ZTE

Governance, Conformance, Openness, and Transparency

Practices of ZTE Cybersecurity Assurance

ZTE Corporation

December 2023

Acknowledgements

This white paper is jointly completed by security experts in all fields of ZTE. Thank you to each author: Cao Kunpeng, Ding Pei, He Ying, Jiang Lu, Kong Tao, Li Xing, Liang Ping, Liu Jianing, Liu Lei, Ping Li, Tang Keke, Tang Lei, Wang Dongmin, Wang Yihua, Wei Yinxing, You Shilin, Zhang Leyi, Zhao Bo, and Zhou Yang.

I would also like to thank Cao Qi, Christopher Mulley, Dai Heng, Han Diangang, Hua Guohong, Huang Zhimin, Jiang Guobing, Li Shuangquan, Liu Hui, Liu Junyan, Lou Aizhen, Luo Yonghong, Ma Wei, Ma Zhiyuan, Tian Li, Wang Huagang, Wang Xia, Wang Yuzhong, Wang Zhi, Xu Min, Yan Wende, Yang Guirong, Yang Yuxin, Yu Ting, Zhang Jinxin, Zhang Yongyi, Zhang Xiangjun, Zheng Jun, Zhou Tiancai, and Zhu Linlin for your support.

Zhong Hong
Chief Security Officer of ZTE Corporation

Contents

1

Preface

With the development of digital technologies, digital infrastructure plays a vital role in social development and economic growth. According to the Global System for Mobile Communications Association (GSMA)[1], global 5G connections will reach 1.5 billion by the end of 2023 and 5.3 billion by 2030. By the end of 2023, the number of connected IoT devices worldwide will grow by 16% to 16.7 billion[2]. Increasing digitization and connectivity have increased risks while virtualization and increased use of IT in communications networks have expanded the security attack surface, resulting in additional cybersecurity challenges, and the urgent need for comprehensive cybersecurity assurance. According to the European Union Cyber Security Agency (ENISA) Threat Landscape 2023[3], the number of cyber-attacks continue to increase globally. Within the report observation period, the number of global security incidents in 2023 was twice that in 2022.

As the key digital infrastructure, communication networks have attracted more attention in relation to security than ever. From the formulation and conformance of industry standards, vulnerability handling and disclosure, to the comprehensive security assurance of manufacturers, the entire industry and stakeholders are working together to meet these challenges.

Governments have strengthened legislation to horizontally improve cybersecurity in communications and across industries to protect critical infrastructure. The EU Cybersecurity Act encourages the implementation of security measures at the earliest stages of design and development. It emphasizes that the security of ICT products, services and processes throughout their life cycle should be ensured through evolving design and development processes to reduce the risk of harm from malicious exploitation. The EU Cyber Resilience Act emphasizes the importance of cybersecurity, requiring manufacturers to implement security throughout the product lifecycle, including security-by-design and security-by-default, as well as vulnerability response and handling throughout the lifecycle to prevent the introduction of vulnerable products to the market. In China, on the basis of the Cybersecurity Law, the Data Protection Law and other laws, more regulatory requirements have been available, such as the Regulations on the Protection of Critical Information Infrastructure and the Regulations on the Management of Network Product Security Vulnerabilities. At the same time, cybersecurity standardization in the industry is also continuing to advance, including the continuously iterative GSMA Network Equipment Security Assurance Scheme (NESAS), the upcoming European Union cybersecurity certification schemes: EUCC and EU5G. China also implements critical infrastructure certification and releases national standards to promote security standardization.

ZTE, founded in 1985, is the world's leading provider of integrated communications and information solutions. It has the obligation and responsibility to comply with laws and regulations and industry standards to ensure the security of communications network equipment. By providing secure and trustworthy products and services to customers, ZTE enables

[1] *5G in Context, Q1 2023: https://data.gsmaintelligence.com/research/research/research-2023/5g-in-context-q1-2023*

[2] *State of IoT 2023: Number of connected IoT devices growing 16% to 16.7 billion globally: https://iot-analytics.com/number-connected-iot-devices/*

[3] *ENISA Threat Landscape 2023: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023*

secure and reliable network connections and digital life for global users.

This white paper describes ZTE's security governance architecture and security assurance system, emphasizing effective governance methods and practices on the basis of product lifecycle security controls, focusing on in-depth improvements in dedicated fields, including security-by-design and security-by-default, third-party component management, incident response and vulnerability handling. Security controls run through the supply chain, R&D, and delivery business flows, and effective implementation and continuous improvement are ensured through the supporting digital infrastructure.

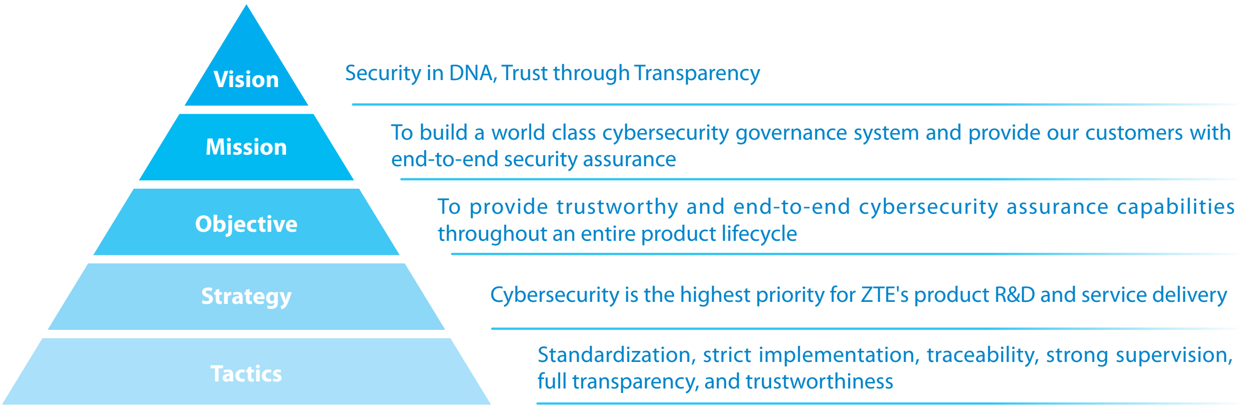
Security is a long journey that needs continuous improvement. With an open and transparent attitude in mind, ZTE welcomes external independent security verification. ZTE is willing to communicate and cooperate closely with operators, regulatory authorities, partners, and other stakeholders to continuously improve managerial and technical practices, jointly establish a secure and trustworthy cyber environment, and maintain the security of the digital world.

2

Cybersecurity Assurance Framework Practices

ZTE regards security as the highest priority for product development and delivery and has established an effective risk-based cybersecurity governance system, 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 trusted connectivity everywhere.



Security in DNA, Trust through Transparency

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

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

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

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

Figure 1 ZTE Cybersecurity Vision

2.1 Three-Line Architecture Ensuring Effective Governance

Enterprises and organizations need highly-efficient risk management through a mature governance architecture. The three lines model[4] issued by the Institute of Internal Auditors (IIA) provides guidance to 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 adopts the security governance organizational structure based on the three lines model and has set up security organizations independent of the first-line business units. The three-line architecture effectively assures cybersecurity from multiple perspectives and multiple levels through self-inspection by business units of the first line, independent security assessment of the second line, and security audit of the third line.

[4] THE IIA’S THREE LINES MODEL: https://www.theiia.org/globalassets/documents/resources/the-iias-three-lines-model-an-update-of-the-three-lines-of-defense-july-2020/three-lines-model-updated-english.pdf

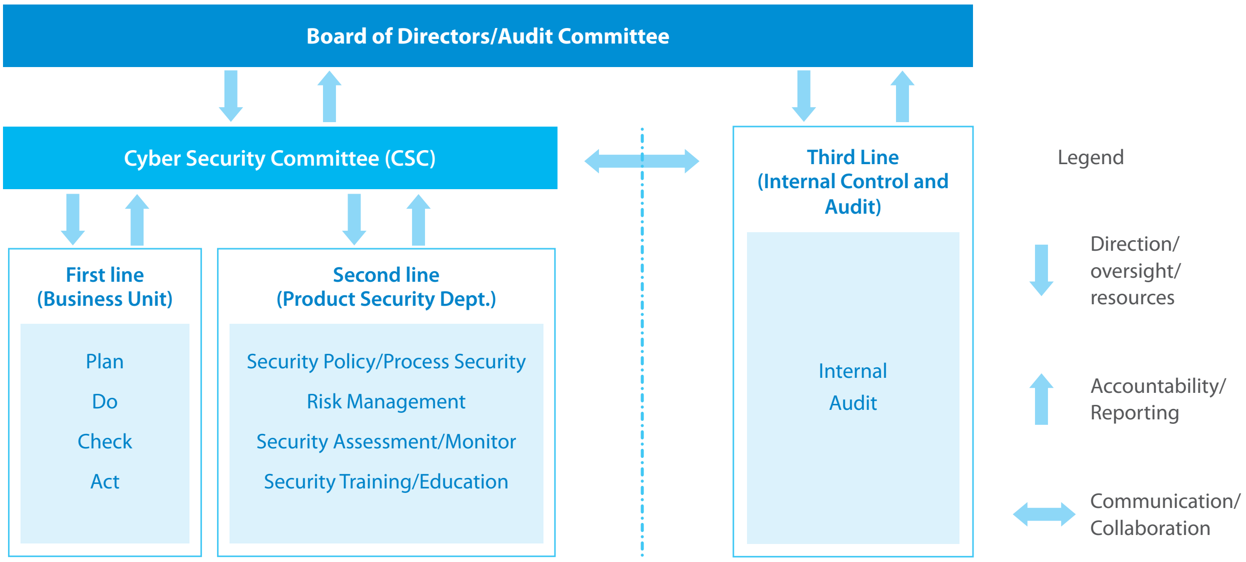

Board of Directors/Audit Committee
Cyber Security Committee (CSC)
First line
(Business Unit)
Plan
Do
Check
Act
Second line
(Product Security Dept.)
Security Policy/Process Security
Risk Management
Security Assessment/Monitor
Security Training/Education
Third Line
(Internal Control and Audit)
Internal
Audit
Legend
Direction/ oversight/ resources
Accountability/ Reporting
Communication/ Collaboration

Figure 2 ZTE Cybersecurity Organizational Structure Based on the three-lines Model

Board of Directors/Audit Committee

The Board of Directors supervises and guides the security governance work of the Cyber Security Committee (CSC), and receives regular security audit results reported by the Internal Control and Audit.

