Greater China

Add value.
Inspire trust.

Cybersecurity and data protection one-stop service

TÜV SÜD Greater China

Choose our professional team

With the rapid increase in the number of Internet of Things products, cybersecurity attacks on Internet of Things products have also increased exponentially. Consumers and international buyers are paying more and more attention to the security of the IoT device. Governments in various regions are scrambling to formulate and publish IoT security and data protection regulations. Enterprises need to urgently solve issues related to product security, meeting regulatory requirements, ensuring information security throughout the lifecycle of implementation, production, upgrading and monitoring.

Cybersecurity requirements for different scenarios in the market:

- Protect computer/network equipment from hackers
- Protect enterprise information from attackers/spies/competitors
- Protects personal equipment from the control of an adversary
- Protect personal privacy from malicious disclosure/collection
- Let human safely roam in the information world

Cybersecurity protection strategies for IoT devices in countries

Countries and organisations	Development	Our services
EU	In May 2018, the EU took the lead in mandating GDPR, the toughest Privacy Data Protection Act in history; In June 2019, EU cybersecurity act came into force, proposing to establish a framework for security certification of cyber products; In June 2020, EU officially published the technical security standard ETSI EN 303 645 for consumer electronics IoT products (based on TS 103 645); In September 2020, safety standard IEC 60335-1 ED6 Annex U for products in the appliance category	▪ ETSI EN 303 645 AoC and report (+ETSI TS 103 701) ▪ Finland cybersecurity label ▪ CSC certification mark ▪ IoT basic security inspection ▪ App assessments ▪ GDPR compliance assessment ▪ Data protection awareness training ▪ Data Protection Impact Assessment (DPIA) ▪ Vulnerability Scans and Penetration Tests (VAPT) ▪ Commercial Transaction Security (CTS) services ▪ Simulated phishing email attack service ▪ Supply chain information security audit
UK	In 2018, code of practice for consumer IoT devices; In 2019, the UK DCMS issued a statement about plans to develop mandatory regulations for the security of consumer electronics IoT products; In 2020, The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU exit) Regulations 2020.	▪ UKCA certification ▪ Data protection compliance assessment ▪ Data protection awareness training ▪ Data Protection Impact Assessment (DPIA)
Finland	In November 2019, Finland released its cybersecurity labeling system, becoming the first European country to issue cybersecurity labels to smart devices.	▪ ETSI EN 303 645 AoC and report ▪ Finland cybersecurity labels (testing and application)
USA	In January 2020, California Act - CA SB 327 and AB 1906, and Oregon Act HB2395 were mandated. In December 2020, the United States released H.R. 1668 - the Internet of Things Cybersecurity Improvement Act.	▪ Test report (based on TÜV SÜD PPP 17003: Operating procedures for NISTIR 8259:2020) ▪ Cybersecurity test for IoT products ▪ Vulnerability scans and penetration tests ▪ App assessments
Singapore	In October 2020, IMDA Singapore issued the Technical Specifications IMDA TS RG-SEC for Security Requirements for Residential Gateways; By October 12, 2021, all relevant residential gateways on the market must meet the relevant requirements.	▪ IMDA TS RG-SEC assessment and registration ▪ CLS label application ▪ Singapore market access certification
Japan	In April 2020, MIC Japan began mandating T. Business Act Amendment 34.10. Cybersecurity requirements were proposed for products, such as routers and webcam.	▪ Router/Webcam product MIC Amendment 34.10 evaluation report ▪ Japanese market access certification
Brazil	In July 2021, Act on Minimum Cybersecurity Requirements for Telecommunications Equipment in Brazil (Act 77/2021) will be mandated.	▪ Brazilian compliance with cybersecurity ▪ Brazilian market access certification

Europe

Security standards for consumer IoT devices

European Telecommunications Standards Institute (ETSI), officially published the standard ETSI EN 303 645 (V2.1.1) in June 2020 which aimed to address the most important and widespread security issues. It has established a security baseline for Internet-connected consumer products that can safeguards user privacy, protect against basic attacks on fundamental design flaws and provide the basis for future IoT certification schemes. The technical standard covers security requirements for devices, communications, and personal data protection.

