Huawei: Security Assurance and Transparency

-- Vision and Strategy

September 2020

Martin Portillo

Developing Future-Proof Capabilities In Security And Trustworthiness

Solid track record in cyber security and stable equipment operations over the past three decades

170+ countries and regions

1,500 telecom networks

3 billion people served

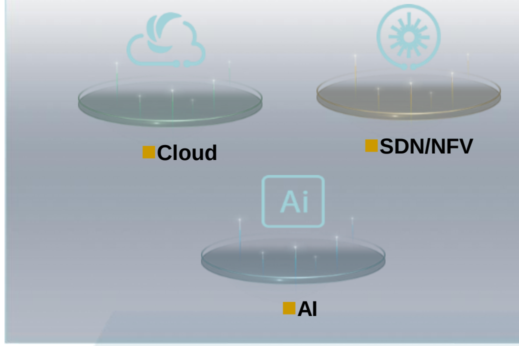
270+ product security certificates

Certificates for security management systems

Continuous investment

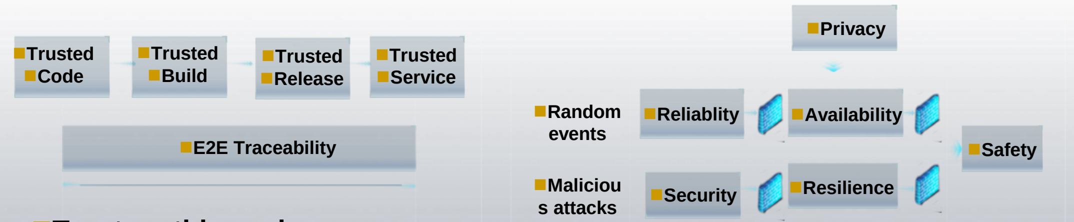
- 2,000+ full-time security employees
- 14 security research centers worldwide

New technologies bring new challenges



- Blurred boundaries for security protection
- More complex data processing; higher risk of data leakage
- Larger attack surface; vulnerabilities increasing

Trustworthiness = Trustworthiness in processes + Trustworthiness in results



Trustworthiness in processes:

From requirements and coding to loading and running

Trustworthiness in results:

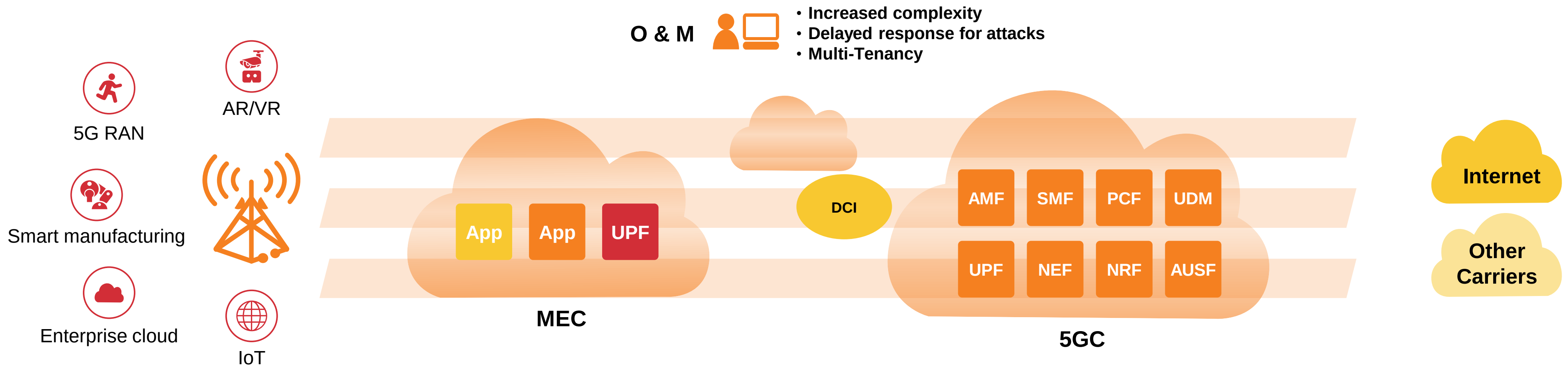
Cyber security + Privacy protection + Network resilience

Customer Requirements - Cyber Resilience

New Services (Vertical Industries)

