ZTE

ZTE Cybersecurity White Paper

Providing Customers with Secure and Trustworthy Products and Services

Security in DNA, trust through transparency

Zhong Hong Chief Security Officer of ZTE Corporation

October, 2021

Acknowledgements

Thank you to Antonio Relvas, Cao Kunpeng, Chris Mulley, Dai Heng, Gao Ruixin, Hao Wenrui, He Ying, Hua Guohong, Jiang Guobing, Jiang Lu, Li Xing, Li Yiyi, Liu Hui, Liu Risheng, Ma Zhiyuan, Marco Costantini, Ping Li, Song Weiqiang, Tang Keke, Wang Dongmin, Wang Huagang, Wang Yuzhong, Wei Yinxing, Xu Guorong, Yang Guirong, Yang Tiejian, Yin Lingling, Yu Ting, Zhang Jinxin, Zhang Jun, Zhang Li, Zhao Bo, Zheng Jun, Zhu Linlin, for your invaluable contributions to the completion of this work.

I would also like to thank everyone who provided support for the publication of this white paper.

Zhong Hong

Chief Security Officer of ZTE Corporation

Contents

Preface

Telecommunications equipment and systems, as critical infrastructure for a nation, have been widely valued by governments, operators, and users worldwide. Currently, the deployment of 5G has begun. Featuring faster speed, greater network capacity, and ultra-low latency, 5G will redefine the operation of critical infrastructure from the factory floor to the cloud. Its new technologies including Software-Defined Networking (SDN), Network Function Virtualization (NFV), Multi-access Edge Computing (MEC), and network slicing are paving the way for smart cities, remote surgery, autonomous vehicles, and large-scale Internet of Things (IoT) connectivity. However, these features increase the attack surfaces of 5G networks, thereby triggering more security challenges and concerns. According to World Economic Forum Strategic Intelligence[1], impending growth in the number of connected devices and a related proliferation of sensitive data demands comprehensive device- and cyber security measures. The GSMA's *Mobile Telecommunications Security Landscape*[2] also states that 5G security needs to be a focus now, as it will be much more difficult to build in security after it is widely rolled out.

In the course of the development of 5G, security has also been strengthened as never before. From the formulation and compliance of industry standards, coordinated vulnerability response and disclosure, to comprehensive security measures for manufacturers, the entire industry and stakeholders are working together to enhance cybersecurity.

[1] *WEF Strategic Intelligence – 5G Security and Critical Infrastructure:*
https://intelligence.weforum.org/topics/a1G0X000006NvAbUAK/key-issues/a1G0X000006NvtqUAC

[2] *GSMA Mobile Telecommunications Security Landscape:*
https://www.gsma.com/security/wp-content/uploads/2021/03/id_security_landscape_02_21.pdf

As a leading global provider of integrated communications solutions, ZTE is dedicated to ensuring network equipment security, providing customers with secure and trustworthy products, thus improving global users' experience through secure and reliable network connections, and fostering the digital transformation of industries.

ZTE 's principles and positions on cybersecurity are as follows:

Cybersecurity is ZTE's highest priority for product R&D and delivery. In accordance with the company's strategic development plan, we follows industry standards and best practices to establish and improve cybersecurity governance structure, promote a culture of security awareness, and emphasize security in the whole business process.

ZTE communicates and cooperates with customers, regulatory agencies, partners, and other stakeholders openly and transparently, abides by relevant laws and regulations, respects the legitimate rights and interests of customers and end-users, continuously improves management and technical practices, and provides secure and trustworthy products and services that support our customers in establishing a secure network environment.

Executive Summary

The 5G era has come. Cloud computing, networking, big data and artificial intelligence technologies have become more widely used. While the application of new technologies has brought industrial transformation, more cybersecurity challenges have emerged. On the one hand, global cybersecurity threats and cyber crimes are rampant. Verizon's 2021 Data Breach Investigations Report[3]explores cybersecurity situations in many industries worldwide, and analyzes 29,207 cybersecurity incidents, including 5,258 confirmed data leakage incidents in 2020. By the end of July 2021, exposed CVE vulnerabilities reached 161,750[4], in which severe vulnerabilities account for 11.6% and high-risk vulnerabilities account for 20.8%. According to ENISA's 2021 Threat Landscape for Supply Chain Attacks[5], since early 2020, the community seems to have been facing a greater number of more organized attacks. It may be that, due to the more robust security protection that organizations have put in place, attackers successfully shifted towards suppliers.

As a telecom infrastructure provider, ZTE not only is a supplier of network operators, but also plays an extensive role in a complex supply chain. ZTE attaches great importance to customers' security, complies with relevant laws and regulations on security, and is committed to delivering secure and reliable products and services to customers. At ZTE, cybersecurity is the highest priority for product R&D and delivery.

[3] *2021 Data Breach Investigations Report: https://www.verizon.com/business/resources/reports/dbir/*

[4] *Data source: https://www.cvedetails.com/*

[5] *Threat Landscape for Supply Chain Attacks: https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks*

With the more complex and changing business environment, especially in the current context of the global COVID-19, ZTE is committed to creating a secure, reliable and flexible supply chain for customers, and delivering secure and reliable products and services. ZTE has established a sound product security governance system, attaches great importance to cultivating the cybersecurity awareness of all its employees, continuously strengthens the cybersecurity assurance of the entire supply chain. At ZTE, security controls have been integrated into the entire product life cycle, based on the principles of security by design and security by default.

This white paper systematically introduces how ZTE uses industry standards and best practices to implement top-down, risk-based cybersecurity governance throughout the product life cycle.

For supply chain, ZTE emphasizes the security and credibility of manufacturing and guarantees continuity and resilience of supply.

For R&D, ZTE adopts the security by design principle to ensure that the product development process is secure and controllable through the continuously improved process.

For engineering service, ZTE complies with standardized operations to ensure the secure delivery of products and services.

The white paper also emphasizes the importance of security maturity verification. ZTE complies with industry technical standards, certification systems, and evaluation frameworks, and leverages its cybersecurity labs to enable customers, regulators, and stakeholders to verify security of ZTE products in a convenient, effective and transparent way.

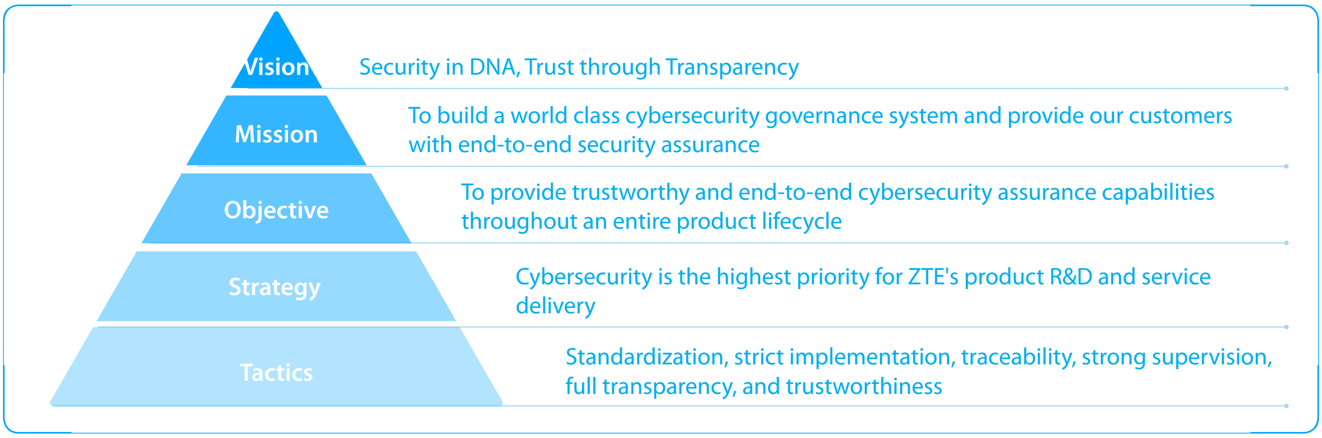
ZTE is committed to providing customers with secure and trustworthy products and services, ensuring the security of communications network equipment, to realize digital transformation enabled by 5G networks. As we know, cybersecurity needs to be safeguarded by the entire industry and all stakeholders, so that global users can fully enjoy the digital life brought about by the transformation of communications technology.

ZTE Cybersecurity Strategy

The communication network is a complex and huge system, involving a large amount of software, hardware and data systems. Ensuring the confidentiality, integrity and availability of these assets is the basis for the secure operation of the network. Due to the diversity and complexity of cybersecurity threats, communication networks must be resilient and resistant to cybersecurity attacks and interference. This is the challenge and responsibility for both equipment suppliers and operators.

ZTE has established an effective cybersecurity governance system based on risks, covering the entire product life cycle.

"Security in DNA, trust through transparency" is ZTE's vision on cybersecurity. Abiding by laws and regulations, following industry standards and customer needs, ZTE is committed to delivering secure and trustworthy products and services to customers, ultimately to enable connectivity and trust everywhere[6].



Vision: Security in DNA, Trust through Transparency

Mission: To build a world class cybersecurity governance system and provide our customers with end-to-end security assurance

Objective: To provide trustworthy and end-to-end cybersecurity assurance capabilities throughout an entire product lifecycle

Strategy: Cybersecurity is the highest priority for ZTE's product R&D and service delivery

Tactics: Standardization, strict implementation, traceability, strong supervision, full transparency, and trustworthiness

Figure 1 Vision and Mission of ZTE Cybersecurity

[6] *ZTE's Corporate Vision: to enable connectivity and trust everywhere*

Risk-based Cybersecurity Practices

Cybersecurity Governance Architecture Based on the Three Lines Model

Enterprises and organizations need highly-efficient risk management through mature governance architecture. The three lines model[7] issued by the Institute of Internal Auditors (IIA) helps enterprises or organizations identify the most useful management structure and processes to achieve goals and clarifies all the respective roles and responsibilities of stakeholders so as to support governance and risk management more effectively.

ZTE has set up an organizational architecture based on the three lines model to promote cybersecurity governance. This structure solves conflicts of interest by setting security organizations independent from the first-line business units. It effectively assures cybersecurity from multiple perspectives and multiple levels through self-inspection by business units of the first line, the independent security assessment of the second line, and the security audit of the third line.

