



TÜV SÜD Cybersecurity Services

Enhance Industrial Cybersecurity

Add value.
Inspire trust.



Cybersecurity should be a priority for every company

Companies want to take advantage of the increased efficiencies, high flexibility and cutting-edge innovation that digitization brings. However, to their detriment, many companies have not taken the threat of internet-based attacks seriously enough. An incident involving malware or ransomware can halt business within minutes and cost an organization thousands of dollars to rectify. And the reputational damage of an IT security breach, especially if it involves personal customer data, is devastating.

Why invest in cybersecurity?

Companies cannot just rely on the basic level security tools delivered with IT infrastructure and software. Today, cyber-attacks are more sophisticated, targeted and effective than ever before. A holistic and overarching approach is needed to ensure the highest levels of cybersecurity; an approach that not only secures physical infrastructure, IT hardware, and applications, but also educates and empowers employees to ensure any cybersecurity threats are minimized or even eliminated.

Investing in cybersecurity infrastructure, having corporate cybersecurity policies and certification, as well as promoting employee awareness, allows companies to proactively minimize threats. By protecting customer data, corporate intellectual property and essential infrastructure, companies can plan the digitization of their business with confidence and take full advantage of the opportunities that await.

Cybersecurity specifically tailored to your industry needs

TÜV SÜD's experts are specialists in cybersecurity advisory, assessment, training, audit, and certification. From cyber risk assessments and cybersecurity training, to carrying out security certification projects, our industry experts have successfully helped companies to improve their cybersecurity. With a structured approach to cybersecurity services developed from many years of experience, domain specific know-how and regulatory expertise, TÜV SÜD offers support to companies across a range of sectors. By helping organizations with compliance to global security standards, TÜV SÜD has ensured our clients have access to markets across the world.

Our services

Cybersecurity and data protection are one of our core capabilities, from risk analysis to safety hazard avoidance, TÜV SÜD always provides comprehensive services at every step of your business life.

Assessment and testing

As an independent third-party testing and certification organization, the TÜV SÜD team have expertise in data regulations and product cybersecurity in specific markets, as well as a deep understanding in the field of cyber threats. The TÜV SÜD team of experts cooperate with customers around the world to fully realize their digital operations.



Data protection assessment service

- EU-General Data Protection Regulation (GDPR) Compliance Service
- Personal Information Protection Law (PIPL) Compliance Service
- Supply Chain Information Security Audit
- Data Protection Impact Assessment (DPIA)
- Cyber Security Law (CN-CSL) compliance services
- Data Security Law (CN-DSL) Data exit security assessment
- External Data Protection Officer Service/ Data Protection Coordinator
- Service Organisation Control (SOC) Reporting Service



Testing

- Web & Application Penetration testing (OWASP/CWE)
- Consumer IoT Products Penetration testing (OWASP)
- Medical Devices Penetration Testing
- IoV (Internet of Vehicle) Penetration Testing
- Infrastructure Penetration Testing
- Mobile Application Security Analysis
- End Point Security Analysis
- Simulated Phishing Email Attack Service
- Industrial Control Equipment Penetration Testing
- Intelligence Lift System Penetration Testing
- Battery Energy Storage System Penetration Testing



Automotive cybersecurity

- Automotive cybersecurity management system assessment (CSMS certification and ISO/SAE 21434 process and product certification)



Railway applications cybersecurity

- Provide IEC 62443 and TS 50701 assessment for asset owners, service providers, and product integrators (including Signaling and Rolling Stock)



Consumer IoT products market access

For the consumer IoT products market, some countries have issued relevant mandatory laws and regulations on cybersecurity, and some regulations have been included as part of mandatory certification. TÜV SÜD provides customers with the following cybersecurity compliance services in regional markets such as:

- Brazil cybersecurity assessment
- India cybersecurity assessment
- Japanese market access certification
- Singapore market access certification
- UK market access assessment
- EU market access assessment
- North America cybersecurity assessment
- Latin America cybersecurity assessment



Industrial cybersecurity

- Industrial communication networks security: IEC 62443
- Smart Industry Readiness Index Assessment
- Risk assessment based on machinery regulation
- Energy smart appliances –Demand side response operation – Code of practice
- Distributed Energy Resources – Cyber Security Connection Guidance Training and Assessment
- Industrial cyber security training, gap analysis
- Cybersecurity Assessment Related to the Functional Safety Lifecycle



Training

With increased digitization, there is a potential increase in the opportunities for cyber-attacks. That's why every company needs to take cybersecurity seriously and invest in measures to defend both their physical and intellectual property. To guarantee the best possible level of protection, digital security should be "built in" to every product, underlying business processes and at every organizational level, including global supply chains. By creating effective, secure barriers against threats and attacks, companies can win the battle against cyber risks. Investing in cybersecurity gives organizations a competitive advantage and enables them to be market leaders in their respective industries. TÜV SÜD provides companies with the following cybersecurity related training:

- [Industrial Cybersecurity Foundation \(Level 1\) according to IEC 62443](#)
- [Industrial Cybersecurity Professional IEC 62443 Training](#)
- [ISO/IEC 27001 Awareness Training](#)
- [ISO 27001:2022 ISMS Lead Auditor Training \(Exemplar Global Certified\)](#)
- [ISO/IEC 27001: 2022 Information Security Management System \(ISMS\) Internal Auditor Training](#)
- [ISO/IEC 27001/27002 Update Training](#)
- [ISO/IEC 27001: 2022 Information Security Management System \(ISMS\) Lead Implementer Training Program](#)

We are also offering an early bird discount. Plan ahead and secure a 15% discount by registering at least 90 days in advance!*

