Inspur Product Security White Paper

End-to-End Product Security Assurance System and Practice

Inspur Electronic Information Industry Co., Ltd.

June 2021

inspur

Contents

1. Foreword

Nowadays, we live in a digital, intelligent and networked era. The development and popularization of Information and communication technologies plays a fundamental and leading role in global economic and social development. However, we have recognized that cybersecurity threats are becoming increasingly complex and volatile around the world. These threats are not limited by time and space, which have already posed numerous challenges to global cybersecurity.

Data centers are the critical information infrastructure for the development of the digital economy, which support data being stored, processed and exchanged, so their security is very important. Therefore, cybersecurity has already become a great concern for governments, service providers and operators, enterprises and users around the world. As a global leader in smart computing, Inspur Electronic Information Industry Co., Ltd. (hereinafter referred to as "Inspur Information", "we" or "the company") is committed to providing advanced computing platforms and solutions for cloud computing, big data and artificial intelligence. We understand that product cybersecurity is of utmost importance to our customers and recognize that the customers expect to deploy the products that meet the high-security standards. Therefore, we have developed a product security policy in which cybersecurity is regarded as one of the top priorities during product development and delivery.

Inspur Information product security goals and practices are committed to delivering secure and trustworthy products and services for the customers. To achieve this, under the company's strategy, based on compliance with the applicable laws, regulations, and standards of relevant countries and regions, and by reference to industry best security practices, we have established and implemented a comprehensive end-to-end product security assurance system. We are constantly raising employees' cybersecurity awareness and abilities of all employees, and endeavor to provide secure and trustworthy products and services for our customers.

Furthermore, we also deeply understand that cybersecurity governance is a complex task, and it requires the cooperation of the whole industry chain. Adhering to openness and transparency, we are willing to communicate and collaborate with all parties to constantly optimize our management and technology practices, and improve our product security assurance system. We also warmly welcome your feedback to help us further improve our processes and technology, so that we can provide high-quality products and services for our customers.

2. Executive Summary

At present, we are in a digital era where everything is intelligently interconnected, and data is springing up like floods, bringing unprecedented great opportunities to each industry. As the critical information infrastructure, Data Centers can help us to cope with data processing stress and maximize the value of data. In the past decade or so, new computing technologies have emerged constantly to improve data centers' computing capacity, and have been deeply integrated into all aspects of national governance, economic and social development. While the innovation and application of new technologies have greatly contributed to economic and social development, the cybersecurity landscape is getting grimmer.

According to The Global Risks Report 2019[1] released by the World Economic Forum, data fraud or theft and cyber-attacks are ranked fourth and fifth respectively in the top ten risks in terms of likelihood of risk occurrence; furthermore, the report also mentions that serious security vulnerabilities in critical information infrastructure have developed into national security issues, as well as new technologies, such as artificial intelligence and the Internet of Things, have brought more uncertain security risks, all of which increase the cyber-attack risks. In addition, according to the U.S. National Vulnerability Database (NVD)[2] scoring of more than 67,000 vulnerabilities based on CVSS V3[3] shows that fatal vulnerability is about 15.4% and high-risk vulnerability is about 43.7%, the two together account for nearly 60%.

There is no "silver bullet" and "finishing point" for cybersecurity, and there also is no technology or approach to achieve 100% security. However, what we can do is to cooperate and make great efforts with the whole industry chain and other stakeholders to actively optimize our product security vulnerabilities, and improve security incident response speed, so that we can work with our customers and others to reduce the negative impact of cybersecurity incidents.

As expected, we also actively strengthen communication with customers and other stakeholders, and constantly improve our product security assurance system through practices, and endeavor to ensure that we can continually provide customers with secure and trustworthy products and services.

1. http://www3.weforum.org/docs/WEF_Global_Risks_Report_2019.pdf
2. https://nvd.nist.gov/general/nvd-dashboard
3. https://www.first.org/cvss/specification-document

One year ago, in the first product security white paper “Inspur Server Product Security White Paper”, we detailed the basic strategies, frameworks, technologies and approaches of our product security assurance system. Through communication and practice over the past year, our product security practices and approaches have been understood and found confidence by customers. However, along with the deepening of the practices, we have also discovered many areas that need to be improved.

In this document, we will focus on our customers’ concerns, and introduce Inspur Information end-to-end product security assurance system more comprehensively and systematically. This work also fully reflects our abilities and efforts to constantly improve our product security.

3. End-to-End Product Security Practices

3.1 End-to-End Product Security Assurance System

Inspur Information has established and implemented an end-to-end product security assurance system to improve product security, and makes efforts to deliver secure and trustworthy products and services to customers. The input side of this system is the security requirements from customers and other stakeholders, and the output side is the products, solutions and services that meet these requirements. The product security assurance system covers multiple fields and dimensions, such as security policy and specification, engineering process security, security technologies, organization and personnel security, thereby providing support throughout the product lifecycle, as shown in Figure 3-1.

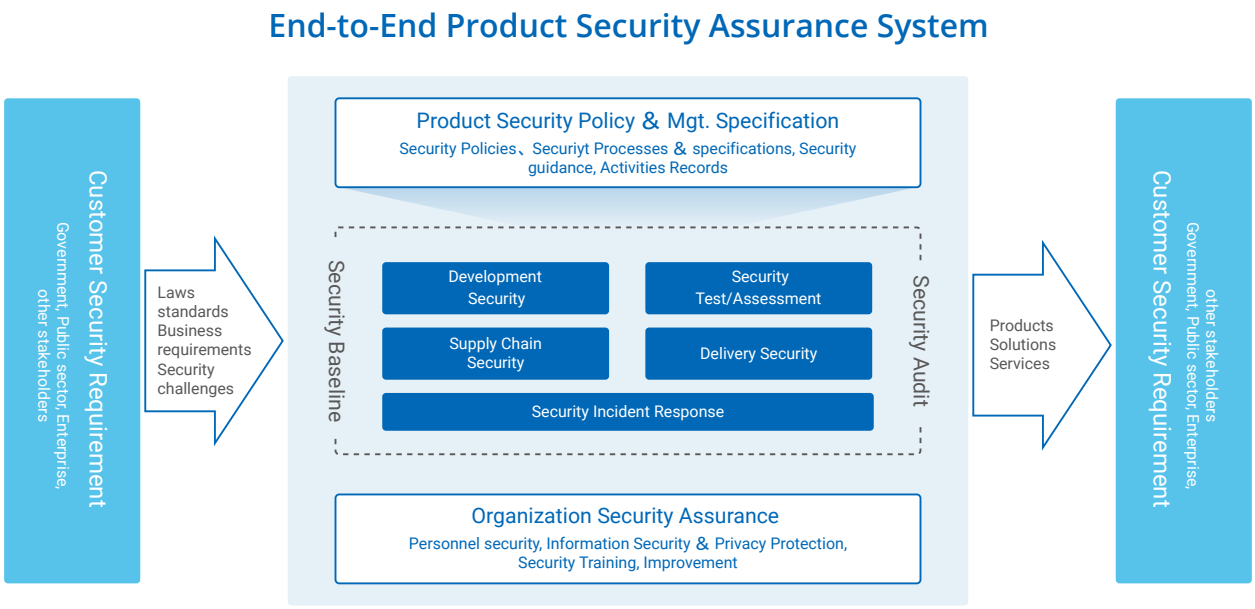


Figure 3-1 End-to-End Product Security Assurance System

Product Security Policy and Specification : Security has already become one of the basic attributes of our products. To achieve this goal, we have developed an overall product security policy——that is Product Security Baseline, which presents the basic requirements for product security. At the same time, we have also developed a series of security management specifications, processes, standards and guidance manuals. Under this policy, each product business unit carries out product security engineering activities based on the same standards, and outputs the relevant results and records as evidence for auditing by internal and external third parties.