[7] *The IIA's Three Lines Model: https://www.iia.org.au/technical-resources/professionalGuidance/the-iia's-three-lines-model*

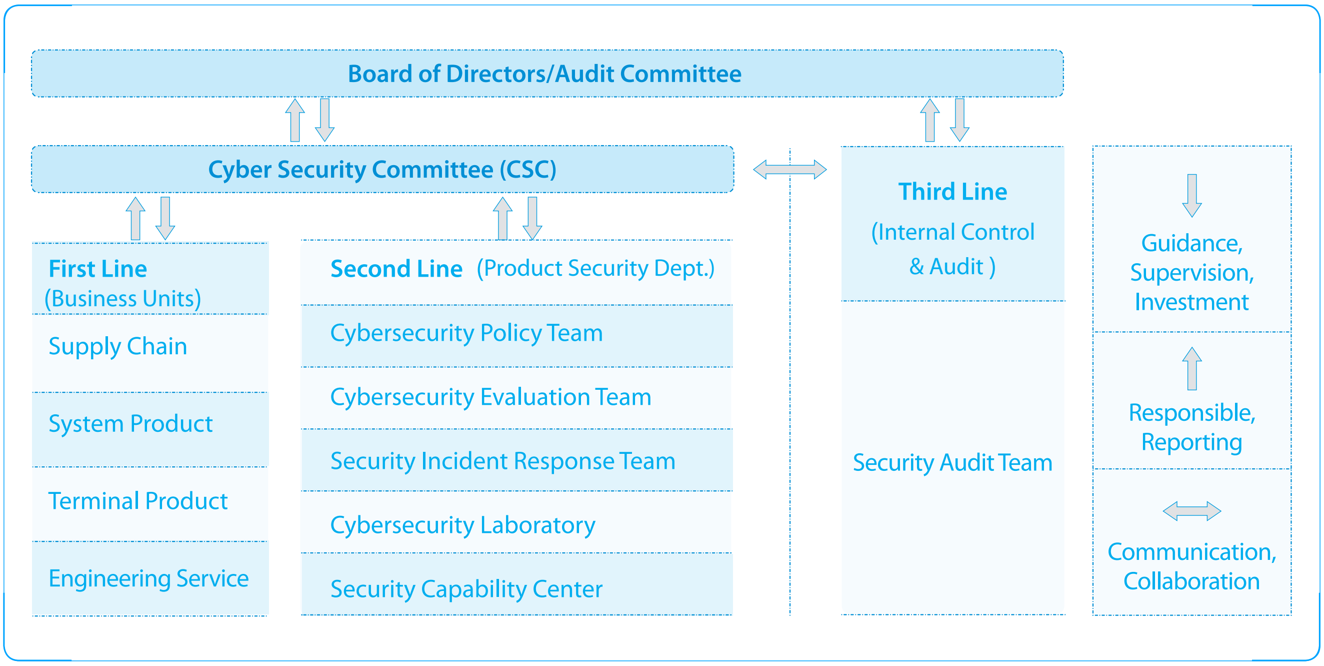

Board of Directors/Audit Committee
Cyber Security Committee (CSC)
First Line
(Business Units)
Supply Chain
System Product
Terminal Product
Engineering Service
Second Line (Product Security Dept.)
Cybersecurity Policy Team
Cybersecurity Evaluation Team
Security Incident Response Team
Cybersecurity Laboratory
Security Capability Center
Third Line
(Internal Control & Audit)
Security Audit Team
Guidance, Supervision, Investment
Responsible, Reporting
Communication, Collaboration

Figure 2 Cybersecurity Governance Architecture Based on the Three Lines Model

Board of Directors/Audit Committee

The Board of Directors supervises and guides the Cyber Security Committee (CSC) to carry out cybersecurity governance work. And the Internal Control & Audit Department regularly reports security audits to the Board of Directors/Audit Committee.

Cyber Security Committee (CSC)

The top decision-making organization responsible for the cybersecurity work of ZTE. The CSC formulates cybersecurity policies and guarantees resources, determines the strategic direction and objective of the cybersecurity work, reviews cybersecurity plans, and decides on major issues related to cybersecurity.

First Line

Business units are the first line for cybersecurity governance. Each business unit realizes its own cybersecurity controls through the processes and procedures approved by the CSC covering planning, implementation, detection and improvement of cybersecurity.

For R&D: embedding security controls into the whole life cycle of the R&D process; assessing and controlling the security risks in the process of technical reviews and version releases of each project; following security principles including security by design (SbD) and privacy by default (PbD) into R&D requirements, design, implementation, verification and release processes; performing penetration testing and regular security regression testing; and continuously tracking, analyzing and resolving security vulnerabilities of third-party components used by products.

For supply chain: embedding security requirements into the process of verifying suppliers and newly introduced materials; communicating cybersecurity requirements to suppliers through the Supplier Security Agreement, and regularly auditing suppliers; establishing the material testing laboratory for sampling inspection of medium- and high-risk materials; and establishing a dedicated network in the production environment to isolate potential security attacks.

For engineering service: continuously benchmarking against the NIST CSF[8] to ensure security governance of the whole business process; building a cross-field professional team to achieve efficient operation and secure delivery.

Second Line

ZTE's Product Security Department is the second line for cybersecurity governance. As a permanent agency of the CSC, the Product Security Department is responsible for promoting the implementation of all management and technical practices related to cybersecurity, coordinating the construction of cybersecurity policies and procedures, inspecting security implementation, and supervising and evaluating the progress of the first line.

The department provides security enpowerment and professional support for business units, assists business units in risk management, and performs independent security assessments to evaluate and supervise first line security practices, and reviews security from multiple perspectives.

The independent security assessment includes process evaluation and product evaluation. The former is used to evaluate the compliance and effectiveness of the security governance implementation processes of business units, and the latter is used to analyze and evaluate the security of products and systems, including vulnerability scanning, code review, protocol robustness testing and penetration testing.

The Product Security Department implements closed-loop management and tracking of problems found in independent security assessments. If any violation of product security red lines[9] is found during the security assessment, the Product Security Department has the right to immediately suspend the corresponding business activities until the product teams fully rectify the identified security issues.

Also, ZTE activitly partners with third-party organizations to evaluate the security of ZTE products, including source code review, security design review, and penetration testing.

[8] *NIST Cybersecurity Framework: https://www.nist.gov/cyberframework*

[9] *ZTE Product Security Redline defines the basic security requirements of ZTE business processes, products and services, which are the must-meet standards for all business units.*

Third Line

The Internal Control & Audit is the third line for monitoring and evaluating cybersecurity governance. Through the independent evaluation of the robustness, rationality and effectiveness of the company's cybersecurity assurance system, the Internal Control & Audit ensures the effective implementation of cybersecurity policies, standards and procedures for the company's management, customers and stakeholders. The Department is also responsible for auditing the first and second lines, including the conformity checks and security testing of the procedures, and reporting the audit results to the Board of Directors and the Audit Committee. The Internal Control & Audit can jointly audit the security implementation of ZTE with external third-party auditors.

With risk-based internal control audits, ZTE continuously examines the maturity and effectiveness of the company's cybersecurity assurance system to ensure that security needs of customers and stakeholders can be met.

Cybersecurity Regulation System

ZTE has established robust cybersecurity policies, standards, procedures, and guidelines. The cybersecurity policies specify the basic requirements for cybersecurity governance. ZTE has also issued a series of security management standards and specifications, which are under regular review. Each business unit carries out practical security activities following these security specifications. During the implementation processes, corresponding results and records are kept available as evidence to relevant parties for auditing.

ZTE cybersecurity documentation system is divided into four layers:

The first layer

The general requirements of cybersecurity is the outline of ZTE’s overall cybersecurity strategy. All underlying documents are based on this cybersecurity policy system. Based on the methods of NIST's system security engineering[10], ZTE has established cybersecurity policies covering the entire life cycle of the system with reference to hundreds of laws and regulations, security standards, security best practices, and customer security tenders, involving the whole business processes of R&D, supply chain, engineering and services, and incident response. The cybersecurity policy is used as a benchmark for identifying shortcomings of internal processes and specifications and evaluating implementation effectiveness.

[10] *https://csrc.nist.gov/publications/detail/sp/800-160/vol-1/final*

The second layer

Cybersecurity management regulations and procedures, which support the operation of the security policies. It includes a series of security standards and procedures from supply chain to R&D, delivery and incident response, such as R&D security standards, supply chain security management regulations, engineering service security management regulations, vulnerability response procedures, security incident response procedures, and security tools management regulations.

The third layer

Cybersecurity guidelines, which are documents that support the regulations and procedures, such as security design guidelines, secure coding specifications, security baseline preparation guidelines, and the security hardening guidelines.

The fourth layer

Cybersecurity records of the implementation of processes and results, such as source code scanning reports, security testing reports, vulnerability analysis records, and security incident review reports.

Security Awareness and Capability Building

ZTE attaches great importance to capability building in both security awareness and skills. It has established a comprehensive talent cultivation mechanism combining career development and training for specialized cybersecurity personnel, who cover fields of security standards, security planning, security design, secure coding, security tools, penetration testing, security operation and maintenance (O&M), etc.

By Q3 2021, more than 170 employees held international security certifications, such as the CISSP, CISA, CISM, CSSLP, CEH, OSCP, to name a few. They help improve the level of the overall security governance, and enhance the capability of security teams.

As for training, ZTE organizes a variety of security training programs in security awareness and capability enhancement for different target groups, for example, seminars and study meetings for managers, orientation and security awareness training for all employees, professional certification courses for security experts, penetration testing and secure coding competitions for engineers. Most training programs end with exams and combine theoretical and practical procedures. To assess the effectiveness of the training, ZTE adopts the Kirkpatrick Model, a globally recognized method for evaluating the results of training and learning programs to improve training programs in a closed-loop manner and increase satisfaction of employees.

In addition, ZTE also has a culture of promoting a variety of security-related information, such as cybersecurity news, cutting-edge security technologies, best practices, to all employees, and organizing security technology conferences, security open days, sharing of case studies and other activities. Through various forms of interesting activities, security awareness education penetrates into the daily work of employees.