Network Architecture Changes

Enhanced Attack Capabilities



- Increased complexity
- Delayed response for attacks
- Multi-Tenancy

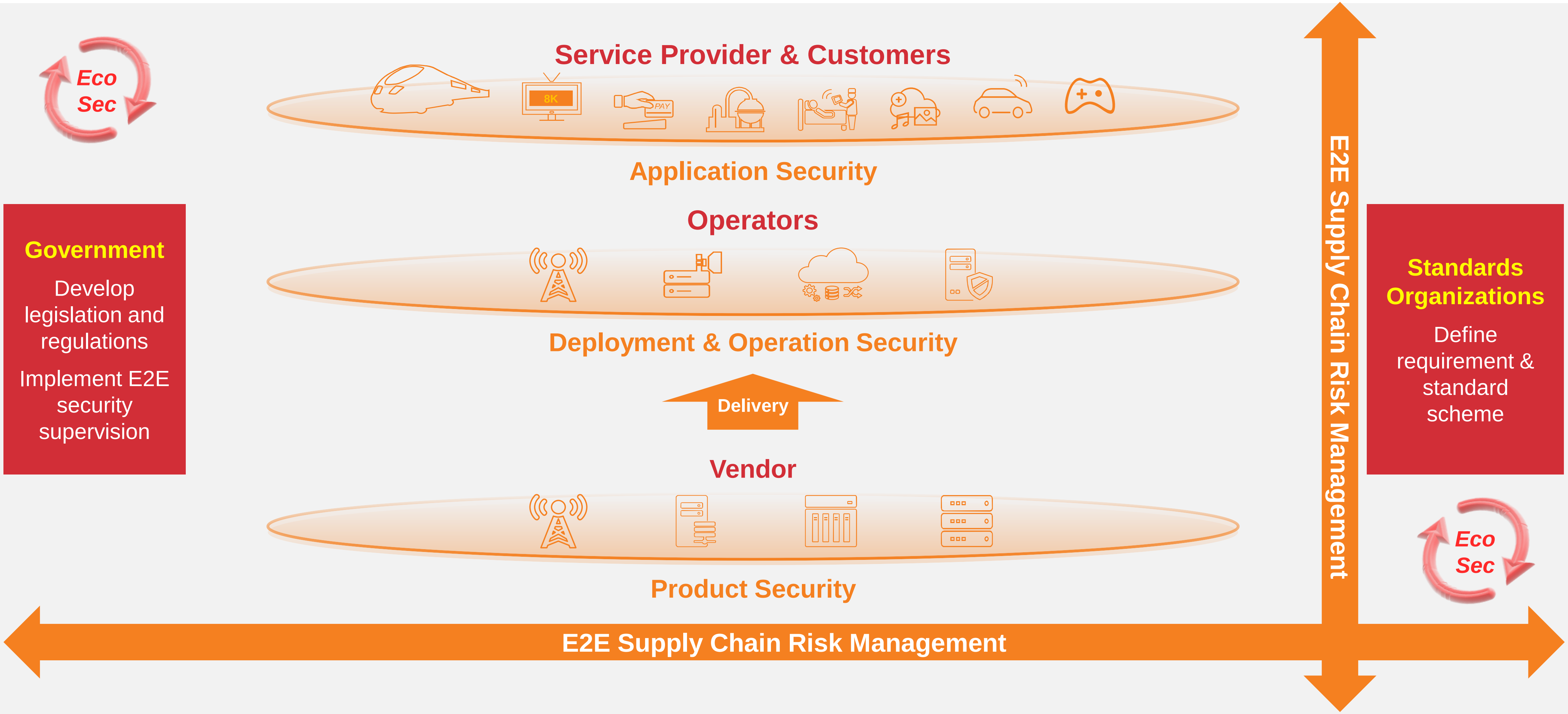
The Threat Landscape hasn't Changed

RAN Threats	Internet Threats	Roaming Threats	O&M Threats	Internal Risks in IP Bearer Network	Cloud-Based Threats	Threats from Mobile Edge Computing	Network Slice Threats	Inter-VNF Security Threats

… but the Attack Landscape has gotten larger!

