คำอธิบาย Cyber Resilience Assessment Framework (CRAF)

1. Governance

No	Questionnaire	คำอธิบาย
Governance - oversight		
Level 1		
1.	Designated members of management are held accountable by the board or an appropriate board committee for implementing and managing the information security and business continuity programs.	คณะกรรมการบริษัทหรือคณะกรรมการที่ได้รับมอบหมาย มีการมอบหมายและกำหนดหน้าที่ให้แก่ผู้บริหารระดับสูง ในการจัดให้มีระบบและการบริหารจัดการด้านความมั่นคงปลอดภัยสารสนเทศ และระบบบริหารจัดการความต่อเนื่องทางธุรกิจ และคณะกรรมการดังกล่าวเป็นผู้รับผิดชอบต่อการประเมิน การสั่งการ และการติดตามผลการดำเนินงานให้มีความเพียงพอและเป็นไปอย่างมีประสิทธิภาพและประสิทธิผล
2.	Information security risks are discussed in management meetings when prompted by highly visible cyber events or regulatory alerts.	บริษัทมีการจัดทำกระบวนการในการสื่อสารความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ ให้แก่ผู้บริหารระดับสูง ทั้งนี้ การสื่อสารอาจกระทำโดยการกำหนดเป็นวาระประจำในการประชุม เพื่อรายงานผลการดำเนินการด้านความมั่นคงปลอดภัยสารสนเทศ (Security report) การรายงานตัวชี้วัดด้านความเสี่ยงสำคัญ (Key risk indicator) หรือ การรายงานความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศจากเหตุการณ์ที่เกิดขึ้นในกลุ่มอุตสาหกรรม หรือเหตุการณ์สำคัญในรายงานข่าวที่อาจมีผลกระทบต่อการให้บริการด้านเทคโนโลยีสารสนเทศของบริษัท เป็นต้น
3.	Management provides a written report on the overall status of the information security and business continuity programs to the board or an appropriate board committee at least annually.	บริษัทมีการจัดทำรายงานภาพรวมของระบบรักษาความมั่นคงปลอดภัยสารสนเทศ และระบบบริหารจัดการด้านความต่อเนื่องทางธุรกิจ เพื่อรายงานต่อคณะกรรมการของบริษัทหรือคณะกรรมการที่ได้รับมอบหมายอย่างน้อยปีละ 1 ครั้ง ทั้งนี้หัวข้อการรายงานควรประกอบด้วยผลการดำเนินงานสำคัญ เช่น ผลการจัดหาและติดตั้งระบบการรักษาความมั่นคงปลอดภัยสารสนเทศ ผลการปฏิบัติงาน ปัญหาและเหตุการณ์สำคัญด้านความมั่นคงปลอดภัยสารสนเทศที่เกิดขึ้นและแนวทางการแก้ไขและป้องกันเหตุการณ์ ผลการดำเนินงานและผลการทดสอบแผนการบริหารความต่อเนื่องทางธุรกิจ เป็นต้น

No	Questionnaire	คำอธิบาย
Level 2		
4.	At least annually, the board or an appropriate board committee reviews and approves the institution's cybersecurity program.	บริษัทจัดทำและนำเสนอแผนการดำเนินงานด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ ให้แก่คณะกรรมการบริษัทหรือคณะกรรมการที่ได้รับมอบหมาย เพื่อสอบทานและอนุมัติอย่างน้อยปีละ 1 ครั้ง ทั้งนี้ แผนการดำเนินการควรประกอบด้วย กรอบการบริหารจัดการด้านความมั่นคงปลอดภัยทางไซเบอร์ ความเสี่ยงสำคัญของบริษัท แนวทางและแผนงานที่เกี่ยวข้องเพื่อบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยทางไซเบอร์ ระบบควบคุมและป้องกันภัยไซเบอร์และแผนด้านการบริหารด้านทรัพยากรบุคคล เป็นต้น
5.	Cybersecurity tools and staff are requested through the budget process.	บริษัทมีการจัดทำแผนงบประมาณประจำปี ในการจัดหาเครื่องมือ ซอฟต์แวร์ และอุปกรณ์ที่เกี่ยวข้องในการป้องกันความปลอดภัยทางไซเบอร์ พร้อมทั้งแผนการจัดการด้านทรัพยากรบุคคลและองค์ความรู้ เป็นส่วนหนึ่งในกระบวนการจัดทำงบประมาณประจำปีของบริษัท
Level 3		
6.	The board or an appropriate board committee has cybersecurity expertise or engages experts to assist with oversight responsibilities.	คณะกรรมการของบริษัทหรือคณะกรรมการที่ได้รับมอบหมาย ประกอบไปด้วย กรรมการผู้มีความรู้และความเชี่ยวชาญด้านความปลอดภัยทางไซเบอร์ หรือมีการจัดหาผู้เชี่ยวชาญเป็นที่ปรึกษาในการให้ความช่วยเหลือ ให้คำปรึกษา หรือให้ข้อเสนอแนะที่เป็นประโยชน์ในกำกับดูแลด้านความมั่นคงปลอดภัยทางไซเบอร์ของคณะกรรมการ
7.	The standard board meeting package includes reports and metrics that go beyond events and incidents to address threat intelligence trends and the institution's security posture.	วาระประจำของการประชุมคณะกรรมการของบริษัท ประกอบไปด้วย วาระการประชุมที่มีหัวข้อด้านความมั่นคงปลอดภัยทางไซเบอร์ ที่ไม่เป็นเพียงแต่การรายงานสรุปเหตุการณ์ที่เกิดขึ้นในรอบระยะเวลาหรือดัชนีชี้วัดและการเฝ้าระวังด้านความปลอดภัยที่มีการกำหนดไว้เท่านั้น แต่มีการรายงานแนวโน้มความเสี่ยงและสถานะของบริษัทด้านความมั่นคงปลอดภัยทางไซเบอร์ของบริษัทในรูปแบบ metrics ด้วย

No	Questionnaire	คำอธิบาย
8.	The institution has a cyber risk appetite statement approved by the board or an appropriate board committee.	บริษัทมีการจัดทำคำประกาศความเสี่ยงที่ยอมรับได้ (Risk appetite statement) สำหรับความเสี่ยงด้านความมั่นคงปลอดภัยทางไซเบอร์ ที่ได้รับการนำเสนอและอนุมัติโดยคณะกรรมการบริษัท หรือคณะกรรมการที่ได้รับมอบหมาย
9.	Cyber risks that exceed the risk appetite are escalated to management.	บริษัทมีการจัดทำกระบวนการในการรายงานความเสี่ยงด้านความมั่นคงปลอดภัยทางไซเบอร์ ที่มีระดับความเสี่ยงสูงกว่าระดับความเสี่ยงที่ยอมรับได้ เพื่อนำเสนอต่อผู้บริหารที่เกี่ยวข้องให้การดำเนินการมาตรการที่จำเป็นเพื่อบริหารความเสี่ยง
10.	The board or an appropriate board committee ensures management's annual cybersecurity self-assessment evaluates the institution's ability to meet its cyber risk management standards.	คณะกรรมการบริษัท หรือคณะกรรมการที่ได้รับมอบหมาย มีการสั่งการและติดตามเพื่อให้มั่นใจได้ว่า ฝ่ายบริหารมีการประเมินตนเอง (Self-assessment) ทุกปี และการประเมินนั้นสามารถวัดความสามารถและความพร้อมของบริษัทในการรับมือกับเหตุการณ์ด้านความมั่นคงปลอดภัยทางไซเบอร์
11.	The board or an appropriate board committee reviews and approves management's prioritization and resource allocation decisions based on the results of the cyber assessments.	คณะกรรมการบริษัท หรือคณะกรรมการที่ได้รับมอบหมาย มีการสอบทานและอนุมัติเกณฑ์การพิจารณางบประมาณของฝ่ายบริหารที่มีการจัดลำดับความสำคัญและจัดสรรทรัพยากร อันเป็นผลจากการประเมินความพร้อมในการรับมือความเสี่ยงด้านความมั่นคงปลอดภัยทางไซเบอร์
Level 4		
12.	The board or board committee approved cyber risk appetite statement is part of the enterprise-wide risk appetite statement.	บริษัทมีการจัดทำคำประกาศความเสี่ยงที่ยอมรับได้ (Risk appetite statement) สำหรับความเสี่ยงด้านความมั่นคงปลอดภัยทางไซเบอร์ ซึ่งเป็นส่วนหนึ่งของคำประกาศความเสี่ยงที่ยอมรับได้ในการบริหารความเสี่ยงระดับองค์กร ทั้งนี้คำประกาศความเสี่ยงที่ยอมรับได้ทั้ง 2 ประเภท ต้องได้รับการนำเสนอและอนุมัติโดยคณะกรรมการบริษัท หรือคณะกรรมการที่ได้รับมอบหมาย
13.	The budget process for requesting additional cybersecurity staff and tools maps current resources and tools to the cybersecurity strategy.	กระบวนการพิจารณาและอนุมัติงบประมาณด้านการจัดหาเครื่องมือและทรัพยากรบุคคลด้านความมั่นคงปลอดภัยทางไซเบอร์ มีการวิเคราะห์เปรียบเทียบกับเครื่องมือและทรัพยากรที่มีในปัจจุบัน และมีความสอดคล้องกับกลยุทธ์ด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ของบริษัท

No	Questionnaire	คำอธิบาย
Level 5		
14.	The board or an appropriate board committee discusses ways for management to develop cybersecurity improvements that may be adopted sector-wide.	คณะกรรมการบริษัท หรือคณะกรรมการที่ได้รับมอบหมาย มีการหารือร่วมกับคณะผู้บริหารของบริษัท ในการพัฒนาหรือปรับปรุงระบบการรักษาความมั่นคงปลอดภัยทางไซเบอร์ ที่สามารถปรับปรุง ประยุกต์ใช้ หรือ ก่อให้เกิดความร่วมมือในกลุ่มอุตสาหกรรมเป็นวงกว้าง และส่งผลต่อการเพิ่มศักยภาพ ความรวดเร็วในการตอบสนองต่อเหตุการณ์หรือความเสี่ยง หรือการบริหารทรัพยากรอย่างมีประสิทธิผล
15.	The board or an appropriate board committee verifies that management's actions consider the cyber risks that the institution poses to other critical infrastructures (e.g., telecommunications, energy).	คณะกรรมการบริษัท หรือคณะกรรมการที่ได้รับมอบหมาย มีการสอบทานการดำเนินงานของคณะผู้บริหาร เช่น การออกผลิตภัณฑ์ การจัดหา พัฒนา และการประยุกต์ใช้งานเทคโนโลยี โดยการดำเนินการดังกล่าวมีการพิจารณาถึงความเสี่ยงด้านความมั่นคงปลอดภัยทางไซเบอร์ที่ผลิตภัณฑ์ หรือเทคโนโลยีที่จะมีการประยุกต์ใช้ อันอาจจะมีผลกระทบต่อกลุ่มอุตสาหกรรมในภาพรวม หรือโครงสร้างพื้นฐานอื่นที่สำคัญของประเทศ เช่น ภาคโทรคมนาคม ภาคพลังงาน เป็นต้น
Governance - Strategy / Policies		
Level – 1		
16.	The institution has policies commensurate with its risk and complexity that address the concepts of information technology risk management.	บริษัทมีการจัดทำนโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศ และความมั่นคงปลอดภัยทางไซเบอร์ โดยนโยบายดังกล่าวมีความเหมาะสมกับระดับความเสี่ยง และความซับซ้อนของการใช้งานเทคโนโลยีขององค์กร และสอดคล้องกับแนวทางการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ
17.	The institution has board-approved policies commensurate with its risk and complexity that address information security.	นโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศ และความมั่นคงปลอดภัยทางไซเบอร์ของบริษัทได้รับการอนุมัติโดยคณะกรรมการบริษัท และนโยบายดังกล่าวมีความเหมาะสมกับระดับความเสี่ยง และความซับซ้อนของการใช้งานเทคโนโลยีขององค์กร
18.	The institution has policies commensurate with its risk and complexity that address the concepts of external dependency or third-party management.	บริษัทมีการจัดทำนโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศ และความมั่นคงปลอดภัยทางไซเบอร์ โดยนโยบายดังกล่าวมีความเหมาะสมกับระดับความเสี่ยง และความซับซ้อนจากการใช้งานทางเทคโนโลยีที่มีการคำนึงถึงการพึ่งพาบริการจากบุคคลภายนอก

No	Questionnaire	คำอธิบาย
		เช่น ความเสี่ยงจากการพึ่งพาด้านเทคโนโลยี ความเสี่ยงจากการประมวลผลข้อมูลโดยบุคคลภายนอก ความเสี่ยงด้านการรั่วไหลของข้อมูลความลับ ความเสี่ยงด้านการไม่ปฏิบัติตามกฎหมาย เป็นต้น โดยบริษัทมีการประยุกต์ใช้กรอบการบริหารจัดการบุคคลภายนอก (Third-party management) ในการกำหนดนโยบาย กระบวนการและการควบคุมที่เกี่ยวข้อง
19.	The institution has policies commensurate with its risk and complexity that address the concepts of incident response and resilience.	บริษัทมีการจัดทำนโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศ และความมั่นคงปลอดภัยทางไซเบอร์ โดยนโยบายดังกล่าวมีความเหมาะสมกับระดับความเสี่ยงและความซับซ้อนจากการใช้งานทางเทคโนโลยี โดยได้ผนวกแนวคิดด้านการตอบสนองและความสามารถในการคงทนในการรองรับต่อเหตุการณ์ไว้แล้ว (incident response and resilience)
20.	A formal process is in place to update policies as the institution's inherent risk profile changes.	บริษัทมีกระบวนการที่ชัดเจนในการทบทวนและปรับปรุงนโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศ และความมั่นคงปลอดภัยทางไซเบอร์เมื่อสภาพความเสี่ยงตั้งต้น (inherent risk) ของบริษัทเปลี่ยนไป เช่น การเปลี่ยนแปลงสภาพแวดล้อมในการประกอบธุรกิจ การใช้งานเทคโนโลยี ภัยคุกคามต่อกลุ่มอุตสาหกรรม ข้อกำหนดของหน่วยงานกำกับดูแล เป็นต้น
Level – 2		
21.	The institution augmented its information security strategy to incorporate cybersecurity and resilience.	บริษัทมีการขยายแผนกลยุทธ์ด้านความมั่นคงปลอดภัยสารสนเทศ ให้ครอบคลุมเรื่องความมั่นคงปลอดภัยทางไซเบอร์ และรองรับเหตุการณ์ภัยคุกคามทางไซเบอร์
22.	The institution has a formal cybersecurity program that is based on technology and security industry standards or benchmarks.	บริษัทมีการจัดทำระบบการรักษาความมั่นคงปลอดภัยทางไซเบอร์ ที่ใช้เทคโนโลยีและความปลอดภัยที่ได้มาตรฐานสากล หรือมาตรฐานที่อุตสาหกรรมยอมรับ เช่น การประยุกต์ใช้กรอบระบบการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (information security management system: ISMS) หรือกรอบการบริหารความมั่นคงปลอดภัยทางไซเบอร์ (Cybersecurity framework)
23.	The institution has policies commensurate with its risk and complexity that address the concepts of threat information sharing.	บริษัทมีการจัดทำนโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศ และความมั่นคงปลอดภัยทางไซเบอร์ โดยนโยบายดังกล่าวมีความเหมาะสมกับระดับความเสี่ยง

No	Questionnaire	คำอธิบาย
		และความซับซ้อนจากการใช้งานทางเทคโนโลยีที่มีเนื้อหากล่าวถึง concept ของการให้ความร่วมมือด้านข้อมูลข่าวสารในกลุ่มอุตสาหกรรม หรือหน่วยงานที่เกี่ยวข้อง เช่น TCM-CERT
Level – 3		
24.	The institution has a comprehensive set of policies commensurate with its risk and complexity that address the concepts of threat intelligence.	บริษัทมีการจัดทำนโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศ และความมั่นคงปลอดภัยทางไซเบอร์ที่เข้มข้นโดยนโยบายดังกล่าวมีความเหมาะสมกับระดับความเสี่ยงและความซับซ้อนจากการใช้งานทางเทคโนโลยี โดยนโยบายดังกล่าวมีการพิจารณาถึงการใช้งานข้อมูลการข่าวด้านภัยคุกคาม (Threat intelligence) ทางไซเบอร์ เช่น การจัดหาบริการด้านการข่าวจากผู้ให้บริการ การติดตามข้อมูลข่าวสารจากแหล่งข้อมูลด้านความมั่นคงปลอดภัยทางไซเบอร์ เป็นต้น
25.	Management periodically reviews the cybersecurity strategy to address evolving cyber threats and changes to the institution's inherent risk profile.	บริษัทมีการสอบทานและปรับปรุงแผนกลยุทธ์ด้านความมั่นคงปลอดภัยสารสนเทศ เพื่อรองรับภัยคุกคามที่เกิดขึ้นใหม่ และการเปลี่ยนแปลงของความเสี่ยงตั้งต้นขององค์กร
26.	Management links strategic cybersecurity objectives to tactical goals.	บริษัทมีการเชื่อมโยงวัตถุประสงค์ด้านความมั่นคงปลอดภัยทางไซเบอร์เชิงกลยุทธ์ ให้สอดคล้องกับเป้าหมายขององค์กร
27.	A formal process is in place to cross-reference and simultaneously update all policies related to cyber risks across business lines.	บริษัทมีกระบวนการสอบทานและปรับปรุงนโยบายความมั่นคงปลอดภัยสารสนเทศ และความมั่นคงปลอดภัยทางไซเบอร์แบบบูรณาการกับส่วนงานที่เกี่ยวข้องทั้งหมด ยกตัวอย่างเช่น นโยบาย มาตรฐาน หรือข้อกำหนดที่มีการปรับปรุงนั้นได้รับการสื่อสารไปอย่างทั่วถึงตลอดทั้งองค์กร เพื่อให้มีการปรับปรุงนโยบาย ระเบียบวิธีปฏิบัติงาน มาตรฐาน คู่มือการทำงาน หรือเอกสารอื่นใดภายในองค์กรให้สอดคล้องกับนโยบายความมั่นคงฯที่มีการปรับปรุงไป
Level – 4		
28.	The cybersecurity strategy outlines the institution's future state of cybersecurity with short-term and long-term perspectives.	บริษัทมีการจัดทำแผนกลยุทธ์ด้านความมั่นคงปลอดภัยทางไซเบอร์ อันประกอบด้วย แผนระยะสั้นและแผนระยะยาว

No	Questionnaire	คำอธิบาย
29.	Industry-recognized cybersecurity standards are used as sources during the analysis of cybersecurity program gaps.	บริษัทมีการประเมินระบบรักษาความมั่นคงปลอดภัยทางไซเบอร์ของบริษัท และวิเคราะห์หาช่องว่าง (gap) โดยเปรียบเทียบกับมาตรฐานความมั่นคงปลอดภัยทางไซเบอร์ที่ได้รับการยอมรับในอุตสาหกรรม เช่น มาตรฐาน IT Governance USA - Cybersecurity Standards and Frameworks, มาตรฐาน NIST Cybersecurity Framework (NIST CSF), มาตรฐาน Information Security Management System (ISMS), หรือ มาตรฐาน IOSCO – Guidance on cyber resilience for financial market infrastructures เป็นต้น
Level – 5		
30.	The cybersecurity strategy identifies and communicates the institution's role as it relates to other critical infrastructures.	บริษัทมีการจัดทำแผนกลยุทธ์ด้านความมั่นคงปลอดภัยทางไซเบอร์ ที่มีการกำหนดและสื่อสารบทบาทหน้าที่ของบริษัทในฐานะที่เป็นโครงสร้างพื้นฐานสำคัญของตลาดทุน ซึ่งเชื่อมโยงกับโครงสร้างพื้นฐานสำคัญอื่นของประเทศ เช่น การมีมาตรการรักษาความปลอดภัยในการเชื่อมโยงทางเครือข่ายในกลุ่มอุตสาหกรรมในระบบนิเวศ (Ecosystem) ของตลาดทุนและโครงสร้างพื้นฐานสำคัญที่เกี่ยวข้อง การจัดเก็บบันทึกเหตุการณ์และคำสั่งรายการเพื่อใช้ตรวจสอบได้อย่างบูรณาการ เป็นต้น
Governance - IT Asset Management		
Level – 1		
31.	An inventory of organizational assets (e.g., hardware, software, data, and systems hosted externally) is maintained.	บริษัทมีการจัดทำและรวบรวมข้อมูลทะเบียนทรัพย์สินด้านเทคโนโลยีสารสนเทศ และ update ข้อมูลให้เป็นปัจจุบันอยู่เสมอ เช่น ทรัพย์สินประเภทฮาร์ดแวร์อุปกรณ์เครื่องคอมพิวเตอร์สำนักงาน เครื่องแม่ข่าย อุปกรณ์เครือข่าย อุปกรณ์รักษาความปลอดภัยสารสนเทศ ซอฟต์แวร์ ทรัพย์สินประเภทข้อมูล หรืออุปกรณ์หรือทรัพย์สินด้านเทคโนโลยีสารสนเทศที่มีการติดตั้งภายนอกบริษัท ได้แก่ ระบบสารสนเทศร่วมกันบนระบบเครือข่ายคอมพิวเตอร์เพื่อการประมวลผลตามความต้องการของผู้ใช้งาน (Cloud Computing) เป็นต้น

No	Questionnaire	คำอธิบาย
32.	Organizational assets (e.g., hardware, systems, data, and applications) are prioritized for protection based on the data classification and business value.	ข้อมูลทะเบียนทรัพย์สินด้านเทคโนโลยีสารสนเทศที่มีการรวบรวม เช่น ทรัพย์สินประเภทฮาร์ดแวร์อุปกรณ์ระบบงาน ทรัพย์สินประเภทข้อมูล หรืออุปกรณ์หรือทรัพย์สินด้านเทคโนโลยีสารสนเทศที่มีการติดตั้งภายนอกบริษัท เป็นต้น ได้รับการจัดระดับความสำคัญเพื่อกำหนดมาตรการและการควบคุมความมั่นคงปลอดภัยที่เหมาะสม โดยพิจารณาถึงชั้นความลับของข้อมูล และมูลค่าของทรัพย์สิน
33.	A change management process is in place to request and approve changes to systems configurations, hardware, software, applications, and security tools.	บริษัทมีการจัดทำขั้นตอนการบริหารจัดการการเปลี่ยนแปลง อันประกอบด้วย ขั้นตอนการร้องขอการแก้ไขเปลี่ยนแปลง การประเมินและอนุมัติการแก้ไขเปลี่ยนแปลงอย่างเป็นลายลักษณ์อักษร เพื่อใช้ในการบริหารจัดการเปลี่ยนแปลงทรัพย์สินด้านเทคโนโลยีสารสนเทศ ได้แก่ การแก้ไขเปลี่ยนแปลงค่าคอนฟิกูเรชั่น การแก้ไขเปลี่ยนแปลงด้านอุปกรณ์ฮาร์ดแวร์ ซอฟต์แวร์ระบบงาน และการแก้ไขปรับปรุงระบบและเครื่องมือรักษาความปลอดภัยสารสนเทศ เช่น อุปกรณ์ไฟร์วอลล์ อุปกรณ์วิเคราะห์พฤติกรรมทางเครือข่ายเพื่อตรวจจับหรือป้องกันผู้บุกรุก เป็นต้น
Level – 2		
34.	The asset inventory, including identification of critical assets, is updated at least annually to address new, relocated, re-purposed, and sunset assets.	ข้อมูลทะเบียนทรัพย์สินด้านเทคโนโลยีสารสนเทศที่บริษัทใช้งานอยู่ เช่น ทรัพย์สินประเภทฮาร์ดแวร์อุปกรณ์ ระบบงาน ทรัพย์สินประเภทข้อมูล หรืออุปกรณ์หรือทรัพย์สินด้านเทคโนโลยีสารสนเทศที่มีการติดตั้งภายนอกบริษัท ได้รับการสอบทานและปรับปรุงอย่างน้อยปีละ 1 ครั้ง เพื่อให้ข้อมูล ของสถานที่ติดตั้งหรือผู้ครอบครองทรัพย์สิน วัตถุประสงค์การใช้งานหรือการยกเลิกการใช้งานของทรัพย์สิน มีความถูกต้องเป็นปัจจุบัน
35.	The institution has a documented asset life-cycle process that considers whether assets to be acquired have appropriate security safeguards.	บริษัทมีการจัดทำกระบวนการบริหารจัดการทรัพย์สินที่กำหนดมาตรฐานด้านความมั่นคงปลอดภัยสารสนเทศในขั้นตอนการจัดหา พัฒนา และติดตั้งทรัพย์สิน เช่น การจัดทำค่าความปลอดภัยมาตรฐาน (Security baseline) การจัดทำข้อกำหนดด้านความปลอดภัย (Security requirement) สำหรับระบบงานหรือซอฟต์แวร์ที่มีการจัดหาและพัฒนาร การจัดทำขั้นตอน