Certification

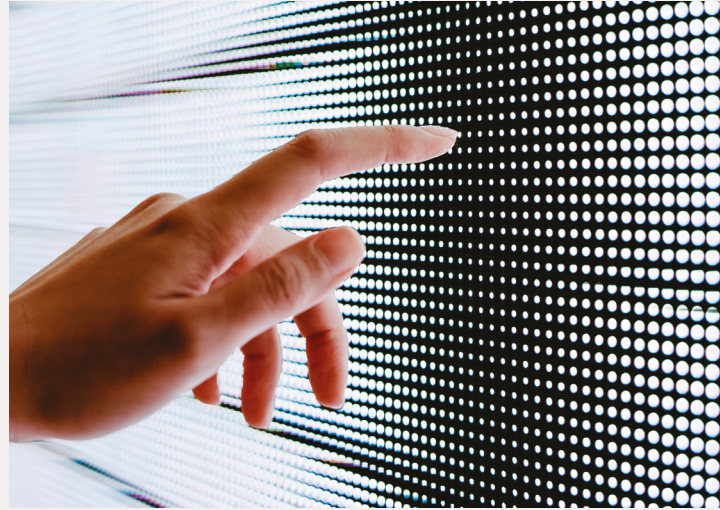
Various certification services provided by TÜV SÜD are based on a series of internationally accepted standards, technical reports and technical specifications that provide a systematic approach for assessing and mitigating current and future cybersecurity risks in each aspect of an industrial control system. Based in part on the principles found in several different national cybersecurity standards, the IEC 62443 series provides a clear yet flexible framework that is equally applicable in discrete and process-oriented manufacturing. TÜV SÜD provides companies with the following cybersecurity related certification:

- [Europrivacy Certification \(GDPR Certification\)](#)
- [ISO 21434 & ISO 24089 Regulatory Compliance](#)
- [ISO/IEC 27701 Privacy Information Management Certification](#)
- [ISO/IEC 27001 Information Security Management Certification](#)
- [TISAX Assessment](#)
- [IEC 62443 Industrial Cyber Security Certification](#)
- [ISO/IEC 27017 Implement robust information security controls to safeguard cloud services](#)
- [ISO/IEC 27018 Enhance cloud security for personally identifiable information](#)
- [ISO 22301 Business Continuity Management System](#)
- [ISO/IEC 20000 IT Service Management](#)
- [CSA star](#)



*The early bird discount cannot be combined with any other promotions.

Industrial Cybersecurity services



TÜV SÜD cybersecurity experts can provide on-site risk assessment services across industries including Manufacturing, Power & Utilities, Automotive and more.

Examples of services TÜV SÜD's panel of experts can provide are as follows:

- ICS/OT Risk Assessment (10 Stage) – On-site for industrial cybersecurity
- ICS/OT Risk Assessment (5-Stage) – On-site for industrial cybersecurity
- Industrial Cyber Insurance Risk Assessment – For industries, underwriters and insurance companies
- NERC CIP Compliance Training - for Bulk Electric System (BES) companies

Automotive Cybersecurity

- ISO/SAE 21434 – Cybersecurity Management System (CSMS)

Critical Infrastructure Protection (CIP) for BES Companies

North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP) is a set of stringent standards designed to secure the assets required for operating North America's Bulk Electric System (BES). These standards must be followed by BES owners, operators, and users.

- NERC CIP Compliance Assessment
- NERC CIP Training
- NERC CIP Advisory Services

Industrial Automation Control Systems (IACS) Cybersecurity

IEC 62443 is an international series of standards developed by the International Electrotechnical Commission (IEC) to address cybersecurity for industrial automation and control systems (IACS). These standards provide a comprehensive framework for securing operational technology (OT) environments, which include systems used in industries such as manufacturing, energy, and transportation.

IEC 62443-2-4 – For IACS service providers

- IEC 62443-4-1 – For IACS Component (Secure product development lifecycle)
- IEC 62443-4-2 – For IACS Component (Technical Security requirements)
- IEC 62443-3-3 – For IACS System (System security requirements)

Add value. Inspire trust.

TÜV SÜD is a trusted partner of choice for safety, security and sustainability solutions. It specializes in testing, certification, auditing and advisory services. Since 1866, the company has remained committed to its purpose of enabling progress by protecting people, the environment and assets from technology-related risks. Through more than 28,000 employees across over 1,000 locations, it adds value to customers and partners by enabling market access and managing risks. By anticipating technological developments and facilitating change, TÜV SÜD inspires trust in a physical and digital world to create a safer and more sustainable future.

Enabling access to markets across the globe

Over 1,000 TÜV SÜD global locations

With an extensive network of multidisciplinary experts, accredited laboratories and offices established in the world's major business hubs and key production centers, we are ready to support your need for safety, security and sustainability wherever you do business throughout North America, Canada, Mexico, South America and the Caribbean.

As well as:

Germany (HQ)
Argentina
Austria
Bahrain
Bangladesh
Belgium
Bosnia &
Herzegovina
Brazil
Canada

China
Croatia
Czech Republic
Denmark
Egypt
Finland
France
Hungary
India
Indonesia

Italy
Japan
Malaysia
Mexico
Netherlands
Norway
Oman
Philippines
Poland
Portugal

Qatar
Romania
Saudi Arabia
Singapore
Slovakia
Slovenia
South Africa
South Korea
Spain
Sweden

Switzerland
Thailand
Turkey
UAE
United Kingdom
United States
Vietnam

Transform your business today with TÜV SÜD

tuvsud.com/en-us

America Headquarters

TÜV SÜD America Inc.
401 Edgewater Place,
Suite 500
Wakefield, MA 01880
United States of America
+1 978 573 2500
tuvsud.com/en-us