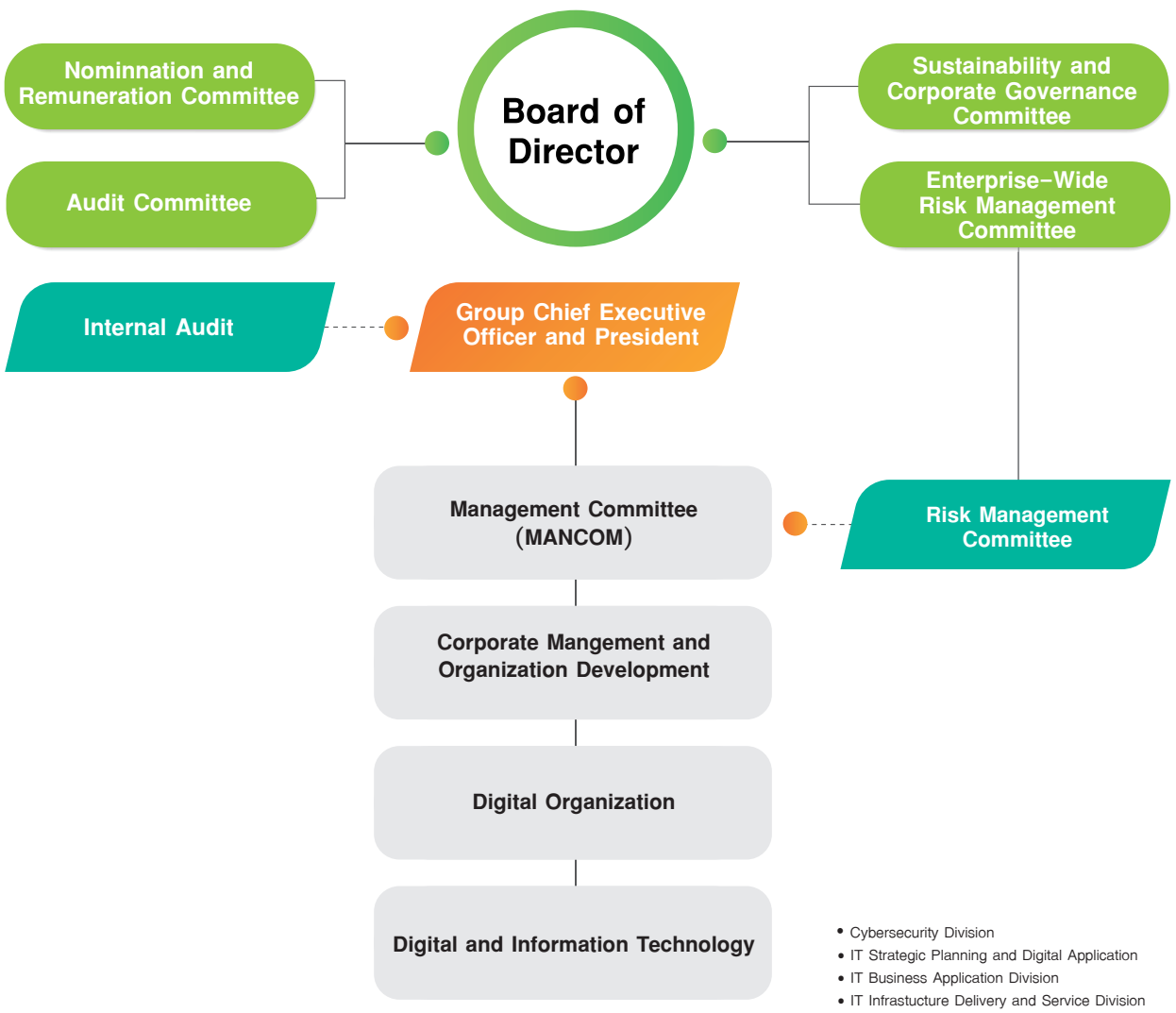
Information Technology (IT) and Cyber Security for Business

Cybersecurity is an important issue that can have an impact on both internal and external stakeholders. This includes potential operational security risk such as system crashes, and the possibility of personal information violation of employees, partners and customers.

Therefore, the company relied on information technology systems as important tools to meet the expectations and needs of stakeholders. It follows practical guidelines, tools, and frameworks to implement up-to-date and efficient standard. Risk management also focuses on security systems in line with international standards and government requirements, such as the Computer Crimes Act, B.E. 2560 (2017), Cyber Security Act, B.E. 2562 (2019), and the Personal Data Protection Act, B.E. 2562 (2019). This approach supports business expansion in accordance with corporate strategic plans and prevent the violation of the stakeholders' rights resulting from the misuse of personal information.

Information Technology and Cyber Security Management Structure

The company has appointed The Information Technology and Cybersecurity Digital Department is responsible for the management of the committee and report performance to the Management Committee (MANCOM), and they also report IT risk management and cybersecurity to the sub-committees and the Enterprise-wide Risk Management Committee (ERMC).



Since 2018, the company has set up a cybersecurity section to be responsible for managing cybersecurity and cybersecurity management occurs in line with international standards, including ISO/IEC 27001:2013, ISO/IEC 27032:2012, ISO/IEC 27018:2019 and NIST Cyber Security Framework.

Information Security Management in accordance with International Standards

- ISO/IEC 27001:2013 Bangchak has received certification for ISO/IES 27001:2013, an Information Security Management Systems standard, since 2012. The company implemented the standard in risk management, design of security system, and in operations to create resiliency in control and development.
- ISO/IEC 27032:2012, Bangchak received ISO 27001 since 2018, which focuses on the confidentiality, integrity and availability in the cyberspace to protect hardware and software assets as well as information and virtual assets such as brand and reputation.
- ISO/IEC 27018:2012 The company has been certified by this standard since 2021, which focuses on information security management to protect of personally-identifiable information in the company's cloud.