Cybersecurity Assurance Throughout the Full Product Life Cycle

The security of a system is affected by each part of the system, and the weakest point determines the overall security strength. ZTE’s security assurance includes supply chain, R&D, engineering services, incident management, and supporting functions, coving the full product lifecycle, and is continuously optimized against industry standards and best practices.

Building a Secure, Reliable and Resilient Supply Chain

Risks and Challenges Faced By Supply Chain

At present, it is widely recognized that the supply chain of the ICT industry is more complex than that of traditional industries, and the probability of security risks is more significant. Especially in the 5G era, 5G network's complexity, modularity, and the separation of software/hardware enable customers to diversify their choices of suppliers, and behind each supplier is a whole supply chain, where any problem in any link may cause a series of consequences. For example, FragAttacks' WiFi series vulnerabilities affected multiple third-party component suppliers. These suppliers needed to cooperate to respond to and repair the vulnerabilities.

Countries worldwide continue to bring out laws and regulations, and optimize industry standards. For example, the US Department of Commerce (DoC) released the regulation on "Securing the Information and Communications Technology and Services Supply Chain"[11]in 2019, which proposed new requirements for 5G products and services. The industry assessment scheme GSMA NESAS (Network Equipment Security Assurance Scheme) release 2.0[12] specifically added a new requirement (absent from release 1.0) for the security of third-party components in the supply chain, to reduce the possibility of equipment suppliers procuring and using vulnerable, contaminated, and unsupported third-party components in the supply chain. All new requirements bring new challenges to the supply chain development and management of enterprises.

Meanwhile, customer requirements are becoming more demanding, and market demand and supply fluctuate sharply. Since the beginning of this year, the pent-up demand due to COVID-19 has erupted. For example, the overall growth of renewable energy vehicles, laptops, mobile phones, servers, etc. requires a high supply of chipsets, but supply chain was weakened due to short supply and lengthened material supply cycle.

In general, regulators and customers increasingly extend their attention to not only the security of network equipment suppliers, but also the security of their sub-suppliers. Also, they expand their awareness from ensuring network security, data security, and personal privacy protection to supply security and resilience. The changes brought new challenges to the supply chain.

[11] *https://www.federalregister.gov/documents/2021/01/19/2021-01234/securing-the-information-and-communications-technology-and-services-supply-chain*

[12] *GSMA NESAS: https://www.gsma.com/security/network-equipment-security-assurance-scheme/*

Supply Chain Security Assurance System

For ZTE, the establishment of a secure and reliable supply chain is not only the internal demand for ensuring the timely delivery of the company's products, but also our commitment to customers. ZTE has obtained several certifications: ISO 28000 certification (Supply Chain Security Management System), ISO 27001 certification (Information Security Management System), and ISO 22301 certification (Business Continuity Management System). In 2020, ZTE once again passed the Authorized Economic Operator (AEO) certification to have convenient and fast access to customs clearance procedures in relevant countries and regions worldwide.

ZTE has a complete supply chain process framework, including five business modules: planning, procurement, manufacturing, delivery, and reverse logistics, focusing on customers' business needs and security requirements, and expanding the scope of the supply chain from suppliers' suppliers to customers' customers.

This section introduces the security governance practices of the supply chain from three aspects: supply security (including third-party components), production security, and delivery security.

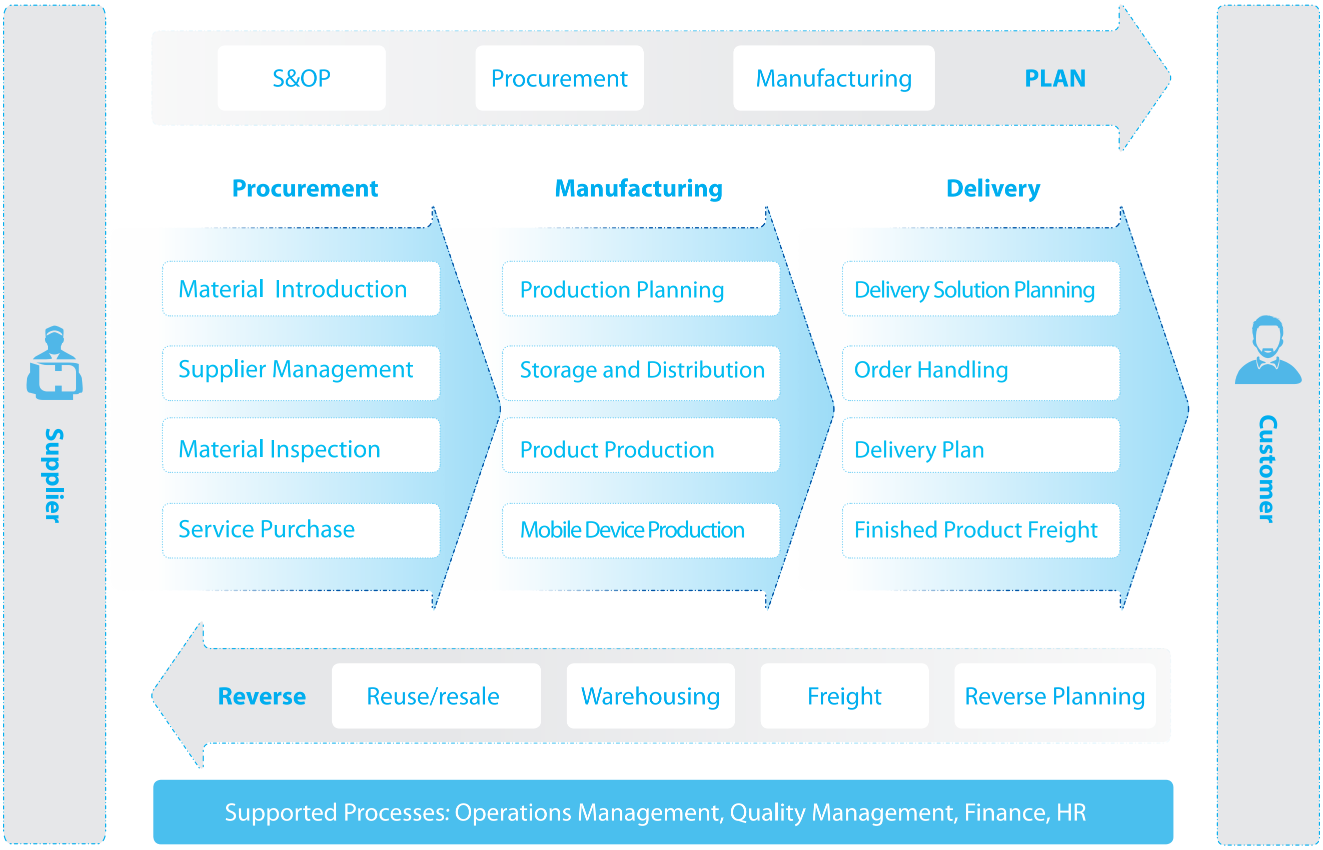


Figure 3 Supply Chain Business Process Framework

Supply Security

Partners are an important part of the supply chain. ZTE has thousands of suppliers worldwide to provide tens of thousands of raw materials, semi-finished products, finished products or services, which are key to providing our customers with products and comprehensive solutions. Therefore, ZTE regards supplier and material security management as core to its business to ensure the security of materials and third-party components.

First of all, choosing secure and reliable suppliers is the first step in ensuring the security of the supply chain. ZTE always attaches great importance to the development and landscape of supplier resources, and has established a complete set of supplier lifecycle management mechanism from sourcing, qualification, to obsolescence, including quality management, information security management, corporate social responsibility (CSR) management, performance appraisal and problem tracing. A potential supplier can only become a qualified supplier of ZTE after passing a series of assessments in terms of business, technology, quality, finance, delivery, safety, compliance, CSR, etc.

ZTE implements incoming materials by category. According to the characteristics of different categories, we classify materials into three risk levels. For high-risk materials, security inspection reports are required during the material introduction process. In addition, ZTE has established a material testing laboratory to carry out spot checks and implement closed-loop management for discovered security issues. For materials with medium- and low-risk levels, suppliers are required to sign Supplier Security Agreements with ZTE to carry out self-management accordingly, and ZTE carries out various forms of security audits.

ZTE requires suppliers to comply with local laws and regulations when providing products and services, abide by the Supplier Security Agreement signed with ZTE, and promptly release vulnerability warnings and solutions. For example, suppose security vulnerabilities are found during our product security testing or product use, relevant suppliers should actively cooperate with ZTE to track and locate vulnerabilities, and promptly provide patches or adopt solutions such as upgrade, replacement, and recall.

ZTE passes on its security requirements to suppliers also through the annual Global Partner Conference and holds annual supplier training programs to publicize our requirements on cybersecurity, information security, and CSR to suppliers.

Production Security

To implement cybersecurity controls for the production and manufacturing process, ZTE has formulated the *Manufacturing Security Management Regulations*, which divides the manufacturing area into three by security control level to control security risks in the manufacturing process and prevent software and hardware from introducing vulnerabilities, including unauthorized hardware replacement, software installation or tampering, and virus infection. Among the three-level security control areas, the level-1 and level-2 areas are strictly controlled, where special security administrators are assigned for implementing security control measures and daily security supervision.

To prevent virus invasion or software tampering, ZTE has built a dedicated production network, which is isolated from office Intranet and Internet to ensure the security of the production environment. Similarly, to prevent tampering with the software in products during the manufacturing process, ZTE engineers can release or archive the software only through the product data management system via authorized access.

Finished Products Delivery Security

ZTE uses its warehousing management system to track the products through the entire process. ZTE promptly upgrades the warehousing IT system, monitoring devices and security facilities to avoid the risk of damage, replacement, or malicious code installation on finished products or core components during warehousing and shipment. ZTE monitors the shipment tracks in real time through a freight tracking system which also supports a stakeholder early warning function.

Building a Resilient Supply Chain

In the face of the risks and challenges arising in product delivery due to the increasingly high requirements of customers and the drastic fluctuations of market demand and supply, ZTE supply chain focuses on the risks that may occur in its three core business scenarios, namely material supply, manufacturing, and logistics. ZTE takes the following measures to ensure the continuous and stable operation of the supply chain business in accordance with the requirements of ISO 22301.

