Privacy & Information Security

Target in 2023	Operational performance against the target
0 case Complaints about information insecurity.	**No** Complaints regarding information insecurity.

Background and relevance

Currently, information technology plays a crucial role in the data management system of organizations. S&P utilizes information technology and cybersecurity to enhance the efficiency and effectiveness of our business operations. This includes improving internal communication infrastructure, data collection, planning production and transportation, as well as quality control and process optimization.

However, despite technology's contribution to enhancing business operations, system downtime and cyberattacks raise significant concerns regarding data security for both customers and consumers. Therefore, our company recognizes that managing information systems is a vital foundation for business operations. We are committed to upgrading our information systems and training our personnel to be prepared to tackle cybersecurity threats.

Commitment

S&P is aware of the importance of using information technology and cybersecurity to enhance business efficiency, along with preparing to cope with cyber risks by maintaining and safeguarding network security to protect personal data (PDPA) in accordance with company regulations. Additionally, this is to avoid human rights violation.

Operational approaches

S&P has undertaken the enhancement of information technology security policy to provide guidelines for data usage, operations, development, and maintenance of information technology system in a suitable manner, in line with international standards such as ISO 27001 and related security requirements. Additionally, cybersecurity management is integrated as part of the organization's risk management to ensure appropriate responses to cybersecurity incidents and system interruptions. This ensures efficient handling of such situations.

Structure of Information Technology Security Committee

S&P has established a management committee responsible for overseeing, advising, and filtering information security measures, as well as providing operational guidelines to ensure efficiency. The Board of Directors appoints the head of the IT department as the management representative to oversee and control our information security system. They are accountable for overall supervision, risk assessment, development of appropriate security measures, and ensuring comprehensive implementation, including effectively addressing any arising issues.

Information Security Policy

S&P has announced an information security policy to ensure the security of the information technology systems, networks, and computer equipment. This policy aims to support our operations continuously, comply with computer-related offenses laws, as well as other relevant laws, and prevent threats that may cause harm to S&P.

Information Technology and Cyber Risk Management

S&P incorporates risk management principles and establishes a risk management committee to manage technology and cyber risks. Additionally, we develop contingency plans for emergency situations where electronic methods cannot be employed. Cybersecurity testing is conducted for employees in simulated real-world scenarios to enhance familiarity and ensure appropriate responses and mitigation.

Measures for dealing with cyber threats

S&P evaluates current high-risk threat patterns, develops an Incident Response Plan, and conducts regular drills at least annually to prevent and efficiently recover from security incidents. This ensures that S&P can continue the operations seamlessly with minimal impact.

Cybersecurity Awareness Training

S&P promotes and supports cybersecurity awareness training aligned with industry standards through certified Cyber Security institutions. This training is provided regularly to employees directly responsible for cybersecurity. We aim to equip them with the knowledge and skills necessary to effectively identify and manage cyber threats in a timely manner.

Cyber Threat Response Testing

S&P conducts simulated cyber threat response scenarios, such as phishing emails, at appropriate frequencies according to predetermined schedules. These tests are conducted randomly to observe the behaviors of users and administrators. The data collected is then analyzed, and recommendations are provided to individuals who may have misunderstood proper response or risk management procedures related to cyber threats.

