science, engineering and health studies

Research Article

Science, Engineering and Health Studies
https://lio1.tci-thaijo.org/index.php/sehs
ISSN (Online): 2630-0087

M-SES: An online cybersecurity self-evaluation system to mitigate the risk of cybersecurity attacks in Thailand

*Narong Chaiwut and Worasak Rueangsirarak**

Computer and Communication Engineering for Capacity Building Research Center, School of Applied Digital Technology, Mae Fah Luang University, Chiang Rai 57100, Thailand

***Corresponding author**:
Worasak Rueangsirarak
worasak.rue@mfu.ac.th

Received: *20 May 2023*
Revised: *27 April 2025*
Accepted: *14 May 2025*
Published: *26 December 2025*

Citation:
Chaiwut, N., & Rueangsirarak, W. (2025). M-SES: An online cybersecurity self-evaluation system to mitigate the risk of cybersecurity attacks in Thailand. Science, Engineering and Health Studies, 19, 25020008.

ABSTRACT

Various preventive and responsive measures have been developed to mitigate the risk of cybersecurity attacks. Enhanced cybersecurity is now crucial to safeguard computer systems against malicious attacks. Implementation of the Personal Data Protection Act (PDPA) in June 2022 mandated compliance by all companies and government units operating in Thailand. Non-IT organizations have experienced significant challenges in adapting and meeting the requirements of this national regulation due to the time and resources required for comprehension and evaluation. This research proposed a novel online self-evaluation system (M-SES) for assessing compliance with the PDPA and related Thai cybersecurity legislation. The M-SES was developed based on a customized framework incorporating ISO/IEC 27001:2013, PDPA, and the Thailand Computer-related Crime Act (CCA). This tool was validated by ten experts from industrial and government sectors and comprised 26 cybersecurity controls. To mitigate the self-evaluation biases of the respondent users, this study adopted a web scraping technique to search for cybersecurity keywords in the data crawled from organizational websites. The final evaluation score was then calculated from the self-evaluation score and the web scraping score and an adjustment factor was applied to indicate the overall cybersecurity implementation status. The system prototype was tested using three organizations from different sectors, yielding cybersecurity implementation levels of one fully implemented and two moderate adoption. Our evaluation offers a practical and time-efficient approach to enable Thai companies to adapt to the national cybersecurity regulations.

Keywords: cybersecurity standard; ISO/IEC 27001:2013; Personal Data Protection Act (PDPA); Thailand Computer-related Crime Act (CCA); web scraping; implementation levels

1. INTRODUCTION

Computing devices such as smartphones and computers have now become important factors for daily living and connection to the expansive digital world. These technologies provide numerous benefits from leisure activities to online trading, social networking, and internet banking. However, the convenience of these technologies brings the risks of losing money and property. In 2019, 4.1 billion personal data records from various websites were

exposed to the public (Samsel, 2019), leading to an estimated economic impact of $6 billion due to security threats (Morgan, 2020).

Several methods have been proposed to protect application data including source code reviews (both static and dynamic analysis) and penetration testing (Shebli & Beheshti, 2018). Despite their popularity, these methods are time-consuming and costly, requiring experts to thoroughly review the software. As an alternative, many companies now adopt security standards to comply with national regulations (Sandfreni & Adikara, 2017; Nwafor et al., 2012). Security standards serve as guidelines to protect against and mitigate the effects of attacks. Prominent examples include ISO/IEC 27001:2013 by the International Organization for Standardization, NIST SP-800 from the National Institute of Standards and Technology, which provides best practices for information security management, and the COBIT 5.0 framework from ISACA (International Organization for Standardization, 2021; National Institute of Standards and Technology, 2021; ISACA, 2021).

The ISO/IEC 27001:2013 standard is comprehensive and widely recognized for its coverage of Information Security Management Systems (ISMS). However, implementing this framework can be time-consuming and costly, often taking almost a year and involving monthly meetings and extensive documentation (International Organization for Standardization, 2021; The British Standards Institution, 2021). The cost for small to mid-size businesses can exceed a million Baht (Thai Credit Guarantee Corporation, n.d.; Department of Disease Control, n.d.). Thailand enacted the Personal Data Protection Act (PDPA) in 2019 to safeguard personal data from unauthorized access and leakage (Personal Data Protection Act B.E. 2562, 2019). The PDPA outlines requirements for data collection, manipulation, and publication to protect user information collected for business purposes. Compliance with the PDPA is mandatory in Thailand but the regulations can be complex and time-consuming for non-IT practitioners to understand and implement (Tirumala et al., 2019; Jinquan et al., 2020). The challenges to implement security controls or standards include 1) lack of financial resources and 2) lack of cybersecurity knowledge and skills (Thamrongthanakit, 2023).

No guidance has been offered to help practitioners evaluate the cybersecurity risks. To bridge this gap, this research developed an online self-evaluation system to identify security weaknesses and assist companies to comply with the cybersecurity standards. The ISO/IEC 27001:2013, PDPA, and the Thailand Computer-Related Crime Act (CCA), encompassing 26 cybersecurity controls across three domains, were integrated as 1) organizational security policy, 2) personal data protection and access control, and 3) log management. Users evaluated their cybersecurity implementation at five levels ranging from 'unaware' to 'fully implemented', interpreted from the final security score calculated using the self-evaluation and web-scraping results. This system also provided users with assessments and suggestions to improve their business processes and data protection. The contributions of this study are explained below.

1. The security standards were mapped to create a new cybersecurity self-evaluation online questionnaire, combining the ISO/IEC 27001:2013, PDPA, and the Thailand CCA. This mapping simplified ISO/IEC 27001:2013, allowing timely compliance with Thailand's cybersecurity regulations. An online self-assessment system with 26 cybersecurity-standard controls was proposed to evaluate corporate implementation levels.
2. The self-evaluation bias was reduced by applying a web scraping technique together with natural language processing (NLP) to find existing security-related keywords elicited from each cybersecurity control on the official websites of user-provided URLs. This enhanced the reliability of the self-evaluation.
3. A description of each security level was interpreted from the security score, calculated using the adjustment factor technique on self-evaluation and web scraping data to provide suggestions for improvement regarding the 26 mapped cybersecurity standards.

2. MATERIALS AND METHODS

The initial stage for implementing an information security management system involved a "gap analysis", typically conducted as a paper-based evaluation of security domains. Experts or auditors then assessed the online security status of companies following the selected security standards (IT Governance, 2021). Nal-Karaki et al. (2022) developed an online application for cybersecurity assessment in the United Arab Emirates (UAE). They created a security index by mapping UAE national laws to ISO/IEC 27001:2013 standards and validated their method with the Institute of Applied Technology (IAT) in Abu Dhabi. Results confirmed company compliance with both international and local standards.

However, this UAE-based method cannot be applied in Thailand because of differences in national legal frameworks. Currently, no online self-evaluation or gap analysis tool is available in Thailand, presenting a challenge for non-IT businesses to align their operations to meet the national PDPA regulations. This study developed an accessible, easy-to-use cybersecurity evaluation survey system to assist companies to identify their necessary requirements.