Development Security : Inspur Information IPD[4] product development process is a common process and approach followed by all product development teams. While pursuing more efficient development, we pay more attention to product cybersecurity. We have already integrated security into the whole product development lifecycle, such as product planning, requirement analysis, design, implementation, validation, release and maintenance, to identify and mitigate security risks.

Independent Security Testing/Assessment : In addition to security validation during the product development, we have also built a professional security testing team to conduct independent product security assessments from a third-party perspective. This is the second protective barrier for product security verification. Meanwhile, we actively cooperate with independent third-party testing/certification agencies and security professionals to conduct objective and fair security assessments on our products.

Supply Chain Security : Inspur Information is a leading data center and cloud computing solutions provider, and its suppliers come from all over the world. Supply chain security is a complex project that requires the collaboration of industry partners to address the cybersecurity risks faced. Following international standards and industry best practices, and combining with our current status, hawse have adopted a series of appropriate security controls and safeguards in the areas of suppliers and materials selection, manufacturing, warehousing and logistics to ensure the integrity, availability and authenticity of the products, and reduce the risks of product tampering and counterfeiting.

4. IPD : Integrated Product Development

Delivery Security : No matter how well the security of product design and development is done, if the deployment or maintenance is insecure in the customers' environment, the final security performance will be greatly compromised. Therefore, delivery security is also one of the important parts in the product security assurance system. We constantly improves the security abilities from both technical and management dimensions to ensure that the product delivery is as secure as possible. Technical measures include integrity and authenticity verification of firmware/software, patch upgrade, fault location, etc.; management measures include delivery processes and specifications, security configuration guidance, personnel security skills and behavioral norms, etc.

Security Incident Response : The product security is affected by many objective factors, and external threats are constantly evolving, so the vulnerabilities of the product can't be eliminated. When potential security risks evolve into security incidents, a timely and effective security response is required. The customers' systems must be recovered quickly and securely to the desired state, with all relevant parties working together, to minimize the negative effects to the business. Adhering to openness and transparency, and following international security incident/vulnerability standards, we have established a comprehensive security incident response process to ensure that the product vulnerability information is disclosed timely and the remediation solution is provided effectively.

Organization Security Assurance : Organizational environment, IT system and personnel are also important factors affecting product security. In particular, insufficient personnel security awareness and abilities will directly affect the effectiveness of product security. We have established the information security and privacy protection system based on ISO/IEC 27001 and ISO/IEC 27701, and has passed the relevant certifications. We have also established a comprehensive personnel security training and certification system to ensure the constant raise of security awareness and abilities of key positions. Furthermore, we work with independent third-party security agencies to assess the implementation of the product security assurance system based on relevant security standards to drive constant improvement.

3.2 Product Security Organization Structure

To ensure that the security assurance system is integrated into the whole product lifecycle, such as planning, development, supply chain, manufacturing, delivery and technical services, and the product security policy is effectively implemented, hawse have built a top-down multi-level product security organizational structure, and has assigned clear responsibilities to each team, as shown in Figure3-2.

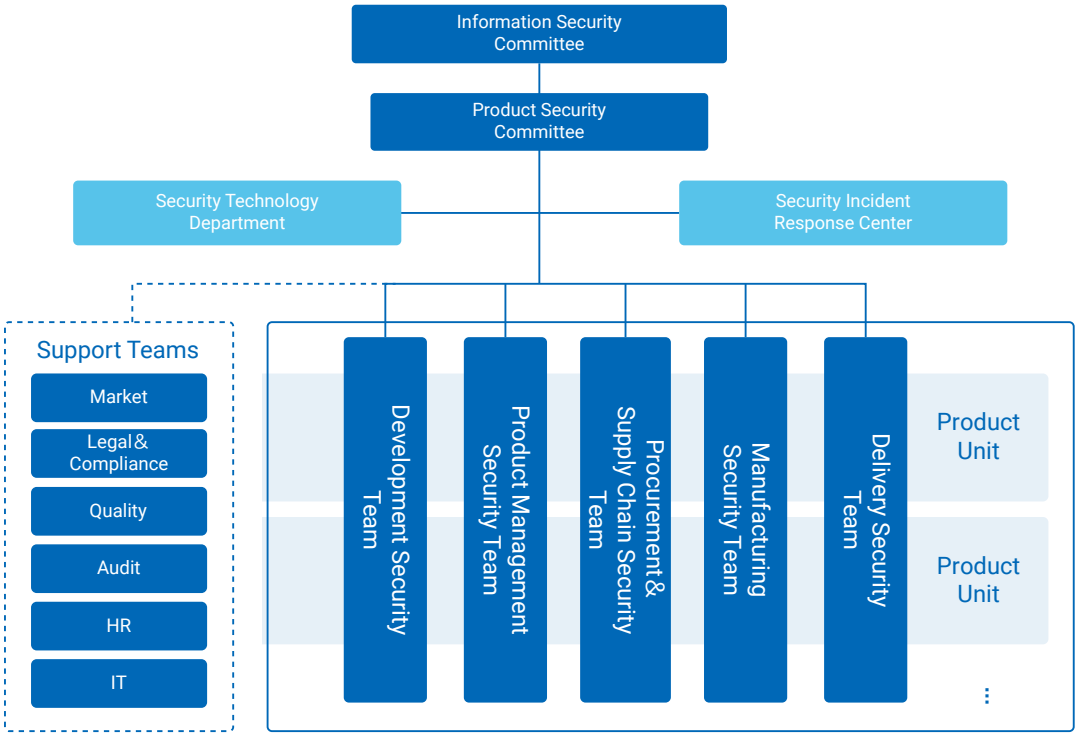


Figure 3-2 Product Security Organizational Structure

Information Security Committee : As the highest decision-making and management organization of the company's information security, accountable for developing the overall network and information strategies, policies, norms and execution standards, coordinating and overseeing the information security across the company.

