Time to Get Serious About Addressing Cyber Security Risk

Andy Purdy
CSO, Huawei Technologies USA
Andy.Purdy@Huawei.com

October 5, 2017

INTRODUCTION – All Cyber Stakeholders

- Understand and address cyber and privacy risks – including from 3rd parties.
- Collaborate and share information more effectively.
- Buyers should leverage their purchasing power.
- Continuous improvement!

Agenda

1. Why Should You Care?
2. Major Cyber Security Threats
3. Risk Management
4. Role of Government
5. Role of Leaders of Private Organizations
6. Huawei Approach
7. Conclusion

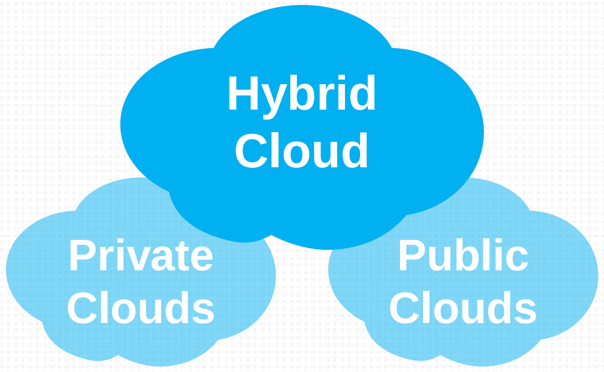
Agenda

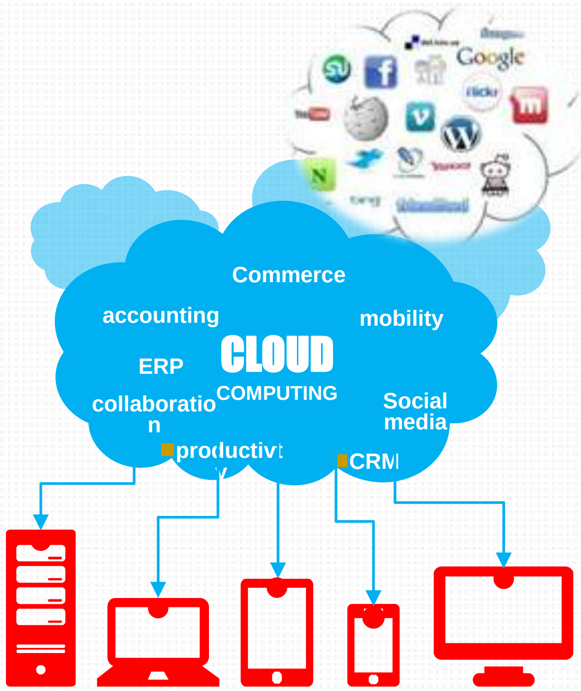
1 Why Should You Care?

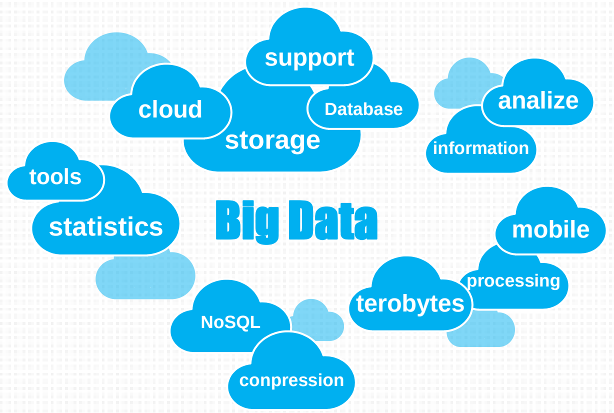
Why Should You Care?

A True Revolution – New technology on the desk, in your home, in your car in your pocket has spawned a global connected world of infrastructures, applications and the movement of data.

There’s an APP for that







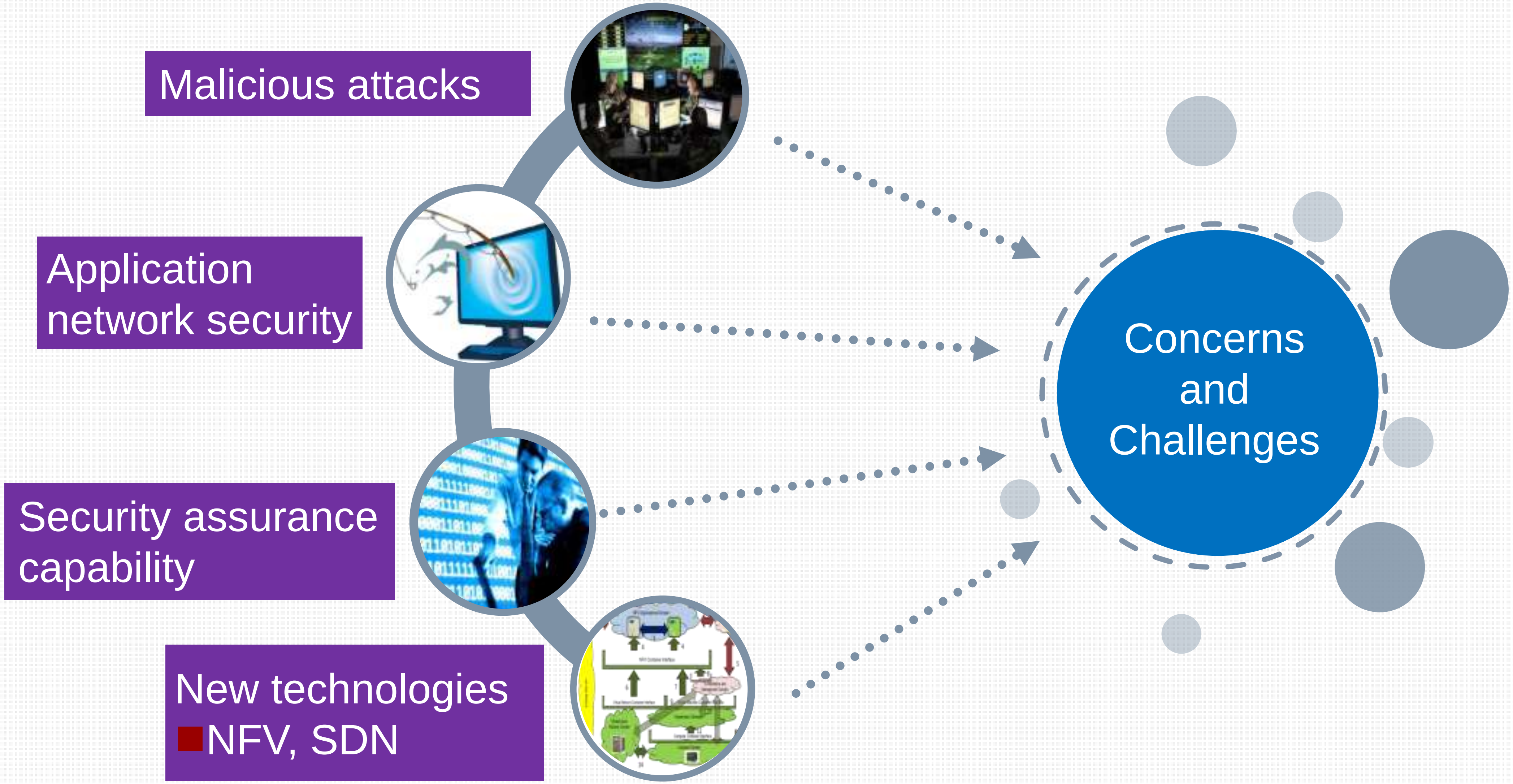
There’s an API for that

Agenda

2 Major Cyber Security Threats

Corresponding Increase in Cyber Threats

Major Challenges Faced by Operators and Users



Malicious attacks

Application network security

Security assurance capability

New technologies

- NFV, SDN

Concerns and Challenges

Cyber threats in technology development and global supply chains

Stakeholders Main Threats	Tainted		Counterfeit	
	Upstream	Downstream	Upstream	Downstream
Malware	√	√	√	
Unauthorized “Parts”	√	√	√	
Unauthorized Configuration		√		
Scrap/Sub-standard Parts			√	
Unauthorized Production			√	√
Intentional Damage	√	√		

Confidentiality Integrity Availability Traceability Authenticity

Courtesy of The Open Group

Agenda

3 Cyber Risk Management

Risk Management

- What is Risk?
  - Threats
  - Vulnerabilities
  - Consequences
- **Responsibility of leaders:** *what to worry about and what to about it!*
- Business objectives, risk environment, critical functions and assets
- Assess risk and prioritize risk management?
  - Nations – Capacity and Preparedness (Global Cyber Index)
  - Organizations – NIST Cybersecurity Framework (supply chain risk – Open Trusted Technology Provider Standards (ISO/IEC 20243)

Agenda

4 Role of Government

Role of Government

- **Responsibility of government leaders**
- What are the key priorities of the nation? Risk environment relative to priorities -- critical functions and assets?
- Risk management approach
- What capacity and preparedness is necessary?
- Collaboration and information sharing
- *Remember third-party risk*

Role of Government
Global Cyber Index (GCI)

- The **Global Cybersecurity Index (GCI)** - measure a nation’s commitment to cybersecurity.
- Cybersecurity cuts across many industries and sectors.
- Level of development analyzed within five categories: Legal Measures, Technical Measures, Organizational Measures, Capacity Building and Cooperation.
- http://www.itu.int/en/ITU-D/Cybersecurity/Pages/GCI.aspx
- **Latvia Cybersecurity Wellness Profile:** http://www.itu.int/en/ITU-D/Cybersecurity/Documents/Country_Profiles/Latvia.pdf

Role of Government – how prepared are you?