Summary of operational performance in 2023

Complaints about data insecurity

0 case

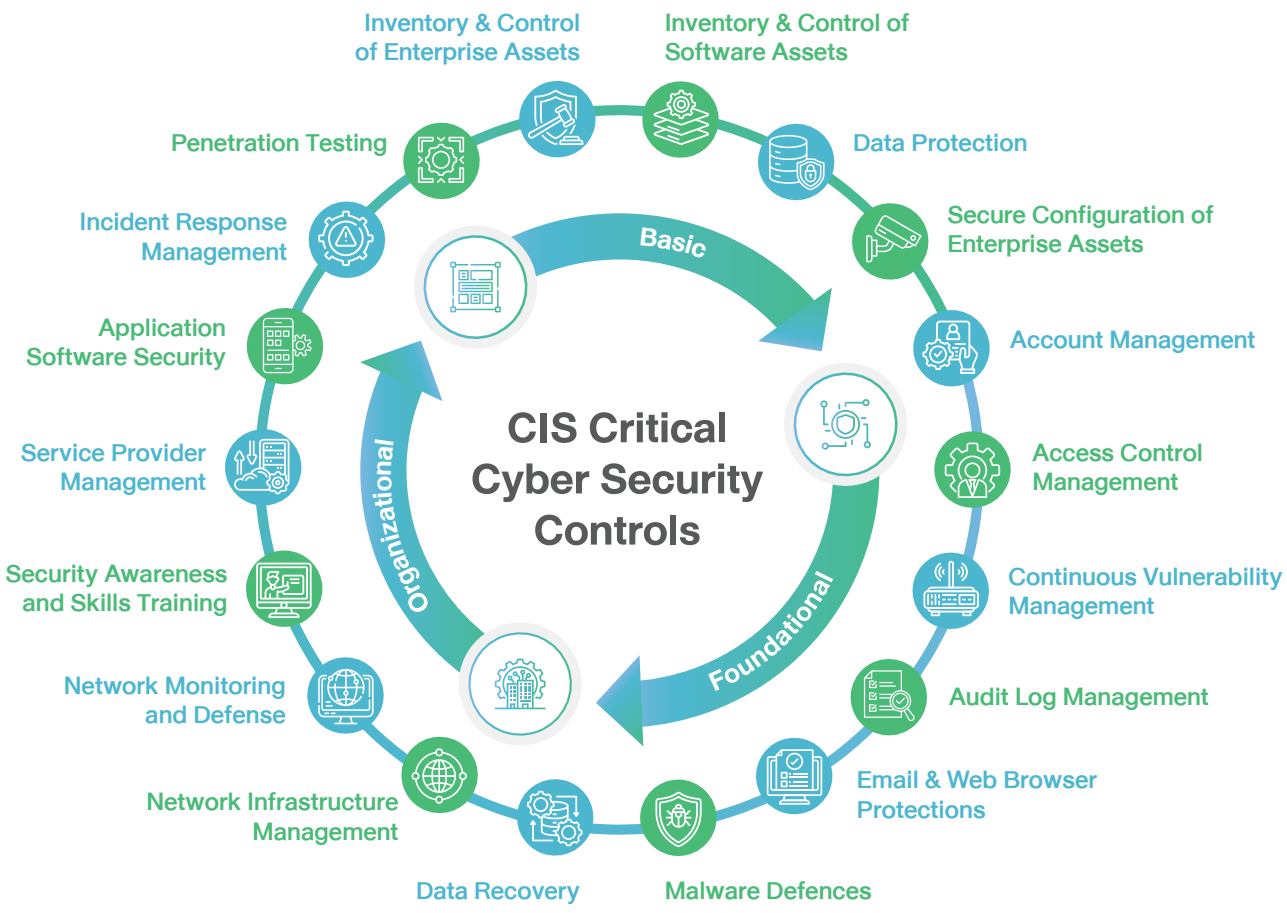
Information security issues from computer virus infections

0 case

Cyber threat incident issues that happened to the organization

Highlight projects in 2023

Standard Cyber Security Project



S&P has a plan to implement Critical Cyber Security Controls (CIS) to mitigate cyber risks and establish cyber security resilience. S&P will commence implementation within the year 2024. Nevertheless, in the year 2023, S&P has prepared and conducted management activities for the organization's data security readiness as follows:

Managing the organization's information security system in 2023

- Network Monitoring and Defense:
  SIEM Platform and Security Operation Center
- Audit Log Management:
  SIEM Platform and Security Operation Center
- Malware Defense:
  Upgrade Endpoint Detection and Response with Bitdefender
- Data Recovery ready on core application
  SAP, BOR, POS
- Data Protection ready on core application
  SAP with Immutable Backup
- Windows Update and Security Up to date:
  Operating System and Security up to date
- EMAIL and Web Browser Protections:
  Security include Google Workspace and Chrome Security up to date
- Continuous Vulnerability Management:
  Security Operation Center, Monitoring and Patching (OS, Network, Antivirus)

Plan for continued management of the organization's information security system in 2024

- Cyber Security Consulting:
  Assessment S&P Security Align Security Framework and ISO 27001
- Account Management:
  Privilege Access Management and Single Sign On
- Security Awareness and Skills Training:
  Cyber Security Awareness and Training
- Inventory and Control Enterprise Assets:
  Asset Management Policies and IT Hardware and Software Inventory

benefits