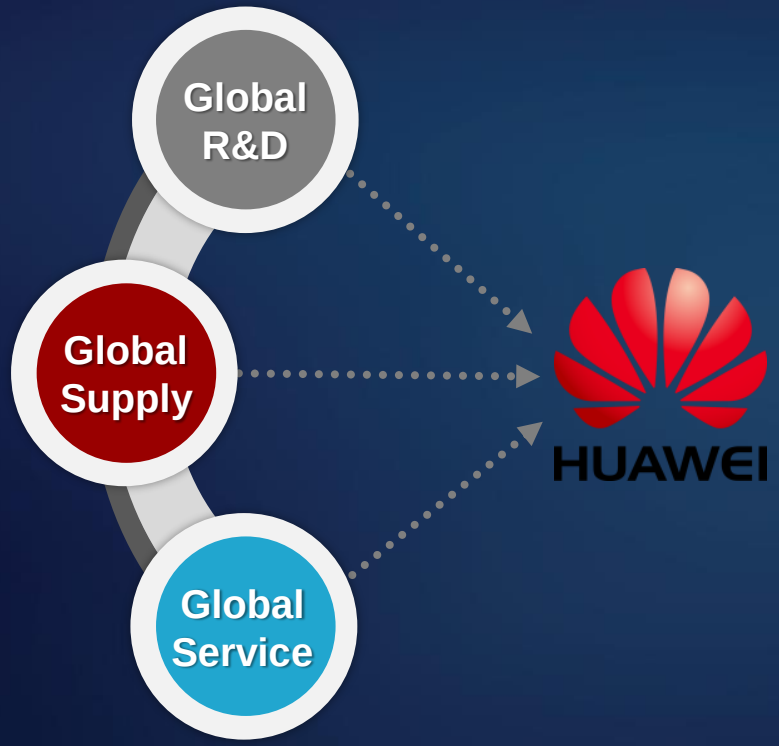
Huawei Cyber Security
-- Strategy and Approach

HUAWEI TECHNOLOGIES CO., LTD.

HUAWEI

We are global – We are facing challenges of global supply chain, cyber security is not a single country or specific company issue



secure products, solutions and services

The Chinese city of Chengdu has 16,000 companies registered and 820 of them are foreign-invested companies. Of these, 189 are Fortune 500 companies. Household brand names such as Intel, Microsoft, SAP, Cisco, Oracle, BAE, Ericsson, Nokia, SAP, Boeing, IBM and Alcatel-Lucent are all located there to name but a few.

Every major telecommunications equipment provider has a substantial base in China :

- Alcatel-Lucent has its biggest manufacturing base globally in China;
- Nokia-Siemens has 14 wholly owned or joint ventures in China, and its factory in Suzhou manufactures a third of its global production of wireless network products;
- Ericsson's joint-venture Nanjing Ericsson Panda Communications Co. has become the biggest supply centre of Ericsson in the world;
- Cisco also has a huge presence in China, with R&D centres in six major cities, Over 25% of all Cisco products are produced by Chinese partners.

Alcatel·Lucent

Nokia Siemens Networks

ERICSSON

CISCO

Cyber security is a Huawei crucial company strategy

Mr. Ren
Huawei CEO

As a leading global ICT solutions provider, we provide information network products and services. The global network needs to be stable at all times. It is our primary social responsibility to support stable and secure networks for customers in any time.

"Huawei hereby undertakes that as a **crucial company strategy**... Taking on an **open, transparent and sincere** attitude, Huawei is willing to work with all governments, customers and partners to jointly cope with cyber security threats and challenges ... Our **commitment to cyber security** will never be outweighed by the consideration of commercial interests."

Our Cyber security vision and mission focusing on the needs of our customers

Vision	**To provide secure, easy and equal access to information services.**
Mission	**Working internationally to develop the most effective approach to cyber security, establishing and implement an end-to-end customer-oriented cyber security assurance system within Huawei, which is transparent and mutually-trusted, so that we ensure customer's long-term security trust.**

Our current focus is on designing and implementing activities to achieve 9 strategic objectives imbedded within our processes. These 9 objectives are common across the majority of challenges we, and others, face