Applicable product scope

This certification applies to consumer IoT products, including but not limited to: smart home/household appliances, consumer electronic robots, smart wearable devices, surveillance devices, such as cameras, networking device, smart camera, consumer electronics.

Many countries adopted ETSI EN 303 645

01

In November, 2019 Finland

Finland launched the first European cybersecurity label

02

In March, 2020 Singapore

Singapore launched the first cyber security label scheme in the Asia-Pacific region

03

In January, 2021 Brazil Anatel

Brazil Anatel issues an act on minimum cybersecurity requirements

04

UK

UK plans to implement mandatory cybersecurity requirements for consumer IoT products

These cybersecurity acts and plans cite references to the technical standard ETSI EN 303 645 to ensure that IoT products meet design security requirements and boast basic information security features.

CSC Certification Mark:
TÜV cybersecurity certification for consumer IoT products

With the rapid development of various information and communication technologies, the demand for smart home systems have grown significantly. This provides significant opportunities for importers, distributors and manufacturers of smart home products. In this future-oriented market, trust is a key factor for success. If smart home solutions are to gain acceptance, it is essential to always ensure that user data is protected and secured. Ensuring information security throughout product lifecycle and guaranteeing the cybersecurity of IoT products and systems are major issues confronting the enterprises.

Applicable product scope

This certification applies to consumer IoT products, including but not limited to: smart gateway/router, smart home/household appliances, personal health equipment, connected children's toys, smart wearable devices, networked devices and consumer electronic products, monitoring equipment, HVAC refrigeration equipment and other Internet-connected products.

CSC Certification Mark

TÜV Cybersecurity Certification Mark

Classification of certification levels

Three levels of certification are available:
- Basic
- Substantial
- High

Assessment of certification scope

The certification scope involves products, processes, and clouds. The higher the certification level, the wider the scope of certification.

Evaluation of development process

In addition to product testing, product development process is evaluated, and development process must include a vulnerability management process, etc.

Based on international standards

Based on internationally recognised standards (including ETSI EN 303 645)

EU-General Data Protection Regulation (GDPR) compliance service

The EU legal framework on data protection has been driving up the cost of processing personal data by organisations. For instance, EU-General Data Protection Regulation (GDPR), aimed at improving the protection of personal data, came into force on 25 May 2018. Organisations need to ensure compliance to the regulation.

Ensure compliance for your organisation

The introduction of the GDPR requires that organisations review existing data management systems and create numerous new processes. In addition, existing business operation models, checklists and contractual documents must be revised, and technical and organisational measures must be adapted. For example, organisations will need to deploy new systems to support the privacy risk assessments required by the GDPR.

Scope and target: GDPR does not only apply to organisations established within EU. As long as your organisation provides goods/services to EU residents or monitors the activities of EU residents, your organisation shall comply with GDPR.

Compliance risks: Organisations that fail to comply with GDPR face fines of up to 20 million Euros or 4 percent of their global annual turnover, whichever is higher.

Personnel awareness: Each and every personnel in your organisation need to take measures to ensure GDPR compliance. You should ensure that the decision makers and key personnel in your organisation are aware of the potential significant implications of GDPR and are able to identify the compliance issues resulting from GDPR.

Privacy by design and by default: The approach ensures that organisations consider privacy and data protection issues at the design phase of any system, service, product or process and then throughout the lifecycle. In the meantime, the privacy settings contributing to data protection should apply by default. For instance, data pseudonymisation and encryption are appropriate safeguards.

Risk assessment: A detailed risk assessment is required by GDPR in some cases before data processing is implemented. The Data Protection Impact Assessments (DPIAs) service we offered can help organisations to mitigate risks.

