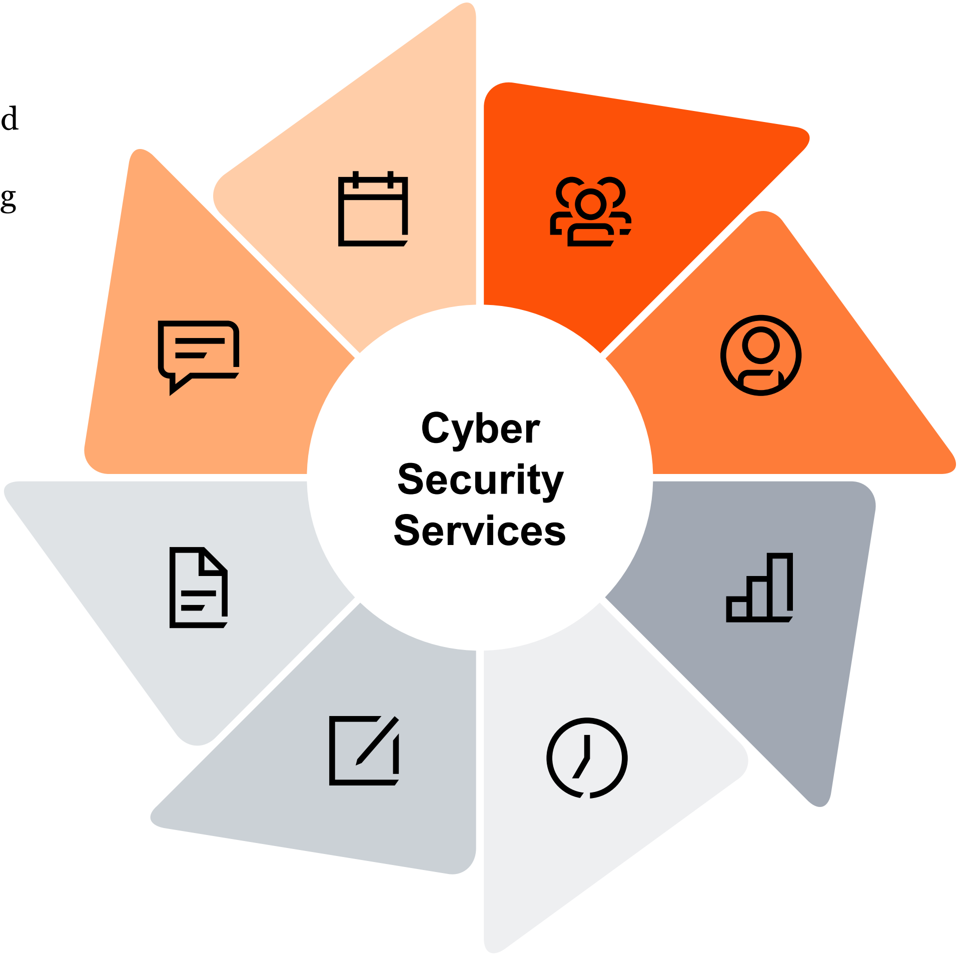
Select, build and implement security products to discover value of optimal solutions and secure your business ecosystem.

03. Identity management

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

04. Data trust

Know your data and its handlers, protect exfiltration and penalties by complying with geographical, sectoral, business and regulatory mandates.



05. Security testing

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

06. Cyber in emerging technology

Strategic focus spanning across key pillars of connected factory, connected products, cybersecurity for AI, next-gen computing, next-gen connectivity, advanced visual technologies, digital assets and cryptocurrencies, and supply chain integrity.

07. Cyber-as-a-service

Ability to detect, manage and respond to security incidents by leveraging our 24 x 7 x 365 Cyber Protection Centre (CPC) and active threat monitoring services, endpoint detection response, etc.

08. Incident response

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

Aligning your sector-specific goals with our deep expertise...

Every industry has distinct challenges and opportunities.

PwC's Cybersecurity teams have deep sector expertise, working across our multiple industry groups.

This enables us to focus on what matters – the present and planning for the future. We help you navigate your challenges and seize your opportunities effectively.