Cyber Readiness Index 2.0

- Assess commitment and maturity
- Incentivize this alignment
- Country reports based on
  - 70+ indicators across seven elements
  - to discern readiness and identify areas for improvement
- The CRI 2.0 shows that few countries have aligned their digital agenda with their cyber security agenda
- http://www.potomacinstitute.org/images/CRIndex2.0.pdf
- Country profiles: http://www.potomacinstitute.org/academic-centers/cyber-readiness-index

Role of Government

ITU Resources

- To assist Member States in building capacity in cybersecurity, ITU proposes two tools, HORNET and AWARE.
  - **Honeypot Research Network (HORNET)** - a sensor network feeding real-time intelligence to help countries enhance their readiness.

    http://www.itu.int/en/ITU-D/Cybersecurity/Pages/HORNET.aspx.
  - **Abuse Watch Alerting & Reporting Engine (AWARE)** to assist the Computer Incident Response Teams (CIRTs) to enhance the incident response function. http://www.itu.int/en/ITU-D/Cybersecurity/Pages/AWARE.aspx.
- To facilitate availability of relevant cyber threat reports to ITU Member states. http://www.itu.int/en/ITU-D/Cybersecurity/Pages/symantec_and_trend_micro.aspx.

Role of Government

Use Purchasing Power to Lower Cyber Risk

EastWest Institute (EWI) *ICT Buyers Guide*

- Incentivize providers of ICT products and services to increase assurance/security levels
- **EWI Buyers Guide**: “*Purchasing Secure ICT Products and Services: A Buyers Guide*”
- For organizations interested in more secure products and services.

https://www.eastwest.ngo/idea/ewi-holds-panel-discussion-launch-buyers-guide

Role of Government

Use Purchasing Power to Lower Cyber Risk

EWI *ICT Buyers Guide* (2)

- Led by Microsoft, Huawei, and The Open Group, the *Guide* helps buyers develop purchasing requirements.
  - ○ “Enterprise Security Governance”
  - ○ “The Product and Service Lifecycle – from Design through Sustainment and Response”

https://www.eastwest.ngo/sites/default/files/EWI_BuyersGuide.pdf

Agenda

5 Role of Leaders of Private Organizations

Role of Private Organizations

Critical Success Factors for Assurance

- Commitment
- Strategy to address future challenges
- Clear governance roles and responsibilities
- Consistent, repeatable processes
- Robust verification
- Openness and transparency regarding progress, successes, and failures

Role of Private Organizations

Assessing and Managing Risk

The NIST Cybersecurity Framework (CSF)

- **A customizable risk-analytic tool** with
  - a set of standards, methodologies, procedures, and processes
  - aligning policy, business, and technological approaches
- Prioritized, flexible, repeatable, performance-based, and cost-effective
- Information security measures and controls
- Identifies areas for improvement.
- Consistent with voluntary international standards.

Courtesy of NIST: https://www.nist.gov/file/354081

Assessing and Managing Risk

The NIST CSF – Risk Management Properties

- Framework
- Profile
- Implementation Tier

Courtesy of NIST: https://www.nist.gov/file/354081

Assessing and Managing Risk

The NIST CSF – Framework Core

Framework Core

Cybersecurity activities and informative references, organized around particular outcomes

Enables communication of cyber risk across an organization

Courtesy of NIST: https://www.nist.gov/file/354081

Assessing and Managing Risk

The NIST CSF – Framework Core (2)

	Function
What processes and assets need protection?	Identify
What safeguards are available?	Protect
What techniques can identify incidents?	Detect
What techniques can contain impacts of incidents?	Respond
What techniques can restore capabilities?	Recover

Courtesy of NIST: https://www.nist.gov/file/354081

Assessing and Managing Risk

The NIST CSF – Framework Component: The Core

Function	Category	ID
Identify	Asset Management	ID.AM
	Business Environment	ID.BE
	Governance	ID.GV
	Risk Assessment	ID.RA
	Risk Management Strategy	ID.RM
Protect	Access Control	PR.AC
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Information Protection Processes & Procedures	PR.IP
	Maintenance	PR.MA
	Protective Technology	PR.PT

Courtesy of NIST: https://www.nist.gov/file/354081

Assessing and Managing Risk

The NIST CSF – Framework Component: The Core

Function	Category	ID
Detect	Anomalies and Events	DE.AE
	Security Continuous Monitoring	DE.CM
	Detection Processes	DE.DP
Respond	Response Planning	RS.RP
	Communications	RS.CO
	Analysis	RS.AN
	Mitigation	RS.MI
	Improvements	RS.IM
Recover	Recovery Planning	RC.RP
	Improvements	RC.IM
	Communications	RC.CO

Courtesy of NIST: https://www.nist.gov/file/354081

The NIST CSF – Subcategories/Informative References

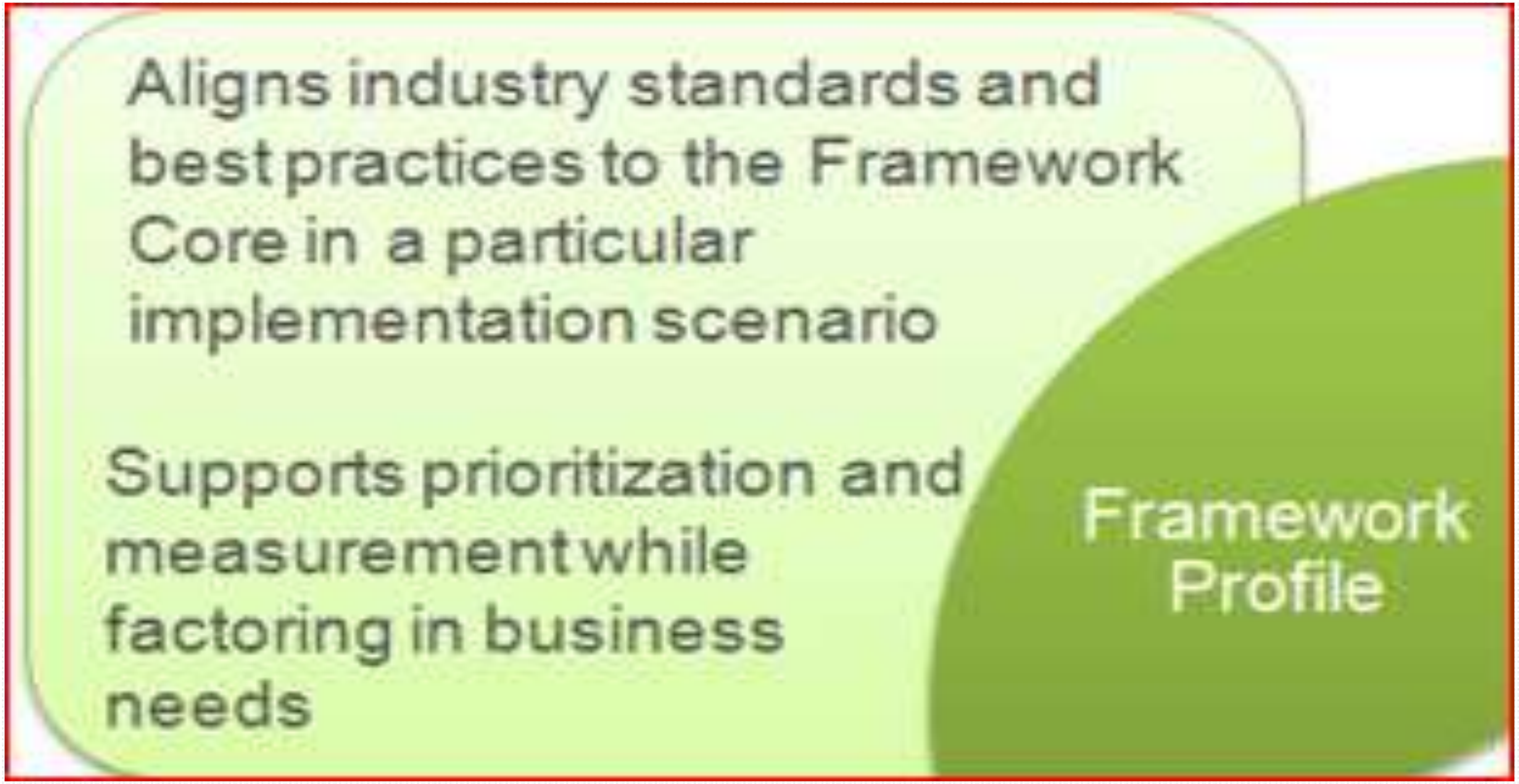
Function	Category	ID
Identify		
	Business Environment	**ID.BE**