Material supply

ZTE has a diverse global supply chain, including suppliers in North America and Europe, and can maintain adequate supplies. At the same time, we actively perceive customer needs through in-depth insights into industry trends and forward-looking analysis of the supply and demand of the market, and adjust procurement strategies in a timely manner to ensure sufficient inventory and resource supply, and maintain the resilience of the supply chain. Meanwhile, ZTE has developed a visual risk map tool that can quickly identify the affected vendors, material codes, products and the degree of impact when an emergency occurs, which helps ZTE complete a comprehensive risk assessment. For example, shortly after the launch of the tool, a 6.7 magnitude earthquake occurred in Hokkaido, Japan in September 2018. We quickly identified 32 suppliers and 65 material codes affected within 2 hours through the supply risk map and promptly initiated response measures to avoid impact. This tool played an important role in risk identification and response.

Manufacturing

ZTE currently has five major production bases in mainland China, namely Shenzhen, Heyuan, Changsha, Nanjing, and Xi'an. Production resources between the bases can be shared, and production capacity can be backed up to each other. The flexible production capacity strategy ensures the continuity of production and capacity requirements.

ZTE has established a capacity risk scanning mechanism to plan mid-to-long-term capacity in advance to meet general needs. ZTE can expand to 120% of standard production capacity within two weeks through temporary measures to meet short-term demands. And for circuit boards, power supply products, and terminal products, ZTE always reserves 20% outsourcing capacity to meet customer delivery requirements.

Logistics

ZTE ensures the security of freight through its diversified logistics network. On the one hand, ZTE strengthens direct cooperation with shipping companies, airlines and other resource-based suppliers to ensure the stable availability of freight resources; on the other hand, ZTE actively plans backup freight routes, including mutual railway transportation, sea transportation and air transportation routes, multiple backup departure locations, and multiple backup routes for the same mode of transportation. For example, on March 21, 2021, when the Ever Given, a large container ship, ran aground and blocked the Suez Canal, ZTE activated a backup plan and coordinated China-Europe rail containers to meet the urgent needs of European shipments.

Securely Managed Product Development Process

ZTE puts security as the highest priority for research and development. Security is regarded as a basic attribute that must be integrated into the entire life cycle of product development, by abiding by the principles of security by design and security by default.

To meet the requirements of different customers and market conditions, we continue to identify cybersecurity threats and keep pace with industry best practices, such as Building Security In Maturity Model (BSIMM), GSMA NESAS, and Capability Maturity Model Integration (CMMI). And by formulating ZTE's R&D security maturity model for process and project evaluations, we make continuous improvements. In 2020, ZTE's 5G product lifecycle process was evaluated against the BSIMM model, attaining the international leading level, and the 5G product lines also passed the NESAS development and lifecycle audit (which evaluated the implementation of security by design processes by our key product lines) and the associated network equipment evaluation against 3GPP SeCurity Assurance Specifications (SCAS).

Process and Organization

A security-embedded R&D process is essential to deliver high-quality and secure products. Back in 2001, the Security Development Lifecycle (SDL) created by Microsoft reduced the number of vulnerabilities in software by more than 50%[13], greatly improved security and efficiency, and became the blueprint for software development by many companies around the world, for their own software customizing and developing. At ZTE, the High Performance Product Development (HPPD) is a process commonly followed in the R&D field. After years of development, it has integrated industry best practices and incorporated security control measures at various stages. Based on this process, ZTE continues to improve security technologies and R&D security maturity, and improve the capabilities of security personnel.

[13] *The Security Development Lifecycle by Michael Howard and Steve Lipner*

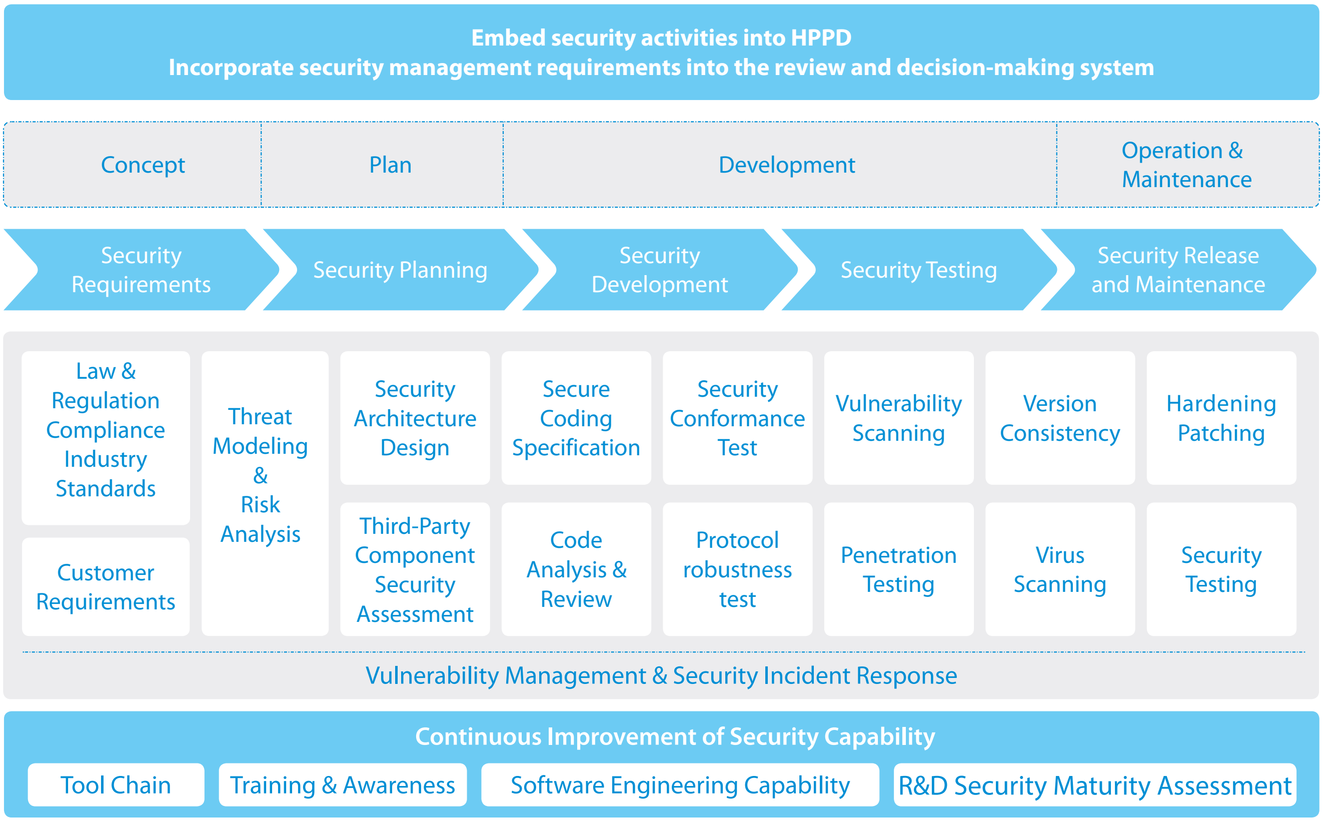

Embed security activities into HPPD
Incorporate security management requirements into the review and decision-making system
Concept
Plan
Development
Operation & Maintenance
Security Requirements
Security Planning
Security Development
Security Testing
Security Release and Maintenance
Law & Regulation Compliance Industry Standards
Customer Requirements
Threat Modeling & Risk Analysis
Security Architecture Design
Third-Party Component Security Assessment
Secure Coding Specification
Code Analysis & Review
Security Conformance Test
Protocol robustness test
Vulnerability Scanning
Penetration Testing
Version Consistency
Virus Scanning
Hardening Patching
Security Testing
Vulnerability Management & Security Incident Response
Continuous Improvement of Security Capability
Tool Chain
Training & Awareness
Software Engineering Capability
R&D Security Maturity Assessment

Figure 4 Security Activities Embedded into HPPD Process

Requirements and Design

Security requirements come from different national and regional regulators, customers, and industry trends. ZTE incorporates mid- and long-term security requirements into product roadmap planning, and short-term security requirements into product version planning.

We address security requirements through threat modeling. Threat modeling is a core step in security design, which is a structured method of analyzing and solving problems, used to identify and quantify threats, and prioritize countermeasures to mitigate risks. The aim is to identify risks at an early stage of the product development process. With reference to industry best practices such as ITU-T X.805, Microsoft STRIDE, DREAD, Synopsys Architecture Risk Analysis (ARA) and other models, we have established a set of system threat modeling methods suitable for products, to find threats, identify risks, and output countermeasures.

The company releases security design technical standards and technology stack catalogs, introduces threat modeling tools, establishes a security design knowledge base, and guides product teams to analyze security requirements and design security architecture and features.

Regarding privacy protection and data compliance issues which are a major concern for the society, ZTE follows the concept of privacy by design, moves security controls sooner, and incorporates data protection requirements at the requirements stage, to detect data protection compliance risks as early as possible and effectively reduce impact.

Development and Testing

In the development and testing phase, we follow the industry's common secure coding standards, such as CERT (Computer Emergency Response Team) coding standards, OWASP (Open Web Application Security Project) development guides, CWE (Common Weakness Enumeration), and STIG (Security Technical Implementation Guide), to formulate and continuously optimize ZTE's secure coding specifications and conduct research and replacement of insecure functions. The code we write needs to go through static inspection and automated scanning to check the quality, reliability, security, and maintainability.

The defects identified by the scanning tools are managed by Kanban (a form of visual framework) and tracked in a closed loop. Each version's security defects are controlled to the target through control gates.

Testing activities include code scanning, vulnerability scanning, protocol robustness testing, penetration testing, and virus scanning, to verify the fulfillment of security requirements including personal data protection requirements. All defects should be remedied at this stage.

Release and Maintenance

ZTE has formulated a set of strict release processes. Products need to pass security tests to comply with ZTE's product security red line requirements, and should be equipped with a security hardening manual and tool.

The R&D team formulates continuous regression testing strategies and performs tests on the products in deployment and in use on the live network to prevent new vulnerabilities, and provides security patches or deploys security hardening solutions to ensure that the security risks of live network products are eliminated or under control.

Managing Third-party Components

ZTE implements the full lifecycle management of open-source third-party components used in the product from introduction to the end of life, and embeds the controls to the HPPD process that is supported by the DevOps toolchain.