SBA：Service Based Architecture

Security is a Shared Responsibility



Eco Sec

Service Provider & Customers

Application Security

Operators

Deployment & Operation Security

Delivery

Vendor

Product Security

Government

Develop legislation and regulations

Implement E2E security supervision

Standards Organizations

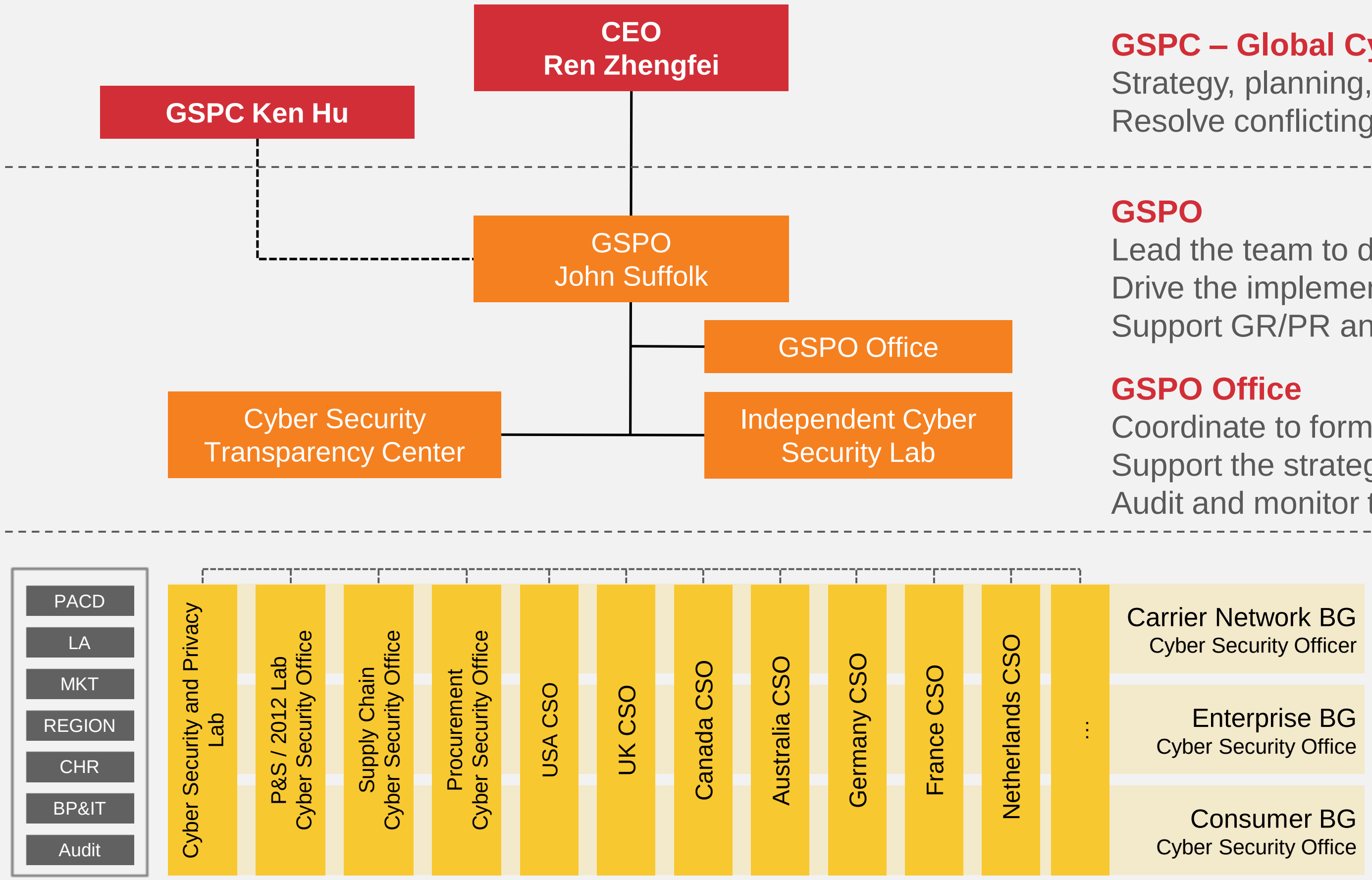
Define requirement & standard scheme

Eco Sec

E2E Supply Chain Risk Management

E2E Supply Chain Risk Management

Cyber Security and Privacy Governance



CEO
Ren Zhengfei

GSPC Ken Hu

GSPO
John Suffolk

GSPO Office

Cyber Security Transparency Center

Independent Cyber Security Lab

PACD
LA
MKT
REGION
CHR
BP&IT
Audit

Cyber Security and Privacy Lab
P&S / 2012 Lab Cyber Security Office
Supply Chain Cyber Security Office
Procurement Cyber Security Office
USA CSO
UK CSO
Canada CSO
Australia CSO
Germany CSO
France CSO
Netherlands CSO
…

Carrier Network BG
Cyber Security Officer

Enterprise BG
Cyber Security Office

Consumer BG
Cyber Security Office

GSPC – Global Cyber Security and Privacy Committee
Strategy, planning, policies, roadmap, and investment;
Resolve conflicting strategic priorities and audit.

GSPO
Lead the team to develop the security strategy;
Drive the implementation of cyber security assurance internally;
Support GR/PR and global accounts customers externally.

GSPO Office
Coordinate to formulate detailed operation;
Support the strategy & implementation;
Audit and monitor the implementation.

Region/BG/BU CSOs

Develop region/BU/BG cyber security strategy and planning, and drive the implementation;

Work with GSPO to identify changes to BG/BU/departmental processes to ensure the cyber security strategy and requirements are fully imbedded.

2000+ full-time security people

Huawei Cyber Security Journey

From product security to solution security

- First technical security specifications focused on product security
- R&D established the Network Security Solution Department

1999-2005

Establish security management in R&D

- Network Security Engineering Technology committee to construct security management system with R&D as the core.

