CYBER SECURITY & DATA PROTECTION

Target and Performance

Long term target by 2030:

The company achieves international standards for cybersecurity and data privacy certifications.



2025 Performance: Achieved the 2030 target, with the company receiving NIST assessment scores for the 3rd consecutive year. The Company's average score is **4.22** (while National average score is 1.91)



100% Complied with Charoen Pokphand Group and external party action list for cybersecurity and data privacy.

- Total number of information security breach case = **0** case
- Total number of clients, customers and employees affected by the cybersecurity and data privacy breaches = **0** person
- Total number of clients, customers and employees affected by the data privacy breaches = **0** case
- **100%** of employees have been trained in cybersecurity awareness and phishing E-mail.
- **100%** of data routes have been conducted the cybersecurity risk assessment.
- **100%** of web and mobile application have been conducted the security testing service.

Opportunities and Challenges

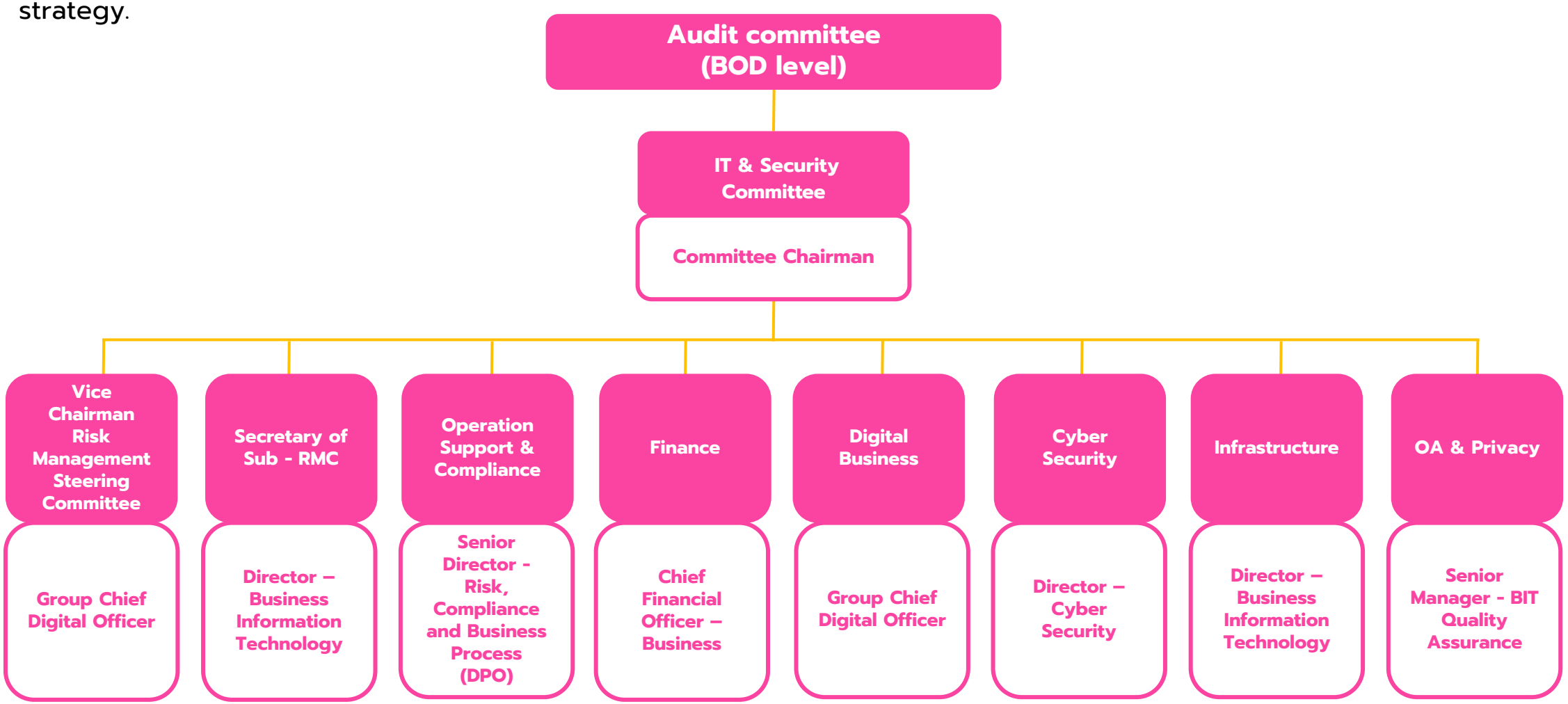
Presently, business operations need to apply information technology to maximize operational efficiency, effectiveness, and more creativity. On the other hand, increasing the risk of emerging risks of cyber-attacks or threats. The Company is enhancing and developing the cybersecurity and data privacy policy to protect data and trustworthiness for customers and stakeholders throughout the value chain.

Policy & Management Approach

The Company prioritizes cybersecurity and data privacy, started assessing risks to prepare a plan to deal with various cyber threats, and announcing policies for all Company personnel to be thoroughly informed, serving as a guideline for raising cyber awareness and attaining ISO27001, international information security standards and Charoen Pokphand Group.

Cybersecurity Governance

The Information Technology and Security Committee reports to the Audit committee (Board level). The committee chairman is Chief Information Technology Officer, Risk committee on the engaged on the cybersecurity strategy process and the Executive Management team with relevant background in IT oversees the company's cybersecurity strategy.



