แผนปฏิบัติการป้องกันและแก้ไขปัญหา ด้านความมั่นคงปลอดภัยทางไซเบอร์ของ กทท. ประจำปี 2565

ฝ่ายเทคโนโลยีสารสนเทศ

สารบัญ

1. บทนำ

การท่าเรือแห่งประเทศไทย (กทท.) เป็นรัฐวิสาหกิจสาธารณูปการในสังกัดกระทรวงคมนาคม เพื่อดำเนินกิจกรรมด้านการขนส่งสินค้าทางน้ำและมีส่วนร่วมในการพัฒนาระบบโลจิสติกส์ เพื่อการเติบโตทางเศรษฐกิจของประเทศอย่างยั่งยืน ปัจจุบันการท่าเรือแห่งประเทศไทยรับผิดชอบบริหารท่าเรือที่สำคัญ ได้แก่ ท่าเรือกรุงเทพ ท่าเรือแหลมฉบัง ท่าเรือเชียงแสน ท่าเรือเชียงของและท่าเรือระนอง มีการนำระบบเทคโนโลยีสารสนเทศและระบบการสื่อสาร เพื่อสนับสนุนการบริหารจัดการและการให้บริการอย่างต่อเนื่อง รวมถึงการเชื่อมโยงแลกเปลี่ยนข้อมูลระหว่างผู้มีส่วนได้ส่วนเสียทั้งภาครัฐและเอกชน โดยเน้นการเพิ่มประสิทธิภาพของโครงสร้างพื้นฐานการขนส่งและระบบโลจิสติกส์

การพัฒนาขีดความสามารถในการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ เป็นส่วนหนึ่งของกลยุทธ์ด้านเทคโนโลยีดิจิทัลของ กทท. เพื่อสร้างความเชื่อมั่นของผู้มีส่วนได้ส่วนเสีย และสอดคล้องเป็นไปตามข้อกำหนดที่หน่วยงานด้านโครงสร้างพื้นฐานที่สำคัญของประเทศตามรายชื่อแนบท้ายประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง รายชื่อหน่วยงานหรือองค์กร หรือส่วนงานของหน่วยงานหรือองค์กรที่ถือเป็นโครงสร้างพื้นฐานสำคัญของประเทศซึ่งต้องกระทำตามวิธีการแบบปลอดภัยในระดับเคร่งครัด พ.ศ.2559 ข้อ 3 ต้องเร่งดำเนินการปรับปรุงระดับการดูแลรักษา ยกระดับขีดความสามารถในการป้องกันภัยคุกคามทั้งภายในและภายนอก ซึ่งรวมถึงภัยคุกคามทางไซเบอร์ตามข้อกำหนดของพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.2562

ในปีงบประมาณ 2563 – 2564 กทท. จ้างที่ปรึกษาด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ เป็นผู้ดำเนินการประเมินช่องโหว่และวิเคราะห์แนวทางการดำเนินงานด้านความมั่นคงปลอดภัยไซเบอร์ (Gap Analysis) ที่เหมาะสมกับ กทท. โดยใช้กรอบแนวทางของ NIST (NIST Cybersecurity Framework) ซึ่งเป็นมาตรฐานที่องค์กรทั่วโลกรวมทั้งกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมของไทยแนะนำให้ใช้เป็นกือบมาตรฐานในการทำงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

ผลการดำเนินงานของที่ปรึกษาฯ ได้กำหนดกลยุทธ์การรักษาความมั่นคงปลอดภัยทางไซเบอร์ของ กทท. และให้คำแนะนำในการปรับปรุงการดำเนินการด้านความมั่นคงปลอดภัยทางไซเบอร์ที่สอดคล้องกับลักษณะของการปฏิบัติงาน ซึ่ง ฝทส. นำมาจัดทำแผนปฏิบัติการป้องกันและแก้ไขปัญหาด้านความมั่นคงปลอดภัยทางไซเบอร์ ประจำปี 2565