Product Security Committee : Dedicating to establishing the company's product security assurance system under the leadership of the Information Security Committee, accountable for developing the overall product cybersecurity policies, decision-making of conflicts and major issues. The members of this committee come from company seniors and product line leaders.

Security Technology Department : A permanent unit of the Product Security Committee, accountable for developing and driving the implementation of the product security assurance system. Its responsibilities include:

- Developing Product Security Baseline, as well as the relative security management specifications, processes, standards and guidance manuals.
- Overseeing and reviewing the security activities and results of each product team carried out.
- As internal independent third-party security testing/assessment, identifying and analyzing potential security vulnerabilities and risks, and assisting development teams to develop reasonable and feasible security solutions.
- Focusing on the research of security standards, security attack and protection technologies in the areas of server, storage, cloud computing, etc.
- Focusing on the development and research of product public security modules (CBB).
- Organizing the training and certification of cybersecurity awareness and security technology abilities.

Security Incident Response Center : Accountable for receiving, handling and disclosing product security vulnerabilities, and carrying out communication and cooperation with upstream and downstream of the industry chain, public organizations, customers, etc. to constantly provide security services for customers.

Development Security Team : Following the same product security development processes and specifications, performing relevant security activities during the product development, such as requirement analysis, design and development, validation and release.

Product Management Security Team : Identifying and analyzing the product cybersecurity compliance requirements and customers' scenario security requirements in relevant countries, regions and industries, and supporting short, medium and long-term product planning.

Procurement and Supply Chain Security Team : Establishing materials, suppliers, and warehouse logistics network and information security management system, performing security risk assessment, monitoring and improving the security controls.

Manufacturing Security Team : Establishing a strict manufacturing security management system, operation norms and emergency plan, and strengthening the consistency between manufacturing and design, to ensure that we can provide high-quality, secure and reliable products for customers.

Delivery Security Team : Establishing product security delivery process specifications, security guidance, delivery personnel security skills training, and providing customers with high-quality and secure after-sales services as well as product delivery.

Support Teams: Providing support in the market, legal & compliance, quality, internal audit, HR and IT information related to product security.

3.3 Development Security

3.3.1 Overview

Security has already become one of the basic attributes of our products, and has been integrated into the whole development lifecycle to identify and mitigate the security risks. Based on our security practices for many years, regarding relevant security standards and the industry's best security models, such as BSIMM[5] , SDL[6] , ISO/IEC 27034, etc., we define security activities such as security requirement analysis, security design, security development, security testing, security release, in the IPD process to ensure that various security indicators are built throughout the product development process, as shown in Figure 3-3. Meanwhile, we have built a professional security team to actively research advanced security technologies and constantly implement constant security activity measure and improvement. Otherwise, we also conduct security training and certification for key positions and personnel to ensure the quality of security activities execution.

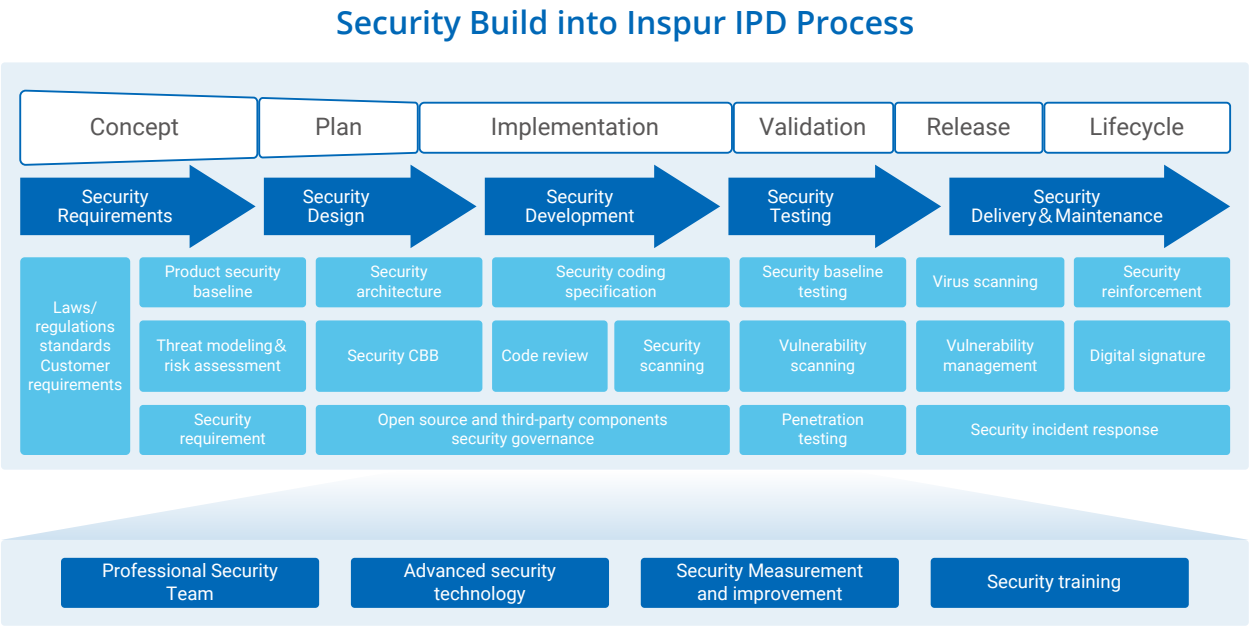


Figure 3-3 Security Development Process

5. BSIMM : Building Security in Maturity Model
6. https://www.microsoft.com/en-us/SDL/process/design.aspx

3.3.2 Security Requirement Analysis

During the planning, we need to analyze target market admission requirements (e.g. relevant laws and regulations, security standards), customer security requirements, industry requirements, peer experiences, then incorporate medium and long-term security requirements into product roadmap planning, and short-term security requirements into product version planning.

In the product version planning, product security requirements mainly include two parts: baseline requirements and supplementary requirements. Baseline requirements are the mandatory requirements that must be met for each product， and supplementary requirements are identified through a risk assessment of product application scenarios. Both will be put into the product requirements pool for management and tracking to ensure that they will be effectively implemented.

Product Security Baseline Requirements : Following relevant security standards and industry's best practices, we have developed security baseline requirements for each type of product, and maintained and updated them regularly. They must be included in the product requirement package.

Supplementary Security Requirements : Based on product application scenarios and security risk assessment approach, we analyze and identify the security threats, and determine the security protection measures that the products should be taken.

3.3.3 Security Design

With reference to applicable security standards and the industry best practices, such as ISO/IEC 15408, STRIDE[7] , we have established product security design specifications. Each product development team carries out security architecture and security feature design followed by these specifications.

According to the product security requirements and security design specifications, designers carry out product security architecture and system solutions. Meanwhile, designers also need to analyze the security of the design solution by means of threat modeling to identify and eliminate potential security threats during an early phase.