Cybersecurity Policy Structure



Cyber Security Management | Cyber Security Risk Assessment | Cyber Security Risk Mitigation | Cyber Security Continuous Management | Cyber Security Awareness

Cybersecurity Management Program

Scope and Implementation	2025 Result
Information security-related business continuity plans	• Following the framework of the ISO22301 to prepare for various crises that may occur and impact key business operations and the Company's risk management protocols. The BCP drills are conducted twice as the Cybersecurity Business Continuity Plan.
Information security vulnerability analysis	• Information security vulnerability analysis was done (Verification and Vulnerability Analysis by External Party)
Internal audit of the IT infrastructure and security management systems	• **100%** are internally audited as annual basis
Independent external audit of the information security management systems	• The company participate the NIST Function Rating, result score = 4.22 of 5 which was the highest ranking of 202 participated companies. • External audit by KPMG for IT Controls Review
Escalation process for employees to report incidents, vulnerabilities or suspicious activities	• **100%** employee are trained and communicated the Policies, information, and practices through training, internal communication email, and bulletin.
Information security awareness training	• **100%** of employee has trained and communicated the cybersecurity policies
Total number of compliant of breaches	• **Zero** Case

Cybersecurity Risk Management

Presently, cyber threats and attacks are more complex and impact cybersecurity risk. The company thus conducts 5-dimensional risk assessments cover a wide range of data routes that could be used to access company data, from head office, mobile phone applications, websites, as well as store and business partners.

Risk Assessment Guidelines	Risk Assessment Scope
Connecting to public networks	Company's servers
Phishing and ransomware	Employees
Identity theft	System administrators and employees
Supply chain attack	Information technology third parties
Information leakage	Employees

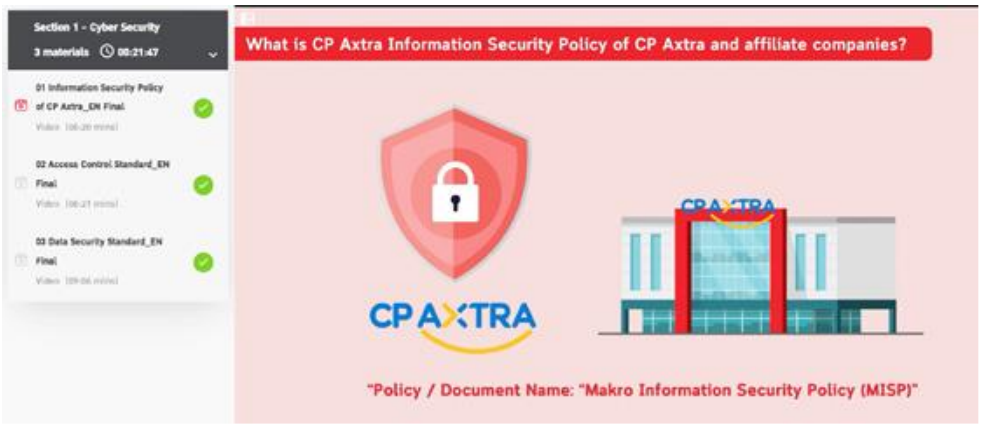
Cybersecurity Awareness Training and Discipline

Awareness being the key to ensuring information system security against cyber threats and data leak prevention, approach is reinforced to raise corporate awareness; communication to introduce and create awareness, alerts to activate response awareness, and testing to assess cyber security awareness.

The cybersecurity is everyone's responsibility with being the one criteria of Annual Performance Evaluation and the year end bonus for employee both staff and manager levels must be reviewed the performance of discipline that related to cyber security and data protection policy.

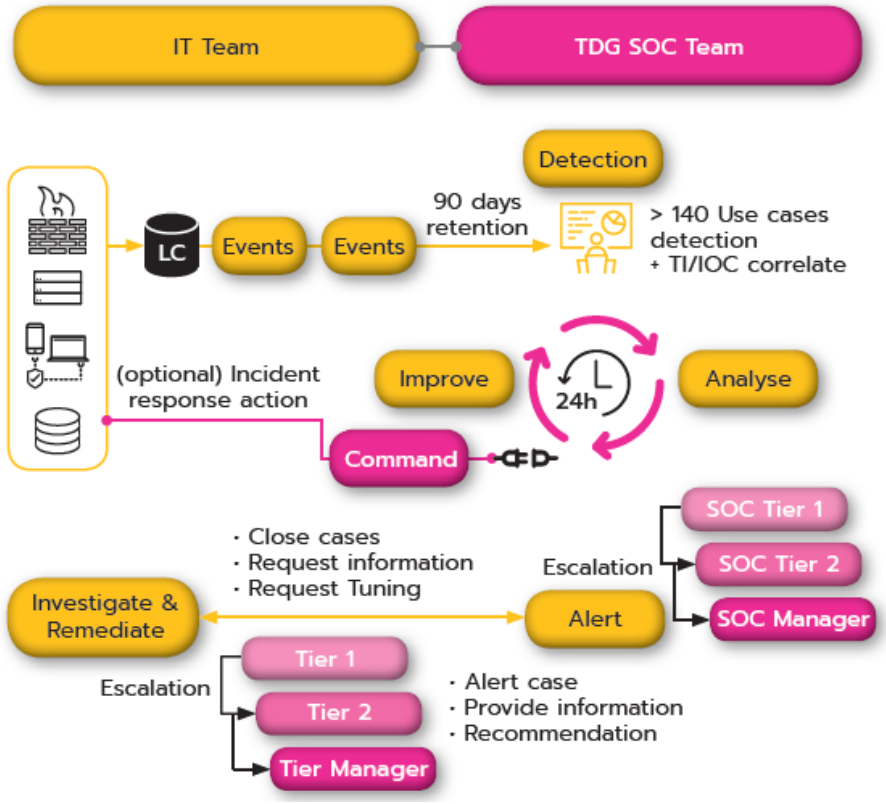
Policy accessibility	• **100%** employees, can access relevant policy through the organization's internal communications website.
Communication	• **100%** employee are trained and communicated the Policies, information, and practices through training, internal communication email, and bulletin.
Response Instruction	• **100%** alerts that alarm relevant parties to internet leakage, security breaches, or susceptible emails.
Testing	• Identity theft phishing simulation (Phishing Test) to test employee awareness
Disciplinary	• **100%** employee must be reviewed the performance of discipline that related to cyber security and data protection policy and acknowledged prior computer login as below picture.