No	Questionnaire	คำอธิบาย
		การตรวจสอบความปลอดภัย (Security checklist) เพื่อตรวจสอบระบบงานก่อนการติดตั้งใช้งาน (Production control) เป็นต้น และมีการบันทึกกระบวนการทั้งหมดเป็นลายลักษณ์อักษร
36.	The institution proactively manages system EOL (e.g., replacement) to limit security risks.	บริษัทมีกระบวนการบริหารจัดการด้านสินทรัพย์ที่อยู่ในแผนการยกเลิกการสนับสนุน (End of life/End of support) จากบริษัทผู้ผลิตเป็นการล่วงหน้า เช่น การจัดทำแผนการปรับปรุงเวอร์ชั่น หรือ การจัดหาระบบงานทดแทน เป็นต้น ทั้งนี้เพื่อป้องกันความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศจากการใช้งานอุปกรณ์ ระบบงาน หรือซอฟต์แวร์ที่หมดอายุ หรือไม่ได้รับการสนับสนุนจากบริษัทผู้ผลิต
37.	Changes are formally approved by an individual or committee with appropriate authority and with separation of duties.	บริษัทมีการจัดทำขั้นตอนการบริหารจัดการการเปลี่ยนแปลง อันประกอบด้วย ขั้นตอนการร้องขอการแก้ไขเปลี่ยนแปลง การประเมินและอนุมัติการแก้ไขเปลี่ยนแปลงโดยบุคคลหรือคณะกรรมการผู้มีอำนาจอย่างเป็นลายลักษณ์อักษร และมีการแบ่งแยกหน้าที่อย่างเหมาะสม ทั้งนี้ นโยบายและขั้นตอนการปฏิบัติงานด้านการบริหารจัดการเปลี่ยนแปลงควรมีการกำหนดบทบาทหน้าที่ความรับผิดชอบ และอำนาจในการอนุมัติการแก้ไขเปลี่ยนแปลงอย่างชัดเจน
Level – 3		
38.	Baseline configurations cannot be altered without a formal change request, documented approval, and an assessment of security implications.	การแก้ไขเปลี่ยนแปลงค่าคอนฟิกูเรชั่นระบบงาน ซอฟต์แวร์ เครื่องแม่ข่าย อุปกรณ์ด้านเทคโนโลยีสารสนเทศไปจากค่ามาตรฐานต้องได้รับการบันทึกคำร้องและมีขั้นตอนการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศจากการเปลี่ยนแปลงนั้น ๆ ทั้งนี้ ผลการประเมินความเสี่ยงต้องได้รับการตรวจทานและอนุมัติจากผู้มีอำนาจอย่างเป็นลายลักษณ์อักษร
39.	A formal IT change management process requires cybersecurity risk to be evaluated during the analysis, approval, testing, and reporting of changes.	กระบวนการบริหารจัดการการเปลี่ยนแปลง ได้มีการพิจารณาและประเมินความเสี่ยงด้านไซเบอร์ ทั้งในขั้นตอนการวิเคราะห์การเปลี่ยนแปลง การอนุมัติ การทดสอบ และการรายงานผลการเปลี่ยนแปลง เช่น มีการจัดทำและบันทึกข้อกำหนดด้านความปลอดภัย (Security requirement) มีการวิเคราะห์ความเสี่ยงด้านความปลอดภัยทางไซเบอร์ในขั้นตอนการวิเคราะห์

No	Questionnaire	คำอธิบาย
		ผลกระทบ (impact analysis) มีการทดสอบด้านความปลอดภัยในขั้นตอนของการทดสอบและควบคุมคุณภาพ (Quality assurance) เป็นต้น
Level – 4		
40.	Supply chain risk is reviewed before the acquisition of mission-critical information systems including system components.	มีการประเมินความเสี่ยงที่เกี่ยวข้องกับผู้ให้บริการที่เกี่ยวข้องทุกรายก่อนเริ่มดำเนินการจัดหาและพัฒนาระบบงานสำคัญ รวมถึงส่วนประกอบของระบบงานด้วย
41.	Automated tools enable tracking, updating, asset prioritizing, and custom reporting of the asset inventory.	บริษัทมีการใช้เครื่องมือแบบอัตโนมัติในการติดตาม ปรับปรุงข้อมูล และจัดลำดับความสำคัญของทรัพย์สินด้านเทคโนโลยีสารสนเทศที่อยู่ในความครอบครองของบริษัทและจัดทำรายงานเป็นประจำ เพื่อให้มั่นใจถึงความครบถ้วนและความถูกต้องของรายงานทรัพย์สินในการบริหารจัดการอย่างมีประสิทธิภาพและประสิทธิผล
42.	Automated processes are in place to detect and block unauthorized changes to software and hardware.	บริษัทมีกระบวนการอัตโนมัติในการตรวจจับและป้องกันการแก้ไขเปลี่ยนแปลงซอฟต์แวร์ และฮาร์ดแวร์โดยไม่ได้รับอนุญาต
43.	The change management system uses thresholds to determine when a risk assessment of the impact of the change is required.	กระบวนการบริหารจัดการการเปลี่ยนแปลง มีการระบุข้อกำหนดและเงื่อนไขอย่างชัดเจน เพื่อกำหนดให้ทุกการเปลี่ยนแปลงที่มีระดับผลกระทบต่อระบบงานหรือการให้บริการต้องมีการประเมินความเสี่ยง พร้อมทั้งมีมาตรการควบคุมความเสี่ยงที่เหมาะสมก่อนเริ่มดำเนินการแก้ไขเปลี่ยนแปลง
44.	A formal change management function governs decentralized or highly distributed change requests and identifies and measures security risks that may cause increased exposure to cyber attack.	บริษัทมีการกำหนดหน่วยงานและหน้าที่ความรับผิดชอบในการกำกับดูแลการบริหารการแก้ไขเปลี่ยนแปลงระบบงานในองค์กร อันอาจมีการดำเนินการในหลายหน่วยงานทั้งภายในและภายนอกฝ่ายงานด้านเทคโนโลยีสารสนเทศ (Decentralised) เพื่อให้มั่นใจถึงมาตรการจัดการความเสี่ยงด้านไซเบอร์อย่างเป็นมาตรฐานเดียวกันตลอดทั้งองค์กร
45.	Comprehensive automated enterprise tools are implemented to detect and block unauthorized changes to software and hardware.	บริษัทมีการจัดหาและติดตั้งระบบเพื่อตรวจจับและป้องกันการแก้ไขเปลี่ยนแปลงซอฟต์แวร์ และฮาร์ดแวร์โดยไม่ได้รับอนุญาต เช่น การใช้งานเครื่องมือ File integrity monitoring (FIM) เป็นต้น

No	Questionnaire	คำอธิบาย
Risk Management - Risk Management Program		
Level – 1		
46.	An information security and business continuity risk management function(s) exists within the institution.	บริษัทมีการกำหนดและมอบหมายหน้าที่ความรับผิดชอบในการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ และความเสี่ยงด้านความต่อเนื่องทางธุรกิจให้กับหน่วยงานที่รับผิดชอบอย่างชัดเจน ทั้งนี้ หน้าที่ความรับผิดชอบในการบริหารจัดการความเสี่ยงดังกล่าวอาจอยู่ภายในหน่วยงานเดียวกัน หรือหลายหน่วยงานก็ได้
Level – 2		
47.	The risk management program incorporates cyber risk identification, measurement, mitigation, monitoring, and reporting.	กระบวนการบริหารจัดการความเสี่ยงของบริษัทมีการพิจารณาถึงความเสี่ยงด้านความมั่นคงปลอดภัยทางไซเบอร์ด้วย โดยมีขั้นตอนการระบุความเสี่ยง การประเมินความเสี่ยง การควบคุมและลดความเสี่ยง ตลอดจนการติดตามและการรายงานความเสี่ยง
48.	Management reviews and uses the results of audits to improve existing cybersecurity policies, procedures, and controls.	บริษัทใช้รายงานผลการตรวจสอบ ในการปรับปรุงนโยบาย ขั้นตอนการปฏิบัติงาน และการควบคุมที่เกี่ยวข้องด้านความมั่นคงปลอดภัยทางไซเบอร์
49.	Management monitors moderate and high residual risk issues from the cybersecurity risk assessment until items are addressed.	บริษัทมีการติดตามผลการดำเนินการจัดการความเสี่ยง (Risk treatment) สำหรับความเสี่ยงด้านความมั่นคงปลอดภัยทางไซเบอร์ที่มีระดับความเสี่ยงอย่างมีนัยสำคัญหรือมีระดับความเสี่ยงสูง จนกว่าความเสี่ยงดังกล่าวจะได้รับการจัดการอย่างลุล่วง และอยู่ในระดับที่ยอมรับได้
Level – 3		
50.	The cybersecurity function has a clear reporting line that does not present a conflict of interest.	หน่วยงานที่รับผิดชอบในการบริหารจัดการความมั่นคงปลอดภัยทางไซเบอร์ มีโครงสร้างในผังโครงสร้างองค์กรและการรายงานผลการปฏิบัติงานที่ชัดเจน และมีความเป็นอิสระและปราศจากการขัดกันของผลประโยชน์ เช่น หน่วยงานที่รับผิดชอบด้านการบริหารจัดการความมั่นคงปลอดภัยทางไซเบอร์ไม่อยู่ภายใต้การกำกับและสั่งการของหน่วยงานหรือผู้บริหารผู้รับผิดชอบในงานด้านการปฏิบัติการสารสนเทศ เป็นต้น
51.	The risk management program specifically addresses cyber risks beyond the boundaries of the technological impacts (e.g., financial, strategic, regulatory, compliance).	กระบวนการบริหารความเสี่ยงของบริษัทมีการประเมินความเสี่ยงด้านไซเบอร์โดยมองผลกระทบอย่างรอบด้านนอกเหนือจากผลกระทบทางเทคโนโลยี เช่น มีการพิจารณาถึงผลกระทบทางการเงิน ผลกระทบเชิงกลยุทธ์ ผลกระทบด้านชื่อเสียง ผลกระทบด้านกฎหมายและการกำกับดูแล เป็นต้น

No	Questionnaire	คำอธิบาย
52.	Management uses the results of independent audits and reviews to improve cybersecurity.	บริษัทมีการอาศัยรายงานผลการตรวจสอบโดยผู้ตรวจสอบที่เป็นอิสระ เพื่อใช้ในการปรับปรุงกระบวนการด้านความมั่นคงปลอดภัยทางไซเบอร์
Level – 4		
53.	Independent risk management sets and monitors cyber-related risk limits for business units.	ความเสี่ยงด้านความมั่นคงปลอดภัยทางไซเบอร์ได้รับการติดตามโดยหน่วยงานด้านการบริหารความเสี่ยงที่มีความเป็นอิสระ เช่น ฝ่ายบริหารความเสี่ยง เป็นต้น
54.	A process is in place to analyze the financial impact cyber incidents have on the institution's capital.	บริษัทมีการจัดให้มีกระบวนการและเกณฑ์การประเมินผลกระทบทางการเงินทั้งทางตรงหรือทางอ้อมเช่น ความสูญเสียต่อทรัพย์สิน หรือ ค่าใช้จ่ายในการแก้ไขปัญหาและกู้คืนระบบงาน เมื่อมีเหตุการณ์ด้านความมั่นคงปลอดภัยทางไซเบอร์
55.	The cyber risk data aggregation and real-time reporting capabilities support the institution's ongoing reporting needs, particularly during cyber incidents.	บริษัทมีการจัดทำกระบวนการรวบรวมข้อมูลและรายงานข้อมูลความเสี่ยงทางไซเบอร์ที่สามารถรายงานผลอย่างทันที (Real time) เมื่อเกิดความเสี่ยงหรือภัยคุกคามทางไซเบอร์ เช่น ระบบตรวจสอบติดตามและรายงานเหตุการณ์ไปยังผู้รับผิดชอบและผู้บริหารระดับสูงโดยอัตโนมัติ เมื่อเกิดเหตุการณ์ด้านความมั่นคงปลอดภัยทางไซเบอร์ และสามารถรายงานสาเหตุและผลกระทบได้อย่างต่อเนื่องทุกขั้นตอนในระหว่างที่เกิดเหตุภัยคุกคาม เพื่อให้บริษัทสามารถนำข้อมูลมาจัดทำรายงานที่จำเป็นได้
Level – 5		
56.	The risk management function identifies and analyzes commonalities in cyber events that occur both at the institution and across other sectors to enable more predictive risk management.	หน่วยงานบริหารความเสี่ยงมีการติดตาม ระบุ และวิเคราะห์เหตุการณ์ด้านความมั่นคงปลอดภัยทางไซเบอร์ที่เกิดขึ้นในภาคการเงินและตลาดทุน เพื่อพิจารณาแนวโน้มของเหตุการณ์และภัยคุกคามที่อาจจะเกิดขึ้นต่อบริษัทและเตรียมความพร้อมหรือจัดให้มีแนวทางการป้องกันหรือรับมือกับภัยคุกคามดังกล่าว
57.	A process is in place to analyze the financial impact that a cyber incident at the institution may have across the financial sector.	บริษัทมีการจัดให้มีกระบวนการและเกณฑ์การประเมินผลกระทบทางการเงินทั้งทางตรงหรือทางอ้อมต่อตัวบริษัทและภาพรวมตลาดทุน เมื่อมีเหตุการณ์ด้านความมั่นคงปลอดภัยทางไซเบอร์

No	Questionnaire	คำอธิบาย
Risk Management - Risk Assessment		
Level – 1		
58.	A risk assessment focused on safeguarding customer information identifies reasonable and foreseeable internal and external threats, the likelihood and potential damage of threats, and the sufficiency of policies, procedures, and customer information systems.	บริษัทมีการประเมินความเสี่ยงต่อข้อมูลสำคัญของลูกค้า โดยการระบุความเสี่ยงและภัยคุกคามที่ครอบคลุมภัยคุกคามทั้งจากภายในและภายนอกองค์กร แนวโน้มโอกาสเกิดความเสี่ยง ความเสียหายจากภัยคุกคาม และความเพียงพอของนโยบาย ขั้นตอนการปฏิบัติงาน และการควบคุมของระบบงานที่บริหารจัดการข้อมูลของลูกค้าขององค์กร
59.	The risk assessment identifies internet-based systems and high-risk transactions that warrant additional authentication controls.	บริษัทมีการประเมินความเสี่ยง ที่ครอบคลุมความเสี่ยงของระบบที่มีการให้บริการผ่านเครือข่ายอินเทอร์เน็ต และธุรกรรมที่มีความเสี่ยงระดับสูง เช่น การทำรายการทางการเงิน เพื่อจัดให้มีการควบคุมด้านการยืนยันพิสูจน์ตัวตนที่เหมาะสม เช่น การใช้รหัสผ่านที่มีมาตรการรักษาความปลอดภัยรหัสผ่านที่เพียงพอ การใช้การพิสูจน์ตัวตนแบบ multi-factor authentication สำหรับการทำรายการหรือการแก้ไขข้อมูลส่วนบุคคลที่สำคัญ เป็นต้น
60.	The risk assessment is updated to address new technologies, products, services, and connections before deployment.	บริษัทมีการประเมินความเสี่ยงเมื่อมีการดำเนินการหรือการเปลี่ยนแปลงที่สำคัญ เช่น การจัดหาและติดตั้งใช้งานเทคโนโลยีใหม่ การออกผลิตภัณฑ์หรือบริการใหม่ หรือการเชื่อมต่อเครือข่าย เพื่อประเมินความเสี่ยงและจัดหามาตรการในการลดระดับความเสี่ยงก่อนเริ่มดำเนินการ
Level – 2		
61.	Risk assessments are used to identify the cybersecurity risks stemming from new products, services, or relationships.	บริษัทมีการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยทางไซเบอร์เมื่อมีการออกผลิตภัณฑ์หรือบริการใหม่ หรือความเสี่ยงจากคู่ค้าและบุคคลภายนอก
62.	The risk assessment considers the risk of using EOL software and hardware components.	บริษัทมีการประเมินความเสี่ยงจากการใช้งานผลิตภัณฑ์ที่ถูกยกเลิกการสนับสนุน (End of life/End of support) จากบริษัทผู้ผลิตซอฟต์แวร์หรือฮาร์ดแวร์ เช่น ความเสี่ยงด้านการไม่ได้รับการออกชุดปรับปรุงและแก้ไขข้อบกพร่องด้านความปลอดภัยสารสนเทศ (Security patch) หรือความเสี่ยงการจัดหาอุปกรณ์และอะไหล่ทดแทน เป็นต้น
Level – 3		
63.	The risk assessment is adjusted to consider widely known risks or risk management practices.	มีการปรับปรุงกระบวนการประเมินความเสี่ยง โดยพิจารณาถึงความเสี่ยง ปัจจัยเสี่ยง และแนวทางการบริหารจัดการความเสี่ยงที่รับรู้ทั่วกันในอุตสาหกรรม

No	Questionnaire	คำอธิบาย
Level – 4		
64.	An enterprise-wide risk management function incorporates cyber threat analysis and specific risk exposure as part of the enterprise risk assessment.	กระบวนการบริหารความเสี่ยงระดับองค์กรจัดให้การวิเคราะห์ความเสี่ยงและภัยคุกคามทางไซเบอร์ และมูลค่าหรือระดับผลกระทบของความเสี่ยงเป็นส่วนหนึ่งของการประเมินความเสี่ยงระดับองค์กร
Level – 5		
65.	The risk assessment is updated in real time as changes to the risk profile occur, new applicable standards are released or updated, and new exposures are anticipated.	บริษัทมีการประเมินความเสี่ยงที่ตอบสนองอย่างทันทีต่อการเปลี่ยนแปลงของความเสี่ยงของบริษัท (Company risk profile) อันอาจจะเกิดจากปัจจัยทั้งภายในและภายนอก เช่น การออกหรือเปลี่ยนแปลงมาตรฐานและข้อกำหนดในอุตสาหกรรม หรือการตรวจพบหรือมีข้อบ่งชี้ด้านความเสี่ยงใหม่เกิดขึ้น
Risk Management – Audit		
Level – 1		
66.	Independent audit or review evaluates policies, procedures, and controls across the institution for significant risks and control issues associated with the institution's operations, including risks in new products, emerging technologies, and information systems.	บริษัทมีผู้ตรวจสอบที่มีความเป็นอิสระ ในการสอบทานและประเมินความเพียงพอของนโยบาย ขั้นตอนการปฏิบัติงาน และการควบคุมภายในของทั้งองค์กรเพื่อตรวจหาความเสี่ยงสำคัญ และข้อบกพร่องด้านการควบคุมทางด้านการปฏิบัติงาน ความเสี่ยงจากการออกผลิตภัณฑ์ใหม่ ความเสี่ยงจากการใช้งานเทคโนโลยีใหม่และความเสี่ยงภายในระบบสารสนเทศ
67.	Logging practices are independently reviewed periodically to ensure appropriate log management (e.g., access controls, retention, and maintenance).	บริษัทมีการตรวจสอบกระบวนการบริหารจัดการบันทึกเหตุการณ์อย่างสม่ำเสมอ เพื่อให้มั่นใจถึงความเพียงพอในกระบวนการควบคุม เช่น การกำหนดสิทธิของผู้ที่สามารถเข้าถึงและตรวจสอบบันทึกเหตุการณ์ ระยะเวลาการจัดเก็บบันทึกเหตุการณ์ที่เหมาะสมและเป็นไปตามกฎหมายหรือข้อกำหนด การแก้ไขเปลี่ยนแปลงบันทึกเหตุการณ์ เป็นต้น
68.	Issues and corrective actions from internal audits and independent testing/assessments are formally tracked to ensure procedures and control lapses are resolved in a timely manner.	ประเด็นข้อบกพร่องด้านการควบคุม และแผนการดำเนินการเพื่อแก้ไขข้อบกพร่องต่าง ๆ จากรายงานผลการตรวจสอบของผู้ตรวจสอบภายใน หรือผู้ตรวจประเมินอิสระได้รับการติดตามเพื่อให้มั่นใจถึงการดำเนินการปรับปรุงแก้ไขเป็นไปตามกำหนดการที่มีการระบุไว้อย่างเหมาะสม ทั้งนี้ แผนการดำเนินงานควรได้รับการติดตามและรายงานไปยังผู้บริหารระดับสูงที่เกี่ยวข้อง คณะกรรมการตรวจสอบหรือคณะกรรมการของบริษัท

No	Questionnaire	คำอธิบาย
Level – 2		
69.	The independent audit function validates that the institution's cybersecurity controls function is commensurate with the institution's risk and complexity.	การดำเนินการของผู้ตรวจสอบที่มีความเป็นอิสระ มีขอบเขตตรวจสอบครอบคลุมการควบคุมด้านความมั่นคงปลอดภัยทางไซเบอร์ เพื่อให้มั่นใจถึงระดับการควบคุมที่สอดคล้องกับระดับความเสี่ยงและความซับซ้อนทางเทคโนโลยีของบริษัท
70.	The independent audit function validates that the institution's third-party relationship management is commensurate with the institution's risk and complexity.	บริษัทมีผู้ตรวจสอบที่มีความเป็นอิสระ ที่มีขอบเขตการตรวจสอบครอบคลุมกระบวนการบริหารจัดการผู้ให้บริการภายนอก เพื่อให้มั่นใจถึงระดับการควบคุมที่สอดคล้องกับระดับความเสี่ยงและความซับซ้อนทางเทคโนโลยีของบริษัท
71.	The independent audit function validates that the institution's incident response program and resilience are commensurate with the institution's risk and complexity.	บริษัทมีผู้ตรวจสอบที่มีความเป็นอิสระ ที่มีขอบเขตการตรวจสอบครอบคลุมกระบวนการบริหารจัดการการตอบสนองและการรับมือต่อเหตุการณ์ภัยคุกคามไซเบอร์ (Incident response and resilience) เพื่อให้มั่นใจถึงระดับการควบคุมที่สอดคล้องกับระดับความเสี่ยงและความซับซ้อนทางเทคโนโลยีของบริษัท
Level – 3		
72.	The independent audit function validates that the institution's threat intelligence and collaboration are commensurate with the institution's risk and complexity.	บริษัทมีผู้ตรวจสอบที่มีความเป็นอิสระ ที่มีขอบเขตการตรวจสอบครอบคลุมในเรื่องการใช้ข้อมูลการข่าว (threat intelligence) และความร่วมมือด้านภัยคุกคามมีความเหมาะสมกับระดับความเสี่ยงและความซับซ้อนทางเทคโนโลยีของบริษัท
73.	Independent audits or reviews are used to identify gaps in existing security capabilities and expertise.	บริษัทมีผู้ตรวจสอบที่มีความเป็นอิสระ ที่มีขอบเขตการตรวจสอบครอบคลุมความเหมาะสมและความเพียงพอของระบบงานและความสามารถและความเชี่ยวชาญของบุคคลากรด้านความมั่นคงปลอดภัยสารสนเทศ
74.	Independent audits or reviews are used to identify cybersecurity weaknesses, root causes, and the potential impact to business units.	ผลการตรวจสอบโดยผู้ตรวจสอบที่มีความเป็นอิสระได้รับการรายงานไปยังผู้บริหารที่เกี่ยวข้อง เพื่อประเมินและระบุหาข้อบกพร่องของการควบคุมความมั่นคงปลอดภัยทางไซเบอร์ การวิเคราะห์สาเหตุของข้อบกพร่อง และผลกระทบที่อาจเป็นไปได้ในทางธุรกิจ

