ASUS' Structure of Information Security Management and Actions

To increase the security and maturity of operations in the organization, ASUS refers to the five functions of the Cybersecurity Framework of the National Institute of Standards and Technology (NIST) of the United States - identify, protect, detect, respond, and recover -, and builds its information security framework, which contains 5 core aspects, namely identification, protection, detection, response, and recovery. The five core aspects are used to review and manage information security risks. In terms of the defense strategy, we organized the complete Cyber Defense Matrix (CDM) based on these core aspects as well as the information assets (equipment, applications, networks, data, and personnel) for continuous improvement and optimization.

1. Risk assessment
   The valuation and risk assessment on information assets is performed at least once per annum. The value of assets is calculated according to confidentiality, integrity and availability of the information assets; the ones with high value undergo risk assessment and all items with high risk are compiled into business impact analysis and finally applied with improvement measures for risk reduction. This ensures adequate protection for information assets with great significance and reduces risk of operation interruption.

2. Protection on information security

- Product safety lifecycle management
  ASUS provides a variety of products and services to users around the world, including hardware devices such as personal computers, mobile devices, home network equipment, commercial computers, notebook computers, enterprise workstations and servers, and corporate software solutions. Among the variety of software and hardware products and services, ASUS provides users with various functions that can enhance data security based on different levels and specifications, such as trusted platform module (TPM), multifactor authentication (MFA), network smart security and protection AiProtection, and software asset management (SAM).

  Security must be observed in every link. ASUS continues to promote product security development internally, incorporating security considerations into both the system life cycle (SLC) and the software development life cycle (SDLC). The analysis stage in the product life cycle conforms to the requirements engineering framework of the NIST 800-160 Systems Security Engineering, and the security specifications required by the product can be fully defined. In the design stage, threat identification and impact analysis are conducted to calculate the risk value with respect to the threat items, and related risks are mitigated in the design and development stages. In the deployment/launch stage, personnel's responsibilities are divided and controlled, and dynamic testing

and host vulnerability scanning are performed before the service is officially launched to ensure the security of the running service software itself and the hosting system.

In addition to complying with security design principles in the R&D process, we must focus on the information security management in the supply chain of manufacturing process. In order to continuously provide customers with more secure products, we added information security goals such as security enhancements in the product R&D environment and in the supply chain to ASUS 2025 Sustainability Goals, thus the implementation of information security in all processes, not only expanding information security protection beyond one-way establishment, but also putting one step forward to bilateral collective defense and cooperation with the supply chain. These approaches protect ASUS information assets from internal and external risks, and ensures the confidentiality, integrity, and availability of the information security management system.

During the manufacturing stage, ASUS confirmed maturity of the information security management of the suppliers by requesting their ISO 27001 certificate to further check the scope and the validity of the certification and the relevance of the business collaboration, as well as working together to manage the information security. During the sales and product use stages, we provided customers and users with instant problem reporting, response, and handling channels. In order to provide better customer service, we established a global service hot-line, information security consultation page, and the technical support team.

- Improvement on information security awareness and the formulation of information security rules
  To ensure information security measures were in place, we conduct information security education training every year to raise awareness of information security among employees. Furthermore, we conducted social engineering drills regarding the security of email use, and focus on the trainings and educations of high-risk groups identified by the drill reports to be careful on emails from unknown sources. We formulated ten rules of information security that covered the targets and measurement from ISO 27001, and at the same time printing small cards with the rules which could be easily carried by the employees.

3. Detection of information security
   As forward-looking detection can reduce potential security threats, ASUS introduced its threat discovery service to quickly and efficiently respond to malicious program intrusion through smart network protection and virus pattern comparison mechanism. With the introduction of ACC (ASUS Control Center), which is self-developed by ASUS, all computers can be managed with one-stop collective system. Employees using any software from unknown sources will receive warning notifications, which also reminded them to comply with the intellectual property rights and relevant internal regulations. Managers will confirm the usage and the necessity of software installed by the colleague to mitigate cyber-attacks.

   ASUS continues to participate in the Hacks In Taiwan Conference (HITCON) held by the Industrial Development Bureau of the MOEA in Taiwan, providing various products for testing to identify potential vulnerabilities through hackers' mindsets. ASUS could leverage the technical capabilities of white hat (ethical) hackers in the information security community to conduct penetration tests and defense scenarios to strengthen product security and enhance the ability to develop subsequent products.