USA

IoT device privacy protection and cybersecurity act

California, USA: Connected Device Information Privacy Protection Act

- SB-327 Information Privacy: Connected Devices
- AB-1906 Information Privacy: Connected Devices

Oregon, USA: Connected Devices Information Privacy Protection Act

- Act HB2395

Implementation

1. This law requires devices to provide effective protection for the devices and the information stored therein, to prevent unauthorised control/theft, alteration and release. Each device which may have access to public networks must have unique default password or have been through security initialisation.
2. After January 1, 2020, all connected products sold in the California and Oregon states shall be security hardened as required.

Coverage

1. Connected products sold in the California area
2. Targeted at product manufacturer and designer

Internet of Things Cybersecurity Improvement Act

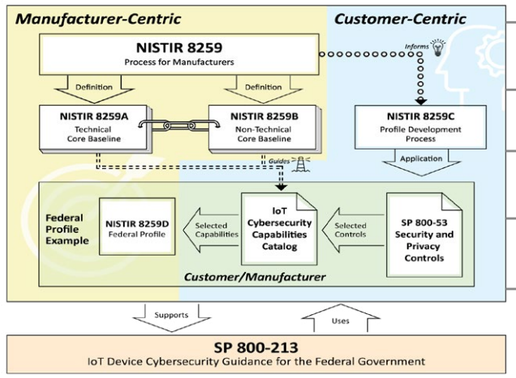
- Act H.R. 1668: Internet of Things Cybersecurity Improvement Act. On December 4, 2020, the President signed into law "the Internet of Things Cybersecurity Improvement Act", which requires the National Institute of Standards and Technology (NIST) to issue standards, and guidance for the federal government's use of IoT devices and directs the White House Office of Management and Budget (OMB) to review government policies to ensure that they comply with NIST guidance and that federal agencies will not be allowed to purchase IoT devices that do not meet security requirements.

NISTIR 8259 Series Standards

The National Institute of Standards and Technology (NIST) has released NISTIR 8259 series of standards designed to help manufacturers of IoT devices establish core benchmarks for cybersecurity activities and cybersecurity capabilities. These standards are helpful in meeting the challenges posed by the U.S. Internet of Things Cybersecurity Improvement Act, and increases consumer confidence in the security of information about IoT products.

Applicable product scope

This certification applies to consumer IoT products, including but not limited to: smart home/household appliances, consumer electronic robots, smart wearable devices, smart city products, network equipments and consumer electronics, monitoring devices, HVACR equipment and other connected products.



NISTIR 8259
Foundational Cybersecurity Activities for IoT Device Manufacturers

NISTIR 8259A
IoT Device Cybersecurity Capability Core Baseline

NISTIR 8259B Draft
IoT Non-Technical Supporting Capability Core Baseline

NISTIR 8259C Draft
Creating a Profile Using the IoT Core Baseline and Non-Technical Baseline

NISTIR 8259D Draft
Profile Using the IoT Core Baseline and Non-Technical Baseline for the Federal Government

Singapore

IMDA TS RG-SEC and CLS Label

IMDA TS RG-SEC

IMDA released the technical standard IMDA TS RG-SEC in October 2020, which requires residential gateways or home routers (RGS products) to obtain CLS Label, as well as registering for IMDA wireless communications certification. From October 12, 2021, CLS and IMDA will be mandatory for all RGS products listed.

Applicable product scope

Residential gateways, home routers.

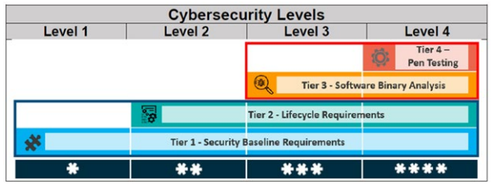
CLS Label

CLS (Cybersecurity Labelling Scheme) is a cybersecurity labelling scheme for smart home devices developed by the Cyber Security Agency of Singapore (CSA), with labels divided into four levels. The aim is to indicate the cybersecurity level of household appliances and smart home devices, and there are plans to promote the standard internationally.