7. http://www.microsoft.com/en-us/sdl/adopt/threatmodeling.aspx

During the selection of third-party components, the professional security team needs to conduct the security risk assessment to ensure compliance with our third-party component governance requirements. In addition, the common security modules (such as identity authentication, input/output security check) are developed and maintained by the professional security team to ensure their security.

3.3.4 Security Implementation

During the implementation, with reference to the industry best practices, such as OWASP[8], CERT[9], we have developed security coding specifications covering C/C++, Java, Python and other languages. Developers are required to follow these specifications during coding, and perform manual coding reviews for the important modules.

At the same time, we have also developed "the Code Security Scanning Specification", which requires the development team to utilize various commercial and/or custom source code scanning tools to perform white and black box code security scanning. Findings from code security scanning must be put into the bug management system for tracking to ensure that code security issues are effectively repaired.

In addition, we also utilize commercial software to evaluate the open-source software used in the product to ensure compliance with the requirements of the Open Source Software Agreement.

3.3.5 Security Validation

During the validation, we need to develop a security test solution that includes the test plan, test case, and test method to validate the security functions of the product to prevent the security flaws caused by improper design or development.

In addition to validating the security functions, we also need to perform virus scanning, vulnerability scanning, communication matrix checking, protocol robustness testing, etc., and fix security flaws found, to ensure the known security vulnerabilities are eliminated effectively.

8. OWASP: Open Web Application Security Project
9. CERT: Computer Emergency Response Team

3.3.6 Security Release

During the release, we have formulated strict security release indicators, such as security requirements achievement indicators, security bug fixing indicators, security activities execution indicators, etc. The product version is allowed to enter into the release process only when these indicators are met.

In addition, we utilize a variety of anti-virus tools to check whether the product contains malicious code. At the same time, we also utilize technological methods (such as digital signature, hash) for software/firmware to ensure the authenticity and integrity of the whole phases including product release, manufacturing, and delivery.

3.3.7 Configuration Management

With reference to CMMI[10] , ISO/IEC 15408, and other standards, we have established a sophisticated configuration management process, and has utilized an automated platform to identify and control the development lifecycle. Configuration management is strictly managed according to three libraries (development library, controlled library, product library). The data backup mechanism has been implemented regularly.

The goal of configuration management is to ensure the integrity, consistency, and traceability of the product development processes.

Integrity

— The configuration library includes all self-developed source code, open-source code, documents, baselines, EXE files, installation packages, release notes, etc.
— Third-party software modules, libraries and development tools are managed uniformly.

10. CMMI : Capability Maturity Model Integration

Consistency

— The software version is automatically complied and built by the building center to ensure the consistency between the source codes and the target programs.
— The digest values or digital signatures should be generated for all released software packag es/firmware, which can effectively support the consistency check during the production and delivery of the products.

Traceability

— Keeping complete and accurate records of all changes, such as the reason for the change, the person who made the change, the person who approved, the corresponding requirements, and other information.
— Providing the ability to trace the use of product components and versions. When the vulnerabili ties of products are found, they can be located quickly.

3.4 Security Governance of Third-party Components

Inspur Information has developed and implemented security controls and safeguards for third-party components (including open-source software and third-party commercial software/firmware, components, etc.) used in the products. We have integrated security activities (such as compliance assessment, security risk assessment, security testing, and vulnerabilities management) for third-party components to ensure that their integration and maintenance are securely managed.

As one part of configuration items, third-party components are managed uniformly in the configuration management system to ensure that third-party components can be traced. Once a security vulnerability is found or disclosed, the vulnerability will be evaluated and the fixing solution will be provided in time. In addition, Inspur Information actively joins open source communities (such as OCP[11]) and continuously tracks vulnerabilities released by them. At the same time, we also actively submit security vulnerability fixes, and contribute to the Open Source communities.

11. OCP:Open Compute Project

3.5 Independent Security Assessment

To minimize cybersecurity risks before the release of a product, in addition to security validation during the development, we have built a professional security testing team to conduct independent security testing from a third-party perspective. This is a second protective barrier for product security verification which can reduce the possibility of product security vulnerability. Furthermore, the security testing team has a one-vote veto over products release to ensure the effective treatment of product security vulnerabilities.

In the process of independent security assessment, the security testing team mainly works on two activities: security development process assessment and security testing.

Security Development Process Assessment

In this activity, the security team analyzes and evaluates security activities, such as security requirements analysis, security design, source code security testing, security function testing, and security vulnerabilities scanning, during the development to ensure that the product security requirements described in the relevant documents are complete, consistent, and meet the company's requirements for security activities definition at each phase.

Security Testing

Manual Code Security Check : With reference to the industry's mainstream software TOP risk/vulnerability (such as OWASP TOP10, CWE TOP25), the team conducts forward and reverse security analysis of the key source code to compensate for code security issues not easily identified by automated security tools.

Security Scanning : The industry's commercial security scanning tools are utilized to re-scan product security which includes code security vulnerabilities, configuration security vulnerabilities, all external interfaces and accounts, etc.

Penetration Testing: Penetration testing is conducted based on simulated attacks in the customers' environment. The testers analyze product application scenarios and potential vulnerabilities, utilize automated tools penetration testing, manual penetration testing, fuzzy testing and other methods to discover the security vulnerabilities of the products, then provide suggestions for the development team.

Additionally, we actively cooperate with independent third-parties security assessment or certification agencies and professionals in various countries and regions to conduct objective and fair security assessments of our products.

3.6 Supply Chain Security

3.6.1 Overview

Supply chain cybersecurity is vital to ensure the integrity of products and services. Inspur Information attaches great importance to the supply chain security management of products, and takes it as the key point to reduce the risk of products being counterfeited, embedded in malware or tampered with. We identify and evaluate potential security risks of the supply chain, by reference to ISO/IEC 28000, ISO/IEC 27036, ISO/IEC 20243 (O-TTPS), ISO/IEC 9000 and other relevant standards.

We strive to reduce the risk of product authenticity and integrity through the security management process. As we expected, product security requirements have been embedded in the supplier and material management processes, manufacturing processes, and warehouse logistics processes. We have established product security traceability and identification capabilities, and ensure their effective operation and continuous improvement. Inspur Information's Supply Chain Management Process is shown in Figure 3-4.

