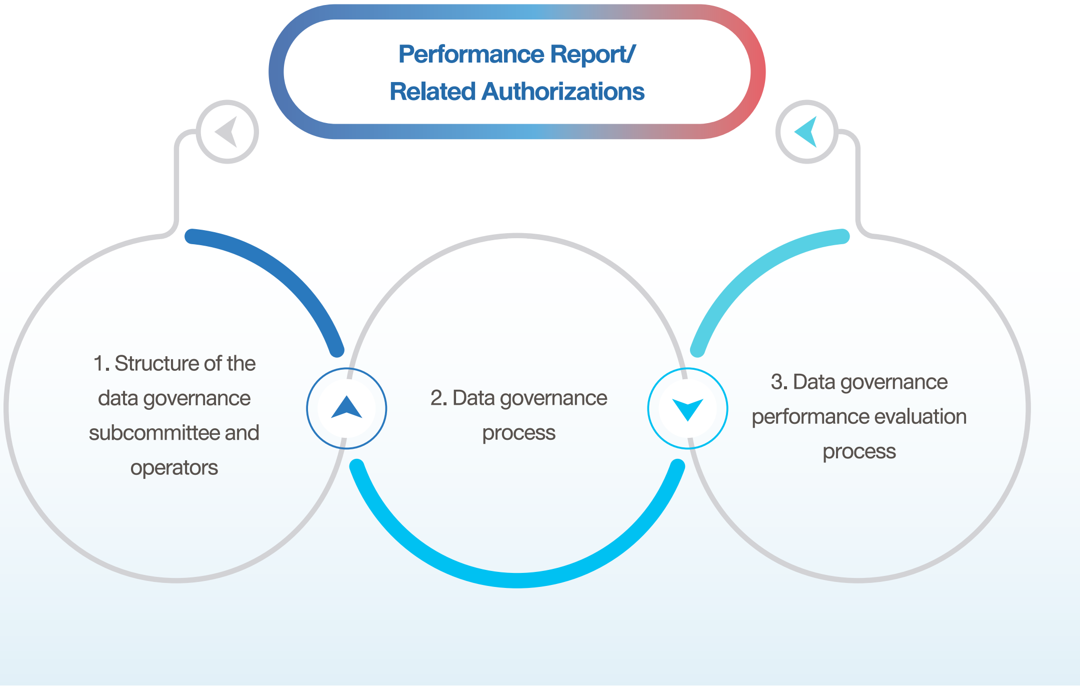
Integration of Data Governance and Data Management

Because the businesses of financial institutes today require the use of information in their operation and analytics in order to drive work in line with the current trend of business sector to becoming data-driven organizations, TISCO Group recognizes and values the importance of data management, especially data quality in terms of volume, variety, velocity and veracity, to make sure that we have correct data for analysis to make decisions and understand the needs of customers through the use of artificial intelligence. Furthermore, in addition to the aforementioend developments and technological changes, from the perspective of regulations and laws, businesses also have to make improvements to ensure compliance in this area.

TISCO Group is convinced that good data governance is a task that must be continuously carried out to safeguard the overall data governance strength. Therefore, We give priority to managing data in terms of ensuring the security and availability for use of data, with the highest level of personal data protection to prevent violation of related policies or laws, especially the Personal Data Protection Act, B.E. 2562 (2019). In doing so, we have created the structure of the Data Governance Subcommitee, the Data Controller and Data Operators, by clearly specified their scope of duties, work processes and performance measurement, setting adequate measures to ensure data security, accuracy, completeness and currency, building confidence with data subjects or customers towards the Company in conducting business


Performance Report/
Related Authorizations
1. Structure of the data governance subcommittee and operators
2. Data governance process
3. Data governance performance evaluation process

In 2023, our data governance and data management were refined as follows:

Additional Data Management Activities in 2023

Reviewed and improved policies and guidelines related to data governance, ranging from collection processes, storage, dissemination, and destruction of data to ensure that they are always appropriate for each business section and up to standard. The reviews also focus on level of security and safety for each data classification, using the "need-to-know" and "least privileges" basis that grant access to data according to duties and responsibilities. These processes are done every year or whenever there are significant changes during the year.

Raised awareness and enhanced understanding about data governance and data management in high-risks group and stakeholders through seminars, training, workshops and communication via the organization's social media. All employees are also required to undergo compulsory testing about the guidelines.