Cyber Security Committee (CSC)

As the decision-making organization for cybersecurity, the CSC makes decisions on strategic direction and security objectives, guarantees resources, reviews cybersecurity plans, and solves major issues. As the Cyber Security Committee (CSC) standing committee members, the top and senior management of the company provide effective security governance.

First line

Business units are the first line of security governance. Each business unit is responsible for implementing cybersecurity through planning, execution, detection, and improvement. In the R&D process, a product is designed to be secure and the product development process is standardized to be secure and controllable. In the supply chain process, ZTE stresses the security of suppliers, materials, and manufacturing procedures to ensure the continuity and resilience of supply. In the delivery process, standard operations are performed to ensure secure delivery of products and services.

Second line

As the second line of security governance, the Product Security Department adopts an independent security assessment mechanism to evaluate and supervise front-line security practices.

ZTE has set up multiple cybersecurity labs to conduct independent security tests, including process audits and product security tests. The process audits evaluate the compliance and effectiveness of the front-line security governance implementation process. The product security tests include vulnerability scanning, code review, protocol robustness testing, and penetration testing. In addition, ZTE actively cooperates with third-party organizations for security assessment of products and processes, such as process audits, source code reviews, security design reviews, and penetration testing.

ZTE attaches great importance to security awareness and capability enhancement. ZTE continuously carries out multi-level and topic-specific security awareness and professional skills training, such as security awareness training for all employees, security design training and penetration testing training for security specialists. Currently, ZTE employees hold 230+ international security certificates.

Third line

As the third line of security governance, the Internal Control and Audit independently audits the work of the front line and second line, and independently evaluates the soundness, reasonableness, and effectiveness of ZTE's cybersecurity assurance system.

In summary, the front-line implementation, second-line supervision, and third-line audit are carried out to ensure that the cybersecurity governance is sound and effective.

2.2 Security Embedded Product Life Cycle

Security governance and control covering the product lifecycle is a basic requirement for cybersecurity.

The EU Cybersecurity Act in 2019 states that security should be ensured throughout the lifetime of ICT products and services by design and development processes that constantly evolve. GSMA NESAS sets out security requirements for product development and the full life cycle, making it a best practice for integrating security into the development and lifecycle processes of communication equipment. ZTE performs risk-based security governance that covers the supply chain, R&D, delivery, incident response, and various support fields, forming a cybersecurity assurance system throughout the product lifecycle while continuously benchmarking against the latest industry standards and best practices. ZTE’s R&D process (High-Performance Product Development, HPPD Process-2017) has passed the GSMA NESAS process audit and the BSI NESAS Cybersecurity Certification Scheme - German Implementation (NESAS CCS-GI) process audit.

For R&D, security controls are incorporated into all phases, including:

- Embedding security requirements into R&D requirements, design, verification, and release processes, such as security design and privacy protection design (Privacy by Design, PbD).
- Performing penetration tests on products and regular security regression tests.
- Continuously tracking, analyzing, and solving security vulnerabilities in third-party components (including open source software).
- Evaluating and controlling security risks in the process of project technical review and release.

For the supply chain, security requirements are incorporated into the qualification of suppliers, newly introduced materials, and production processes, including:

- Imposing cyber security requirements on suppliers through the signing of supplier security agreements, and the performance of regular supplier audits.
- Leveraging the material security testing lab for spot inspection of medium-and-high-risk materials.
- Establishing a dedicated private network in a production environment to prevent security problems.

For delivery, technical and managerial methods are used to continuously improve network security and resilience and ensure delivery of secure products and services. For example:

- Taking security control measures and providing relevant training for personnel in key positions who have access to key equipment in customer's networks.
- Any network changes must be first authorized by the customer, then recorded, and auditable.
- Conducting incident response drills regularly to continuously improve the incident response capability.

In addition, end-to-end business flows, such as third-party component management and vulnerability management, are assured and supported by the DevSecOps tool chain to implement end-to-end security management of the supply chain, R&D, and delivery, and quickly respond to security incidents and vulnerabilities.

2.3 Digital Infrastructure Supporting the Product Lifecycle

ZTE has integrated security governance into the product lifecycle processes, and established the digital infrastructure for cybersecurity that runs through the front-line business units.

ZTE's digital systems, such as the Intelligent Supply Coordination Platform (ISCP), Product R&D Cloud (RD Cloud), and Global Customer Support Center (GCSC), achieve efficient operation in resilient supply, continuous planning, collaborative development, integrated testing, release and deployment, and problem solving. The configuration management system and vulnerability management system are used to efficiently track and trace security issues of products.

In addition, the DevSecOps tool chain is equipped to implement security management and controls in each phase. In key security activities such as material security testing, third-party software security scanning, code scanning, vulnerability scanning, version protection, and security hardening, security tools are used to automatically check whether products and services meet security requirements.

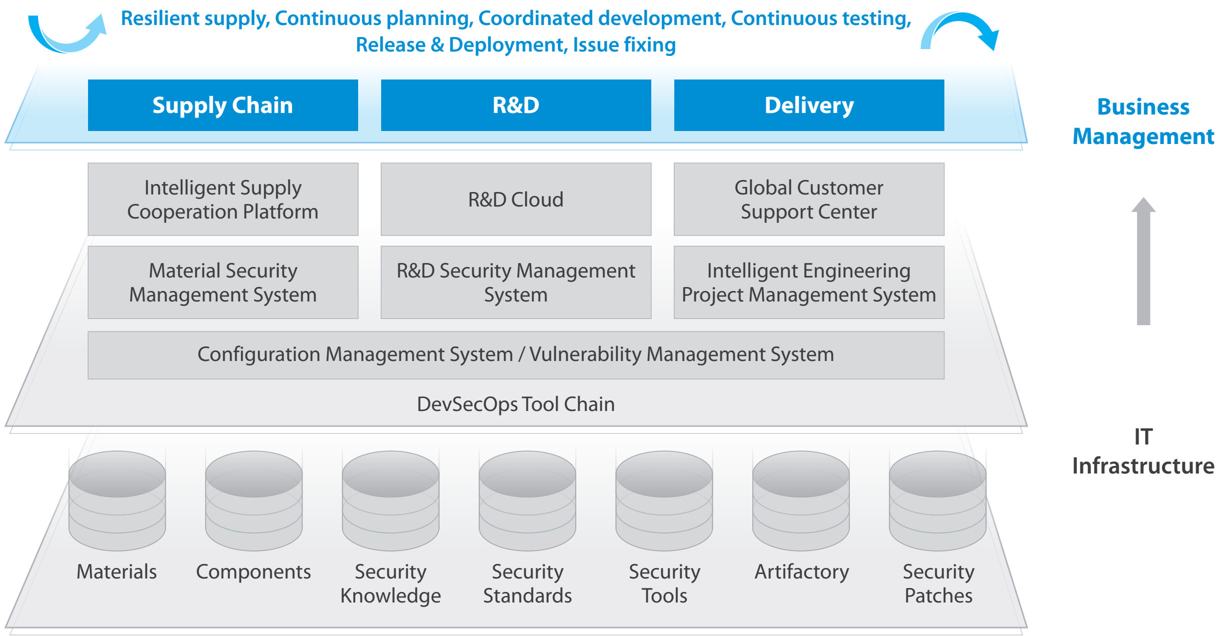

Resilient supply, Continuous planning, Coordinated development, Continuous testing, Release & Deployment, Issue fixing
Supply Chain
R&D
Delivery
Business Management
Intelligent Supply Cooperation Platform
R&D Cloud
Global Customer Support Center
Material Security Management System
R&D Security Management System
Intelligent Engineering Project Management System
Configuration Management System / Vulnerability Management System
DevSecOps Tool Chain
IT Infrastructure
Materials
Components
Security Knowledge
Security Standards
Security Tools
Artifactory
Security Patches

Figure 3 Digital infrastructure supports the product life cycle

3

Realizing Security-by-Design & Security-by-Default

The GSMA NESAS '*Development and Life Cycle Security Requirements*'[5] requires that network products shall apply security-by-design principles throughout the development and product lifecycle.