Courtesy of NIST: https://www.nist.gov/file/354081

Subcategory	Informative References
ID.BE-1: The organization’s role in the supply chain is identified and communicated	**COBIT 5** APO08.04, APO08.05, APO10.03, APO10.04, APO10.05 **ISO/IEC 27001:2013** A.15.1.3, A.15.2.1, A.15.2.2 **NIST SP 800-53 Rev. 4** CP-2, SA-12
ID.BE-2: The organization’s place in critical infrastructure and its industry sector is identified and communicated	**COBIT 5** APO02.06, APO03.01 **NIST SP 800-53 Rev. 4** PM-8
ID.BE-3: Priorities for organizational mission, objectives, and activities are established and communicated	**COBIT 5** APO02.01, APO02.06, APO03.01 **ISA 62443-2-1:2009** 4.2.2.1, 4.2.3.6 **NIST SP 800-53 Rev. 4** PM-11, SA-14

Assessing and Managing Risk

The NIST CSF – Profile



Aligns industry standards and best practices to the Framework Core in a particular implementation scenario

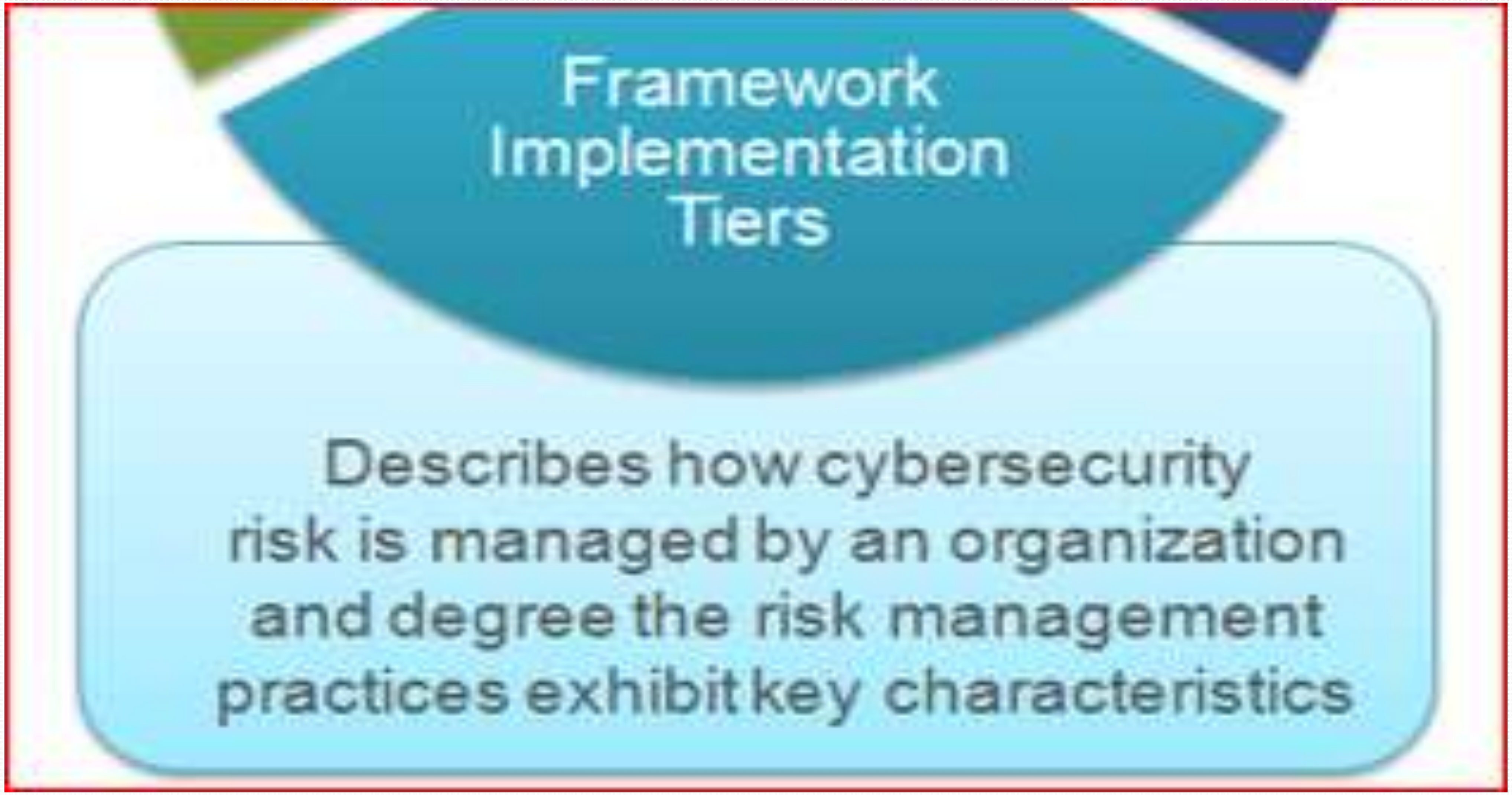
Supports prioritization and measurement while factoring in business needs

Framework Profile

Courtesy of NIST: https://www.nist.gov/file/354081

Assessing and Managing Risk

The NIST CSF – Implementation Tier



Framework Implementation Tiers

Describes how cybersecurity risk is managed by an organization and degree the risk management practices exhibit key characteristics

Courtesy of NIST: https://www.nist.gov/file/354081

Addressing Supply Chain Risk
The Open Group Trusted Technology Forum (OTTF)

A global industry-led initiative defining best practices for secure engineering and supply chain integrity so that you can "*Build with Integrity and Buy with Confidence™*"

IBM

Microsoft

CISCO

ORACLE

NASA

hp

EMC²

Raytheon

HUAWEI

DEPARTMENT OF DEFENSE UNITED STATES OF AMERICA

STRATEGIC COMMUNICATIONS
VOICE, DATA & VIDEO SOLUTIONS

DELL

EWA
Enabling a More Secure Future

BOEING

@SEC
the information security provider

MITRE

Booz | Allen | Hamilton

Office of the Under Secretary of Defense for
Acquisition, Technology and Logistics

EXO
STRATEGIES

NTG

pcitec
PANAMERICA COMPUTERS, INC.

INTEROS
Reducing Your Supply Chain Risk

QUINSIGAMOND
Community College

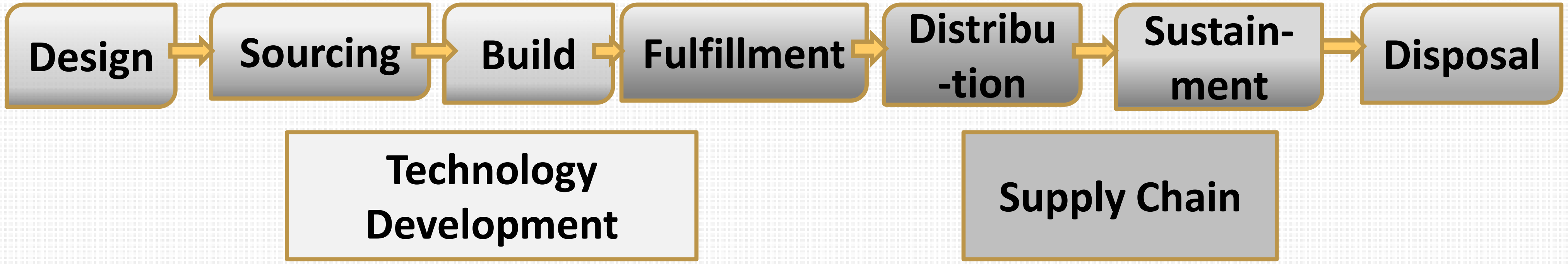
TATA
TATA CONSULTANCY SERVICES

Software Engineering Institute | Carnegie Mellon

Trusted Technology Provider Standard (ISO 20243)

Mitigating Risk of Malicious Taint and Counterfeit Products

- ***Two areas of requirements***
  - ***Technology Development*** - *mostly* provider’s in-house supervision
  - ***Supply Chain activities*** *mostly* where provider interacts with third parties



Design

Sourcing

Build

Fulfillment

Distribution

Sustainment

Disposal

Technology Development

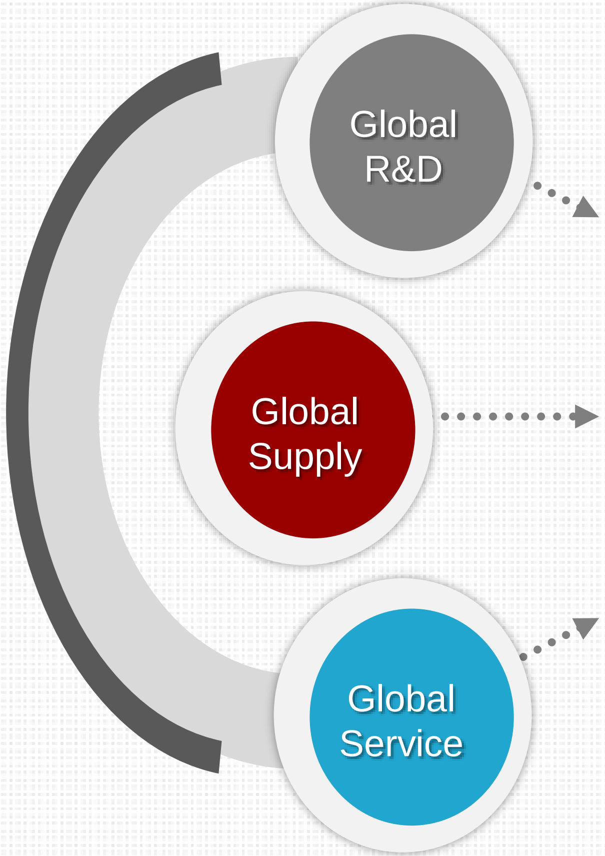
Supply Chain

- **ISO/IEC 20243.** Across the product life cycle.
- 3 years’ collaborative consensus-based effort
- Some highly correlated to threats of maliciously tainted and counterfeit products - others more foundational but considered essential

