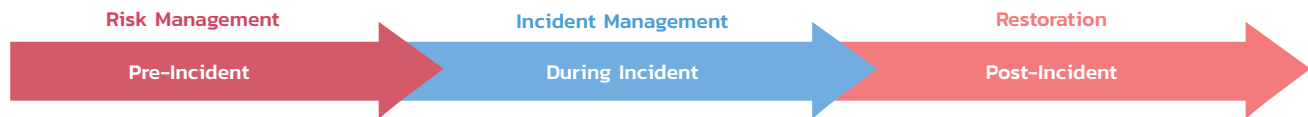


## Risk Management

The Company is committed in risk management, which is a crucial mechanism in identifying risks and any future challenges that may affect the Company. Simultaneously, effective risk management and risk mitigation measure are important factors that will facilitate the Company to achieve its goals. Both factors also create values for all stakeholder groups. The Company therefore stipulate risk management framework to ensure the Company can work according to its risk management approach, and is able to identify and forecast risks with potential negative

impacts to the Company’s operation and goals in every aspects. Similarly, the Company has develop plans to continuously control, monitor, and improve risks through management, control and review mechanisms. These components ensures risk level is within risk appetite, as well as embedding corporate-wide risk management culture. Such arrangement promotes understanding, raises awareness and engagement for all level of employees on the topic of corporate-wide risk management.

### Risk and Incident Management Framework for Sustainable Business Operations



#### Incident Sequence

Objective for overall restoration: restore to normal state as soon as possible



#### Occident Occurrence

Timeline		
Incident Response	Business Continuity	Recovery / Resumption Back to Normal
<b>Minutes to hours :</b> <ul style="list-style-type: none"> <li>• Staff and visitors accounted for</li> <li>• Casualty addressed</li> <li>• Limitscale of damage</li> <li>• Assessment of damage</li> <li>• Invocation of BCP</li> </ul>	<b>Minutes to days :</b> <ul style="list-style-type: none"> <li>• Contact staff, customers, suppliers etc.</li> <li>• Recovery of critical business processes</li> <li>• Rebuild lost work-in-progress</li> </ul>	<b>Weeks to months :</b> <ul style="list-style-type: none"> <li>• Damage repair / replacement</li> <li>• Relocation to permanent place of work</li> <li>• Recover of costs from insurers</li> </ul>

BS 25999-1 : 2006 Part 1 : Code of Practice

The Company established Risk Management Unit and Compliance Unit, operating under Risk Management Committee. The Company appoints representatives in each function to jointly work in the Unit. They are also tasked with summarizing and reporting performance to Management, the audit committee and the Board, twice a year. This routine reviews efficiency and effectiveness of

risk management process, such as financial risks, tax risks, strategic risks, compliance risks, operational risks, social risks, environmental risks, climate change risks, economic risks, corruption risks, and reputation risks. Additionally, risk management process is reviewed and assessed according to COSO Framework annually.



In 2019, Risk Management Unit divides risk management structures into 3 categories, which are

- 1 Operational risk
- 2 Sustainability risk, and
- 3 Emerging risk

Functions collaborate in annual risk assessment, trainings and seminars. Representatives from different functions, or risk champions, who drive for development of risk mitigation measures and processes, will participate on a quarterly basis. Data Protection Officer has also been appointed to provide knowledge. Similarly, there are clear process for internal control and risk monitoring, which requires close collaboration with risk champions. The process and performance are as follows.

### Emerging Risks

The Company reviews risks and analyzes emerging risks which may affect the Company's business operations continuously. This ensures immediate measures and responses to address them. In 2019, there are two types of emerging risks, as follows: digital transformation and cyber security.



### Digital Transformation Risks

Business operations and internal processes are quickly becoming more digitized. This increases business competitiveness, changes consumers' demands and behaviours; thus creating business risks. The Company sets forth appropriate digital strategy and business plans through

**1** Expansion of channels for consumers, such as Omni Channel, which serves as an accessible and convenient distribution channel through both online and offline system; allowing a seamless transitioning experience



**2** Development of a large variety of payment methods, such as Alipay Wallet and TrueMoney Wallet



**3** Development of ALL Member program to accumulate points for purchases at 7-Eleven, which also offers privileges with subsidiaries; along with promotional activities offered via online application and digital marketing to support entrepreneurs and increase customer engagement



**4** Explore novel forms of service solutions to address customers of digital era

**5** development of distribution system

**6** Adjust operational structure and format to facilitate digital era's work; this includes deploying prevention measures against digital risks, such as privacy violation, and cybersecurity

**7** Human resource development, preparing for transition to a digital era



### Cyber Security Risks

The Company's internal operations are becoming more digitized. This exposes the business to more information security and cyber security risks, which may directly impact the Company's image, reputation and reliability. The Company therefore established Information Technology Security Management and Online Security Strategic Management System, which comprises 3 components, as follows.