The Security Operation Center (SOC)

The Company acknowledges the risks and has set up a 24-hour cyber security team to manage the Security Operation Center (SOC) with the objective of monitoring and responding to various threats in a timely manner under specified SLA and Charoen Pokphand Group information security standards.



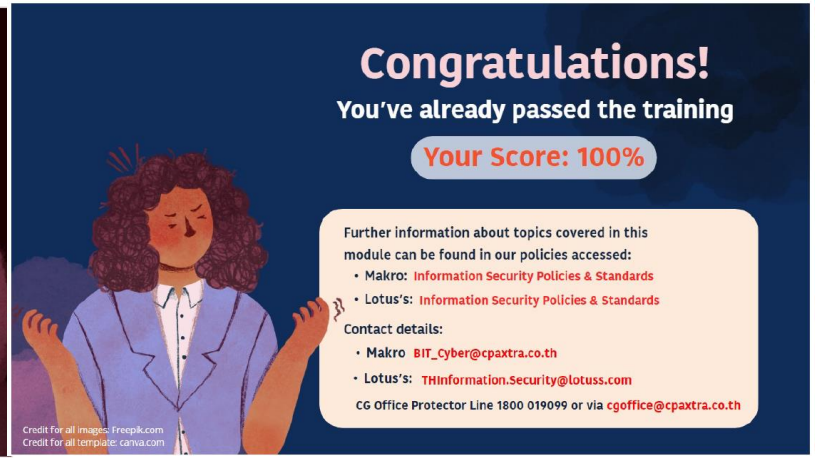
Cybersecurity Awareness Training

The Company has organized training of the cybersecurity policy, awareness of suspicious and proper responding instruction to all employees as annually basis. The training course provides techniques to notice the 4 key scam patterns which are:

1) Emotive content
2) Invalid links
3) Invalid sender email addresses
4) Invalid email attachments

Including the instruction to response whenever they notice suspicious email or incident.