EXTERNALLY FOCUSSED

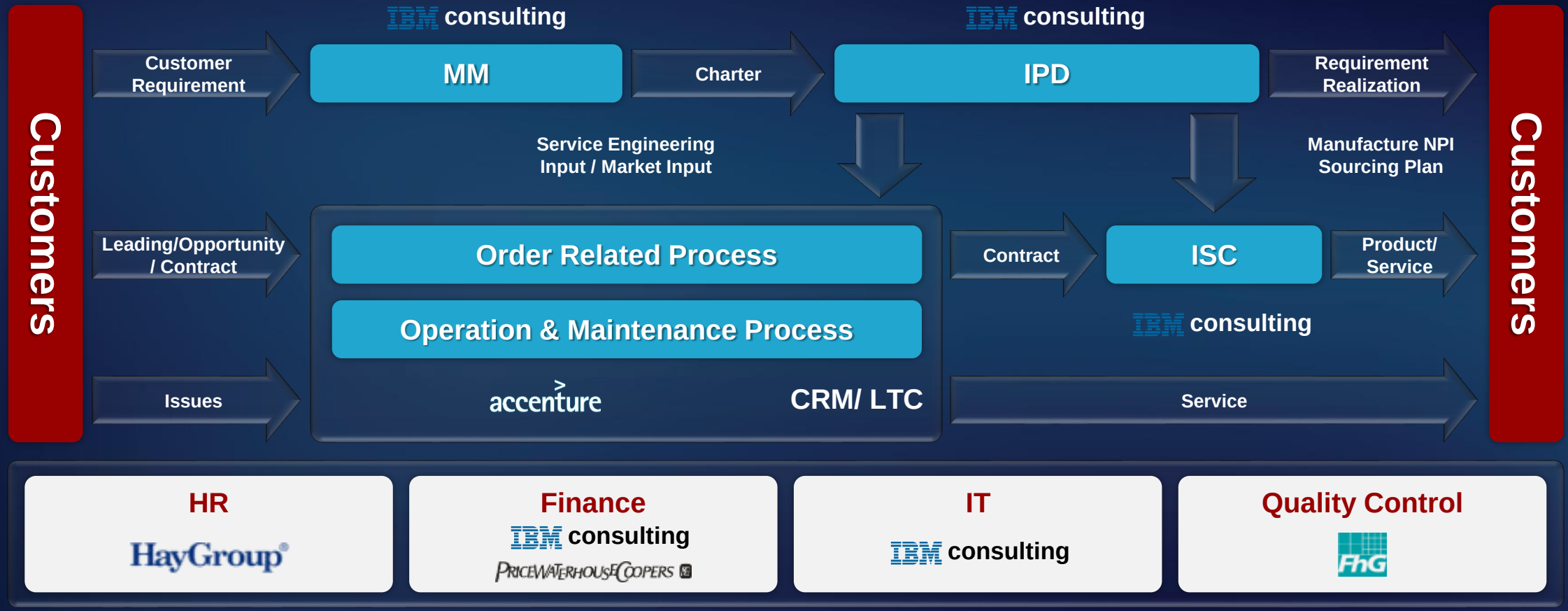
- **OPENESS, TRANSPARENCY AND COOPERATION:** We will actively work with stakeholders in an open and transparent manner to meet and resolve the security challenges and concerns of our customers and Governments.
- **PROACTIVE COMMUNICATIONS:** We will proactively communicate the global nature of ICT and cyber security to as wide an audience as possible encouraging mature debate with a recognition that we must all positively work together and champion international fair, reasonable and non discriminatory standards, policies and regulation.
- **COMPLIANCE WITH LAWS AND REGULATIONS:** We aim to comply with security and privacy protection standards and laws of relevant countries or regions, by analysing these laws and regulations and imbedding these requirements into our products and services and the way we do business. We will ensure the delivered products and services can withstand legal investigations and the result of investigation will prove positive to Huawei.
- **VERIFIED BY INDEPENDENT THIRD-PARTIES:** We will construct and develop a global capability to support independent testing, verification and certification of our products using approved third-parties, so that our customers receive internationally recognized security assurance.
- **EMERGENCY RESPONSE:** We aim to monitor threats on our own technology, national, international and company security vulnerabilities so as to be in a position to responsibly report or pre-warn our customers, respond quickly to threats and apply appropriate security patches to protect our customers.

Our current focus is on designing and implementing activities to achieve 9 strategic objectives imbedded within our processes. These 9 objectives are common across the majority of challenges we, and others, face