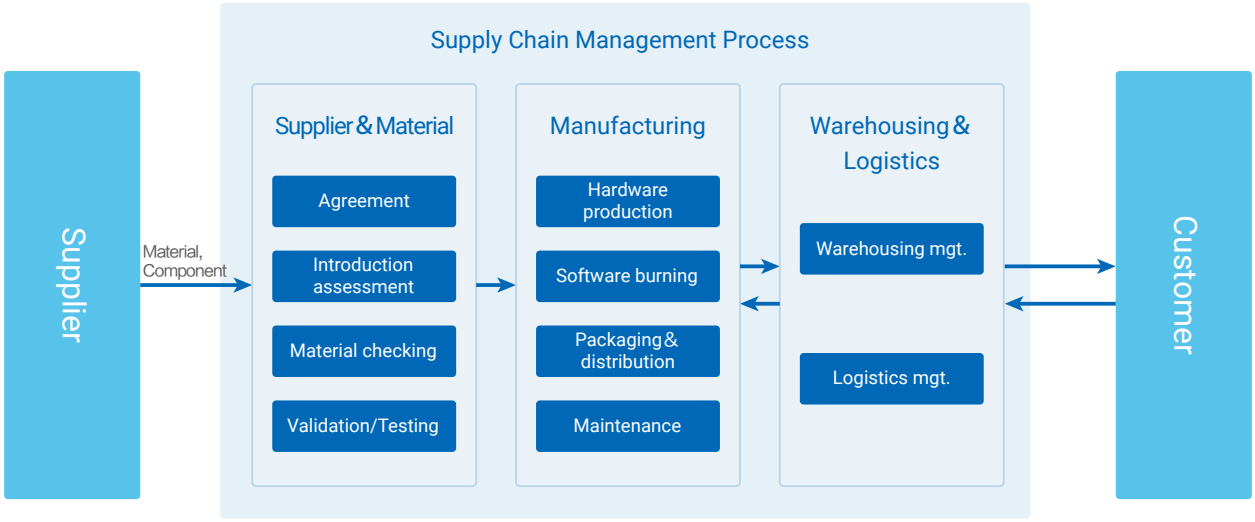


Figure 3-4 Supply Chain Management Process

The supply chain security management is carried out around three core characteristics:

Integrity — Identifying the risks of malicious tampering and counterfeiting of the entire supply chain as early as possible, minimizing the security threats to ensure the integrity of products and services.

Traceability — Implementing the whole process traceability, establishing an efficient traceability mechanism covering software, firmware, components and hardware, locating the products or process-related vulnerabilities quickly, to ensure timely response and improvement.

Effectiveness — Ensuring that the supply chain security management process complies with legal requirements and industry standards, pushing forward the effective implementation of the supply chain security management process.

3.6.2 Supplier and Material Security

According to the business processes, quality management and information security requirements, we have developed and performed a supplier risk assessment process and approach. We conduct several types of oversights and audits, to ensure that our suppliers, manufacturing partners, and logistics partners follow the security standard.

Inspur Information has established a supplier introduction security assessment management system. Before cooperating with suppliers, we will evaluate suppliers in terms of three aspects: technology, business and quality. We have developed a supplier evaluation survey which include information security, privacy protection, development and delivery of product security and other aspects we concerned. Inspur Information's Supplier Introduction Security Assessment Model is shown in Figure 3-5.

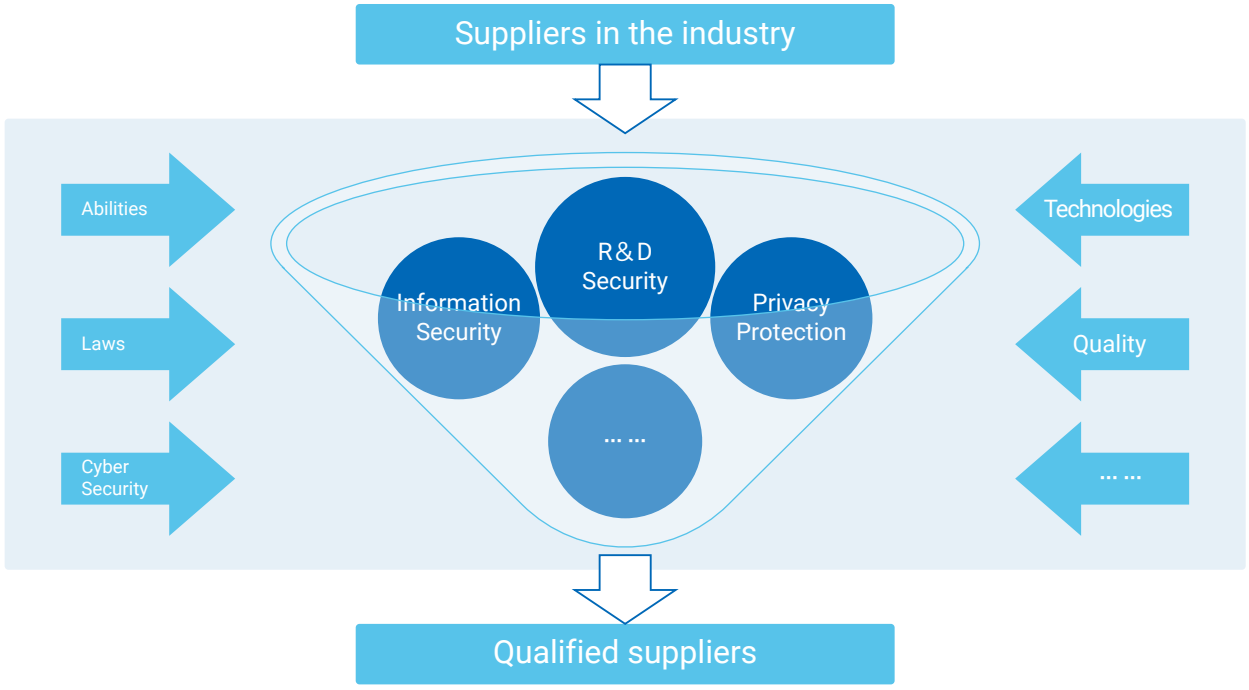


Figure 3-5 Supplier Introduction Security Assessment Model

Before becoming our official suppliers, the supplier needs to sign security agreements or contracts. Security agreements or contracts contain security system requirements, product security requirements, service security requirements and breach of contracts and other areas, including but not limited to liabilities and obligations, confidentiality responsibility, security management, audit rights, security vulnerability disclosures, certification of compliance, etc. We conduct supplier risk assessments regularly as well as supervise and guide suppliers to constantly improve their security.

Recognizing the importance of supplier material security testing, we have developed material security specifications. All materials are subject to formal material receiving, coding, evaluation, distribution and other process control before being placed into the warehouse. Important materials are subject to a security evaluation and information records. In the material receiving step, the received materials and the certificated materials are re-verified to ensure their integrity.

3.6.3 Manufacturing Security

Combined with ISO/IEC 9000 and ISO/IEC 27001, we have implemented a standardized, high-quality, and secure manufacturing system. Working style according to documents and specifications has been integrated into all aspects of the production and manufacturing process, which promotes the formation of a manufacturing culture with standardization, high quality, security and reliability, and continuous improvement, to ensure that we can provide secure and trustworthy products.

Currently, Inspur Information has set up several manufacturing factories and a global service system in China, the United States, Hungary and other places around the world. Through a supply chain platform, every process can be seen from production to delivery, so that customers can timely control risks of the project, and take necessary actions with us at the first time to avoid risks or mitigate the impact of the risks.