Agenda

6 Huawei Approach

Huawei – Challenges of Enterprise & Supply Chain Risk



- A leading global ICT solutions, Fortune Global 500 company

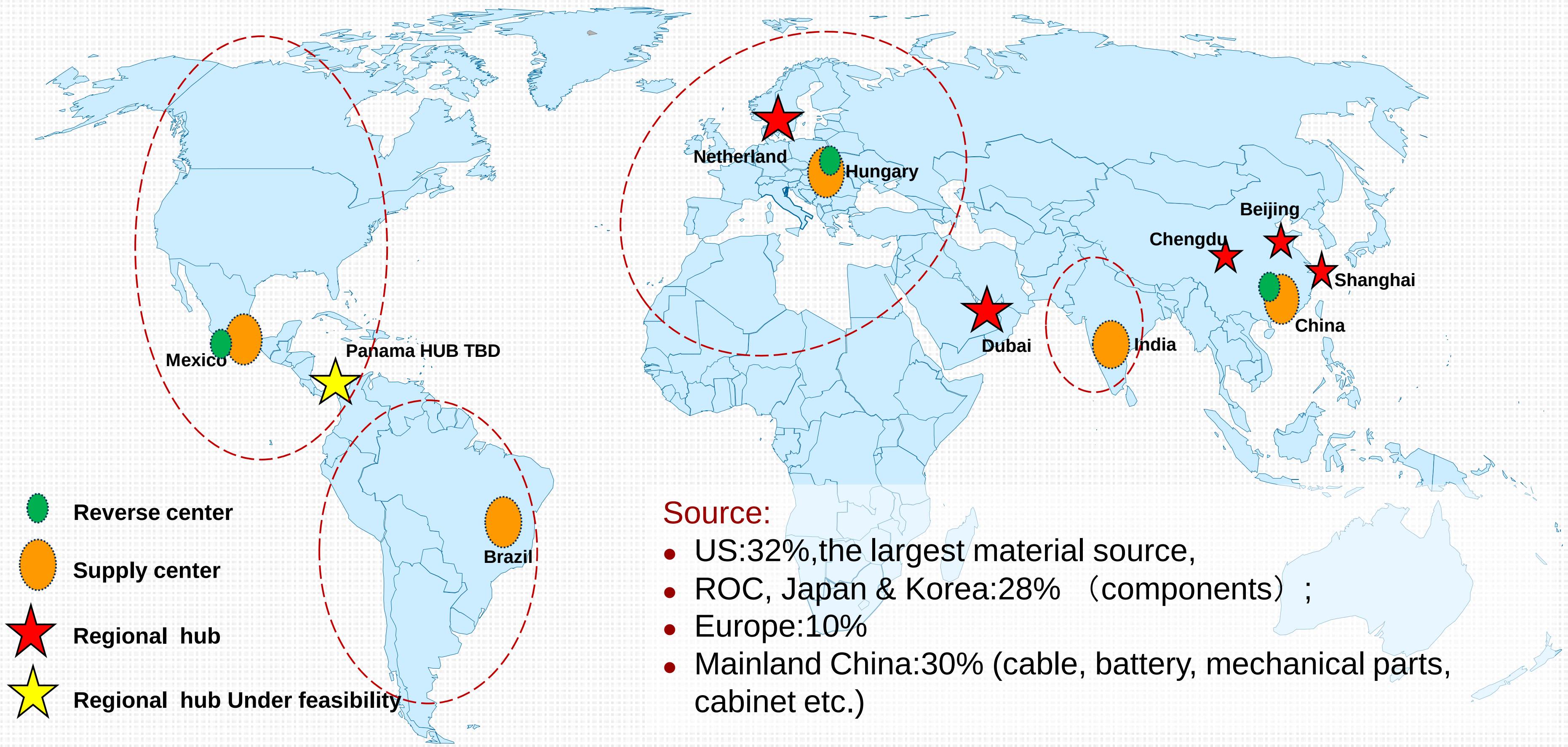
- Operations in 170 countries, 170,000 employees, 73% recruited locally

- 70,000+ employees in R&D
- 15 R&D centers; 25 Joint Innovation Centers

- $74.5 B revenue in 2016
- Serving 45 of the world's top 50 operators

Secure products, solutions and services

Huawei’s Global Supply Network



Source:

- US:32%,the largest material source,
- ROC, Japan & Korea:28% （components）;
- Europe:10%
- Mainland China:30% (cable, battery, mechanical parts, cabinet etc.)

Supply Center

- China (Delivery for the globe)
- Europe (Delivery for West Europe &North Africa)
- Mexico (Delivery for North America & Latin America)
- Brazil (Delivery for South Latin America)
- India (Delivery for India)

Regional Hub

- Dubai (United Arab Emirates)
- Netherlands

Reverse Center

- China
- Mexico
- Europe

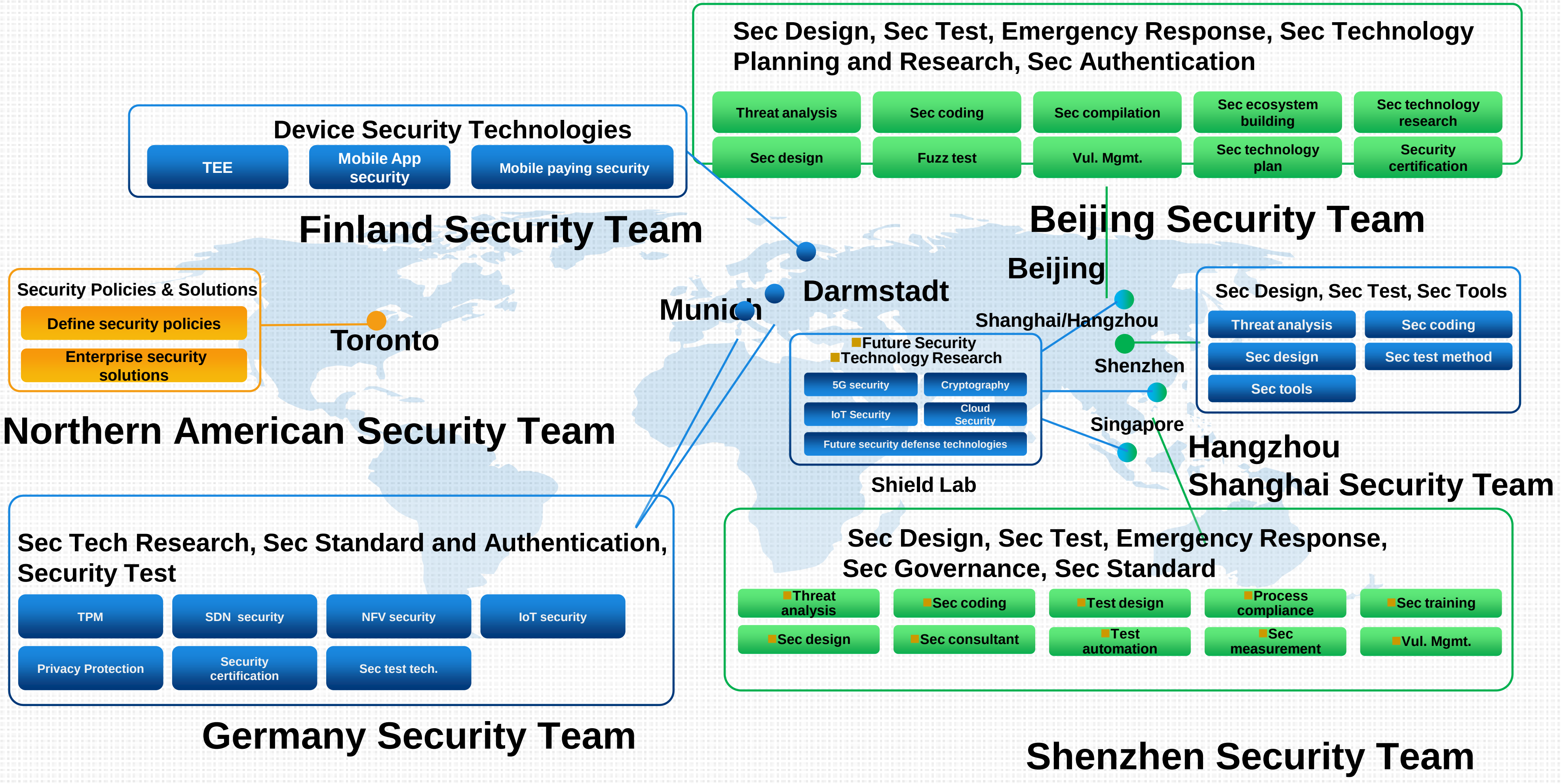
Local EMS

- Brazil , Mexico, India and Hungary supply centers work with local partners to do manufacturing and make delivery

Huawei Perspective

- A global problem: everything is vulnerable. How to establish trust?
- Concerted, collaborative action.
- Use standards and best practices.
- Understand, assess, and mitigate risk.
- Leverage our collective ICT buying power.
- Competition and innovation to bring the benefits of ICT to all of humanity.