No	Questionnaire	คำอธิบาย
Level – 4		
75.	A formal process is in place for the independent audit function to update its procedures based on changes to the evolving threat landscape across the sector.	หน่วยงานตรวจสอบที่มีความเป็นอิสระ มีกระบวนการและขั้นตอนในการปรับปรุงขั้นตอนและแนวทางการตรวจสอบเพื่อตอบสนองต่อการเปลี่ยนแปลง และภัยคุกคามใหม่ ๆ ในภาคตลาดทุน เช่น ความเสี่ยงหรือภัยคุกคามเกิดใหม่ เหตุการณ์ด้านความมั่นคงปลอดภัยทางไซเบอร์ที่เกิดขึ้นในอุตสาหกรรม เป็นต้น
Level - 5		
76.	A formal process is in place for the independent audit function to update its procedures based on changes to the evolving threat landscape across other sectors the institution depends upon.	หน่วยงานตรวจสอบที่มีความเป็นอิสระ มีกระบวนการและขั้นตอนในการปรับปรุงขั้นตอนและแนวทางการตรวจสอบเพื่อตอบสนองต่อการเปลี่ยนแปลง และภัยคุกคามในภาคอุตสาหกรรมที่เกี่ยวข้อง โดยไม่จำกัดอยู่เพียงภาคอุตสาหกรรมการเงินและการลงทุน
77.	The independent audit function uses sophisticated data mining tools to perform continuous monitoring of cybersecurity processes or controls.	หน่วยงานตรวจสอบที่มีความเป็นอิสระ มีการใช้เครื่องมือวิเคราะห์ฐานข้อมูลที่ซับซ้อน หรือเครื่องมืออื่นใดเพื่อใช้ในการเฝ้าระวัง ตรวจสอบกระบวนการทำงานหรือการควบคุมด้าน cybersecurity อย่างต่อเนื่อง (Continuous monitoring)
Resources - Staffing		
Level - 1		
78.	Information security roles and responsibilities have been identified.	บริษัทมีการกำหนดและมอบหมายหน้าที่ความรับผิดชอบในการดูแลและรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศให้แก่ผู้บริหารและบุคลากรที่เกี่ยวข้อง ทั้งนี้ บทบาทหน้าที่ความรับผิดชอบควรได้รับการกำหนดและระบุอย่างชัดเจนในเอกสารบรรยายลักษณะงาน (Job description)
79.	Processes are in place to identify additional expertise needed to improve information security defences.	บริษัทมีกระบวนการในการประเมินความเพียงพอเพื่อการจัดหาทรัพยากรบุคคลและองค์ความรู้ในการปรับปรุงงานป้องกันและการบริหารจัดการด้านความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ
Level - 2		
80.	Management with appropriate knowledge and experience leads the institution's cybersecurity efforts.	บุคลากรระดับผู้บริหารด้านงานเทคโนโลยีสารสนเทศมีองค์ความรู้ ประสบการณ์ และความเชี่ยวชาญที่เพียงพอ ในการเป็นผู้นำและบริหารจัดการองค์กรในด้านความมั่นคงปลอดภัยทางไซเบอร์

No	Questionnaire	คำอธิบาย
81.	Staff with cybersecurity responsibilities have the requisite qualifications to perform the necessary tasks of the position.	ผู้ปฏิบัติงานที่รับผิดชอบด้านความมั่นคงปลอดภัยทางไซเบอร์ มีประสบการณ์และคุณสมบัติที่เหมาะสมสอดคล้องกับหน้าที่ความรับผิดชอบ เช่น มีคุณวุฒิที่เกี่ยวข้องโดยตรงในการบริหารจัดการความมั่นคงปลอดภัยทางไซเบอร์ หรือประสบการณ์และความเชี่ยวชาญจากการปฏิบัติงานเป็นระยะเวลาที่เหมาะสม หรือมีวุฒิบัตรที่เกี่ยวข้องในสายงานการรักษาความมั่นคงปลอดภัยทางไซเบอร์ เป็นต้น
82.	Employment candidates, contractors, and third parties are subject to background verification proportional to the confidentiality of the data accessed, business requirements, and acceptable risk.	บริษัทมีกระบวนการตรวจสอบประวัติผู้สมัครรับการคัดเลือกเป็นพนักงาน พนักงานจ้างเหมา หรือบริษัทผู้ให้บริการภายนอก โดยการตรวจสอบคุณสมบัตินั้นอาจทำโดยการตรวจสอบประวัติการทำงาน ประวัติอาชญากรรม หรือบัญชีผู้ไม่พึงประสงค์ของหน่วยงานกำกับดูแล ทั้งนี้ ขึ้นอยู่กับหน้าที่ความรับผิดชอบตามตำแหน่งงาน การเข้าถึงข้อมูลชั้นความลับ ข้อกำหนดทางธุรกิจ และความเสี่ยงที่ยอมรับได้
Level – 3		
83.	The institution has a program for talent recruitment, retention, and succession planning for the cybersecurity and resilience staffs.	บริษัทมีกระบวนการในการจัดหาผู้ที่มีความสามารถสูง กระบวนการในการสร้างและรักษาบุคลากร และแผนความก้าวหน้าทางสายอาชีพและการสืบทอดตำแหน่งงาน สำหรับพนักงานด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์
Level - 4		
84.	The institution benchmarks its cybersecurity staffing against peers to identify whether its recruitment, retention, and succession planning are commensurate.	บริษัทมีกระบวนเปรียบเทียบด้านทรัพยากรบุคคลกับบริษัทคู่เทียบในกลุ่มอุตสาหกรรมเพื่อให้มั่นใจถึงความเหมาะสมของกระบวนการในการสร้างและรักษาบุคลากรด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ และแผนความก้าวหน้าทางสายอาชีพและการสืบทอดตำแหน่งงาน
85.	Dedicated cybersecurity staff develops, or contributes to developing, integrated enterprise-level security and cyber defence strategies.	พนักงานผู้รับผิดชอบด้านความมั่นคงปลอดภัยทางไซเบอร์ มีการดำเนินการหรือมีส่วนร่วมในการพัฒนาระบบการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศระดับองค์กร และแผนกลยุทธ์ในการป้องกันภัยคุกคามทางไซเบอร์

No	Questionnaire	คำอธิบาย
Level - 5		
86.	The institution actively partners with industry associations and academia to inform curricula based on future cybersecurity staffing needs of the industry.	บริษัทมีการเข้าร่วมกับสมาคมภายในภาคอุตสาหกรรม หรือหน่วยงานด้านวิชาการ เพื่อร่วมกันศึกษาและจัดทำแผนความต้องการด้านบุคลากรในสายงานการรักษาความมั่นคงปลอดภัยทางไซเบอร์ เพื่อให้มั่นใจถึงความเพียงพอของการพัฒนาบุคลากร
Training & Culture - Training		
Level - 1		
87.	Annual information security training is provided.	บริษัทมีการจัดฝึกอบรมด้านความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ ให้แก่ พนักงานและผู้บริหาร เป็นประจำ หรืออย่างน้อยปีละ 1 ครั้ง
88.	Annual information security training includes incident response, current cyber threats (e.g., phishing, spear phishing, social engineering, and mobile security), and emerging issues.	หัวข้อการอบรมด้านความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศประจำปี ประกอบด้วย หัวข้อด้านแนวทางการรับมือเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ ภัยคุกคามทางไซเบอร์ที่เป็นประเด็นในปัจจุบัน เช่น การหลอกลวงแบบ phishing การหลอกลวงแบบ social engineer หรือ ความปลอดภัยในการใช้งานอุปกรณ์เคลื่อนที่ เป็นต้น รวมถึงเหตุการณ์ที่เกิดขึ้นในภาคการเงิน
89.	Situational awareness materials are made available to employees when prompted by highly visible cyber events or by regulatory alerts.	บริษัทมีช่องทางในการสื่อสารเพื่อสร้างความตระหนักหรือการแจ้งเตือนต่อพนักงานและผู้ที่เกี่ยวข้องอย่างทันท่วงที เมื่อมีการตรวจพบเหตุการณ์ด้านความมั่นคงปลอดภัยทางไซเบอร์ หรือการแจ้งเตือนจากหน่วยงานกำกับดูแล เช่น เมื่อตรวจพบเหตุการณ์หรือภัยคุกคามทางไซเบอร์ในช่องทางข่าวสาร เป็นต้น
Level – 2		
90.	The institution has a program for continuing cybersecurity training and skill development for cybersecurity staff.	บริษัทมีโปรแกรมฝึกอบรมทักษะและความรู้อย่างต่อเนื่องสำหรับพนักงานที่รับผิดชอบต่องานการรักษาความมั่นคงปลอดภัยทางไซเบอร์
91.	Management is provided cybersecurity training relevant to their job responsibilities.	บริษัทมีการจัดอบรมหัวข้อด้านความมั่นคงปลอดภัยทางไซเบอร์ที่เกี่ยวข้องกับงานที่รับผิดชอบอย่างสม่ำเสมอ ให้แก่ ผู้บริหารระดับสูง
92.	Business units are provided cybersecurity training relevant to their particular business risks.	บริษัทมีการจัดอบรมหัวข้อด้านความมั่นคงปลอดภัยทางไซเบอร์ ให้แก่ พนักงานและเจ้าหน้าที่ โดยเฉพาะในส่วนที่เกี่ยวข้องกับความเสี่ยงต่อธุรกิจ

No	Questionnaire	คำอธิบาย
Level – 3		
93.	Management incorporates lessons learned from social engineering and phishing exercises to improve the employee awareness programs.	บริษัทมีการปรับปรุงหัวข้อการฝึกอบรมและการสร้างความตระหนักด้านความมั่นคงปลอดภัยทางไซเบอร์ โดยอาศัยผลการทดสอบ social engineering หรือการทดสอบ phishing ที่มีการดำเนินการต่อกลุ่มพนักงานเป้าหมาย
94.	Cybersecurity awareness information is provided to retail customers and commercial clients at least annually.	บริษัทมีโครงการสร้างความตระหนัก โดยการสื่อสารข้อมูลด้านความมั่นคงปลอดภัยทางไซเบอร์ไปยังลูกค้าบุคคล และ ลูกค้านิติบุคคล อย่างน้อยปีละ 1 ครั้ง ทั้งนี้ ช่องทางการสื่อสารต้องไม่ก่อให้เกิดความเสี่ยงในการใช้เป็นช่องทางการหลอกลวง เช่น การส่ง e-mail phishing
95.	The institution routinely updates its training to security staff to adapt to new threats.	บริษัทมีการจัดอบรมให้แก่พนักงานด้านการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศอย่างสม่ำเสมอ เพื่อให้มีความเท่าทันในการรับมือกับภัยคุกคามเกิดใหม่
Level – 4		
96.	Independent directors are provided with cybersecurity training that addresses how complex products, services, and lines of business affect the institution's cyber risk.	บริษัทจัดให้มีการอบรมด้านความมั่นคงปลอดภัยทางไซเบอร์ให้แก่ กรรมการอิสระของบริษัท อย่างสม่ำเสมอ โดยต้องมีข้อมูลความเสี่ยงด้านความมั่นคงปลอดภัยทางไซเบอร์ต่อผลิตภัณฑ์และบริการ และลักษณะธุรกิจของบริษัท
Level – 5		
97.	Key performance indicators are used to determine whether training and awareness programs positively influence behaviour.	บริษัทมีการจัดทำดัชนีวัดผลด้านประสิทธิภาพเพื่อประเมินผลสัมฤทธิ์ของการจัดฝึกอบรมสร้างความตระหนักด้านความมั่นคงปลอดภัยทางไซเบอร์ว่ามีผลต่อการเปลี่ยนแปลงพฤติกรรมของพนักงานอย่างไร เพื่อให้เป็นแนวทางการปรับปรุงหัวข้อการฝึกอบรม
Training & Culture - Culture		
Level - 1		
98.	Management holds employees accountable for complying with the information security program.	ผู้บริหารมีความรับผิดชอบต่อการปฏิบัติตามกฎระเบียบและข้อบังคับด้านการรักษาความมั่นคงปลอดภัยสารสนเทศของพนักงานภายในบริษัท

No	Questionnaire	คำอธิบาย
Level - 2		
99.	The institution has formal standards of conduct that hold all employees accountable for complying with cybersecurity policies and procedures.	บริษัทมีการจัดทำมาตรการด้านความประพฤติและจริยธรรมสำหรับพนักงาน เพื่อให้มั่นใจถึงการปฏิบัติตามนโยบายและขั้นตอนการปฏิบัติงานด้านความมั่นคงปลอดภัยทางไซเบอร์ เช่น เอกสารลงนามการยอมรับและปฏิบัติตามนโยบายและกฎระเบียบด้านความมั่นคงปลอดภัยทางไซเบอร์ ก่อนเริ่มปฏิบัติงาน
100.	Employees have a clear understanding of how to identify and escalate potential cybersecurity issues.	บริษัทมีการจัดทำและสื่อสารแนวทางการปฏิบัติเมื่อพนักงานตรวจพบเหตุการณ์ด้านความมั่นคงปลอดภัยทางไซเบอร์ และแนวทางการแจ้งเหตุไปยังผู้รับผิดชอบ ทั้งนี้ การสื่อสารทำความเข้าใจให้แก่พนักงานอาจอยู่ในรูปแบบการแจ้งเตือนผ่านช่องทางการสื่อสารของบริษัท การฝึกอบรมสร้างความตระหนัก เป็นต้น
Level - 3		
101.	Management ensures performance plans are tied to compliance with cybersecurity policies and standards in order to hold employees accountable.	ผู้บริหารมีการพิจารณาหัวข้อการประเมินการปฏิบัติตามนโยบายและมาตรฐานด้านความมั่นคงปลอดภัยทางไซเบอร์ เป็นส่วนหนึ่งของการประเมินผลงานประจำปี เพื่อให้มั่นใจถึงความตระหนักและความรับผิดชอบของพนักงานในการปฏิบัติตามนโยบายฯ
102.	Cyber risk reporting is presented and discussed at the independent risk management meetings.	รายงานด้านความเสี่ยงทางไซเบอร์ ได้รับการนำเสนอและหารือในที่ประชุมผู้บริหารหรือคณะกรรมการบริหารความเสี่ยงที่มีความเป็นอิสระ
Level - 4		
103.	Management ensures continuous improvement of cyber risk cultural awareness.	ผู้บริหารของบริษัทมีหน้าที่ในการปรับปรุงกระบวนการอย่างต่อเนื่อง ในการสร้างความตระหนักด้านความเสี่ยงทางไซเบอร์ ให้แก่ พนักงาน ผู้บริหาร และผู้ที่เกี่ยวข้องในองค์กร
Level - 5		
104.	The institution leads efforts to promote cybersecurity culture across the sector and to other sectors that they depend upon.	บริษัทมีความเป็นผู้นำในการสร้างความตระหนักและส่งเสริมวัฒนธรรมด้านความมั่นคงปลอดภัยทางไซเบอร์ไปยังกลุ่มอุตสาหกรรมการเงินการลงทุน และกลุ่มอุตสาหกรรมที่เกี่ยวข้อง เช่น การจัดตั้งสมาคม หรือกลุ่มความร่วมมือในภาคอุตสาหกรรม การสร้างความร่วมมือด้านข้อมูลข่าวสาร จัดแคมเปญส่งเสริม awareness ในตลาดทุน เป็นต้น

2. Threat intelligence

No	Questionnaire	คำอธิบาย
Threat intelligence - Threat Intelligence and Information		
Level - 1		
105.	The institution belongs or subscribes to a threat and vulnerability information sharing source(s) that provides information on threats (e.g., Financial Services Information Sharing and Analysis Center [FS-ISAC], U.S. Computer Emergency Readiness Team [US-CERT], TCM Cert, Thai Cert, TB Cert)	บริษัทเข้าร่วม หรือเป็นสมาชิกในแหล่งข้อมูลสำหรับความร่วมมือด้านการข่าวภัยคุกคามด้านความปลอดภัยทางไซเบอร์ หรือช่องโหว่ทางเทคนิค เช่น ● Financial Services Information Sharing and Analysis Center [FS-ISAC], ● U.S. Computer Emergency Readiness Team [US-CERT], ● Thai Capital Market Cert [TCM-CERT], ● Thai Cert, ● Thai Bank Cert [TB-CERT] เป็นต้น
106.	Threat information is used to monitor threats and vulnerabilities.	ข้อมูลการข่าวได้รับการใช้งานในการติดตามภัยคุกคามและช่องโหว่ทางเทคนิค เช่น การตรวจสอบข้อมูลการสื่อสารไปยังหมายเลข IP Address หรือโดเมนปลายทางต้องสงสัย (Indicator of Compromise: IOC) หรือการใช้ข้อมูลช่องโหว่ทางเทคนิคที่มีการค้นพบใหม่เพื่อปรับปรุงระบบวิเคราะห์พฤติกรรมทางเครือข่าย เป็นต้น
Level - 2		
107.	Threat information received by the institution includes analysis of tactics, patterns, and risk mitigation recommendations.	บริษัทรับข้อมูลการข่าว ที่ประกอบด้วย ข้อมูลเชิงวิเคราะห์ของเทคนิคและพฤติกรรมของผู้บุกรุกโจมตีระบบหรือภัยคุกคามที่เกิดขึ้น ข้อเสนอแนะเพื่อใช้ในการจัดการความเสี่ยงและจัดทำแนวทางการป้องกันความเสี่ยง
Level - 3		
108.	A formal threat intelligence program is implemented and includes subscription to threat feeds from external providers and internal sources.	บริษัทมีการจัดทำกระบวนการบริหารจัดการข้อมูลการข่าวด้านความมั่นคงปลอดภัยทางไซเบอร์ ที่ครอบคลุมถึงการจัดหาข้อมูลการข่าวโดยการเป็นสมาชิกจากผู้ให้บริการภายนอก และแหล่งข้อมูลจากภายใน
109.	A read-only, central repository of cyber threat intelligence is maintained.	ข้อมูลการข่าวที่มีการรวบรวมได้รับการจัดเก็บในฐานข้อมูลกลางเพื่อใช้ในการอ้างอิง โดยมีการจำกัดสิทธิในการเข้าถึงเฉพาะผู้เกี่ยวข้องในลักษณะให้อ่านอย่างเดียว เพื่อป้องกันการเข้าถึงเพื่อใช้ประโยชน์ข้อมูลสำคัญโดยผู้ไม่ได้รับอนุญาต หรือการแก้ไขเปลี่ยนแปลงข้อมูล

No	Questionnaire	คำอธิบาย
Level - 4		
110.	Threat intelligence is automatically received from multiple sources in real time.	บริษัทมีการรับข้อมูลการข่าวจากหลายแหล่งข้อมูลในรูปแบบทันทีและตลอดเวลา (Real time) เพื่อให้ผู้รับผิดชอบมั่นใจในการรับมือกับภัยคุกคามด้านความมั่นคงปลอดภัยทางไซเบอร์ รวมถึงได้รับข้อมูลอย่างครบถ้วนและมีความสามารถในการรับมือเหตุการณ์ได้อย่างทันเวลา
111.	The institution's threat intelligence includes information related to geopolitical events that could increase cybersecurity threat levels.	บริษัทมีการรับข้อมูลการข่าวจากแหล่งข้อมูลที่ระบุถึงข้อมูลทางภูมิศาสตร์ ที่แสดงถึงความน่าจะเป็นด้านภัยคุกคามอันอาจจะเกิดขึ้นในภูมิภาคและมีนัยต่อบริษัท
Level - 5		
112.	The institution is investing in the development of new threat intelligence and collaboration mechanisms (e.g., technologies, business processes) that will transform how information is gathered and shared.	บริษัทมีการลงทุนในการพัฒนากระบวนการและความร่วมมือด้านการข่าว เช่น การพัฒนาเทคโนโลยีหรือกระบวนการที่จำเป็น เพื่อสร้างความร่วมมือในการรวบรวมและแบ่งปันข้อมูลในกลุ่มอุตสาหกรรม
Monitoring and Analyzing - Monitoring and Analyzing		
Level - 1		
113.	Audit log records and other security event logs are reviewed and retained in a secure manner.	บริษัทมีการจัดเก็บและจัดให้มีกระบวนการสอบทานบันทึกเหตุการณ์เพื่อการตรวจสอบ (audit log) และเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ (security event log) อย่างสม่ำเสมอ ทั้งนี้ บันทึกเหตุการณ์มีการจัดเก็บและรักษาอย่างปลอดภัย เป็นระยะเวลาที่เหมาะสมอันอาจจะอยู่ทั้งในรูปบันทึกเหตุการณ์แบบ Online หรือบันทึกเหตุการณ์แบบ Offline ในสื่อบันทึกข้อมูล
114.	Computer event logs are used for investigations once an event has occurred.	บริษัทมีการใช้ประโยชน์จากบันทึกเหตุการณ์ที่มีการจัดเก็บ (event log) เพื่อการสืบสวนเหตุการณ์เมื่อมีเหตุการณ์ต้องสงสัยหรือมีเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ ทั้งนี้ บันทึกเหตุการณ์ต้องมีการเก็บรักษาอย่างปลอดภัยเพื่อป้องกันการแก้ไขเปลี่ยนแปลง ลบทำลาย และเพื่อคงความน่าเชื่อถือในการใช้งาน

No	Questionnaire	คำอธิบาย
Level - 2		
115.	A process is implemented to monitor threat information to discover emerging threats.	บริษัทมีการจัดให้มีกระบวนการในการติดตามตรวจสอบข้อมูลด้านภัยคุกคามจากแหล่งข้อมูลต่าง ๆ เพื่อค้นหาภัยคุกคามในรูปแบบใหม่อันอาจจะเกิดขึ้นกับบริษัท
116.	Security processes and technology are centralized and coordinated in a Security Operations Center (SOC) or equivalent.	บริษัทมีกระบวนการและเทคโนโลยีด้านความมั่นคงปลอดภัยสารสนเทศที่เพียงพอสำหรับศูนย์ปฏิบัติการด้านความมั่นคงปลอดภัย (Security Operation Center: SOC) หรือผู้รับผิดชอบที่ได้รับมอบหมายในการติดตาม วิเคราะห์และแก้ไขเหตุการณ์ผิดปกติด้านความมั่นคงปลอดภัย เช่น การใช้เทคโนโลยีระบบจัดเก็บ บริหารจัดการและวิเคราะห์ข้อมูลความปลอดภัยของระบบเครือข่าย (Security information and event management (SIEM))
117.	Monitoring systems operate continuously with adequate support for efficient incident handling.	ระบบและกระบวนการติดตามเหตุการณ์ผิดปกติด้านความมั่นคงปลอดภัยสารสนเทศได้รับการติดตามเฝ้าระวังอย่างต่อเนื่อง หากมีการแจ้งเตือนเหตุการณ์ต้องสงสัย บริษัทมีการจัดทำกระบวนการสนับสนุนในการรองรับและจัดการเหตุการณ์ เช่น การแจ้งเตือนไปยังผู้เกี่ยวข้องเพื่อวิเคราะห์เหตุการณ์ การยืนยันเหตุ การส่งต่อ (Escalation) ไปยังผู้รับผิดชอบในการแก้ไขเหตุการณ์ รวบรวมและจัดเก็บหลักฐาน และการกู้คืนระบบงาน
Level – 3		
118.	A threat intelligence team is in place that evaluates threat intelligence from multiple sources for credibility, relevance, and exposure.	บริษัทมีทีมที่รับผิดชอบในการวิเคราะห์ข้อมูลการข่าวที่มาจากหลายแหล่งข้อมูลเพื่อตรวจสอบยืนยันความน่าเชื่อถือของข้อมูล ความเกี่ยวข้องและเชื่อมโยงกับบริษัท และความเสียหายอันอาจจะเกิดขึ้นเมื่อเกิดเหตุการณ์ ซึ่งจะทำให้ผู้รับผิดชอบในการรับมือกับภัยคุกคามด้านความมั่นคงปลอดภัยทางไซเบอร์ได้รับข้อมูลที่มีคุณภาพ
119.	Threat intelligence is analyzed to develop cyber threat summaries including risks to the institution and specific actions for the institution to consider.	บริษัทมีการวิเคราะห์ข้อมูลการข่าว เพื่อจัดทำรายงานสรุปข้อมูลเหตุการณ์สำคัญ ความเสี่ยงที่มีต่อบริษัท และกิจกรรมที่ต้องมีการดำเนินการเพื่อส่งต่อให้ผู้ปฏิบัติงานดำเนินมาตรการที่จำเป็นในการป้องกันเหตุการณ์

