Digital Enterprise. Protected.

Your Global Partner for Digital and Cybersecurity Solutions.

www.tuv.com/informationsecurity

TÜVRheinland®
Precisely Right.

Protecting Your Digital Enterprise with our Complete, Global Cybersecurity Portfolio

Achieving faster time to market, greater economies of scale and an improved customer experience are only a few of the reasons why your organization—no matter the size, industry or location—is undergoing a digital transformation. Yet as computing, storage, network, cloud and sensor technologies continue to evolve and enable new possibilities, they also significantly expand your enterprise's attack surface. They grow the exposure to increasingly sophisticated cyberattacks by criminals who are targeting data and intellectual property (IP) for financial gain, to sell to your competitors, disrupt operations or cause even greater harm. Once your organization is a target, it is only a matter of time before an advanced, persistent cyber attacker finds a way inside your digital walls. Yet it is not practical or financially feasible to have every security control operating everywhere at all times. That is why it is critical to continuously assess cyber risks, prioritize security investments and implement cyber defenses and controls that will keep your digital enterprise protected.

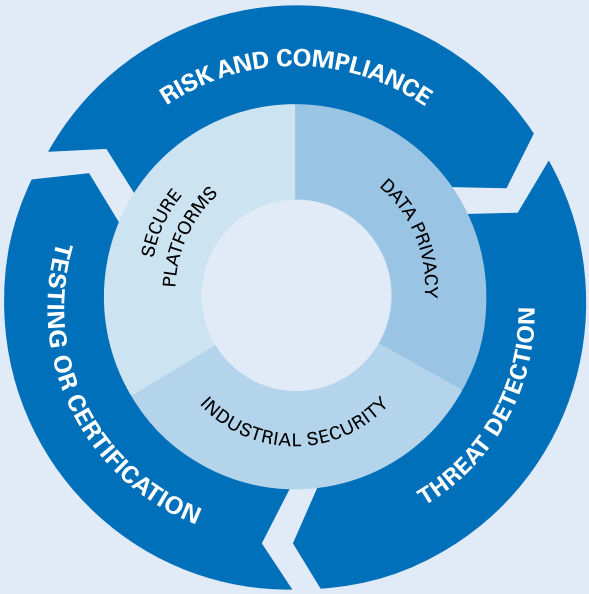
Our Approach:

A TIGHTLY INTEGRATED, RISK-BASED METHODOLOGY

TÜV Rheinland has been keeping society safe for over 145 years. Our global, end-to-end cybersecurity services portfolio spans consulting, technology implementation, testing, managed services or certifications. We protect organizations around the world from the ever-increasing cyber threat and enable safety, security and privacy in an increasingly digital world.

What truly differentiates TÜV Rheinland is our unmatched depth of specialized security experience and extensive, global services to keep digital enterprises protected—all based on a tightly integrated, risk-based approach to cybersecurity.

Our Best-in-Class Cybersecurity Capabilities



DATA PRIVACY, INDUSTRIAL SECURITY, AND SECURE PLATFORMS

These areas are heavily impacted by digitalization. Data privacy is a key design factor for IoT connected consumer devices, increasingly becoming a part of our connected personal and professional worlds. Industrial security is the core challenge for converged operational and information technology networks, which are no longer air gap protected, exposing operational technology to new cyberattacks. The growing digitalization and sophistication of cybercrime make traditional security platforms less effective - in need of better architecture and often the deployment of more advanced cybersecurity controls.

RISK AND COMPLIANCE, THREAT DETECTION, AND TESTING OR CERTIFICATION

The outer circle areas represent the core aspects of our risk-based approach. Each capability feeds the next in a virtuous cycle, always improving the visibility of cyber risk and continuously re-focusing efforts and prioritizing investment on the controls, with most impact on protecting the digital enterprise.

RISK AND COMPLIANCE

Helps your organization establish policies based on business-specific needs and risks, puts programs into action through standards and procedures, and not only manages risk, but masters it.

THREAT DETECTION

Creates an interwoven security architecture that enables rapid detection and response. Identifies security gaps to intercept and safeguard your organization from the most sophisticated cyberattacks.

TESTING OR CERTIFICATION

Enables your organization to assess and certify active controls, identify security gaps, evaluate response preparedness and recommend future mitigation and remediation efforts.

SECURE PLATFORMS

Empowers your organization to secure digital assets and processes, integrating public cloud services with IT platforms to provide the agility necessary to thrive in an always connected and mobile environment.