Our focused sectors are as follows:

Government

- Critical information infrastructure protection
- AI/ML security
- AI driven - cyber resiliency
- Unified cybersecurity solutions

Financial services

- Regulatory compliance
- API security and fraud prevention
- Supply chain security
- Cyber resiliency

Energy and utilities

- SCADA systems, smart grids, and industrial control systems (ICS) security
- AI and automation in cyber defense
- Advanced persistent threats (APT) security

Pharmaceutical and lifesciences

- Clinical trial data security
- Protection of intellectual property (IP)
- Supply chain security
- Regulatory compliance & security governance (DPDP Act, GDPR/HIPPA)

Healthcare

- Patient data and electronic health records (EHRs) data security
- Mitigating advanced persistent threats (APTs) and AI-driven attacks
- Internet of medical things (IoMT) security

Telecommunications

- 5G security
- Data privacy and security
- Cloud and edge security (SASE, container, API)
- Regulatory compliance (dot, TRAI, cert-in) and incident response

Global capability centers

- Regulatory compliance
- Real-time threat monitoring and security analytics
- Data privacy
- Automation, AI and GenAI security

Industrial manufacturing

- Operational technology (OT) and SCADA systems security
- AI-driven threat detection
- Smart manufacturing security
- Ransomware defense

Technology

- AI/ML security
- Blockchain security
- Post quantum cryptography
- System and data security

Media

- Content/data trust and transparency
- Digitisation and AI security
- Content control, quality and integrity

Retail and consumer

- POS and cloud security
- Supply chain security
- Consumer data privacy
- Cyber board awareness
- Omnichannel security (online, mobile, physical)

…in partnership with the product ecosystem…

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

Governance, risk and compliance

- Workiva
- MetricStream
- SAP GRC
- ServiceNow
- RSA Archer

Application security management

- Automox
- Fortify

Network security

- Microsoft
- Palo Alto
- Fortinet

Cloud security

- Microsoft
- Palo-Alto
- Wiz.IO
- Google
- HTCD

Operational technology

- Microsoft Tenable
- Honeywell

Data security management

- Microsoft
- OneTrust
- TrendMicro
- Netskope
- Klassify
- Seqrite
- Varonis
- Securiti.AI

Vehicle security operations center (V-SOC)

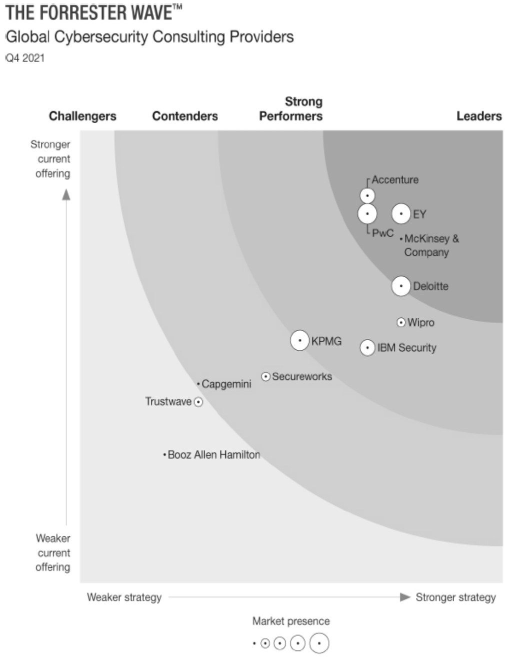
- Securethings
- Karamba

...and endorsed by leading analysts...

Our Cybersecurity practice is recognised as a leader in the industry by Forrester, Google and other respected analysts. This recognition underscores our unwavering commitment to safeguarding digital landscapes with innovative and robust solutions.

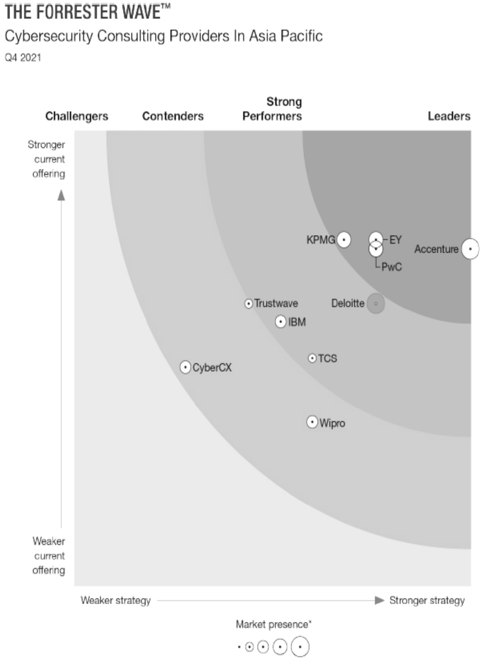
Global

The Forrester Wave
Global cybersecurity consulting providers



Forrester

The Forrester Wave
Asia-Pacific cybersecurity consulting Providers



Google

Google Cloud Next 2025
Security Partner of the Year – Asia Pacific

Images to come

Additional Analyst Recognitions

Logos to come

2024 Leader in the Managed Security Services
IDC Marketscape Asia/Pacific

2024 Leader in the Professional Security Services
IDC Marketscape Asia/Pacific

2023-2024 Leader in the Cloud Security Services
Asia/Pacific

2023 Cybersecurity Risk Management Services Leader
Global

2021 Worldwide Incident Readiness Services
Global

2020 Leader
IDC Marketscape Worldwide Risk Consulting Services

…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

A lightweight framework for evaluating desktops and thick clients, integrating with AIM (SAM) to pull SCCM inventory and improve risk scoring using VirusTotal and NVD.