A web-based self-evaluation system was proposed comprising two main components. First an online self-evaluation questionnaire generated from the cybersecurity controls and derived from the ISO/IEC 27001:2013, the PDPA, and the CCA with 26 cybersecurity controls. This proposed system used a web-scraping technique to investigate the existing cybersecurity keywords published on the company official websites to cross-check with survey input and reduce bias in the online questionnaire. Natural language processing was implemented to extract the information, reduce word ambiguity, and enhance the matching likelihood. Second, a cybersecurity implementation level was computed with scores ranging from 0 to 5 from the self-evaluation survey and web scraping using the adjustment factor calculation. Figure 1 shows an overview of the framework of the proposed system.

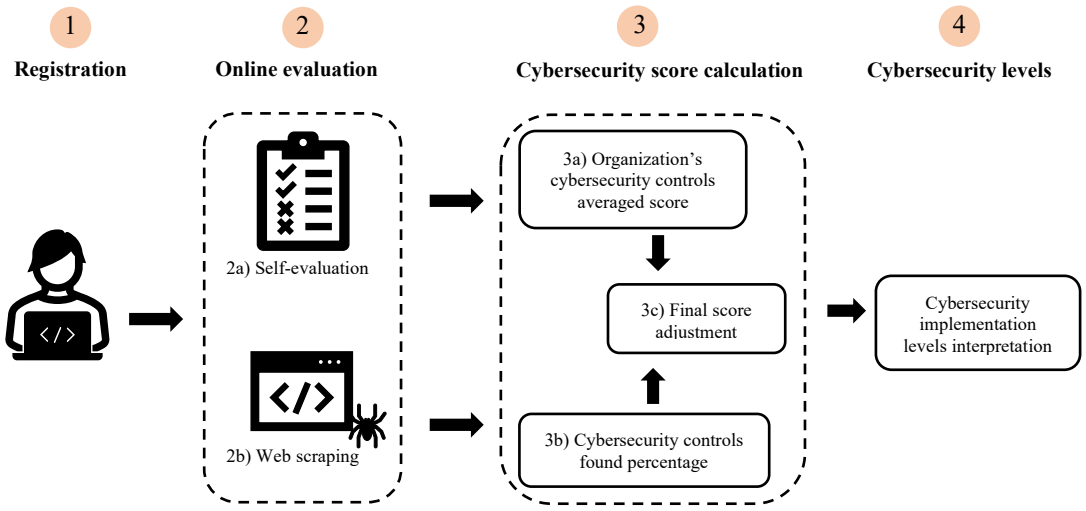

Figure 1. An overview of the proposed system

Our proposed cybersecurity self-evaluation system operates through a series of interconnected processes, as illustrated in Figure 1. Users first register their information such as name and company details, which are securely stored in the database (Figure 1). After logging in, users engage in an online assessment by completing a cybersecurity questionnaire consisting of 26 questions to evaluate various aspects of cybersecurity implementation. Simultaneously, to mitigate potential biases inherent in self-reported data, the system uses web scraping to crawl information from user-provided URLs of their official company websites, extracting cybersecurity-related keywords through NLP (Figure 1). The system next performs the cybersecurity score calculation on self-evaluation using the average score from the questionnaire and a percentage of cybersecurity controls, with keywords identified from the web scraping (Figure 1-3b). An adjustment factor is then applied to finalize the cybersecurity score and determine the cybersecurity implementation level. Our integrated approach ensured a nuanced and thorough evaluation of cybersecurity standard controls, balancing user-provided information with objectively gathered data. The following subsections detail the proposed methods.

2.1 Registration

Our system was implemented with Java and the Spring Boot framework as a web application that contained an online survey asking 26 questions about cybersecurity elicited from three distinguished standards. The web-scraping feature was used to investigate published information on the provided URLs of the users' official company websites. Most users created an account and provided information before starting the evaluation. The company URLs were used for the crawling process in web scraping.

2.2 Online evaluation

2.2.1 Users' self-evaluation of the cybersecurity questionnaire

The relevant security standards and acts were examined to create a time-efficient tool for cybersecurity self-evaluation that allowed companies in Thailand to comply with the PDPA directive, using the information security management system standard, ISO/IEC 27001:2013 (International Organization for Standardization, 2021) as a comprehensive security guideline. The PDPA and the CCA are mandatory acts that all Thai companies must follow. Table 1 compares the differences of involved security domains between each standard and related act. The first column presents the control indexes and security domains of ISO/IEC 27001:2013 Annex A, which encompasses 14 security domains on 114 security controls (hereafter, "ISO" refers to ISO/IEC 27001:2013). The second column represents the PDPA, which is a subset of the ISO's "Compliance: Internal and external" domain (A.18) and partially overlaps with the "Cryptography" domain (A.10). The third column depicts the CCA, which addresses cybersecurity activities and punishment terminology. Our comparison revealed that the CCA aligned with portions of the ISO's "Access control" (A.9), "Physical and environmental security" (A.11), and "Compliance: Internal and external" (A.18) domains.

Table 1 illustrates the PDPA and CCA cover on several security domains of the ISO, reflecting their objectives. The PDPA focuses on privacy and personal data protection, while the CCA addresses security-related criminal terminology and punishments. This observation led us to question, *"What is a suitable security evaluation that is both time-efficient for auditing and implementation?"* The ISO security standard comprises 14 security domains, including 114 security controls, but is not suitable for assessing all ISO security controls during a self-evaluation. The process is time-consuming, and not all security domains are mandated in Thailand. Therefore, we conducted a mapping process to reduce several security controls and Thailand's cybersecurity acts to identify the most dominant security domains that influenced others. This analysis revealed that "Information Security Policies" should be established first, as the other security domains could not be implemented without this foundation. The selected security domains, presented in Table 2, were adopted into the cybersecurity self-evaluation. The "Information Security Policies (A.5)" from the ISO served as a primary security domain in the questionnaire. The second component was derived from the PDPA, which

aligned with the "Compliance: Internal policies and External laws (A.18)" domain of the ISO. The "Access Control (A.9)" domain was also selected as corresponding to "Log Control and Management" in the CCA. Lastly, the "Physical and Environmental Security (A.11)" domain was selected to map with the "Physical and Access Control" of the CCA.

These security domains covered all cybersecurity aspects mentioned in Table 1, comprising the three mapped cybersecurity domains: Information Security Policies, Personal Data Protection, and Information Management. Twenty-six cybersecurity controls were incorporated into this cybersecurity self-evaluation framework and explained as follows.