INTERNALLY FOCUSSED

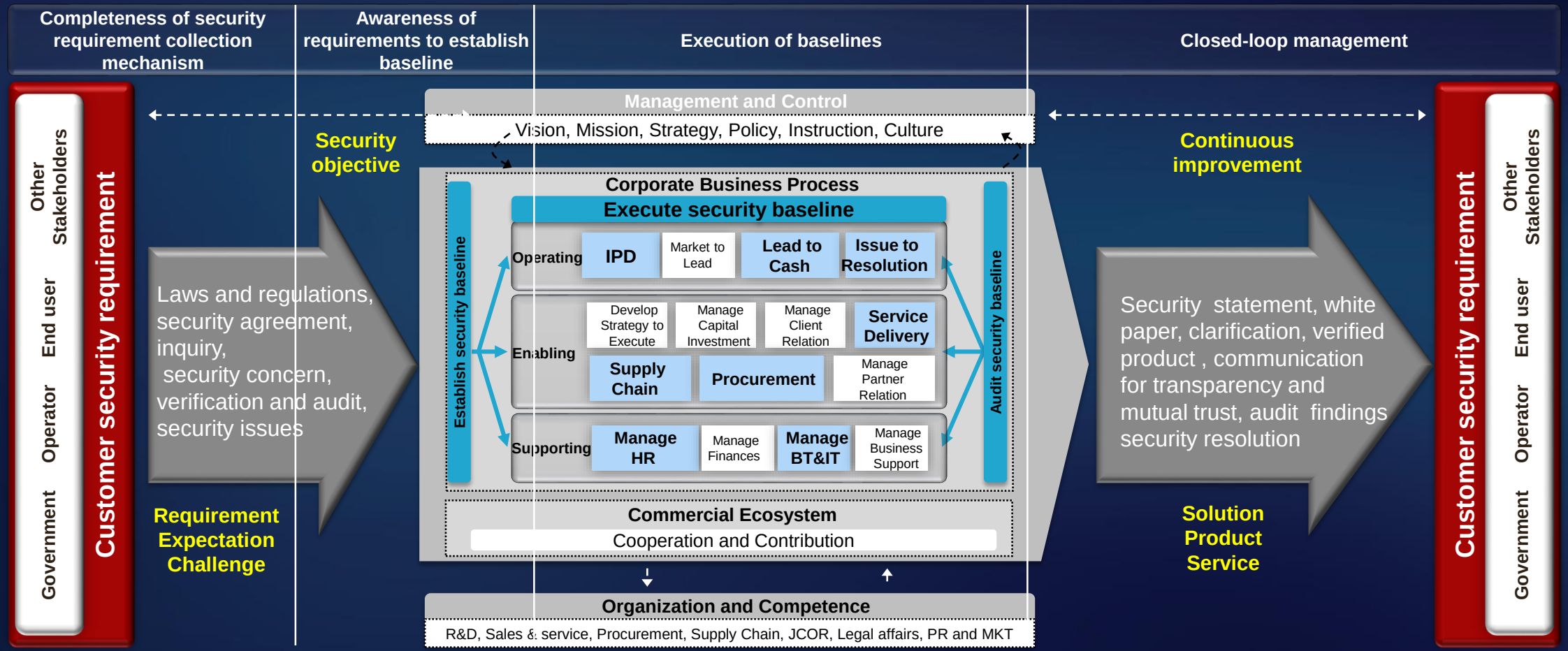
- **EMPLOYEE AWARENESS AND RESPONSIBILITIES:** We will raise employees' cyber security awareness based on law to make them understand they need to bear the liability for their behaviours even without malicious intention. For all critical positions appropriate security qualifications must be obtained and we will take measures to deter employees with malicious intention and prevent the occurrence of malicious acts.
- **SECURE BY DESIGN, DEVELOPMENT AND DELIVERY:** From the continuous analysis of emerging and actual technology threats across our complete product and service portfolio, we will build security into our processes, designs, development & delivery. We will separate out Huawei software from Huawei hardware thus enabling our competitor's software to execute on our hardware avoiding the claim that Huawei technology has hidden capability. We will also split our software so that our base software, country specific software (only allowed to be sold in certain countries) and engineering support tools are all individually approved and under the total control of our customers.
- **NO "BACK DOOR" AND TAMPER PROOF:** We will never knowingly allow a "back door" to be implemented and we will protect the integrity of software by implementing processes to protect against unauthorized tampering and potential breach using technologies such as digital signatures. We will legally manage remote access in case of trouble shooting from our several Global Technical Assist Centres, and never transfer data from customers' network to other country without the customer's permission.
- **TRACEABILITY:** We aim to make relevant products, solutions, services and components traceable through the complete product lifecycle using professional management tools and integrated systems.

Our strategy will be achieved by implementing consistently understood, globally rolled-out repeatable processes on which to imbed the change – a "built-in" strategy – our corporate processes are the foundation stones