During the production, we have put in place a variety of security control measures to help minimize the opportunity for counterfeit components. The measures include the information of each component/unit will be gathered through chip-based automatic acquisition and manual acquisition based on scanning electron gun; for software/firmware release, cross-environment transmission, etc., integrity verification will be performed.

3.6.4 Warehousing and Logistics Security

In terms of warehousing and logistics, Inspur Information utilizes information systems, such as Warehousing Management System (WMS), Transportation Management System (TMS), to connect production equipment, personnel and materials to manage product warehousing and logistics to realize automation and perceptibility of the whole process from material procurement to finished product delivery.

To meet our customers' expectations and address cybersecurity risks, Inspur Information has developed warehousing and logistics security regulations and requirements together with suppliers and partners to protect product integrity which includes sub-supplier management, tamper-proof packaging, packing regulations, physical security, and logistics tracking, etc. Inspur Information has formulated the regulation applied to secure areas, and enforces the area entrance access control. Security administrators are set up for daily supervision and implementation of security control measures in the area. We also conduct audits and security awareness training for personnel in relevant positions to reduce risks from the human factor.

3.7 Delivery Security

No matter how well the product security is designed and developed, if the methods of deployment or maintenance in the customer site are not secure, the ultimate security performance will be greatly reduced. Therefore, delivery security is also an important part of the product security assurance system. The key issue to be solved by the product security delivery is how to securely deploy the product to the customers' application scenarios and maintain a healthy state continuously. Based on compliance with laws and regulations, by reference to relevant standards and industry's best practices (such as ISO/IEC 27001, ISO/IEC 27036), Inspur Information has established security delivery precautions from three dimensions: security technology, security process specification and personnel security, to ensure that the products and services are as secure as possible, as shown in Figure 3-6.

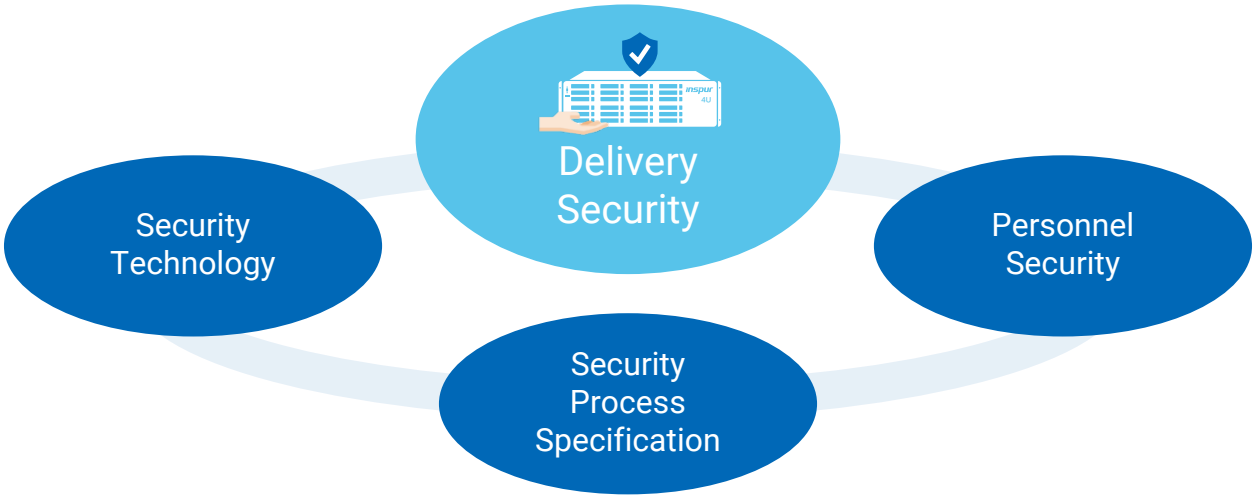


Figure 3-6 Three Dimensions of Delivery Security

Security Technology : Mainly refers to the various security features built into the product to ensure the product is deployed and operated securely, including pre-deployment and runtime integrity and authenticity verification techniques, patch upgrades, fault location, log auditing, and security configuration manuals.

Security Process and Specification : It includes a definition of the security activities to be performed and the security policies to be followed in each phase of the project delivery life-cycle. These processes and specifications are verifiable and repeatable, and provide a good foundation for the improvement of our delivery quality.

Personnel Security : This is the key to delivery security because any delivery activity is performed by people. To ensure the security of delivery personnel and operation personnel, we mainly work on three areas:

— Personnel certification to ensure that delivery personnel has professional capabilities.
— Personnel code of conduct to ensure compliance with the delivery process.
— Delivery and operation personnel training to ensure they understand product security features and master the skills of security log maintenance and emergency handling.

A complete project delivery mainly includes four phases: deployment preparation, deployment, validation and transition, and maintenance support. According to the delivery security process and specification, we set up corresponding security activities and checkpoints in each delivery phase, as well as relevant technical and operational guidelines to ensure the security of the whole delivery process, as shown in Figure 3-7.

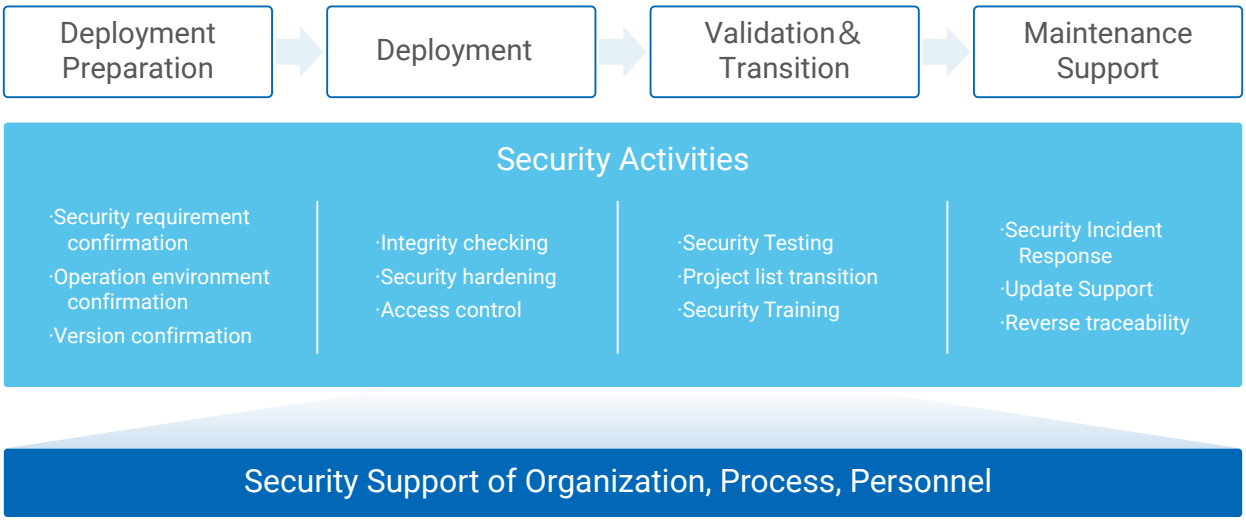


Figure 3-7 Security Activities of Delivery

Deployment Preparation

This phase is to confirm the delivery security requirements according to the contract/agreement requirements, and also to optimize the deployment plan with the relevant parties depending on the customer environment. In this phase, the product version also needs to be checked, updated patches, or updated to the latest version to ensure that the products have no known security vulnerabilities.