Table 1. The security standards and related acts

ISO/IEC 27001:2013	PDPA	CCA
A.5 Information security policies	×	×
A.6 Organization of information security	×	×
A.7 Human resource security	×	×
A.8 Asset management	×	×
A.9 Access control	×	✓
A.10 Cryptography	partial	×
A.11 Physical and environmental security	×	✓
A.12 Operation security	×	×
A.13 Communication security	×	×
A.14 System acquisition, development and maintenance	×	×
A.15 Supplier relationships	×	×
A.16 Information security incident management	×	×
A.17 Information security aspects of business continuity management	×	×
A.18 Compliance: Internal such as policies and External such as laws	✓	✓

Table 2. Selected security domains for the new proposed cybersecurity self-evaluation

Control number	ISO/IEC 27001:2013	PDPA	CCA
Information security policies domain			
1	Information security policies (A.5)	×	×
Personal data protection domain			
2	Compliance: Internal such as policies, and external such as laws (A.18)	Personal Data Protection Act	×
Information management domain			
3	Access control (A.9)	×	Log control and management
4	Physical and environmental security (A.11)	×	Physical and access control

a) Information security policies domain

The cybersecurity controls within the information security policies domain evaluated company policy and the leadership's acknowledgment of cybersecurity. This domain played an important role as the core of cybersecurity governance, comprising five cybersecurity controls primarily derived from ISO/IEC 27001:2013 Annex A, as explained in Table A1 of Appendix A.

b) Personal data protection domain

This cybersecurity domain formed the main part of our self-evaluation. It addressed company mandatory compliance requirements and comprised four subdomains based on the PDPA as 1) data collection process, ensuring that companies obtained users' consent before collecting personal data; 2) data publishing evaluation, involving the consent process for transferring data to third parties; 3) data owner rights, addressing users' rights to access or delete their data; and 4) data protection officer, requiring staff members to manage data responsibly. Table A2 (in Appendix A) presents a comprehensive overview of these 14 controls comprising the four cybersecurity subdomains.

c) Information management domain

This cybersecurity domain, mapped from the CCA, regulated users' access to the systems and mandated appropriate log retention. There were two subdomains: 1) access control, which focused on limiting users' access to the system, and 2) log management, which involved controls for managing system logs. These subdomains encompassed seven controls, as explained in Table A3 of Appendix A.

d) Cybersecurity controls validation

To validate the comprehensiveness and practicality of our proposed cybersecurity self-evaluation tool against relevant Thai legislation, we invited cybersecurity experts from both industrial and government sectors to participate in the research. These experts had different working experiences in educational institutions, private sectors, and local municipalities. Ten experts responded and rated our survey for the proposed 26 mapped cybersecurity controls. The percent agreement method (Altman, 1991) was used to assess the inter-rater reliability and agreement among the raters. The experts could decide to

agree (1), be neutral (0), or disagree (-1) with the proposed cybersecurity controls across the three cybersecurity domains. Results showed an 89.29% agreement across all the raters for all items. This high level of agreement was further supported by a 98.93% agreement of all individual ratings (rated as 1). The discrepancy between these two percentages was due to a small number of items (3 answers out of 260 total rated answers) where one or two raters disagreed with the majority. We investigated some of the disagreements and discussed them with the raters. Results revealed that some raters were unfamiliar with certain cybersecurity controls, e.g., log management, which is a technical aspect and not a part of the PDPA regulation. Our results showed that the experts assessed these cybersecurity controls with almost unanimous agreement.

This process highlighted a clear understanding and unambiguous evaluation of the proposed questionnaire as an effective cybersecurity assessment tool. The final version of our proposed self-evaluation tool was distributed to companies to assess their compliance with the national cybersecurity legislation (Figure 1).

2.2.2 Web scraping

Web scraping is a technique used to extract interesting data from a website. Glez-Peña et al. (2014), and Kinne and Axenbeck (2019) showed the advantage of web scraping as affirmative data collection rather than using a questionnaire. This research used web scraping to collect data from company websites and employed this as a web mining resource to cross-check the questionnaire results (Figure 1). Mirtsch et al. (2021) used web scraping to extract ISO/IEC 27001:2013 certificate keywords from firms in Germany. Their findings revealed the reliability of data on official company websites, with keywords crawled on the web.

To prevent potential biases in the self-evaluation responses, we adopted the web scraping method utilized in Python together with a natural language toolkit (NLTK) (Loper & Bird, 2002) to extract and analyze website contents based on predefined keywords. This approach calculated the web scraping score corresponding to the proposed cybersecurity controls integrated into the questionnaire. Figure 2 shows the web scraping process and score generation, beginning with receiving the users' official company website address. Then, the web scraping sends a request to the provided URL to obtain an initial response from the targeted website before generating twenty unique hyperlinks to establish a crawler depth within the website's structure. These hyperlinks serve as entry points for crawling and extracting content from multiple pages across the website. In our proposed system, the content cleaning technique was applied to remove extraneous elements such as HTML and script tags. The refined data were consolidated into an output file, serving as the resource for the subsequent extraction of keywords.

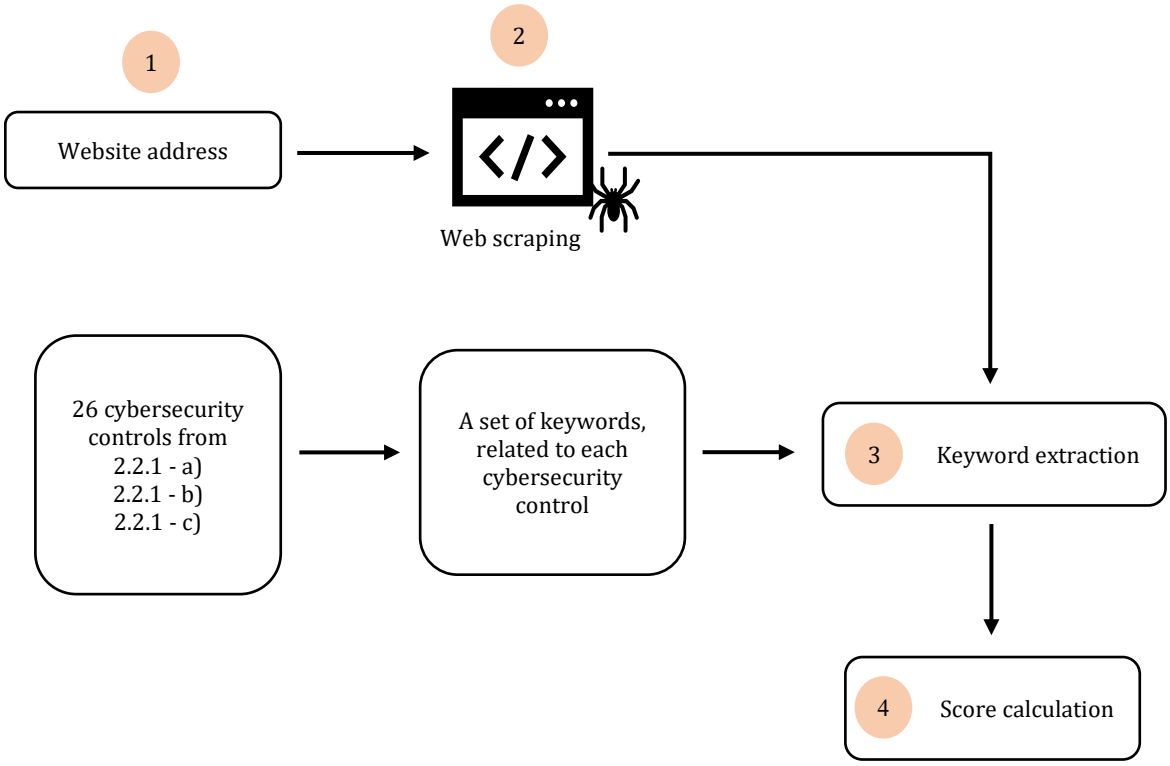

Figure 2. The proposed web scraping process

In Figure 2-3, the NLTK provides robust natural language processing to mitigate the false positives often associated with regex or simple string matching. The Thai language processing was performed using PyThaiNLP (Phatthiyaphaibun et al., 2023). The keyword extraction used 26 sets of provided keywords, related to each cybersecurity controller, to match with the crawled contents tokenized into sentences from the generated output file of the website's response message. A detailed breakdown of these keywords is shown in Table A4 of Appendix A. Both English and Thai keywords were used to target the cybersecurity controls. The calculation process was used to calculate a

score by matching the crawled sentences with the provided keywords for each cybersecurity control. If keywords were found, then a score of 1 was assigned for the cybersecurity control; otherwise, a score of 0 was assigned. We also manually verified the correctness by rechecking the sentences that contained keywords. The system repeated this process until all sets of keywords for the 26 cybersecurity controls were computed.