2006-2009

Build and implement an E-2-E cyber security assurance system

- Global Cyber Security Committee (GCSC)
- Global Cyber Security & Privacy Officer (GCSO)
- Established Internal Cyber Security Lab (ICSL)
- Released CERT process
- Launched an E-2-E cyber security assurance system, including strategies, policies, processes, and baselines

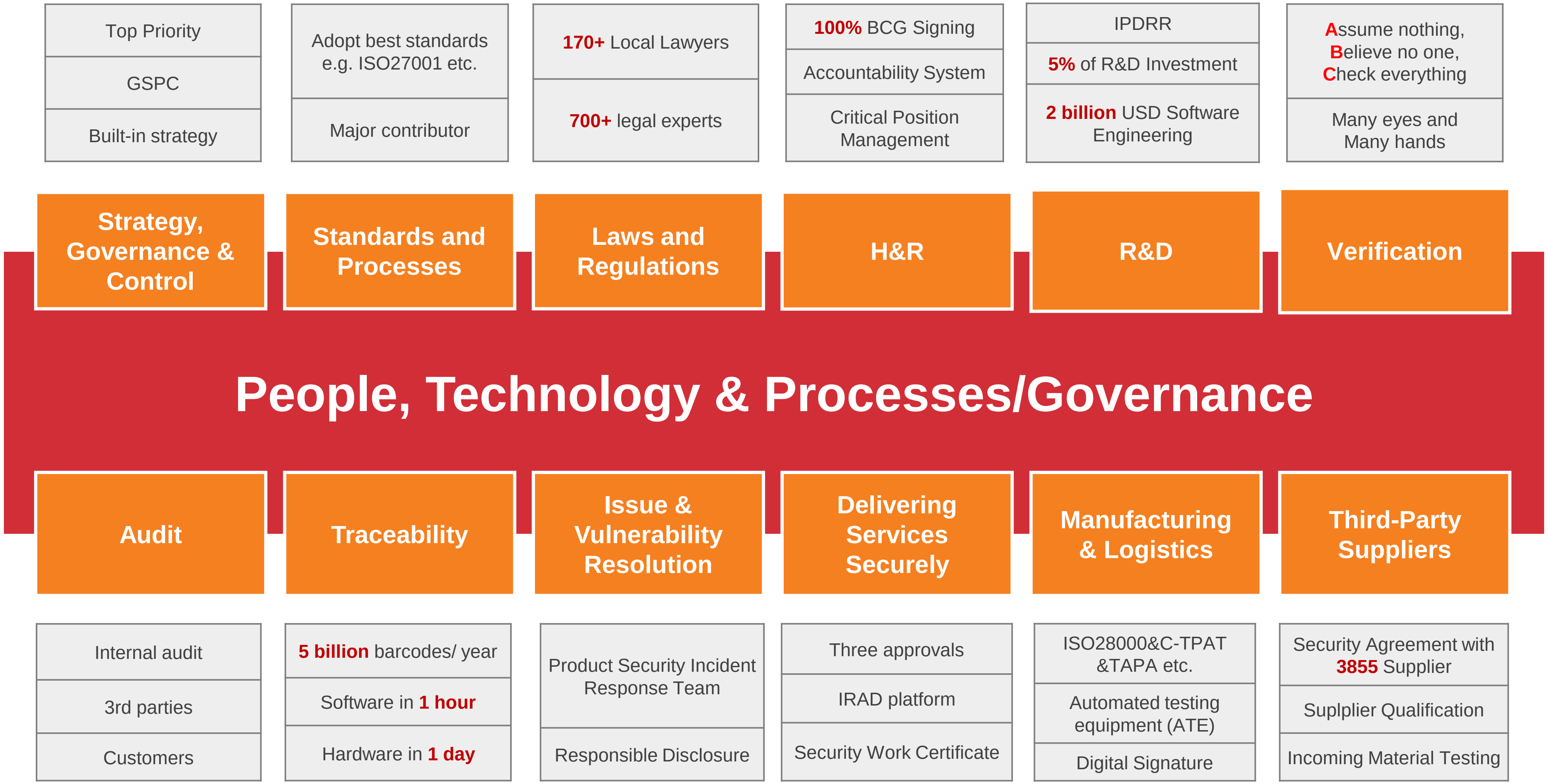
2010-2017

Help customers build cyber resilience with trustworthy product & solutions

- Elevated cyber security to top-priority status
- Open letter Comprehensively Enhancing Software Engineering Capabilities and Practices to Build Trustworthy, Quality Products to all employees
- Opened Transparency Center
- Software Engineering Transformation