At the third-party components introduction stage, ZTE fully analyzes and verifies component functions and performance to meet export control, data protection and open-source licensing, and the company's product security red line requirements, etc. At the same time, we consider the components' replaceability and the lifecycle promised by the supplier to ensure that they match our product lifecycle in order to achieve the service commitment to customers. Only third-party components that have passed the security assessment and have been certified can enter the company's component management system. Developers can obtain the access rights to the components after approval, and select components needed for the required products.

The third-party components selected for the product must pass the security tests and can be released with the product only after meeting the security requirements. In the life cycle of our products, once a security vulnerability is found by a customer, supplier, third party or ZTE, we will evaluate the vulnerability, provide solutions or mitigation measures, and eliminate the risk promptly.

During the product life cycle, when the version of the third-party software is updated or patches are introduced due to function, performance or security needs, or when the third-party software lifecycle ends, we update or abandon the third-party software through the component management system to ensure that the third-party software used in our product is up-to-date.

The security risk assessment of third-party software runs through the whole process from component selection, introduction, testing, delivery to maintenance, and is included in the node management and control of HPPD process to ensure that security risks are found in time, so that we provide appropriate security solutions or mitigation measures.

Also, we regard the third-party software as a product configuration item and include it into the configuration management process to trace its use. If vulnerabilities are found later, we can track the scope of its use and solve all problems related to the third-party software.

As an active contributor to the open source community, ZTE continues to track vulnerabilities released by the community and contribute to providing vulnerability repair solutions.

Secure Development Assurance

The continuous and secure delivery of products is guaranteed by a solid configuration management system, a DevOps toolchain integrated development process, and the development of internal information security management and control strategies.

ZTE's configuration management system ensures that customers' original requirements are traced along all stages of the process, covering design, development, testing, delivery, and relevant key elements including people, tools, components, R&D and production environment that are involved in the software.

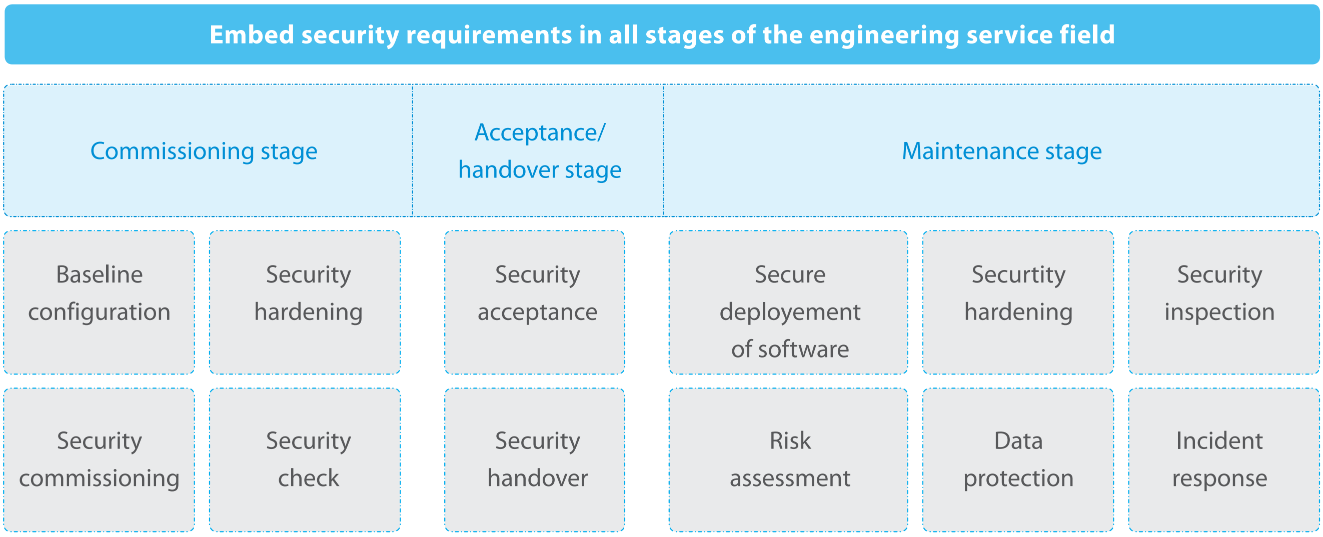
Security tools are integrated into the entire DevOps toolchain, which iteratively connects four activities: continuous planning, collaborative development, continuous testing, release and deployment. Tools can be effectively used for security testing such as code scanning, vulnerability scanning, and penetration testing, to form a closed loop of operation and maintenance monitoring.

ZTE has carried out information security risk identification and implemented control measures on procedural deliverables such as code and technical documents. The code is compiled, undergoes unit and functional testing, and is reviewed in the R&D cloud to form a delivery version. There are strict control strategies for the circulation of code and documents into or out of the R&D cloud, so the software is securely controlled during the development process.

Delivering Secure Networks and Services

As products are delivered to the customer, new security risks emerge in the business scenarios that also change. ZTE takes appropriate protection measures to ensure the integrity, confidentiality, and availability of products and data during the delivery process, thus achieving end-to-end security.

ZTE has established a risk-based delivery security governance system across global sites, covering authorization management, secure deployment, remote access management, network data protection, asset security management, incident response, and third-party partner management. Cybersecurity requirements have been fully integrated into the commissioning, acceptance/handover, and O&M phases to ensure secure and reliable delivery behaviors, secure operation of network devices, and effective protection of customers' networks and data. In addition, ZTE regularly conducts drills and spot checks to ensure the security awareness and standard operations of engineering personnel are in place.



Embed security requirements in all stages of the engineering service field

Commissioning stage		Acceptance/ handover stage	Maintenance stage		
Baseline configuration	Security hardening	Security acceptance	Secure deployement of software	Securtity hardening	Security inspection
Security commissioning	Security check	Security handover	Risk assessment	Data protection	Incident response

Figure 5 End-to-End Guarantee of Delivery Security

Authorization Management

Before operating customers' network and data (such as software upgrade, security hardening, and network preventive maintenance), ZTE technical personnel obtain customer authorization first and perform operations within the agreed scope and time period. All of operations are recorded, and the individuals who perform operations can be traced and identified through logs.

Secure Deployment

To ensure the end-to-end secure deployment of software, ZTE implements strict processes in accordance with its management regulations. Only authorized personnel can download product software from the support website, and all download operations are logged. In addition, all downloaded software shall undergo integrity and virus checks before upgrade. The tools and software required for deployment are obtained from the specified official websites, ensuring security, reliability, and intellectual property compliance.

Remote access Management

To ensure secure and efficient remote technical support, ZTE allows its product experts to troubleshoot faults or provide service support through the internal Advanced Operations Suite (AOS) platform[14] and demilitarized zones to access customer networks after customer authorization, while still following the local laws and regulations. All remote operations can be audited afterwards to ensure no violation of customer authorization.

[14] *Advanced Operations Suite (AOS): primary portal and entry deployed by ZTE to assist product experts in providing remote support*

Network Data Protection

To protect the security of network data, ZTE requires that basic security protection measures be available on terminals connecting to customers' networks, for example, installing critical system patches and anti-virus software, and only authorized work-related software without any information security risks are allowed. With customer's authorization, measures such as data desensitization and encryption shall be adopted to protect the data temporarily stored on terminal devices according to data sensitivity, and such data can only be transferred under the "Least-to-Know" and "Need-to-Know" principles and in accordance with local laws and regulations.

Asset Security Management

To ensure that the protection of customers' network equipment is not degraded due to changing internal and external threats, ZTE regularly carries out security checks, security hardening, and risk assessments under contract requirements, to practically fulfill its obligations regarding the risk identification and control on customers' network assets.

Incident Response

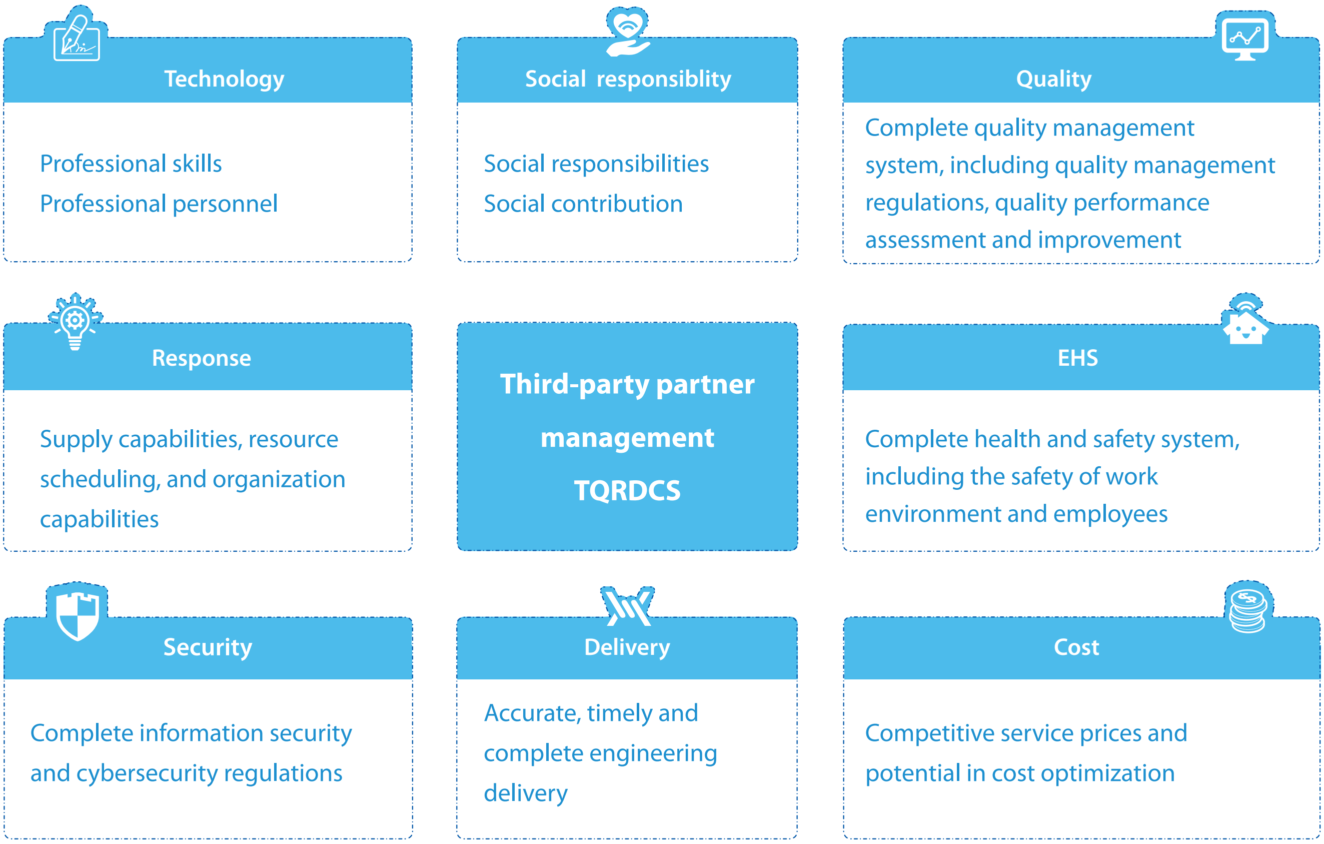
If a security incident occurs, ZTE on-site engineers will immediately report it to the ZTE Global Customer Support Center (GCSC) system, and mark it as "Product Security". The problem is then notified to the Product Security Incident Response Team (PSIRT). Depending on the severity, the problem is transferred to the corresponding product teams and resolved within the time period specified in the SLA. Moreover, ZTE regularly performs emergency drills regarding major disasters, cyber attacks, and other unexpected incidents, so as to continuously improve the capability of incident response and handling.