2.3 Cybersecurity score calculation

The data collected from both the users' self-evaluation and the web scraping process were converted to a unique score to define the cybersecurity implementation level. The operation was separated into three calculations (Figure 1) as follows.

a) Cybersecurity control average score

To identify the implementation levels of the 26 proposed cybersecurity controls, a ranking score system from 0 to 5 was used. This score indicated the level of cybersecurity implementation split into six levels as 'not performed', 'performed informally', 'planned', 'well-defined', 'quantitatively controlled', and 'continuously improving'. These indicators were adapted from research by Kinne and Axenbeck (2019), together with the ISO, and described in Table 3. This online self-evaluation required users to complete all 26 questions regarding the mapped cybersecurity controls. For each question, the users selected an answer that best reflected the level of cybersecurity implemented in their organization, ranging from 0 to 5. Then, the 26 self-evaluation answers were averaged using Equation 1:

$$Q = \frac{1}{n}\sum_{i=0}^{n} s_i \quad (1)$$

where;
Q is the cybersecurity average score.
n is the total number of cybersecurity controls.
i is a sequence of cybersecurity controls.
s is the score of cybersecurity implementation level in each control.

b) Web scraping score

To calculate the score from the web scraping results, we assigned a value of 1 if the keyword for that cybersecurity control was found. Otherwise, we assigned 0 if we could not match any related keywords of that cybersecurity control. The total score was then computed as an average of the 26 controls, representing the proportion of found cybersecurity controls with matched keywords relative to the total number of cybersecurity controls, and mathematically expressed as:

$$W = \frac{1}{n}\sum_{i=1}^{n} s_i \quad (2)$$

where;
W is the web scraping score.
Si is the number of found cybersecurity controls.
n is the total number of cybersecurity controls.

Table 3. Evaluation score levels for each cybersecurity control (Kinne & Axenbeck, 2019)

Level scores	Implementation stages in ISO/IEC 27001:2013	Definition
0	Not performed	The controls and security plans are non-existent.
1	Performed informally	The control area's fundamental procedures are often carried out on an as-needed basis.
2	Planned	The control area's fundamental security requirements are planned, carried out, and repeated.
3	Well defined	The processes are more developed than Level 2, repeatable, approved, and applied across the entire organization.
4	Quantitatively controlled	The process is gauged and confirmed (e.g., auditable).
5	Continuously improving	The standard procedures are continuously updated and revised.

c) Final score adjustment

The final cybersecurity score represented the total score combining the questionnaire averaged score and web scraping score, calculated using an adjustment factor. First, we scaled the web scraping score to within a range of 0–5. Due to some limitations in our web scraping process, we could not extract the text from images and from all pages of a website; therefore, we optimized the adjustment factor to a weight of 30%. This approach best balanced the self-evaluation average score. Then, we set up the interval of the final cybersecurity score calculation from 0 to 5. The pseudo code below explains how the adjustment factor was applied for the final score calculation.

Let:

- *Q = Self-evaluation averaged score (range: 0.0–5.0)*
- *W = Web scraping score (range: 0.0–1.0)*
- *α = Adjustment percentage (e.g., 0.30 for 30%)*

Then:

1. *Scale the web scraping score (W'): W' = W * 5*
2. *Adjustment factor (AF): AF = α(W' - Q)*
3. *Adjusted score (AS): AS = Q + AF*
4. *Final adjusted score (FAS): FAS = max(0, min(AS, 5))*

where:

- *max(0, x) ensures the score is not negative*
- *min(x, 5) ensures the score does not exceed 5*

2.4 Cybersecurity score interpretation

The system ultimately adjusted the final score for each company categorized into five distinct cybersecurity implementation levels. This final score was classified into cybersecurity adoption levels, as illustrated in Table 4. The cybersecurity implementation levels were distinguished as 1) unaware: no cybersecurity controls were implemented, 2) partial adoption: cybersecurity controls were implemented in an ad-hoc manner, 3) moderate adoption: cybersecurity controls were planned and are being implemented but with no monitoring measures, 4) almost complete adoption: the cybersecurity controls based on planning

were implemented, and 5) fully implemented: all cybersecurity controls were implemented and evaluated. This approach offered companies a clear understanding of their current cybersecurity implementation stage and the actionable insights required to enhance their cybersecurity performance.

Table 4. The cybersecurity implementation stages classified using the cybersecurity level final score (modified from Nal-Karaki et al., 2022)

Cybersecurity implementation levels	Score	Definition
Unaware	0.1–1.0	No cybersecurity controls were implemented.
Partial adoption	1.1–2.0	Cybersecurity controls were implemented on an ad-hoc basis with no security planning.
Moderate adoption	2.1–3.0	Planning and follow-up of cybersecurity controls were implemented but with no control.
Almost complete adoption	3.1–4.0	Cybersecurity controls were implemented based on planning.
Fully implemented	4.1–5.0	Cybersecurity controls were evaluated and improved.

3. RESULTS AND DISCUSSION

3.1 Experimental results

We tested our proposed cybersecurity self-evaluation system using only one educational organization when Thailand's PDPA was first established in late 2021. We also invited a provincial hospital and a local municipality to participate in this research in July 2024, representing different operational sectors.

Each organization was asked to access our online self-evaluation system. This system was user-friendly and comprehensive, allowing the company representatives to complete the assessment at their convenience. We reached out to the key personnel who possessed a thorough understanding of their respective IT infrastructures, cybersecurity protocols, and operational procedures.

The first organization, coded as org-001, was an information technology support unit in the educational sector and the main department responsible for managing and maintaining IT infrastructure and services. This department employed 50 professional staff, including software developers, database administrators, and network engineers. Their main responsibility was to ensure the smooth operation of IT systems, with oversight from the board, to perform activities following institutional goals and regulations.

The second organization, invited in July 2024 and designated as org-002, was a large provincial hospital center in the area employing over a thousand healthcare workers, including medical professionals, administrative personnel, and support staff. The hospital attended to more than five thousand patients who visited regularly. The sensitive nature of healthcare data and the critical importance of maintaining patient privacy and system integrity presented a unique set of challenges and requirements for IT security and data protection.

The third organization invited to join the research in July 2024 was a local municipality, coded as org-003, responsible for providing a wide range of services to a city with a residential population of around 11,000. Municipal services typically include urban planning, public safety, taxing, waste management, and various administrative functions, and the IT infrastructure must be robust to handle diverse operations while ensuring the security and privacy of citizen data.