ISO 27001 estimation template

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

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

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

Images to come

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.

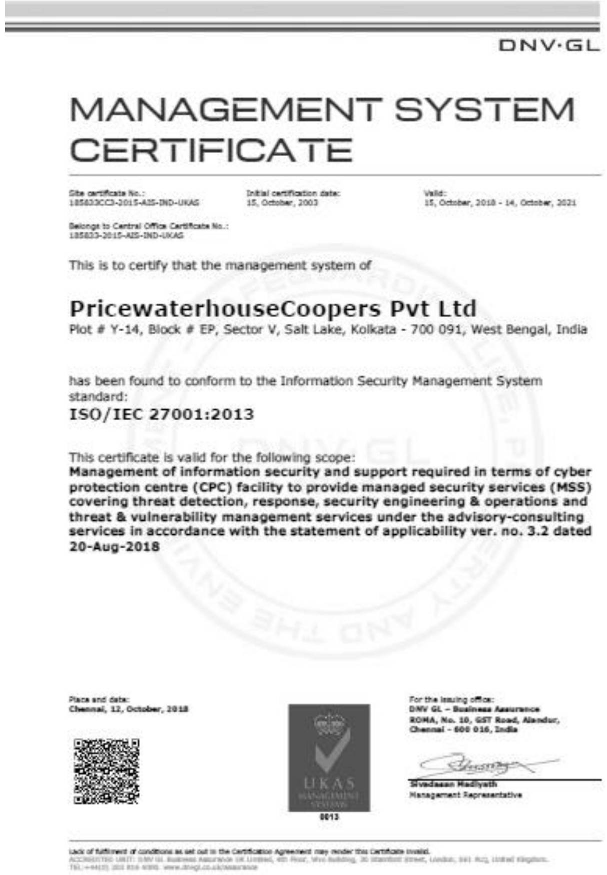
Multi-level security

- 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

Site certificate No.: 185833CC3-2015-AIS-IND-UKAS
Initial certification date: 15, October, 2003
Valid: 15, October, 2018 - 14, October, 2021

Belongs to Central Office Certificate No.: 185833-2015-AIS-IND-UKAS

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

Place and date:
Chennai, 12, October, 2018

UKAS MANAGEMENT SYSTEMS
0013

For the issuing office:
DNV GL – Business Assurance
ROMA, No. 10, GST Road, Alandur,
Chennai - 600 016, India

Sivadasan Madiyath
Management Representative

Lack of fulfilment of conditions as set out in the Certification Agreement may render this Certificate invalid.
ACCREDITED UNIT: DNV GL Business Assurance UK Limited, 4th Floor, Vivo Building, 30 Stamford Street, London, SE1 9LQ, United Kingdom. TEL: +44(0) 203 816 4000. www.dnvgl.co.uk/assurance

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

Our Global Managed Delivery Center in Kolkata (India) is the center for excellence for remote delivery of services across multiple domains.

Methodologies

OWASP Top 10, SANS Top 25, CIS Benchmarks, Black box, Grey Box and White Box testing for Threat and Vulnerability assessment (including manual & automated testing). Frameworks & standards like ISO 27001:2013, ISO 22301, COBIT, HIPAA, NIST, GDPR etc.

Certifications

Microsoft, Google, Azure, AWS, CEH, ECSA, CWASE, ISO 27001 LA, OSCP, PMP, CISSP, CISA, ITIL, CISM, Six Sigma, CHFI, MCP, MCITP, CCNA, CCNP, CNAPP, CSPM, CWPP, CCSE, PRINCE2, SailPoint IIQ Engineer, Okta Professional/Consultant, CCDE Certifications, ISO 21434, ISA 62443, CIoTSP, GICSP, ISO 26262, ISO 15048, ISO 21434

Technologies/Tools

PwC proprietary SOC solution, and tools like Nessus, Burp suite, Qualys-Guard, HP-Web Inspect, Veracode, HP Fortify, Fuzz API, pURL, Acunetix, ZAP Proxy, dex2jar, appuse VM, Android SDK, Checkmarx, IBMAppScanMetasploit, Nmap/Zenmap, SQL Ping, Kali, Wireshark, Air Crack NG etc.