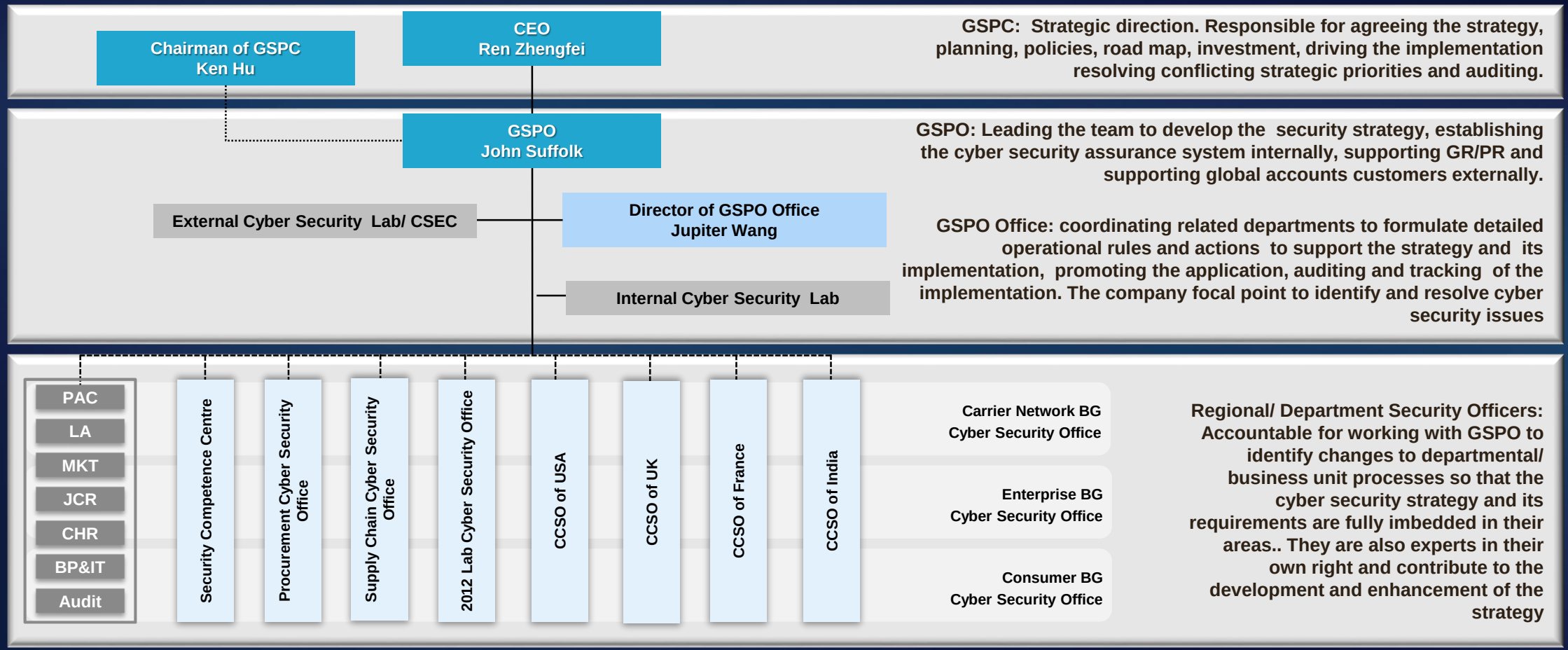


MM: Market Management | **IPD:** Integrated Product Development | **ISC:** Integrated Supply Chain | **LTC:** Lead To Cash

End to End Cyber Security Management covers every process and every part of Huawei including our suppliers



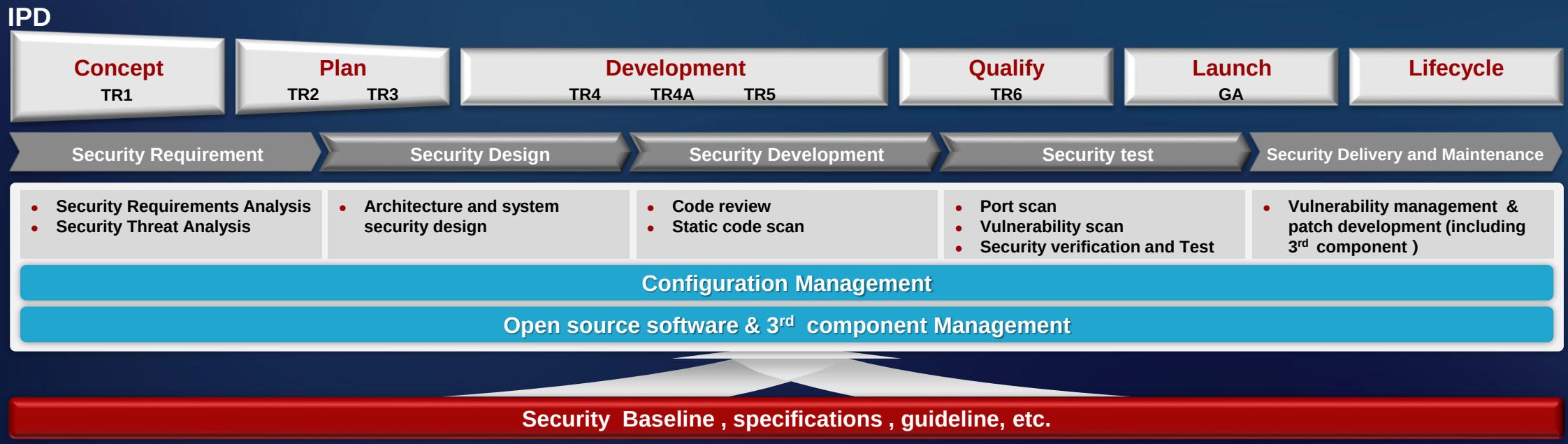
The cyber security strategy is "built-in" to everything we do, including Governance, Audit, Processes, Policies, Procedures, Standards and Objectives