Integrated data governance guidelines and standard to all newly developed work systems and continuously audited existing major systems according to the approved work plans. Data governance performance, as well as outcomes of operation risks and IT risk management of these systems were then quarterly summarized and reported Data Governance Committee to reinforce adherence to the control measures.

Created and enhanced effectiveness for data management in a centralized manner, to ensure ease of management, comprehensiveness, simplicity, and convenience in taking action according to control standards, including metadata collection and access under the control of the Data Controller, data retention and destruction, data quality verification, data usage, and data sharing, etc.

Customer Data Protection and Privacy

TISCO Group gives importance to personal data protection by including it as part of the data governance system, defining processes and control systems in accordance with the Personal Data Protection Act in order to strengthen management effectiveness. We also regularly review guidelines, procedures and work methods related to data security and customer data protection to make certain that they are always current, consistent, and able to prevent risk from unauthorized usage and disclosures of personal data, breach of intended purpose consented by the data subject, or noncompliance to related laws. Moreover, we have created a data breach response plan to serve as a mechanism to prevent and mitigate potential damage in cases of data breaches.

In addition, TISCO Group has formulated guidelines for data protection impact assessment (DPIA) for related data users or data handlers to use when assessing potential risks and impacts from data misuse that might violate the rights and freedoms of personal data subject, in order to have proper security mechanisms in place and reduce the risk or severity of impacts.

Example of Personal Data Protection Guidelines

- Collection, use, and disclosure of personal data
- Consent management
- Data subject rights management
- Data protection
- Data retention, duration of storage and destruction of data
- Data protection impact assessment (DPIA)
- Data breach response management

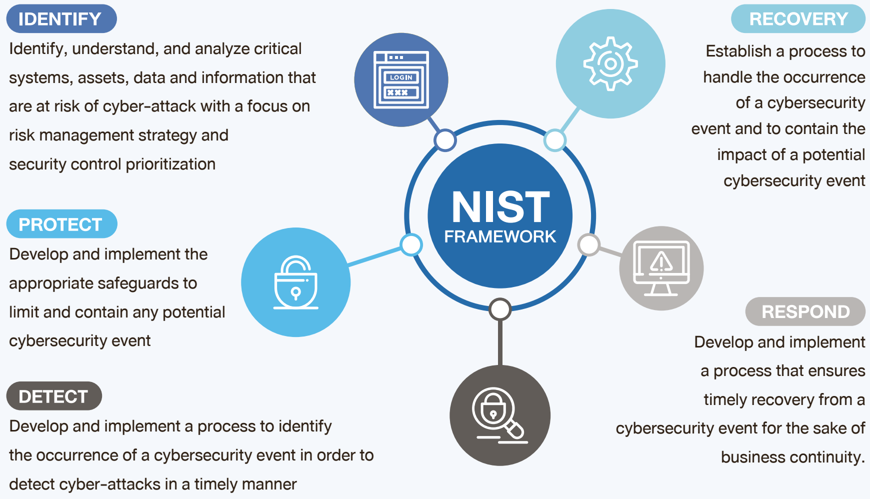
Additional Data Protection Activities in 2023

- Reviewed and updated guidelines and procedures related to data security and data protection to ensure that they are up-to-date with current situations while still consistent with TISCO Group's operating practices
- Safeguarding and protecting the security of customers' personal information. In 2023 TISCO Group received no complaints related to significant breaches of customer data privacy.

Cyber Security

Today, personal data and important information used inside organizations have become assets that are highly valuable to businesses, especially in the finance and banking sector. At the same time, cyber security threats are risks that banks have to pay attention to, especially due to today's business model which relies on a wide range of modern information technologies to develop new financial products and services that meet the needs of customers and business partners, as well as provide business opportunities and competitive edge, allowing the business to achieve sustainable growth.

For this reason, TISCO Group places great importance to the formulation of policies and guidelines for cyber security and IT risk management in accordance with international standards. TISCO Group constantly integrate modern technologies for risk management and controls to ensure that the system is always ready to detect, prevent, and respond to cyber threats. We has also adopted international control measures such as the ISO/IEC 27001 and NIST Cybersecurity Framework to be part of IT security policies and guidelines, in order to foster trust with customers and business partners while providing safety when using our services.



