International Institute for
Trade and Development

แนวทางปฏิบัติการตรวจสอบ ด้านความมั่นคงปลอดภัยไซเบอร์

พฤษภาคม ๒๕๖๗

กลุ่มงานสารสนเทศ
สำนักยุทธศาสตร์และสารสนเทศ

สารบัญ

แนวทางการตรวจสอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

๑. บทนำ (Introduction)

ตามที่สถาบันระหว่างประเทศเพื่อการค้าและการพัฒนา (องค์การมหาชน) ได้ออกประกาศ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ พ.ศ. ๒๕๖๗ นั้น กำหนดให้มีการตรวจสอบความมั่นคงปลอดภัยไซเบอร์จะต้องดำเนินการอย่างน้อยปีละหนึ่ง หรือความถี่ที่สูงกว่านั้นตามที่สถาบันของรัฐ และสถาบันโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ของสถาบันระหว่างประเทศเพื่อการค้าและการพัฒนา (องค์การมหาชน) กำหนดในกรณีใดกรณีหนึ่ง และดำเนินการโดยผู้ตรวจสอบที่ได้รับอนุมัติหรือแต่งตั้งโดยสถาบัน

๒. วัตถุประสงค์ (Purpose)

เอกสารฉบับนี้มีวัตถุประสงค์เพื่อกำหนดความคาดหวังในการตรวจสอบ และใช้เป็นแนวทางสำหรับผู้ตรวจสอบที่ได้รับการอนุมัติ หรือได้รับการแต่งตั้งเพื่อทำการตรวจสอบความมั่นคงปลอดภัยไซเบอร์

เอกสารนี้ไม่ได้หมายถึงแหล่งข้อมูลที่ละเอียดถี่ถ้วนสำหรับการดำเนินการตรวจสอบการรักษาความมั่นคงปลอดภัยไซเบอร์ของสถาบัน

ในกรณีที่การตรวจสอบความมั่นคงปลอดภัยไซเบอร์ไม่มีหัวข้อใดที่กำหนดในเอกสารนี้ ผู้ตรวจสอบควรใช้ดุลยพินิจเยี่ยงผู้ประกอบวิชาชีพและระบุสถานการณ์ดังกล่าวในรายงานการตรวจสอบ

๓. กลุ่มเป้าหมาย (Audience)

กลุ่มเป้าหมายของเอกสารนี้:

ก. ผู้ตรวจสอบที่ได้รับการอนุมัติหรือแต่งตั้งอย่างเป็นทางการจากคณะกรรมการ และ

ข. ผู้มีส่วนได้ส่วนเสีย (เช่น หัวหน้าหน่วยงาน เจ้าของระบบและผู้ขาย หัวหน้าเจ้าหน้าที่รักษาความมั่นคงปลอดภัยข้อมูล ฯลฯ) ที่จำเป็นต้องรู้เกี่ยวกับความคาดหวังในการตรวจสอบความมั่นคงปลอดภัยไซเบอร์สำหรับการตรวจสอบสถาบันของตน

๔. ขอบเขต (Scope)

เอกสารนี้ครอบคลุมการตรวจสอบความมั่นคงปลอดภัยไซเบอร์ ตามมาตรา ๕๔ แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒

๕. การอนุมัติผู้ตรวจสอบ (Auditor Approval)

ผู้ตรวจสอบต้องได้รับการอนุมัติหรือแต่งตั้งโดยสถาบัน เพื่อดำเนินการตรวจสอบความมั่นคงปลอดภัยไซเบอร์ในสถาบัน โดยสถาบันและผู้ตรวจสอบจะต้องส่งแบบฟอร์มที่เกี่ยวข้องตามที่สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์ (สกมช.) กำหนด ใบสมัครจะถือว่าสมบูรณ์ก็ต่อเมื่อแบบฟอร์มที่เกี่ยวข้องทั้งหมดและเอกสารประกอบที่ส่งมาโดยสถาบัน และผู้ตรวจสอบนั้นครบถ้วนและเป็นไปตามลำดับ

เกณฑ์การพิจารณามี ๒ ประการ ได้แก่ ความเป็นอิสระและความสามารถที่สำนักงานตรวจสอบหรือทีมงาน (Audit Firm/Team) และผู้ตรวจสอบ (Auditors) ที่เสนอจำเป็นต้องปฏิบัติตาม สำนักงานตรวจสอบหรือทีมงาน และผู้ตรวจสอบที่ได้รับการแต่งตั้ง:

ก. ไม่ควรอยู่ในตำแหน่งที่มีผลประโยชน์ทับซ้อน (Conflict of interest) ใด ๆ ไม่ว่าจะเกิดขึ้นจริง มีแนวโน้ม หรือได้รับรู้ ผลประโยชน์ทับซ้อน หมายถึง สถานการณ์ใด ๆ ที่ผลประโยชน์ของผู้ตรวจสอบอาจแทรกแซงการปฏิบัติหน้าที่ของผู้ตรวจสอบอย่างเป็นอิสระและมีวัตถุประสงค์ และ

ข. ควรมีความสามารถทางเทคนิคที่จำเป็น (เช่น คุณวุฒิวิชาชีพ/ใบรับรอง ทักษะ ความรู้ และประสบการณ์ที่เกี่ยวข้อง) เพื่อดำเนินการตรวจสอบ

ทั้งนี้ สถาบันอาจพิจารณาแตกต่างกันไปตามที่สถาบันเห็นสมควร ในประเด็นต่อไปนี้

(๑) จำนวนผู้ตรวจสอบของแต่ละสำนัก

(๒) ระยะเวลาในการขออนุญาต เช่น รายปีหรือตามรอบการตรวจสอบ เป็นต้น

ในกรณีที่ผู้ตรวจสอบของสถาบันที่ลงทะเบียนแล้วลาออกจากการเป็นเจ้าหน้าที่ก่อนการดำเนินการตรวจสอบหรือมีการเปลี่ยนแปลงเจ้าหน้าที่ที่ลงทะเบียนไว้แล้วสถาบันจะแจ้ง สกมช. ภายใน ๓๐ วันนับจากวันที่มีการเปลี่ยนแปลงอย่างเป็นทางการ

๖. ความคาดหวังในการตรวจสอบ (Audit Expectations)

ส่วนนี้กำหนดความคาดหวังในการตรวจสอบ มีวัตถุประสงค์เพื่อช่วยให้ผู้อ่านเข้าใจว่าควรดำเนินการและรายงานการตรวจสอบความมั่นคงปลอดภัยไซเบอร์อย่างไร

สถาบันได้ระบุความคาดหวังในการตรวจสอบไว้ ๗ ด้านในหัวข้อ ๖.๑ ถึง ๖.๗

๖.๑ หลักการตรวจสอบ (Principles of Auditing)

การตรวจสอบควรยึดหลักการต่อไปนี้เพื่อให้ข้อสรุปการตรวจสอบที่เกี่ยวข้องและเพียงพอ ทั้งนี้เพื่อช่วยให้ผู้ตรวจสอบซึ่งทำงานอย่างอิสระสามารถบรรลุข้อสรุปที่คล้ายคลึงกันในสถานการณ์ที่คล้ายคลึงกัน

ก. ความซื่อสัตย์ (Integrity): รากฐานของความเป็นมืออาชีพ

- ดำเนินการตรวจสอบด้วยความซื่อสัตย์และรับผิดชอบ
- ทำให้แน่ใจว่ามีความสามารถในขณะดำเนินการตรวจสอบ

- ดำเนินการตรวจสอบอย่างเป็นกลาง
- ทำให้แน่ใจว่ามีความยุติธรรมและเป็นกลางในการติดต่อทั้งหมด ระมัดระวังต่ออิทธิพลใด ๆ ที่อาจส่งผลต่อดุลยพินิจของผู้ตรวจสอบระหว่างการตรวจสอบ

ข. การนำเสนออย่างยุติธรรม (Fair Presentation): หน้าที่ในการรายงานตามความเป็นจริงและถูกต้อง
- ตรวจสอบให้แน่ใจว่าผลการตรวจสอบ ข้อสรุปการตรวจสอบ และรายงานการตรวจสอบสะท้อนกิจกรรมการตรวจสอบตามความเป็นจริงและถูกต้อง
- รายงานอุปสรรคสำคัญที่พบในระหว่างการตรวจสอบและความเห็นที่แตกต่างระหว่างทีมตรวจสอบและผู้ตรวจประเมินที่ยังไม่ได้ข้อยุติ
- ตรวจสอบให้แน่ใจว่าการสื่อสารนั้นเป็นความจริง ถูกต้อง ตรงวัตถุประสงค์ ตรงเวลา ชัดเจน และครบถ้วน