When applied to product development, Security-by-design principles can prevent malicious network attacks, such as illegal access to network devices, data, or infrastructure. When applying these principles, network equipment manufacturers should conduct risk assessments to identify and enumerate prevalent cyber threats to critical systems and incorporate mitigation into product blueprints.

The EU Cybersecurity Act requires enterprises to design their ICT products, services and/or processes with a higher level of security so that users can obtain products and services with the best security default configuration.

Products with security-by-default are security protected on delivery, and users can use them "out of the box" with no additional configuration needed.

Security-by-design and security-by-default not only benefit users but also manufacturers, reducing vulnerabilities and the cost to fix them.

ZTE advocates transparency and accountability and believes that it is the manufacturer's responsibility to provide products that are secure by design and by default. The company adopts security design principles as early as possible in the product development life cycle, conducts threat analysis and risk assessment during the product design stage, and establishes and optimizes product security protection guidelines and baselines. Security design principles include but are not limited to: attack surface reduction, secure defaults, privacy protection, least privileges, defense in depth, fail secure, separation of duties, etc.

3.1 Security Design Process

In ZTE's product R&D process, security design is a key step in the early stage. It is necessary to identify product threats, evaluate risks properly, and establish control measures to minimize security risks and costs. Security-by-design and security-by-default requirements are included in the security design process to ensure that a product achieves the objectives of out-of-box delivery and intelligent operation.

5. *Official Document FS.16 – Network Equipment Security Assurance Scheme – Development and Lifecycle Security Requirement, Version 2.1*
https://www.gsma.com/security/wp-content/uploads/2022/02/FS.16-v2.1.pdf

ZTE has set up an industry-leading security design process with its own characteristics. Based on industry specifications, technical standards, and market requirements, ZTE has built security knowledge base to implement product-oriented threat modeling, create a security technology benchmark base to implement security design benchmark planning, make risk acceptance decisions, and provide the product security solution design. Based on DevSecOps, a platform-based security design process is developed online, and a closed-loop measurement improvement mechanism is established and continuously optimized.

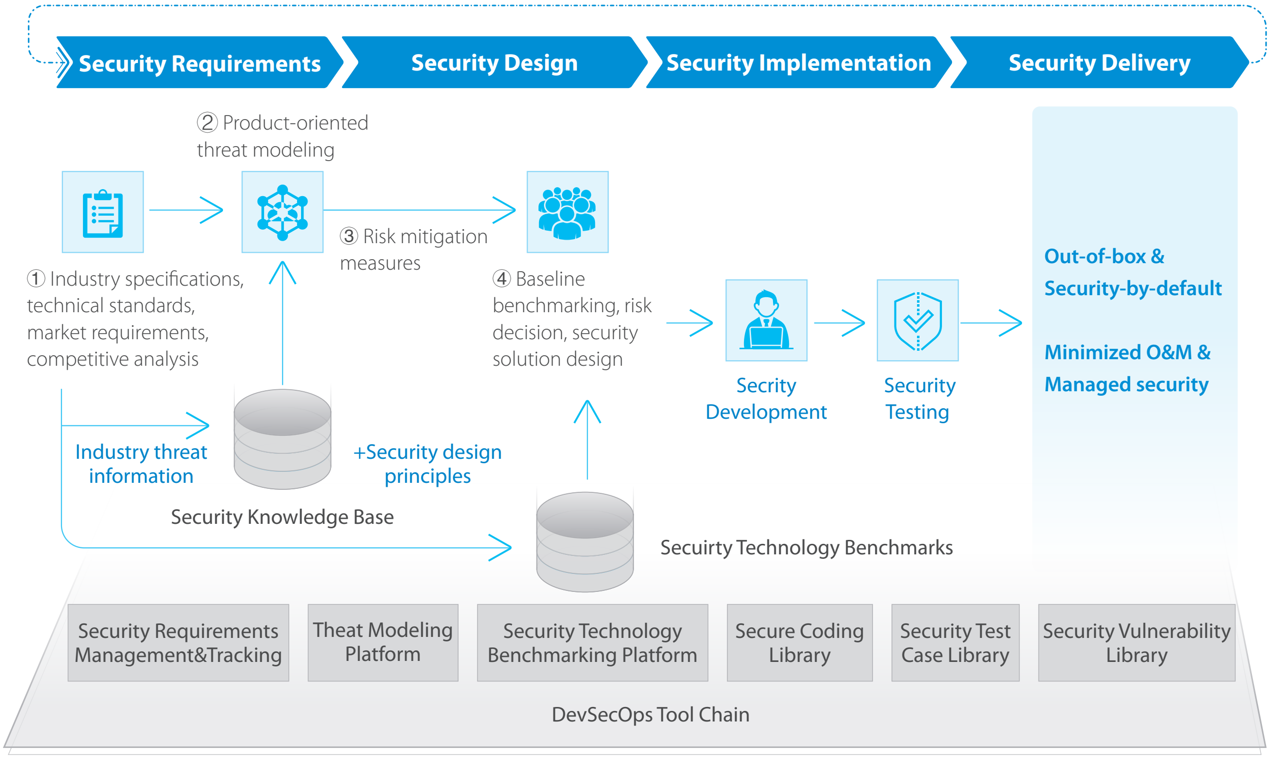

Security Requirements
Security Design
Security Implementation
Security Delivery
② Product-oriented threat modeling
③ Risk mitigation measures
① Industry specifications, technical standards, market requirements, competitive analysis
④ Baseline benchmarking, risk decision, security solution design
Secrity Development
Security Testing
Out-of-box & Security-by-default
Minimized O&M & Managed security
Industry threat information
+Security design principles
Security Knowledge Base
Secuirty Technology Benchmarks
Security Requirements Management&Tracking
Theat Modeling Platform
Security Technology Benchmarking Platform
Secure Coding Library
Security Test Case Library
Security Vulnerability Library
DevSecOps Tool Chain

Figure 4 Security Design Model Applicced in R&D Process

3.2 Security Design Practices

ZTE uses its security knowledge base, security technology benchmark base, and the threat modeling platform to perform its security design. Cybersecurity knowledge and experience is accumulated in the security knowledge base to continuously improve professionalism and effectiveness of the security design. The security technology benchmark base complies with industry security standards and specifications, and provides baseline requirements for the security design. The threat modeling platform supports online, automated, and visualized collaborative operations.

Security Knowledge Base

The security knowledge base incorporates industry specifications and best practices, including general threat and vulnerability information (such as CAPEC, ATT&CK, CWE, and CVE), industry security technical standards and specifications (such as 3GPP SCAS specifications and IETF RFC standards), and cybersecurity experience accumulated by ZTE. The knowledge base is built in conformance with the structured threat information expression (STIX) specifications, and includes key elements such as assets, threats, risk criteria, control measures, attack patterns, and abuse cases.

Security Technology Benchmark Base

The repository of security technology benchmarks includes the directory panorama of security technology stacks and security design technical standard families. The technology stacks directory uniformly classifies the technology stacks involved in products according to the principle of "hierarchical architecture, domain-specific technology". A series of security design technology guides are compiled for the key security technology stacks, and are released as enterprise technical standards. ZTE records all released security technical requirements into the security technology benchmarking platform on the RD Cloud, and embeds the security technical requirement baseline controls in the product R&D process.

Threat Modeling Platform

By building a threat modeling platform, ZTE implements digital processes for key threat modeling activities such as asset identification, threat analysis, risk assessment and handling, control measure selection, and security tracking matrix, in order to achieve standardization, automation, hierarchy, and visualization of processes. The threat modeling platform has been integrated into the DevSecOps platform, supporting cross-team collaborative R&D and flexibly carrying out threat modeling.

4

Security Development and Testing

ZTE considers security as the highest priority for R&D, and "security" must be incorporated into the product development process as a basic attribute of the product.

ZTE benchmarks industry standards and best practices for product development and testing. Referring to the Building Security In Maturity Model (BSIMM), Network Equipment Security Assurance Scheme (NESAS), and Capability Maturity Model Integration (CMMI), ZTE has formulated its security maturity model and corresponding regulations, and performs regular reviews in order to make continuous improvements.

ZTE's security coding standards are based on general guidelines in the industry, 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). In the development process, source code scanning is a key control point. It is necessary to measure the quality and security of code through static check and automatic scanning, and conduct Kanban closed-loop management of defects scanned by tools. ZTE focuses on improving developers' ability to code securely and continually improve their competency through regular assessments.

Each product project shall develop security testing procedures and testing plans, and conduct security tests such as code scanning, vulnerability scanning, protocol robustness testing, and virus scanning on the product during the testing phase to fully verify the implementation of security requirements and fix defects. The company has established a professional penetration testing team to explore vulnerabilities more deeply.

In the release process, the company requires that a product must undergo security testing and security risk assessment. Security hardening manuals and tools must be provided during product release. The release process is verified by a Certificate Authority (CA) to ensure consistency and traceability in the release process.

In the maintenance process, ZTE regularly performs regression tests to identify whether new vulnerabilities affect existing versions. The R&D team updates security patches and formulates security hardening plans in a timely manner, so that users can eliminate or control security risks.