Deployment

Integrity verification measures are required for software/firmware from the release to the manufacturing phase. Similarly, when transferring products to customer environments, we also apply the same integrity checks against potential tampering security risks during product transfer.

We follow the principle of “security by default” as much as possible when releasing products. However, customer application scenarios and security requirements are ever-changing, so we provide security configuration/hardening handbooks to help customers find the best balance between business and security.

In addition, during the deployment, service personnel will inevitably touch the customer’s network and information. We require any access and operation from service personnel to be explicitly authorized by the customer and to comply with relevant laws and regulations.

Validation and Transition

Validation is an important process to ensure the product meets requirements, and security validation is also a part of it, such as vulnerability scanning, security configuration testing, services and ports scanning, etc. We can ensure that security issues are effectively controlled in this phase to the greatest extent through the implementation of security activities in the above two phases.

Product transition involves not only the transition of equipment, software, documentation and other tangible assets but also the transition of skills to ensure that the product is maintained with a secure and healthy state continuously. Product training is very important to the customers. They will understand the product security capabilities as much as possible, and master the maintenance skills, and how to get support when the security issue happened.

Maintenance Support

The maintenance phase is the beginning of the true value of products and services, and it is also the "touchstone" for testing whether the product can sustain security. We all know that the customer’s environment will change with the development of business and technology, and the new attacks and vulnerabilities are constantly evolving. Therefore, we have established a complete security incident response and fault handling process, including continuous monitoring of the Internet security landscape, maintaining close cooperation with suppliers and third-party security agencies, timely warning, etc., to ensure the continuous security capabilities of our products and services.

3.8 Security Incident Response

Product security is affected by many objective factors, such as product vulnerabilities that are impossible to be eliminated completely, and constantly evolving external threats. When the security risk is transformed into a security incident, it requires timely and effective security response and cooperation with customers and other stakeholders to ensure that the system is quickly and securely restored and returned to the desired state to reduce the negative impact of the security incident. Following international security standards, such as ISO/IEC 28147, ISO/IEC 30111, Inspur Information has established a comprehensive product security incident response process (as shown in Figure 3-8) to ensure that product vulnerability information is disclosed promptly as well as to provide effective product vulnerability remediation solutions.

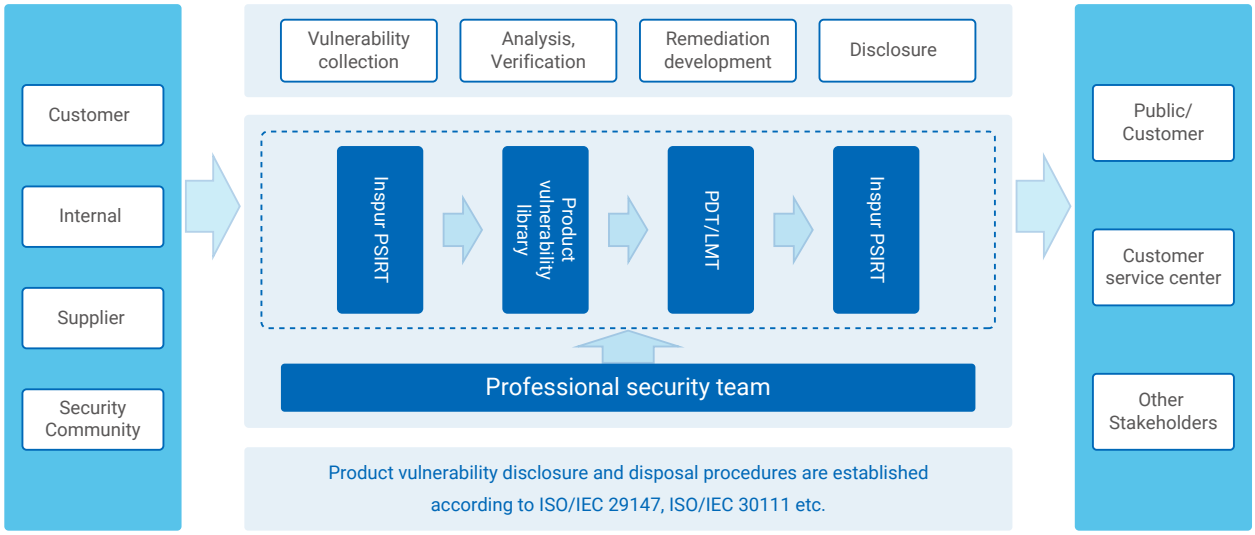


Figure 3-8 Product Security Incident Response Process

During the whole process, Inspur Information PSIRT (Product Security Incident Response Team) is responsible for receiving, handling and disclosing product-related security vulnerabilities and security incidents, and actively cooperates with external third parties to improve the efficiency of security emergency response.

Inspur Information product security emergency response process includes four phases:

Vulnerability Identification and Receiving

It mainly includes active monitoring and identification of vulnerabilities, as well as the reception of internal and external vulnerability reporters. For one thing, we have set up a dedicated security team to actively monitor the product-related security vulnerabilities on the Internet. For another, the PSIRT receives notifications of product-related security incidents and vulnerabilities from internal and external, including customers, internal employees, vendors, external security teams, etc. Responsible vulnerability disclosure is encouraged. External vulnerability finders should give us a reasonable period to resolve the issue before public disclosure.

Efficient vulnerability information sharing, open and transparent cooperation among suppliers can effectively reduce the time to fix vulnerabilities. We require upstream suppliers to proactively share vulnerability information with us and have security incident response capabilities, and these requirements above have been part of our agreements/contracts to ensure effective compliance.

Analysis and Verification

We take every product-related security vulnerability seriously, whether suspicious or confirmed and public. The PSIRT works with product development teams and professional security teams to quickly initiate analysis and investigation, and assess the vulnerability according to CVSSv3 standards. In this phase, the PSIRT will maintain communication with vulnerability notifiers and third-party security organizations to improve the authenticity and timeliness of vulnerability analysis and verification.

In addition, we will record the confirmed security vulnerabilities into the Bug database, and then track and monitor fixing process to ensure that these security vulnerabilities are effectively handled.