Protection of Assets, Information and Systems

Bangchak has implemented the Information Technology and Cyber Security Policy to ensure protection coverage through:

1. Conduct risk assessment of important IT systems and develop backup system and emergency management plan in an event where operations cannot be conducted electronically. The backup system and emergency plan are frequency tested for readiness.
2. Information technology management shall have measures to control and protect assets and equipment to ensure operational readiness and deterrent against unauthorized access from both onsite and offsite usage.
3. Control access to information and information technology usage based on level of importance as part of data management and confidentially. This includes control of electronic messaging as well as providing a written contract on confidentiality and information protection with external entities.
4. The company provided Multi-Factor Authentication (MFA), advance Endpoint Protection, Zero Trust advanced security information and event management (Advance SIEM) systems. In addition, Deception Technology that can help analyze new attacks quickly and accurately, helping admin to responds confidently to protect the company's information systems. The company conducts awareness raising activities with relevant users. Technical vulnerabilities are managed through:

- Testing of procedures and processes to manage security incidents at least once a year including conducting a cyber security drill.
- Conducting a penetration test on important operation systems to analyze risks and impacts to the business at least once every year.
- Conducting vulnerability assessment of the operating system (OS) Software and network/security equipment to determine whether there are any vulnerability and impact level so system operators/managers can determine the likelihood of attacks and develop corrective actions.

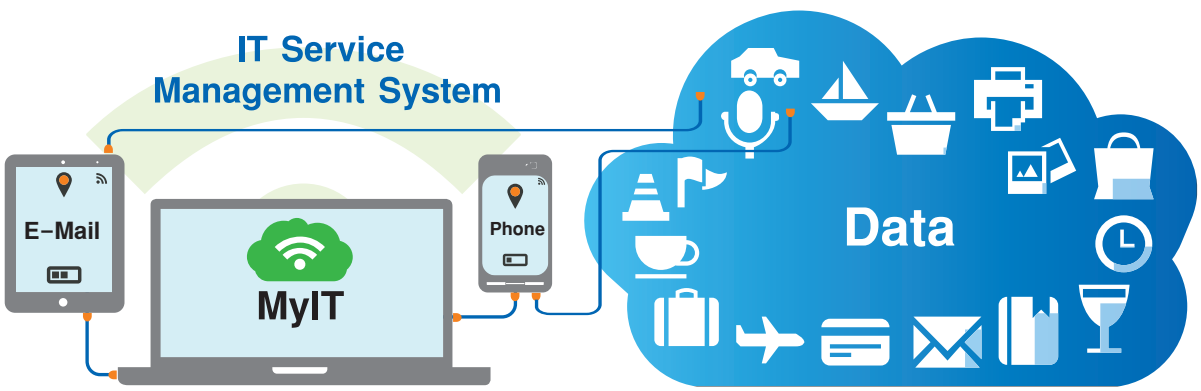
Internal communication to raise awareness and increase effectiveness of IT system usage.

Internal communication has been increasingly implemented in internal operations and businesses. Therefore, Bangchak has provided communications and training for employees which included:

- Orientation for new employees through the use of operational training and measure understanding of cybersecurity awareness as well as requirements for the use of corporate information systems and regulatory compliance such as the Computer Crime Act of 2017 and Personal Data Protection Act of 2019.
- Communicate potential cyber risks to create knowledge and security awareness through Company's e-mails.
- Conducted Cybersecurity Awareness Improvement Program annually through phishing mail assessment understanding assessment which includes conducting phishing simulation in order to determine the level of risk to the company. To assess users' awareness, the Security Awareness Assessment is conducted. Results are documented, analyze, and use to develop further training plans as well as to improve phishing mail prevention measures. In 2021, 4 scenarios were conducted along with the assessment of errors from the test to employees immediately to create awareness (rapid improvement program). In addition, the various scenarios revealed some weaknesses in which Bangchak used the information to conduct analysis to close the vulnerabilities by communicating with employees to learn, be aware, and know how to deal with the threat of Phishing Mail better.
- Cyber Security Response for Bangchak Group is another measure implemented to improve cyber security. The company educated employees, executives, and subsidiaries through cyber security incident case studies such as business email compromise (BEC) (e.g. fake invoice). The company also implemented Strictly Process Confirming as follow:
  1. Requests: Registration or change to important information, especially bank account information.
  2. Use the company form to verify and confirm the change of information and must be signed by responsible person of the counter party.
  3. Must have relevant, formal, and legal documents or issued by a government agency.
  4. Re-Check with requester by telephone.
  5. Add these steps into the operation manual.

Countermeasures in Case of Cyber Threats

Emergency drill and business continuity plan: The company has instituted plans and procedures for Incident Response Plans which are considered as a high-risk, to be able to prevent and recover effectively and rapidly in order to operate the business continuously and minimize the impacts. In operation, the company set up an IT Service Management System using BMC Remedy system named MyIT, which has procedures for managing information security incidents. Employees can report to the Information Technology Service in 3 channels: MyIT system, email, and telephone.



Number of Data Breach Incidents, Inadvertent Disclosures and Data Leakage

Year	2017	2018	2019	2020	2021	2022
Number of Time	0	0	0	0	0	0

Number of Customer Data Leaks or Unauthorized Disclosures/Uses

Year	2017	2018	2019	2020	2021	2022
Number of Time	0	0	0	0	0	0