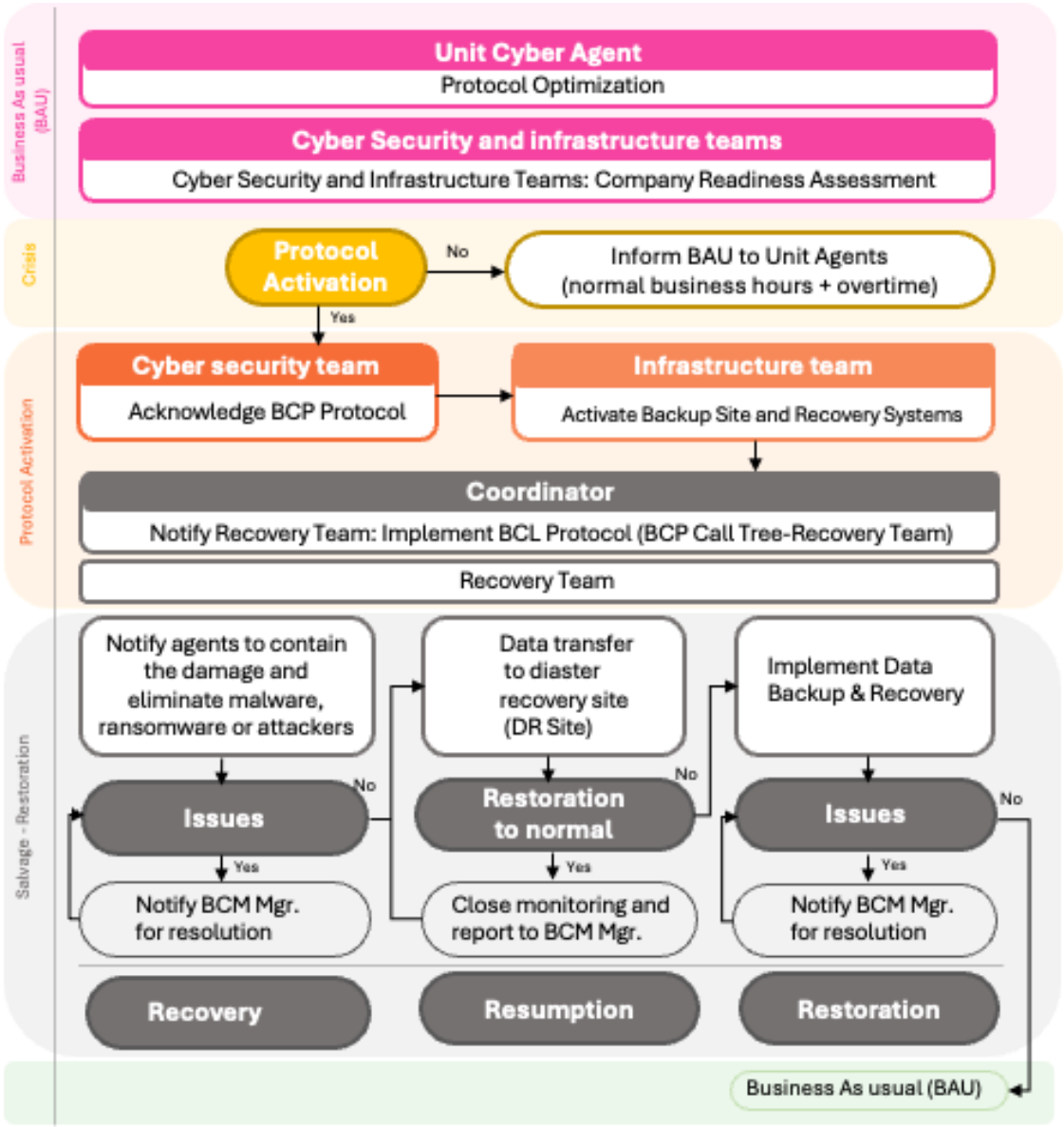


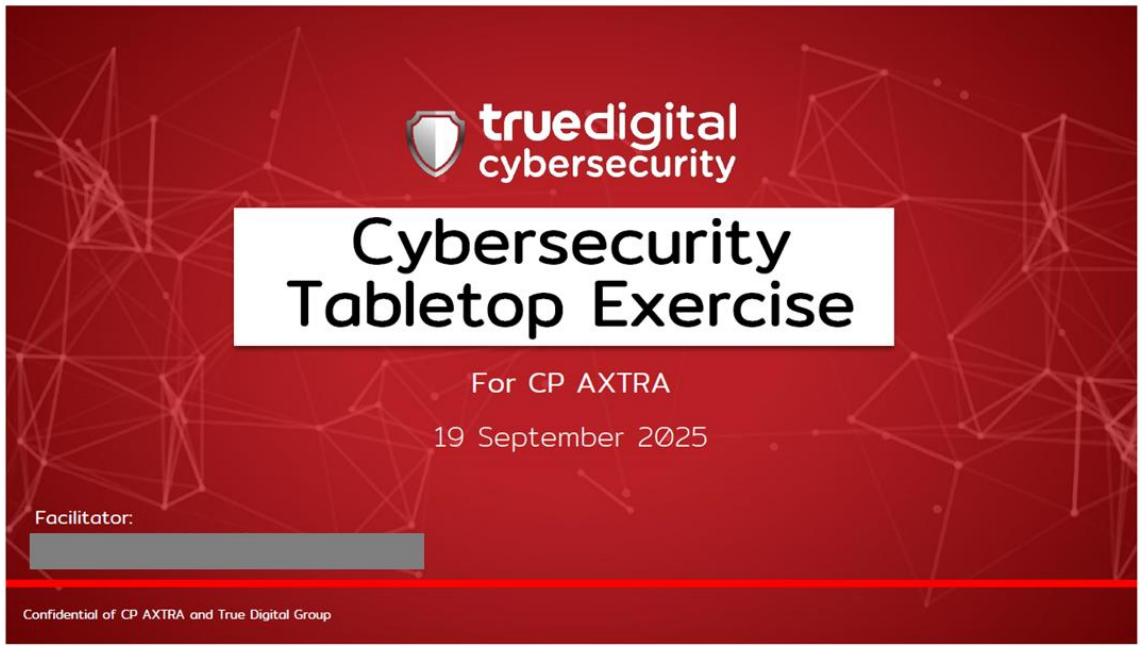
2025 Result:

- **2,953** trained employees (**100%**)
- **2,110** employees participated in email scam tests.
- **73%** has properly responded and **4%** reporting suspicious email.

Cybersecurity Business Continuity Plan

Following the framework of the ISO22301 to prepare for various crises that may occur and impact key business operations and the Company's risk management protocols. In 2025, the BCP drills are conducted twice.





"The simulation scenario on cybersecurity or data privacy incidents that may occur within the organization. It is designed to test the incident response plan and the coordination among teams, ensuring preparedness to effectively respond when an actual event occurs"

Verification and Vulnerability Analysis by External Party

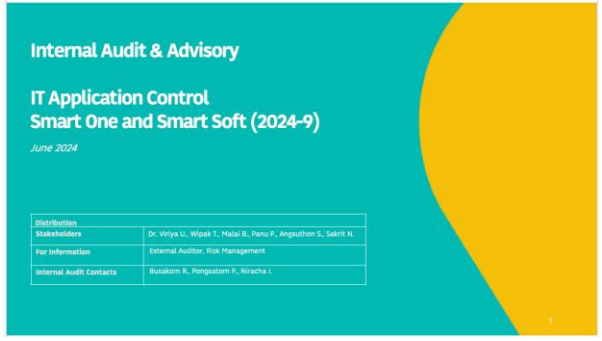
The company has conducted the external audit & Vulnerability Analysis by external party as NIST and external auditor to verity effectiveness of cybersecurity management system, infrastructure, and process.

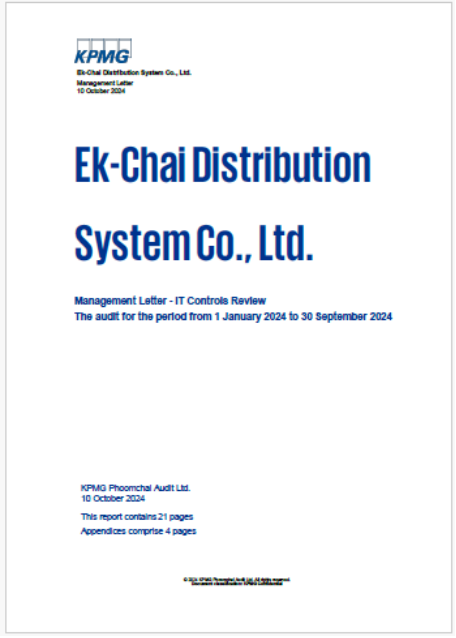
Internal Audit

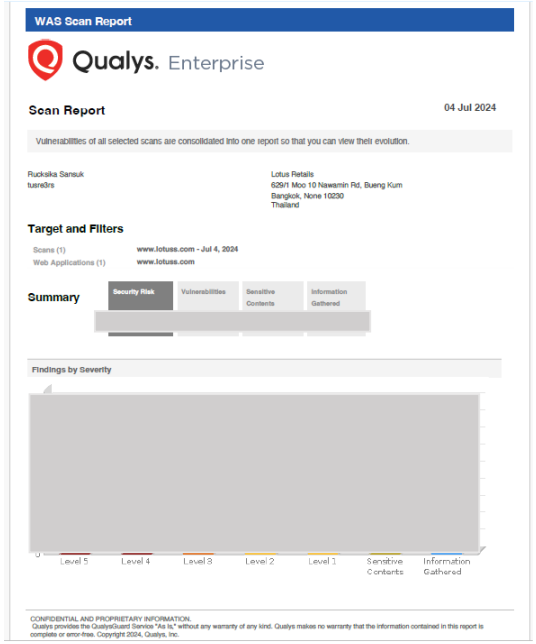
Infra-structure & management systems have been audited