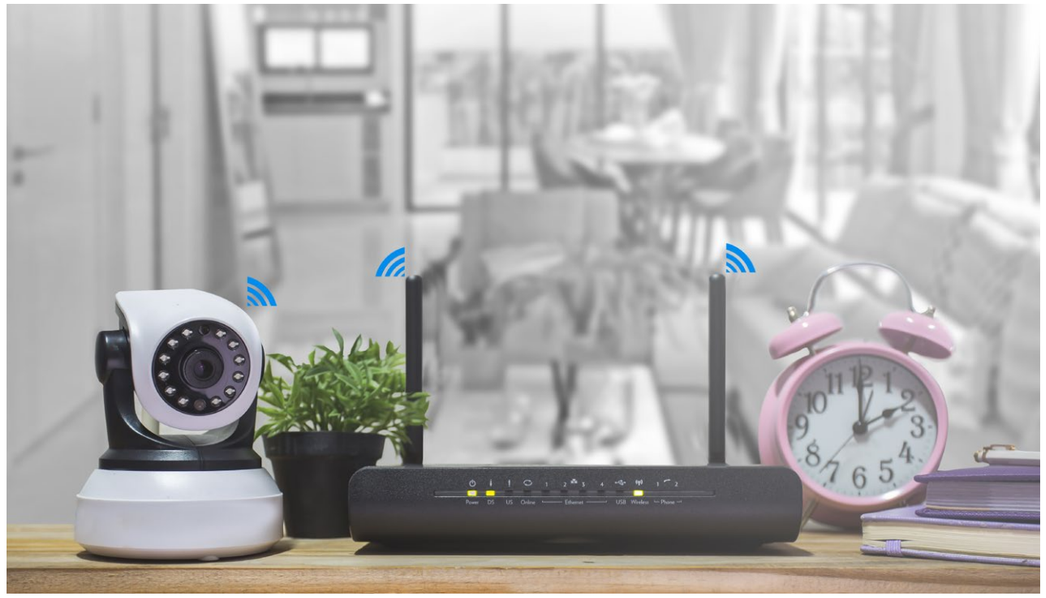
Applicable product scope

Smart home devices. The CLS was first introduced to cover Wi-Fi routers and smart home hubs.

CLS Label



CLS 4 levels of Cybersecurity



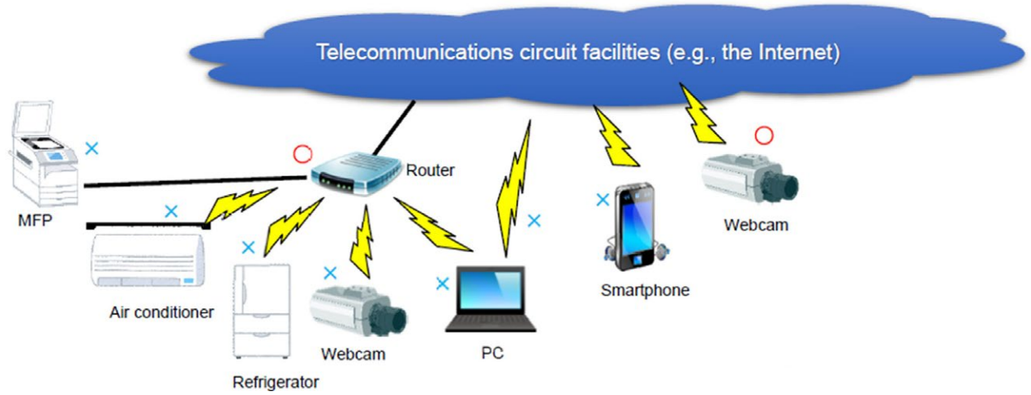
Japan

Market access regulation (MIC Amendment 34.10)

On April 1, 2020, MIC Japan began enforcing T. Business Act Amendment 34.10, which imposes cybersecurity requirements on routers/Webcam products.

MIC-Article 34-10 applicable product scope

Dedicated communication line equipment terminal and uses the Internet protocol and can change telecom settings.