No	Questionnaire	คำอธิบาย
Level - 4		
120.	A dedicated cyber threat identification and analysis committee or team exists to centralize and coordinate initiatives and communications.	บริษัทมีการจัดตั้งทีมงานหรือคณะกรรมการในการติดตามข้อมูลและวิเคราะห์ข้อมูลการข่าว เพื่อให้การเตรียมการรับมือ การประสานงาน และการสื่อสารไปยังบุคคลที่เกี่ยวข้องเป็นไปอย่างมีประสิทธิภาพและประสิทธิผล
121.	Emerging internal and external threat intelligence and correlated log analysis are used to predict future attacks.	บริษัทมีการรวบรวมข้อมูลการข่าวทั้งจากภายใน และแหล่งข้อมูลภายนอก วิเคราะห์ร่วมกับ log เหตุการณ์ของบริษัท เพื่อเชื่อมโยงเหตุการณ์ติดตามและทำนายการโจมตีอันอาจจะเกิดขึ้นในอนาคต
122.	Threat intelligence is used to update architecture and configuration standards.	บริษัทมีการใช้ข้อมูลการข่าวที่มีการรวบรวม เพื่อดำเนินการปรับปรุงด้านสถาปัตยกรรมความปลอดภัยของบริษัท รวมถึงการปรับปรุงค่ามาตรฐานด้านความปลอดภัย (Security configuration standard) อันเป็นมาตรการเชิงป้องกันต่อเหตุการณ์ภัยคุกคาม
Level - 5		
123.	The institution uses multiple sources of intelligence, correlated log analysis, alerts, internal traffic flows, and geopolitical events to predict potential future attacks and attack trends.	บริษัทมีการใช้ข้อมูลการข่าวจากหลายแหล่งข้อมูล ข้อมูลจากระบบวิเคราะห์และเชื่อมโยงเหตุการณ์ ข้อมูลการแจ้งเตือนจากแหล่งข้อมูล ข้อมูลจราจรเครือข่าย และเหตุการณ์ที่เกิดขึ้นในภูมิภาค เพื่อทำนายและประเมินแนวโน้มการเกิดเหตุการณ์ที่มีลักษณะคล้ายคลึงกันต่อระบบเครือข่ายและข้อมูลสารสนเทศของบริษัท
124.	IT systems automatically detect configuration weaknesses based on threat intelligence and alert management so actions can be prioritized.	บริษัทมีการจัดหาเครื่องมือในการตรวจสอบจุดอ่อนหรือช่องโหว่ของค่าคอนฟิกูเรชั่นด้านความปลอดภัยแบบอัตโนมัติที่เชื่อมโยงได้กับข้อมูลข่าวกรองหรือฐานข้อมูลและการเตือนภัย เพื่อให้ผู้บริหารที่เกี่ยวข้องสามารถจัดระดับความสำคัญในการแก้ไขปัญหา
Information Sharing - Information Sharing		
Level - 1		
125.	Information security threats are gathered and shared with applicable internal employees.	มีการรวบรวม สื่อสาร และแจ้งเตือนภัยคุกคามด้านความมั่นคงปลอดภัยสารสนเทศไปยังพนักงานภายในองค์กร เพื่อให้ทราบถึงความเสี่ยง วิธีสังเกตเมื่อเกิดเหตุการณ์ วิธีการหลีกเลี่ยงและข้อควรปฏิบัติเมื่อเกิดเหตุการณ์ ผ่านการสื่อสารผ่านช่องทางที่กำหนด เช่น การแจ้งเตือนผ่านระบบ e-mail หรือประกาศของบริษัท เป็นต้น

No	Questionnaire	คำอธิบาย
126.	Contact information for law enforcement and the regulator(s) is maintained and updated regularly.	บริษัทมีการจัดเตรียมข้อมูลช่องทางการติดต่อสำหรับหน่วยงานบังคับใช้กฎหมาย และหน่วยงานกำกับดูแลที่เกี่ยวข้อง เพื่อให้สามารถดำเนินการได้อย่างรวดเร็ว ข้อมูลการติดต่อต้องได้รับการปรับปรุงให้เป็นปัจจุบันและถูกต้องอย่างสม่ำเสมอ
127.	Information about threats is shared with law enforcement and regulators when required or prompted.	บริษัทมีกระบวนการในการแจ้งไปยังหน่วยงานบังคับใช้กฎหมายและหน่วยงานกำกับดูแล เมื่อเกิดเหตุหรือเมื่อมีสถานการณ์จำเป็นโดยไม่ชักช้า
Level – 2		
128.	A formal and secure process is in place to share threat and vulnerability information with other entities.	บริษัทมีการจัดเตรียมกระบวนการเพื่อใช้ในการสื่อสารและแจ้งข้อมูลด้านภัยคุกคาม หรือข้อมูลเกี่ยวกับช่องโหว่ด้านความมั่นคงปลอดภัยสารสนเทศ ไปยังหน่วยงานภายนอก ทั้งนี้ กระบวนการในที่นี้ควรพิจารณาถึงขั้นตอนและบุคลากรผู้มีอำนาจในการเปิดเผยข้อมูล และการกำหนดประเภทและชนิดข้อมูลที่สามารถเปิดเผยได้และข้อมูลไม่พึงเปิดเผย
129.	A representative from the institution participates in law enforcement or information-sharing organization meetings.	บริษัทมีการส่งตัวแทนเข้าร่วม เพื่อสร้างความร่วมมือกับหน่วยงานบังคับใช้กฎหมาย หรือเข้าร่วมประชุมกับหน่วยงานที่ทำงานด้านการแชร์ข้อมูลด้านไซเบอร์
Level – 3		
130.	Information is shared proactively with the industry, law enforcement, regulators, and information-sharing forums.	บริษัทมีการดำเนินการเชิงรุกในการเปิดเผยข้อมูลที่สามารถเปิดเผยได้ ให้แก่ หน่วยงานด้านการบังคับใช้กฎหมาย หน่วยงานกำกับดูแล และ/หรือกลุ่มความร่วมมือด้านข้อมูลข่าวสารในอุตสาหกรรม
131.	A process is in place to communicate and collaborate with the public sector regarding cyber threats.	บริษัทมีการจัดทำกระบวนการในการสื่อสารและการสร้างความร่วมมือกับภาคประชาสังคม ทางด้านภัยคุกคามทางไซเบอร์ เช่น การแจ้งเตือน หรือการสร้างความตระหนักถึงภัยคุกคามและข้อควรปฏิบัติ เพื่อป้องกันความเสี่ยงจากการใช้งานระบบอิเล็กทรอนิกส์แก่ลูกค้า ผู้ใช้งานและบุคคลทั่วไป
Level - 4		
132.	Management communicates threat intelligence with business risk context and specific risk management recommendations to the business units.	บริษัทโดยผู้บริหารมีการสื่อสารด้านข้อมูลการข่าวและภัยคุกคาม โดยชี้ให้เห็นถึงความเสี่ยงในรูปแบบที่เข้าใจง่ายและเชื่อมโยงกับความเสี่ยงทางธุรกิจ พร้อมทั้งสื่อสารกระบวนการป้องกันและบริหารความเสี่ยง ให้แก่หน่วยงานทางธุรกิจ

No	Questionnaire	คำอธิบาย
133.	A network of trust relationships (formal and/or informal) has been established to evaluate information about cyber threats.	บริษัทมีการเป็นสมาชิกเครือข่ายที่น่าเชื่อถือระหว่างกลุ่มบุคคลหรือบริษัท ไม่ว่าจะในรูปแบบเป็นทางการหรือไม่เป็นทางการ เพื่อสร้างความร่วมมือในการแบ่งปันข้อมูล และประเมินข้อมูลร่วมกันด้านภัยคุกคามด้านความปลอดภัยทางไซเบอร์
Level - 5		
134.	A mechanism is in place for sharing cyber threat intelligence with business units in real time including the potential financial and operational impact of inaction.	บริษัทมีกระบวนการในการสื่อสารด้านข้อมูลการข่าวและภัยคุกคามให้แก่หน่วยงานทางธุรกิจ แบบทันทีและตลอดเวลา (Real time) เพื่อแจ้งเตือนเหตุการณ์ภัยคุกคามให้ผู้บริหารหน่วยงานทางธุรกิจรับทราบพร้อมทั้งข้อมูลด้านความเสียหายอันอาจจะเกิดขึ้นต่อกิจกรรมทางธุรกิจ และผลเสียหายด้านการปฏิบัติงาน
135.	A system automatically informs management of the level of business risk specific to the institution and the progress of recommended steps taken to mitigate the risks.	บริษัทมีระบบในการแจ้งเตือนเหตุการณ์ไปยังผู้บริหารระดับสูงของบริษัทแบบอัตโนมัติ เมื่อเกิดเหตุภัยคุกคามโดยการแจ้งเตือนประกอบด้วยข้อมูลภัยคุกคาม ระดับความเสี่ยงของภัยคุกคามที่มีต่อบริษัท และข้อเสนอแนะในการป้องกันความเสี่ยง

3. Cybersecurity Controls

No	Questionnaire	คำอธิบาย
Preventative Controls - Infrastructure Management		
Level - 1		
136.	Network perimeter defence tools (e.g., border router and firewall) are used.	บริษัทมีการจัดหาเครื่องมือเพื่อควบคุมการเข้าถึงเครือข่าย เพื่อติดตั้งอยู่ระหว่างเครือข่ายภายในบริษัทและเครือข่ายภายนอก เช่น อุปกรณ์เราท์เตอร์ที่มีการกำหนด Access Control List (ACL) หรืออุปกรณ์ไฟร์วอลล์ เป็นต้น
137.	Up to date antivirus and anti-malware tools are used on key enterprise communication channel i.e. Server, Mail, Internet)	บริษัทมีการติดตั้งระบบป้องกันไวรัส และโปรแกรมไม่พึงประสงค์ สำหรับควบคุมช่องทางการสื่อสารสำคัญระหว่างบริษัทและบุคคลภายนอก เช่น การติดตั้งระบบป้องกันไวรัสบนเครื่องแม่ข่าย ระบบอีเมล ระบบให้บริการอินเทอร์เน็ต เป็นต้น ทั้งนี้ โปรแกรมป้องกันไวรัส และโปรแกรมไม่พึงประสงค์ต้องมีขีดความสามารถในการปรับปรุงฐานข้อมูล และโปรแกรมให้มีความเป็นปัจจุบันอย่างสม่ำเสมอและยังอยู่ในการสนับสนุนจากบริษัทผู้ผลิต
138.	Systems configurations (for servers, desktops, routers, etc.) follow industry standards and are enforced.	บริษัทมีการจัดทำค่าความปลอดภัยมาตรฐาน (Security configuration baseline) โดยอ้างอิงค่าแนะนำที่ได้รับการยอมรับเป็นมาตรฐาน เช่น SANS CIS เป็นต้น และค่าความปลอดภัยมาตรฐานดังกล่าวได้รับการติดตั้งบังคับใช้สำหรับอุปกรณ์สารสนเทศสำคัญของบริษัท เช่น เครื่องแม่ข่าย เครื่องคอมพิวเตอร์ อุปกรณ์เราท์เตอร์ เป็นต้น
139.	Ports, functions, protocols and services are prohibited if no longer needed for business purposes.	บริษัทมีการปิดหรือยกเลิกการใช้งานบริการทางเครือข่าย โปรโตคอล หรือช่องทางการสื่อสารที่ไม่มีการใช้งานแล้ว หรือไม่มีความจำเป็นทางธุรกิจ โดยอาจมีการควบคุมโดยอุปกรณ์ป้องกันและรักษาความปลอดภัยเครือข่าย ไฟร์วอลล์ อุปกรณ์เครือข่ายเราท์เตอร์ หรือการยกเลิกบริการบนเครื่องแม่ข่ายระบบงาน เป็นต้น
140.	Access to make changes to systems configurations (including virtual machines and hypervisors) is controlled and monitored.	บริษัทมีการควบคุมการเข้าถึงอุปกรณ์สำคัญด้านเทคโนโลยีสารสนเทศ เครื่องแม่ข่าย ระบบเครือข่าย ระบบเครื่องแม่ข่ายและเครือข่ายเสมือน (Virtualised system) ในการควบคุมและติดตามการแก้ไขเปลี่ยนแปลงค่าคอนฟิกูเรชั่น เช่น การควบคุมบัญชี

No	Questionnaire	คำอธิบาย
		และการติดตามการใช้งานบัญชีผู้ใช้งานที่มีสิทธิระดับสูง (Privilege) กระบวนการควบคุมและบริหารการแก้ไขเปลี่ยนแปลงที่ครอบคลุมการแก้ไขค่าคอนฟิกูเรชั่น เป็นต้น
141.	System sessions are locked after a pre-defined period of inactivity and are terminated after pre-defined conditions are met.	บริษัทมีมาตรการระงับและยกเลิกการเข้าถึงระบบงานสำคัญ เมื่อไม่มีกิจกรรมการเคลื่อนไหว หรือไม่มีการใช้งาน (Session time out) เป็นระยะเวลาที่กำหนด หรือเมื่อมีการใช้งานผิดปกติหรือการใช้งานตามเงื่อนไขที่กำหนดไว้ล่วงหน้า
142.	Wireless network environments require security settings with strong encryption for authentication and transmission. (*N/A if there are no wireless networks.)	บริษัทมีการใช้งานเทคโนโลยีการเข้ารหัสโดยวิธีและเทคนิคที่ได้รับการยอมรับในอุตสาหกรรม ในขั้นตอนการยืนยันและพิสูจน์ตัวตน และ การรับส่งข้อมูลผ่านเครือข่ายไร้สาย (Wireless network)
143.	Guest wireless networks are fully (at least logically) segregated from the internal network(s). (*N/A if there are no wireless networks.)	บริการเครือข่ายไร้สายสำหรับบุคคลภายนอกบริษัท (Guest Wifi) ได้รับการแบ่งแยกจากเครือข่ายไร้สายสำหรับพนักงานภายในบริษัท โดยการแบ่งแยกสามารถทำได้ทาง Logical เช่น การแบ่งกลุ่มเครือข่ายที่มีการควบคุมการเข้าถึง หรือ การแบ่งแยกทาง Physical เช่น การแบ่งแยกอุปกรณ์ Access Point และแบ่งแยกเครือข่าย
Level - 2		
144.	There is a firewall at each Internet connection and between any Demilitarized Zone (DMZ) and internal network(s).	บริษัทมีการติดตั้ง firewall ทุกจุดเชื่อมต่อ ทั้งการเชื่อมต่อระหว่างเครือข่าย Internet รวมถึงจุดเชื่อมต่อระหว่างเครือข่ายที่ให้บุคคลภายนอกเข้าถึง (DMZ) และเครือข่ายภายใน (Internal network)
145.	Antivirus and intrusion detection/prevention systems (IDS/IPS) detect and block actual and attempted attacks or intrusions.	บริษัทมีการติดตั้งระบบป้องกันไวรัส และระบบตรวจสอบและวิเคราะห์พฤติกรรมทางเครือข่าย เพื่อตรวจจับ และระงับความพยายามในการบุกรุกโจมตีระบบ
146.	Technical controls prevent unauthorized devices, including rogue wireless access devices and removable media, from connecting to the internal network(s).	บริษัทมีมาตรการควบคุมเพื่อป้องกันการใช้งานอุปกรณ์ที่ไม่ได้รับอนุญาต ได้แก่ การติดตั้งอุปกรณ์เครือข่ายไร้สายที่ไม่ได้รับการลงทะเบียนไว้ และ การใช้งานอุปกรณ์ที่สามารถถอดเคลื่อนย้ายได้ ในการเชื่อมต่อกับอุปกรณ์เครื่องคอมพิวเตอร์ หรือ เครือข่ายของบริษัท มาตรการดังกล่าว เช่น การตรวจค้นหาเครือข่ายไร้สาย การระงับและป้องกันการใช้งาน USB หรือ สื่อบันทึกข้อมูล CD/DVD เป็นต้น

No	Questionnaire	คำอธิบาย
147.	A risk-based solution is in place at the institution or Internet hosting provider to mitigate disruptive cyber attacks (e.g., DDoS attacks).	บริษัทมีการป้องกันความเสียหายหรือการหยุดชะงักของการให้บริการจากการโจมตีทางไซเบอร์ เช่น DDoS โดยพิจารณาถึงความเสี่ยง เช่น การจัดเตรียมช่องทางการสื่อสารสำรอง การจัดเตรียมมาตรการป้องกันโดยข้อตกลงระหว่างบริษัทและบริษัทผู้ให้บริการเครือข่ายในการคัดกรองข้อมูลจราจรทางเครือข่ายจากแหล่งที่มาที่เป็นการโจมตี การใช้บริการเช่น Clean pipe เป็นต้น
148.	Critical systems supported by legacy technologies are regularly reviewed to identify for potential vulnerabilities, upgrade opportunities, or new defence layers.	บริษัทมีการสอบทานและประเมินความเสี่ยงจากการใช้งานเทคโนโลยีที่ไม่ได้รับการพัฒนาต่อยอด (Legacy technology) เพื่อประเมินความเสี่ยงจากการไม่ได้รับการสนับสนุน หรือการไม่ได้รับการปรับปรุงชุดโปรแกรมแก้ไขข้อบกพร่องด้านความปลอดภัยสารสนเทศ (Security patch) เพื่อจัดทำแนวทางป้องกันความเสี่ยง หรือ แผนการปรับปรุงและ/หรือการจัดหาระบบงานทดแทน
Level - 3		
149.	The enterprise network is segmented in multiple, separate trust/security zones with defense-in-depth strategies (e.g., logical network segmentation, hard backups, air gapping) to mitigate attacks.	เครือข่ายขององค์กร (Enterprise network) ต้องมีการแยก Zone ของ network และมีการกำหนดมาตรการการป้องกันเป็นลำดับชั้น (Defense-in-depth strategies) เช่น การแยก network Zone ระหว่างบุคคลภายนอกและ network ภายใน (Air gapping) เพื่อที่จะลดโอกาสถูกโจมตี
150.	Security controls are used for remote access to all administrative consoles, including restricted virtual systems.	บริษัทมีการควบคุมการใช้งานบัญชีผู้ใช้งานที่มีสิทธิระดับสูงในการบริหารจัดการระบบ (Administrative console) ที่มีการเข้าถึงจากเครือข่ายระยะไกล (Remove access) รวมถึงการเข้าถึงเครื่องแม่ข่ายที่มีลักษณะเป็นเครื่องแม่ข่ายเสมือน (Virtualized system) โดยประกอบไปด้วยมาตรการ เช่น มาตรการสื่อสารผ่านช่องทางที่ปลอดภัยที่มีการเข้ารหัส การกำหนดหมายเลขประจำตัวเครือข่าย (IP Address) อย่างเฉพาะเจาะจงให้อยู่ในกลุ่มเครื่องหรือเครือข่ายที่ได้รับอนุญาตเท่านั้น มาตรการใช้งานการยืนยันและพิสูจน์ตัวตนแบบ Multi-factor เป็นต้น

No	Questionnaire	คำอธิบาย
151.	Wireless network environments have perimeter firewalls that are implemented and configured to restrict unauthorized traffic. (*N/A if there are no wireless networks.)	การให้บริการเครือข่ายไร้สายในการเข้าถึงเครือข่ายภายในบริษัท ได้รับการป้องกันและควบคุมการเข้าถึงโดยระบบรักษาความปลอดภัยเครือข่าย ไฟร์วอลล์ หรืออุปกรณ์เทียบเคียง ทั้งนี้บริษัทควรมีมาตรการรักษาความปลอดภัยบังคับสำหรับเครือข่ายไร้สายเทียบเท่ากับการเข้าถึงผ่านเครือข่ายภายนอก (Perimeter network)
152.	Wireless networks use strong encryption with encryption keys that are changed frequently. (*N/A if there are no wireless networks.)	การให้บริการเครือข่ายแบบไร้สายของบริษัทมีการใช้งานเทคโนโลยีการเข้ารหัสที่มีความปลอดภัย และกุญแจการเข้ารหัส (Encryption key) ได้รับการเปลี่ยนแปลงตามรอบเวลาที่กำหนด
153.	The broadcast range of the wireless network(s) is confined to institution-controlled boundaries. (*N/A if there are no wireless networks.)	บริษัทมีการกำหนดและควบคุมความแรงของสัญญานเครือข่ายแบบไร้สาย เพื่อให้อยู่ในขอบเขตที่ตั้งของสำนักงานของบริษัท เพื่อป้องกันความเสี่ยงจากการดักจับสัญญานจากบุคคลภายนอก
Level - 4		
154.	Only one primary function is permitted per server to prevent functions that require different security levels from co-existing on the same server.	บริษัทมีการกำหนดหน้าที่หลักของ server แต่ละเครื่อง (1 server ไม่ควรมีหลายหน้าที่) เพื่อที่จะสามารถกำหนดมาตรการการป้องกันได้อย่างเหมาะสม
155.	Anti-spoofing measures are in place to detect and block forged source IP addresses from entering the network.	บริษัทมีมาตรการป้องกันความพยายามในการใช้งานและการปลอมแปลงหมายเลขประจำตัวเครือข่าย (IP Address) ต้นทางเป็นหมายเลขเครือข่ายภายใน หรือ IP Spoofing โดยการกำหนดมาตรการ เช่น ACL IP Spoofing บนอุปกรณ์เราท์เตอร์ หรือ ไฟร์วอลล์
Level - 5		
156.	The institution risk scores all of its infrastructure assets and updates in real time based on threats, vulnerabilities, or operational changes.	คะแนนของประเมินความเสี่ยง (Risk score) ขององค์กรต้อง update และสะท้อนการเปลี่ยนแปลงของภัยคุกคาม/ช่องโหว่ หรือ Operational change ได้อย่างทันท่วงที (real time)
157.	Automated controls are put in place based on risk scores to infrastructure assets, including automatically disconnecting affected assets.	บริษัทมีระบบหรือมาตรการวิเคราะห์พฤติกรรมผู้ใช้งานเครือข่าย หรืออุปกรณ์สารสนเทศ (Behavioural based security) เพื่อวิเคราะห์ระดับความเสี่ยง และการยกเลิกการเชื่อมต่อกับอุปกรณ์ที่ผิดปกติโดยอัตโนมัติ
158.	The institution proactively seeks to identify control gaps that may be used as part of a zero-day attack.	บริษัทหาจุดบอดในการควบคุมและป้องกันความเสี่ยงจากการบุกรุกโจมตีประเภท Zero-day attack อย่างจริงจัง

No	Questionnaire	คำอธิบาย
Preventative Controls - Access and Data Management		
Level - 1		
159.	Employee access is granted to systems and confidential data based on job responsibilities and the principles of least privilege.	บริษัทมีกระบวนการควบคุมการเข้าถึงระบบงาน และข้อมูลชั้นความลับของบริษัท โดยพิจารณาถึงการให้สิทธิตามหน้าที่ความรับผิดชอบ และเป็นไปตามหลักการให้สิทธิเท่าที่จำเป็นเท่านั้น โดยการควบคุมเช่น การกำหนดตารางสิทธิมาตรฐานสำหรับผู้ใช้งานในแต่ละส่วนงานและระดับการเข้าถึง การร้องขอและอนุมัติสิทธิการเข้าถึงโดยผู้มีอำนาจ เป็นต้น
160.	Elevated privileges (e.g., administrator privileges) are limited and tightly controlled (e.g., assigned to individuals, not shared, and require stronger password controls).	บริษัทมีการควบคุมการเข้าถึงและใช้งานบัญชีผู้ใช้งานที่มีสิทธิระดับสูง (Administrative Privilege) ครอบคลุมถึงการกำหนดผู้รับผิดชอบโดยตรงของบัญชีผู้ใช้งานและระงับการใช้งานบัญชีผู้ใช้งานร่วมกัน การควบคุมรหัสผ่านของบัญชีผู้ใช้งาน เป็นต้น
161.	User access reviews are performed periodically for all systems and applications based on the risk to the application or system.	บริษัทมีการสอบทานความเหมาะสมของสิทธิการใช้งานสำหรับระบบงานอย่างสม่ำเสมอ โดยมีรอบการสอบทานตามความเสี่ยงของระบบงานและข้อมูลสารสนเทศ
162.	Changes to physical and logical user access, including those that result from voluntary and involuntary terminations, are submitted to and approved by appropriate personnel.	บริษัทมีการควบคุมการเข้าถึงพื้นที่ปฏิบัติงาน (Physical access) และการเข้าถึงระบบงาน โดยจัดให้มีขั้นตอนการร้องขอ และอนุมัติการให้สิทธิจากผู้มีอำนาจอย่างเป็นลายลักษณ์อักษร โดยกระบวนการบริหารจัดการบัญชีผู้ใช้งานครอบคลุมถึง การร้องขอเพื่อสร้างบัญชีผู้ใช้งาน การเปลี่ยนแปลงสิทธิการใช้งาน และการยกเลิกสิทธิการใช้งานทั้งจากการลาออกหรือพ้นสภาพความเป็นพนักงานโดยการไม่สมัครใจ
163.	Identification and authentication are required and managed for access to systems, applications, and hardware.	บริษัทมีการบังคับใช้มาตรการระบุตัวตน (Identification) เช่น การใช้งาน User ID หรือ Certificate และมาตรการพิสูจน์ตัวตน (Authentication) ในการจัดการและเข้าถึงระบบโปรแกรม และอุปกรณ์ เช่น การใช้งานรหัสผ่าน ในการบริหารจัดการเข้าถึงระบบงานภายใน
164.	Access controls include password complexity, password expiration interval, and limits to password attempts and reuse.	บริษัทมีมาตรการป้องกันตัวตนของผู้ใช้งาน เช่น การใช้รหัสผ่านที่มีความปลอดภัยซึ่งประกอบด้วย ● ข้อกำหนดความซับซ้อนและความยาวของรหัสผ่าน ● การกำหนดอายุการใช้งานรหัสผ่าน