Vulnerability analysis by third party

Simulated hacker attacks by third party





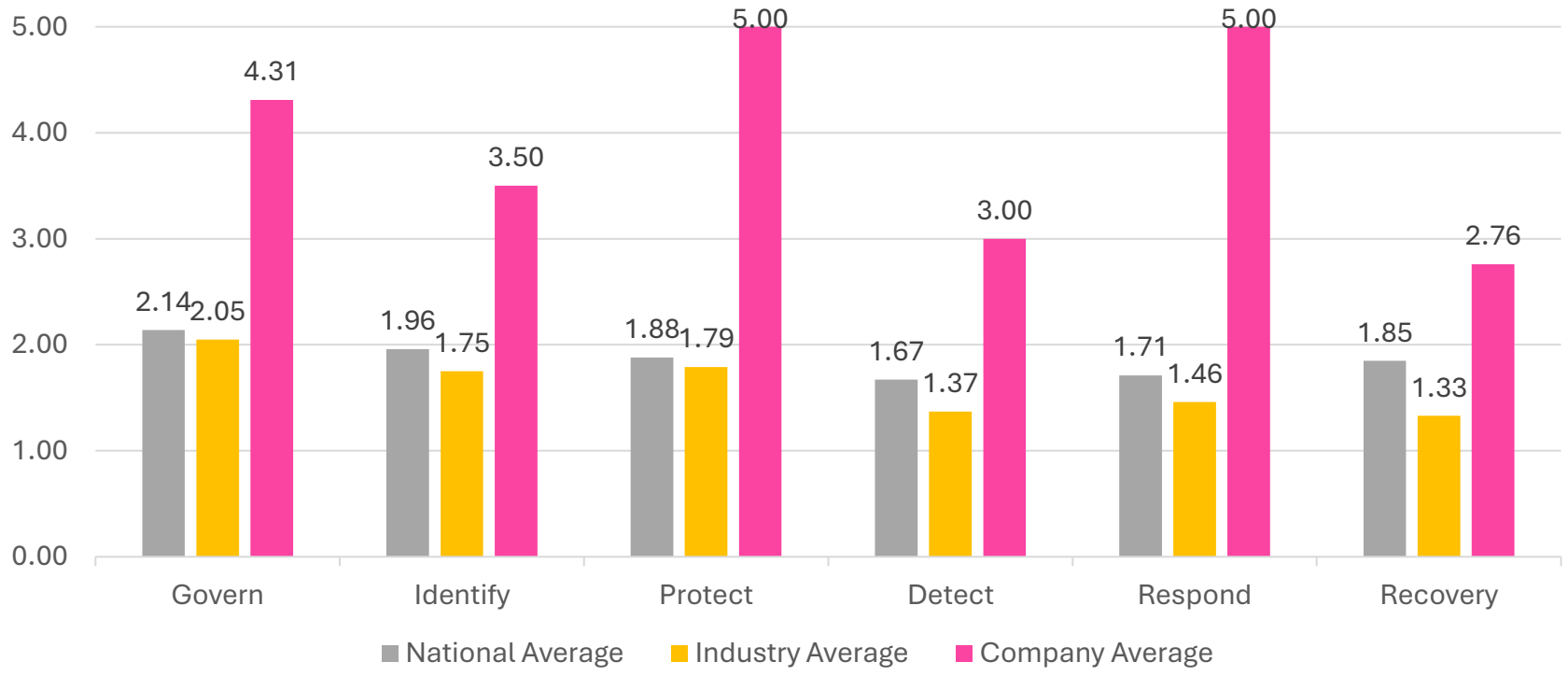


" See more details in page 12"

The NIST Function Rating by SEC

The Company participated the Cyber Security Assessment Program for Listed Companies under the Office of the Securities and Exchange Commission (SEC) and the NIST Cyber Security Framework that ranks organizational cyber security by readiness level. The program regularly verified the NIST Function's in 6 dimensions of Controlling system which are Govern, Identify, Protect, Detect, Respond, and Recovery for whole organization. The result shows the Company's score of **4.22** out of 5 levels which is highest rated comprising 202 of the companies that participated.

Score 4.22
Above NIST Function Average Rating



"Infrastructure Security Testing" (Hecker Attacks)

The Company hires the external party to simulate external hacker attacks (Red Teaming) to test the effectiveness of protection and evaluate the vulnerabilities in the system for improvement such as ASPX Debug Mode, Azure Domain Tenant, and Git-config Publicly Accessible.