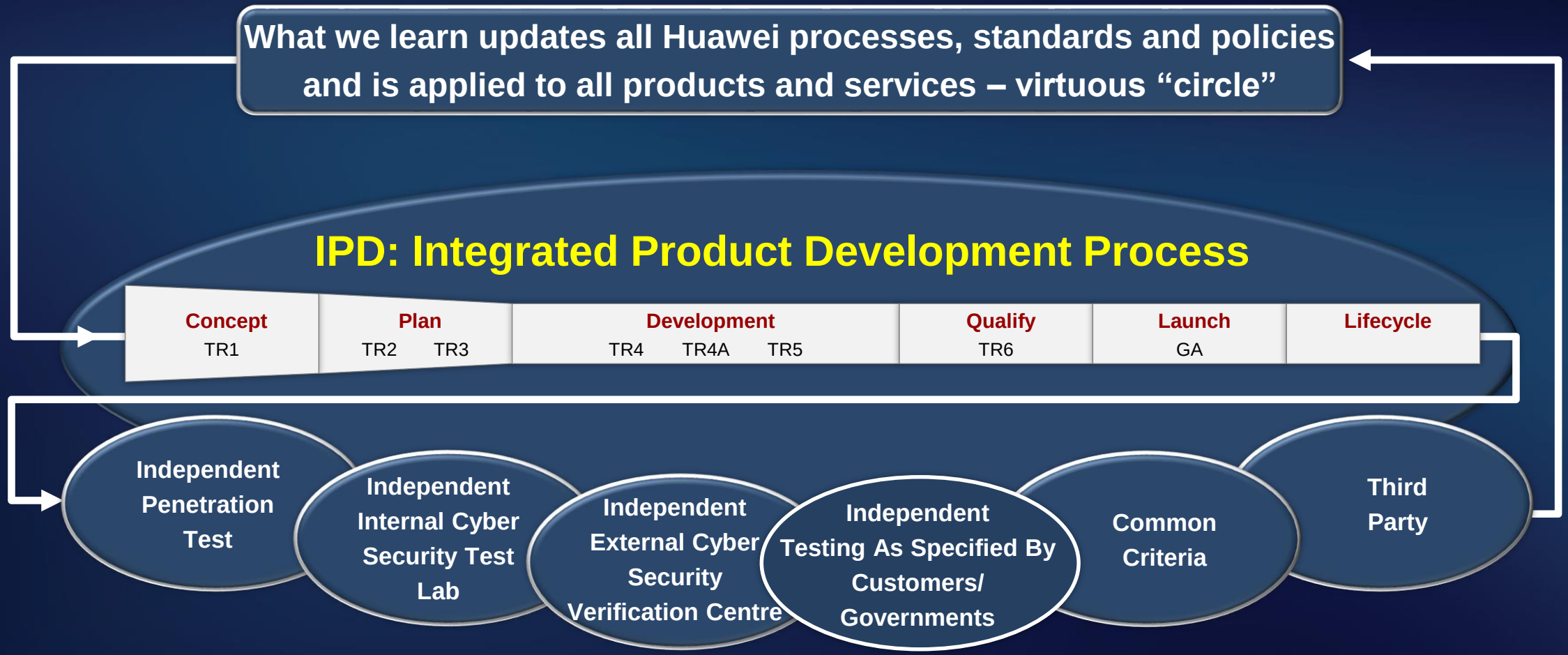
Through our Integrated Product Development Process (IPD) we are continually enhancing our R&D approach, upgrading legacy technology, and developing new technology based on latest thinking – a never ending journey

- IPD was introduced in 1997 from IBM which had been implemented and optimized in Huawei in past over 10 years.
- Since 2010, referred industry security practices (OpenSAMM, SSE_CMM ,etc), have been integrated into the IPD process to improve product security.
- Use configuration management to ensure the integrity, consistency and traceability of R&D process and products.

IPD : Integrated Product Development



We have created a virtuous circle of “many eyes and many hands” ensuring we continuously improve our knowledge our technology, our people and our processes, this creates a win-win-win process – customers, Government, Huawei



Our strength comes from our total focus on our customers, delivering against their requirements and learning from them – we are subject to regular audit and inspection and are probably one of the most reviewed and approved companies

Operator	Test/Audit Areas	Test/Audit Details	What We Learned
BT	21CN and NGA Product Version Test	BT OS security specification compliance test	OS security specification form BT has been adopted into Huawei security specification
vodafone	UMTS Femtocell	Security tests & simulated hacker attacks by Recurity Labs (a 3rd party security consultant)	Enhance Huawei's 3GPP security standard verification method
Deutsche Telekom	Call control, MSAN, SBC, Application Server, MGW	Security tests following 27 DT security specifications Simulated hacker attacks by P3 Network (a 3rd party security consultant)	Make Huawei do more and deeper in security design and test of the following security areas of IMS: service logical security, robustness test and tools
T-Mobile	LTE-SAE, PS core	Security testing in T-Mobile's LTE Project	Enhance Huawei's 3GPP security standard verification method
france telecom	IMS solution	Tests by FT internal security team	Start up the IMS solution security test , including security scanning and anti-attack test, DOS defence, then Huawei minimized OS, hardened Linux and established multi-layer defence

Developing secure technology will be wasted if the delivery and support of the technology is not adequately secured – Secure by delivery

Service Delivery	Consultation and evaluation	Network planning	Network design, rollout and integration	Customer support and assurance	Learning and skill development	Managed service