Huawei global cyber security engineering capability and technology map



Finland Security Team

Device Security Technologies

- TEE
- Mobile App security
- Mobile paying security

Beijing Security Team

Sec Design, Sec Test, Emergency Response, Sec Technology Planning and Research, Sec Authentication

- Threat analysis
- Sec coding
- Sec compilation
- Sec ecosystem building
- Sec technology research
- Sec design
- Fuzz test
- Vul. Mgmt.
- Sec technology plan
- Security certification

Northern American Security Team

Security Policies & Solutions

- Define security policies
- Enterprise security solutions

Germany Security Team

Sec Tech Research, Sec Standard and Authentication, Security Test

- TPM
- SDN security
- NFV security
- IoT security
- Privacy Protection
- Security certification
- Sec test tech.

Shield Lab

Future Security Technology Research

- 5G security
- Cryptography
- IoT Security
- Cloud Security
- Future security defense technologies

Hangzhou Shanghai Security Team

Sec Design, Sec Test, Sec Tools

- Threat analysis
- Sec coding
- Sec design
- Sec test method
- Sec tools

Shenzhen Security Team

Sec Design, Sec Test, Emergency Response, Sec Governance, Sec Standard

- Threat analysis
- Sec coding
- Test design
- Process compliance
- Sec training
- Sec design
- Sec consultant
- Test automation
- Sec measurement
- Vul. Mgmt.

Huawei Cybersecurity Overview – Building trust

Security is in our DNA!

Partners Ecosystem	Partnership with Leading Security Solutions Providers	Joint solutions, Reference Cases Reference Architectures	TREND MICRO IBM RSA SPIRENT Microsoft symantec.
Industry Solutions	Finance, Public Security, Energy, Manufacturing	Smart City 100+, Energy 300+, Bank 300+, Transport 100K+ km	HSBC iDA DHL Santander GAZPROM
Horizontal Solutions	Cloud, IoT, Security, Converged Data Center, Big Data	Industry Awards, Analysts Recognition, Reference Arch.	Cyber Security Organization of the Year, Excellence in Information Security, Transparency Award for Cyber Security Gartner analysys mason Current Analysis FROST & SULLIVAN
Product Security Capabilities	Industry Leading Security & Privacy Controls, Multi-Plane & Layer Security	Common Criteria EAL 3, PCI DSS, FIPS 140-2 ISO/IEC17025, Huawei ICSL UK Cybersec Evaluation Centre 3rd Party Tests, Code Reviews	nccgroup PCI DSS secunet dn systems Nessus FORTIFY SmartIDE CODEX coverity PC-lint
Product Security Architecture	Secure Design/Coding/Testing, STRIDE[1], Encryption, Architecture, CERT		
Huawei Processes	Most Comprehensive Industry Controls, Privacy Protection, Third Party Audit, Standards, Compliance and Certification	ISO 9001, ISO 27001 ISO 14001, ISO 18001 Ecovadis	IBM accenture BCG HayGroup Fraunhofer pwc

STRIDE: STRIDE is a threat classification model developed by Microsoft for thinking about computer security threats. It is often used by security experts to check the system for possible threats. S: Spoofing, T: Tampering, R: Reputation, I: Information Disclosure, D: Denial of Service, E: Elevation of Privileges

Huawei and Cyber Security

"Huawei guarantees that its commitment to cyber security will never be outweighed by the consideration of commercial interests. … It (Cyber Security) is for our survival."

- To meet our customers' security and assurance requirements with transparency
- To strengthen – and promote transparency.
- To promote adoption of a level-playing field.

Huawei Cyber Security Assurance

- A security assurance system.
- Security integrated into all business processes and implemented under management regulations and technical specifications.

  “Making cyber security a part of a company’s DNA - A set of integrated processes, policies and standards (October 2013)” http://www.huawei.com/en/cyber-security/hw_310548.

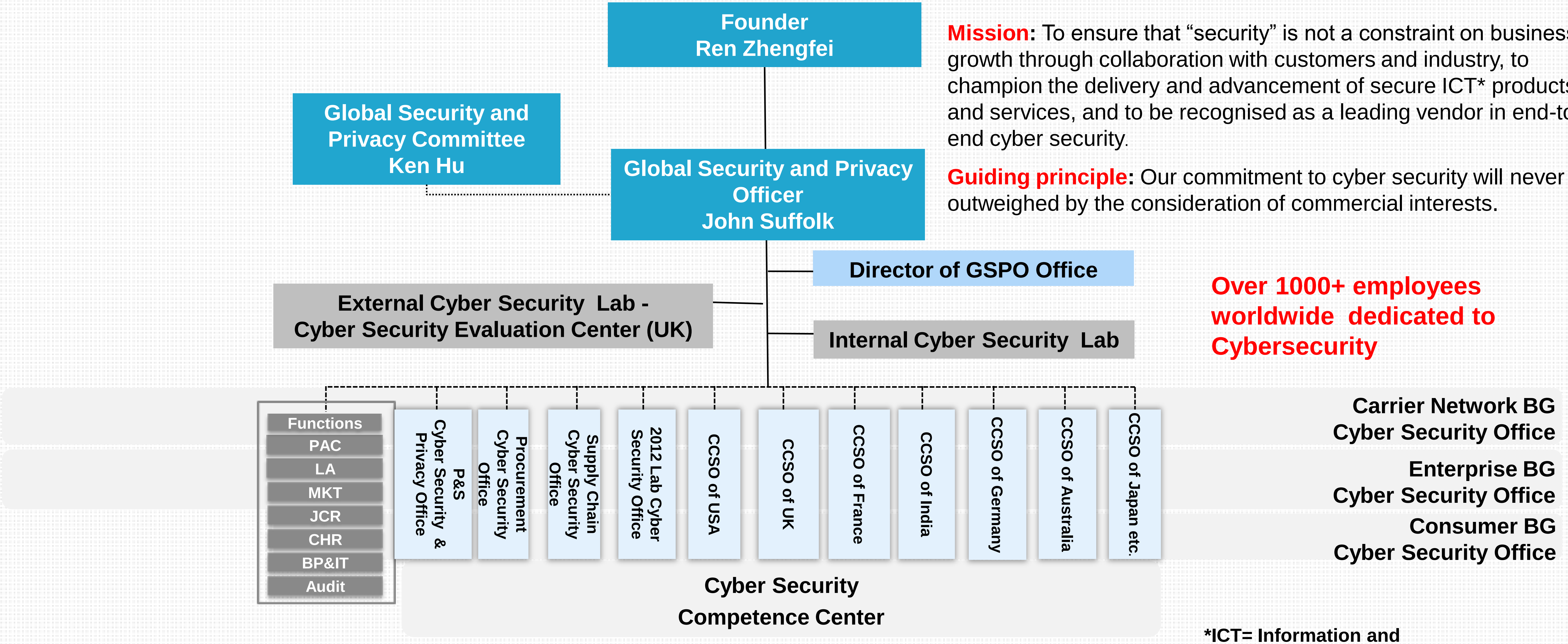
- Compliance with cyber security policies / requirements; appropriate training.
- Violations will be sanctioned.
- *Lack of bad intent is not a defense*.

Huawei Organizational Governance for Cyber Security and Privacy

Vision: It is our primary social responsibility to support stable and secure networks for our customers at all times.

Mission: To ensure that “security” is not a constraint on business growth through collaboration with customers and industry, to champion the delivery and advancement of secure ICT* products and services, and to be recognised as a leading vendor in end-to-end cyber security.

Guiding principle: Our commitment to cyber security will never be outweighed by the consideration of commercial interests.



Founder
Ren Zhengfei

Global Security and Privacy Committee
Ken Hu

Global Security and Privacy Officer
John Suffolk

Director of GSPO Office

External Cyber Security Lab -
Cyber Security Evaluation Center (UK)

Internal Cyber Security Lab

Functions
PAC
LA
MKT
JCR
CHR
BP&IT
Audit

P&S Cyber Security & Privacy Office
Procurement Cyber Security Office
Supply Chain Cyber Security Office
2012 Lab Cyber Security Office
CCSO of USA
CCSO of UK
CCSO of France
CCSO of India
CCSO of Germany
CCSO of Australia
CCSO of Japan etc.