2025 Result:

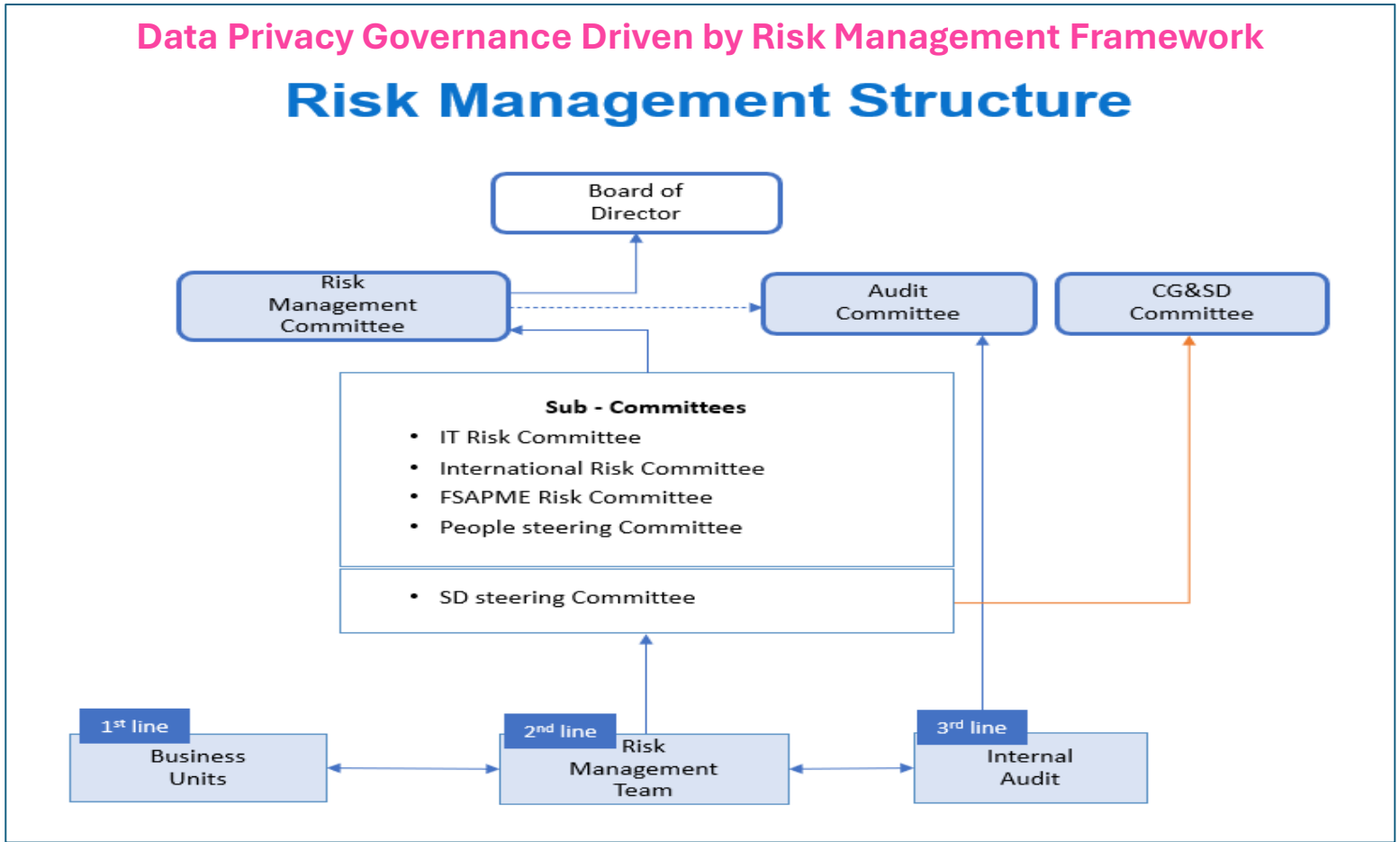
- **100%** passed the security system test on all topics.
- No incidents of damage from cyber-attacks.



DATA Privacy Protection

Governance

The Company has appointed a Data Protection Officer (DPO) with responsibilities to monitor and evaluate compliance with data protection laws, raise awareness and provide training on personal data practices, advise the Board, executives, and employees, act as the primary contact point for data subjects and the Personal Data Protection Commission, and maintain the confidentiality of personal data in the performance of duties. The DPO plays a pivotal role in governing privacy matters in close collaboration with relevant functions and senior management, who place strong emphasis on ensuring that privacy and data protection are taken seriously and embedded into the Company's governance and operations.



Data Privacy Protection Policy

Privacy policy is applied to the entire Company and its subsidiaries, supplier, vendor, contractor, including any foundations or funds established or to be established by the Company in the future. They are also applied to suppliers, where applicable, through contractual obligations and in compliance with the Personal Data Protection Act (PDPA). See more detail at https://www.cpaxtra.com/en/personal-data-protection-policy



1. Process personal data in a fair and lawful manner.
2. Process personal data in accordance with the purposes for which it was collected, used, or disclosed.
3. Ensure that personal data processed is adequate, relevant, and not excessive.
4. Ensure personal data is accurate and up-to-date.
5. Do not retain personal data longer than necessary.
6. Process data in accordance with individuals' rights to access and correct their data.
7. Ensure personal data is kept secure.
8. Personal data must not be transferred to countries with inadequate data protection standards, unless consent is obtained or as required by law.
9. Personal data must be used correctly and in a way that does not cause harm to the data subject.

Data Privacy Protection Management System

The Company implements measures to prevent unauthorized access and mitigate potential breaches of personal information. In line with the Personal Data Protection Act (PDPA), the Company prioritizes the protection of Personally Identifiable Information (PII) and has announced comprehensive Personal Data Protection Policy along with supplementary documents. Data management tools such as data classification and labelling for confidentiality, along with data loss prevention (DLP) systems, have been implemented to automatically detect and prevent potential data leakage.

The effectiveness of these measures is regularly monitored and reported, with statistical tracking such as the number of employees assessed, the number of employees found in breach of data protection requirements, and other relevant performance indicators. These monitoring results are consolidated and reported under the Company's risk management framework to ensure accountability and continuous improvement in line with international practices.

The Company also promotes a strong speak-up culture by providing multiple secure whistleblowing channels for employees and suppliers. Reports, including data privacy concerns, can be made confidentially and anonymously, with the option to use an independent third-party channel. All reports are treated with strict confidentiality, with a strong commitment to non-retaliation and the protection of whistleblowers' rights.

Action	2025 Result
Embedded in group-wide risk management	• The company has embedded the privacy policy in group wide risk management. The Risk Management Steering Committee (RMSC) as a working committee under the oversight of the Audit Committee. The RMSC supports the effective implementation of the corporate risk management framework, including oversight of privacy risk as part of the Company's significant corporate risks. By aligning with international practices, the RMSC enhances the Company's ability to manage risks proactively, promote accountability across functions, and provide assurance to the Audit Committee and the Board that key corporate risks are being effectively governed and monitored. • **100%** of data privacy risks were reviewed, and mitigation plans were identified.
Disciplinary actions in case of breach	• **100%** of employees were evaluated on compliance with company policies, including privacy policy, adherence through the disciplinary process as part of the annual performance review and year end bonus evaluation. • **100%** of employees, suppliers, and contractors were communicated with regarding incidents and responsibilities for personal data leakage in compliance with Personal Data Protection Act. • If any company personnel directly or indirectly violate or fail to comply with policies, practices, or measures, they will be subject to disciplinary action in accordance with the Company's work regulations.
Third-party audits of the privacy policy compliance	• **Completed** 3rd party audited. CLICK HERE *to external audit report on web*
Internal audits of the privacy policy compliance	• **100%** implementation of the privacy compliance program was audited as part of the annual internal audit plan.