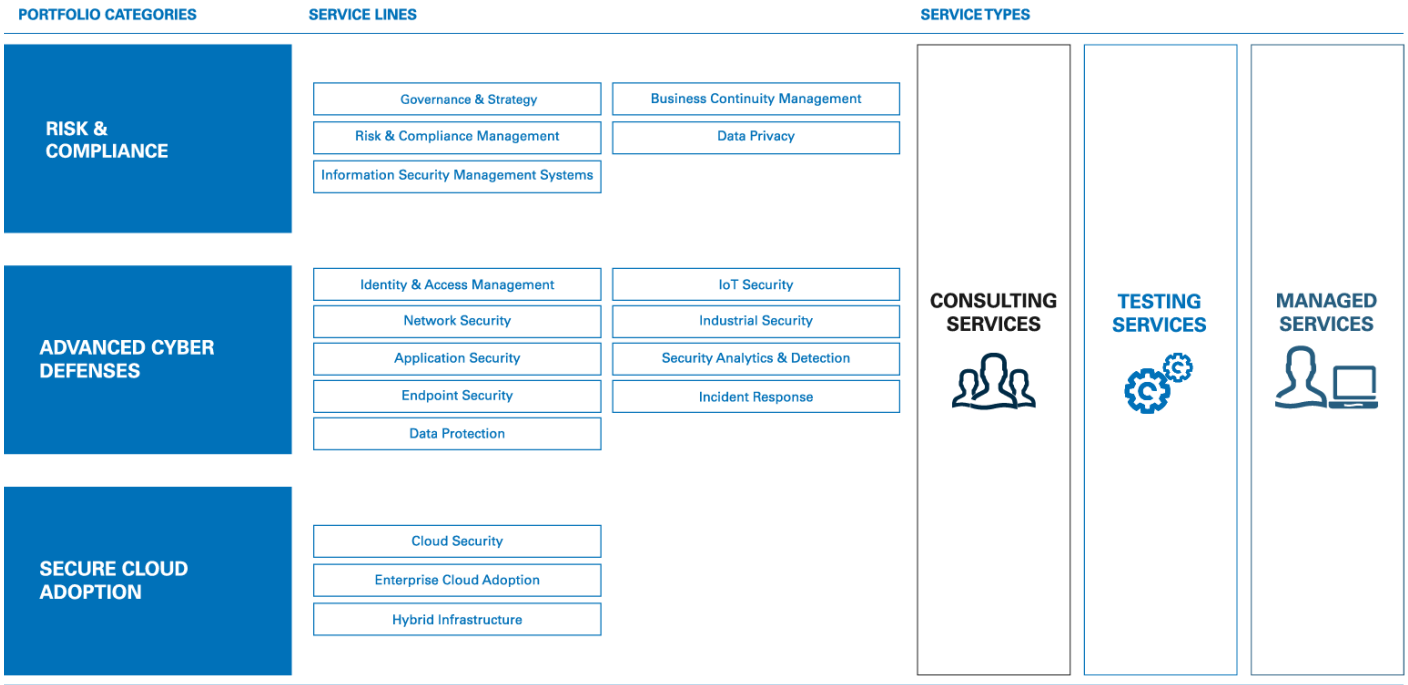
DATA PRIVACY

Helps your organization implement company-wide controls and privacy management policies in accordance with country- and region-specific requirements.

INDUSTRIAL SECURITY

Ensures safe and secure operation of smart factories, processing plants, energy and utilities, transportation systems and critical infrastructures by offering pragmatic solutions for a wide range of strategic and operational cybersecurity risks.

Our Complete, Global Cybersecurity Portfolio



OUR SERVICES AT A GLANCE

Globally consistent, far-reaching and equally deep portfolio of carefully selected service offerings gives your organization access to the strategic guidance, proven processes and best-in-class technology necessary to effectively manage risk, protect critical assets and thrive in the digital era.

End-to-end consulting, testing and managed services are forward-looking solutions that help our customers always stay ahead of the threat and competitive with alternatives.

Service-based approach helps you see the complete transparent picture and make informed, actionable investment decisions.

Comprehensive, top-down procedure ensures each stakeholder—from your CXO's to your technology and security practitioners—are involved and engaged in the necessary buy-in, ongoing collaboration and long-term success.

Single source for your organization's complete, end-to-end cybersecurity needs, with simplified processes and minimized operating expense to help accelerate your digital transformation.

Our services are deployed consistently worldwide, including consulting, integration of solutions, testing and managed services.