Cyber Security Competence Center

Carrier Network BG
Cyber Security Office

Enterprise BG
Cyber Security Office

Consumer BG
Cyber Security Office

Over 1000+ employees worldwide dedicated to Cybersecurity

*ICT= Information and Communications Technology

Proactive End-2-End (E-2-E) Assurance System

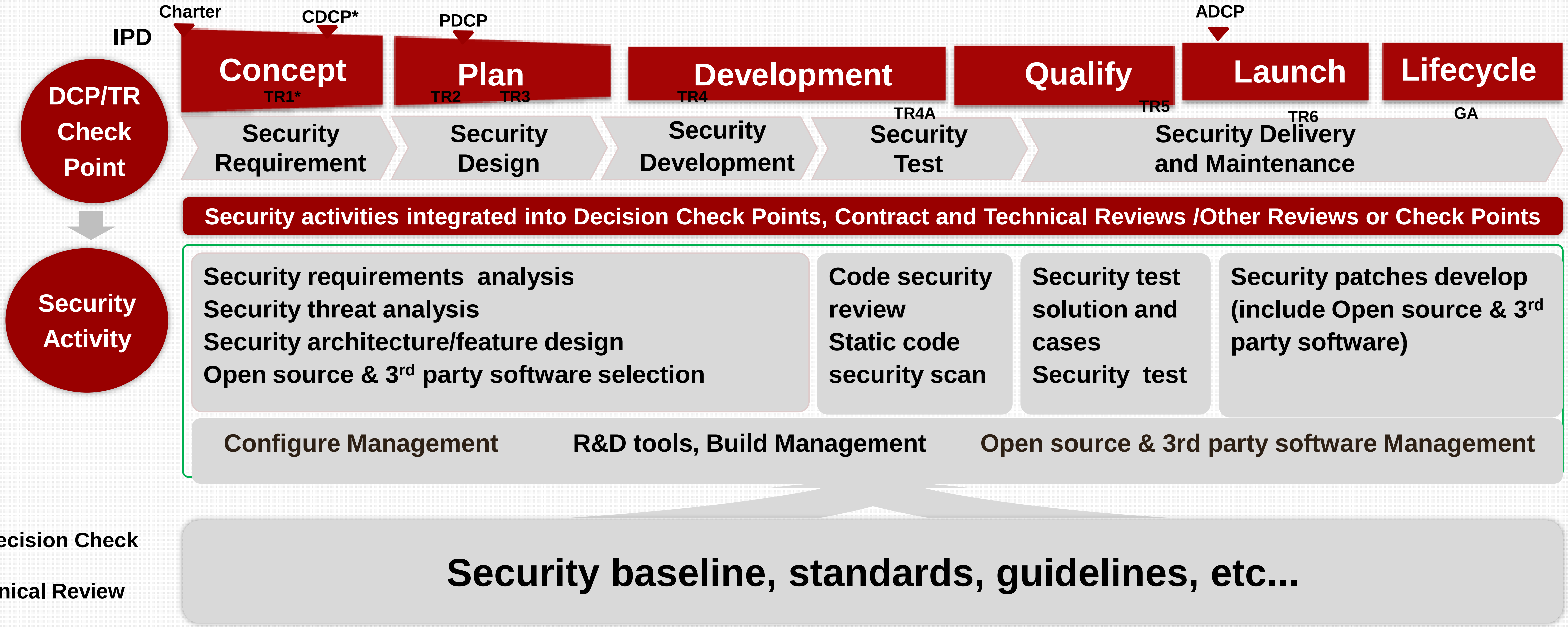
No.	Area	Focus
1	Strategy, Governance and Control	Having an overall strategy and the accountability to make it happen
2	Standards and Processes	Using the best standards and approaches to protect against threats and risks
3	Laws and Regulations	Making your products and operations legally compliant in every country you operate in
4	Human Resources	Getting the right people, in the right roles with the right behaviour to limit insider issues
5	Research and Development	Designing, building, testing products in a secure way that builds on the above building blocks

End-2-End Assurance (2)

No.	Area	Focus
6	Verification: Assume nothing, believe no one, check everything	Many eyes, many hands many checks. Tiered independent approach to security verification
7	Third-Party Supplier Management	Getting your suppliers to take security seriously – 70% in the box is not Huawei’s
8	Manufacturing and Logistics	Manufacturing products that secure each step along the way – right through to delivery
9	Delivering Services Securely	Ensuring installation, service and support is secured. No tampering, fully auditable
10	Issue, Defect and Vulnerability Resolution	As issues arise, solving them quickly and ensuring customers technology is secured
11	Audit	Using rigorous audit mechanisms to ensure every part of Huawei conform to the strategy

Huawei adopts a built-in approach

Security activities in the Integrated Product Delivery (IPD) process



IPD

Charter

CDCP*

PDCP

ADCP

Concept

Plan

Development

Qualify

Launch

Lifecycle

TR1*

TR2

TR3

TR4

TR4A

TR5

TR6

GA

DCP/TR Check Point

Security Requirement

Security Design

Security Development

Security Test

Security Delivery and Maintenance

Security activities integrated into Decision Check Points, Contract and Technical Reviews /Other Reviews or Check Points

Security Activity

Security requirements analysis
Security threat analysis
Security architecture/feature design
Open source & 3rd party software selection

Code security review
Static code security scan

Security test solution and cases
Security test

Security patches develop (include Open source & 3rd party software)

Configure Management

R&D tools, Build Management

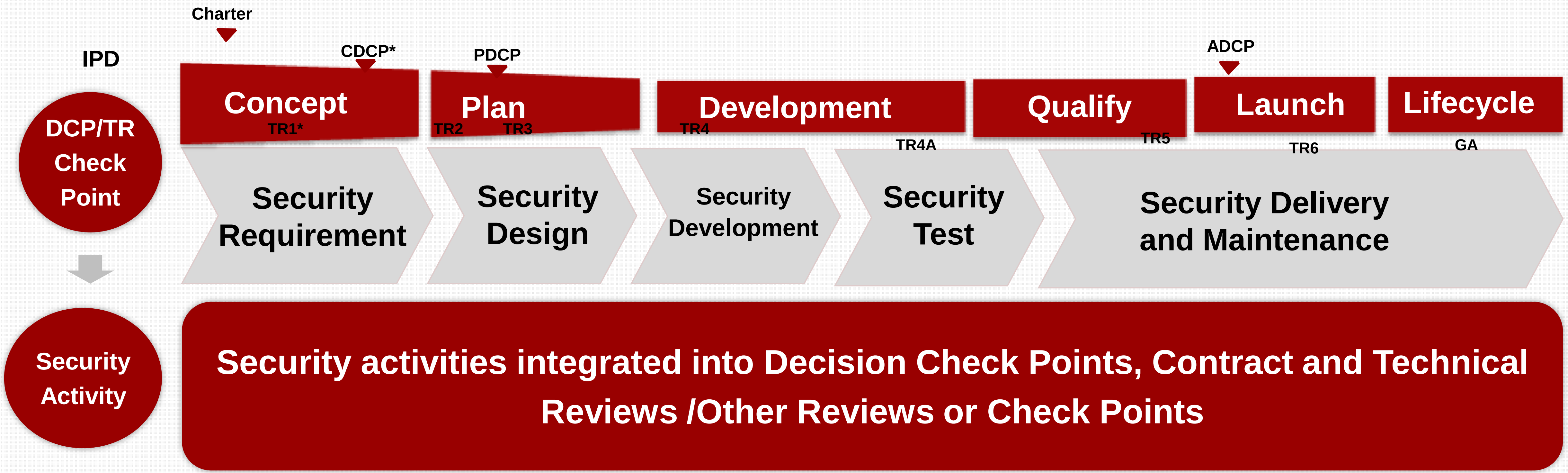
Open source & 3rd party software Management

Security baseline, standards, guidelines, etc...