No	Questionnaire	คำอธิบาย
		• การกำหนดจำนวนครั้งของการเข้าระบบโดยใช้รหัสผ่านที่ไม่ถูกต้องก่อนการระงับบัญชีผู้ใช้งาน • การป้องกันการใช้งานรหัสผ่านซ้ำ เป็นต้น
165.	All default passwords and unnecessary default accounts are changed before system implementation.	บริษัทมีการตรวจสอบและยกเลิกการใช้งานบัญชีผู้ใช้งานและรหัสผ่านที่ติดตั้งมาพร้อมกับระบบงาน (Default user) และ/หรือ บัญชีผู้ใช้งานของบริษัทผู้ให้บริการ (Vendor account) กรณีมีความจำเป็นในการใช้งาน บริษัทควรดำเนินมาตรการที่จำเป็น เช่น การเปลี่ยนรหัสผ่านไปจากรหัสผ่านตั้งต้น
166.	Physical security controls are used to prevent unauthorized access to information systems and telecommunication systems.	บริษัทมีการดำเนินมาตรการป้องกันความปลอดภัยทางกายภาพสำหรับระบบสารสนเทศ และเครือข่ายสื่อสาร ได้แก่ การควบคุมการเข้าถึงศูนย์คอมพิวเตอร์ และศูนย์เครือข่ายสื่อสาร ทั้งนี้อุปกรณ์เครือข่ายที่มีการติดตั้งในพื้นที่สำนักงานควรได้รับการจัดเก็บในตู้อุปกรณ์ที่มีการล็อคกุญแจ และติดตั้งในพื้นที่ที่มีการรักษาความปลอดภัย
167.	All passwords are encrypted in storage and in transit.	รหัสผ่านต้องได้รับการเข้ารหัสทั้งในพื้นที่จัดเก็บข้อมูล เช่น ฐานข้อมูลผู้ใช้งาน และการเข้ารหัสระหว่างการรับส่งผ่านเครือข่าย เช่น ขั้นตอนการยืนยันและพิสูจน์ตัวตนโดยเทคโนโลยีการเข้ารหัสมีความปลอดภัยและได้รับการยอมรับในอุตสาหกรรม บริษัทควรระงับการใช้งานบริการทางเครือข่ายที่มีความเสี่ยงต่อการรั่วไหลจากการจัดส่งข้อมูลรหัสผ่านโดยไม่มีการเข้ารหัส เช่น การใช้งาน telnet ftp หรือการใช้งานบริการประเภท http ในขั้นตอนการยืนยันและพิสูจน์ตัวตน
168.	Confidential data are encrypted when transmitted across public or untrusted networks (e.g., Internet).	ข้อมูลรหัสผ่านหรือข้อมูลเพื่อการยืนยันและพิสูจน์ตัวตนต้องได้รับการเข้ารหัส เมื่อมีการจัดส่งผ่านเครือข่ายสาธารณะหรือเครือข่ายที่ไม่มีความน่าเชื่อถือ เช่น เครือข่ายอินเทอร์เน็ต
169.	Mobile devices (e.g., laptops, tablets, and removable media) are encrypted if used to store confidential data. (*N/A if mobile devices are not used.)	บริษัทต้องจัดให้มีมาตรการเข้ารหัสสำหรับพื้นที่ในการจัดเก็บข้อมูลที่มีข้อมูลชั้นความลับสำหรับอุปกรณ์เคลื่อนที่ เช่น พื้นที่จัดเก็บข้อมูลของอุปกรณ์คอมพิวเตอร์แบบพกพา อุปกรณ์ tablet โทรศัพท์เคลื่อนที่ หรืออุปกรณ์จัดเก็บข้อมูลอื่นใด

No	Questionnaire	คำอธิบาย
170.	Administrative, physical, or technical controls are in place to prevent users without administrative responsibilities from installing unauthorized software.	บริษัทต้องมีการควบคุมและป้องกันการติดตั้งซอฟต์แวร์ที่ไม่ได้รับอนุญาตให้ใช้งาน เช่น การระงับและยกเลิกสิทธิการติดตั้งซอฟต์แวร์ การป้องกันทางกายภาพเช่น การระงับการใช้งานอุปกรณ์จัดเก็บข้อมูลเคลื่อนที่ เป็นต้น
171.	Customer service (e.g., the call center) utilizes formal procedures to authenticate customers commensurate with the risk of the transaction or request.	บริษัทมีการจัดให้มีกระบวนการในการพิสูจน์ตัวตนสำหรับลูกค้าเมื่อมีการติดต่อขอใช้บริการหรือการทำรายงานผ่านช่องทางต่างๆของบริษัท เช่น ศูนย์ลูกค้าสัมพันธ์ (Call center) โดยการตรวจสอบตัวตนของลูกค้าเป็นไปตามระดับความเสี่ยงของบริการที่มีการร้องข้อ การให้หรือเปิดเผยข้อมูล หรือการทำรายการ เป็นต้น
172.	Data is disposed of or destroyed according to documented requirements and within expected time frames.	บริษัทมีกระบวนการทำลายข้อมูล เมื่อสิ้นสุดระยะเวลาการจัดเก็บข้อมูลที่กำหนด (Data retention period) หรือเมื่อมีการยกเลิกการใช้งานอุปกรณ์สารสนเทศ ทั้งในส่วนข้อมูลที่มีการจัดเก็บอยู่ในอุปกรณ์สารสนเทศ สื่อบันทึกข้อมูล อุปกรณ์ฮาร์ดดิสก์ อุปกรณ์เครื่องถ่ายเอกสารที่มีสื่อบันทึกข้อมูล เป็นต้น
Level - 2		
173.	Use of customer data in non-production environments complies with legal, regulatory, and internal policy requirements for concealing or removing of sensitive data elements.	บริษัทมีการควบคุมการจัดเก็บข้อมูลในสภาพแวดล้อมที่ไม่ใช่ระบบงานหลัก (Non-production) ให้เป็นไปตามกฎหมาย ข้อบังคับ หรือ นโยบายภายในบริษัท เช่น มาตรการปิดบังข้อมูล (Data masking) มาตรการเปลี่ยนแปลงข้อมูลให้ไม่สามารถระบุตัวตนได้ (De- identifying) หรือการลบข้อมูลความลับ เป็นต้น
174.	Physical access to high-risk or confidential systems is restricted, logged, and unauthorized access is blocked.	ระบบงานที่จัดเก็บข้อมูลชั้นความลับ เช่น ระบบจัดพิมพ์เอกสารสำคัญหรือรหัสผ่านของลูกค้า ควรได้รับการติดตั้งอยู่ในบริเวณที่มีการควบคุมการเข้าถึงทางกายภาพ การบันทึกการเข้าถึง และ การตรวจสอบและป้องกันการเข้าถึงจากผู้ที่ไม่ได้รับอนุญาต
175.	Controls are in place to prevent unauthorized access to cryptographic keys.	กุญแจการเข้ารหัสและถอดรหัส ควรได้รับการจัดเก็บในพื้นที่ที่มีการควบคุมการเข้าถึง เช่น อุปกรณ์จัดเก็บข้อมูลที่มีการเข้ารหัส ซอฟต์แวร์บริหารจัดการกุญแจการเข้ารหัส อุปกรณ์จัดเก็บข้อมูลในตู้นิรภัย เป็นต้น

No	Questionnaire	คำอธิบาย
Level - 3		
176.	The institution has implemented tools to prevent unauthorized access to or exfiltration of confidential data.	บริษัทมีการติดตั้งใช้งานเครื่องมือเพื่อป้องกันการเข้าถึงหรือ ป้องกันการรั่วไหลของข้อมูลชั้นความลับ เช่น การกำหนดและจำกัดสิทธิการเข้าถึงข้อมูลชั้นความลับ การติดตั้งระบบตรวจจับพฤติกรรมผู้บุกรุก หรือ ระบบป้องกันการรั่วไหลของข้อมูล (Data loss prevention : DLP) เป็นต้น
177.	Controls are in place to prevent unauthorized escalation of user privileges.	บริษัทมีกระบวนการควบคุมเพื่อป้องกันการเข้าใช้งานและยกระดับสิทธิการใช้งานโดยผู้ที่ไม่ได้รับอนุญาต เช่น การระงับและยกเลิกบัญชีผู้ใช้งานและสิทธิการใช้งานระดับสูง การใช้เครื่องมือควบคุมบัญชีผู้ใช้งานที่มีสิทธิระดับสูง (Privilege access management: PAM) ระบบติดตามแจ้งเตือนเมื่อมีการใช้งานสิทธิระดับสูง เป็นต้น
178.	All physical and logical access is removed immediately upon notification of involuntary termination and within 24 hours of an employee’s voluntary departure.	บริษัทมีการควบคุมเพื่อให้มั่นใจว่าสิทธิการเข้าถึงพื้นที่ปฏิบัติงาน และระบบงาน ได้รับการระงับหรือยกเลิกอย่างทันทีเมื่อพนักงานพ้นสภาพความเป็นพนักงานโดยไม่สมัครใจ หรือ ภายใน 24 ชั่วโมงในกรณีพ้นสภาพจากการลาออกโดยสมัครใจ
179.	Confidential data are encrypted in transit across private connections (e.g., frame relay and T1) and within the institution’s trusted zones.	การรับส่งข้อมูลการยืนยันและพิสูจน์ตัวตนได้รับการเข้ารหัสเมื่อมีการรับส่งผ่านเครือข่ายไม่ว่าจะเป็นเครือข่ายการต่อเชื่อมแบบจุดต่อจุด หรือเครือข่ายภายในบริษัท
Level - 4		
180.	Encryption of select data at rest is determined by the institution’s data classification and risk assessment.	บริษัทมีกระบวนการจัดระดับชั้นความลับข้อมูล พร้อมทั้งดำเนินการประเมินความเสี่ยงของข้อมูลเพื่อการกำหนดมาตรการควบคุมที่เหมาะสมในแต่ละระดับชั้นความลับ ข้อมูลชั้นความลับควรได้รับการเข้ารหัสเมื่อมีการจัดเก็บอยู่ในพื้นที่จัดเก็บข้อมูล (Data at rest)
181.	Customer authentication for high-risk transactions includes methods to prevent malware and man-in-the-middle attacks (e.g., using visual transaction signing).	บริษัทมีกระบวนการควบคุมด้วยการยืนยันและพิสูจน์ตัวตนอีกครั้งเมื่อมีการทำรายการธุรกรรมที่สำคัญผ่านระบบอิเล็กทรอนิกส์ เพื่อป้องกันความเสี่ยงจากการโจมตีด้วยวิธีการ man-in-the-middle

No	Questionnaire	คำอธิบาย
Level - 5		
182.	Tokenization is used to substitute unique values for confidential information (e.g., virtual credit card).	บริษัทควรดำเนินมาตรการป้องกันความเสี่ยงจากการรั่วไหลของข้อมูลในขั้นตอนการจัดเก็บและรับส่งข้อมูลสำคัญ เช่น การใช้กรรมวิธี Tokenization
183.	Real-time risk mitigation is taken based on automated risk scoring of user credentials.	บริษัทมีระบบหรือมาตรการวิเคราะห์พฤติกรรมผู้ใช้งาน (Behavioural based security) เพื่อวิเคราะห์ระดับความเสี่ยง และการยกเลิกการเชื่อมต่อโดยอัตโนมัติ หรือมาตรการอื่นใดเพื่อป้องกันความเสี่ยง
Preventative Controls - Device / End-Point Security		
Level - 1		
184.	Controls are in place to restrict the use of removable media to authorized personnel.	บริษัทมีการป้องกันการใช้งานอุปกรณ์จัดเก็บข้อมูลเคลื่อนที่โดยไม่ได้รับอนุญาต เช่น การระงับการใช้งาน USB หรือ สื่อบันทึกข้อมูล เช่น CD/DVD
185.	Antivirus and anti-malware tools are deployed on end-point devices (e.g., workstations, laptops, and mobile devices).	อุปกรณ์เครื่องคอมพิวเตอร์ และอุปกรณ์ประมวลผลเคลื่อนที่ ได้รับการติดตั้งโปรแกรมป้องกันไวรัส และโปรแกรมป้องกันมัลแวร์ครบถ้วน เพื่อป้องกันความเสี่ยงจากการบุกรุกโจมตีระบบ
Level - 2		
186.	Tools automatically block attempted access from unpatched employee and third-party devices.	บริษัทมีมาตรการป้องกันการเชื่อมต่อเข้าสู่ระบบเครือข่ายของบริษัทโดยอัตโนมัติ จากการใช้อุปกรณ์ของพนักงาน หรือผู้ให้บริการภายนอกที่ไม่ได้รับการติดตั้งชุดโปรแกรมแก้ไขข้อบกพร่องด้านความมั่นคงปลอดภัยสารสนเทศ (Security patch) ตามมาตรฐานบริษัท เช่น การตรวจสอบ Patch level ของอุปกรณ์ก่อนอนุญาตให้เชื่อมต่อเครือข่าย เป็นต้น
187.	Tools automatically block attempted access by unregistered devices to internal networks.	บริษัทมีมาตรการป้องกันการเชื่อมต่อเครือข่ายภายในของบริษัทแบบอัตโนมัติ ในการใช้อุปกรณ์ที่ไม่มีการลงทะเบียนไว้ เช่น การตรวจสอบ MAC address เป็นต้น
188.	Controls are in place to prevent unauthorized individuals from copying confidential data to removable media.	บริษัทมีมาตรการตรวจสอบและป้องกันการทำสำเนาข้อมูล ที่มีข้อมูลชั้นความลับไปยังอุปกรณ์จัดเก็บข้อมูลเคลื่อนที่ เช่น การระงับการใช้งาน USB การระงับการใช้งานสื่อบันทึกข้อมูล CD/DVD หรือ ระบบป้องกันการรั่วไหลของข้อมูล (Data loss prevention : DLP) เป็นต้น
189.	The institution wipes data remotely on mobile devices when a device is missing or stolen. (*N/A if mobile devices are not used.)	บริษัทมีมาตรการในการลบข้อมูลที่จัดเก็บอยู่บนอุปกรณ์เคลื่อนที่ เมื่อได้รับการรายงานด้านอุปกรณ์ศูนย์หาย เช่น การใช้งานระบบ Mobile Device Management (MDM)

No	Questionnaire	คำอธิบาย
Level - 3		
190.	Data loss prevention controls or devices are implemented for inbound and outbound communications (e.g., e-mail, FTP, Telnet, prevention of large file transfers).	บริษัทมีการควบคุมหรือมีการติดตั้งระบบป้องกันการรั่วไหลของข้อมูล (Data loss prevention : DLP) เพื่อตรวจสอบข้อมูลที่มีการรับส่งผ่านช่องทางการสื่อสารต่างๆ เช่น การรับส่งอีเมล การรับส่งไฟล์ผ่านเครือข่าย (FTP) การรับส่งข้อมูลไปยังพื้นที่จัดเก็บข้อมูลบนระบบอินเทอร์เน็ต (Internet storage) เป็นต้น
191.	Mobile device management includes integrity scanning (e.g., jailbreak/rooted detection). (*N/A if mobile devices are not used.)	บริษัทมีมาตรการตรวจสอบและการอนุญาตให้ใช้งานอุปกรณ์เคลื่อนที่เพื่อต่อเชื่อมและเข้าถึงทรัพยากรเครือข่ายภายในบริษัท โดยมีการตรวจสอบและป้องกันการใช้งานอุปกรณ์ที่มีการ jailbreak หรือ rooted
192.	Mobile devices connecting to the corporate network for storing and accessing company information allow for remote software version/patch validation. (*N/A if mobile devices are not used.)	บริษัทมีมาตรการตรวจสอบและการอนุญาตให้ใช้งานอุปกรณ์เคลื่อนที่เพื่อต่อเชื่อมและเข้าถึงทรัพยากรเครือข่ายภายในบริษัท โดยมีการจำกัดซอฟต์แวร์และตรวจสอบเวอร์ชันของซอฟต์แวร์ที่ได้รับอนุญาตเท่านั้น
Level - 4		
193.	Employees' and third parties' devices (including mobile) without the latest security patches are quarantined and patched before the device is granted access to the network.	บริษัทมีมาตรการในการติดตั้งชุดโปรแกรมแก้ไขข้อบกพร่องด้านความมั่นคงปลอดภัยสารสนเทศ (Security patch) ให้เป็นไปตามมาตรฐานบริษัท สำหรับอุปกรณ์เคลื่อนที่ของพนักงาน หรือผู้ให้บริการภายนอกก่อนอนุญาตให้เชื่อมต่อเข้าสู่เครือข่ายภายในบริษัท
194.	Confidential data and applications on mobile devices are only accessible via a secure, isolated sandbox or a secure container.	การจัดเก็บข้อมูล ข้อมูลความลับ หรือ ข้อมูลระบบงาน (Application data) บนอุปกรณ์เคลื่อนที่ได้รับการจัดเก็บในพื้นที่จัดเก็บข้อมูลเฉพาะที่ได้รับการรักษาความปลอดภัย และป้องกันการเข้าถึงจากอุปกรณ์โทรศัพท์เคลื่อนที่โดยตรง
Level - 5		
195.	A centralized end-point management tool provides fully integrated patch, configuration, and vulnerability management, while also being able to detect malware upon arrival to prevent an exploit.	บริษัทมีการจัดหาเครื่องมือในการบริหารจัดการอุปกรณ์เคลื่อนที่ ที่มีความสามารถในการบริหารจัดการชุดโปรแกรมแก้ไขข้อบกพร่องด้านความมั่นคงปลอดภัยสารสนเทศ (Security patch) การบริหารและติดตั้งค่าคอนฟิคกูเรชั่นของอุปกรณ์ การบริหารจัดการช่องโหว่ด้านความปลอดภัย รวมถึงการบริหารจัดการด้านการป้องกันไวรัสและโปรแกรมไม่พึงประสงค์

No	Questionnaire	คำอธิบาย
Preventative Controls - Secure Coding		
Level - 1		
196.	Developers working for the institution follow secure program coding practices, as part of a system development life cycle (SDLC), that meet industry standards.	บริษัทมีการจัดทำแนวทางและคู่มือการพัฒนาโปรแกรมอย่างปลอดภัย (Secure code) ที่สอดคล้องกับมาตรฐานอุตสาหกรรม เช่น OWASP Secure Coding Practices และใช้ในขั้นตอนการพัฒนาระบบงาน
197.	The security controls of internally developed software are periodically reviewed and tested. (*N/A if there is no software development.)	บริษัทมีขั้นตอนการตรวจสอบด้านการควบคุมความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศอย่างสม่ำเสมอ สำหรับระบบงานที่มีการพัฒนาเป็นการภายใน
198.	The security controls in internally developed software code are independently reviewed before migrating the code to production. (*N/A if there is no software development.)	บริษัทมีขั้นตอนในการตรวจสอบภายในด้านการควบคุมความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศก่อนการนำเข้าสู่ระบบงานจริงเพื่อการใช้งาน
Level - 2		
199.	Security testing occurs at all post-design phases of the SDLC for all applications, including mobile applications. (*N/A if there is no software development.)	บริษัทมีการตรวจสอบด้านความปลอดภัยของโปรแกรมหรือระบบงานที่มีการพัฒนาอย่างครบถ้วน รวมถึงโปรแกรมบนอุปกรณ์โทรศัพท์เคลื่อนที่
Level - 3		
200.	The security of applications, including Web-based applications connected to the Internet, is tested against known types of cyber attacks (e.g., SQL injection, cross-site scripting, buffer overflow) before implementation or following significant changes.	บริษัทมีการทดสอบช่องโหว่ด้านความปลอดภัยสำหรับโปรแกรมระบบงานที่มีการให้บริการในลักษณะเว็บเซอร์วิส และสามารถเข้าถึงได้ผ่านเครือข่ายอินเทอร์เน็ต โดยการทดสอบมีการดำเนินการก่อนนำระบบงานเข้าสู่ระบบงานจริงเพื่อการใช้งาน หรือ เมื่อมีการเปลี่ยนแปลงที่สำคัญ ทั้งนี้ขอบเขตการทดสอบด้านความปลอดภัยครอบคลุมช่องโหว่ด้านความปลอดภัยที่เป็นที่รู้จัก เช่น SQL injection, cross-site scripting, buffer overflow หรือ เป็นไปตามมาตรฐานที่ได้รับการยอมรับ เช่น OWASP Top Ten เป็นต้น
201.	Software code executables and scripts are digitally signed to confirm the software author and guarantee that the code has not been altered or corrupted.	ไฟล์โปรแกรมต้นฉบับ (Executable file) ของระบบงาน รวมถึงซอฟต์แวร์สคริป ได้รับการลงนามด้วยลายเซ็นแบบอิเล็กทรอนิกส์ (Digitally signed) และมีการจัดเก็บค่า Hash value เพื่อการตรวจสอบและป้องกันการแก้ไขเปลี่ยนแปลงโดยไม่ได้รับอนุญาต

No	Questionnaire	คำอธิบาย
Level - 4		
202.	Vulnerabilities identified through a static code analysis are remediated before implementing newly developed or changed applications into production.	บริษัทมีการตรวจสอบวิเคราะห์สำเนาโปรแกรมด้วยวิธีการและเครื่องมือแบบ static code analysis เป็นอย่างน้อย สำหรับโปรแกรมระบบงานที่มีการพัฒนาใหม่ หรือ ในขั้นตอนการแก้ไขเปลี่ยนแปลงโปรแกรม ช่องโหว่ที่ได้รับการตรวจสอบจากการตรวจสอบสำเนาโปรแกรมต้นฉบับ ได้รับการแก้ไขก่อนการนำเข้าสู่ระบบงานจริงเพื่อการใช้งาน (Production)
203.	All interdependencies between applications and services have been identified.	บริษัทมีการจัดทำรายละเอียดความเชื่อมโยงของระบบงานและบริการ
204.	Independent code reviews are completed on internally developed or vendor-provided custom applications to ensure there are no security gaps.	บริษัทมีการตรวจสอบสำเนาโปรแกรมต้นฉบับ (Code review) โดยผู้ตรวจสอบที่เป็นอิสระสำหรับโปรแกรมระบบงานที่มีการพัฒนาเป็นการภายใน หรือ โปรแกรมระบบงานที่มีการปรับปรุง (customization) เพื่อให้มั่นใจถึงความปลอดภัยของระบบงานจากช่องโหว่ด้านความปลอดภัยเทคโนโลยีสารสนเทศ
Level - 5		
205.	Software code is actively scanned by automated tools in the development environment so that security weaknesses can be resolved immediately during the design phase.	บริษัทมีการตรวจสอบสำเนาโปรแกรมต้นฉบับ (Code review) ด้วยเครื่องมืออัตโนมัติอย่างสม่ำเสมอในขั้นตอนการพัฒนาโปรแกรม เพื่อให้มั่นใจว่าช่องโหว่ด้านความปลอดภัยได้รับการแก้ไขอย่างทันทีในขั้นตอนการพัฒนาระบบ
Detective Controls - Threat and Vulnerability Detection		
Level - 1		
206.	Independent testing (including penetration testing and vulnerability scanning) is conducted according to the risk assessment for external- facing systems and the internal network.	บริษัทมีการดำเนินการทดสอบด้านความปลอดภัย ประกอบด้วยการทดสอบเจาะระบบ (Penetration test) และการทดสอบช่องโหว่ระบบ (Vulnerability scan) สำหรับระบบสำคัญที่มีการเชื่อมต่อและสามารถเข้าถึงได้ผ่านเครือข่ายอินเทอร์เน็ต ระบบเครือข่ายภายใน และระบบงานสำคัญของบริษัท
207.	Firewall rules are audited or verified at least quarterly.	บริษัทมีการตรวจสอบความถูกต้องเหมาะสมของกฎของไฟร์วอลล์อย่างสม่ำเสมอ อย่างน้อยไตรมาสละ 1 ครั้ง เพื่อให้มั่นใจถึงการควบคุมการเข้าถึงบริการทางเครือข่ายเป็นไปตามวัตถุประสงค์ทางธุรกิจและบริการทางเครือข่ายที่อนุญาตให้ใช้งานมีความปลอดภัย