ค. การปฏิบัติอย่างมืออาชีพ (Due Professional Care): การใช้ความรอบคอบและวิจารณญาณในการตรวจสอบ
- ใช้ความระมัดระวังอย่างเหมาะสมตามความสำคัญของงานและความเชื่อมั่นที่ผู้ตรวจสอบและผู้มีส่วนได้เสียอื่น ๆ มอบให้แก่ผู้ตรวจสอบ
- ใช้ดุลยพินิจอย่างมีเหตุผลในทุกสถานการณ์การตรวจสอบ

ง. การรักษาความลับ (Confidentiality): ความมั่นคงปลอดภัยของข้อมูล
- ใช้ดุลยพินิจในการใช้และปกป้องข้อมูลที่ได้รับระหว่างการตรวจสอบ
- ห้ามใช้ข้อมูลการตรวจสอบเพื่อประโยชน์ส่วนตัวหรือในทางที่เสียหายต่อผลประโยชน์ที่ชอบด้วยกฎหมายของผู้ตรวจสอบ
- จัดการกับข้อมูลที่ละเอียดอ่อนหรือเป็นความลับอย่างเหมาะสม

จ. ความเป็นอิสระ (Independence): พื้นฐานสำหรับความเป็นกลางของการตรวจสอบและความเที่ยงธรรมของข้อสรุปการตรวจสอบ
- ตรวจสอบความเป็นอิสระของกิจกรรมที่กำลังตรวจสอบ
- ดำเนินการในลักษณะที่ปราศจากอคติและผลประโยชน์ทับซ้อนในทุกกรณี
- รักษาความเป็นกลางตลอดกระบวนการตรวจสอบ
- ตรวจสอบให้แน่ใจว่าผลการตรวจสอบและข้อสรุปขึ้นอยู่กับหลักฐานการตรวจสอบ (audit evidence) เท่านั้น

๖.๒ วัตถุประสงค์ในการตรวจสอบ

วัตถุประสงค์ของการตรวจสอบ คือ:

ก. ตรวจสอบการปฏิบัติตามของสถาบันกับข้อกำหนดที่ระบุไว้ในประมวลแนวทางปฏิบัติและกรอบมาตรฐาน รวมถึงกฎหมาย กฎหมายย่อย คำสั่งที่เป็นลายลักษณ์อักษรที่ใช้บังคับที่เกี่ยวข้อง

ข. ประเมินความเพียงพอและประสิทธิผลของการควบคุมหรือมาตรการที่ใช้ในการปกป้องของสถาบัน ตามหลักการบริหารความเสี่ยง

๖.๓ ขอบเขตการตรวจสอบ (Audit Scope)

การตรวจสอบจะครอบคลุมสิ่งต่อไปนี้:

ขอบเขต (Scope)	คำอธิบาย (Description)
หัวข้อการตรวจสอบ (Audit Subject)	หัวข้อการตรวจสอบควรครอบคลุมสถาบันทั้งหมดที่กำหนดภายใต้กฎหมาย
ระยะเวลาการตรวจสอบ (Audit Period)	ระยะเวลาการตรวจสอบขั้นต่ำควรมีการตรวจสอบอย่างน้อยปีละ ๑ ครั้ง
เกณฑ์การตรวจสอบ (Audit Criteria)	เกณฑ์การตรวจสอบควรรวมถึงการปฏิบัติตามกฎหมาย กฎหมายย่อย คำสั่งที่เป็นลายลักษณ์อักษรที่เกี่ยวข้อง

๖.๔ แนวทางการตรวจสอบ (Audit Approach)

การตรวจสอบควรใช้ทั้งแนวทางการปฏิบัติตามข้อกำหนด (Compliance Approach) และตามความเสี่ยง (Risk-Based Approach)

ก. การปฏิบัติตามข้อกำหนด

ดำเนินการทดสอบการปฏิบัติตามข้อกำหนดเพื่อยืนยันความเพียงพอและประสิทธิผลของการควบคุมที่ใช้ในสถาบัน เพื่อให้สอดคล้องกับพระราชบัญญัติ กฎหมายลำดับรอง หรือคำสั่งที่เป็นลายลักษณ์อักษรที่เกี่ยวข้อง