China

Cybersecurity requirements for home smart gateways

Voluntary assessment

"Technical Requirements for Security of Smart Gateway Devices": TAF-WG9-AS0040-V1.0.0 2019. This standard includes technical requirements for security of smart gateway devices and hierarchical security requirements. It specifies the security technical requirements for intelligent gateway devices in terms of device hardware, system software, business functions, network management, application software, etc. Concerning the degree of security capabilities supported in different application scenarios and smart gateway devices, the device security capabilities are divided into three levels from low to high.

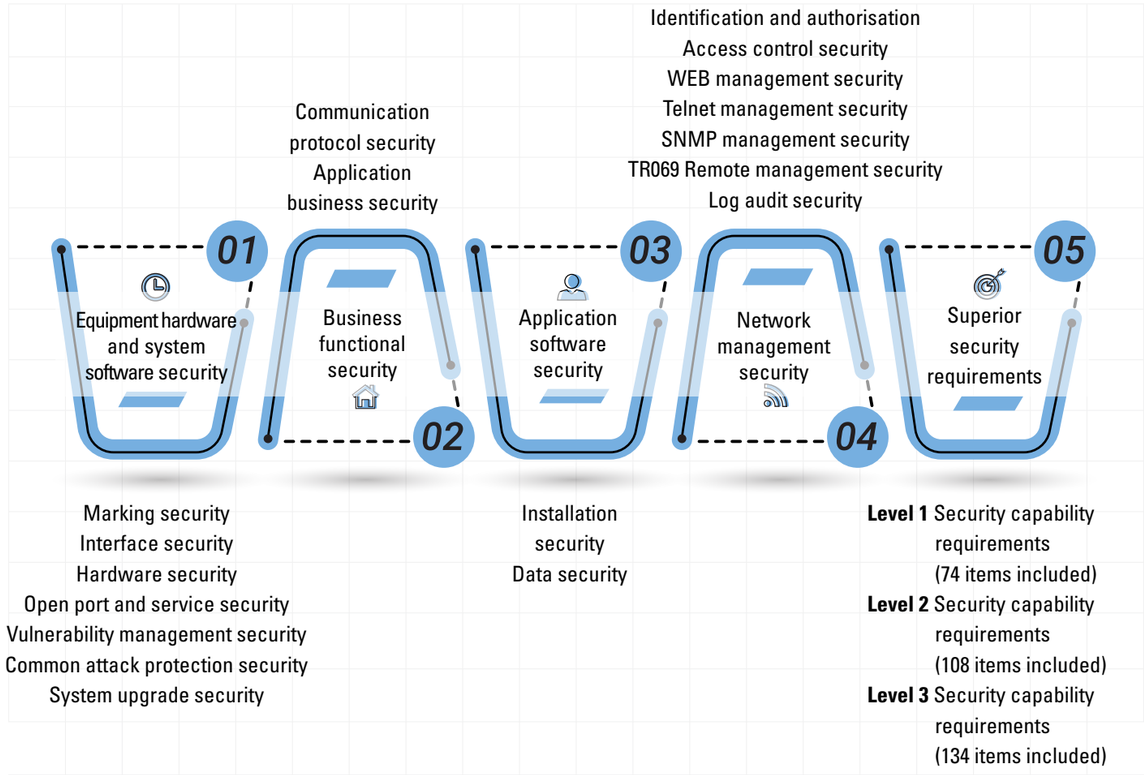
Applicable product scope

Smart gateway devices, home/office routers

Certification and test basis

- PPP: CCB03121A:2019Rev.0
- Test method: TAF-WG9-AS0040-V1.0.0 2019 "Technical Requirements for the Security of Smart Gateway Devices"

Core technical requirements



Our services

We offer test report and certificate joint certification by CTTL and TÜV SÜD

Penetration test

Referring to the 2019 cybersecurity statistics, ransomware attacks every 14 seconds. According to the 2019 assessment report, companies are subject to ransomware attacks every 14 seconds. In fact, serious and Destructive Cyber-Attack not merely of ransomware, following Denial-of-Service (DoS) and Distributed Denial-of Service (DDoS) attacks. Considering that cyber-attacks affect the retail, medical, and automotive industries. Whereby, the industries should be increased the awareness on the cybersecurity protection. In addition, the usage of computer technology in the company (includes hardware and software) should consider cybersecurity protection. With reference to national standards, related industries must determine vulnerability in computer technology product design through penetration testing.