5

Third-party Component Management

As the ICT industry continues to evolve and more third-party components are used in ICT products[6], new threats may emerge from newly discovered vulnerabilities or end-of-service.

Third-party component management is a critical part of security assurance. Regulators and industry organizations successively release guidelines and requirements aimed at enhancing third-party component management and minimizing associated risks. For example, GSMA NESAS has added "Sourcing and Lifecycle Management of 3rd-Party Components" in the 2.0 version, requiring that the equipment vendor shall have processes in place to ensure the quality of third-party components during the product lifecycle. The equipment vendor shall select supported third-party components and shall avoid using those reaching the end of life. Meanwhile, it is necessary to evaluate if potential threats are found from newly discovered vulnerabilities in the third-party components.

5.1 Third-Party Component Management Strategy

Third-party components include open source software, commercial components, and commercial auxiliary software. These components are part of the product and may be used by multiple products. In accordance with laws, regulations and industry best practices, ZTE continuously accumulates experience and practices in the process of supply chain management, product R&D, and delivery to implement full-lifecycle management of third-party components.

The security management of ZTE’s third-party components covers introduction, use, O&M, and exit, and the management requirements have been incorporated into ZTE’s High Performance Product Development (HPPD) process.

[6] *Object with discrete structure, such as an assembly, a software package, which is sourced from an external entity and incorporated into a Network Product, Official Document FS.16 – Network Equipment Security Assurance Scheme – Development and Lifecycle Security Requirement, Version 2.1*

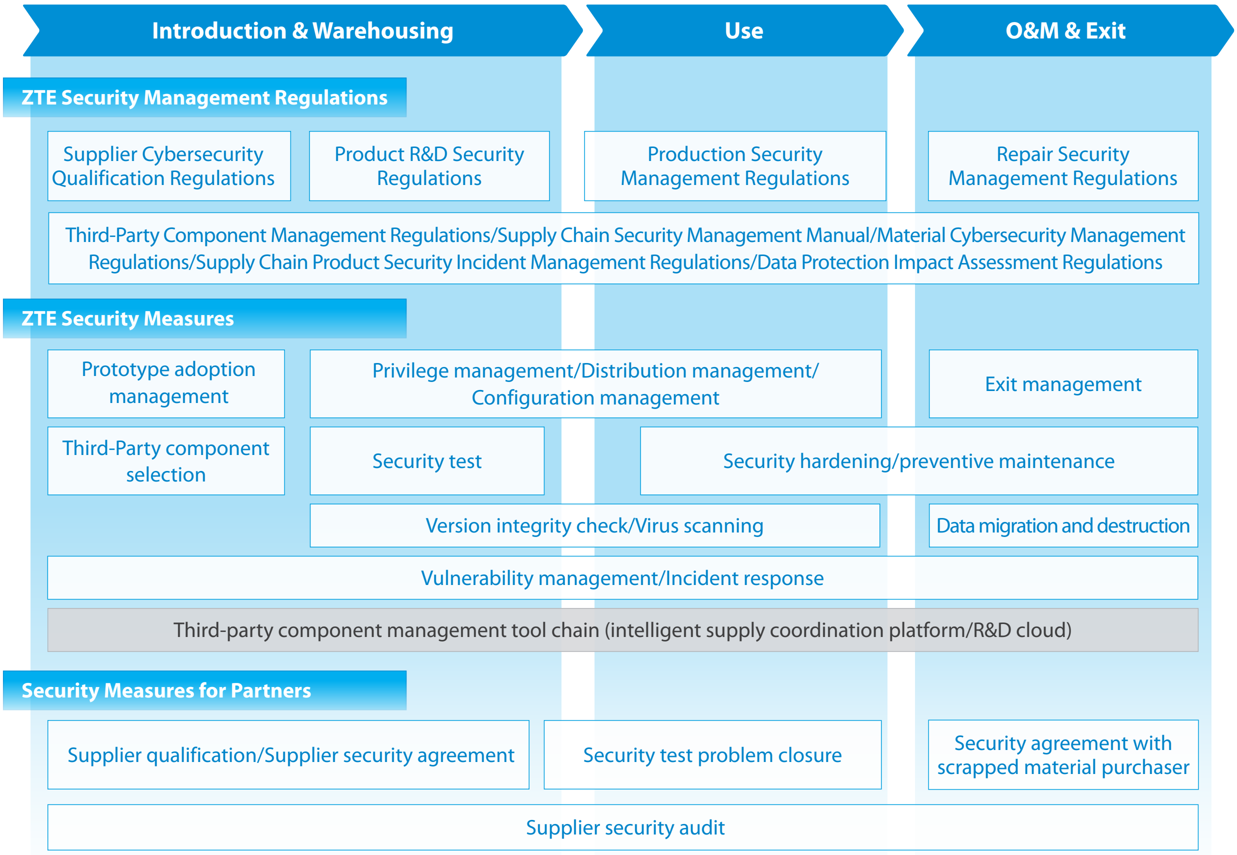

Introduction & Warehousing
Use
O&M & Exit
ZTE Security Management Regulations
Supplier Cybersecurity Qualification Regulations
Product R&D Security Regulations
Production Security Management Regulations
Repair Security Management Regulations
Third-Party Component Management Regulations/Supply Chain Security Management Manual/Material Cybersecurity Management Regulations/Supply Chain Product Security Incident Management Regulations/Data Protection Impact Assessment Regulations
ZTE Security Measures
Prototype adoption management
Privilege management/Distribution management/ Configuration management
Exit management
Third-Party component selection
Security test
Security hardening/preventive maintenance
Version integrity check/Virus scanning
Data migration and destruction
Vulnerability management/Incident response
Third-party component management tool chain (intelligent supply coordination platform/R&D cloud)
Security Measures for Partners
Supplier qualification/Supplier security agreement
Security test problem closure
Security agreement with scrapped material purchaser
Supplier security audit

Figure 5 Third-Party Component Management

Introduction & Warehousing

- The ZTE component library (iComp) can only introduce third-party components that satisfy the selection requirements. To ensure compliance with export controls, data protection, and open source licensing, the selection processes include security compliance scanning, analysis and verification of functions and performance, and risk evaluation. The life-cycle and sustainability of third-party components must also be taken into account.
- For the third-party components that have met selection requirements, a component guard shall be set to manage the full lifecycle of the components.
- Security agreements are signed with commercial component suppliers to ensure they understand and are committed to the security requirements for third-party components. ZTE regularly organizes empowerment activities for suppliers so that together we contribute to the security ecosystem.

Use

- Only third-party components from iComp are allowed to be used in ZTE's products.
- In the phase of product solution design, development, test and release, risk assessment of third-party components is embedded to ensure security solutions or prevention are implemented in a timely manner.
- The product can be released only after it passes the device-level security tests and meets the security standard.
- Third-party components are included in the product configuration items to ensure traceability. If vulnerabilities of third-party components are found, the impact of vulnerabilities can be tracked through the product configuration items.

O&M and Exit

- The component guard is responsible for implementing the updates when the third-party component is updated for function, performance, or security problems reasons, or a new patch is introduced. If the third-party component provider stops maintenance and the lifecycle ends, the component guard performs the deactivation operation. The update and deactivation notifications are both automatically sent to the R&D team to update product solutions.
- In the product delivery phase, ZTE Product Security Incident Response Team (PSIRT) collaborates closely with suppliers and the security community to obtain the vulnerability information of third-party components in a timely manner. PSIRT works with related teams to analyze the impact, formulate, verify, and implement the vulnerability mitigation solution to ensure prompt response and address the security problems and risks brought by third-party components.

Open Source Component Management

- During the introduction, open source components that are secure, compliant, highly active in the community, complete in the ecosystem, and highly reliable are preferred, and an open source component maturity evaluation model is established as a reference for product selection and security evaluation.
- Open source software component analysis tools and vulnerability scanning tools are used to evaluate the security and license compliance of open source components, and identify and fix known vulnerabilities.
- ZTE submits security problems and solutions of open source components to the open source community to share results.

5.2 Third-Party Component Management Practices

ZTE's iComp provides a secure and trustworthy platform for introducing, using and managing third-party components, and is an important part of the RD Cloud. For product planning, development, testing, integration, release, and O&M, iComp provides functions such as same source management, security compliance management and control, invocation tracking, retrieval, and review.