Business requirement	Information asset management	Access management	Software integrity	Authorization management	Privacy protection	Security design and reinforcement
Behavior requirement	Physical and environmental security	Telecommunication and operation security	Access control	Information systems development and maintenance	Information asset classification and control	

Key points on field operation security :

- Filed operation must obtain customer authorization, the computer must be checked with Antivirus software before accessing to customer network
- the source of software and tools
- Use appropriate recourses on key positions

Key points on local support security :

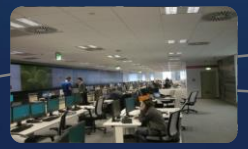
- Data collection and transfer must obtain customer authorization, and comply with the local legal request
- before remote access customer authorization must be obtained
- Use appropriate recourses on key positions

Key points on remote support security :

- before remote access must obtain customer authorization, use third party access software
- The tools and platform accessing to customer network must be auditable
- Delete data promptly according to the authorization request


Site


Equipment Room

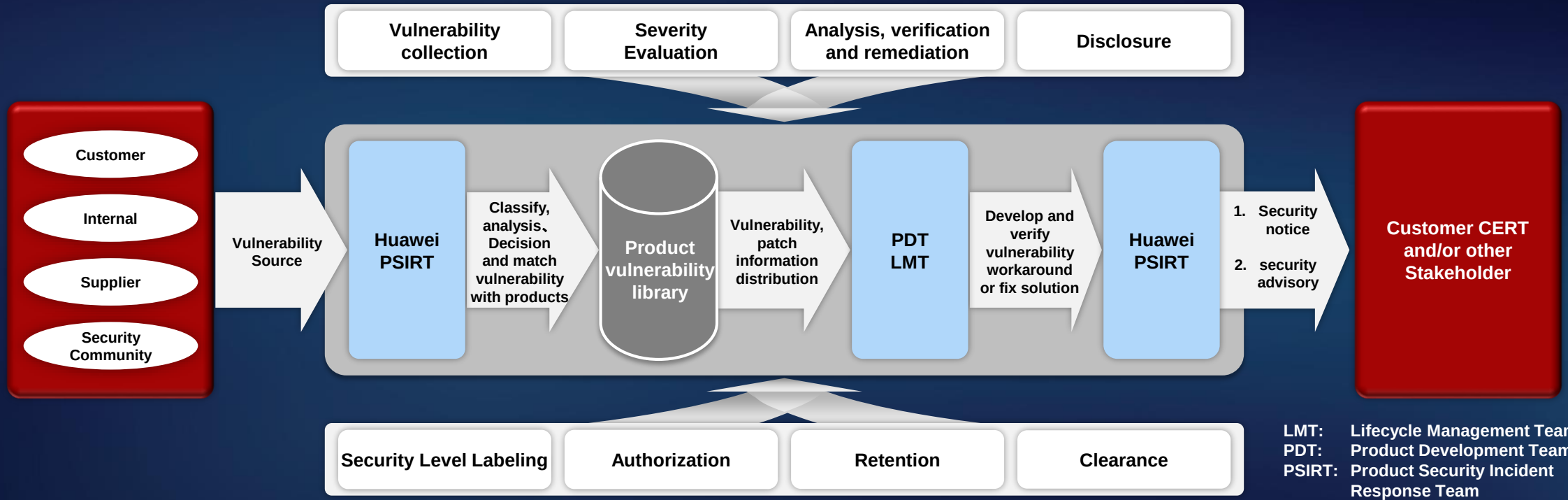

NOC/GNOC


Out of office


TAC


GTAC

We are enhancing our vulnerability management. We adopt responsible disclosure processes with vendors, CERT organizations and security researchers. We coordinate the resolution of the product vulnerability



LMT: Lifecycle Management Team
PDT: Product Development Team
PSIRT: Product Security Incident Response Team

- For different BG customers use responsible disclosure: Carrier Network BG, Enterprise Business BG, Consumer Business BG
- Learn from the industry's vulnerability management best practices: CVSS, CPE, CVRF etc.
- PSIRT response to the vulnerability of the self-development, open source and third-party components, speed up response to the vulnerabilities which are already in the wild

To ensure integrity & traceability from material, production to customer in Supply Chain so that you know you have genuine “clean” un-tampered with products requires comprehensive integrated processes and technology

- ISO28000 supply chain security system operating and 3rd certification.
- Global multi-supply centres to provide efficient and resilient supply to customers.
- Set up barcode system to support multi-ways of tracing.