The diverse nature of the three participating organizations, spanning education, healthcare, and local government sectors, allowed us to test the effectiveness and applicability of our proposed cybersecurity self-evaluation system across varied operational contexts. Each sector presented unique challenges and regulatory requirements, providing valuable insights into the versatility and robustness of our proposed system. Table 5 summarizes the experimental results for each organization's cybersecurity implementation level calculated using our proposed system and presented in Figure 1. Org-001a was invited to join the study in 2021. Their final cybersecurity score was 1.4, indicating a partial implementation level, and explained their situation at the start of Thailand's PDPA enactment. They received 1.4 for information security policies, 0.7 in personal data protection, and 2.1 in information management but 0.0 for web scraping. The low web scraping score reflected the lack of knowledge in how to implement the upcoming PDPA, while the first version of our proposed web scraping technique matched the core keywords of the standard to the crawled data to identify an existing standard, with no matches found on their official website in 2021. However, for org-001b, the latest experiment in July 2024 showed an improvement in proposed web scraping (Figure 2), and their official website was updated to include regards the national cybersecurity regulation. Org-001b achieved an average self-evaluation score of 4.5 from a senior member of the institution, with cybersecurity scores of 4.4, 4.3, and 4.7 for each cybersecurity domain. The web scraping also showed a high score of 0.6 after crawling their official website, which provided a main page showing published PDPA policies and regulations as support for all company members. The final cybersecurity score of 4.1 indicated that this organization had fully implemented cybersecurity standards with frequent re-evaluation and improvement of all cybersecurity controls.

The second organization (org-002) from the healthcare sector achieved an average overall self-evaluation score of 2.4, with 2.4 in information security policies, 2.0 in personal data protection, 2.9 in information management, and 0.6 in web scraping. With a final cybersecurity score of 2.6, this organization had a moderate level of cybersecurity adoption; they planned and followed the national regulations but did not employ any staff to take care of this concern.

The third organization invited to participate in this experiment, org-003, was a local municipality storing residential data such as income, properties, and tax history. This institution achieved an average score of 2.5 for the self-evaluation, calculated from three domains of 2.3 in information security policies 2.7 in personal data protection and 2.6 in information management. Their web scraping score was 0.2, with scant cybersecurity policy detailed on their website. This organization achieved a final cybersecurity score of 2.1, showing a moderate level of cybersecurity adoption.

Table 5. Results from the proposed cybersecurity domains using a 30% adjustment percentage (α = 0.3)

No.	Security domain	Organization			
		org-001 (a)*	org-001 (b)	org-002	org-003
1.	Online self-evaluation				
1.1	Information security policies	1.4	4.4	2.4	2.3
1.2	Personal data protection	0.7	4.3	2.0	2.7
1.3	Information management	2.1	4.7	2.9	2.6
1.4	Average self-evaluation score	1.4	4.5	2.4	2.5
2.	Web scraping	0.0**	0.6	0.6	0.2
3.	Final cybersecurity score	1.4	4.1	2.6	2.1
4.	Interpreted implementation level	Partially	Fully	Moderate	Moderate

Note: * org-001(a) and org-001(b) are two different results from the same organization at different times: org-001(a) was tested in late 2021, while 001(b) was tested in July 2024.
** org-001(a) used a different technique for web scraping by searching with core keywords, e.g., "certified by ISO27001" while 001(b) used our proposed technique in Figure 2.

The variation in self-evaluation scores across these three organizations is noteworthy and may warrant further investigation into the effectiveness of our proposed self-evaluation system in different cybersecurity situations. The web scraping results revealed significant differences in publicly available cybersecurity information, with only org-001 and org-002 showing cybersecurity content on their websites.

3.2 Discussion

The cybersecurity implementation status of each invited institution was analyzed. The IT support unit of the educational institute, org-001, was first classified as partial cybersecurity adoption in 2021 and then later classified as fully implemented cybersecurity in July 2024. Org-001 applied and implemented all cybersecurity controls and achieved high scores following our proposed self-evaluation system. After manual investigation and analysis, the ISO/IEC 27001:2013 certification was awarded to this organization in 2023. They also established a new Data Protection Officer (DPO) department, responsible for providing and regulating personal data protection. Cybersecurity policy information is published on their official website, showing enhanced transparency and reliability for stakeholders. Our web scraping method confirmed that more than 60% of cybersecurity controls were mentioned on their website, with the majority as personal data protection domains.

The invited provincial hospital, org-002, was classified at the moderate adoption level of cybersecurity. Org-002 had established cybersecurity policies, but these required a thorough evaluation and improvement to enhance their effectiveness. The personal data protection domain was only partially implemented at the time of this experiment. This lack of implementation was attributed to the unclear regulations and the absence of a definitive direction within the organization. In spite of this, org-002 recorded an acceptable score of 2.9 in the information management domain, suggesting significant implementation of the CCA requirements, with partial access control and log management. The relatively robust implementation in this domain reflected that the CCA had been promulgated for several years before our experiment, allowing time for adaptation. By contrast, the web scraping results showed that more than half of the cybersecurity controls were found on their website. As with org-001, most of the published information was related to personal data protection domains. As a result, they under-evaluated their cybersecurity controls during self-evaluation following our proposed system, and this led to a slight enhancement in the final cybersecurity score after computing the adjustment (Figure 2-4).

The final cybersecurity score of org-003 was at the moderate implementation level, aligning with their established policies for cybersecurity control in the PDPA domains with evidence of log management. However, web scraping found only one URL dedicated to the PDPA of their institution. Further analysis confirmed that org-003 only employed one IT officer who was invited to participate in this experiment. Like org-002, org-003 has not yet fully implemented cybersecurity controls.

To enhance cybersecurity aspects and public trust, org-002 and org-003 should 1) develop and implement a comprehensive cybersecurity planning process, 2) address the gaps in personal data protection implementation, and 3) regularly assess and improve existing cybersecurity policies. However, org-003 showed increased transparency by publishing appropriate cybersecurity-related information on its official website. Following these three steps would improve the cybersecurity implementation levels of org-002 and org-003 and enhance their reliability in the eyes of stakeholders and the general public.

4. CONCLUSION

This research proposed a novel online self-evaluation tool to assess institutional cybersecurity implementation levels. Our online tool integrated key elements from

ISO/IEC 27001:2013, focusing on information security policies, along with the requirements of the PDPA and the CCA. This integration resulted in a comprehensive and tailored cybersecurity evaluation.

Our proposed online system comprised two features: a cybersecurity self-evaluation consisting of 26 cybersecurity controls, categorized into three primary cybersecurity domains, and a web scraping function that extracted cybersecurity-related keywords from established websites, serving to mitigate potential biases in user self-evaluation. The final cybersecurity score was derived from an adjustment calculation incorporating the results of both features to provide a more reliable cybersecurity implementation status assessment.

To validate the efficiency of the system, we conducted experiments with three organizations invited from diverse sectors. Twenty-six cybersecurity controls were proposed and integrated into an online questionnaire which was validated by ten experts. One of the three invited organizations was classified as fully implemented, with certification from the well-known ISO security standard, while the other two earned a moderate adoption level, with a lack of understanding about the cybersecurity acts and limited equipment and labor resources. They also lacked representation of cybersecurity-related information on their official websites. This discrepancy significantly impacted their perceived reliability among stakeholders. Our proposed system could be adopted as an assessment framework to indicate the status of cybersecurity control implementation in Thai companies.

ACKNOWLEDGMENTS

This research was financially supported by the Reinventing University System 2021 at Mae Fah Luang University and by the Computer and Communication Engineering for Capacity Building Research Center, School of Applied Digital Technology, Mae Fah Luang University. The authors would like to thank all the participants from the public and private sectors for their support and feedback. This study was approved by the MFU Ethics Committee on Human Research, approval no. 22093-13.