Third-Party Partner Management

Third-party partners are an important workforce in the delivery field. However, ZTE has extended its security protection boundaries while collaborating with third-party partners, and new security risks may be introduced. Therefore, a sophisticated mechanism is needed for security management on these third-party partners to ensure security and reliability. ZTE has set up a third-party partner certification management scheme, covering certification assessment, qualification management, security management, performance management, and credit management, which are used in the whole life cycle including selection, cooperation, and exit stages of third-party partners. Also, ZTE achieves end-to-end visual management for its third-party partners by using the supplier relationship management system, financial system, and engineering project management system.

ZTE has formulated and enforced a security baseline for the certification and procurement of third-party partners, specifying the minimum security standards of products and services that must be met. Potential third-party partners can be selected only after passing the assessment involving cybersecurity and other factors. All certified third-party partners shall sign the Product Security Commitment specifying product security requirements and liabilities as a result of the breach of contracts.

ZTE regularly conducts a comprehensive risk assessment on both the service performance and security level of its third-party partners, performs level-based management, and then determines future cooperation opportunities and frequencies in accordance with assessment results.



Technology

Professional skills
Professional personnel

Social responsiblity

Social responsibilities
Social contribution

Quality

Complete quality management system, including quality management regulations, quality performance assessment and improvement

Response

Supply capabilities, resource scheduling, and organization capabilities

Third-party partner management TQRDCS

EHS

Complete health and safety system, including the safety of work environment and employees

Security

Complete information security and cybersecurity regulations

Delivery

Accurate, timely and complete engineering delivery

Cost

Competitive service prices and potential in cost optimization

Figure 6 Third-Party Partner Management System of ZTE Delivery Field

Security Incident Management

As threats and vulnerabilities change, the security risks of the network cannot be completely eliminated. When a security risk turns into a security incident, it needs to be mitigated in a timely manner to reduce the adverse impact. At the same time, handling vulnerabilities can largely avoid the occurrence of security incidents. Therefore, any information regarding identified product vulnerabilities should be disclosed to customers in a timely manner, and a vulnerability handling plan should be provided.

In addition, security incident response and vulnerability handling mechanisms rely on the cooperation of stakeholders in order to coordinate and share information efficiently, respond in a timely manner, and effectively mitigate security risks.

Security Incident Response Mechanism

ZTE's incident response mechanism covers supply chain, R&D and engineering service fields. The PSIRT is responsible for receiving, processing and disclosing security vulnerabilities on ZTE products and solutions. The PSIRT collaborates effectively with customers and stakeholders to quickly provide solutions. A hierarchical response mechanism for security incidents and data breaches is established to ensure unified collaboration, rapid repair, and rapid business recovery.

For security incident handling, ZTE adopts a closed-loop process including prevention, detection, correction and recovery, and post-incident feedback. Once a security incident occurs, the PSIRT quickly analyzes the incident and takes necessary measures to control the impact of the incident until the service is recovered. After the incident is effectively controlled, review and improvement will be carried out to prevent the recurrence of similar incidents Figure 7 below shows ZTE's major security incident response mechanism.

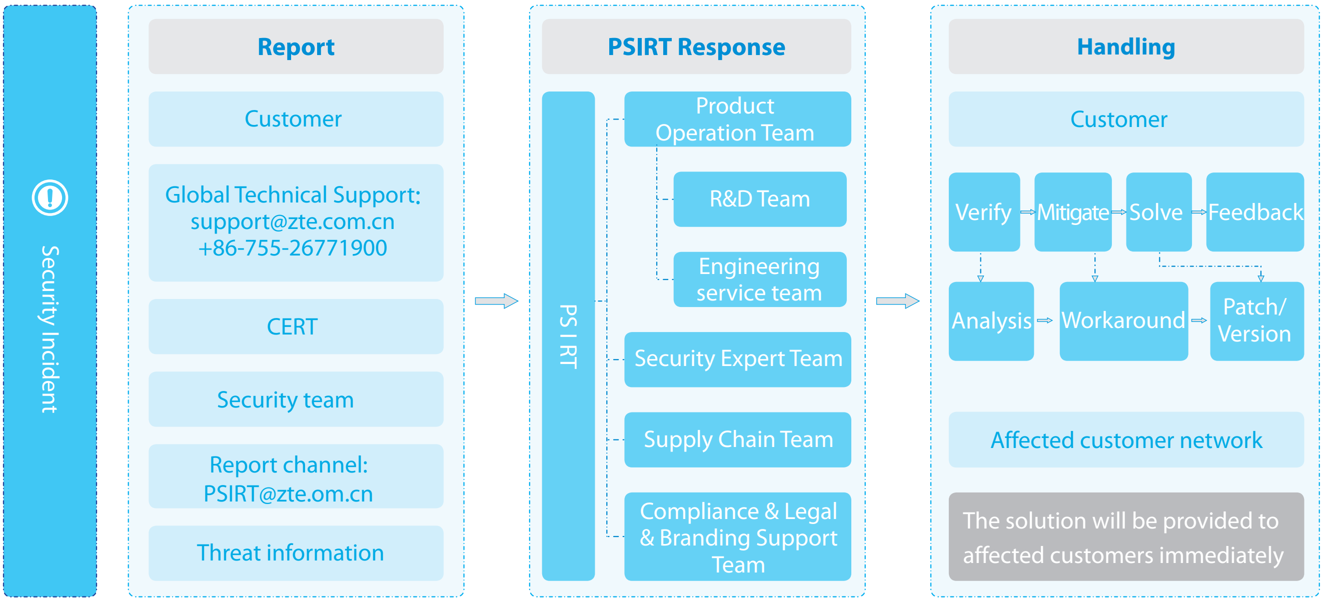


Figure 7 Major Security Incident Response Mechanism

Security Vulnerability Handling Mechanism

Adhering to the principle of openness and transparency, ZTE actively cooperates with security organizations and makes responsible disclosures of vulnerabilities discovered internally and externally by customers and related parties. For confirmed vulnerabilities, ZTE provides mitigation measures and solutions, and monitors the result after the customer implements the solutions, so as to iterate solutions in a closed-loop manner.

ZTE is a member of the Forum of Incident Response and Security Teams (FIRST) and is one of the CVE Numbering Authorities (CNA), and actively participates in GSMA Coordinated Vulnerability Disclosure (CVD) program.

In 2020, ZTE has released its new bug bounty programs covering multiple product categories such as 5G core network, 5G base station, fixed network, multimedia, cloud video, cloud computing, distributed database, terminal products and web application systems, and cooperates with well-known third-party bug bounty platforms to encourage global security researchers and organizations to report security vulnerabilities in ZTE products and services Figure 8 below illustrates ZTE's security vulnerability handling process.