2018-

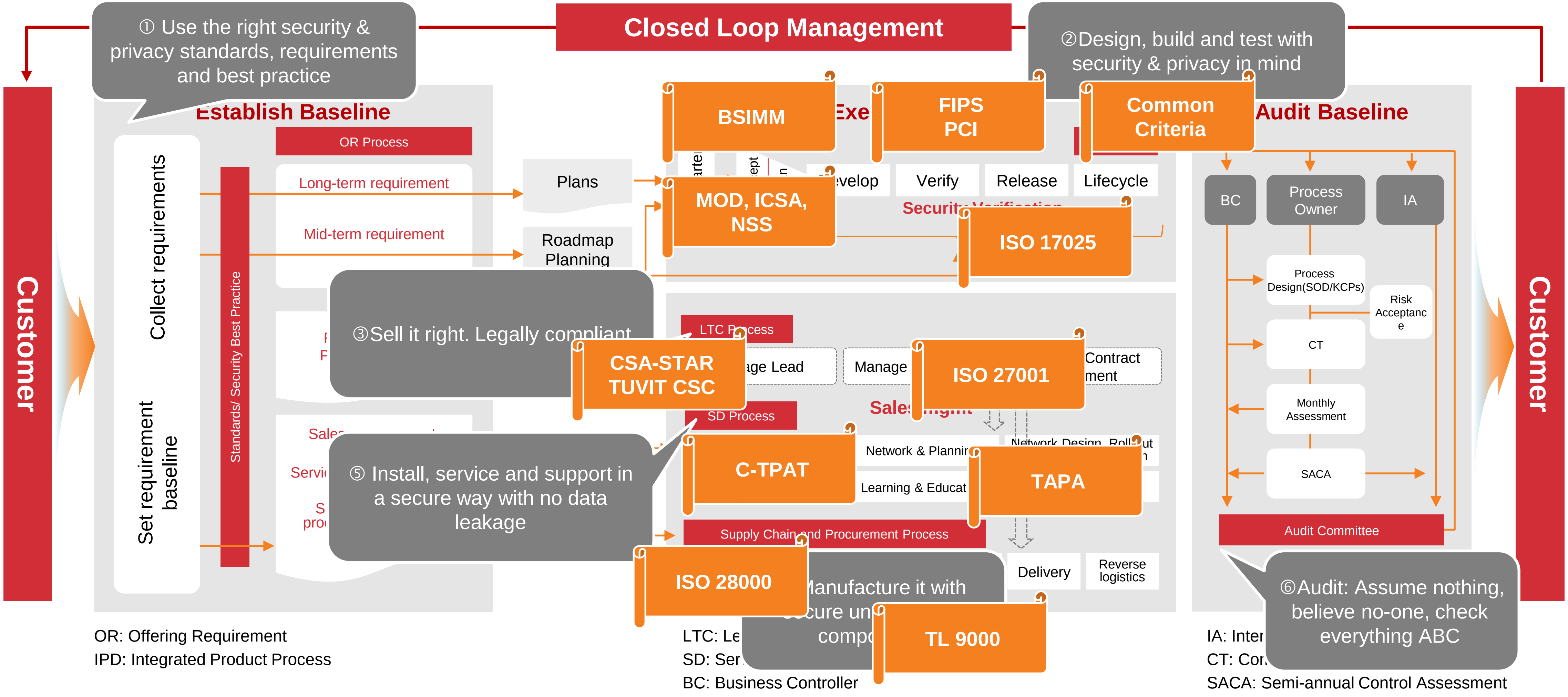
End-to-end Cyber Security Assurance System Focused on 12 Areas



People, Technology & Processes/Governance

Area	Details
Strategy, Governance & Control	Top Priority GSPC Built-in strategy
Standards and Processes	Adopt best standards e.g. ISO27001 etc. Major contributor
Laws and Regulations	**170+** Local Lawyers **700+** legal experts
H&R	**100%** BCG Signing Accountability System Critical Position Management
R&D	IPDRR **5%** of R&D Investment **2 billion** USD Software Engineering
Verification	**A**ssume nothing, **B**elieve no one, **C**heck everything Many eyes and Many hands
Audit	Internal audit 3rd parties Customers
Traceability	**5 billion** barcodes/ year Software in **1 hour** Hardware in **1 day**
Issue & Vulnerability Resolution	Product Security Incident Response Team Responsible Disclosure
Delivering Services Securely	Three approvals IRAD platform Security Work Certificate
Manufacturing & Logistics	ISO28000&C-TPAT &TAPA etc. Automated testing equipment (ATE) Digital Signature
Third-Party Suppliers	Security Agreement with **3855** Supplier Suplplier Qualification Incoming Material Testing

Strategy, Plans, Governance, Processes, Accountability and Supporting Technology Are Integrated, Seamless, Repeatable and Auditable



OR: Offering Requirement

IPD: Integrated Product Process

LTC: Le

SD: Ser

BC: Business Controller

IA: Inter

CT: Cor

SACA: Semi-annual Control Assessment

Huawei Cyber Security Certification Milestones

NE Routers obtained Huawei's first CC certificate.