*DCP= Decision Check Point
TR=Technical Review

Huawei adopts a built-in approach

Security activities in the Integrated Product Delivery (IPD) process



IPD

Charter

CDCP*

PDCP

ADCP

Concept

Plan

Development

Qualify

Launch

Lifecycle

TR1*

TR2

TR3

TR4

TR4A

TR5

TR6

GA

DCP/TR Check Point

Security Requirement

Security Design

Security Development

Security Test

Security Delivery and Maintenance

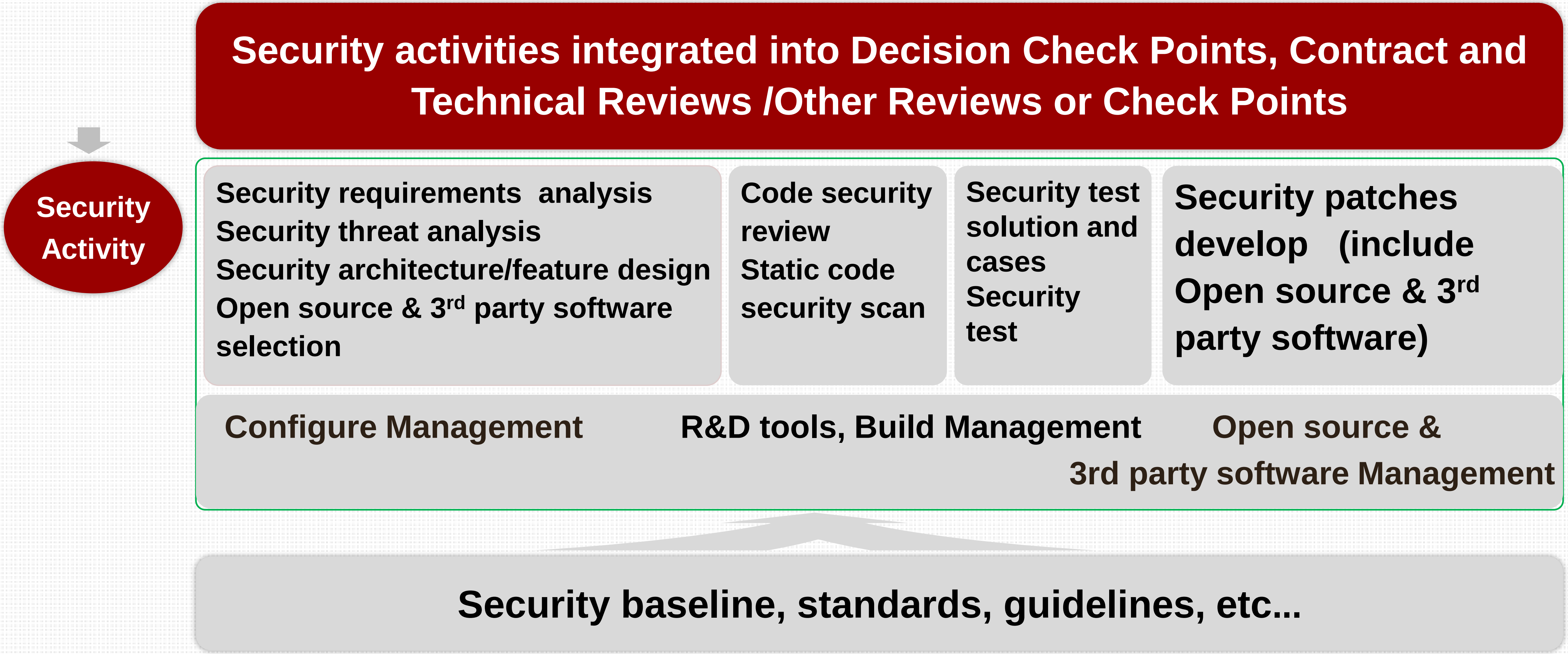
Security Activity

Security activities integrated into Decision Check Points, Contract and Technical Reviews /Other Reviews or Check Points

*DCP= Decision Check Point
TR=Technical Review

Huawei adopts a built-in approach

Security activities in the Integrated Product Delivery (IPD) process



Security activities integrated into Decision Check Points, Contract and Technical Reviews /Other Reviews or Check Points

Security Activity

Security requirements analysis
Security threat analysis
Security architecture/feature design
Open source & 3rd party software selection

Code security review
Static code security scan

Security test solution and cases
Security test

Security patches develop (include Open source & 3rd party software)

Configure Management

R&D tools, Build Management

Open source & 3rd party software Management

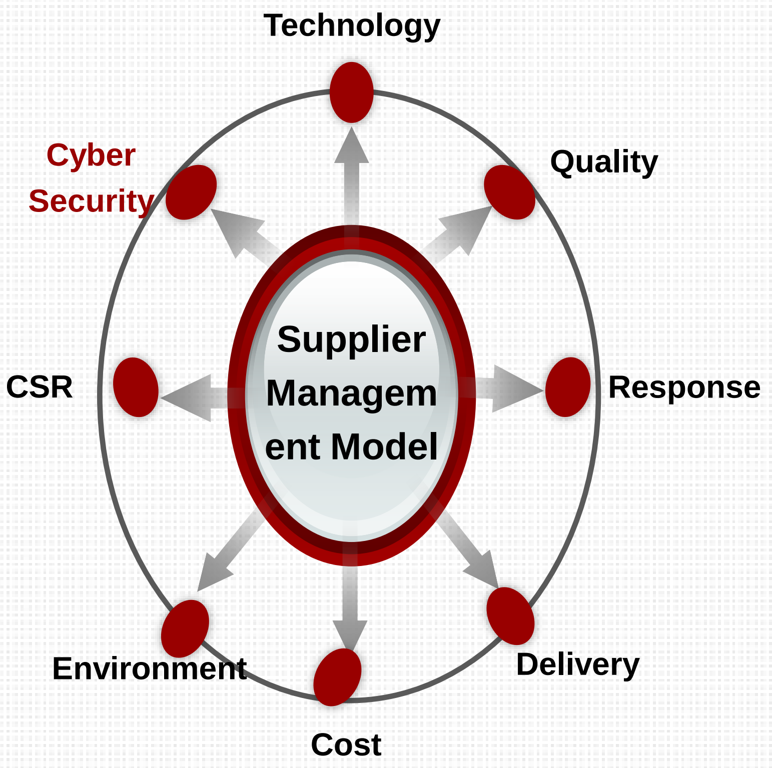
Security baseline, standards, guidelines, etc...

Huawei's Approach

Eight Elements of Supplier Management: TQRDCESS

Security integrated into the procurement business processes, including procurement cyber security policies, baseline, and process criteria.

Supplier Management Model



CSR: customer satisfaction representative
TCO: total cost of ownership

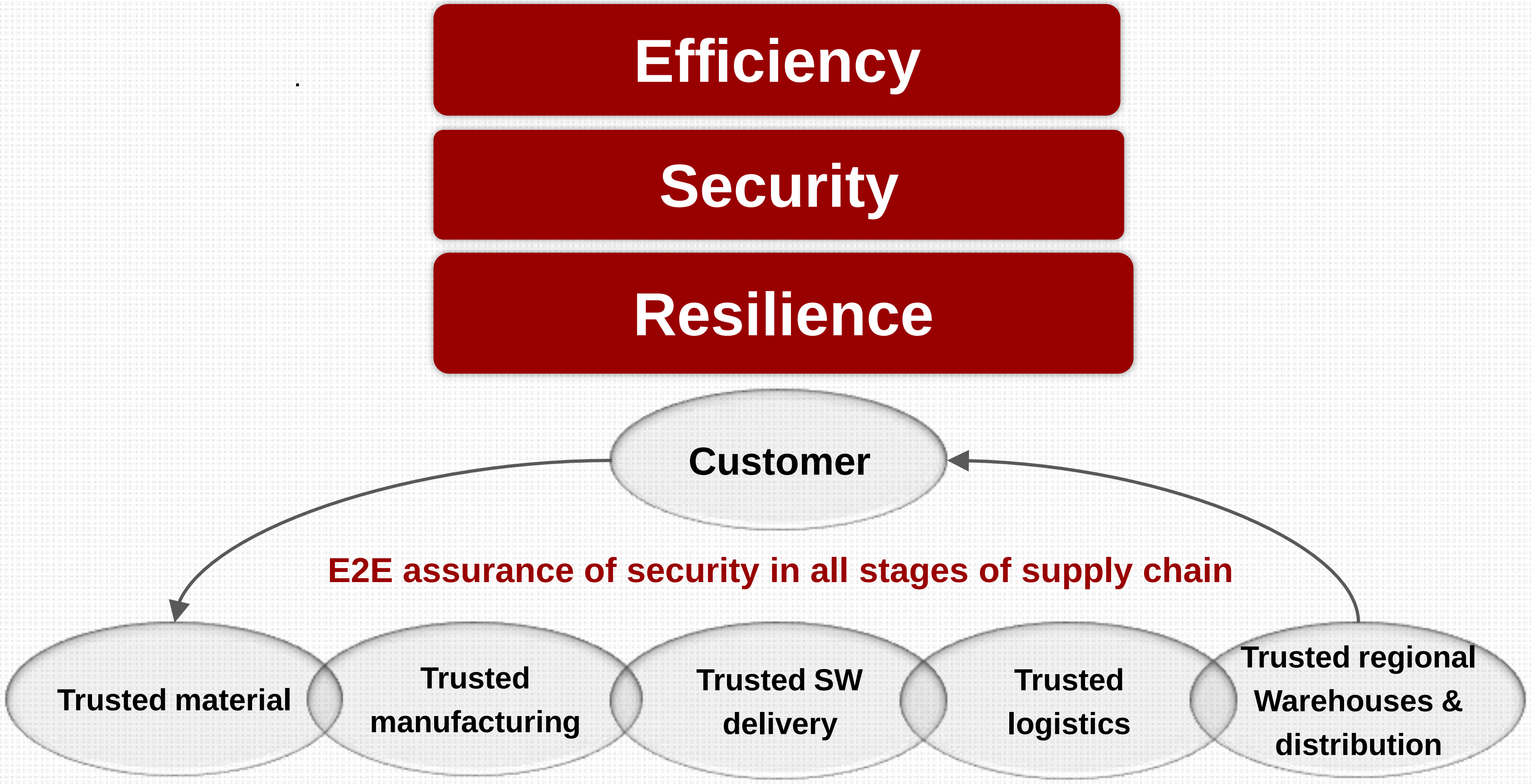
Elements

1. Technology
2. Quality
3. Response
4. Delivery
5. Cost
6. Environment
7. CSR
8. **Cyber security: policy, baseline, process, agreement, training, test, emergency response**