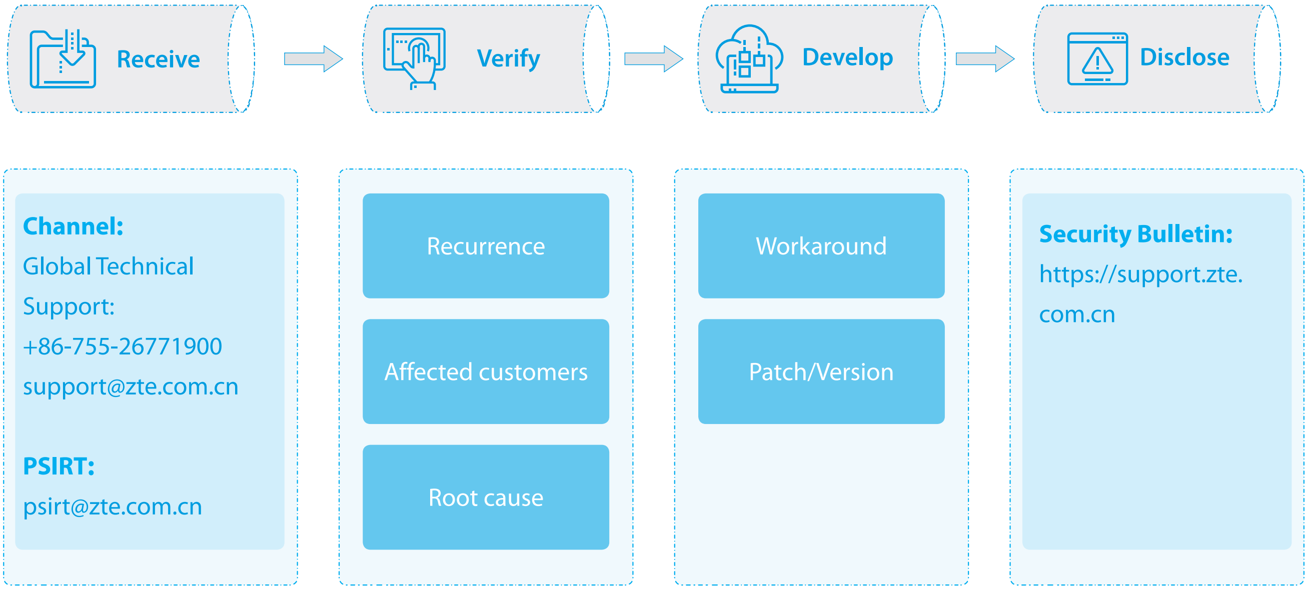


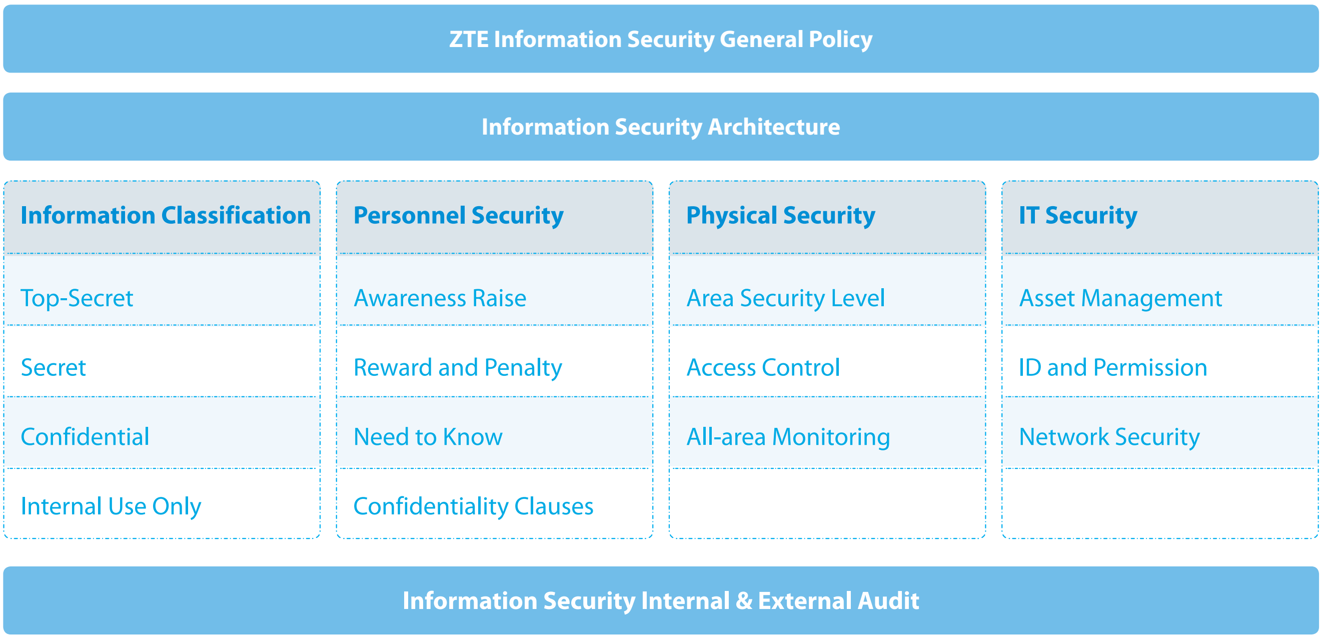
Figure 8 Security Vulnerability Handling Process

Information Security

Information security is used to protect the security of the company's assets so that product R&D, production, and operation can be carried out in a secure environment. By establishing a comprehensive information security management system, control measures can be defined in terms of organization, personnel, procedure, and technology to ensure the confidentiality, integrity, and availability of data and assets and safeguard the business development of the company.

ZTE has established an Information Security Management System (ISMS) where the management processes including Information Security General Policy, Information Classification, Risk Assessment, and Security Audit are defined, with information security red lines embedded as control points. The information security organization shall use red lines to supervise, investigate, and tackle any violations of the company's information security, and infringements on the company's business secrets. Each year, all employees will receive security training and be tested to enhance their security awareness. When identifying information security breaches and other issues, such as risks and vulnerabilities, employees can immediately report them to the information security organization via e-mail, phone, and the company's official website to mitigate security risks, fix the vulnerabilities, and optimize the security rules in a timely manner.

ZTE has adopted a series of initiatives with respect to information classification, personnel security, physical security, and IT security to ensure security of the company's information assets, and ensure the confidentiality, integrity, and availability of information assets, while improving the information security as a core competency of the company.



ZTE Information Security General Policy

Information Security Architecture

Information Classification	Personnel Security	Physical Security	IT Security
Top-Secret	Awareness Raise	Area Security Level	Asset Management
Secret	Reward and Penalty	Access Control	ID and Permission
Confidential	Need to Know	All-area Monitoring	Network Security
Internal Use Only	Confidentiality Clauses		

Information Security Internal & External Audit

Figure 9 Information Security Framework Overview

Privacy Protection

The continuous development and application of information and communication technologies such as big data, artificial intelligence, cloud computing, the Internet of Things, and 5G have promoted our society to rapidly enter into the digitally connected world. The large-scale use of data brings convenience and efficiency, as well as challenges for data compliance and privacy protection (hereinafter referred to as "privacy protection"), which may affect personal rights, organizational business interests, public safety and even national security. To this end, major countries and regions around the world have successively introduced privacy protection-related laws and regulations, such as the EU's General Data Protection Regulation (GDPR), the US's California Consumer Privacy Act, China's Cyber Security Law, the Data Security Law, and the Personal Information Protection Law.

ZTE attaches great importance to privacy protection and regards it as one of the major basic areas of the company's compliance strategy. ZTE believes that privacy protection is not only a strict compliance with legal requirements, but also an important cornerstone for building mutual trust in the industry and practicing ethical values.

Privacy Protection System Implementation

ZTE is committed to establishing an applicable, effective, and leading privacy protection system, and is risk-oriented, carrying out comprehensive system Implementation from the dimensions of organization, personnel, system, and technology.

ZTE has established a privacy protection control mechanism including a compliance audit team, a data protection compliance team, and business units for risk prevention and control.

ZTE has carried out various forms of privacy protection training, actively conveying value orientation, effectively enhancing the privacy protection awareness and capabilities of all employees, and creating a good privacy protection culture across the company.

ZTE focuses on the laws, regulations and regulatory requirements of major global jurisdictions, comprehensively considering the requirements of other typical countries and regions, and analyzes the organization environment based on business distribution, and determines the company's unified privacy protection strategy and management system to ensure that the privacy protection management and control requirements can be "Established once, applicable globally". In addition, ZTE has also established targeted business processes and compliance guidelines based on the characteristics of its business areas to provide better support for the effective implementation of management and control requirements in the business.

To effectively implement management requirements, ZTE is also actively exploring privacy protection technologies. By introducing industry best practices and research and development of management tools, we continue to improve the overall level of privacy protection. At present, ZTE has obtained dozens of privacy protection patents. For the computing technology for privacy protection, ZTE is also actively engaged in technological innovation.

Privacy Protection Control in Key Scenarios

ZTE has established a comprehensive management and control mechanism for various high-risk scenarios to protect the data and privacy of users, customers, and employees.

ZTE has established a mechanism, which manages and controls relevant incidents through the "personal data leakage response system", and tracks and records the incident response process.

The data subject rights response mechanism uses ZTE's data protection public mail and data subject rights response system, which facilitates the data subject to submit rights claims quickly and at the same time ensures the security of personal data during the exercise of rights, thereby enhancing social trust.

The cross-border data transfer management and control mechanism adheres to the authorization consent and the principle of data minimization. Data protection impact assessment is required in advance. Cross-border transfer activities that are indeed necessary must meet the requirements for the performance of the contract or obtain formal authorization. Only after approval, the data can be transferred in accordance with the cross-border control requirements.

ZTE also extends privacy protection requirements to suppliers, fully evaluates their privacy protection capabilities during supplier certification or procurement, manages risks from the beginning of cooperation, and builds open, secure and trustworthy privacy protection ecosystem with global suppliers and partners.

Privacy Protection Practices

ZTE actively carries out innovations in privacy protection practices, and explores secure and compliant solutions for products and services.

In external business activities, when interacting with customers, ZTE may process customer’s personal data as a data controller. When ZTE acts as simply a product provider, it usually does not participate in data processing activities, and it mainly provides the privacy protection capabilities of its products. When ZTE is a service provider, it usually processes data in accordance with customer requirements, and it mainly acts as the data processor. In some specific operating scenarios such as customer support center for end users and ZTE sales websites and apps, ZTE will also act as the data controller. Therefore, it is necessary to comply with the relevant obligations of the controller or processor when providing services.

ZTE follows the concept of Privacy by Design, focuses on user rights protection and data security, moves privacy protection management and control to the design stage of product and service solutions, and introduces privacy protection requirements into product and service requirements, integratingdata protection into products and services by default, ensuring that data processing meets the principles of legality, fairness, and transparency, to realize the control of product and service privacy protection.

ZTE is committed to providing reliable, end-to-end full life-cycle cybersecurity and privacy protection. In 2020, ZTE benchmarked ISO/IEC 27701:2019, introduced and established a privacy information management system (PIMS) in key products, and continued to improve the system in accordance with the business, and obtained the industry’s first ISO/IEC 27701:2019 privacy Information management system certification for its 5G products. At present, ZTE has successively obtained multiple certificates in the fields for 5G RAN, core network, terminal products, office suite products, and ZTE's HR system.

As a "road builder" in the digital economy, ZTE will fit the characteristics of the communications industry, match internal risk appetite and external regulatory environment, and is committed to establishing an applicable, effective and leading privacy protection system. ZTE will also strive to become the leader and benchmark of Chinese companies in the field of privacy protection and become the forerunner and model for global companies.