2011

2014

LTE obtained CC EAL4+ certificate。

Mobile Money obtained H's first PCI PA DSS certificate.

2015

2015

Huawei's first GB/T 18336 EAL3+ certificate.

USG obtained the first Firewall CC EAL4+ certificate in the world.

2016

2016

Kirin 960 Technology Certification of Mobile Financial Service certificate.

AR Routers obtained FIPS 140-2 certification.

2017

2018

Huawei iTrustee CC EAL2+ certificate.

HongMengv1.2 obtained CC EAL5+ certificate.

2019

2019

Huawei Cloud obtained CSA-STAR gold medal certificate.

Huawei EulerOS obtained CC EAL4+ certificate.

2019

2020

Huawei ID obtained EuroPrise certificate.

Independent Cyber Security Lab (ICSL)
Huawei checks itself and allows others to do the same

Independent

Professional

Open

Deep-dive security testing and code review

This security verification platform is open to customers

Communications Security and Resilience - Call to action

Telecom equipment suppliers should be called upon to develop and implement minimum industry standards and best practices for assurance and transparency. Global community needs to:

Identify standards, best practices, and other objective criteria, and implement independent conformance and testing protocols for telecom and mobile operators, and telecom equipment (and other third-party) suppliers

Organize and incentivize experts to strengthen assurance AND transparency processes and technologies

Strengthen international norms of conduct for cyberspace and work collaboratively to reduce the frequency, impact and risk of malicious activity.

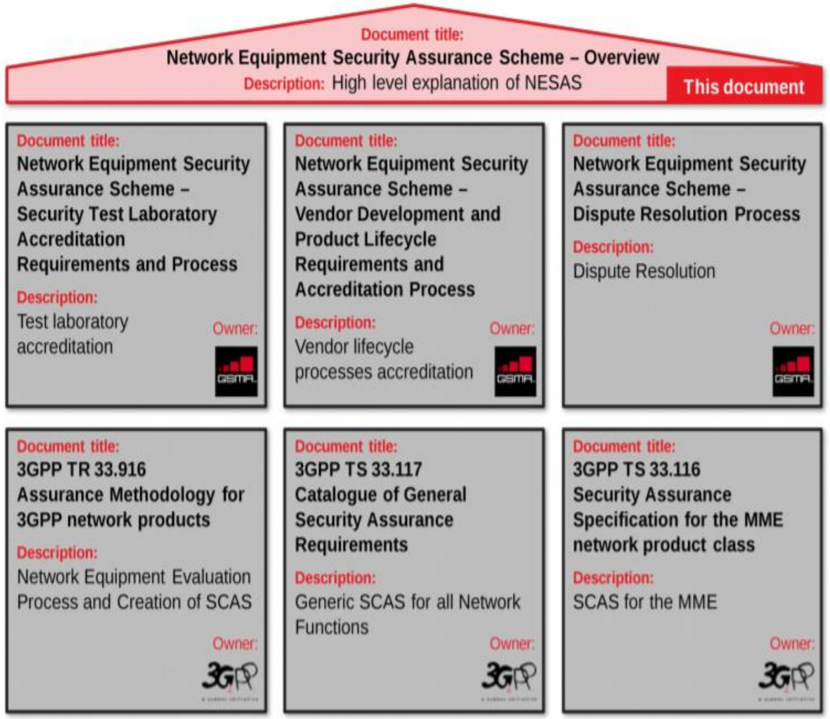
Best Practice: EU's General Data Protection Regulation (GDPR)

- GDPR is the EU's biggest reform of data protection laws over the past two decades. It aims to establish a unified data protection law covering all EU residents. This regulation took effect on May 25, 2018 in all EU member states.
- GDPR has become a benchmark for other countries in personal data transfer legislation.
- GDPR aims to strengthen the protection of personal data of all EU residents, regardless of where the data is collected or stored. All companies that access EU resident data must comply with this regulation.
- GDPR is a great improvement to the cross-border data flow policy. It includes provisions on cross-border data flow, with human rights protection as the top priority. It offers more legitimate ways for cross-border data transfer and allows for a higher level of flexibility.

GDPR took effect on May 25, 2018 in all EU member states.