S-NPI	Plan	Make	Order Fulfillment	Return	Manage Supply Operation

Security of incoming materials

- Identity verification of deliveryman
- Inspection of goods packing
- Review & inspection of goods
- Performance test
- SW integrity check
- Product distribution & pre-production inspection

Security of Factory (EMS)

- Employee security training
- Control of sensitive area
- Separated & controlled production network
- Control of SW & documentation
- SW download verification & QC inspection
- Digital certificate loading & check
- Product 100% anti-virus inspection
- Regular equipment verification
- control of personal account & system authority

Security of logistics & warehousing

- Realize electronic customs declaration, transportation route design & monitoring of logistics process through IT system
- Set up dedicated documents to check & monitor the integrity of containers, shipment &loading
- Seal mgmt & correct sealing

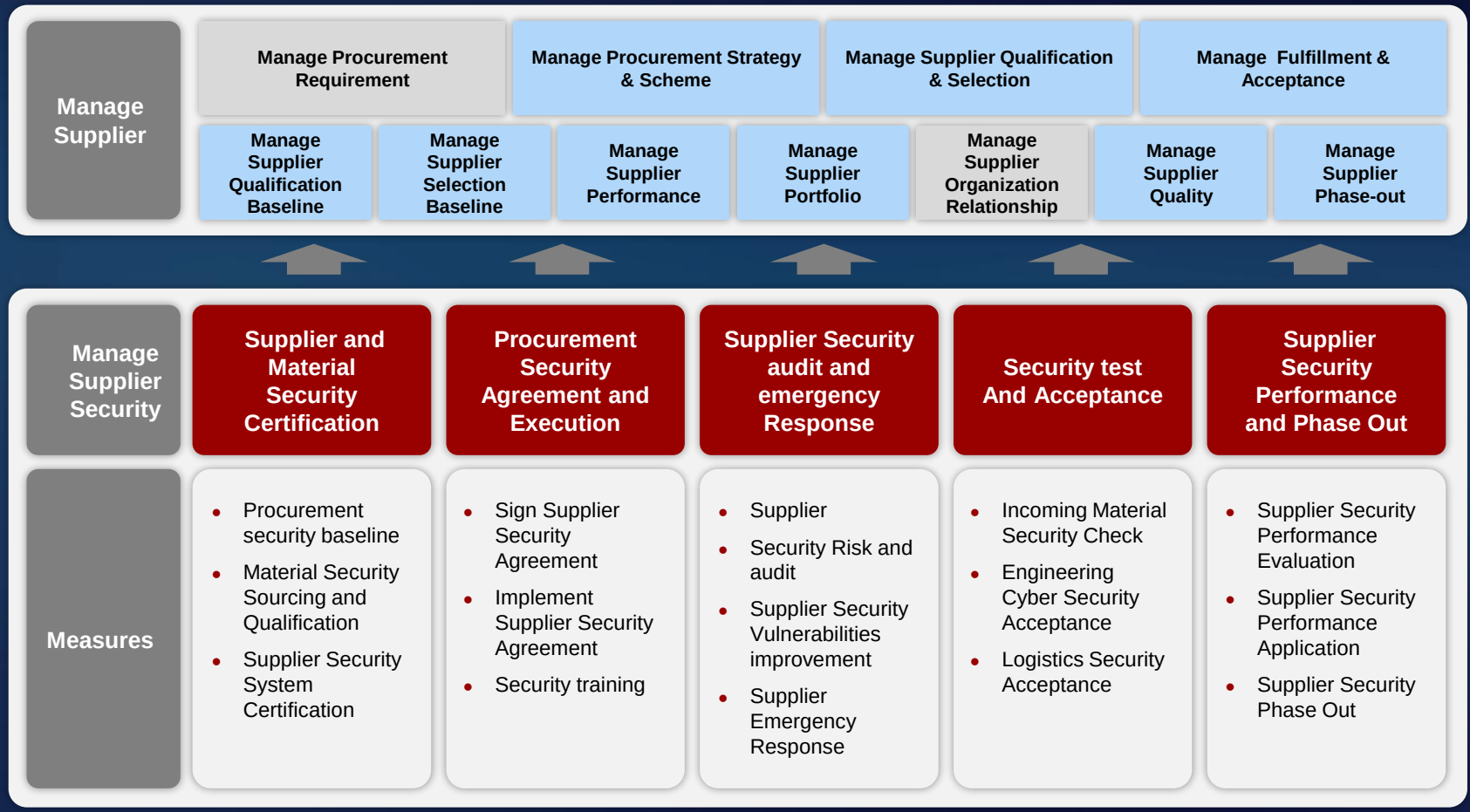
Infrastructure & entry control：7*24 security guard and CCTV monitoring, Electronic entry control & identify identification system