REFERENCES

Altman, D. G. (1991). *Practical statistics for medical research*. CRC Press.

Department of Disease Control. (n.d.) *ISMS based on ISO/IEC 27001:2013 cost estimation*. https://ddc.moph.go.th/uploads/files/1709020210219105509.pdf [in Thai]

Glez-Peña, D., Lourenço, A., López-Fernández, H., Reboiro-Jato, M., & Fdez-Riverola, F. (2014). Web scraping technologies in an API world. *Briefings in Bioinformatics*, *15*(5), 788–797. https://doi.org/10.1093/bib/bbt026

International Organization for Standardization. (2021). *ISO/IEC 27001: Information security management*. https://www.iso.org/isoiec-27001-information-security.html

ISACA. (2021). *COBIT: An ISACA framework*. https://www.isaca.org/resources/cobit

IT Governance. (2021). *ISO 27001 gap analysis*. https://www.itgovernance.co.uk/iso-27001-gap-analysis

Jinquan, J., Al-Absi, M. A., Al-Absi, A. A., & Lee, H. J. (2020). Analysis and protection of computer network security issues. In *Proceedings of the 22nd International Conference on Advanced Communications Technology (ICACT)* (pp. 577–580). IEEE. https://doi.org/10.23919/ICACT48636.2020.9061266

Kinne, J., & Axenbeck, J. (2019). *Web mining of firm websites: A framework for web scraping and a pilot study for Germany*. SSRN. https://doi.org/10.2139/ssrn.3240470

Loper, E., & Bird, S. (2002). *NLTK: The natural language toolkit*. arXiv. https://arxiv.org/abs/cs/0205028

Mirtsch, M., Kinne, J., & Blind, K. (2021). Exploring the adoption of the international information security management system standard ISO/IEC 27001: A web mining-based analysis. *IEEE Transactions on Engineering Management*, *68*(1), 87–100. https://doi.org/10.1109/TEM.2020.2977815

Morgan, S. (Ed.). (2020, November 13). Cybercrime to cost the world $10.5 trillion annually by 2025. *Cybercrime Magazine*. https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/

Nal-Karaki, J. N., Gawanmeh, A., & El-Yassami, S. (2022). GoSafe: On the practical characterization of the overall security posture of an organization information system using smart auditing and ranking. *Journal of King Saud University - Computer and Information Sciences*, *34*(6 Part A), 3079–3095. https://doi.org/10.1016/j.jksuci.2020.09.011

National Institute of Standards and Technology. (2021). *Security best practices*. https://www.nist.gov/itl/voting/security-best-practices

Nwafor, C. I., Zavarsky, P., Ruhl, R., & Lindskog, D. (2012). A COBIT and NIST-based conceptual framework for enterprise user account lifecycle management. In *Proceedings of the World Congress on Internet Security (WorldCIS-2012)* (pp. 150–157). IEEE. https://ieeexplore.ieee.org/abstract/document/6280218

Personal Data Protection Act B.E. 2562. (2019, May 27). *Royal Thai Government Gazette*. No. 136 Special Section 69 A. pp. 52–95. https://ratchakitcha.soc.go.th/documents/17082307.pdf [in Thai]

Phatthiyaphaibun, W., Chaovavanich, K., Polpanumas, C., Suriyawongkul, A., Lowphansirikul, L., Chormai, P., Limkonchotiwat, P., Suntorntip, T., & Udomcharoenchaikit, C. (2023). PyThaiNLP: Thai natural language processing in Python. In L. Tan, D. Milajevs, G. Chauhan, J. Gwinnup, & E. Rippeth (Eds.), *Proceedings of the 3rd Workshop for Natural Language Processing Open Source Software (NLP-OSS 2023)* (pp. 25–36). Association for Computational Linguistics. https://doi.org/10.18653/v1/2023.nlposs-1.4

Samsel, H. (2019, August 22). *With 4.1 billion records exposed in six months, 2019 is on course to be record year for data breaches*. Security Today. https://securitytoday.com/articles/2019/08/22/with-4.1-billion-records-exposed-in-six-months-2019-is-on-course-to-be-record-year-for-data-breaches.aspx

Sandfreni, S., & Adikara, F. (2017). Capability level assessment of IT governance in PTP Mitra Ogan: COBIT 5 framework for BAI 04 process. In *Proceedings of the 4th International Conference on Computer Applications and Information Processing Technology (CAIPT)* (pp. 1–5). IEEE. https://doi.org/10.1109/CAIPT.2017.8320665

Shebli, H. M. Z. A., & Beheshti, B. D. (2018). A study on penetration testing process and tools. In *Proceedings of*

the 2018 IEEE Long Island Systems, Applications and Technology Conference (LISAT) (pp. 1–7). IEEE. https://doi.org/10.1109/LISAT.2018.8378035

Thai Credit Guarantee Corporation. (n.d.). *ISMS based on ISO/IEC 27001 cost estimation*. https://www.tcg.or.th/uploads/file/ประกาศเปลี่ยนแปลงราคากลาง%20จ้างที่ปรึกษา%20iso%202565-ประกาศ.pdf [in Thai]

Thamrongthanakit, T. (2023). *Impacts of cybersecurity practices on cyberattack damage and protection among small and medium enterprises in Thailand* [Master's thesis, Stockholm University]. Digitala Vetenskapliga Arkivet. https://www.diva-portal.org/smash/get/diva2:1784412/FULLTEXT01.pdf

The British Standards Institution. (2021). *BSI Thailand*. https://www.bsigroup.com/th-TH/ [in Thai]

Tirumala, S. S., Valluri, M. R., & Babu, G. (2019). A survey on cybersecurity awareness concerns, practices and conceptual measures. In *Proceedings of the 2019 International Conference on Computer Communication and Informatics (ICCCI)* (pp. 1–6). IEEE. https://doi.org/10.1109/ICCCI.2019.8821951

Appendix A

Table A1. Information security policy domain and cybersecurity controls (International Organization for Standardization, 2021)

Controller number	Details
Organization aspects	
1	The company must identify both internal and external challenges that are pertinent to its goals and have an impact on its capacity to carry out the information security management system's planned outcome(s).
2	The organization shall determine: a) parties with an interest in the information security management system; and b) the information security requirements of these interested parties.
3	According to the specifications of this International Standard, the business must create, implement, maintain, and constantly enhance an information security management system.
Leadership aspects	
4	Top management must lead by example and show dedication to the information security management system.
5	The top management must see to it that roles with responsibilities for information security are assigned and communicated.