No	Questionnaire	คำอธิบาย
208.	E-mail protection mechanisms are used to filter for common cyber threats (e.g., attached malware or malicious links).	บริษัทมีการดำเนินมาตรการป้องกันความปลอดภัยระบบอีเมล โดยการตรวจสอบและคัดกรองเนื้อหาที่ไม่เหมาะสม และภัยคุกคามด้านความปลอดภัยทางไซเบอร์ เช่น โปรแกรมไวรัส และโปรแกรมไม่พึงประสงค์
Level - 2		
209.	Independent penetration testing of network boundary and critical Web- facing applications is performed routinely to identify security control gaps.	บริษัทมีการดำเนินการทดสอบด้านความปลอดภัย ประกอบด้วยการทดสอบเจาะระบบ (Penetration test) และการทดสอบช่องโหว่ระบบ (Vulnerability scan) สำหรับระบบสำคัญที่มีการเชื่อมต่อและสามารถเข้าถึงได้ผ่านเครือข่ายอินเทอร์เน็ต ระบบเครือข่ายภายใน และระบบงานสำคัญของบริษัทอย่างสม่ำเสมอ โดยมีรอบการทดสอบตามผลการประเมินความเสี่ยงของระบบงาน
210.	Independent penetration testing is performed on Internet-facing applications or systems before they are launched or undergo significant change.	ระบบงานสำคัญที่สามารถเข้าถึงได้ผ่านเครือข่ายอินเทอร์เน็ตจะต้องได้รับการทดสอบเจาะระบบ ก่อนขั้นตอนการนำระบบเข้าสู่ระบบงานจริงเพื่อการใช้งาน (Production) และ มีการทดสอบเจาะระบบทุกครั้งเมื่อมีการเปลี่ยนแปลงที่สำคัญ
211.	Vulnerability scanning is conducted and analyzed before deployment/redeployment of new/existing devices.	อุปกรณ์ด้านเทคโนโลยีสารสนเทศ เช่น อุปกรณ์เครือข่าย เครื่องแม่ข่าย เป็นต้น ได้รับการทดสอบช่องโหว่ระบบ (Vulnerability scan) ก่อนการนำระบบเข้าสู่ระบบงานจริงเพื่อการใช้งาน (Production)
Level - 3		
212.	Audit or risk management resources review the penetration testing scope and results to help determine the need for rotating companies based on the quality of the work.	บริษัทมีการประเมินขอบเขตและผลการดำเนินการทดสอบเจาะระบบ เพื่อประเมินคุณภาพของการทดสอบเจาะระบบ และประเมินความจำเป็นในการหมุนเวียนหรือสับเปลี่ยนบริษัทผู้ดำเนินการทดสอบ
213.	E-mails and attachments are automatically scanned to detect malware and are blocked when malware is present.	อีเมลที่มีการรับส่งไฟล์แนบได้รับการตรวจสอบโดยอัตโนมัติเพื่อป้องกันโปรแกรมไวรัส หรือโปรแกรมไม่พึงประสงค์
Level - 4		
214.	Automated tool(s) proactively identifies high-risk behaviour signalling an employee who may pose an insider threat.	บริษัทมีระบบหรือมาตรการวิเคราะห์พฤติกรรมผู้ใช้งาน (Behavioural based security) โดยอัตโนมัติ เพื่อวิเคราะห์ความเสี่ยง และพฤติกรรมอันเป็นภัยคุกคามด้านความปลอดภัยทางไซเบอร์

No	Questionnaire	คำอธิบาย
Level - 5		
215.	User tasks and content (e.g., opening an e-mail attachment) are automatically isolated in a secure container or virtual environment so that malware can be analyzed but cannot access vital data, end-point operating systems, or applications on the institution's network.	บริษัทมีการวิเคราะห์พฤติกรรมการใช้งาน และเอกสารไฟล์แนบจากอีเมลผู้ใช้งาน ในสภาพแวดล้อมเสมือน เช่น การใช้งานเครื่องมือ ประเภท Sandbox เพื่อตรวจสอบพฤติกรรมเสี่ยง และป้องกันความเสียหายจากการเข้าถึงข้อมูลและระบบงานสำคัญของบริษัท
216.	Weekly vulnerability scanning is rotated among environments to scan all environments throughout the year.	บริษัทมีการการทดสอบช่องโหว่ระบบ (Vulnerability scan) อย่างสม่ำเสมอ เช่นมีการทดสอบหมุนเวียนประจำสัปดาห์ เพื่อให้ระบบเครือข่ายและอุปกรณ์ด้านเทคโนโลยีสารสนเทศของบริษัทได้รับการทดสอบอย่างครบถ้วน
Detective Controls - Anomalous Activity Detection		
Level - 1		
217.	The institution is able to detect anomalous activities through monitoring across the environment.	บริษัทมีการตรวจสอบพฤติกรรมต้องสงสัยในการใช้งานระบบสารสนเทศ ผ่านระบบติดตามตรวจสอบพฤติกรรมหรือการตรวจสอบบันทึกเหตุการณ์ ครอบคลุมเครือข่ายและอุปกรณ์สารสนเทศสำคัญของบริษัท
218.	Logs of physical and/or logical access are reviewed following events.	บริษัทมีการตรวจสอบบันทึกเหตุการณ์การเข้าถึงทั้งทางกายภาพและการเข้าถึงระบบงาน/ทรัพยากรสำคัญของบริษัท
219.	Access to critical systems by third parties is monitored for unauthorized or unusual activity.	บริษัทมีการตรวจสอบการเข้าถึงระบบงานสำคัญโดยบริษัทผู้ให้บริการภายนอกอย่างสม่ำเสมอ เพื่อสอบทานการเข้าถึงโดยไม่ได้รับอนุญาต หรือ พฤติกรรมที่ไม่เหมาะสม ทั้งการเข้าถึงบนระบบงาน การเข้าถึงผ่านช่องการการสื่อสารระยะไกลที่มีการอนุญาตไว้ เป็นต้น
220.	Elevated privileges are monitored.	บริษัทมีการตรวจสอบการใช้งานบัญชีผู้ใช้งานที่มีสิทธิระดับสูง ทั้งจากการใช้งานบัญชีผู้ใช้งานที่มีสิทธิสูงโดยตรง หรือ กิจกรรมการยกระดับสิทธิการใช้งาน เช่น Switch user
Level - 2		
221.	Systems are in place to detect anomalous behavior automatically during customer, employee, and third-party authentication.	บริษัทมีระบบตรวจสอบพฤติกรรมต้องสงสัยของลูกค้า พนักงาน หรือ บริษัทผู้ให้บริการภายนอก ในขั้นตอนการพิสูจน์และยืนยันตัวตน เช่น พฤติกรรมการใช้รหัสผ่านที่ไม่ถูกต้องในรูปแบบที่ซ้ำกัน พฤติกรรมการเดาสุ่มรหัสผ่าน การเข้าสู่ระบบงานจากเครื่องคอมพิวเตอร์ต้นทางพร้อมกันหลายเครื่อง เป็นต้น

No	Questionnaire	คำอธิบาย
222.	Security logs are reviewed regularly.	บริษัทมีกระบวนการสอบทานบันทึกเหตุการณ์อย่างสม่ำเสมอ โดยรอบระยะเวลาการสอบทานต้องมีระยะเวลาที่สามารถให้บริษัทดำเนินมาตรการแก้ไขเหตุการณ์ได้อย่างทันเวลา
223.	Logs provide traceability for all system access by individual users.	บริษัทมีการจัดเก็บบันทึกเหตุการณ์สำหรับระบบงานอย่างครบถ้วน และมีข้อมูลที่เพียงพอ เพื่อให้บริษัทสามารถตรวจสอบย้อนกลับไปจนถึงตัวบุคคลผู้ใช้งาน
224.	Thresholds have been established to determine activity within logs that would warrant management response.	บริษัทมีการกำหนดเกณฑ์การตรวจสอบบันทึกเหตุการณ์อย่างชัดเจน เพื่อใช้ในการระบุความผิดปกติและเพื่อเป็นเงื่อนไขในการยกระดับเหตุการณ์และการแจ้งเตือนไปยังผู้รับผิดชอบอย่างทันเวลา เช่น เกณฑ์ด้านจำนวนและความถี่ของเหตุการณ์ผิดปกติที่เกิดขึ้นภายในระยะเวลาที่กำหนด
Level - 3		
225.	Tools actively monitor security logs for anomalous behaviour and alert within established parameters.	บริษัทมีการจัดหาเครื่องมือในการติดตามตรวจสอบบันทึกเหตุการณ์ หรือพฤติกรรมต้องสงสัย เพื่อแจ้งเตือนไปยังผู้ที่เกี่ยวข้องตามเงื่อนไขที่กำหนด โดยระบบมีความสามารถในการปรับเปลี่ยนเงื่อนไขการตรวจสอบวิเคราะห์เหตุการณ์ และเงื่อนไขการแจ้งเตือนได้ตามความเหมาะสม
226.	Audit logs are backed up to a centralized log server or media that is difficult to alter.	บันทึกเหตุการณ์เพื่อการตรวจสอบได้รับการจัดเก็บบนระบบจัดเก็บบันทึกเหตุการณ์กลาง หรือ สื่อบันทึกข้อมูลสำรอง ที่มีการควบคุมและป้องกันการแก้ไขเปลี่ยนแปลงโดยไม่ได้รับอนุญาต
Level - 4		
227.	An automated tool triggers system and/or fraud alerts when customer logins occur within a short period of time but from physically distant IP locations.	บริษัทมีระบบอัตโนมัติในการตรวจสอบและแจ้งเตือนพฤติกรรมต้องสงสัยของลูกค้าอันอาจเป็นการทุจริต ในขั้นตอนการพิสูจน์และยืนยันตัวตน เช่น การเข้าสู่ระบบงานจากเครื่องคอมพิวเตอร์ต้นทางพร้อมกันหลายเครื่องหรือเครื่องคอมพิวเตอร์ที่มีหมายเลขต้นทางที่มีความแตกต่างกันด้านสถานที่ทางภูมิศาสตร์ภายในระยะเวลาอันสั้น เป็นต้น
228.	A system is in place to monitor and analyze employee behaviour (network use patterns, work hours, and known devices) to alert on anomalous activities.	บริษัทมีระบบตรวจสอบและแจ้งเตือนพฤติกรรมต้องสงสัยของพนักงานในเครือข่ายของบริษัท เช่น พฤติกรรมการใช้งานเครือข่ายที่ผิดปกติ การถ่ายโอนข้อมูลเป็นจำนวนมาก การเข้าใช้งานในระบบงานในช่วงเวลา

No	Questionnaire	คำอธิบาย
		ผิดปกติ หรือ การเข้าใช้งานจากเครื่องคอมพิวเตอร์ที่ไม่เคยมีการใช้งาน เป็นต้น
229.	Tags on fictitious confidential data or files are used to provide advanced alerts of potential malicious activity when the data is accessed.	บริษัทมีการจัดทำข้อมูลหรือแฟ้มข้อมูลปลอม (Fictitious data) ที่มีการติดฉลากข้อมูล (Labelling) ในระดับข้อมูลชั้นความลับ เพื่อให้บริษัทมีข้อมูลความพยายามในการเข้าถึงข้อมูลปลอมดังกล่าวและได้รับการแจ้งเตือนล่วงหน้าเมื่อมีความพยายามในการเข้าถึงข้อมูลชั้นความลับ
Level - 5		
230.	The institution has a mechanism for real-time automated risk scoring of threats.	บริษัทมีระบบหรือมาตรการวิเคราะห์พฤติกรรมผู้ใช้งาน เครือข่าย หรืออุปกรณ์สารสนเทศ (Behavioural based security) เพื่อวิเคราะห์ระดับความเสี่ยงและภัยคุกคามอย่างทันที่และตลอดเวลา (Real-time)
Detective Controls - Event Detection		
Level - 1		
231.	A normal network activity baseline is established.	บริษัทมีการรวบรวมข้อมูล และพฤติกรรมการใช้งานเครือข่ายประจำภายในของบริษัท ทั้งนี้ข้อมูลพฤติกรรมดังกล่าวใช้เพื่อเป็นข้อมูลฐานอ้างอิง (baseline) เพื่อให้บริษัทมีความสามารถในการตรวจพบเหตุการณ์ผิดปกติเมื่อมีพฤติกรรมหรือความพยายามในการเข้าถึงเครือข่ายที่ผิดไปจากข้อมูลฐานอ้างอิงดังกล่าว
232.	Mechanisms (e.g., antivirus alerts, log event alerts) are in place to alert management to potential attacks.	บริษัทมีเครื่องมือในการแจ้งเตือนผู้รับผิดชอบด้านความมั่นคงปลอดภัยสารสนเทศ เมื่อมีเหตุการณ์ผิดปกติเกิดขึ้นบนระบบเครือข่าย หรือระบบสารสนเทศของบริษัท เช่น การแจ้งเตือนเมื่อมีการตรวจพบกิจกรรมของไวรัสคอมพิวเตอร์เป็นจำนวนมาก การแจ้งเตือนเมื่อมีการตรวจสอบบันทึกเหตุการณ์ที่มีระดับความสำคัญตามเกณฑ์ที่กำหนดไว้ เป็นต้น
233.	Processes are in place to monitor for the presence of unauthorized users, devices, connections, and software.	บริษัทมีกระบวนการในการตรวจสอบหรือแจ้งเตือนเมื่อมีความพยายามในการเข้าถึงเครือข่าย หรือ ระบบงาน โดยผู้ที่ไม่ได้รับอนุญาต รวมถึงความพยายามในการใช้อุปกรณ์ที่ไม่ได้รับอนุญาตและไม่ได้รับการลงทะเบียนไว้เพื่อการเชื่อมโยงเข้าสู่เครือข่ายและระบบงานภายในและการใช้งานซอฟต์แวร์ที่ไม่ได้รับอนุญาตอันอาจเป็นความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ เป็นต้น

No	Questionnaire	คำอธิบาย
234.	Responsibilities for monitoring and reporting suspicious systems activity have been assigned.	บริษัทมีการกำหนดและมอบหมายหน้าที่ความรับผิดชอบในการตรวจสอบ และ ติดตามพฤติกรรมของระบบที่ผิดปกติ และการรายงานไปยังผู้ที่รับผิดชอบอย่างเป็นลายลักษณ์อักษร และกำหนดชัดเจนในคำบรรยายลักษณะงาน (Job description)
Level - 2		
235.	A process is in place to correlate event information from multiple sources (e.g., network, application, or firewall).	บริษัทมีกระบวนการในการรวบรวมข้อมูลเหตุการณ์ จากแหล่งข้อมูลเช่น อุปกรณ์เครือข่าย ระบบงาน ระบบรักษาความปลอดภัยเครือข่าย เพื่อใช้ในกระบวนการเชื่อมโยงและวิเคราะห์เหตุการณ์ด้านความมั่นคงปลอดภัยเครือข่าย
Level - 3		
236.	Controls or tools (e.g., data loss prevention) are in place to detect potential unauthorized or unintentional transmissions of confidential data.	บริษัทมีการควบคุม หรือ เครื่องมืออัตโนมัติในการตรวจจับ ป้องกันหรือติดตามความพยายามในการเข้าถึงและรับส่งข้อมูลชั้นความลับไปยังผู้ที่ไม่ได้รับอนุญาต เช่น การใช้ระบบป้องกันการรั่วไหลของข้อมูล (Data loss prevention : DLP) เป็นต้น
237.	Event detection processes are proven reliable.	ข้อมูลเหตุการณ์ที่มีการจัดเก็บและประมวลผล ได้รับการควบคุมด้านความถูกต้องและน่าเชื่อถือ เช่น การป้องกันการเข้าถึงเพื่อแก้ไข เปลี่ยนแปลง หรือ ทำลายข้อมูล ข้อมูลที่ได้รับการเชื่อมโยงได้รับการเทียบเวลาให้เป็นมาตรฐานเวลาเดียวกัน เป็นต้น
Level - 4		
238.	Automated tools detect unauthorized changes to critical system files, firewalls, IPS, IDS, or other security devices.	บริษัทมีการจัดหาและติดตั้งเครื่องมืออัตโนโมติในการตรวจจับความพยายามในการเข้าถึงและแก้ไขเปลี่ยนแปลงแฟ้มข้อมูลสำคัญ เช่น การใช้งานซอฟต์แวร์ File integrity monitoring (FIM) รวมถึงความพยายามในการเข้าถึงและแก้ไขเปลี่ยนแปลงค่าคอนฟิคกูเรชันอุปกรณ์รักษาความปลอดภัย เช่น อุปกรณ์ไฟร์วอลล์ อุปกรณ์ตรวจจับและป้องกันผู้บุกรุก หรือ ระบบรักษาความปลอดภัยอื่นๆ
239.	Real-time alerts are automatically sent when unauthorized software, hardware, or changes occur.	บริษัทมีเครื่องมืออัตโนมัติในการแจ้งเตือนผู้รับผิดชอบอย่าง ทันที และตลอดเวลา (Real-time) เมื่อมีการติดตั้งใช้งานซอฟต์แวร์ ฮาร์ดแวร์ หรือความพยายามในการแก้ไขเปลี่ยนแปลงระบบโดยไม่ได้รับอนุญาต

No	Questionnaire	คำอธิบาย
240.	Tools are in place to actively correlate event information from multiple sources and send alerts based on established parameters.	บริษัทมีการจัดหาเครื่องมือในการติดตามตรวจสอบและเชื่อมโยงเหตุการณ์จากหลายแหล่งข้อมูล เพื่อติดตามพฤติกรรมต้องสงสัยและแจ้งเตือนไปยังผู้ที่เกี่ยวข้องตามเงื่อนไขที่กำหนด โดยระบบมีความสามารถในการปรับเปลี่ยนเงื่อนไขการตรวจสอบวิเคราะห์เหตุการณ์และเงื่อนไขการแจ้งเตือนได้ตามความเหมาะสม
Level - 5		
241.	The institution is leading efforts to develop event detection systems that will correlate in real time when events are about to occur.	บริษัทมีการพัฒนาเครื่องมือในการติดตามตรวจสอบเหตุการณ์ หรือพฤติกรรมอันผิดปกติอย่างทันทีและตลอดเวลา เพื่อการแจ้งเตือนผู้ที่เกี่ยวข้องเป็นการล่วงหน้าก่อนเหตุการณ์บุกรุกโจมตีระบบหรือความเสียหายจะเกิด
Corrective Controls - Patch Management		
Level - 1		
242.	A patch management program is implemented and ensures that software and firmware patches are applied in a timely manner.	บริษัทมีกระบวนการบริหารจัดการชุดโปรแกรมแก้ไขข้อบกพร่อง (Patch management) เพื่อติดตามชุดซอฟต์แวร์ที่ออกโดยบริษัทผู้ผลิต และดำเนินการติดตั้งภายในระยะเวลาที่กำหนด
243.	Patches are tested before being applied to systems and/or software.	บริษัทมีกระบวนการทดสอบชุดโปรแกรมแก้ไขข้อบกพร่อง เพื่อให้มั่นใจถึงความเข้ากันได้ของซอฟต์แวร์ที่เกี่ยวข้อง ก่อนการดำเนินการติดตั้งบนระบบงานหลัก เพื่อป้องกันความเสี่ยงจากการหยุดชะงักของระบบ
244.	Patch management reports are reviewed and reflect missing security patches.	บริษัทมีกระบวนการสอบทานรายงานผลการติดตั้งชุดโปรแกรมแก้ไขข้อบกพร่อง เพื่อให้มั่นใจถึงความครบถ้วนในการติดตั้งชุดโปรแกรมแก้ไขข้อบกพร่องที่ออกโดยบริษัทผู้ผลิตซอฟต์แวร์ ทั้งนี้รายงานควรประกอบด้วยรายการเครื่องแม่ข่ายหรืออุปกรณ์ที่ได้รับผลกระทบทั้งหมด ผลการดำเนินการติดตั้งชุดโปรแกรมแก้ไขข้อพกพร่อง และ รายการเครื่องแม่ข่ายหรืออุปกรณ์ที่ไม่สามารถติดตั้งชุดโปรแกรมแก้ไขข้อบกพร่องดังกล่าว สาเหตุ และแนวทางการแก้ไขปัญหาหรือการป้องกันความเสี่ยงชั่วคราว พร้อมทั้งมีกระบวนการในการติดตามเครื่องแม่ข่ายหรืออุปกรณ์เครือข่ายคงค้างให้ได้รับการติดตั้งชุดโปรแกรมดังกล่าวอย่างครบถ้วน

No	Questionnaire	คำอธิบาย
Level - 2		
245.	A formal process is in place to acquire, test, and deploy software patches based on criticality.	บริษัทมีกระบวนการบริหารจัดการชุดโปรแกรมแก้ไขข้อบกพร่อง (Patch management) ประกอบด้วย ขั้นตอนการติดตามชุดซอฟต์แวร์ที่ออกโดยบริษัทผู้ผลิต ขั้นตอนการทดสอบด้านความเข้ากันได้ของชุดโปรแกรม และขั้นตอนการดำเนินการติดตั้งภายในระยะเวลาที่กำหนด โดยพิจารณาถึงความเสี่ยงและผลกระทบของชุดโปรแกรม
246.	An automated tool(s) is used to identify missing security patches as well as the number of days since each patch became available.	บริษัทมีการใช้เครื่องมืออัตโนมัติ เพื่อติดตามชุดโปรแกรมแก้ไขข้อบกพร่องที่มีการติดตั้งบนเครื่องแม่ข่าย ซอฟต์แวร์ และอุปกรณ์เครือข่าย เพื่อระบุถึงชุดโปรแกรม ฯ ที่ยังคงค้างและไม่ได้รับการติดตั้ง และรายงานระยะเวลาเป็นจำนวนวันตั้งแต่บริษัทผู้บริษัทผู้ผลิตออกชุดโปรแกรมแก้ไขข้อบกพร่องจนถึงปัจจุบัน
247.	Missing patches across all environments are prioritized and tracked.	บริษัทมีขั้นตอนการติดตามให้มีการดำเนินการติดตั้งชุดโปรแกรมแก้ไขข้อบกพร่องที่ยังคงค้างอย่างครบถ้วน โดยรายงานประกอบด้วยเครื่องแม่ข่ายและรายละเอียดชุดโปรแกรมแก้ไขข้อบกพร่องที่คงค้าง ระดับความสำคัญของชุดโปรแกรมฯ แผนการดำเนินการ และผู้รับผิดชอบ
Level - 3		
248.	Patches for high-risk vulnerabilities are tested and applied when released or the risk is accepted and accountability assigned.	บริษัทมีการจัดทำเกณฑ์ในการประเมินความเสี่ยงและผลกระทบของชุดโปรแกรมแก้ไขข้อบกพร่องที่มีความสำคัญระดับสูงขึ้นไปและอาจก่อให้เกิดความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ ทั้งนี้เพื่อการวางแผนการติดตั้ง การทดสอบ และการตัดสินใจในการดำเนินการติดตั้งชุดโปรแกรมดังกล่าว หรือการตัดสินใจงดเว้นการติดตั้งเพื่อป้องกันความเสี่ยงและความเสียหายจากการหยุดชะงักของระบบให้บริการ กรณีเกิดข้อผิดพลาด พร้อมทั้งจัดทำแผนการป้องกันความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศเป็นการชั่วคราว
Level - 4		
249.	The institution monitors patch management reports to ensure security patches are tested and implemented within aggressive time frames (e.g., 0-30 days).	บริษัทมีกระบวนการสอบทานรายงานผลการติดตั้งชุดโปรแกรมแก้ไขข้อบกพร่อง เพื่อให้มั่นใจถึงความครบถ้วนในการติดตั้งชุดโปรแกรมแก้ไขข้อบกพร่องเพื่อให้มั่นใจถึงความครบถ้วนของการทดสอบและการติดตั้งชุดโปรแกรมภายในระยะเวลาที่กำหนด