Third-party audits of the privacy policy compliance by PDPC firm

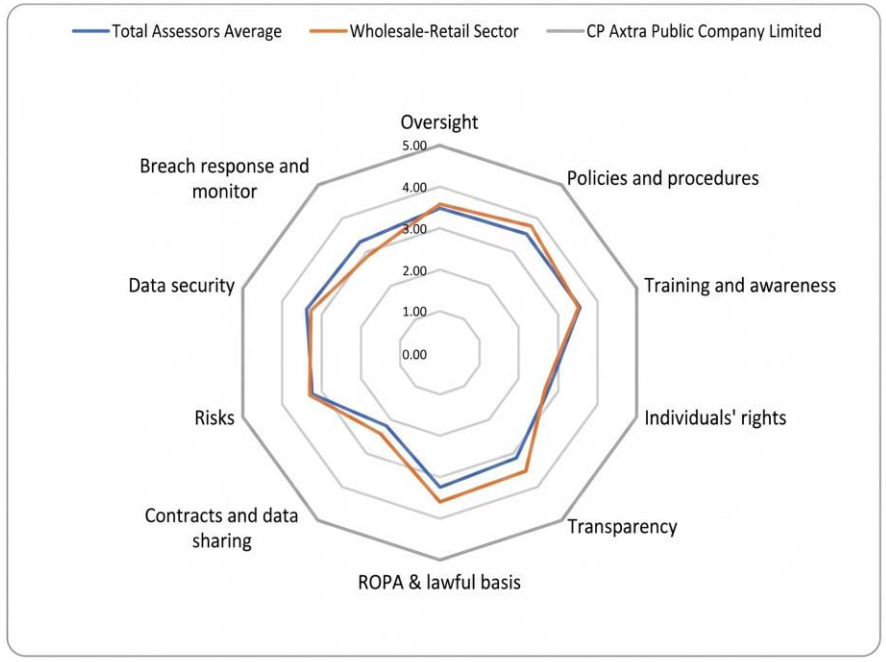
รายงานผลการประเมินระดับการคุ้มครองข้อมูลส่วนบุคคล

(Privacy Maturity Model)

บริษัท ซีพี แอ็กซ์ตร้า จำกัด (มหาชน)

External privacy policy compliance audit report:
Office of the Personal Data Protection Commission
Personal Data Protection Level Assessment Report (Privacy Maturity Model)
CP Axtra Public Company Limited.

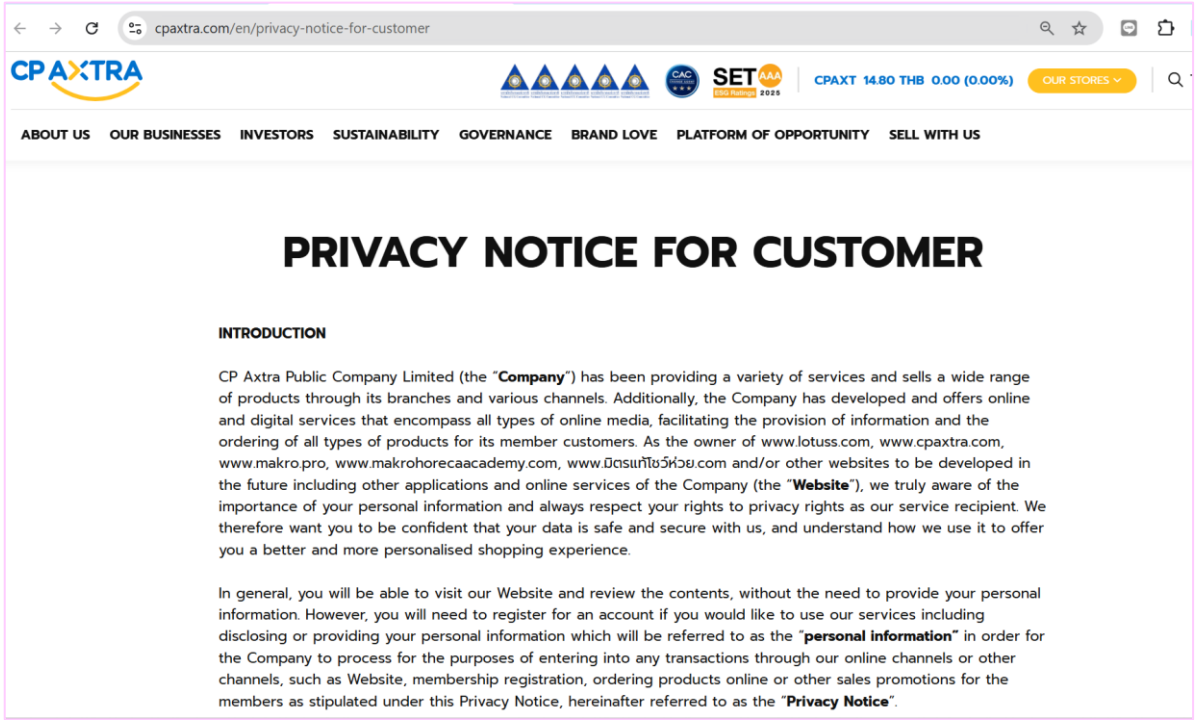
Evaluation Score 5.00 Points	Your current score is higher than the average score of all participating organizations. (Average score of all assessors is 3.18 points)	Your current score is higher than the average score in the Wholesale-Retail and Online Commerce group. (Average score for your industry group is 3.26 points)