Table A2. Personal data protection domains and cybersecurity controls (Personal Data Protection Act, 2019)

Controller number	Details
Personal data collection	
6	Unless it is impossible by nature, a request for consent must be given expressly in writing or electronically.
7	The consent of the data subject may be withdrawn at any time.
8	The consent of the person who has parental responsibility for the minor must be obtained in cases where the minor is under the age of ten.
9	The Personal Data Controller must explain the reason for collecting, using, or disclosing the Personal Data to the data subject when seeking their consent.
10	The Data Controller must notify the data subject of the following information prior to or at the time of the collection of their personal information, unless they are already aware of it. a) the reason for collecting the personal data, including any use or disclosure allowed by section 24 of the act that involves collecting the data without the subject's consent. b) notification of situations in which the data subject must disclose personal information in order to comply with a law, a contract, or in order to enter into a contract, as well as notification of the potential consequences if the data subject does not supply the requested personal information; c) The personal information to be gathered and the time frame in which it will be kept. d) Communication channel to the data collector.
11	Without the subject's express consent, it is forbidden to collect any Personal Data pertaining to race, ethnic origin, political opinions, cult, religious or philosophical beliefs, sexual behavior, criminal records, health information, disability, trade union information, genetic information, biometric information, or any other information that may have an impact on the data subject in the same way.
Data disclosure	
12	Unless the Personal Data was gathered without the need for consent, the Data Controller may not use or disclose Personal Data without the approval of the data subject.
13	The destination country or international organization that receives the Personal Data must have an acceptable level of data protection if the Data Controller sends or transfers the Personal Data to a foreign jurisdiction.
Rights of the data subject	
14	The data subject has the right to ask for access to and a copy of any personal information about them that the data controller is in charge of maintaining.
15	The data subject has the right to object at any time to the collection, use, or disclosure of personal information about him or her.
16	The data subject has the right to ask the data controller to delete or otherwise dispose of their personal information.
The data protection officer	
17	Advising the Data Controller or the Data Processor on how to comply with this act, as well as the employees or service providers of the Data Controller or the Data Processor.
18	Examine the actions taken by the Data Controller or the Data Processor, as well as their employees or service providers, with regard to the gathering, using, or disclosing of Personal Data to determine whether they are in conformity with this act.
19	In the event that there are issues with the collection, use, or disclosure of Personal Data by the Data Controller or the Data Processor, coordinate and work with the Office, as well as any staff members or service providers, with regard to compliance with this act.

Table A3. Information management domain and controls

Controller number	Details
Access control	
20	In accordance with the needs of the business and information security, an access control policy must be created, recorded, and periodically evaluated.
21	To grant or remove access privileges for all user types to all systems and services, a formal user access provisioning process must be put in place.
22	To enable the assignment of access permissions, a formal user registration and deregistration
23	Users must only have access to networks and network services for which they have been specifically granted permission.
24	Owners of the asset must periodically review the access privileges of users.
Log management	
25	Collect logs not less than 90 days and not exceed 2 years.
26	Backup the systems, operating system images regularly.

Table A4. The 26 sets of provided keywords (corresponding to each Cybersecurity Control explained in Tables A1, A2, and A3)

Cybersecurity controls	Keywords*
1. Internal and external challenges:	internal challenges, external challenges, risk assessment, SWOT analysis, *ความท้าทายภายใน*, *ความท้าทายภายนอก*, *การประเมินความเสี่ยง*, organization goals, information security management system, planned outcome, *เป้าหมายขององค์กร*, *ระบบการจัดการความมั่นคงปลอดภัยสารสนเทศ*, *ผลลัพธ์ที่วางแผนไว้*, threat analysis, vulnerability assessment, gap analysis, *การวิเคราะห์ภัยคุกคาม*, *การประเมินความเสี่ยง*, *การวิเคราะห์ช่องว่าง*
2. Interested parties and security requirements	stakeholders, interested parties, security requirements, *ผู้มีส่วนได้ส่วนเสีย*, *ข้อกำหนดด้านความปลอดภัย*, information security management system, parties with interest, information security needs, *ระบบการจัดการความมั่นคงปลอดภัยสารสนเทศ*, *บุคคลที่เกี่ยวข้อง*, *ความต้องการด้านความปลอดภัยข้อมูล*, privacy requirements, data protection needs, *ผู้เกี่ยวข้อง*
3. ISMS implementation	ISMS, information security management system, *ระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ*, implement, maintain, improve, International Standard, *ดำเนินการ*, *บำรุงรักษา*, *ปรับปรุง*, *มาตรฐานสากล*, security controls, policy implementation, security policy, *การควบคุมด้านความปลอดภัย*, *การดำเนินนโยบาย*, *นโยบายความปลอดภัย*
4. Top management commitment	leadership commitment, top management, *ความมุ่งมั่นของผู้บริหาร*, *ผู้บริหารระดับสูง*, lead by example, show dedication, information security management system, *เป็นแบบอย่าง*, *แสดงความทุ่มเท*, *ระบบการจัดการความมั่นคงปลอดภัยสารสนเทศ*, executive support, management endorsement, commitment to security, *การสนับสนุนจากผู้บริหาร*, *การรับรองจากผู้บริหาร*, *ความมุ่งมั่นต่อความปลอดภัย*
5. Security roles and responsibilities	security roles, security responsibilities, *บทบาทด้านความปลอดภัย*, *ความรับผิดชอบด้านความปลอดภัย*, assign roles, communicate responsibilities, information security, *กำหนดบทบาท*, *สื่อสารความรับผิดชอบ*, *ความมั่นคงปลอดภัยข้อมูล*, role assignment, responsibility delegation, security duties, *การมอบหมายบทบาท*, *การมอบหมายความรับผิดชอบ*, *หน้าที่ด้านความปลอดภัย*
6. Consent request	consent request, written consent, electronic consent, *การขอความยินยอม*, *ความยินยอมเป็นลายลักษณ์อักษร*, express consent, request for consent, *ความยินยอมที่ชัดเจน*, *คำขอความยินยอม*, explicit consent, digital consent, *คำยินยอมอย่างชัดเจน*
7. Consent withdrawal	consent withdrawal, revoke consent, *การถอนความยินยอม*, *เพิกถอนความยินยอม*, withdraw consent, cancel consent, *ถอนความยินยอม*, *ยกเลิกความยินยอม*, retraction of consent, consent cancellation, *การถอนคำยินยอม*
8. Parental consent	parental consent, minor consent, *ความยินยอมของผู้ปกครอง*, *ความยินยอมสำหรับผู้เยาว์*, consent of guardian, consent for minors, parental responsibility, *ความยินยอมจากผู้ปกครอง*, *ความยินยอมสำหรับผู้เยาว์*, *ความรับผิดชอบของผู้ปกครอง*, child consent, guardian approval, *ความยินยอมของเด็ก*, *การอนุมัติของผู้ปกครอง*
9. Explanation for data collection	reason for data collection, purpose of data collection, *เหตุผลในการเก็บข้อมูล*, *วัตถุประสงค์ในการเก็บข้อมูล*, explain data collection, data use, data disclosure, *อธิบายการเก็บข้อมูล*, *การใช้ข้อมูล*, *การเปิดเผยข้อมูล*, data collection rationale, purpose explanation, *เหตุผลในการรวบรวมข้อมูล*, *การอธิบายวัตถุประสงค์*
10. Data collection notification	data collection notification, prior notification, *การแจ้งเก็บข้อมูล*, *การแจ้งล่วงหน้า*, inform data collection, notification of data use, data subject, *แจ้งการเก็บข้อมูล*, *การแจ้งการใช้ข้อมูล*, *เจ้าของข้อมูล*, collection notice, information disclosure, *การแจ้งการรวบรวมข้อมูล*, *การเปิดเผยข้อมูล*
11. Sensitive data collection	sensitive data, special category data, *ข้อมูลอ่อนไหว*, *ข้อมูลประเภทพิเศษ*, collect sensitive data, express consent, data subject impact, *เก็บข้อมูลอ่อนไหว*, *ความยินยอมที่ชัดเจน*, *ผลกระทบต่อเจ้าของข้อมูล*, sensitive information, special data, *ข้อมูลที่อ่อนไหว*, *ข้อมูลพิเศษ*