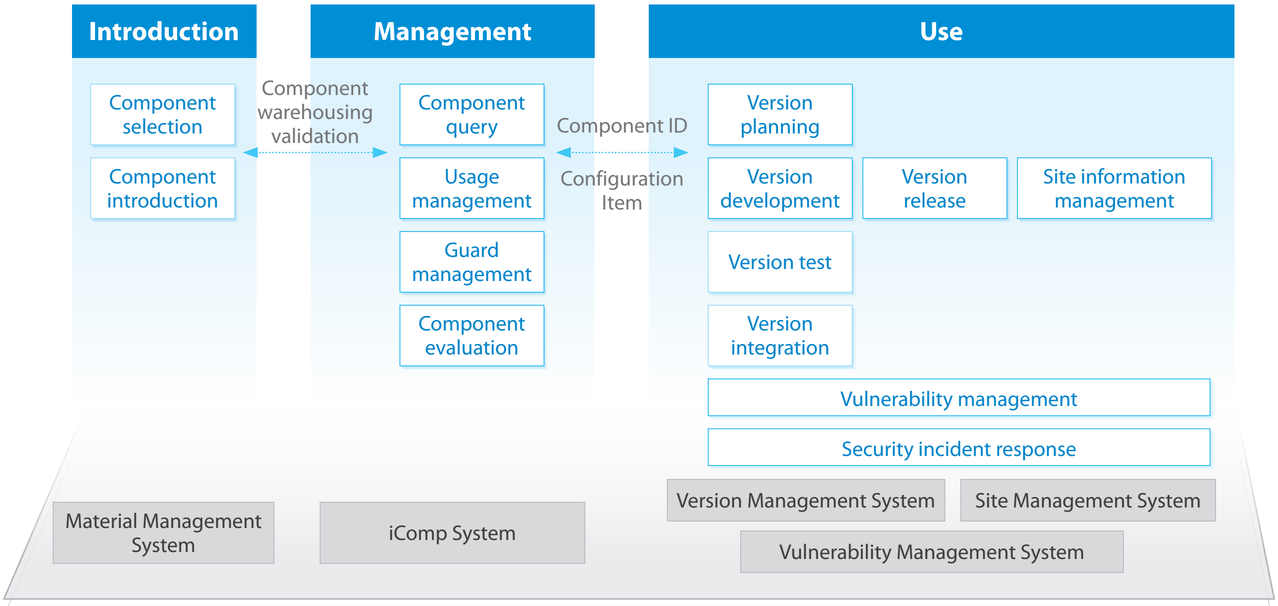


Figure 6 Third-Party Component Management Practices

Based on mature management of product configuration items, ZTE has established a product lifecycle vulnerability management process that integrates third-party components. Once the vulnerabilities of third-party components are detected, the vulnerability management system can automatically locate the affected products, versions and customers so that they can be tracked and mitigated.

6 Resilient Supply Chain

The ICT industry's supply chain is more complicated and prone to security issues when compared to traditional industries. The network's complexity, modularity, and virtualization provide operators with a variety of options when choosing suppliers. Every supplier has a unique supply chain, and any issue anywhere in the network might have a domino effect of unfavorable outcomes.

According to the 2023 ENISA Threat Landscape, 61% of companies were affected by software supply chain attacks in the past 12 months, and it is estimated that the total cost to enterprises of these attacks will grow 76% over 2023 by 2026.

Therefore, the regulators and customers of each country extend their security concerns from network equipment suppliers to their level-2 or even level-3 suppliers, and at the same time, expand their focus from network security, data security, and personal privacy protection to supply security and business continuity. This places greater demands on the security and resiliency of the supply chain.

6.1 Supply Chain Security

For ZTE, building a secure, reliable, and resilient supply chain[7] is not only the intrinsic requirement for the secure delivery of ZTE’s product, but also ZTE's solemn commitment to its customers. ZTE has passed the ISO 27001 information security management system certification, ISO 28000 supply chain security management system certification, and ISO 22301 business continuity management system certification. In addition, ZTE has passed the Authorized Economic Operator (AEO) certification, which ensures fast customs clearance in relevant countries or regions.

ZTE has a complete supply chain business process. It focuses on the customer's business and security requirements, and emphasizes security governance in four aspects: supplier management, materials, manufacturing, and logistics and freight, to support the whole supply chain business process. According to the Supply-Chain Operation Reference-model (SCOR)[8], ZTE expands the supply chain security scope to the supplier’s supplier and customer’s customer.

[7] The ‘supply chain’ introduced in section 6.1 and 6.2 indicates the upstream and downstream supply chain from the perspective of equipment vendor.

[8] Supply-Chain Operations Reference-model, which is developed and supported by Supply-chain Council development of the International Supply Chain Association.

Supplier Security

ZTE has thousands of supplier partners all over the world, to provide tens of thousands of raw material components, semi-finished products, finished products, or services. Therefore, ZTE considers supplier security management and material security management as core business processes to ensure the security of materials and third-party components.

The first step in ensuring supply chain security is to choose a secure and reliable supplier. ZTE attaches great importance to the development and deployment of supplier resources, and has established a set of full-lifecycle processes for supplier management, including sourcing, qualification certification, and exit. In the process of providing products and services, ZTE requires suppliers to comply with local laws and regulations, keep improving the security management level, and comply with the product security agreements signed by both parties. For newly discovered security vulnerabilities, suppliers are required to work with ZTE to track and locate them, and provide patches or upgrades, replace, or recall them in a timely manner.

ZTE continuously passes product security and Corporate Social Responsibility (CSR) requirements to suppliers, and empowers suppliers through the annual Global Partner Conference and supplier training camps.

Material Security

ZTE defines the risk level of materials as high, medium, and low. For high-risk materials, in the material introduction phase, suppliers are required to provide product security testing reports. For medium-level and low-risk materials, by signing security agreements with suppliers, suppliers are required to perform self-management and constraint, and ZTE is allowed to perform multiple forms of security auditing. In addition, ZTE has set up a product security material inspection laboratory to spot-check medium and high-risk materials, and implement closed-loop management of security problems found in spot checks.

Manufacturing Security

ZTE has formulated manufacturing security management regulations to divide manufacturing areas into three levels to manage risks, such as unauthorized hardware replacement, software implantation or tampering, and virus infection. Different security control measures are taken for different levels of security control areas. Level-1 and level-2 control areas are strictly controlled areas to avoid risks. Security administrators are set in these areas to implement security controls and routine security supervision.

To ensure the security of the production environment, ZTE has built a dedicated production network to prevent virus intrusion or software tampering. Only authorized engineers can use this private network.

Logistics and Freight Security

ZTE tracks the whole processing cycle of goods in the warehouse through the warehousing management system. The logistics warehousing IT system, monitoring devices, and security facilities eliminate the damage, replacement, or malicious code injection of finished products or core components during the warehousing and freight process. The logistics warehousing IT system, monitoring devices and security facilities are upgraded regularly to ensure their effectiveness. The freight trail is monitored in real-time through the freight middle platform system (iLMS), and an early warning function for stakeholders is deployed.

6.2 Supply Chain Resilience

Adhering to the concept of a secure, precise, intelligent, reliable, and efficient SPIRE supply chain and aiming to deliver competitive products and services, ZTE has built three core capabilities into its supply chain: anticipation, immunity, and adaptation. Through its intelligent systems, ZTE visualizes service monitoring, early warning, coordination, and scheduling functions to build a secure, reliable and resilient supply chain.

Anticipation

In the planning and purchase phase, analysis of basic information is conducted, including purchase requirements, supplier production capacity, and purchase period. In the production, delivery and reverse logistics phases, ZTE focuses on supply resilience and critical lower-level materials. Based on the internal and external environments, ZTE makes proactive insights, balances supply and demand, and makes dynamic adjustments to build a robust and intelligent supply chain plan and improve the ability to predict fluctuations in demand.

Immunity

In the purchase phase, material planning and product planning is carried out at the same time to select preferred materials, manage and control exclusive sources of supply, output alternative solutions, and plan resource storage. ZTE continuously optimize the long-term material management and multi-location storage mechanisms, carries out strategic cooperation with high-quality suppliers, and cooperates with upstream and downstream suppliers to ensure the continuity and stability of supply.

In the manufacturing phase, a production capacity risk scanning mechanism is established, and multiple manufacturing bases are used to ensure continuous production by sharing production resources, unifying scheduling, and mutually backing up production capacity. ZTE has set up five production bases in Shenzhen, Heyuan, Changsha, Nanjing, and Xi'an, and works with outsourced factories to meet production requirements by flexibly adjusting production capacity to ensure a resilient production base.

In the freight phase, ZTE has over 50,000 transportation lines around the world, and backs up multiple freight solutions to ensure the continuity and stability of logistics delivery. With a digital freight risk map, freight risks, in-transit risks, common risks, and port congestion can be monitored and alerted in real-time.