4. Information security notification and response

- ASUS Security Advisory
  We strive to ensure safety of ASUS products at all costs for protecting the privacy of our valued clients. We always strive in improvement of our safety and protective measures on personal information according to all applicable laws and regulations. We also welcome clients to notify us on

safety or privacy issues related to the product. As a result, the product and information security notification and management platform were established as an exclusive channel for the consumers, information security experts or researchers to report security vulnerabilities or problems with ASUS products or information systems. This Platform automates the management of notified cases, has a product safety response team for horizontal communication and maintain the management quality on case notification and response. Through the Platform, we would make random announcements on security of ASUS products, so consumers could understand security updates of ASUS products, as well as keeping good communication and interaction with information security experts or researchers over the internet community.

- Information security trends and joint defense mechanisms
  Regarding the latest trend on information security, ASUS introduced the warning notification provided by an external consulting company, which can provide preventive measures of handling through notification once the new type of attack appears. This prevents important information assets of the Company from new types of external attacks on information security. In addition, we regularly participate in information security research forums, such as the Taiwan Information Security Conference and the joint defense mechanism, to learn from industry practices and share the latest trends to improve the vulnerability prevention and problem solving capabilities.

  Vulnerability identification was conducted through three major aspects: product safety engineering, joint defense of intelligence and information, and external notification. We focused on product development and testing stages incorporating multiple automated detection tools to identify known vulnerabilities as early as possible, and also established a trustworthy joint defense mechanism with the National Information Sharing and Analysis Center (ISAC) and the Taiwan Computer Emergency Response Team / Coordination Center (TWCERT/CC), so that new cyber security incidents or exploited loopholes could be reported as soon as possible to rapidly implement effective countermeasures.

5. Business Continuation of information service
   The continuous operation capacity of the core information system for Company operation was improved. In addition to the information facility located at our headquarters, we hired the facility that passed ISO 27001 information security certification as an extended facility provided to the core information system for establishing structure of remote backup. At present, the important operation core information system of the Company has been completed with establishment of backup structure and operated with application of Active-Active loading balance structure. This ensures that the information system of the remote backup facility can take over the operation within the shortest time when a major accident occurs. Moreover, in 2020, the remote backup and switchover drill for the business continuity capability of the global core information system were completed to ensure that risk of operation interruptions reduced to a minimum.

   - Information security management of AI cloud software services
     The AI cloud software services provided by ASUS Intelligent Cloud Service Center (AICS) was certified by ISO/IEC 27001:2013 in December 2020, and the smart medical services also passed the information security management assessment for Health Insurance Portability and Accountability Act (HIPAA), demonstrating ASUS' comprehensive efforts to strengthen information security and ensuring that service processes comply with the most advanced and complete world-class medical and health privacy protection regulations, thus setting a new industry benchmark.

     AICS utilizes natural language processing, computer vision, deep learning, and big data analytics as the core of its AI cloud-based software as a services (SaaS) which applies in data-driven precision healthcare and medical treatment, and management in manufacturing Environmental Safety and Health (ESH) to help business customers solve their most challenging problems and

propel the development of Taiwan's next world-class industry leader. Smart healthcare is a major trend. In terms of opportunities of related applications, services such as the collection, transmission, storage and analysis of health information present two major challenges in information security and privacy. The capabilities of protecting the electronic Protected Health Information (ePHI) from internal and external threats and ensuring the confidentiality, availability and integrity of the data will be keys to the future development of smart medicine. AICS actively establishes a program safety and quality culture in the development environment, and sets quantifiable quality indicators for program quality management as well as designing multiple review mechanisms. Detection services are also carried out in the software development process, scanning each service code that will be launched to check for possible errors and security loopholes. These measures greatly reduce data loss, improve the overall information security condition and the availability of the service system, ensuring that safety and efficiency of the products and services can satisfy customers.

As information security risks increase significantly, the most important benefit of introducing the ISO 27001 is to build the mechanism on the management of information security and goals to reach a consensus of information security and thus enhancing the awareness in the organization. The introduction of ISMS-based risk inventory, secure software development life cycle (SSDLC), outsourcing management and information security incident handling help reduce the possibility and impact of information security incidents such as malware infections, data leakage and operational interruption, and enhances the confidence of customers and interested parties in the stable operation of the company.