* aligned with the same sequence as in the system source code (combined Thai and English)

Table A4. The 26 Sets of provided keywords (corresponding to each Cybersecurity Control explained in Tables A1, A2, and A3) (continued)

Cybersecurity controls	Keywords*
12. Data use and disclosure	data use, data disclosure, *การใช้ข้อมูล*, *การเปิดเผยข้อมูล*, use of personal data, approval of data subject, data controller, *การใช้ข้อมูลส่วนบุคคล*, *การอนุมัติของเจ้าของข้อมูล*, *ผู้ควบคุมข้อมูล*, information usage, data sharing, *การใช้ข้อมูล*, *การแบ่งปันข้อมูล*
13. International data transfer	international data transfer, cross-border data transfer, *การโอนข้อมูลระหว่างประเทศ*, *การถ่ายโอนข้อมูลข้ามพรมแดน*, transfer of personal data, foreign jurisdiction, data protection level, *การโอนข้อมูลส่วนบุคคล*, *เขตอำนาจศาลต่างประเทศ*, *ระดับการปกป้องข้อมูล*, data export, international transfer, *การส่งออกข้อมูล*, *การถ่ายโอนข้อมูลระหว่างประเทศ*
14. Data subject access rights	data access rights, right to access personal data, *สิทธิในการเข้าถึงข้อมูล*, *สิทธิในการขอสำเนาข้อมูลส่วนบุคคล*, access to personal information, data subject rights, maintaining data, *การเข้าถึงข้อมูลส่วนบุคคล*, *สิทธิของเจ้าของข้อมูล*, *การรักษาข้อมูล*, right of access, personal data access, *สิทธิในการเข้าถึง*, *การเข้าถึงข้อมูลส่วนตัว*
15. Right to object	right to object, objection to data processing, *สิทธิในการคัดค้าน*, *การคัดค้านการประมวลผลข้อมูล*, object to data use, data subject rights, data collection, *คัดค้านการใช้ข้อมูล*, *สิทธิของเจ้าของข้อมูล*, *การเก็บข้อมูล*, data objection, processing objection, *การคัดค้านข้อมูล*, *การคัดค้านการประมวลผล*
16. Right to erasure	right to erasure, right to be forgotten, *สิทธิในการลบข้อมูล*, *สิทธิที่จะถูกลืม*, delete personal data, dispose of information, data subject request, *ลบข้อมูลส่วนบุคคล*, *ทำจัดข้อมูล*, *คำขอของเจ้าของข้อมูล*, data deletion, information erasure, *การลบข้อมูล*, *การลบข้อมูล*
17. DPO advisory role:	DPO advice, data protection officer advisory, *คำแนะนำจาก* DPO, *บทบาทที่ปรึกษาของเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล*, advise on compliance, DPO role, data controller, data processor, *ให้คำแนะนำเกี่ยวกับการปฏิบัติตาม*, *บทบาทของ* DPO, *ผู้ควบคุมข้อมูล*, *ผู้ประมวลผลข้อมูล*, compliance advice, DPO duties, *คำแนะนำด้านการปฏิบัติตาม*, *หน้าที่ของ* DPO
18. DPO compliance monitoring	DPO monitoring, compliance examination, *การตรวจสอบการปฏิบัติตามกฎหมายโดย* DPO, *การตรวจสอบการปฏิบัติตาม*, monitor data activities, compliance with act, data use examination, *ติดตามกิจกรรมข้อมูล*, *ปฏิบัติตามกฎหมาย*, *การตรวจสอบการใช้ข้อมูล*, data protection monitoring, compliance checks, *การติดตามการคุ้มครองข้อมูล*, *การตรวจสอบการปฏิบัติตาม*
19. DPO coordination	DPO coordination, data protection coordination, *การประสานงานของ* DPO, *การประสานงานด้านการคุ้มครองข้อมูล*, coordinate data protection, work with office, compliance issues, *ประสานงานการคุ้มครองข้อมูล*, *ทำงานกับสำนักงาน*, *ปัญหาการปฏิบัติตาม*, DPO collaboration, data protection tasks, *การประสานงานของ* DPO, *งานด้านการคุ้มครองข้อมูล*
20. Access control policy	access control policy, *นโยบายควบคุมการเข้าถึง*, create policy, document policy, review policy, business needs, *สร้างนโยบาย*, *บันทึกนโยบาย*, *ทบทวนนโยบาย*, *ความต้องการธุรกิจ*, access policy, policy development, *นโยบายการเข้าถึง*, *การพัฒนานโยบาย*
21. User access provisioning	user access provisioning, *การจัดการสิทธิ์การเข้าถึงของผู้ใช้*, grant access, remove access, user types, systems and services, *ให้สิทธิ์การเข้าถึง*, *ยกเลิกการเข้าถึง*, *ประเภทผู้ใช้*, *ระบบและบริการ*, access management, user privileges, *การจัดการการเข้าถึง*, *สิทธิพิเศษของผู้ใช้*
22. User registration and deregistration	user registration, user deregistration, *การลงทะเบียนผู้ใช้*, *การยกเลิกการลงทะเบียนผู้ใช้*, assign access permissions, formal process, registration system, *มอบสิทธิ์การเข้าถึง*, *กระบวนการทางการ*, *ระบบลงทะเบียน*, user enrollment, deregister users, *การลงทะเบียนผู้ใช้*, *การยกเลิกผู้ใช้*
23. Network access control	network access control, *การควบคุมการเข้าถึงเครือข่าย*, grant network access, network services, specific permission, *ให้สิทธิ์การเข้าถึงเครือข่าย*, *บริการเครือข่าย*, *สิทธิ์เฉพาะ*, network permissions, access network services, *การให้สิทธิ์เครือข่าย*, *การเข้าถึงบริการเครือข่าย*
24. Access privilege review	access privilege review, *การทบทวนสิทธิ์การเข้าถึง*, review user privileges, asset owners, periodically review, *ทบทวนสิทธิ์ผู้ใช้*, *เจ้าของทรัพย์สิน*, *ทบทวนเป็นระยะ*, access rights review, privilege reassessment, *การทบทวนสิทธิ์การเข้าถึง*, *การประเมินสิทธิพิเศษ*
25. Log retention	log retention, log collection, *การเก็บรักษาล็อก*, *การเก็บบันทึกข้อมูล*, retain logs, collect logs, log retention period, *เก็บรักษาล็อก*, *รวบรวมล็อก*, *ระยะเวลาการเก็บล็อก*, log storage, log duration, *การจัดเก็บล็อก*, *ระยะเวลาการเก็บล็อก*
26. System backup	system backup, operating system images, *การสำรองข้อมูลระบบ*, *ภาพระบบปฏิบัติการ*, backup systems, regular backup, data integrity, *สำรองข้อมูลระบบ*, *สำรองข้อมูลเป็นประจำ*, *ความสมบูรณ์ของข้อมูล*, data backup, system redundancy, *การสำรองข้อมูล*, *ความซ้ำซ้อนของระบบ*

* aligned with the same sequence as in the system source code (combined Thai and English)