No	Questionnaire	คำอธิบาย
Level - 5		
250.	Segregated or separate systems are in place that mirror production systems allowing for rapid testing and implementation of patches and provide for rapid fallback when needed.	บริษัทมีการจัดเตรียมเครื่องหรือระบบสำหรับการทดสอบที่มีลักษณะเทียบเท่าเสมือนกับระบบงานหลัก เพื่อให้บริษัทสามารถดำเนินการทดสอบชุดโปรแกรมแก้ไขข้อบกพร่องได้อย่างรวดเร็วและเสมือนจริง ในการป้องกันความเสี่ยงหรือข้อผิดพลาดอันอาจจะเกิดขึ้นจากการติดตั้งชุดโปรแกรม
Corrective Controls - Remediation		
Level - 1		
251.	Issues identified in assessments are prioritized and resolved based on criticality and within the time frames established in the response to the assessment report.	รายงานตรวจประเมินด้านการควบคุมและรักษาความมั่นคงปลอดภัยสารสนเทศ ได้รับการจัดระดับความสำคัญและติดตามให้มีการแก้ไขภายในระยะเวลาที่กำหนด
Level - 2		
252.	Data is destroyed or wiped on hardware and portable/mobile media when a device is missing, stolen, or no longer needed.	บริษัทมีมาตรการในการลบทำลายข้อมูลที่จัดเก็บอยู่บนอุปกรณ์เคลื่อนที่ อุปกรณ์เครือข่าย เครื่องแม่ข่าย อุปกรณ์จัดเก็บข้อมูลแบบถอดย้ายได้ เมื่อได้รับการรายงานด้านอุปกรณ์ศูนย์หาย เมื่อไม่มีการใช้งานแล้ว หรือก่อนการจัดส่งอุปกรณ์เพื่อการซ่อมแซมหรือบำรุงรักษาโดยบริษัทผู้ให้บริการ
253.	Formal processes are in place to resolve weaknesses identified during penetration testing.	รายงานข้อบกพร่องด้านความมั่นคงปลอดภัยสารสนเทศจากผลการทดสอบเจาะระบบได้รับการรวบรวมและจัดทำแผนการแก้ไขข้อบกพร่อง ระยะเวลาในการดำเนินการ มาตรการป้องกันความเสี่ยง และมีการติดตามผลการดำเนินการแก้ไขให้แล้วเสร็จตามระยะเวลาที่กำหนด
Level - 3		
254.	Remediation efforts are confirmed by conducting a follow-up vulnerability scan.	ข้อบกพร่องด้านความมั่นคงปลอดภัยสารสนเทศจากผลการทดสอบช่องโหว่ระบบ (Vulnerability scan) ได้รับการติดตามและทดสอบซ้ำเพื่อให้มั่นใจว่าข้อบกพร่องได้รับการแก้ไขอย่างถูกต้องลุล่วง
255.	Penetration testing is repeated to confirm that medium- and high-risk, exploitable vulnerabilities have been resolved.	ข้อบกพร่องด้านความมั่นคงปลอดภัยสารสนเทศจากผลการทดสอบเจาะระบบ (Penetration test) ที่มีระดับความเสี่ยงอย่างมีนัยสำคัญได้รับการติดตามและทดสอบซ้ำเพื่อให้มั่นใจว่าข้อบกพร่องได้รับการแก้ไขอย่างถูกต้องลุล่วง

No	Questionnaire	คำอธิบาย
Level - 4		
256.	All medium and high risk issues identified in penetration testing, vulnerability scanning, and other independent testing are escalated to the board or an appropriate board committee for risk acceptance if not resolved in a timely manner.	ข้อบกพร่องด้านความมั่นคงปลอดภัยสารสนเทศจากผลการทดสอบช่องโหว่ระบบ (Vulnerability scan) และการทดสอบเจาะระบบ (Penetration test) และการตรวจสอบโดยผู้ตรวจประเมินอิสระอื่นๆ ที่มีระดับความเสี่ยงอย่างมีนัยสำคัญและไม่สามารถดำเนินการแก้ไขได้ตามระยะเวลาที่กำหนด ได้รับการรายงานไปยังคณะกรรมการบริษัท หรือ คณะกรรมการที่ได้รับมอบหมาย เพื่อพิจารณาแนวทางป้องกันความเสี่ยงชั่วคราว และอนุมัติยอมรับความเสี่ยง
Level - 5		
257.	The institution is developing technologies that will remediate systems damaged by zero-day attacks to maintain current recovery time objectives.	บริษัทมีเทคโนโลยี และมาตรการในการควบคุมและป้องกันความเสี่ยงจากการบุกรุกโจมตีประเภท Zero-day attack

4. External Dependency

No	Questionnaire	คำอธิบาย
Connections - Connections		
Level - 1		
258.	The critical business processes that are dependent on external connectivity have been identified.	บริษัทมีการรวบรวมข้อมูลกิจกรรมทางธุรกิจที่สำคัญที่มีการเชื่อมโยงและความต้องการการเชื่อมต่อทางเครือข่ายภายนอกอย่างครบถ้วน
259.	The institution ensures that third-party connections are authorized.	บริษัทมีกระบวนการร้องขอ ประเมินความเสี่ยงและมาตรการควบคุม และการอนุมัติเพื่อการเชื่อมต่อไปยังบริษัทหรือผู้ให้บริการภายนอกอย่างเป็นลายลักษณ์อักษร ทั้งนี้รูปแบบการเชื่อมต่ออาจอยู่ในลักษณะ การเชื่อมต่อแบบจุดต่อจุดผ่านวงจรเช่า (Leased line) การเชื่อมต่อแบบเครือข่ายส่วนบุคคลเสมือน (Virtual private network) หรือ การเชื่อมต่อผ่านบริการทางเครือข่ายที่ควบคุมโดยอุปกรณ์ไฟร์วอลล์ เป็นต้น
260.	A network diagram is in place and identifies all external connections.	บริษัทมีการจัดทำผังโครงสร้างเครือข่ายที่มีรายละเอียดการเชื่อมต่อไปยังเครือข่ายภายนอกอย่างครบถ้วน
Level - 2		
261.	Critical business processes have been mapped to the supporting external connections.	บริษัทมีการรวบรวมข้อมูลกิจกรรมทางธุรกิจที่สำคัญและมีการเชื่อมต่อทางเครือข่ายภายนอก และมีการระบุรายละเอียดช่องทางการเชื่อมต่อที่กำหนดไว้ เพื่อให้บริษัทสามารถบริหารจัดการการเชื่อมต่อได้อย่างมีประสิทธิผล
262.	The network diagram is updated when connections with third parties change or at least annually.	บริษัทมีการจัดทำผังโครงสร้างเครือข่ายที่มีรายละเอียดการเชื่อมต่อไปยังเครือข่ายภายนอกอย่างครบถ้วน และผังเครือข่ายได้รับการปรับปรุงเมื่อมีการเปลี่ยนแปลงที่สำคัญ หรือมีการสอบทานอย่างน้อยปีละ 1 ครั้ง
263.	Network and systems diagrams are stored in a secure manner with proper restrictions on access.	ผังโครงสร้างเครือข่ายมีการจัดเก็บในพื้นที่จัดเก็บข้อมูลที่มีการควบคุมและจำกัดการเข้าถึงอย่างปลอดภัย
Level - 3		
264.	Monitoring controls cover all external connections (e.g., third-party service providers, business partners, customers).	บริษัทมีการควบคุมและติดตามการใช้งานทางเครือข่ายและการวิเคราะห์พฤติกรรมทางเครือข่ายที่ครอบคลุมการเชื่อมต่อทางเครือข่ายไปยังบริษัทผู้ให้บริการภายนอก คู่ค้าทางธุรกิจ และลูกค้า

No	Questionnaire	คำอธิบาย
265.	Monitoring controls cover all internal network-to-network connections.	บริษัทมีการควบคุมและติดตามการใช้งานทางเครือข่ายและการวิเคราะห์พฤติกรรมทางเครือข่ายที่ครอบคลุมการเชื่อมต่อของเครือข่ายสำคัญภายใน
Level - 4		
266.	The security architecture is validated and documented before network connection infrastructure changes.	บริษัทมีการสอบทานด้านความเหมาะสมของโครงสร้างสถาปัตยกรรมทางเครือข่าย ก่อนการเปลี่ยนแปลงหรือการดำเนินการต่อเชื่อมกับเครือข่ายภายนอก ทั้งนี้การเปลี่ยนแปลงทางเครือข่ายได้รับการร้องขอ ประเมินความเสี่ยง และอนุมัติโดยผู้มีอำนาจตามกระบวนการบริหารการเปลี่ยนแปลงที่กำหนด
267.	The institution works closely with third-party service providers to maintain and improve the security of external connections.	บริษัทมีการติดตามการใช้งานทางเครือข่าย ระหว่างบริษัทและบริษัทผู้ให้บริการภายนอก ในการบำรุงรักษาและการปรับปรุงการควบคุมความปลอดภัยทางเครือข่าย เช่น การตรวจสอบบริการทางเครือข่ายที่มีการอนุญาตให้ใช้งานอย่างสม่ำเสมอ การตรวจสอบและปรับปรุงเทคโนโลยีและมาตรฐานการเข้ารหัส เมื่อมีการเปลี่ยนแปลง เป็นต้น
Level - 5		
268.	The institution's connections can be segmented or severed instantaneously to prevent contagion from cyber attacks.	บริษัทมีการแบ่งแยกช่องทางการเชื่องโยงทางเครือข่ายเป็นหลายช่องทางตามลักษณะการใช้งาน เพื่อป้องกันความเสี่ยงจากการบุกรุกโจมตีทางไซเบอร์อันอาจก่อให้เกิดความเสียหายของระบบเครือข่ายองค์กร
Relationship Management - Due Diligence		
Level - 1		
269.	Risk-based due diligence is performed on prospective third parties before contracts are signed, including reviews of their background, reputation, financial condition, stability, and security controls.	บริษัทมีกระบวนการบริหารจัดการผู้ให้บริการภายนอกที่ครอบคลุมขั้นตอนการประเมินและคัดเลือกผู้ให้บริการ ได้แก่ การตรวจสอบประวัติ ชื่อเสียง ความสามารถทางการเงิน ความมั่นคง และการควบคุมด้านการรักษาความปลอดภัยทางเทคโนโลยีสารสนเทศ ทั้งนี้การดำเนินการประเมินและคัดเลือกผู้ให้บริการต้องดำเนินการก่อนการสรุปผลการคัดเลือกและจัดทำสัญญาการใช้บริการ
270.	A list of third-party service providers is maintained.	บริษัทมีการรวบรวมข้อมูลและรายชื่อบริษัทผู้ให้บริการภายนอก เพื่อให้การควบคุมคุณภาพของการให้บริการเป็นไปอย่างมีประสิทธิภาพและประสิทธิผล

No	Questionnaire	คำอธิบาย
Level - 2		
271.	A formal process exists to analyze assessments of third-party cybersecurity controls.	บริษัทมีการจัดทำกระบวนการและเกณฑ์การประเมินการควบคุมด้านความมั่นคงปลอดภัยทางไซเบอร์ของบริษัทผู้ให้บริการภายนอกอย่างชัดเจนเป็นลายลักษณ์อักษร และบริษัทผู้ให้บริการภายนอกได้รับการประเมินการควบคุมด้านความมั่นคงปลอดภัยทางไซเบอร์อย่างครบถ้วน
Level - 3		
272.	A process is in place to confirm that the institution's third-party service providers conduct due diligence of their third parties (e.g., subcontractors).	บริษัทมีขั้นตอนเพื่อให้มั่นใจว่าบริษัทผู้ให้บริการภายนอกที่เป็นคู่สัญญากับบริษัทนั้น มีการควบคุมและประเมินบริษัทผู้รับเหมาช่วงในการให้บริการตามสัญญา
273.	Pre-contract, physical site visits of high-risk vendors are conducted by the institution or by a qualified third party.	บริษัทมีการประเมินบริษัทผู้ให้บริการภายนอก ณ. สถานที่ของบริษัทผู้ให้บริการภายนอก โดยบริษัทหรือผู้ตรวจประเมินอิสระที่ได้รับการยอมรับ สำหรับบริการหรือบริษัทผู้ให้บริการที่มีระดับความเสี่ยงระดับสูง
Level - 4		
274.	A continuous process improvement program is in place for third-party due diligence activity.	บริษัทมีการปรับปรุงขั้นตอนการประเมินและคัดเลือกบริษัทผู้ให้บริการภายนอกอย่างต่อเนื่องสม่ำเสมอ เพื่อให้มั่นใจถึงความเหมาะสมของเกณฑ์การประเมินที่สอดคล้องกับความเสี่ยง บริการ หรือเทคโนโลยีที่มีการเปลี่ยนแปลงไป
Level - 5		
275.	The institution is leading efforts to develop new auditable processes and for conducting due diligence and ongoing monitoring of cybersecurity risks posed by third parties.	บริษัทมีการพัฒนากระบวนการที่ตรวจสอบได้เพื่อใช้ในการประเมินและคัดเลือกบริษัทผู้ให้บริการภายนอก และกระบวนการติดตามความเสี่ยงด้านความปลอดภัยทางไซเบอร์จากการใช้งานบริษัทผู้ให้บริการภายนอก
Relationship Management - Contracts		
Level - 1		
276.	Formal contracts that address relevant security and privacy requirements are in place for all third parties that process, store, or transmit confidential	บริษัทมีการจัดทำสัญญามาตรฐานระหว่างบริษัทและบริษัทผู้ให้บริการภายนอก ที่ประกอบด้วยข้อกำหนดด้านความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ และข้อกำหนดด้านการรักษาความปลอดภัยข้อมูลส่วนบุคคลสำหรับบริษัทผู้ให้บริการที่มีการจัดเก็บ ประมวลผล และนำส่งข้อมูลความลับหรือข้อมูลส่วนบุคคล

No	Questionnaire	คำอธิบาย
277.	Contracts acknowledge that the third party is responsible for the security of the institution's confidential data that it possesses, stores, processes, or transmits.	บริษัทมีการจัดทำสัญญามาตรฐานระหว่างบริษัทและบริษัทผู้ให้บริการภายนอก ที่กำหนดหน้าที่ความรับผิดชอบของบริษัทผู้ให้บริการในการรักษาความลับข้อมูลของบริษัทที่อยู่ในความครอบครอง จัดเก็บ ประมวลผล และนำส่งโดยผู้ให้บริการ
278.	Contracts stipulate that the third-party security controls are regularly reviewed and validated by an independent party.	บริษัทมีการจัดทำสัญญามาตรฐานระหว่างบริษัทและบริษัทผู้ให้บริการภายนอก ที่กำหนดให้มีการตรวจประเมินการควบคุมด้านการรักษาความมั่นคงปลอดภัยสารสนเทศโดยผู้ตรวจประเมินอิสระ
279.	Contracts specify the security requirements for the return or destruction of data upon contract termination.	บริษัทมีการจัดทำสัญญามาตรฐานระหว่างบริษัทและบริษัทผู้ให้บริการภายนอก ที่ประกอบด้วยเงื่อนไขการส่งคืน หรือทำลายข้อมูลของบริษัทที่อยู่ในความครอบครองของบริษัทผู้ให้บริการ เมื่อสิ้นสุดสัญญาการให้บริการ
Level - 2		
280.	Responsibility for notification of direct and indirect security incidents and vulnerabilities is documented in contracts or service-level agreements (SLAs).	บริษัทมีการจัดทำสัญญามาตรฐานระหว่างบริษัทและบริษัทผู้ให้บริการภายนอก ที่กำหนดหน้าที่ความรับผิดชอบในการแจ้งเตือนผู้รับผิดชอบบริษัทเมื่อมีเหตุด้านความมั่นคงปลอดภัยสารสนเทศ และ/หรือ มีการกำหนดข้อกำหนดการแจ้งเตือนเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศเป็นส่วนหนึ่งของสัญญาระดับการให้บริการ (service-level agreements (SLAs))
281.	Contracts stipulate geographic limits on where data can be stored or transmitted.	บริษัทมีการจัดทำสัญญามาตรฐานระหว่างบริษัทและบริษัทผู้ให้บริการภายนอก ที่กำหนดข้อจำกัดทางภูมิศาสตร์ในการจัดเก็บและนำส่งข้อมูลของบริษัทโดยบริษัทผู้ให้บริการภายนอกไปยังกลุ่มประเทศที่ไม่ได้รับความยินยอม เช่น กลุ่มประเทศที่มีกฎหมายและมาตรฐานการป้องกันและรักษาความปลอดภัยข้อมูลส่วนบุคคลต่ำกว่ามาตรฐานที่กำหนดใน พรบ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 เป็นต้น

No	Questionnaire	คำอธิบาย
Level - 3		
282.	Third-party SLAs or similar means are in place that require timely notification of security events.	บริษัทมีการจัดทำสัญญาระดับการให้บริการ (service-level agreements (SLAs)) ระหว่างบริษัท และ บริษัทผู้ให้บริการภายนอกในการแจ้งเตือนด้านเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศภายในระยะเวลาที่กำหนด และยอมรับได้
Level - 4		
283.	Contracts require third-party service provider's security policies meet or exceed those of the institution.	บริษัทมีการจัดทำสัญญามาตรฐานระหว่างบริษัทและบริษัทผู้ให้บริการภายนอก ที่ประกอบด้วยข้อกำหนดด้านความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ ที่มีรายละเอียดขั้นต่ำเป็นไปตามนโยบายความมั่นคงปลอดภัยสารสนเทศของบริษัท
Level - 5		
284.	The institution promotes a sector-wide effort to influence contractual requirements for critical third parties to the industry.	บริษัทมีการจัดทำความร่วมมือในกลุ่มอุตสาหกรรม เพื่อให้มีอำนาจต่อรองในการจัดทำข้อกำหนดและร่างสัญญามาตรฐาน สำหรับบริษัทผู้ให้บริการภายนอกที่มีการให้บริการที่มีความสำคัญระดับสูงสำหรับบริษัทในกลุ่มอุตสาหกรรม
Relationship Management - Ongoing Monitoring		
Level - 1		
285.	The third-party risk assessment is updated regularly.	บริษัทมีการประเมินความเสี่ยงจากการใช้งานบริษัทผู้ให้บริการภายนอกอย่างสม่ำเสมอ เพื่อให้สอดคล้องกับบริการด้านเทคโนโลยีสารสนเทศ และความเสี่ยงที่อาจมีการเปลี่ยนแปลงไป
286.	Audits, assessments, and operational performance reports are obtained and reviewed regularly validating security controls for critical third parties.	บริษัทมีการติดตามรายงานการตรวจสอบการควบคุม รายงานการตรวจประเมิน และรายงานผลการปฏิบัติงานตามข้อกำหนดข้อตกลงการให้บริการของบริษัทผู้ให้บริการภายนอก และสอบทานความถูกต้องอย่างสม่ำเสมอ
Level - 2		
287.	A formal program assigns responsibility for ongoing oversight of third- party access.	บริษัทมีการกำหนดบทบาทหน้าที่ความรับผิดชอบอย่างเป็นทางการในการกำกับดูแลบริษัทผู้ให้บริการภายนอกอย่างเป็นลายลักษณ์อักษร

No	Questionnaire	คำอธิบาย
288.	Monitoring of third parties is scaled, in terms of depth and frequency, according to the risk of the third parties.	บริษัทมีการติดตามผลการปฏิบัติงานและบริการที่ได้รับจากบริษัทผู้ให้บริการภายนอก โดยมีรายละเอียดการตรวจสอบ และความถี่ในการตรวจสอบ สอดคล้องกับความเสี่ยงของบริการและบริษัทผู้ให้บริการภายนอก
Level - 3		
289.	Third-party employee access to the institution's confidential data are tracked actively based on the principles of least privilege.	บริษัทมีการกำหนดการควบคุมการเข้าถึงข้อมูลชั้นความลับของบุคลากรของบริษัทผู้ให้บริการภายนอก โดยการให้สิทธิเป็นไปตามหน้าที่ความรับผิดชอบและขอบเขตการให้บริการ
290.	Periodic on-site assessments of high-risk vendors are conducted to ensure appropriate security controls are in place.	บริษัทมีการตรวจประเมินการควบคุมด้านความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศของบริษัทผู้ให้บริการภายนอกที่มีความเสี่ยงระดับสูงเป็นรอบๆ ณ. สถานที่ของผู้ให้บริการ เพื่อให้มั่นใจถึงกระบวนการควบคุมเป็นไปตามข้อกำหนด
Level - 4		
291.	Third-party employee access to confidential data on third-party hosted systems is tracked actively via automated reports and alerts.	บริษัทมีการดำเนินมาตรการตรวจสอบการเข้าถึงข้อมูลชั้นความลับของบุคคลากรบริษัทผู้ให้บริการภายนอก ที่อยู่ในความครอบครองของบริษัทผู้ให้บริการอย่างสม่ำเสมอ โดยให้มีการรายงาน หรือแจ้งเตือนอัตโนมัติเมื่อมีการเข้าถึง
292.	Independent Audits of high-risk vendors are conducted on an annual basis.	บริษัทมีการจัดให้มีการตรวจสอบบริษัทผู้ให้บริการภายนอกที่มีความเสี่ยงระดับสูงโดยผู้ตรวจสอบอิสระอย่างน้อยปีละ 1 ครั้ง
Level - 5		
293.	The institution is leading efforts to develop new auditable processes for ongoing monitoring of cybersecurity risks posed by third parties.	บริษัทมีการพัฒนากระบวนการที่ตรวจสอบได้เพื่อใช้ในการติดตามความเสี่ยงด้านความปลอดภัยทางไซเบอร์จากการใช้งานบริษัทผู้ให้บริการภายนอก

5. Cyber incident management

No	Questionnaire	คำอธิบาย
Incident Resilience Planning and Strategy - Planning		
Level - 1		
294.	The institution has documented how it will react and respond to cyber incidents.	บริษัทมีการจัดทำขั้นตอนการตอบสนองและรับมือเหตุการณ์ด้านความมั่นคงทางไซเบอร์อย่างเป็นลายลักษณ์อักษร ซึ่งจะครอบคลุมขั้นตอนการตรวจพบเหตุการณ์ การแจ้งเหตุ การพิสูจน์เหตุการณ์ การระงับและควบคุมความเสียหาย การจัดเก็บหลักฐานเพื่อการสืบสวน รวมถึงขั้นตอนการกู้คืนระบบงานและบริการ
295.	Communication channels exist to provide employees a means for reporting information security events in a timely manner.	บริษัทมีการจัดทำช่องทางการสื่อสารให้แก่พนักงานในการแจ้งเหตุด้านความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ เพื่อให้พนักงานผู้พบเหตุการณ์สามารถรายงานเหตุไปยังผู้รับผิดชอบได้อย่างรวดเร็วทันต่อเหตุการณ์
296.	Roles and responsibilities for incident response team members are defined.	บริษัทมีการจัดโครงสร้างและการกำหนดบทบาทหน้าที่ความรับผิดชอบของคณะทำงานในการรับมือเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ (Incident response team) อย่างเป็นลายลักษณ์อักษร
297.	The response team includes individuals with a wide range of backgrounds and expertise, from many different areas within the institution (e.g., management, legal, public relations, as well as information technology).	โครงสร้างคณะทำงานในการรับมือเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศประกอบไปด้วยผู้ที่มีความเชี่ยวชาญและความรู้ที่จำเป็นต่อการรับมือเหตุการณ์ ได้แก่ การบริหาร ข้อกฎหมาย การสื่อสารองค์กร รวมถึงองค์ความรู้ด้านเทคโนโลยีสารสนเทศ
298.	A formal backup and recovery plan exists for all critical business lines.	บริษัทมีการจัดให้มีการสำรองข้อมูลและแผนการกู้คืนระบบงานสำหรับระบบงานสำคัญของบริษัทตามการประเมินความเสี่ยงและผลกระทบทางธุรกิจ
299.	The institution plans to use business continuity, disaster recovery, and data backup programs to recover operations following an incident.	บริษัทมีการจัดทำแผนต่อเนื่องทางธุรกิจ (BCP) แผนกู้คืนเมื่อเกิดภัยพิบัติ (DR) และการสำรองข้อมูล เพื่อที่จะกู้คืนระบบงานที่เสียหายจากเหตุการณ์
Level - 2		
300.	The remediation plan and process outlines the mitigating actions, resources, and time parameters.	บริษัทมีการจัดทำแผนการแก้ไขเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ โดยประกอบด้วยกระบวนการและขั้นตอนในการควบคุมความเสียหาย ทรัพยากรที่ใช้ในการดำเนินการ และกรอบระยะเวลาในการดำเนินการ