Risk and Compliance

You need confidence, flexibility and speed to succeed with digital transformation. Mastering risk and compliance allows your business to understand how, when and where to take risks in order to grow and transform in today's fast-paced environment.

We help you do this by deeply understanding your business to develop a holistic and highly customized threat profile to:

INFORM

We provide a clear picture of the specific threats your organization faces, supporting you with prioritizing top risks, creating actionable risk statements and automating governance risk and compliance (GRC) processes.

PLAN, BUILD, RUN

We assist your organization to plan, build and run enterprise-wide security management programs related to risk management, information and technology security, business continuity and data privacy.

We consider your specific requirements, size, products and culture. Our services ensure your organization implements a solid strategy that is chartered, governable and measurable—with emphasis on threat analysis. Our unique approach provides assurance and certification of market access requirements, including a broad catalogue of regulations and standards, from GDPR to risk & control frameworks such as ISO, NIST and IEC.

OUR RISK AND COMPLIANCE SERVICES

GOVERNANCE AND STRATEGY. Helps to ensure your organization has the management decision platform in place to not only manage risk, but to master it.

RISK AND COMPLIANCE MANAGEMENT. From IT risk maturity and prioritization to GRC configuration and enablement, our extensive line of proven risk and compliance management solutions empowers your business with decision-making confidence.

INFORMATION SECURITY MANAGEMENT SYSTEMS (ISMS). Optimize your organization's compliance efforts with industry-standard frameworks such as ISO 27000, NIST Cybersecurity Framework and COBIT.

BUSINESS CONTINUITY MANAGEMENT (BCM). Implement a robust business continuity management program to fulfill compliance requirements, prevent process failures and downtime, and protect your brand's reputation.

DATA PRIVACY. Analyze processes to guide you in implementing company-wide control and privacy management in accordance with country or region-specific legislation, compliance requirements and standards.

Advanced Cyber Defenses

Equipped with a comprehensive understanding of risk and compliance, the next step is to design and operate an effective cyber defense program. To accomplish that, your organization needs a combination of preventative, detective and responsive controls, which must be architected and implemented in line with your risk or threat prioritization.

Using our expertise, we provide a way to find the ideal solution for your organization to:

TRANSFORM

We provide the services and expertise your organization needs to bring your cybersecurity defenses into the digital era, empowering you to fully embrace a risk-based approach to prevention, detection and response.

OPERATE

We enhance your organization's existing cybersecurity operations by implementing and managing controls, identifying and remediating risks with comprehensive threat monitoring and threat hunting, to enhance an effective and timely incident response program. We align and integrate our cybersecurity operations with your organization's risk management program.

Our consulting, testing and managed services provide proven solutions to defend against advanced cyber threats.

OUR ADVANCED CYBER DEFENSE SERVICES

IDENTITY & ACCESS MANAGEMENT (IAM). Enhance productivity, security and compliance by efficiently controlling customer, employee and partner access to services and information beyond traditional IT boundaries

NETWORK SECURITY. Provide end-to-end infrastructure architecture, implementation and support designed to defend against advanced cyberattacks. Identify and remediate security weak points through extensive network security testing services.

APPLICATION SECURITY. Manage the security lifecycle of custom software development and acquired applications. Identify and remediate vulnerabilities through in-depth security testing, design consulting for application layer and defensive control technologies.

ENDPOINT SECURITY. Protect a wide range of internet enabled endpoints with advanced security controls while supporting enterprise mobility.

DATA PROTECTION. Implement effective controls and processes to ensure the privacy and integrity of sensitive or valuable information, prevent data exfiltration, and reduce the impact of compromised data.

IoT SECURITY. Identify and manage cyber risk through specialized Internet of Things (IoT) security testing and threat monitoring.

INDUSTRIAL SECURITY. Monitor and manage your organization's cyber risks for industrial and operational technology through purpose-fit security assessment and threat monitoring.

SECURITY ANALYTICS AND DETECTION. Utilize our next generation, risk-based threat detection managed service, leveraging behavior analytics, machine learning and real-time threat-hunting; or build and enhance your own solution.

INCIDENT RESPONSE. Design, implement and continuously improve your Computer Emergency Response Team (CERT) capabilities to rapidly identify incidents, contain damage, eliminate an attacker's presence, and securely recover. Provide flexible assistance with managing and responding to security incidents.

Secure Cloud Adoption

With a risk-based security architecture at the center of your design processes, you can adopt advanced cloud platforms with confidence, unlocking the value of mobility, analytics, collaboration, capacity and flexibility. A well-planned approach to cloud adoption and integration will significantly reduce the risks of integrating legacy systems.