Adaptability

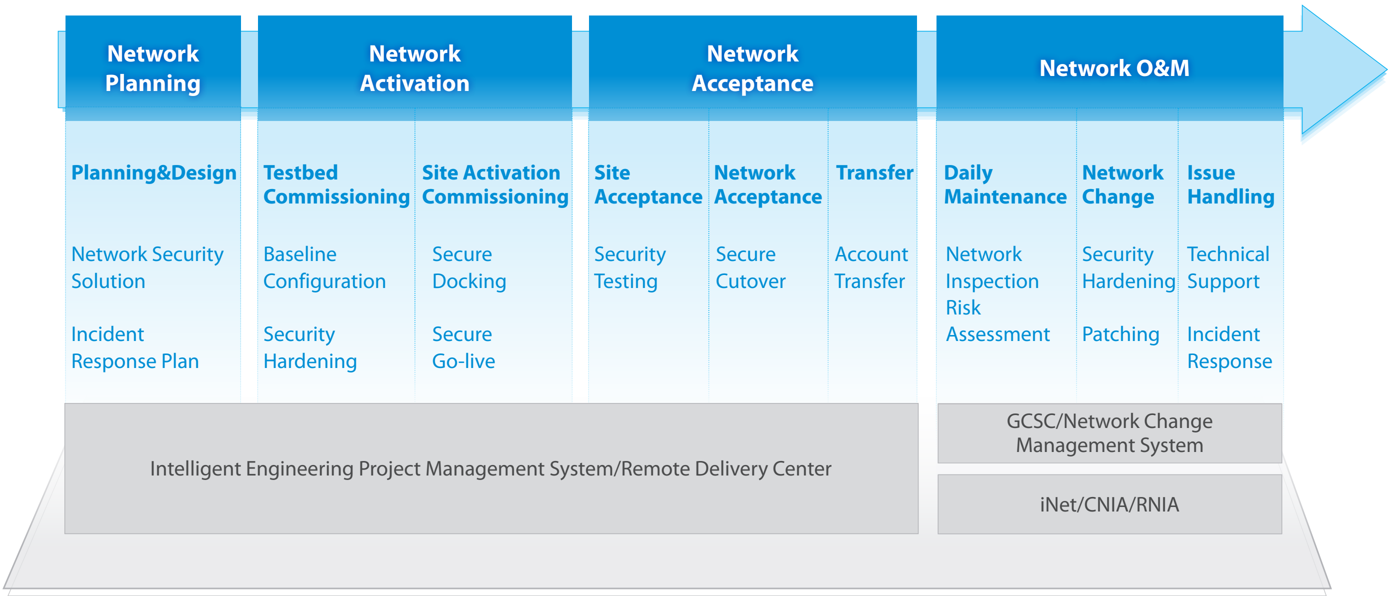
Through the use of digital platforms, including the supply resource risk map, intelligent manufacturing center, and freight risk map, ZTE can integrate core data, identify and analyze abnormal conditions, locate them accurately, and ultimately improve efficiency. In this way, the purchase, manufacturing, freight, and customs affairs businesses are visible across a whole region, making the business visible, clear, and accurate.

7 Secure Delivery

With the delivery of products to customers, service scenarios change, and new security risks arise. Proper protection measures need to be taken to ensure integrity, confidentiality, and availability during the delivery of products and services.

7.1 Secure Delivery Strategy

With reference to the NIST CSF security risk management framework, ISO 27001, and other industry security standards, best practices, and customer network security requirements, ZTE has established a risk-based delivery governance system, and incorporated a series of specifications. This series of specifications covers network planning, commissioning, acceptance, and O&M phases to ensure secure and reliable delivery, secure operation of network devices, and secure protection of customer network data.



Network Planning	Network Activation		Network Acceptance			Network O&M		
Planning&Design	**Testbed Commissioning**	**Site Activation Commissioning**	**Site Acceptance**	**Network Acceptance**	**Transfer**	**Daily Maintenance**	**Network Change**	**Issue Handling**
Network Security Solution Incident Response Plan	Baseline Configuration Security Hardening	Secure Docking Secure Go-live	Security Testing	Secure Cutover	Account Transfer	Network Inspection Risk Assessment	Security Hardening Patching	Technical Support Incident Response
Intelligent Engineering Project Management System/Remote Delivery Center						GCSC/Network Change Management System iNet/CNIA/RNIA		

Figure 7 ZTE End-to-end Secure Delivery Assurance

7.2 Secure Delivery Practices

ZTE's secure delivery system covers modules for personnel management, authorization management, software deployment, network change, security verification, remote access management, data protection, and incident response. Based on AI, big data and other technologies, ZTE visualizes the indicators of the entire engineering service process, identifies and tracks risks in a timely manner, and assists customers in secure and stable network operation.

Personnel Management

ZTE regularly conducts a comprehensive security evaluation of engineers, and determines their positions and levels. During project delivery, position matching is performed in accordance with the personnel evaluation results, operation permissions are allocated in accordance with customer requirements, and a Non-Disclosure Agreement (NDA) is signed. Based on routine tasks such as commissioning, O&M, preventive maintenance, troubleshooting, and security hardening, ZTE conducts a variety of activities such as class projects, workshops, practice and skill competitions to help delivery personnel enhance their security capabilities.

Authorization Management

Before performing operations on a customer's network and data, such as software upgrade, security hardening, and security preventive maintenance, ZTE obtains the customer's authorization in advance, and completes the operations within the agreed scope and time period. The operation process is recorded and the specific operation can be traced through logs.

Software Deployment

To ensure end-to-end software deployment, ZTE implements strict processes and management regulations. Only authorized personnel can download required versions or patches from ZTE's technical support website (support.zte.com.cn). Historical download records are kept, and the downloaded software is checked for integrity or digital signature before upgrade. The tools and software required for software deployment are obtained from the specified channels. If personal work terminals are to be connected to a customer network, it's mandatory to install basic security protection, such as system patches and anti-virus software. Only authorized software, without information security risks,related to service purposes is permitted to be installed.

Network change

After obtaining the customer's authorization for network changes, ZTE's engineer submits the specific implementation in the network change system (ZXRDC). After the solution passes the review of product experts, the engineer implements the change within the specified time and scope. To ensure the stable operation of services after network changes, the related personnel are on duty for a period of time to observe, record, and analyze specific indicators. For personal work terminals connected to customer networks, intelligent management and control tools are deployed to intercept high-risk instructions and unexpected actions in real time.

Security Check

Through security-by-default principles, the delivery of secure products "out of the box" is considered in the product R&D stage, however,risks will also vary and may be present due to internal and external threats. Based on contract requirements, ZTE performs regular security checks, and identifies, evaluates, and handles risks in accordance with the security situation awareness system and the results of customer's vulnerability scanning and penetration testing.

Remote Access Management

To ensure efficient and secure remote technical support, under the prerequisite of complying with local laws and regulations and customer authorization, ZTE product experts may be required to remotely access the customer network through the Advanced Operations Suite (AOS) and the security isolation area for troubleshooting or service support. All remote operations on a customer's network are logged and can be audited afterwards.

Data protection

In accordance with local laws, regulations and customer requirements, ZTE implements security protection operations upon important and sensitive network data, such as data masking, encrypted storage, and encrypted transmission. In the countries and regions where GDPR or similar regulations are in force, ZTE will sign the Data Processing Agreement and Data Transfer Agreement along with the contract clarifying the personal data protection terms and responsibilities. During the contract period, the engineer will perform any required service operations in accordance with the contract terms. In special cases, for example, if faulty boards containing personal data are returned for repair, engineers will strictly operate in accordance with the contract requirements for data protection.

Incident Response

To effectively deal with possible security incidents, ZTE formulates security solutions and emergency response plans in accordance with specified project scenarios. The project teams regularly carry out cross-team and cross-region emergency drills with customers, product teams, and third-party partners.

After ZTE receives an incident reported by a customer, the PSIRT immediately creates an incident ticket in the Global Customer Support Center and distributes it to the corresponding product support team to ensure that the security incident is solved, based on its severity, within the time specified in the customer service level agreement (SLA).

8

Incident Response and Vulnerability Management

In an increasingly complex supply chain environment, proper management of security incidents and vulnerabilities is significantly important. The EU Network Information Security Directive (NIS2) introduces key measures to enhance cybersecurity, including incident response, vulnerability handling and reporting. The EU Cyber Resilience Act requires digital product manufacturers to proactively report exploited vulnerabilities. China has issued the Regulations on Network Product Security Vulnerability Management to require network product providers to fulfill their vulnerability management obligations.

Incident response and vulnerability management processes rely on the collaborative efforts of stakeholders. Equipment vendors have the responsibility and obligation to assist customers in handling security incidents and eliminate security vulnerabilities in a timely manner. ZTE PSIRT is responsible for responding to the incidents and handling vulnerabilities found in ZTE products. ZTE is a member of the Forum of Incident Response Security Teams (FIRST) and a CVE Numbering Authority (CNA). ZTE has also launched bug bounty programs to encourage security researchers and organizations worldwide to report vulnerabilities in ZTE products.

8.1 Incident Response Process

ZTE offers customers rapid assistance in handling security-related issues. With the authorization of the customer, PSIRT assists them in quickly handling an incident and takes necessary measures to control the situation until the issue is completely resolved.

The incident response process consists of four key stages:

1.Preparation: Develop an incident response plan and conduct regular drills, equipped with tools and resources;

2.Detection & Analysis: Collect, record and analyze incident-related data, determine whether an intrusion has occurred and has consequences, and analyze the scope of impact, including affected versions and affected customers. If the incident is caused by a vulnerability, the vulnerability management process will be triggered;

3.Containment, Eradication & Recovery: Implement mitigation plans to suppress the impact of the incident and prevent its continued spread; Provide solutions to eliminate the impact of the incident and recover normal business;

4.Post-incident activities: Organize reviews, summarize experiences, and continue to improve incident response capabilities.