**1** **Units and employees;** Cyber Security Officer's duties are stipulated to be in alignment and address aforementioned risks. They work to ensure that any risks occur is within risk appetite. Information and Network Security Unit was established, trainings and assessments were regularly carried out to ensure employees stay current – as well as enhancing their cyber security awareness. Communication were made through internal channels and assessments were carried out through cyber simulation programs

**2** **Measures and operational processes** in addition to the Company's network and information security policy, the Company also established for relevant measures to be reviewed at least once annually. The reviews are conducted by Go Soft (Thailand) Co. Ltd, under international framework of ISO 20000 and ISO27001. The Company has also developed a cyber security incident response plan.

**3** **Technology** the Company prioritizes the use of defensive technology system, per international safety standard or NIST Framework; as well as development of computer hubs and information system's accessibility to meet the monitoring standards. The Company is also committed in exchange knowledge with service users and invest in novel defense system – ensuring the technology remains relevant and effective against new risks.

#### People



- Cyber Security Officer (CSO), reporting directly to high level management
- Security system unit and employees certified with security certificates
- Training and testing employees at all levels, using phishing simulation test, cyber awareness, and war game

#### Process



- The Company's Information and network security policy
- Process and standards certified by ISO20000 and ISO27001
- Cyber security incident response plan

#### Technology



- Defensive technological system in alignment with NIST
- Computers hubs, monitoring and information system's accessibility meeting international standards required
- Knowledge exchange with service users and investing in new defensive systems

Furthermore, the Company remains committed in raising awareness of internal risk identification through “Participatory Corporate Risk Identification Program” with employees to Management, facilitating “Black Swan” identification. Black Swan incident may obstruct the Company from achieving its goal, create insecurity or instability to the Company. The 6 related risk issues comprise

- 1 **Business Continuity**
- 4 **Outsourcing**
- 2 **Work Process**
- 5 **Corporate Sustainability**
- 3 **Product and Service**
- 6 **Other Activities Related to Companies in The Group Management**

Via employees participated in the Risk Identification program through various channels, such as Electronic Platform, QR Code; which provides convenience and enhances employees’ engagement further. The program’s key concept is “to identify and address potential Black Swan incidents, facilitating control and management”

### Black Swan Award




In 2019, employees have submitted

# 1,169

issues of risks in total

- 1) Compliance Risk
- 2) Data Security
- 3) Human Right Risk
- 4) Environmental Risk
- 5) Product and Service Liability



5 risks being awarded the Black Swan Award, which are:

Risk issues receiving awards will be presented to Management for development of response measures. This can lead to effective real-life application.

### Cyber Resilience Preparation Project



Risks of Cyber Threats

The Company recognizes the importance of protecting customers’ data. Online transactions are exposed to the risks of cyber threats. In the previous year, the Company has reviewed and developed measures ensuring readiness against cyber threats. Efforts include putting in place a governance framework, management of human capital risk, process risks, as well as equipment or technological risks. To ensure minimization of impacts against customers and the overall system, the Company has developed Cyber Resilience Readiness Assessment Framework. In 2019, there are trainings and seminars organized to proactively raise Management and employees’ awareness and understanding of cybersecurity. The Company also conducted phishing simulation tests to increase readiness in managing cybersecurity incidents.

Performance

Reviewed different function’s process to manage cybersecurity threats. Develop a guideline for minimization of risk severity

# 100%

of relevant Management received trainings and participated in the workshop.



Cyber Threat Crisis Management

In 2019, the Company conducted a simulation, ‘Cyber War Game,’ for high-level Management to try their hands resolving possible cyber threats in the Company’s system. Relevant high-level Management comprises CEO, CIO, CSO, CFO, COO, and those in communication and laws. This simulation is organized once a year.

Performance

- 100% of high-level Management participated in the project
- Ensuring readiness to promptly address mentioned crisis
- Minimize damage and corporate negative image