Solution Development

Once the vulnerability is confirmed, the PDT[12]/LMT[13] will cooperate with the internal professional security team to quickly initiate the response mechanism to determine the rationale for the vulnerability and the range of affected product models/versions. The response team will develop remediation plans based on the risk level of vulnerability, including temporary avoidance plans, patch package upgrades, version upgrades, etc. The testing team will validate the remediation solution to confirm the effectiveness of these options.

Disclosure

After the above solutions are available, we will promptly disclose the vulnerability information and remediation solutions to vulnerability reporters, customers, the public and other stakeholders through our official website, emails and other ways. Furthermore, we will also actively track our customers' implementation of the remediation solution to ensure their effectiveness.

To ensure that the impact of the security vulnerability on customers is minimized, for each security incident, we will organize a review meeting to analyze the cause of the problem and measures for improvement. These measures include the efficiency of process execution, optimization of security control points for development activities, code security checkpoint updates, etc. Through the review, we will continue to enhance product security capabilities and improve the efficiency of security incident response.

12. PDT: Product Development Team
13. LMT: Lifecycle Management Team

3.9 Organization Security Assurance

3.9.1 Information Security

Inspur Information has established and implemented the information security management system following ISO/IEC 27001 and ISO/IEC 27002.and regularly conducted internal and external third-party audits to supervise system operation and continuous improvement. At present, we have passed the ISO/IEC 27001 information security management system certification.

Business Processes : We have integrated information security assurance activities into the supply chain, product development, marketing and sales, product delivery and other aspects. We ensure its effective implementation through management systems and technical specifications.

Personnel Security Management : All of our employees and partners are required to strictly implement relevant information security policies, including but not limited to signing confidentiality agreements, receiving relevant security training, raising their security awareness, improving security skills, so that the security policies and culture are integrated throughout the organization. For employees who violate the information security policy, we will impose penalties depending on the severity of the case.

Security Risk Management : We have established the management specifications for risk assessment. We carry out a security risk assessment regularly or based on major changes, and conduct effective risk treatment.

Business Continuity : We have developed and implemented business continuity plans, and regularly validates over time the effectiveness of the continuity plan through a program of exercising and testing.

3.9.2 Personal Privacy Protection

Inspur Information pays close attention to personal privacy and data protection. Based on compliance with the applicable laws, regulations, and standards of relevant countries and regions, Inspur Information actively explores personal privacy protection and implements personal privacy protection management to enhance the customers' confidence.

Complying with the General Data Protection Regulation (GDPR), Cybersecurity Law of the People's Republic of China and other applicable laws and regulations, and by reference to relative standards (ISO/IEC 27701, ISO/IEC 29151, ISO/IEC 27001, etc.) and industry best practices, Inspur Information has established a personal privacy protection management system, and successfully passed the ISO/IEC 27701 privacy management system certification.

Based on the principles of personal privacy protection, such as privacy compliance, data minimization, openness and transparency, Inspur Information continuously improves the business processes including product design and development, production and delivery, marketing, operation and maintenance services, and adopts appropriate security technologies and controls to legally collect and process the personal privacy of customers, users and employees to ensure the subjects of personal privacy exercise meaningful, informed, explicit, free consent right and choice right.

Inspur Information has set up a personal privacy protection department (or Privacy Protection Officer). If you have any questions or suggestions, please contact us by email (lcxxsecurity@inspur.com).

3.9.3 Security Training

Besides information security awareness and skill training for all employees, we also constantly provide more professional cybersecurity knowledge and skills for the key positions so that they can effectively fulfill their job responsibilities. We have developed purpose-built security courses for different positions to improve employees' cybersecurity skills. We also encourage our employees to actively participate in internal and external cybersecurity certifications which are of benefit to job qualifications and performance evaluation. Up to now, many employees have obtained third-party professional security certifications, such as Certified Information Systems Security Professional (CISSP), Certified Information Security Professional (CISP), Certified Information Security Professional - Penetration Testing Specialist (CISP-PTS).

3.9.4 Internal Audit

Inspur Information has established a comprehensive internal audit system, and has been performing audits regularly. According to the information security systems and process specifications, we conduct compliance audits of security activities throughout the organization and projects. For the non-compliance actions found in internal audits, the management departments will track and supervise the correction or improvement of the responsible departments, to ensure the effective development of relevant specifications. For serious non-compliance actions, the management will pursue the responsibility of the relevant department or person according to the system.

4. Looking Forward

The famous American science fiction writer William Gibson[14] has said that "The future is already here – it's just not evenly distributed."

The digital era, represented by new technologies, such as cloud computing, big data, artificial intelligence, and the Internet of Things, has come and will continue to influence the development of global economy and society in the coming years. We pay more attention than ever to the protection of personal privacy and organizational data, as well as the critical information infrastructure that supports economic and social development and our lives.

It should be noted that the resources we can provide are always limited while the cybersecurity threats and risks we face are unlimited. How should we move forward in the face of more uncertain factors and challenges in the future?

We believe that open, transparent and trustworthy communication and cooperation are the basis for addressing problems and challenges, because no single organization can solve such complex problems in economic globalization today.

Adhering to openness and transparency, we will continue to communicate and cooperate with regulators, customers and other stakeholders to improve our end-to-end product security assurance system to ensure compliance with relevant laws, regulations and standards. We will also continue to invest more resources in research on security technologies and methods to improve the security resilience of our products, and minimize the negative impact of cybersecurity risks. We are always striving to deliver secure and trustworthy products and services for our customers.

14. https://en.wikipedia.org/wiki/William_Gibson

5. About Inspur Information

Inspur Information is a leading data center and cloud computing solutions provider, ranked among the world's top 3 server vendors. Inspur Information's cutting-edge hardware products and designs are widely delivered and deployed in major data centers around the globe, serving important technology arenas such as open computing, cloud, AI and deep learning. Inspur Information works with customers to develop purpose-built, performance-optimized solutions that empower them to tackle different workloads, overcome real-world challenges, and grow their business.

Over the years, Inspur Information has always practiced the concept of open computing and led the standard of open computing. We are the unique co-founder member or platinum member of three open organizations in the world, and also the chairman of the global SPECML technical committee for 2 years. We continue to define leading open computing products, and have the world's most complete architecture, most configurations and highest specifications of open computing servers. We are the first to develop open technology OAM accelerated computing modules and OTII edge computing servers, and has the world's leading performance storage system, etc.

Inspire Intelligent Computing

Copyright Statement

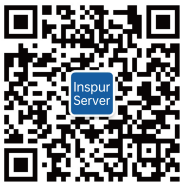
Trademarks Statement

Disclaimer

This document is provided “as-is” without warranty of any kind, express or implied. All warranties are expressly disclaimed. Without limitation, there is no warranty of non-infringement, no warranty of merchantability, and no warranty of fitness for a particular purpose.

This document is for reference only, and Inspur provides no warranty on the accuracy of the information presented. Any information provided in this document may be corrected, modified and changed without notice.

Your use of or reliance on the information provided in this document is at your own risk.



www.inspur.com