Risk and compliance

- Third-party assurance and supplier assessment
- IT general controls review
- General Data Protection Regulation (GDPR)
- IRDA regulatory assessment
- IT security/compliance audits
- ISO 27001 : 2013 (information security)
- ISO 22301

Identity and access management

- Strategy and architecture
- Design and implementation services across various IAM solutions
- Managed services to sustain an identity implementation
- User access reviews

Threat and vulnerability management

- Web application security assessment
- Network assessment and penetration testing
- API security assessment
- Secure code review
- Mobile security assessment
- Secure configuration review

Key attributes

- Successful in ramping up the team at short notice
- Ability to support global clients due to integrated delivery capabilities

…where clients can experience futuristic cyber risks associated with IoT, devices, vehicles and more (1/2)

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.**

Images to come

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

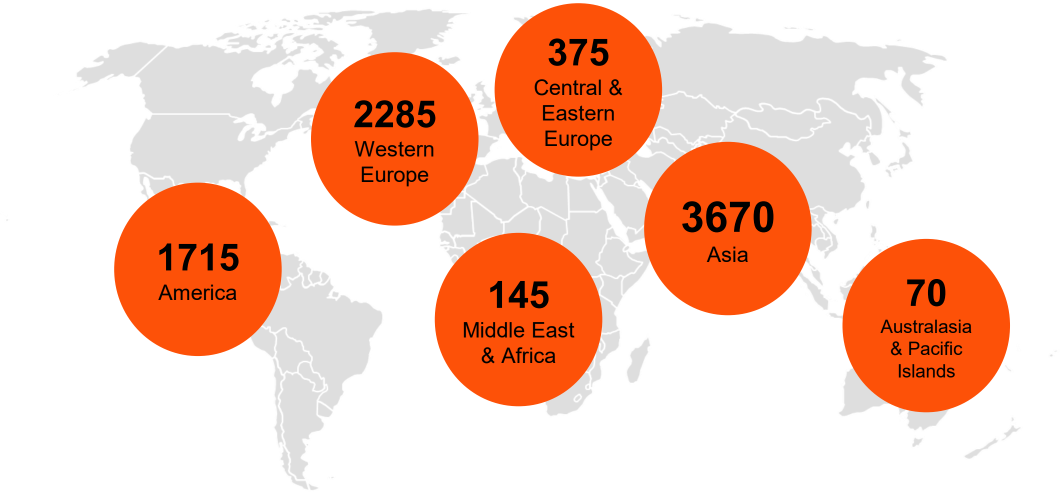
…where clients can experience futuristic cyber risks associated with IoT, devices, vehicles and more (2/2)

Our automotive presence around the world

Total of **8,200+ automotive** sector professionals

Total of **1,000+ auto cybersecurity** professionals

100+ auto cyber professionals in **India**



Training & Certifications

- ISO 21434
- ISA 62443
- CIoTSP
- GICSP
- OSCP
- CISM
- ISO 26262
- ISO 15048
- ISO 21434
- ISO 24089
- CACSP
- CISSP
- OSEP
- OSCP
- GPEN
- GIAC
- AUTOSAR
- ASPICE
- ISO 42001
- CRISC
- CCSP

PwC Autofacts®: Our market intelligence team to highlight market projections and trends

Global expert network	Scenario-planning and long-term forecasts	Deep industry knowledge	Strategic decision-making support
Holistic **industry knowledge** through a global network of analysts	Profound data to develop a **vision of the future of the automotive industry**	Our **dedicated market studies** give us a thorough understanding on the transformation of the industry	**Individual solutions** for business planning and assessment of business risks
Support the development of a market entry strategy	Client-specific powertrain/segment forecast to support strategic portfolio planning until 2030	Business plan validation and risk assessment relating to market trends	Market modelling and product/technology mapping to assess business potential

Outcomes you achieve:

- Enhanced operational visibility: Improved visibility into vehicle and its ecosystem
- Integrated IT, OT, IoT and vehicle SOC with rapid identification and response
- Accurate inventory of automotive devices of interest for vehicle SOC
- Early detection of abnormal behaviour and potential cyber threats
- Identification and remediation of vulnerabilities in in-vehicle systems and adherence to industry regulations and security standards
- Vehicle-specific custom use cases with proactive identification of abnormal behavior and potential cyber threats

PwC proprietary TARA Tool

- Purpose-built cybersecurity for various connected mobility verticals, including passenger and commercial vehicles, **fleets, and 2, 3, and 4+ wheelers**.
- Depth of service from advisory, testing, implementation and monitoring

Thank you

Data classification: DC0 (Public)

Disclaimer needs to be updated as per given entity

KA/November 2025/M&C 49843