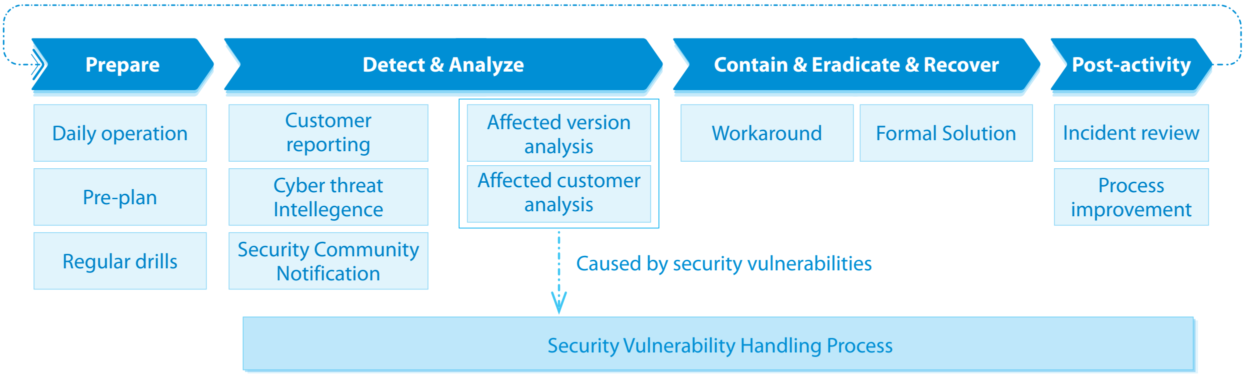

Prepare
Detect & Analyze
Contain & Eradicate & Recover
Post-activity
Daily operation
Pre-plan
Regular drills
Customer reporting
Cyber threat Intellegence
Security Community Notification
Affected version analysis
Affected customer analysis
Workaround
Formal Solution
Incident review
Process improvement
Caused by security vulnerabilities
Security Vulnerability Handling Process

Figure 8 ZTE Incident Response Process

8.2 Vulnerability Management Process

ZTE attaches great importance to cooperation with security organizations, and responsibly discloses vulnerabilities discovered internally and externally in accordance with the principle of openness and transparency. After the customer implements the solution, the effectiveness of the solution is monitored, and the solution is iterated based on feedback to achieve closed-loop vulnerability management.

The vulnerability handling process consists of five stages:

1.Receive: Receive vulnerabilities discovered from customers, suppliers, open source communities, security groups and internal security assessments;

2.Verify: Verify vulnerabilities, analyze impacts, and assess risks;

3.Resolve: After confirming that the product is affected by the vulnerability, provide mitigation measures and solutions;

4.Disclose: Maintain communication with vulnerability reporting parties and affected customers, report progress in real time, assist customers in repairing vulnerabilities, and complete coordinated disclosure of vulnerabilities;

5.Review: Accumulate experience from management, technology and other perspectives to improve the efficiency and capability of vulnerability management.

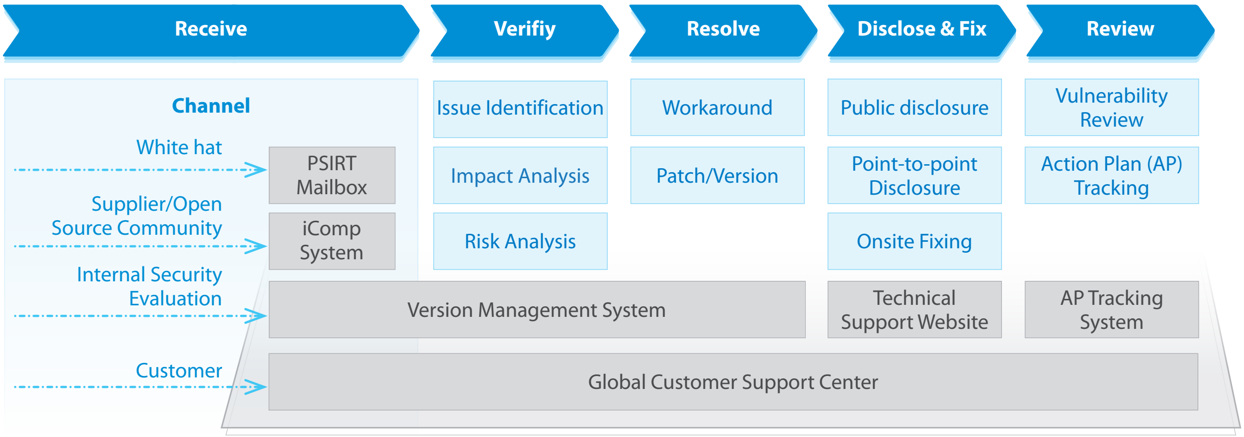


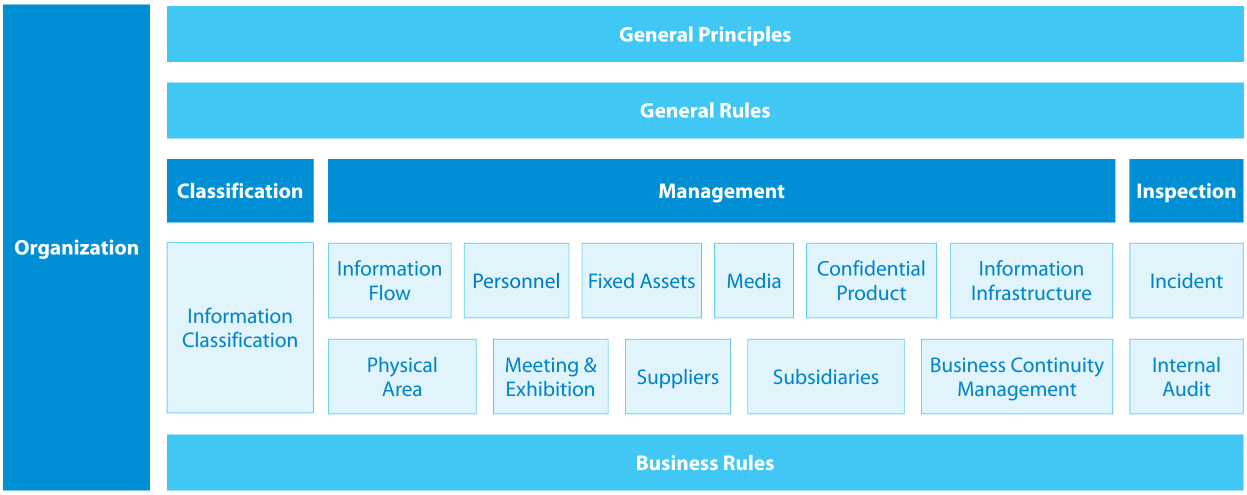
Figure 9 ZTE Security Vulnerability Handling Process and IT System

9

Information Security and Privacy Protection

9.1 Information Security

The purpose of information security management is to protect the confidentiality, integrity, and availability of ZTE's information assets, and to maintain a secure environment for key services such as product R&D, production, and operation. ZTE has established a hierarchical, complete, and closed-loop information security management system to prevent information leakage and intrusion. Once an information security event occurs, the system can respond quickly to the event and minimize losses, ensuring the normal operation of business activities.



Organization

General Principles

General Rules

Classification

Management

Inspection

Information Classification

Information Flow

Personnel

Fixed Assets

Media

Confidential Product

Information Infrastructure

Incident

Physical Area

Meeting & Exhibition

Suppliers

Subsidiaries

Business Continuity Management

Internal Audit

Business Rules

Figure 10 ZTE Information Security Management System

Based on the standard architecture and requirements of the ISO 27001 standard for information security management, in compliance with local laws and regulations and industry standards, ZTE implements hierarchical control and closed-loop management of information. Firstly, by identifing objects, so as to focus on core assets. Secondly, by managing and controlling the information flow itself, focusing on the people, events, and things associated with the information flow. Thirdly, by assessing and enhancing the system's compliance, and looking into and managing information security incidents.

For the information generated, collected and received in its production and operation activities, ZTE classifies them into four confidentiality levels: top secret, secret, internal use, and public. For customer information accessed and processed in business activities, they are mapped to the corresponding confidentiality level for hierarchical management. In order to fully protect the core data, important data, business information, and personal information from business activities associated with national interests, public interests, corporate interests, and personal interests, a series of technical methods are used, such as storage and transmission encryption, authentication and others.

In 2005, ZTE became the first listed company in Mainland China to obtain ISO 27001:2005 certificate for information security management. As of 2023, ZTE's headquarters and global subsidiaries have obtained a total of 27 ISO 27001 certificates. ZTE continues to learn advanced management concepts and explore information security management models with its own characteristics, to cope with the information security challenges brought about by global digitization.

9.2 Privacy Protection

ZTE abides by the privacy protection laws and regulations of the country and region where the business is located, and regards "legal compliance, joint building of trust, and ethics implementation" as important baselines for privacy protection. ZTE takes proactive action on meeting legal requirements, preventing and controlling business risks, winning market trust, and building a sound ecosystem by building a privacy protection system, controlling privacy protection in key scenarios, and exploring privacy protection practices.

ZTE builds a risk-based comprehensive system from the dimensions of organization, people, system, and technology, and continuously optimizes the system during its operation to ensure the adaptability, effectiveness, and advancement. The company has established scenario-based business process compliance guidelines and established management and control mechanisms for high-risk scenarios to protect the data and privacy of users, customers, and employees. A three-line defense has been built to effectively manage the risks. ZTE has established data protection compliance mechanisms, such as the data breach response process, data subject request process, data cross-border transfer control process, and supplier compliance control system.

Following the concept of Privacy by Design (PbD), ZTE embeds privacy protection controls into the design phase of product and service solutions, in order to integrate data protection requirements into products by default.
Adhering to the concept of open and transparent data compliance, ZTE has launched the Privacy Center on its official website to show global customers, partners, consumers, and other relevant parties about progress on privacy protection and provide feedback windows[9].