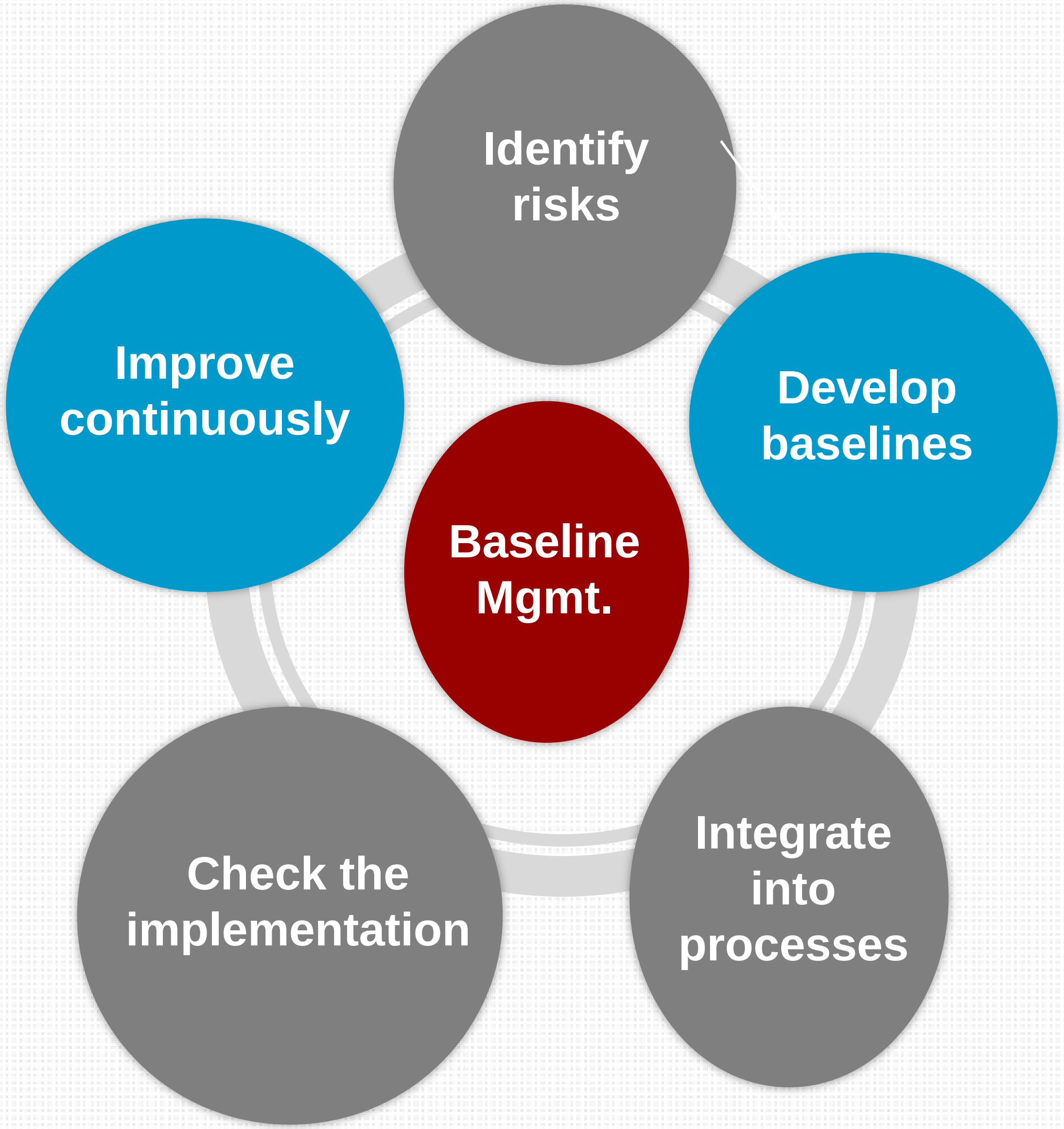
Huawei’s Approach

Supply Chain Security Strategy

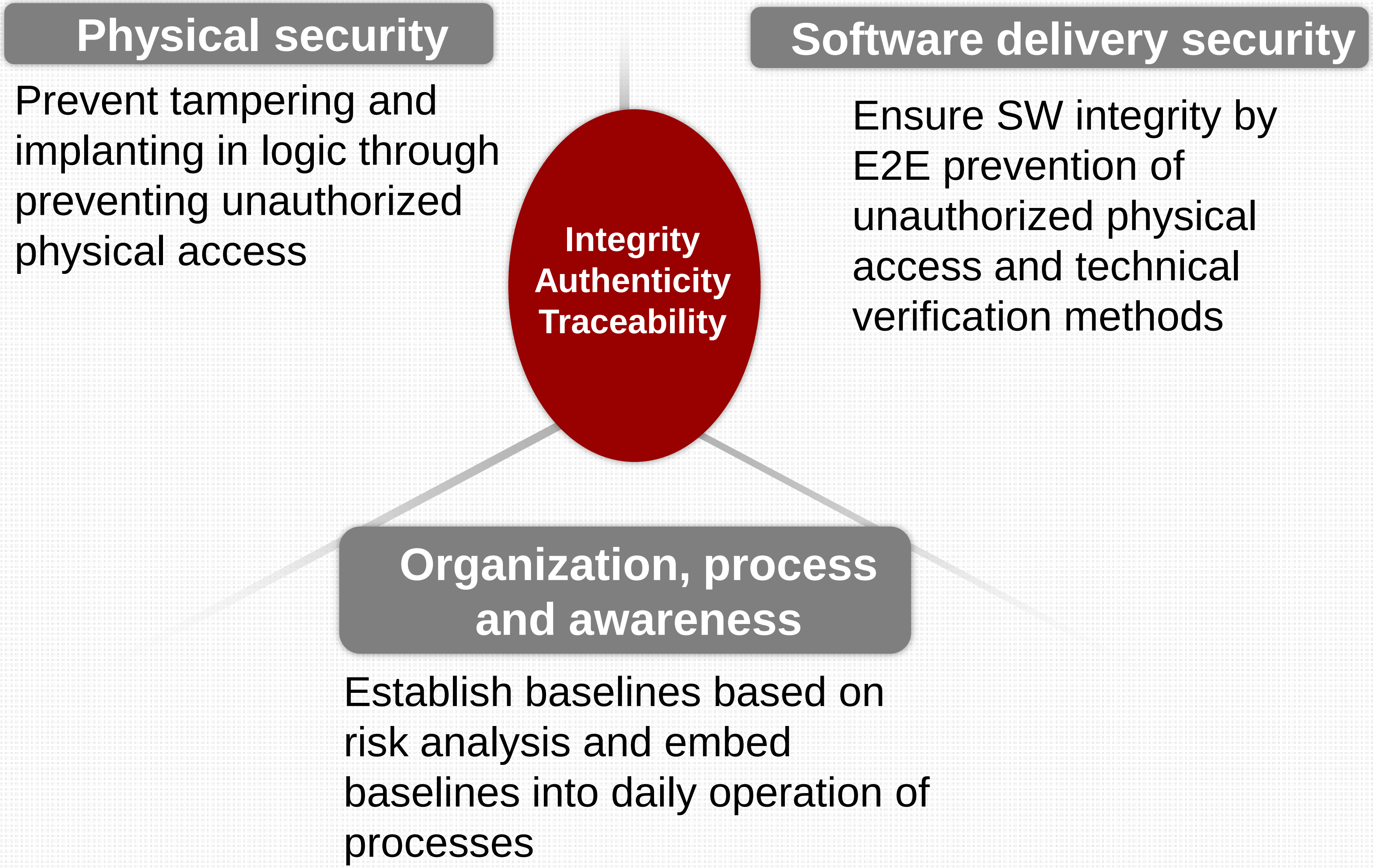
Based on the overall corporate security strategy, we are committed to a supply chain with the following DNA:



Supply Chain Cyber Security Baseline Management



Framework of SCM Cyber Security Baselines



Physical security

Prevent tampering and implanting in logic through preventing unauthorized physical access

Integrity
Authenticity
Traceability

Software delivery security

Ensure SW integrity by E2E prevention of unauthorized physical access and technical verification methods

Organization, process and awareness

Establish baselines based on risk analysis and embed baselines into daily operation of processes

Supply Chain Cyber Security Baseline Management

- Based on risks to the supply chain and customer & government requirements:
  - we develop cyber security baselines, aiming to protect product integrity, traceability, and authenticity, and
  - take a built-in approach to integrate the baselines into processes.
- We have developed nearly 100 baselines around 10 security elements.

Supply Chain Cyber Security Baseline Management

Security elements

- Laws and regulations
- Infrastructure security
- Access control
- Incoming material security
- Manufacturing security
- Software delivery security
- Order fulfillment security
- Traceability system
- Emergency response
- Risk analysis improvement and audit

Deal with risk in a controlled way. High risk/ low risk; high privacy/ low privacy; trusted/ untrusted….

Protect users

Hierarchical key architecture: multi layer security protection of user signaling and user data

Low latency security handover: support fast handover of vehicles in dense network

User identity and privacy protection: enhance the protection of user identity information in heterogeneous access network

Physical Layer Security: enhance the protection of user traffic on the air interface

Can you and your vendors manage in this more complex, architected world?

Deal with risk in a controlled way. High risk/ low risk; high privacy/ low privacy; trusted/ untrusted….

Protect networks, simplify security management

Multi-level and isolated domain: A multi-level and domain-based mechanism is used that divides networks into three security levels: high, medium, and low.

Trusted and Traceable network: Adopt Trusted and Traceable technologies to ensure network security

Unified authentication: Share authentication materials across platforms based on USIM

Aggregate authentication: Aggregate multiple authentication messages into one for authentication on the network side, thereby reducing authentication signaling loads.

Can you and your vendors manage in this more complex, architected world?

Agenda

7 Conclusion

CONCLUSION AND SUMMARY

- Enterprise-wide risk management.
- Collaborate and share information.
- Consider 3rd party risk.
- Buyers should use their collective purchasing power to incentivize assurance.
- Consider the Trusted Technology Provider Standard (ISO 20243).

Thank you.

Andy Purdy

Andy.Purdy@Huawei.com