Best Practice: Network Equipment Security Assurance Scheme (NESAS)

- **The NESAS is a voluntary program defined by 3GPP and GSMA for the mobile industry.**
- **The NESAS provides an easy-to-implement security assurance framework for carriers and vendors. It provides a security baseline to evidence that network equipment satisfies a list of security requirements and has been developed in accordance with security standards. To achieve this goal, NESAS provides two approaches:**
  - **1. Security assessment of the vendor development and product lifecycle processes**
  - **2. Security evaluation of network equipment by recognized and competent test laboratories through a well-defined and standardized security testing**
- **These two approaches help carriers determine the security level of network products and determine which vendor to work with.**



Document title: Network Equipment Security Assurance Scheme – Overview
Description: High level explanation of NESAS
This document

Document title: Network Equipment Security Assurance Scheme – Security Test Laboratory Accreditation Requirements and Process
Description: Test laboratory accreditation
Owner: GSMA

Document title: Network Equipment Security Assurance Scheme – Vendor Development and Product Lifecycle Requirements and Accreditation Process
Description: Vendor lifecycle processes accreditation
Owner: GSMA

Document title: Network Equipment Security Assurance Scheme – Dispute Resolution Process
Description: Dispute Resolution
Owner: GSMA

Document title: 3GPP TR 33.916 Assurance Methodology for 3GPP network products
Description: Network Equipment Evaluation Process and Creation of SCAS
Owner: 3GPP

Document title: 3GPP TS 33.117 Catalogue of General Security Assurance Requirements
Description: Generic SCAS for all Network Functions
Owner: 3GPP

Document title: 3GPP TS 33.116 Security Assurance Specification for the MME network product class
Description: SCAS for the MME
Owner: 3GPP

NESAS is a voluntary program for carriers and equipment vendors in the mobile industry.

Case Germany, from vision to strategy

Description:

- **Kick Off for European Cybersecurity works was started 2001 in Stockholm**
- **2013 EU Commission was publishing EU’s Cybersecurity strategy, which was actually a policy paper, stating that all EU countries need to have Cyber strategy**
- **ENISA (European Cyber Agency) was mandated to make the work and build NCSS (National Cybersecurity Strategies)**
- **Today ENISA has been keeping 7 Strategy workshps in different countries**
- **Germany was first European country to make own Cyber Strategy calles ”National Plan for Infrastructure Protection” 2005**

EUROPEAN COMMISSION

HIGH REPRESENTATIVE OF THE EUROPEAN UNION FOR FOREIGN AFFAIRS AND SECURITY POLICY

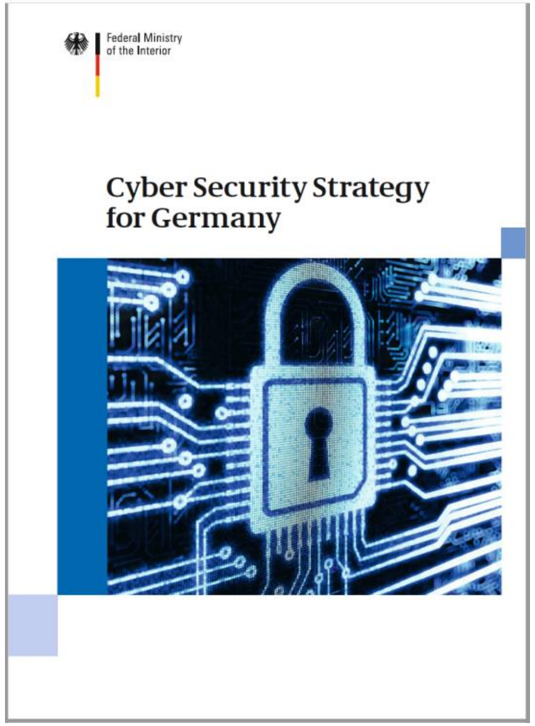
Brussels, 7.2.2013
JOIN(2013) 1 final

JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS

Cybersecurity Strategy of the European Union:

An Open, Safe and Secure Cyberspace

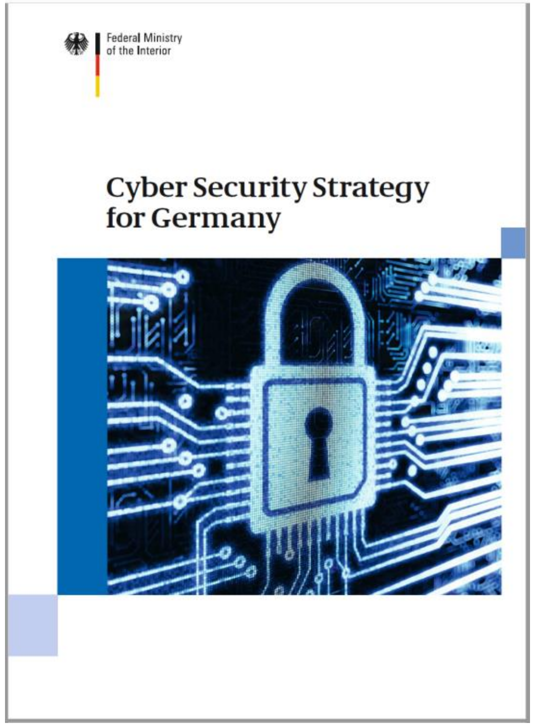
EN EN



Federal Ministry of the Interior

Cyber Security Strategy for Germany

German Cyber Security strategy 7th November 2016



Federal Ministry
of the Interior

Cyber Security Strategy
for Germany

9 Objectives

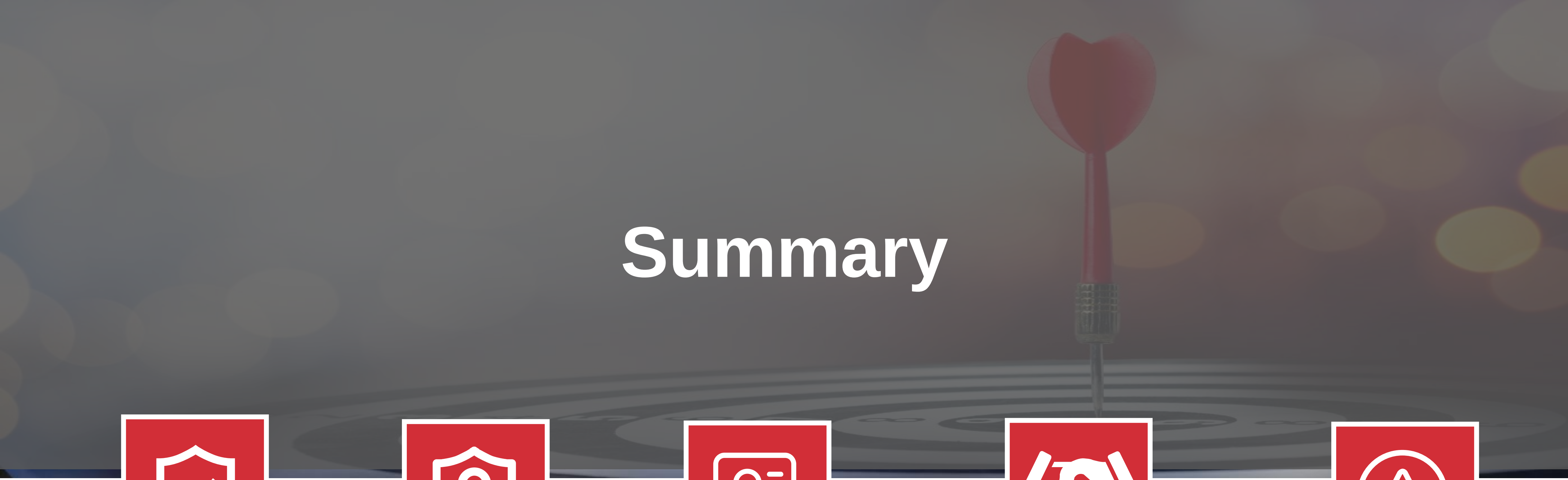
- Address cyber crime
- Citizen's awareness
- Critical Information Infrastructure Protection
- Develop national cyber contingency plans
- Engage in international cooperation
- Establish an incident response capability
- Establish an institutionalized form of cooperation between public agencies
- Establish baseline security requirements
- Foster R&D

Germany: from strategy to legistlation

- On 15th Oct, 2019，BNetzA of Germany unveiled ***Catalog of Security Requirements for Operating Telecommunication System and Data Processing System as well as for Processing Personal Data According to Section 109 of Telecommunication Act, Version 2.0*****. Germany has set technology-neutral cyber security standards that apply to all vendors.**

- **Ten criteria for the trustworthiness of manufacturers and suppliers**

1. **Cooperation with users**
2. **Protecting users from contractual data leakages**
3. **Preventing confidential data to be transferred foreign country**
4. **Assurance not to disclose data to third parties**
5. **Notification obligations in case of non compliance**
6. **Obligation to provide information from safety related issues**
7. **Obligation to use trustworthy employees**
8. **Declaration of willingness to support security reviews**
9. **No backdoors- assurance**
10. **Notification obligation from vulnerabilities**



Summary

Huawei security assurance journey began more than 20 years ago

Cybersecurity and user privacy protection are of utmost importance

Huge investment in people and resources to manage risk effectively, steeped in standards and best practices, separation of duties, and independent verification

For the past 30 years, Huawei has served more than 3 billion people, supported more than 1,500 carrier networks, and earned the trust of thousands of customers in over 170 countries

The reputations of our Customers and Huawei are priceless.

Thank you.

martin.portillo@huawei.com

把数字世界带入每个人、每个家庭、
每个组织，构建万物互联的智能世界。

Bring digital to every person, home, and organization for a fully connected, intelligent world.

**Copyright©2020 Huawei Technologies Co., Ltd.
All Rights Reserved.**

The information in this document may contain predictive statements including, without limitation, statements regarding the future financial and operating results, future product portfolio, new technology, etc. There are a number of factors that could cause actual results and developments to differ materially from those expressed or implied in the predictive statements. Therefore, such information is provided for reference purpose only and constitutes neither an offer nor an acceptance. Huawei may change the information at any time without notice.