We guide your organization to plan, implement and run a secure cloud solution to:

CHANGE

Adoption of cloud platforms and Software as a Service (SaaS) is an integral part of many organizations' digital transformation initiatives. While securely adopting and integrating new cloud capabilities, companies will concurrently continue to support their existing platforms. While this may include developing a multi-cloud strategy, designing a hybrid mission critical customer support platform, or implementing IoT edge computing, we help businesses effectively adopt and secure cloud platforms within their enterprise technology portfolio.

OPTIMIZE

Secure and agile cloud services are powerful tools, enabling new service models for businesses on a digital transformation journey. Whether your firm is a cloud native or wrestling with bimodal IT, we can help architect and design security into your solutions.

OUR CLOUD ADOPTION SERVICES

CLOUD SECURITY. Enable your team with the leading cloud security practices to help your organization reduce risk across IT environments. We support your organization to improve critical areas such as server hygiene, secure communication, security policy optimization leading to improved security posture.

ENTERPRISE CLOUD ADOPTION. Simplify challenges by securely integrating existing IT systems with cloud services. We provide improved security controls by designing and implementing secure networks, improving identity management and utilizing cloud automation to remove inconsistencies across operations.

HYBRID INFRASTRUCTURE. Optimize and accelerate enterprise IT capability to provide services to customers. We enable your organization to seamlessly manage IT regardless of the service location (on premise, hybrid or cloud). We help to improve cost efficiency by utilizing the latest cloud services to provide business continuity and disaster recovery.

Our Service Types

We offer flexible engagement models to match your unique needs and requirements:

CONSULTING SERVICES

Our core expertise is the provision of consulting services that span across all service categories and service lines—from designing and architecting enterprise cybersecurity programs to full integration and implementation services. Encompassing strategy, people, processes and technology, our consulting services empower your organization to embrace a digital transformation journey with confidence.

TESTING SERVICES

Our testing services—for example, vulnerability assessments, penetration testing, application security testing—help your organization take your security program to the next level. By auditing your processes, documents and infrastructure against industry best practices and international standards, we strengthen your defenses and protect critical data, customer information and key investments.

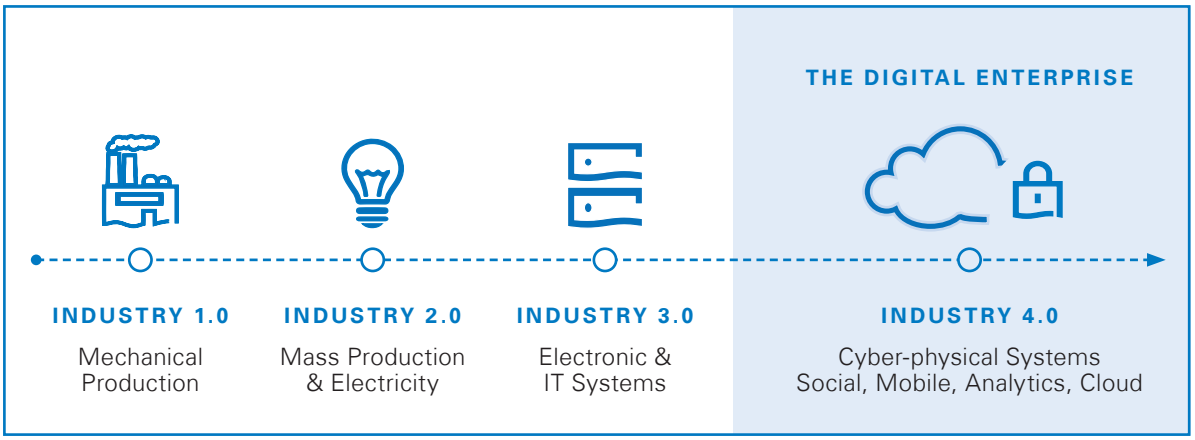
MANAGED SERVICES

Our managed services help your organization simplify information technology management and minimize operational challenges. Offering a flexible sourcing model, we support the varying demands of our clients. We go beyond traditional managed services with integration and automation services, leveraging best-in-class technology. With the integration of security operations and risk management, we help to better manage risks and improve incident response time.

Our Deep Industry Expertise

TÜV Rheinland's 145+ year heritage gives us a deep understanding of the markets we serve, with unmatched depth of experience solving complex safety, security, data privacy, and infrastructure challenges. Global enterprises spanning product manufacturing, automotive, financial services, health care and much more rely on our best-in-class capabilities to secure their critical assets and to thrive in the digital era.