IDENTIFY

Identify, understand, and analyze critical systems, assets, data and information that are at risk of cyber-attack with a focus on risk management strategy and security control prioritization

PROTECT

Develop and implement the appropriate safeguards to limit and contain any potential cybersecurity event

DETECT

Develop and implement a process to identify the occurrence of a cybersecurity event in order to detect cyber-attacks in a timely manner

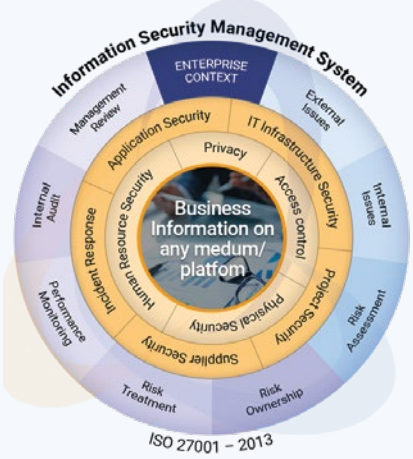
RECOVERY

Establish a process to handle the occurrence of a cybersecurity event and to contain the impact of a potential cybersecurity event

RESPOND

Develop and implement a process that ensures timely recovery from a cybersecurity event for the sake of business continuity.

NIST Cybersecurity Framework



ISO/IEC 27001 Framework

TISCO Group has created an organization structure that incorporated IT governance, where roles, duties and responsibilities are clearly and appropriately defined, from the level of the Board of Directors and high-ranking executives. This shows our emphasis on driving and enhancing IT risk management. The other mechanism includes the three lines of defense system to handle and manage IT risks systematically and consistently through the clearly divided roles and responsibilities as follows:

1st Line of Defense

refers to IT operational staff who oversee IT tasks and the internal management of IT safety.

2nd Line of Defense

points to a unit responsible for risk management, supervision and monitoring of the overall enterprise risk, which is tasked with managing both the IT risk and the Operation Risk

3rd Line of Defense

refers to units responsible for auditing that can independently review operation performance, IT operation and IT risk management and supervise legal and IT regulatory compliance.

Furthermore, TISCO Group places emphasis on creating a culture concerning cyber security threats inside the organization by promoting cyber security awareness with focus on 4 target groups as follows:

The Board of Directors and High-ranking Executives:

Cyber security threats are given priority as one of the primary goals of the Board of Directors and high-ranking executives. Thus, annual IT security awareness training is provided to high-ranking executives to enable executives to acknowledge and understand the new, complex, and diverse types of cyber-attacks and trends, allowing them to use this information in formulating or adjusting policies and measures to effectively deal with cyber risks and attacks.

IT Personnel:

Employees performing IT functions are provided several training on the essential technology knowledge required for their work, as well as on how to respond to cyber attacks. This includes cyber drill exercises, where realistic cyber attacks are simulated internally or by external institutions such as the Thailand Banking Sector Computer Emergency Response Team (TB-CERT), in order to raise the level of collaboration and understanding about the financial industry, in order to test and rehearse practice guidelines for use in response to attacks and to enhance readiness for dealing with potential cyber-attacks against TISCO Group.

Employees of TISCO Group:

All employees are provided training about how to maintain IT security and knowledge about new cyber threats through e-learning, posters, infographics, as well as training about the international standards on IT security. These trainings also encourages employees to use their knowledge, while performing thier work, which will lead to safety in the products and services of TISCO Group. Moreover, cyber drills are held annually, in which false phishing emails are sent to all employees to test responses to the scenarios. The test results showed that employees are aware and can respond correctly to phishing emails within the organization.

Customers:

TISCO Group regularly provides knowledge about cyber threats and how to conduct online transactions safely to customers through many communication channels of TISCO Group such as websites or online social media to raise customers' awareness and ability to deal with the various acts of deception and cyber threats that are widespread nowadays.

TISCO
4 วิธี
รู้เท่าทันแอปดูดเงิน
1
2
3
4
UPDATE
หากได้รับความเสียหาย หรือต้องการความช่วยเหลือ สามารถสอบถามหรือแจ้งเหตุ
ได้ที่ TISCO Contact Center โทร. 02 633 6000 กด*7 ตลอด 24 ชั่วโมง

TISCO
How to
เช็กเพจปลอม รู้ไว้ไม่โดนหลอก
Fake ?
Real ?
ดูเครื่องหมาย Verified Badge
ชื่อเพจ
ยอดผู้ติดตาม
URL ของเพจ
ดูรายละเอียดของเพจ
เนื้อหาและการแสดงความคิดเห็นของผู้ติดตาม
เพจจริง จะไม่ทักข้อความหาผู้ติดตามก่อน

From the assessment and audit results **in 2023, there were no complaints about any issue regarding the safety of customer information or losses, alterations or falsification of data, or data access to data by unauthorized parties.**