ข. ตามความเสี่ยง

ระบุความเสี่ยงและภัยคุกคามที่สถาบันเผชิญ และตรวจสอบว่าการควบคุมที่วางไว้นั้นเหมาะสมเพื่อลดความเสี่ยงและภัยคุกคามที่ทราบหรือไม่

๖.๕ ข้อค้นพบการตรวจสอบ (Audit Finding)

ผู้ตรวจสอบควรเน้นสิ่งต่อไปนี้:

ก. ข้อค้นพบการตรวจสอบใด ๆ ที่ระบุในระหว่างการตรวจสอบ

ข. เน้นการค้นหาอย่างเป็นระบบ (Systemic Finding) ซึ่งการค้นพบจะกระจายไปทั่วทั้งสถาบันซึ่งอาจเป็นจุดอ่อนในการออกแบบการควบคุม

ค. เน้นการค้นพบที่เกิดซ้ำ เช่น การค้นพบที่เกิดขึ้นจากการตรวจสอบในอดีตที่เกิดขึ้นซ้ำในการตรวจสอบปัจจุบัน แม้ว่าจะดำเนินการแก้ไข (Corrective Action) แล้วก็ตาม

ง. เน้นแนวปฏิบัติที่ดี (Good Practices) ในด้านการกำกับดูแลและการควบคุม ซึ่งระบุไว้ในระหว่างการตรวจสอบ

เมื่อเสนอข้อค้นพบการตรวจสอบ ผู้ตรวจสอบควรระบุคุณลักษณะต่อไปนี้ของข้อค้นพบการตรวจสอบอย่างชัดเจน

องค์ประกอบ (Attributes)	คำอธิบาย (Description)
สภาพหรือเงื่อนไข (Condition)	ถ้อยแถลงที่อธิบายผลลัพธ์ของการค้นพบการตรวจสอบ
เกณฑ์ (Criteria)	มาตรฐาน/ กฎ/ เกณฑ์มาตรฐาน (เช่น กฎหมายว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ นโยบาย และแนวทางปฏิบัติที่ดีที่สุด) ที่ใช้เทียบกับสภาพหรือเงื่อนไขที่ตรวจสอบ
สาเหตุ (Cause)	สาเหตุที่แท้จริง (Root Cause) และเหตุผลที่สนับสนุนสำหรับสภาพหรือเงื่อนไขที่ตรวจสอบ
ผลกระทบ (Effect)	ผลกระทบและนัยสำคัญของสภาพหรือเงื่อนไขที่ตรวจสอบ(ทันทีในอนาคตหรือที่อาจเกิดขึ้น) ผู้ตรวจสอบควรเชื่อมโยงการค้นพบการตรวจสอบกับผลกระทบต่อบริการที่จำเป็นของสถาบัน ซึ่งฝ่ายบริหารคุ้นเคย เช่น ผลกระทบเชิงปริมาณ (เช่น ต้นทุน เวลา และการผลิต) และผลกระทบเชิงคุณภาพ (เช่น การบริการและการตัดสินใจที่ไม่เหมาะสม) สิ่งนี้ช่วยโน้มน้าวฝ่ายบริหารถึงความจำเป็นในการดำเนินการแก้ไข
คำแนะนำ (Recommendation)	แนะนำให้ดำเนินการแก้ไขสาเหตุเพื่อป้องกันการเกิดการตรวจสอบซ้ำซ้อน

๖.๖ สรุปผลการตรวจสอบ (Audit Conclusion)

ผู้ตรวจสอบควรให้ความเห็นและข้อสรุปในเรื่องต่อไปนี้

ก. ความเหมาะสมของความเห็นของฝ่ายบริหารในการตอบสนองต่อผลการตรวจสอบ

ข. ความเพียงพอและประสิทธิผลของการควบคุมที่จัดทำโดยสถาบันเพื่อจัดการกับความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ของสถาบัน และโอกาสในการปรับปรุงเพื่อรักษาความมั่นคงปลอดภัยของสถาบัน

๖.๗ รูปแบบรายงานการตรวจสอบ (Audit Report Format)

รายงานการตรวจสอบควรมีอย่างน้อยดังต่อไปนี้:

เนื้อหา	คำอธิบาย
บทสรุปผู้บริหาร (Executive Summary)	รายงานควรจัดให้มีการประเมินโดยรวมของข้อค้นพบที่บันทึกไว้ พร้อมด้วยคำอธิบายของปัญหา ความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์และผลกระทบที่อาจเกิดขึ้นกับสถาบัน คำแนะนำ ความเห็นของฝ่ายบริหาร และการประเมินความเหมาะสมของความเห็นของฝ่ายบริหารของผู้ตรวจสอบ บทสรุปสำหรับผู้บริหารควรรวมถึงข้อสรุปของผู้ตรวจสอบเกี่ยวกับความเพียงพอโดยรวมและประสิทธิผลของการควบคุมในการจัดการกับความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ต่อสถาบัน
วัตถุประสงค์ (Purpose)	รายงานควรอธิบายถึงวัตถุประสงค์ของการดำเนินการตรวจสอบความมั่นคงปลอดภัยไซเบอร์ (เช่น เพื่อปฏิบัติตามข้อผูกพันภายใต้พระราชบัญญัติความมั่นคงปลอดภัยไซเบอร์ เพื่อปฏิบัติตามคำแนะนำเฉพาะกิจที่ได้รับจาก กกม. ฯลฯ)
วัตถุประสงค์การตรวจสอบ (Audit Objective)	วัตถุประสงค์ในการตรวจสอบกำหนดไว้ในหัวข้อ ๖.๒ ของเอกสารนี้
ขอบเขตการตรวจสอบ (Audit Scope)	ขอบเขตการตรวจสอบกำหนดไว้ในส่วน ๖.๓ ของเอกสารนี้
ผู้มีส่วนได้ส่วนเสีย (Stakeholders)	ผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้องกับการตรวจสอบความมั่นคงปลอดภัยไซเบอร์และบทบาทและความรับผิดชอบควรระบุไว้อย่างชัดเจนในรายงาน
วิธีการและแนวทางการตรวจสอบ (Audit Methodology and Approach)	รายงานควรให้คำอธิบายว่าการตรวจสอบความมั่นคงปลอดภัยไซเบอร์ดำเนินการอย่างไรเพื่อให้บรรลุวัตถุประสงค์ในการตรวจสอบ โดยเฉพาะอย่างยิ่งคำอธิบายควรระบุ: ก. มีการพึ่งพางานของผู้ตรวจสอบรายอื่น (เช่น การตรวจสอบในอดีต) หรือผู้ประกอบวิชาชีพด้านการรับประกันความมั่นคงปลอดภัยไซเบอร์หรือไม่ และขอบเขตของการพึ่งพาดังกล่าว ข. ประเภทของการวิเคราะห์และเทคนิคที่ใช้ในการตรวจสอบ (เช่น การสัมภาษณ์ คำแนะนำ การตรวจสอบเอกสาร) ค. วิธีการสุ่มตัวอย่างที่นำมาใช้ (หากเลือกตัวอย่างเพื่อประเมินประสิทธิผลของการควบคุม)
การค้นพบการตรวจสอบ (Audit Finding)	การค้นพบการตรวจสอบกำหนดไว้ในส่วน ๖.๕ ของเอกสารนี้
สรุปการตรวจสอบ (Audit Conclusion)	ข้อสรุปการตรวจสอบกำหนดไว้ในส่วน ๖.๖ ของเอกสารนี้

๗. ขั้นตอนการปฏิบัติในการตรวจสอบ

๑. ผู้ตรวจสอบ ทำการวางแผน และจัดทำแผนการตรวจสอบ พร้อมทั้งจัดเตรียมทรัพยากรที่เกี่ยวข้อง

๒. ผู้ตรวจสอบและคณะทำงานของสถาบัน ร่วมการประชุมเปิดการตรวจสอบ โดยมีวัตถุประสงค์ของการประชุมเปิดการตรวจสอบ ดังนี้

- เพื่อชี้แจงวัตถุประสงค์ ขอบเขต และแผนการตรวจสอบ
- การสรุปวิธีการตรวจสอบ เกณฑ์การพิจารณา และกิจกรรมที่จะทำการตรวจสอบ
- การกำหนดผู้รับผิดชอบหรือช่องทางการสื่อสาร
- การชี้แจงรูปแบบการรายงานและการปิดตรวจสอบ
- ยืนยันแผนการตรวจสอบ

๓. ผู้ตรวจสอบดำเนินการตรวจสอบ โดยคณะทำงานทำหน้าที่ตอบข้อซักถาม และจัดเตรียมหลักฐานประกอบตามขอบเขตและข้อกำหนดประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