Our services are based on international cybersecurity standard, for example:

- Testing Internet Web portal and intranet web applications in order to avoid insufficient authentication/authorisation and privacy concerns.
- Testing insecure network services, cloud infrastructure and/or mobile application.
- Test scope includes detection of insufficient security control and misconfiguration.
- Conducting vulnerability assessment and penetration test on server, network and workstation environment.
- Cybersecurity incident management - assisting clients in conducting forensic investigations and providing remediations thereafter.

Related services

TÜV SÜD provides the following related services:

- Market access:
  - Brazil cybersecurity assessment
  - India cybersecurity assessment
- Simulated phishing email attack service
- Commercial transaction security:
  - PCI DSS
  - PCI PA-DSS
  - ASV - Approved Scanning Vendor (merchant portal) website compliance
  - S@ferShopping
- Industrial security:
  - Industrial communication networks security: IEC 62443
  - Smart Industry Readiness Index Assessment

Greater China

For a one-stop service provider of German expertise in Greater China please contact us:

www.tuvsud.cn
info.cn@tuvsud.com

Add value. Inspire trust.

TÜV SÜD is a trusted partner of choice for safety, security and sustainability solutions. It specialises 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 25,000 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.

Our branches in Greater China:

TÜV SÜD Greater China Headquarters Shanghai
3-13, No.151 Heng Tong Road,
200070, Shanghai
Tel.: +86 021 6141 0123

Shanghai Testing Center
Tel.: +86 021 6037 6300
Tel.: +86 021 6037 9100

Wuxi
Tel.: +86 510 8820 3737

Ningbo
Tel.: +86 574 2786 6658

Jinhua
Tel.: +86 579 8288 8708

Nanjing
Tel.: +86 025 8779 0058

Hefei
Tel.: +86 551 6537 8730

Taizhou
Tel.: +86 576 8966 1886

Suzhou
Tel.: +86 512 6809 5318

Chengdu
Tel.: +86 028 8592 0656

Hangzhou
Tel.: +86 571 8111 0758

Ningbo
Tel.: +86 574 2786 6658

Changzhou Battery Lab
Tel.: +86 519 8109 8308

Changzhou Rail Lab
Tel.: +86 519 8123 9872

Wuhan
Tel.: +86 027 8571 4927

Zhengzhou
Tel.: +86 371 5538 2208

Chongqing
Tel.: +86 023 8980 9513

Beijing
Tel.: +86 010 6590 6186

Tianjin
Tel.: +86 022 8319 2258

Qingdao
Tel.: +86 532 8503 0106

Qingdao Lab
Tel.: +86 532 8513 1716

Dalian
Tel.: +86 411 8230 4203

Shenyang
Tel.: +86 024 8668 5949

Changchun
Tel.: +86 431 8462 9833

Shenzhen
Tel.: +86 755 8828 6998

Shenzhen Guanlan Lab
Tel.: +86 755 3359 5385

Guangzhou
Tel.: +86 020 3832 0668

Guangzhou Testing Center
Tel.: +86 020 3817 0580

Xiamen Lab
Tel.: +86 592 7706 188

Xiamen Siming Office
Tel.: +86 592 7311 931

Dongguan
Tel.: +86 769 2168 7092

Changsha
Tel.: +86 731 8458 5815

Liuzhou
Tel.: +86 772 3858 696

Hong Kong
Tel.: +852 2776 1323

Hong Kong Lab
Tel.: +852 2443 3774

Taipei
Tel.: +886 2 2898 6818

Taichung
Tel.: +886 4 2486 3966

* Some of the services listed are provided due to local regulations only and may not be available in other regions. Please contact us for further details.