[9] https://www.zte.com.cn/china/privacy_center.html

10

Business Continuity Management

To deliver secure and reliable products and services, ZTE continuously builds its capabilities for emergency response and business recovery by using a systematic framework and methodology. ZTE has passed the ISO 22301 certification for business continuity management (BCM).

The reliability and resilience of ZTE's products is is focused on service solutions and infrastructure solutions. By default, the backup solutions and disaster recovery capabilities of devices and networks are considered in the product design and solution design phases.

To ensure BCM of R&D resources, ZTE regularly refreshes high-risk points, and manages high-risk scenarios such as exclusive supply agreements, key IT systems, core laboratories, and virus attacks. The subsidiaries of ZTE all around the world are capable of rapid remote office deployment to ensure the normal operation of core services.

The BCM of the supply chain is oriented to the purchase, manufacturing, and freight business processes. The intelligent supply management system is used to implement full-service monitoring, early warning, coordination, and scheduling, ensuring the continuity and stability of purchase, supply, manufacturing, and logistics delivery.

The service continuity management of delivery includes engineering delivery and network services. To guarantee the network construction and O&M services of global customers, ZTE has formed a set of management processes, including early warning prevention, drills, incident handling and review.

11

Openness, Cooperation, and Engagement

11.1 Cybersecurity Labs

To promote openness and transparency, ZTE established three cybersecurity labs in Nanjing in China, Rome in Italy, and Dusseldorf in Germany, and two cybersecurity transparency centers in Belgium and Turkey.

As the platform for customers, regulatory authorities, and stakeholders to evaluate and verify the security of ZTE products, services, and processes, the cybersecurity labs support penetration testing, document review, source code review, technical exchange and sharing. The labs have hosted a number of important customers and institutions for technical exchanges and security assessments. Taking the Italy cybersecurity lab as an example, our customers used the lab to perform penetration testing and source code review on a number of products, including 5G, home terminals, and mobile phones. Some of the projects were performed under the independent supervision of the National Inter-University Consortium for Telecommunications (CNIT)[10]. ZTE also participated in events organized by security organizations in Italy and throughout Europe to share knowledge and experience to contribute to the cybersecurity ecosystem.

Different from the cybersecurity lab, ZTE cybersecurity transparency centers are scaled down to facilitate source code and documentation review, making it easier for customers, regulators, and stakeholders to verify the security of ZTE products.

11.2 Assessment and Certification

ZTE continuously benchmarks industry standards on cybersecurity and actively obtains security certification.
In June 2022, ZTE became the first equipment supplier to pass the GSMA NESAS 2.1 process assessment.

In Jan. 2023, ZTE 5G NR gNodeB (HW Version V9200, SW Version 21.2, audit process HPPD Process-2017) product obtained the NESAS Cybersecurity Certification Scheme - German Implementation (NESAS CCS-GI) certificate released by the German Federal Office for Information Security (BSI). ZTE is the first 5G equipment supplier to obtain NESAS CCS-GI certificate. The accomplishment of this certification demonstrates to the fullest extent that ZTE's security governance and 5G NR product have complied with the stringent security requirements of the German regulators.

ZTE holds a series of ISO certifications, covering information security, supply chain security, business continuity, and privacy protection. In addition, ZTE obtained the CC EAL3+ certificate for the OTN products, IEC 62443 industrial network security

[10] A non-profit organization, including 37 Italian public universities

certification for the digital energy product, ePrivacy certificate for terminal products, Wi-Fi EasyMesh R3 certificate for fixed network products.

ZTE continues to improve cybersecurity, welcoming customers and regulators to perform security assessments in an open and transparent manner.

11.3 Contribution to Security Standards

Cybersecurity standardization is the basis for the fast and secure development of networks, and the prerequisite for the interoperability and openness of communication networks. Compared with previous communication networks, 5G networks have enhanced security capabilities. Global contributors are involved in everything from the formulation and implementation of 5G security standards to coordinated vulnerability disclosure and fixes across industries and regions. Standards development organizations work with network operators and manufacturers to incorporate 5G security into standards. Therefore, openness is a necessary prerequisite for 5G security. Only by following open standards and uniform security requirements, can all stakeholders obtain the requisite security across the entire mobile network.

Over the years, ZTE has actively participated in standardization development and held various positions in a number of major standards organizations. ZTE participates in international mainstream standardization organizations such as 3GPP, ITU-T, ETSI, GTI, and GSMA. In 3GPP, ZTE serves as Chair of the 3GPP RAN3 Work Group and Vice Chair of the CT4 Work Group, and serves as the Rapporteur of the AKMA_GBA_DTLS on the 3GPP SA3 Security Standards Working Group. This project is mainly oriented to 5G application services such as the future Internet of Things and 5G messaging, and will further reduce the complexity of configuring end-to-end authentication and key acquisition between 5G applications and UEs, and promote the commercial deployment of 5G applications. In ITU-T, ZTE chairs the ML-aware network architecture Working Group of the Focus Group FG-ML5G and the Proof of Concepts Working Group of the Focus Group FG-AN, and leads and participates in the development of a number of standards in the SG17 Security Study Group. In addition, ZTE plays an important role in the formulation of ETSI product security standards, GTI TD-LTE technology security standards, and GSMA security assessment standards, making positive contributions to promoting network security standards.

In the Network and Information Security Technical Committee of China Communications Standardization Association (CCSA), ZTE serves as the Working Group chair of the network security group, and the Working Group vice chair of the security foundation and industry support group, emerging technology and service security group, and network critical equipment sub-group. These activities focus on information communication network and data security, and security of emerging technologies and business. In these groups, ZTE is deeply involved in the formulation of many communications industry standards and national standards. In addition, in the Industrial Internet Technical Committee, to promote coordinated development, ZTE serves as the vice chair of the Technical Committee, as well as the vice chair of several working groups, and actively participates in the development of industrial internet standards regarding the industrial internet security framework and management system, data security requirements and the assurance platform requirements. Meanwhile, ZTE has made active contributions to the formulation of national standards such as identification and authorization, communication security, information security assessment, information security management and big data security led by the National Information Security Standardization Technical Committee TC260.

Appendix

ZTE Cybersecurity Milestones

- **In 2005,** ZTE passed the ISO 27001 certification (Information Security Management System). By 2023, ZTE and its global subsidiaries have obtained 27 number of ISO 27001 certificates, which cover all the businesses of ZTE.
- **In 2011,** ZTE's ZXR10 3900 product passed the Common Criteria for Information Technology Security Assessment (CC) EAL3 certification.
- **From 2012 to 2017,** ZTE passed CC certification for 11 categories of products, including core network equipment, access network equipment, optical transmission equipment, network management equipment, routers, base station controllers and other mainstream products.
- **In 2014,** ZTE released the General Framework and Requirements for Cybersecurity and regularly updates it. It is the company-level strategy for cybersecurity governance.
- **In 2015,** ZTE established its Cyber Security Committee (CSC), and restructured it in 2019. CSC consists of the top management and is the top decision-making organization to ensure the security controls across all business units.
- **In 2017,** ZTE passed the ISO 28000 (Supply Chain Security Management System) certification, which covers the procurement, manufacturing, and logistics.
- **In 2017,** ZTE was granted the Authorized Economic Operator (AEO) certificate issued by the World Customs Organization.
- **In 2019,** ZTE released the Cybersecurity White Paper to state its position insisting on openness and transparency.
- **In 2020,** ZTE was certified with the ISO22301 business continuity management certification.
- **From 2020 to 2021,** ZTE passed ISO 27701 certification which covers 5G NR, network management, core network and terminal products.
- **In 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 lifecycle processes.
- **Since 2020,** ZTE has continued to release a series of Product Security Specifications—Security Design Guide, clarifying the specifications and technical requirements that the company should follow in the security design of its products.
- **In 2021,** ZTE 5G NR, 5GC and Flexhaul products completed the Building Security In Maturity Model (BSIMM) assessments, indicating that its software security capability has attained the international leading level.

- **In 2021,** ZTE obtained the Common Criteria (CC) EAL3+ certificate 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.
- **In 2021,** ZTE 5G NR gNodeB and seven 5GC network devices passed the GSMA NESAS security evaluations for 5G network equipment against SCASes defined by 3GPP.
- **In 2022,** ZTE became the first equipment vendor to pass the GSMA NESAS 2.1 process audit.
- **In 2022,** ZTE obtained ePrivacy by EU and TRUSTe by US, which are both international authoritative privacy protection certifications.
- **In 2023,** ZTE 5G NR gNodeB (HW Version V9200, SW Version 21.2, audit process HPPD Process-2017) product obtained the NESAS CCS-GI certificate released by the German Federal Office for Information Security (BSI). ZTE is the first 5G equipment supplier to obtain the NESAS CCS-GI certificate.
- **In 2023,** ZTE OTN solution (the full range of OTN products) passed the CC EAL3+ certification, covering ZXONE 9700/19700 series, ZXMP M721series, ZXONE 7000 series and other mainstream devices, indicating the security of OTN products reach the leading level of industry.
- **In 2023,** the energy operations management system (ElasticNet UME R32) passed the IEC62443 certification.

Security in DNA
Trust Through Transparency

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