อย่างไรก็ตาม ความรับผิดชอบในด้านการรักษาความมั่นคงปลอดภัยของโครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศเป็นหน้าที่ของพนักงานทุกคนใน กทท. (คณะกรรมการ ผู้บริหาร พนักงานประจำ และลูกจ้างที่ได้รับอนุญาตให้เข้าถึงระบบ) รวมถึงผู้ให้บริการจากภายนอก

2. สภาพแวดล้อมด้านความมั่นคงปลอดภัยทางไซเบอร์

วิสัยทัศน์การเป็นท่าเรือมาตรฐานโลก หรือ Port 4.0 เน้นการนำเทคโนโลยีดิจิทัลมาใช้ยกระดับการบริหารจัดการและปรับปรุงการบริการที่มีประสิทธิภาพ สามารถลดต้นทุนการดำเนินงาน ดังนั้น สภาพแวดล้อมในระบบเทคโนโลยีดิจิทัลจึงมีลักษณะการขยายตัวเพิ่มขึ้นแบบก้าวกระโดด ซึ่งผลกระทบที่เห็นได้ชัดและหลีกเลี่ยงไม่ได้ คือ ช่องโหว่ที่เกิดจากการนำเทคโนโลยีมาใช้ และความตระหนักของพนักงาน กทท. และผู้ปฏิบัติงานที่สามารถเข้าถึงโครงสร้างพื้นฐานด้านเทคโนยีสารสนเทศของ กทท. ในการใช้งานอย่างมั่นคงปลอดภัย

นอกจากนี้ องค์กร IMO ออกมติ Resolution MSC.428(98) ในการบูรณาการการบริหารจัดการด้านความมั่นคงปลอดภัยในอุตสาหกรรมการขนส่งสินค้าทางน้ำ ที่จะผนวกภัยความเสี่ยงจากภัยคุกคามทางไซเบอร์เข้าเป็นส่วนหนึ่งของ ISM Code ส่งผลให้กิจกรรมต่างๆ ของท่าเรือ เช่น การบรรทุก-ขนถ่ายสินค้า/ตู้สินค้า สิ่งอำนวยความสะดวกต่างๆ ของท่าเรือ ฯลฯ ต้องมีการบริหารจัดการด้านความปลอดภัยที่คำนึงด้านภัยคุกคามทางไซเบอร์ร่วมด้วย

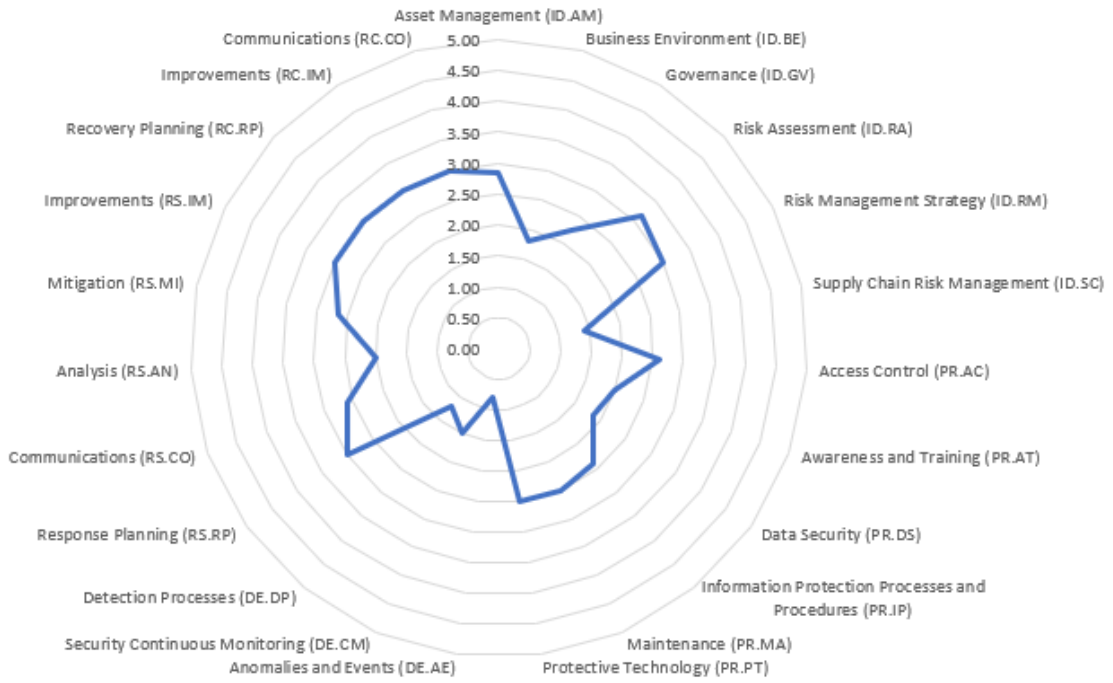
3. สถานะปัจจุบันด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์

ผลการประเมินการดำเนินงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ในฟังก์ชั่นงาน 5 ด้าน ได้แก่ ด้านการระบุความเสี่ยง (Identify) การป้องกัน (Protect) การตรวจจับ (Detect) การรับมือหรือตอบสนอง (Respond) และการกู้คืนระบบ (Recover) ตามกรอบแนวทางของ NIST Framework พบว่า กทท. มีคะแนนเฉลี่ยโดยรวมอยู่ที่ 2.21 จาก 5 ซึ่งคะแนนมาตรฐานที่ควรได้ คือ มากกว่า 3 คะแนน โดยมีคะแนนต่ำสุดในด้านการตรวจจับภัยคุกคามอยู่ที่ระดับคะแนน 1.17

ตารางที่ 1 ผลการประเมินการดำเนินงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ในฟังก์ชั่นงาน 5 ด้าน

ฟังก์ชั่นงาน	ฟังก์ชัน	หมวดหมู่	หัวข้อ	คะแนน	เฉลี่ย
ID (Identify)	การระบุความเสี่ยง	ID.AM	การบริหารจัดการทรัพย์สิน	2.83	2.41
		ID.BE	สภาพแวดล้อมทางธุรกิจ	1.80	
		ID.GV	การกำกับดูแล	2.25	
		ID.RA	การประเมินความเสี่ยง	3.17	
		ID.RM	กลยุทธ์การบริหารความเสี่ยง	3.00	
		ID.SC	การบริหารความเสี่ยงในโซ่อุปทาน	1.40	
PR (Protect)	การป้องกันความเสี่ยง	PR.AC	การบริหารจัดการข้อมูลระบุตัวตนและการควบคุมการเข้าถึง	2.60	2.31
		PR.AT	การสร้างความตระหนักรู้และการฝึกอบรม	2.00	
		PR.DS	ความมั่นคงปลอดภัยของข้อมูล	1.86	
		PR.IP	กระบวนการและขั้นตอนการคุ้มครองข้อมูล	2.42	
		PR.MA	การบำรุงรักษา	2.50	
		PR.PT	เทคโนโลยีการปกป้อง	2.50	
DE (Detect)	การตรวจจับภัยคุกคาม	DE.AE	ความผิดปกติและเหตุการณ์	0.80	1.17
		DE.CM	การเฝ้าระวังด้านความมั่นคงปลอดภัยอย่างต่อเนื่อง	1.50	
		DE.DP	กระบวนการตรวจจับ	1.20	
RS (Respond)	การตอบสนองต่อภัยคุกคาม	RS.RP	แผนการตอบสนอง	3.00	2.65
		RS.CO	การสื่อสาร	2.60	
		RS.AN	การวิเคราะห์	2.00	
		RS.MI	การบรรเทา	2.67	
		RS.IM	การปรับปรุง	3.00	
RC (Recovery)	การกู้คืน	RC.RP	การวางแผนกู้คืน	3.00	3.00
		RC.IM	การปรับปรุง	3.00	
		RC.CO	การสื่อสาร	3.00	
				คะแนนเฉลี่ยโดยรวม	2.21