๔. ผู้ตรวจสอบและคณะทำงาน ร่วมการประชุมปิดการตรวจสอบ และสรุปผลการตรวจสอบเบื้องต้น โดยมีวัตถุประสงค์ของการประชุมปิดการตรวจสอบ ดังนี้

- ยืนยันข้อค้นพบการตรวจสอบจากการตรวจสอบ
- ระดับความไม่สอดคล้องของข้อตรวจพบ
- ข้อเสนอแนะในการปรับปรุง
- สรุปผลการตรวจสอบ
- กำหนดการตรวจติดตาม (ถ้ามี)

๕. ผู้ตรวจสอบจัดทำรายงานผลการตรวจสอบ และชี้แจงผลการตรวจสอบให้คณะทำงานรับทราบ

๖. คณะทำงานรับทราบผลการตรวจสอบ

๗. ผู้ตรวจสอบดำเนินการบันทึกความไม่สอดคล้อง จากข้อตรวจพบลงแบบฟอร์มรายงานความไม่สอดคล้อง (Non-Conformity Report (NCR) Form) ของสถาบัน และจัดส่งรายงานการตรวจสอบให้กับสถาบันเฉพาะผู้ที่เกี่ยวข้องตามที่สถาบันกำหนด เพื่อรักษารักษาความลับในการตรวจสอบ

๘. คณะทำงานนำเสนอผลการตรวจสอบให้ผู้บริหารระดับสูงของสถาบัน หรือคณะกรรมการตรวจสอบของสถาบัน หรือคณะกรรมการอื่น ๆ ที่ได้รับมอบหมายจากสถาบัน

๙. คณะทำงาน ดำเนินการแก้ไขความไม่สอดคล้องจากข้อตรวจพบ โดยดำเนินการตามกระบวนการปฏิบัติการแก้ไขความไม่สอดคล้อง (Corrective Action Procedure) ของสถาบัน

๑๐. ผู้ตรวจสอบดำเนินการติดตามการดำเนินการแก้ไขความไม่สอดคล้องของคณะทำงาน

๘. กระบวนการจัดทำผลกระทบทางธุรกิจ (Business Impact Analysis)

กระบวนการวิเคราะห์กิจกรรมการดำเนินงานของสถาบัน และผลกระทบที่อาจเกิดขึ้นต่อการดำเนินงานหากกิจกรรมดังกล่าวเกิดการหยุดชะงักขึ้น ในการวิเคราะห์ผลกระทบทางงาน มีขั้นตอนหลัก ๔ ขั้นตอน ดังนี้

๑. การระบุกิจกรรมการดำเนินงาน (Business Process) เพื่อส่งมอบผลิตภัณฑ์หรือบริการของสถาบัน

๒. การประเมินผลกระทบหากกิจกรรมดังกล่าวเกิดการหยุดชะงักตามระยะเวลาที่กำหนด เพื่อหากิจกรรมสำคัญ (Critical Business Process) ของสถาบัน

๓. การกำหนดกรอบระยะเวลาและเป้าหมายในการกลับมาดำเนินงานได้ของกิจกรรมสำคัญ (Critical Business Process) ของสถาบันหลังการหยุดชะงัก ซึ่งกรอบระยะเวลาและเป้าหมายที่ต้องกำหนดประกอบด้วยค่าต่าง ๆ คือ

- วัตถุประสงค์ความต่อเนื่องทางธุรกิจขั้นต่ำสุด (Minimum Business Continuity Objective หรือ MBCO) หมายถึง ระดับต่ำสุดของการบริการ และ/หรือ ผลิตภัณฑ์ที่สถาบันยอมรับโดยยังคงสามารถบรรลุวัตถุประสงค์ทางธุรกิจในระหว่างเกิดการหยุดชะงัก
- ช่วงเวลาการหยุดชะงักที่ยอมรับได้สูงสุด (Maximum Tolerable Period of Disruption หรือ MTPD) หมายถึง ช่วงเวลาที่ส่งผลกระทบต่อสถาบันทำให้ไม่สามารถยอมรับได้จากการจัดส่งสินค้า หรือให้บริการ หรือดำเนินกิจกรรม หรือระยะเวลาที่การดำเนินงานของสถาบันสามารถหยุดชะงักได้นานที่สุด
- ระยะเวลาเป้าหมายในการฟื้นคืนสภาพ (Recovery Time Objective หรือ RTO) หมายถึง ระยะเวลาภายหลังจากเกิดอุบัติการณ์ขึ้นที่ทำให้ผลิตภัณฑ์หรือบริการต้องกลับคืนสภาพเดิม กิจกรรมต้องกลับมาดำเนินการได้ และทรัพยากรต้องได้รับการฟื้นฟู
- เป้าหมายของการฟื้นคืนสภาพ (Recovery Point Objective หรือ RPO) หมายถึง จุดซึ่งสารสนเทศที่ใช้ในกิจกรรมต้องได้รับการฟื้นฟูเพื่อให้สามารถกลับมาดำเนินกิจกรรมต่อไปได้ หรือ ความถี่ในการสำรอง (backup) ข้อมูลของสถาบัน