Security Maturity Verification

ZTE believes that security maturity is verifiable. First of all, there are many internationally recognized security certification systems in ICT industries, such as ISO27000 series and Common Criteria (CC). In the more complex telecommunications industry, the International Organization for Standardization has specified security requirements in technical specifications. With the development of telecommunications networks, Standards Development Organizations (SDOs) such as 3GPP, ITU, ETSI, are constantly updating technical standards and expanding security specifications. Secondly, national governments and various stakeholders have gradually realized the importance of 5G network security and strengthened assessment and certification of security. The European Union is committed to developing unified communication network security certification schemes, and the requirement to develop these schemes has been written into the EU Cyber Security Act. The EU 5G Toolbox further requires member states to adopt EU unified certification for 5G network components and supplier processes[15]. At the same time, GSMA, on behalf of hundreds of operators and manufacturers around the world, has developed GSMA NESAS, a security assessment and assurance scheme, to audit the network equipment development and lifecycle processes, and work with 3GPP to enrich NESAS's network equipment security evaluation. The European Union and many countries have adopted NESAS and the relevant parts of the Common Criteria as the blueprint for unified security certification and assessment.

These common technical standards, certification frameworks, and evaluation schemes can enable our products to be verified in all aspects and let customers

[15] *EU 5G Toolbox (TM09): https://digital-strategy.ec.europa.eu/en/library/cybersecurity-5g-networks-eu-toolbox-risk-mitigating-measures*

understand our products' security in terms of development process and technology. Different manufacturers following the recognized norms can improve the security level of the entire industry.

ZTE has been committed to industry standard benchmarking and security verification. We cooperate with external security certification and assessment bodies, to verify whether our security assurance practices are effective by going deep into technology, products, and the entire development life cycle process. From 2020 to 2021, under the rigorous testing of the industry's top security companies, ZTE's 5G product lines passed GSMA's NESAS audit for development and product life-cycle processes, and 8 of ZTE 5G products passed the 3GPP SCAS test cases. Our 5G RAN solution has obtained the CC EAL3+ level certificate, which is the first level-3 certificate obtained in the industry for a whole system solution (including 15 products of 5G RAN) as the protection profile. In the practice of benchmarking against the BSIMM model, we invited Synopsys to conduct a BSIMM evaluation on the 5G core network and access network product line, and the results proved that our software security reached the industry-leading level. At the same time, we hold a series of ISO certifications, covering information security, supply chain security, business continuity, privacy protection, etc.

In order to allow customers, regulators, and stakeholders to verify ZTE products easily, effectively and transparently, we have established three laboratories in Nanjing, China, Rome, Italy, and Brussels, Belgium. The Nanjing Laboratory is ZTE's largest and most complete cybersecurity laboratory. It provides industry-leading integrated network environment and evaluation infrastructure, and supports multiple security evaluation functions, including source code review, document review, and penetration testing. At the same time, it promotes capacity building and conducts in-depth research and exploration in the security field. In Europe, taking the Italian laboratory as an example, our customers have used the laboratory featuring rich equipment environment to conduct penetration testing and source code review of multiple products, including 5G, home and mobile terminal products, of which some have been performed under the supervision of the National Inter-University Consortium for Telecommunications (CNIT). In the future, ZTE will build more cybersecurity laboratories as needed, open our code, and welcome more external cooperation, supervision and verification.

By actively seeking flexible and diverse external cooperation and verification, ZTE continues to improve security. With the gradual popularization and development of 5G networks, this open and transparent initiative will continue. We believe this is the best way for all industry players to gain trust.

Jointly Enhancing Cybersecurity through Openness and Transparency

Standardization is the foundation for mobile network security, achieving interoperability and openness. It is especially true for 5G networks. From open and transparent 5G standard formulation and compliance, unified 5G network security verification, to cross-regional and cross-industry coordinated vulnerability disclosure and rectification, contributions are made by participants from all over the world. Together with network operators and manufacturers, SDOs are designing 5G security into standards. Therefore, openness and transparency is essential to ensure 5G security. Only following the open standards and consistent assurance requirements, can we obtain sufficient security in the entire network.

Over the years, ZTE has leveraged its technological advantages in telecommunications networks, actively participating in the formulation of domestic and international standards, and is deeply involved in international mainstream standard organizations. Currently, ZTE holds the positions of Chair of the 3GPP RAN3 Working Group and Vice Chair of the RAN2 Working Group. In the 3GPP's leading working group on security standards, 3GPP SA3, ZTE leads the Security Assurance Specification for 5G Inter PLMN User Plane Security (SCAS_5G_IPUPS) and Network Exposure Function (SCAS_NEF) activities. As the most important security standard for network equipment, 3GPP SCAS specification have been continuously expanded and updated. With the development of 5G and later networks, it will continue to develop more security specifications.

In ITU-T, ZTE holds the positions of SG17 (Security) Vice Chair and SG17 WG5 Chair. It also plays an important role in ETSI, GTI, GSMA and other international organizations, making contributions to cybersecurity standards.

Look Forward and Advance Together

Through years of practice and technological innovation, ZTE continues to accumulate experience in providing solutions in 5G technology, secure network operations, and industrial applications. Utilizing its own R&D advantages, ZTE is committed to the United Nations Global Compact, a voluntary initiative that encourages companies to adopt more sustainable business practices and models to empower the digital transformation of the industry with new technologies and achieve sustainable development. By June 2021, ZTE has filed over 80,000 patent applications, with 40,000 granted. In 2020, ZTE ranks top 3 in 5G declared standards-essential patents (SEPs) to ETSI.

In the 5G era, only under the premise of ensuring security, can the digital transformation of technology-based industries be better realized, and sustainable development is not empty talk. ZTE will keep investing more resources into research of the security technologies and methods, continuous innovation, and introduce and learn advanced cybersecurity management concepts and methods to enhance product security and service capabilities to meet new security requirements brought by new technologies, new applications, and new business models. In the case of the changing business environment, we must be well prepared, benchmarking industry standards and best practices, taking into account the security of every aspect of the business, not only our own security measures, but also include our upstream supply chain. Insisting on the concept of transparency, openness, trust, and cooperation, ZTE works with customers, partners, governments, vendors, standards organizations more closely to deal with cybersecurity challenges in the future, in order to build a reliable and resilient supply chain, and continuously provide secure and trustworthy products and services for customers.

Appendix A: Acronyms and Abbreviations

Abbreviations or symbols	Full name
3GPP	3rd Generation Partnership Project
5G	Fifth generation mobile communication
AEO	Authorized Economic Operator
AOS	Advanced Operations Suite
CC	Common Criteria
CERT	Computer Emergency Response Team
CNA	CVE Numbering Authority
CSA	Cloud Security Alliance
CSC	Cyber Security Committee
CSR	Corporate Social Responsibility
CVD	Coordinated Vulnerability Disclosure
CVE	Common Vulnerabilities and Exposures
CWE	Common Weakness Enumeration
EAL	Evaluation Assurance Level
ENISA	European Union Agency for Cybersecurity
ETSI	European Telecommunications Standards Institute
FIRST	Forum of Incident Response and Security Teams
GDPR	General Data Protection Regulation
HPPD	High Performance Product Development
IETF	Internet Engineering Task Force
ISO	International Organization for Standardization
ITU	International Telecommunication Union
NESAS	Network Equipment Security Assurance Scheme
OWASP	Open Web Application Security Project
PDM	Product Data Management
PbD	Privacy by Design
PSIRT	Product Security Incident Response Team
S&OP	Sales & Operations Planning
SCAS	Security Assurance Specifications
SEP	Standard Essential Patent
SDO	Standards Development Organization
SSG	Software Security Group
STIG	Security Technical Implementation Guide
WSIS	World Summit on the Information Society

Appendix B:
Major Cybersecurity Events of ZTE

2005 ZTE passed the ISO 27001 certification (Information Security Management System). In 2021, ZTE and its 23 global subsidiaries have passed this certification, which covered all the business of ZTE.

2005 ZTE took on the position of Vice Chair of ITU-T SG17 . ZTE had long been active in international standards organizations such as 3GPP, IETF, ITU-T, and CSA, and security forums, playing a role in promoting the standardization work in the security field.

2011 ZTE Netnumen U31 passed the Common Criteria for Information Technology Security Assessment (CC) EAL2 certification.

2013 ZTE established the cybersecurity lab and Product Security Incident Response Team (PSIRT).

2015 ZTE became a member of Forum of Incident Response and Security Teams (FIRST).

2017 ZTE passed the ISO 28000 (Supply Chain Security Management System) certification, which covered the procurement, manufacturing, and logistics of 26 types of telecommunication products (including mobile devices).

2017 ZTE was granted the certificate of Authorized Economic Operator (AEO) issued by the World Customs Organization.

ZTE became one of the CVE Numbering Authorities (CNAs).

2017

ZTE released its product security red lines, designated Zhong Hong as the Chief Security Officer of the company.

2018

ZTE passed CC certification in 12 categories of products, including core network equipment, access network

2018 equipment, optical transmission equipment, network management equipment, routers, base station controllers and other mainstream products.

2019 ZTE opened three cybersecurity laboratories around the world.

2019 China Cybersecurity Review Technology and Certification Center (CCRC) certified that ZTE conformed to the first class requirements in providing security integration service.

2020 ZTE was certified with the ISO22301 certification.

2020-2021 ZTE passed ISO 27701 certification which covers 5G NR, network management, core network and terminal products.

2020 ZTE 5G New Radio (NR) and 5G Common Core (5GC) products passed GSMA's Network Equipment Security Assurance Scheme (NESAS) audit for their development and product life-cycle processes.

2020 ZTE received the CCRC-ISV-C01:2018 certificate, which proves that ZTE's information security risk assessment level has reached the first-level service qualification.

2020 ZTE launched new Bug Bounty Programs to encourage security researchers and organizations worldwide to identify vulnerabilities in ZTE's products and services.

2021 ZTE was awarded the Privacy Strategy Contribution Award by British Standards Institute.

2021 ZTE completed the BSIMM assessment of its full series of 5G products. ZTE achieves near industry-best high-water marks in 10 out of 12 practices, indicating that its software security capability has reached the leading level in the industry.

2021 ZTE successfully passed the Common Criteria (CC) EAL3+ certification for its 5G RAN solution. The certification makes ZTE the first telecommunications vendor in the world that has obtained the CC EAL3+ certificate for a whole system solution consisting of a series of 5G RAN products.

2021 ZTE 5G NR gNodeB and seven 5GC network devices passed NESAS security evaluations of its 5G network equipment against SCAS defined by 3GPP.

ZTE ZTE CORPORATION

NO.55, Hi-tech Road South, ShenZhen,P.R. China Postcode:518057
Website:www.zte.com.cn Tel:+86-755-26770000 Fax:+86-755-26771999