No	Questionnaire	คำอธิบาย
301.	The corporate disaster recovery, business continuity, and crisis management plans have integrated consideration of cyber incidents.	บริษัทมีการจัดทำแผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ แผนบริหารความต่อเนื่องทางธุรกิจ และแผนการจัดการภาวะวิกฤติ ที่มีความเชื่อมโยงและครอบคลุมเหตุการณ์ด้านความปลอดภัยทางไซเบอร์ พร้อมทั้งมีแนวทางการบริหารจัดการเหตุการณ์ที่สอดคล้องต้องกัน เช่น เกณฑ์การประเมินระดับความรุนแรงของเหตุการณ์ การรายงานเหตุการณ์ไปยังคณะทำงานในการรับมือเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศและคณะทำงานในการรับมือเหตุการณ์ในภาวะวิกฤติ การประกาศใช้แผนฉุกเฉินด้านเทคโนโลยีสารสนเทศ และแผนบริหารความต่อเนื่องทางธุรกิจ เป็นต้น
302.	Alternative processes have been established to continue critical activity within a reasonable time period.	บริษัทมีการจัดทำแผนทางเลือก เพื่อให้ระบบให้บริการสามารถให้บริการต่อไปได้ภายในระยะเวลาที่กำหนด
303.	Business impact analyses have been updated to include cybersecurity.	การประเมินผลกระทบทางธุรกิจที่มีการจัดทำครอบคลุมถึงการประเมินผลกระทบที่เกิดจากเหตุการณ์ด้านความมั่นคงปลอดภัยทางไซเบอร์
304.	Due diligence has been performed on technical sources, consultants, or forensic service firms that could be called to assist the institution during or following an incident.	กรณีมีความจำเป็น บริษัทมีการจัดเตรียมองค์ความรู้และทรัพยากรจากบริษัทผู้ให้บริการภายนอก หรือ ที่ปรึกษาที่สามารถให้บริการได้เมื่อเกิดเหตุการณ์ด้านความมั่นคงทางไซเบอร์ในการแก้ไขสถานการณ์ หรือ การสืบสวนเหตุการณ์
Level - 3		
305.	A strategy is in place to coordinate and communicate with internal and external stakeholders during or following a cyber attack.	บริษัทมีการจัดเตรียมกลยุทธ์ในการประสานงานและสื่อสารกับผู้มีส่วนได้ส่วนเสียทั้งภายใน เช่น ผู้ถือหุ้น ผู้บริหาร พนักงาน และ ผู้มีส่วนได้ส่วนเสียภายนอก เช่น ลูกค้า บริษัทผู้ให้บริการภายนอก ผู้บังคับใช้กฎหมาย หน่วยงานกำกับดูแล เป็นต้น เพื่อให้การประสานงานและการสื่อสารระหว่างเกิดเหตุการณ์การโจมตีทางไซเบอร์เป็นไปอย่างมีประสิทธิผล
306.	Plans are in place to re-route or substitute critical functions and/or services that may be affected by a successful attack on Internet-facing systems.	บริษัทมีการจัดเตรียมช่องทางและระบบให้บริการสำรองในกรณีบริการที่อาจได้รับผลกระทบจากการโจมตีทางไซเบอร์ผ่านระบบอินเทอร์เน็ต

No	Questionnaire	คำอธิบาย
307.	Lessons learned from real-life cyber incidents and attacks on the institution and other organizations are used to improve the institution's risk mitigation capabilities and response plan.	บริษัทมีการถอดบทเรียนจากเหตุการณ์การโจมตีทางไซเบอร์ที่เกิดขึ้นจริง แล้วนำไปปรับปรุงความสามารถในการลดความเสี่ยงของบริษัท และปรับปรุงแผนรับมือภัยคุกคามทางไซเบอร์
Level - 4		
308.	Multiple systems, programs, or processes are implemented into a comprehensive cyber resilience program to sustain, minimize, and recover operations from an array of potentially disruptive and destructive cyber incidents.	บริษัทมีการจัดเตรียมระบบงาน เครื่องมือ และกระบวนการที่จำเป็นเพื่อรองรับการให้บริการอย่างต่อเนื่องเมื่อเกิดเหตุการณ์โจมตีทางไซเบอร์ เพื่อจำกัดผลกระทบหรือความเสียหายจากการโจมตี พร้อมทั้งขั้นตอนการกู้คืนกิจกรรมและระบบงานสำคัญในการให้บริการ
Level - 5		
309.	The incident response process includes detailed actions and rule-based triggers for automated response.	บริษัทมีการจัดเตรียมขั้นตอนการรับมือเหตุการณ์ในรายละเอียดในการตอบสนองต่อเหตุการณ์ อันประกอบด้วยกิจกรรมและขั้นตอนการดำเนินการในแต่ละขั้นตอน แนวทางและเงื่อนไขการตัดสินใจเมื่อเกิดเหตุการณ์ เพื่อให้การดำเนินการเป็นไปอย่างรวดเร็ว หรือการตอบสนองเป็นไปอย่างอัตโนมัติ
Incident Resilience Planning and Strategy - Testing		
Level - 1		
310.	Business continuity testing involves collaboration with critical third parties.	บริษัทมีการทดสอบแผนความต่อเนื่องทางธุรกิจที่ครอบคลุมสถานการณ์เหตุการณ์ความปลอดภัยทางไซเบอร์ และขอบเขตการทดสอบครอบคลุมบริษัทผู้ให้บริการภายนอกที่สำคัญ
311.	Systems, applications, and data recovery is tested at least annually.	แผนการกู้คืนระบบ ระบบงาน และข้อมูลได้รับการทดสอบอย่างน้อยปีละ 1 ครั้ง
Level - 2		
312.	Recovery scenarios include plans to recover from data destruction and impacts to data integrity, data loss, and system and data availability.	การจำลองสถานการณ์การกู้คืนระบบ ครอบคลุมแผนการกู้คืนระบบและข้อมูลที่ได้รับความเสียหาย หรือได้รับผลกระทบจากเหตุการณ์ ได้แก่สถานการณ์ที่มีผลกระทบต่อความถูกต้องของข้อมูล ระบบงานและข้อมูลสูญหายหรือถูกทำลาย

No	Questionnaire	คำอธิบาย
313.	Widely reported events are used to evaluate and improve the institution's response.	บริษัทมีการรวบรวมข้อมูลเหตุการณ์ที่เกิดขึ้นในสาธารณะเพื่อประเมินสถานการณ์ที่อาจจะเกิดขึ้น ทั้งนี้เพื่อปรับปรุงแนวทางการรับมือต่อเหตุการณ์ด้านความปลอดภัยทางไซเบอร์
314.	Information backups are tested periodically to verify they are accessible and readable.	บริษัทมีการทดสอบแหล่งข้อมูลสำรองอย่างสม่ำเสมอ เพื่อให้มั่นใจถึงความพร้อมใช้ของแหล่งข้อมูลและความสามารถในการกู้คืนระบบ
Level - 3		
315.	Cyber-attack scenarios are analyzed to determine potential impact to critical business processes.	บริษัทมีการประเมินและวิเคราะห์สถานการณ์การโจมตีทางไซเบอร์ เพื่อประเมินสถานการณ์และผลกระทบที่เป็นไปได้ต่อกิจกรรมทางธุรกิจที่สำคัญ
316.	Resilience testing is based on analysis and identification of realistic and highly likely threats as well as new and emerging threats facing the institution.	การทดสอบด้านแผนการรับมือเหตุการณ์และการกู้คืนระบบ มีการจำลองสถานการณ์ โดยอาศัยผลการวิเคราะห์เหตุการณ์ที่มีโอกาศเกิดขึ้นและมีความเป็นไปได้อย่างสมเหตุสมผล รวมถึงเหตุการณ์หรือสถานการณ์การโจมตีทางไซเบอร์ในรูปแบบใหม่ที่ปรากฏขึ้น
Level - 4		
317.	Resilience testing is comprehensive and coordinated across all critical business functions.	การทดสอบด้านแผนการรับมือเหตุการณ์และการกู้คืนระบบจากการโจมตีทางไซเบอร์ มีขอบเขตการทดสอบครอบคลุมถึงเหตุการณ์สำหรับกิจกรรมทางธุรกิจที่สำคัญ
318.	Incident response testing evaluates the institution from an attacker's perspective to determine how the institution or its assets at critical third parties may be targeted.	การทดสอบด้านแผนการรับมือเหตุการณ์การโจมตีทางไซเบอร์มีการประเมินสถานการณ์โจมตี โดยวิเคราะห์แนวทางการโจมตีจากมุมมองของผู้บุกรุกโจมตีระบบ ที่มีเป้าหมายต่อทรัพย์สินสำคัญด้านสารสนเทศของบริษัทหรือทรัพย์สินสำคัญที่อยู่ในความดูแลของบริษัทผู้ให้บริการภายนอก
Level – 5		
319.	The institution tests the ability to shift business processes or functions between different processing centers or technology systems for cyber incidents without interruption to business or loss of productivity or data.	บริษัทมีการทดสอบแผนการรับมือเหตุการณ์ โดยครอบคลุมการทดสอบการโอนย้ายกระบวนการทางธุรกิจหรือ การโอนย้ายการประมวลผลไปยังศูนย์ประมวลผลสำรอง โดยจำกัดความเสียหายหรือการหยุดชะงักของระบบให้บริการ และการสูญหาของข้อมูล

No	Questionnaire	คำอธิบาย
320.	The institution has validated that it is able to remediate systems damaged by zero-day attacks to maintain current recovery time objectives.	บริษัทมีมาตรการและการทดสอบการควบคุมและป้องกันความเสี่ยงจากการบุกรุกโจมตีประเภท Zero-day attack
Detection, Response, and Mitigation - Detection		
Level - 1		
321.	Alert parameters are set for detecting information security incidents that prompt mitigating actions.	บริษัทมีการกำหนดให้มีระบบตรวจจับเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ เพื่อแจ้งเตือนไปยังบุคลากรผู้รับผิดชอบต่อเหตุการณ์
322.	Tools and processes are in place to detect, analyse problem, assess impact, alert, and trigger the incident response program.	บริษัทมีการจัดทำเครื่องมือและกระบวนการในการตรวจจับ วิเคราะห์ปัญหา ประเมินผลกระทบ และแจ้งเตือนเหตุการณ์บุกรุก หรือ เหตุการณ์ด้านความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ เพื่อให้ผู้รับผิดชอบสามารถตอบสนองต่อเหตุการณ์ได้อย่างทันเวลา
Level - 2		
323.	The institution has processes to detect and alert the incident response team when potential insider activity manifests that could lead to data theft or destruction.	บริษัทมีกระบวนการในการตรวจพบเหตุการณ์และแจ้งเตือนไปยังคณะทำงานในการรับมือเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ (Incident response team) เมื่อปรากฏแนวโน้มการเกิดเหตุด้านความปลอดภัยอันอาจนำไปสู่การขโมยข้อมูล หรือ การทำลายข้อมูลที่เกิดจากบุคคลภายใน
Level - 3		
324.	The incident response program is triggered when anomalous behaviours and attack patterns or signatures are detected. (e.g. IDS/IPS)	บริษัทมีการบันทึกเหตุการณ์ด้านความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศเพื่อดำเนินการตรวจสอบตามขั้นตอนที่กำหนด เมื่อมีการตรวจพบพฤติกรรมต้องสงสัยหรือรูปแบบการโจมตีระบบที่ตรวจสอบโดยระบบ เช่น ระบบตรวจจับและป้องกันผู้บุกรุก
325.	Incidents are detected in real time through automated processes that include instant alerts to appropriate personnel who can respond.	บริษัทมีการใช้งานเครื่องมือตรวจสอบเหตุการณ์แบบอัตโนมัติอย่างทันทีและตลอดเวลา (Real-time) เพื่อแจ้งเตือนเหตุการณ์ไปยังบุคคลผู้รับผิดชอบในการตอบสนองต่อเหตุการณ์นั้น
326.	Incident detection processes are capable of correlating events across the enterprise. (SIEM)	บริษัทมีการใช้งานเครื่องมือตรวจสอบเหตุการณ์แบบอัตโนมัติอย่างทันทีและตลอดเวลา (Real-time) ที่มีความสามารถในการรวบรวมและเชื่อมโยงเหตุการณ์ เช่น การใช้งานระบบบริหารจัดการและวิเคราะห์ข้อมูลความปลอดภัยของระบบเครือข่าย (Security information and event management (SIEM))

No	Questionnaire	คำอธิบาย
Level - 4		
327.	Automated tools are implemented to provide specialized security monitoring based on the risk of the assets to detect and alert incident response teams in real time. (APT, WAF, DB Firewall, Behaviour)	บริษัทมีการใช้งานเครื่องมืออัตโนมัติในการตรวจสอบเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศแบบเฉพาะทางเพื่อตรวจพบ และ แจ้งเตือนไปยังผู้รับผิดชอบอย่างทันทีและตลอดเวลา (Real-time) เช่น ระบบ advanced persistent threat (APT) ระบบ web application firewall (WAF) ระบบ database firewall (DB firewall) ระบบวิเคราะห์พฤติกรรมการใช้งาน Behavioural based security เป็นต้น
Level - 5		
328.	The institution is able to detect and block zero-day attempts and inform management and the incident response team in real time.	บริษัทมีมาตรการในการควบคุมและป้องกันความเสี่ยงจากการบุกรุกโจมตีประเภท Zero-day attack และแจ้งเตือนไปยังคณะทำงานในการรับมือเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ (Incident response team) เมื่อมีการตรวจพบเหตุการณ์
Detection, Response, and Mitigation - Response and Mitigation		
Level - 1		
329.	Appropriate steps are taken to contain and control an incident to prevent further unauthorized access to or use of customer information.	บริษัทมีการจัดทำมาตรการและแนวทางปฏิบัติ เพื่อควบคุมและจำกัดความเสียหายของเหตุการณ์ เพื่อป้องกันการบุกรุกโจมตีระบบอย่างต่อเนื่องและขยายการโจมตีไปยังระบบงานอื่น เช่น มาตรการระงับและตัดการเชื่อมโยงทางเครือข่าย หรือระบบอินเทอร์เน็ตกรณีจำเป็น เป็นต้น
Level - 2		
330.	The incident response plan is designed to prioritize incidents and analyse vulnerabilities, enabling a rapid response for significant cybersecurity incidents or vulnerabilities.	แผนการตอบสนองต่อเหตุการณ์ด้านความปลอดภัยทางไซเบอร์มีการจัดทำและประกอบด้วยขั้นตอนการประเมินระดับความสำคัญของเหตุการณ์ และวิเคราะห์ช่องโหว่ ทั้งนี้เพื่อบริษัทมีขีดความสามารถให้การตอบสนองต่อเหตุการณ์ที่มีระดับสำคัญสูงได้อย่างทันท่วงทีต่อสถาณการณ์
331.	A process is in place to help contain incidents and restore operations with minimal service disruption.	แผนการตอบสนองต่อเหตุการณ์ด้านความปลอดภัยทางไซเบอร์ที่มีการจัดทำประกอบด้วยขั้นตอนการจำกัดความเสียหาย และขั้นตอนการกู้คืนระบบสนับสนุนการปฏิบัติงานในการจำกัดระยะเวลาหยุดชะงักของระบบให้บริการ

No	Questionnaire	คำอธิบาย
332.	Procedures include containment strategies and notifying potentially impacted third parties.	แผนการตอบสนองต่อเหตุการณ์ด้านความปลอดภัยทางไซเบอร์ที่มีการจัดทำ ประกอบด้วยแนวทางรับมือเชิงกลยุทธ์ในการสื่อสารกับบุคคลภายนอกที่อาจได้รับผลกระทบจากเหตุการณ์
333.	Processes are in place to trigger the incident response program when an incident occurs at a third party.	แผนการตอบสนองต่อเหตุการณ์ด้านความปลอดภัยทางไซเบอร์ที่มีการจัดทำประกอบด้วยแนวทางการจัดการเหตุการณ์ที่อาจจะเกิดขึ้นต่อบริษัทผู้ให้บริการภายนอกที่อาจส่งผลต่อความต่อเนื่องในการให้บริการของบริษัท หรือเหตุการณ์ความเสียหายต่อข้อมูลของบริษัทที่อยู่ภายใต้ความครอบครองและบริหารจัดการโดยบริษัทผู้ให้บริการภายนอกนั้นๆ
334.	Records are generated to support incident investigation and mitigation.	บริษัทมีการรวบรวมข้อมูลเพื่อใช้ในการสืบสวนเหตุการณ์ด้านความปลอดภัยทางไซเบอร์ภายหลังจากการกู้คืนระบบ พร้อมทั้งเพื่อสืบหาสาเหตุช่องโหว่เพื่อจัดทำแนวทางการป้องกันหรือลดผลกระทบของเหตุการณ์ในอนาคต
Level – 3		
335.	Processes are in place to ensure assets affected by a security incident that cannot be returned to operational status are quarantined, removed, disposed of, and/or replaced.	บริษัทมีการจัดทำแผนและขั้นตอนการปฏิบัติงานที่ครอบคลุมการจัดเก็บและทำลายข้อมูลและระบบงานที่ได้รับความเสียหายจากเหตุการณ์ด้านความปลอดภัยทางไซเบอร์ และไม่สามารถในการกู้คืนระบบงานให้กลับมาใช้งานได้
336.	Processes are in place to ensure that restored assets are appropriately reconfigured and thoroughly tested before being placed back into operation.	บริษัทมีการจัดทำขั้นตอนการกู้คืนระบบให้อยู่ในสภาวะปลอดภัย (Safe state) รวมถึงขั้นตอนการทดสอบระบบงานก่อนนำกลับสู่การให้บริการ
Level - 4		
337.	The incident management function collaborates effectively with the cyber threat intelligence function during an incident.	คณะทำงานในการรับมือเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ (Incident response team) มีการปฏิบัติงานร่วมกับผู้รับผิดชอบด้านการข่าวไซเบอร์ (cyber threat intelligence function) ตลอดกระบวนการแก้ไขสถานการณ์จากการโจมตีทางไซเบอร์

No	Questionnaire	คำอธิบาย
Level - 5		
338.	The institution's risk management of significant cyber incidents results in limited to no disruptions to critical services.	บริษัทมีกระบวนการบริหารความเสี่ยงจากเหตุการณ์ด้านความปลอดภัยทางไซเบอร์ และมีมาตรการควบคุมและลดความเสี่ยงเพื่อให้ระบบให้บริการสำคัญมีขีดความสามารถในการให้บริการอย่างต่อเนื่อง และจำกัดระยะเวลาหยุดชะงักของการให้บริการ
339.	The technology infrastructure has been engineered to limit the effects of a cyber attack on the production environment from migrating to the backup environment (e.g., air-gapped environment and processes).	บริษัทมีการดำเนินมาตรการ และจัดหาเทคโนโลยีป้องกันเหตุการณ์โจมตีทางไซเบอร์ เพื่อลดผลกระทบและลดโอกาสหรือสถานการณ์ที่ต้องโอนย้ายระบบประมวลผลไปยังศูนย์ประมวลผลสำรอง
Escalation and Reporting - Escalation and Reporting		
Level - 1		
340.	A process exists to contact personnel who are responsible for analyzing and responding to an incident.	แผนการตอบสนองต่อเหตุการณ์ด้านความปลอดภัยทางไซเบอร์ได้รับการจัดทำและประกอบด้วยรายละเอียดการติดต่อผู้รับผิดชอบในการวิเคราะห์และตอบสนองต่อเหตุการณ์ด้านความปลอดภัยทางไซเบอร์
341.	Procedures exist to notify customers, regulators, and law enforcement as required or necessary when the institution becomes aware of an incident involving the unauthorized access to or use of sensitive customer information.	บริษัทมีการกำหนดผู้รับผิดชอบที่ได้รับมอบอำนาจ และจัดทำกระบวนการในการติดต่อสื่อสารไปยังลูกค้า หน่วยงานกำกับดูแล หน่วยงานบังคับใช้กฎหมาย เมื่อบริษัทตระหนักถึงการเกิดเหตุการณ์ด้านความปลอดภัยทางไซเบอร์ หรือ เหตุการณ์ที่เกี่ยวข้องกับการเข้าถึง หรือใช้ข้อมูลสำคัญของลูกค้าเช่นข้อมูลทางการเงิน เป็นต้น
342.	The institution prepares an annual report of security incidents or violations for the board or an appropriate board committee.	บริษัทมีการรวบรวมและจัดทำรายงานสรุปเหตุการณ์ด้านความมั่นคงปลอดภัยทางไซเบอร์ประจำปี เพื่อรายงานต่อคณะกรรมการบริษัท หรือคณะกรรมการที่ได้รับมอบหมาย
343.	Incidents are classified, logged, and tracked.	เหตุการณ์ด้านความมั่นคงปลอดภัยทางไซเบอร์ได้รับการจัดระดับความสำคัญ บันทึก และติดตามเหตุการณ์
Level - 2		
344.	Criteria have been established for escalating cyber incidents or vulnerabilities to the board and senior management based on the potential impact and criticality of the risk.	บริษัทมีการจัดทำเกณฑ์การประเมินระดับความสำคัญของเหตุการณ์ด้านความมั่นคงปลอดภัยทางไซเบอร์ และขั้นตอนการสื่อสารเหตุการณ์ไปยังคณะกรรมการบริษัทและผู้บริหารระดับสูง เมื่อเหตุการณ์ดังกล่าวมีแนวโน้มจะเกิดผลกระทบระดับร้ายแรงต่อบริษัท

No	Questionnaire	คำอธิบาย
345.	Tracked cyber incidents are correlated for trend analysis and reporting.	เหตุการณ์ด้านความมั่นคงปลอดภัยทางไซเบอร์ได้รับการติดตาม และมีการเชื่อมโยงเหตุการณ์เพื่อวิเคราะห์แนวโนมการบุกรุกโจมตี เพื่อรายงานไปยังผู้บริหารที่เกี่ยวข้อง
Level - 3		
346.	Employees that are essential to mitigate the risk (e.g., fraud, business resilience) know their role in incident escalation.	บริษัทมีการสื่อสารบทบาทหน้าที่ไปยังพนักงานและหน่วยงานที่เกี่ยวข้องในกระบวนการรับมือเหตุการณ์ด้านความมั่นคงปลอดภัยทางไซเบอร์ เช่น หน่วยงานตรวจสอบทุจริต หน่วยงานด้านการบริหารความต่อเนื่องทางธุรกิจ หน่วยงานด้านกฎหมาย หน่วยงานสื่อสารองค์กร เป็นต้น
347.	A communication plan is used to notify other organizations, including third parties, of incidents that may affect them or their customers.	บริษัทมีการจัดทำแผนการสื่อสารไปยังหน่วยงานภายนอกที่อาจได้รับผลกระทบจากเหตุการณ์ด้านความมั่นคงปลอดภัยทางไซเบอร์ เพื่อแจ้งผลกระทบที่อาจมีต่อบริษัทหรือลูกค้าของบริษัท
348.	An external communication plan is used for notifying media regarding incidents when applicable.	บริษัทมีการกำหนดบุคคลผู้มีหน้าที่รับผิดชอบและมีอำนาจในการสื่อสาร พร้อมทั้งจัดเตรียมแผนการสื่อสารต่อเหตุการณ์ด้านความมั่นคงปลอดภัยทางไซเบอร์ไปยังสื่อสาธารณะ เช่น สำนักข่าว เป็นต้น
Level - 4		
349.	Detailed metrics, dashboards, and/or scorecards outlining cyber incidents and events are provided to management and are part of the board meeting package.	บริษัทมีการจัดทำรายงานด้านเหตุการณ์ความมั่นคงปลอดภัยทางไซเบอร์ในรูปแบบที่เข้าใจง่าย เพื่อการสื่อสารไปยังผู้บริหารระดับสูง และ เป็นส่วนหนึ่งในวาระการประชุมของคณะกรรมการบริษัท
Level - 5		
350.	A mechanism is in place to provide instantaneous notification of incidents to management and essential employees through multiple communication channels with tracking and verification of receipt.	บริษัทมีการจัดเตรียมช่องทางการสื่อสารที่มีประสิทธิภาพในการแจ้งเตือนเหตุการณ์ด้านความมั่นคงปลอดภัยทางไซเบอร์ ไปยังผู้บริหารระดับสูง และพนักงานที่เกี่ยวข้องอย่างรวดเร็ว และสามารถตรวจสอบผลการรับรู้ข่าวสารและการแจ้งเตือนได้