Customer Privacy Notice

The Company places the highest importance on protecting our customers' personal data. In line with the Personal Data Protection Act (PDPA), we ensure transparency in how customer information is collected, used, disclosed, and safeguarded. Beyond compliance, our commitment reflects genuine care for our customers and stakeholders, ensuring their rights are respected and their trust is maintained. In our Privacy Notice for Customers, the topics below are covered:

- Scope of the Privacy Notice
- Personal Information We Collect When We Interact With Customers
- Purposes of Collection, Use and Disclosure
- Disclosure of Customer Personal Information
- Sending or Transfer of Customer Personal Information to Overseas
- Retention Period of Customer Personal Information
- Customer Rights
- Updating Customer Personal Information
- Security Measures for Customer Personal Information
- Marketing Research and Communications
- Cookies and Similar Technologies
- Redirecting to Other Parties' Websites
- Changes to the Privacy Notice
- Notification of Customer Data Breach and Leakage
- Contact Us
- Data Protection Officer



http://www.cpaxtra.com/en/privacy-notice-for-customer

2025 Result:

- **3%** of users whose customer data is used for secondary purpose.

Customer Privacy Notice



1. NATURE OF INFO CAPTURED

Personal Information We Collect…

Details categories of collected data: profiles, purchase history, device info.



2. USE OF COLLECTED INFO

Purposes of Collection, Use and Disclosure

Specifies primary objectives: enhance services, operations, customer experience.



3. OPT-OUT OPTION AVAILABLE

Customer Rights (Right to Object / Withdraw)

Ensures right to decline data processing or revoke consent.



4. OPT-IN CONSENT REQUIRED

Consent Basis

Explicit and proactive consent acquired prior to data collection.



5. REQUEST ACCESS TO DATA

Customer Rights (Right to Access)

Empowers customers to request access and obtain copies of held data.



6. REQUEST DATA PORTABILITY

Customer Rights (Right to Data Portability)

Request data in structured format and transfer to another controller.



7. REQUEST DATA RECTIFICATION

Customer Rights (Right to Rectification)

Channel for correcting inaccurate or incomplete personal information.



8. REQUEST DATA DELETION

Customer Rights (Right to Erasure / Deletion)

Request deletion or anonymization under legal conditions.



9. RETENTION PERIOD

Retention Period of Customer Personal Information

Strict timeframes and criteria for data retention.



10. INFORMATION PROTECTION

Security Measures for Customer Personal Information

Rigorous cybersecurity protocols, encryption, data protection.



11. THIRD-PARTY DISCLOSURE

Disclosure of Customer Personal Information

Transparentizes conditions, purposes, and entities for data sharing.



12. MONITORING SECONDARY USE

Percentage of users whose data is used for secondary purposes.

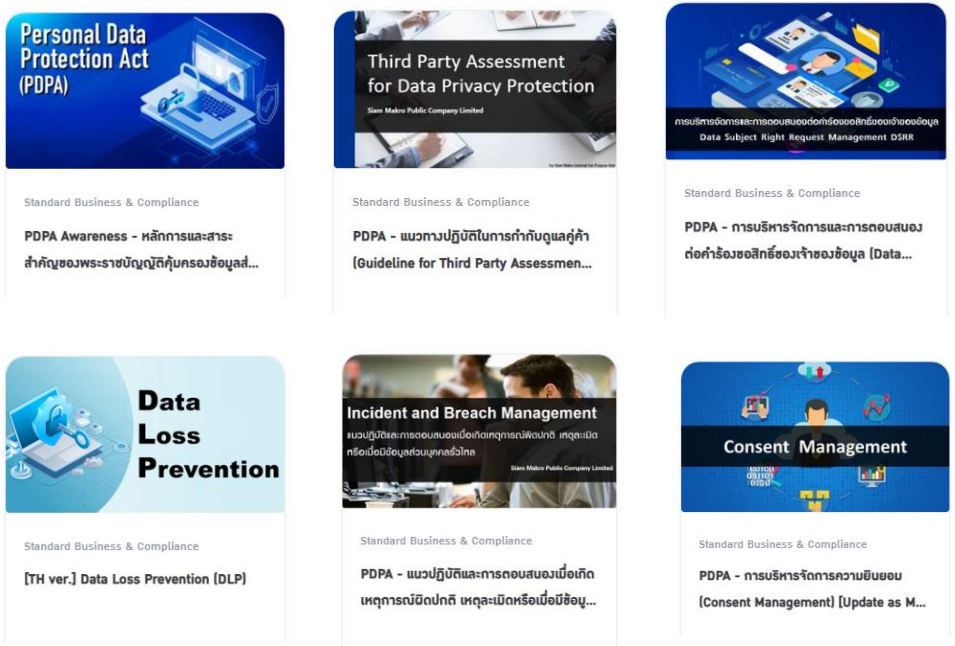
2025 RESULT: 3%

Remark: (*) means topic of privacy notice for customer which disclose at http://www.cpaxtra.com/en/privacy-notice-for-customer

Fostering Organization-Wide Commitment to Personal Data Privacy

The Company requires all employees to complete mandatory annual training with a 100% pass rate. In addition, a variety of e-learning modules are available throughout the year, enabling employees to refresh their knowledge and strengthen their understanding of data privacy and compliance at their own pace. The Company also extends privacy awareness to suppliers through contractual obligations aligned with the PDPA, including the Supplier Code of Conduct, as well as ongoing communication channels.

By fostering continuous learning among employees and reinforcing privacy awareness with suppliers, the Company ensures that the personal information of customers and stakeholders is protected with vigilance, accountability, and care.







2025 Result:

- **100%** employees completed mandatory annual training.
- **Zero** employees, suppliers, and contractors were impacted by any material data leakage or privacy breach cases.