๔. การระบุทรัพยากรที่สนับสนุนกิจกรรมสำคัญ เพื่อให้กิจกรรมสำคัญเหล่านี้สามารถกลับมาดำเนินการได้ตามกรอบระยะเวลาที่กำหนดไว้หลังจากเกิดเหตุหยุดชะงัก

๙. การวิเคราะห์ผลกระทบทางธุรกิจ สามารถจำแนกกระบวนการทำงานของสถาบันที่ต้องให้ความสำคัญและกลับมาดำเนินหรือฟื้นคืนให้ได้ภายในระยะเวลาที่กำหนดด้วยตารางต่อไปนี้

กระบวนการหลัก	ระดับผลกระทบ/ความเร่งด่วน	ระยะเวลาเป้าหมายในการฟื้นคืนสภาพ (ชั่วโมง)					
		๓ ชม.	๖ ชั่วโมง	๑๒ ชม.	๒๔ ชม.	๔๘ ชม.	๗๒ ชม.
ITD Expert anywhere	**สูง**	√					
BCG Connex	**สูง**		√				
เว็บไซต์สถาบัน	**สูง**			√			
ระบบงานสารบรรณ	**สูง**			√			
ระบบโทรศัพท์	**สูง**			√			

หมายเหตุ ระยะเวลาเป้าหมายในการฟื้นคืนสภาพ หมายถึง ระยะเวลาภายหลังจากเกิดเหตุการณ์ขึ้น ที่ทำให้ภารกิจหรือบริการต้องกลับคืนสู่สภาพเดิมกิจกรรมต้องกลับมาดำเนินการให้ได้ และทรัพยากรต้องได้รับการฟื้นฟู

สำหรับกระบวนการอื่น ๆ ที่ประเมินแล้วอาจไม่ได้รับผลกระทบในระดับสูงสุดถึงสูงมาก หรือมีความยืดหยุ่นสามารถชะลอการดำเนินงานและการให้บริการได้ โดยให้ผู้บริหารเทคโนโลยีสารสนเทศระดับสูงประเมินความจำเป็นและเหมาะสม ทั้งนี้หากมีความจำเป็นให้ปฏิบัติตามแผนการบริการและความต่อเนื่องเช่นเดียวกันกับกระบวนการหลัก

๑๐. บริการสำคัญที่สถาบันเป็นเจ้าของและใช้บริการ

ประเภททรัพยากรณ์	แหล่งข้อมูล	ระยะเวลาเป้าหมายในการฟื้นคืนสภาพ (ชั่วโมง)					
		๓ ชม.	๖ ชั่วโมง	๑๒ ชม.	๒๔ ชม.	๔๘ ชม.	๗๒ ชม.
อีเมล	**สูง**	√					
ระบบอินเตอร์เน็ต	**สูง**		√				
CCTV	**สูง**		√				

เอกสารอ้างอิง

๑. GUIDELINES FOR AUDITING CRITICAL INFORMATION INFRASTRUCTURE, Cyber Security Agency of Singapore, JANUARY ๒๐๒๐
Link: https://www.csa.gov.sg/docs/default-source/csa/documents/legislation_supplementary_references/guidelines_for_auditing_critical_information_infrastructure.pdf

๒. ISO ๑๙๐๑๑:๒๐๑๘ Guidelines for auditing management systems, ISO, July ๒๐๑๘
Link: https://www.iso.org/standard/๗๐๐๑๗.html

๓. แนวทางการตรวจสอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ Link: https://bit.ly/ncsa๔๔