ISO28000 certificate

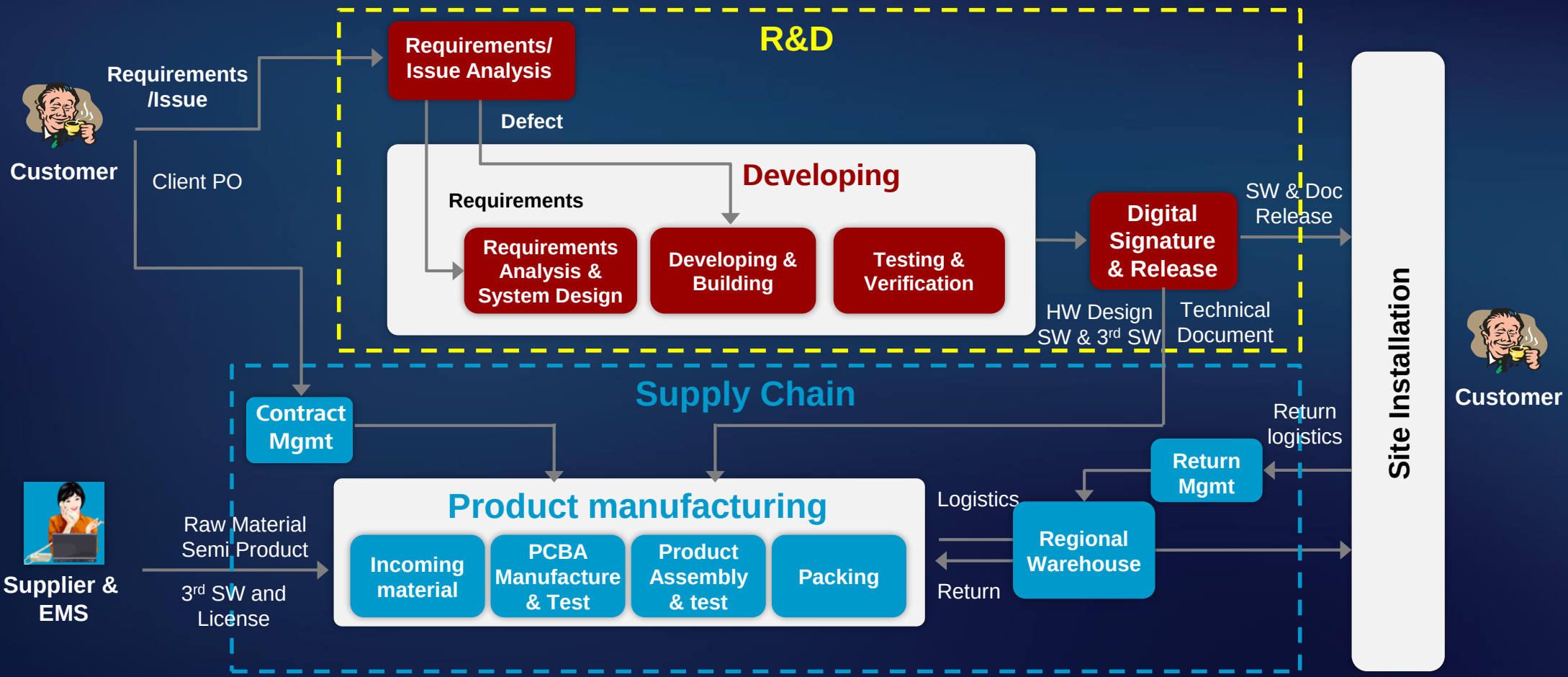
C-TPAT 3rd party audit report

We must work with our Suppliers to effectively reduce potential risks and mitigate security threats

- Security is one of the seven elements of supplier management TQRDCES (Technology, Quality , Response, Delivery, Cost , Environment and CSR, security)
- All suppliers that are related to cyber security must sign the cyber security agreement, and pass the cyber security system qualification
- All materials of cyber security must pass the material security test and qualification.



Huawei have built an E2E traceability system: From customer requirement/issue analysis, developing, to release, and from contract to incoming, manufacturing, regional warehouse to delivery, In order for quick resilience and traceability when any issue happens



Imbedding awareness and understanding of cyber security as well as changing behaviour is a key HR deliverable of the strategy

- HR Strategy & Policy Management
- Organization Management
- Sourcing & Staffing Management
- Leadership & Talent Management
- Employee Relations Management
- Employee Service & Delivery Management
- HR Operations Management

Scheme

Ensure cyber security awareness and foster acceptable behaviour and standards

Process

Embed appropriate cyber security elements into HR process and policies

HR Policy

Our people are the crucial element to ensure we deliver our cyber security strategy. Huawei HR shall clarify the individuals responsibility in relation to cyber security of employees, contractors and third party users. We will also foster their security awareness and ensure conformance to the policies.

Laws & Regulations

In case of any violation of laws or regulations e.g. unauthorized access , illegal control or destruction of technology systems, theft or fraud through client/customer systems or using system or personal data illegally), the person will be criminally/civilly liable for his/her action or omission accordingly.

Closing Thoughts： Threats will never stop, we never stop

- The development of networks has helped to advance social progress. Open networks have encouraged information flow and sharing, provided more opportunities for innovations, lowered the costs of innovation, and has helped improve the world's health, wealth and prosperity.
- Cyber security is not a single country or specific company issue. All stakeholders – governments and industry alike – need to recognize that cyber security is a shared global problem requiring risk-based approaches, best practices and international cooperation to address the challenge.
- As a crucial company strategy, Huawei has established and will constantly optimize an end-to-end cyber security assurance system.
- This is a continual effort, and Huawei is committed to providing best-in-class products and services to meet the needs of our customers. We take cyber security seriously and have invested substantial resources into our efforts to promote and improve the ability of our company, our peers and others to provide the best-possible security assurance and ensure a safer and more secure cyber world for all.

Thank you