Expertise for Worldwide Industry Challenges



Functional Safety Meets Cybersecurity

As the fourth industrial revolution gains more momentum there is an increasing need to consider the often disparate worlds of functional safety and cybersecurity together. TÜV Rheinland combines unmatched experience in functional safety and cybersecurity with industrial expertise.

A Deeper Look Into Our Industries

AUTOMOTIVE

As the industry moves toward the age of autonomous vehicles, car manufacturers need to ensure that their connected cars are properly secured. With our robust security services, we support the full automotive cybersecurity lifecycle, addressing cybersecurity at the products manufacturing stage all the way to on-going vehicle maintenance.

DISTRIBUTION

Distribution is a crucial part of the supply chain process, which is increasingly becoming connected and managed on-demand. Any compromise in the supply chain related to information validation, or payment processing, can result in costly delays and failed return on investment. It is not surprising that the global supply chain is the second most attacked industry.

ENERGY

We ensure the on-going safety of energy resources and help energy providers minimize risks to property and assets. From increasing your situational awareness and identifying vulnerabilities to optimizing practices and processes to detect outsider attacks and terrorist events, our team of experts are here to help you maintain sustainable energy production and distribution.

FINANCIAL SERVICES

The increasingly intricate attacks on the financial services sector put the industry in continuous need to drive more sophisticated and tested solutions that address risk as well as close scrutiny of compliance with growing regulations and new stringent levels of governance. We provide the experience and methodologies to identify potential threats and vulnerabilities, and offer tested ways of mitigating the risks to banks and financial institutions.

HEALTHCARE

Modern day healthcare needs regulation that emphasizes the sharing of information as much as safeguarding privacy. There is tremendous value to disease diagnosis and treatment delivery through digital transformation. Our experts take a holistic approach, assisting organizations from hospitals to pharmaceutical companies to insurance. We have tailored our approach for risk, compliance, identity management, monitoring and many other services to serve the unique needs of healthcare.

MANUFACTURING

Manufacturing is becoming smarter and more connected, therefore becoming increasingly susceptible to cyberattacks. We provide comprehensive risk assessment and testing to ensure that your manufacturing operations are not disrupted and your intellectual property remains intact.

RETAIL

As an international retailer, you want the goods you offer your customers to be safe and of superior quality. Our team of experts has the technical know-how to help you identify and mitigate cybersecurity risks at every stage of the product production, distribution and customer delivery process.

TELECOMMUNICATIONS

With the increasing pace of digitalization and scale of cyberattack sophistication, protecting corporate and personal communication is becoming ever more important. Our cybersecurity experts offer comprehensive cyber risk assessment and threat management solutions to help you protect telecommunication data, assets and networks.

Note: this is only an excerpt - we cover all industries.

Why TÜV Rheinland?

TÜV Rheinland, founded 145 years ago, is a global leader in independent inspection services with more than €1.9 billion in annual revenue. The group employs 20,000+ professionals across 70 countries, with native speaking experts, spanning the Americas, EMEA and APAC.

Our independent experts stand for quality and safety of people, technology and the environment in nearly all industrial sectors and areas of life. TÜV Rheinland inspects technical equipment, products and services, and oversees projects, processes and information security for companies. Our experts also train people in a wide range of careers and industries.

Our company operates a global network of approved labs, testing and education centers. Since 2006, TÜV Rheinland has been a participant of the United Nations Global Compact to promote sustainability and combat corruption.

WE SUPPORT
UN GLOBAL COMPACT

About TÜV Rheinland ICT & Business Solutions

For nearly 20 years, TÜV Rheinland has been supporting enterprises of all sizes and sectors with comprehensive consulting and solutions expertise in IT, cybersecurity and digital transformation processes. With specialists available around the world, ICT & Business Solutions provides strategic advisory, consulting, design and process optimization services by implementing, testing, monitoring, managing, or certifying products, systems and solutions with the mission to enable a secure and safe digital future.

Start your Digital Enterprise. Protected. journey with us today! To find out more, visit our website at **www.tuv.com/informationsecurity**.

® TÜV, TUEV and TUV are registered trademarks. Utilisation and application requires prior approval. April 2018

TÜV Rheinland
ICT & Business Solutions
cybersecurity@tuv.com

www.tuv.com/informationsecurity

TÜVRheinland®
Precisely Right.