ผลคะแนนโดยรวมเฉลี่ยของ กทท. แสดงให้เห็นว่า กทท. มีการดำเนินการควบคุมความปลอดภัยทางไซเบอร์ในรูปแบบทำซ้ำเดิมตามแนวปฏิบัติที่เป็นมาตรฐาน ISO27001 เฉพาะในส่วนของศูนย์ข้อมูล (Data Center) ของ ฝทส. และระบบสารสนเทศ ERP หรือ SAP แต่ยังไม่มีการกำหนดวัตถุประสงค์ที่ชัดเจนในการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศโดยรวมที่คำนึงถึงสภาพแวดล้อมทางธุรกิจของ กทท. ที่ได้รับการอนุมัติจากคณะกรรมการ และฝ่ายบริหารของ กทท. อย่างเป็นทางการ รวมทั้งไม่มีการตรวจสอบผลลัพธ์การดำเนินงานตามเป้าหมาย



รูปที่ 1 ผลประเมินการดำเนินงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของ กทท.ในปี 2563-2564 ตามกรอบ NIST Framework

4. เป้าหมาย

เพื่อให้การรักษาความมั่นคงปลอดภัยทางไซเบอร์ของ กทท. สอดคล้องตามข้อกำหนดของระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.2562 และสามารถลดช่องโหว่หรือจุดอ่อนที่พบจากการประเมินสถานภาพปัจจุบันตามรายงานของที่ปรึกษาด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ ในด้าน

(1) **<u>การป้องกันโครงสร้างพื้นฐานสำคัญทางสารสนเทศ</u>**

กทท. มีดำเนินงานด้านความปลอดภัยทางไซเบอร์ที่มีแนวปฏิบัติที่ชัดเจนตามมาตรฐานสากลและเป็นไปตามข้อกำหนดของกฎหมาย ระเบียบข้อบังคับในการรักษาความปลอดภัยทางไซเบอร์ของข้อมูลและความปลอดภัยของโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

(2) **<u>การเพิ่มขีดความสามารถในการรับมือและตอบสนองต่อเหตุการณ์ภัยคุกคาม</u>**

กทท. มีแนวทางในการจัดการกระบวนการป้องกันและรับมือจากภัยคุกคามทางไซเบอร์อย่างมีประสิทธิภาพต่อเนื่องและยั่งยืน

(3) **<u>การเพิ่มขีดความสามารถในการรักษาความปลอดภัยทางไซเบอร์</u>**

กทท. เร่งพัฒนาความรู้ทักษะและสร้างความตระหนักในการรักษาความปลอดภัยและจัดหาเทคโนโลยีเป้าหมายของการรักษาความมั่นคงปลอดภัยทางไซเบอร์

5. ระดับความสำคัญในการดำเนินงาน

การลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ ประกอบด้วยการปิดจุดอ่อนหรือช่องโหว่ที่มีนัยสำคัญ โดยเร่ง**ดำเนินการปิดจุดอ่อน/ช่องโหว่ที่มีผลคะแนนประเมินต่ำ แต่ระดับความเสี่ยงสูง ใช้เวลาน้อยในการแก้ไขหรือสามารถดำเนินงานได้ในทันที โดยใช้พนักงานของ ฝทส. และการปิดจุดอ่อน/ช่องโหว่ต้องไม่ส่งผลกระทบต่อการดำเนินงานด้านเทคโนโลยีสารสนเทศในปัจจุบันของ กทท.**

ปัจจัยที่ใช้ในการพิจารณานัยสำคัญของจุดอ่อนหรือช่องโหว่ของโครงสร้างพื้นฐานระบบเทคโนโลยีสารสนเทศ

(1) ระดับผลคะแนนประเมิน

(2) ระดับความเสี่ยงของการเกิดภัยคุกคาม

ก. ระดับความเสี่ยงที่ยอมรับได้

ข. มาตรการจัดการความเสี่ยง ประกอบด้วย การยอมรับความเสี่ยง การลด/ควบคุมความเสี่ยง การกระจายความเสี่ยง และการหลีกเลี่ยงความเสี่ยง

(3) แผนงาน/โครงการตามแผนปฏิบัติการดิจิทัลประจำปี (Action Plan)

(4) ความยากของการปรับปรุงในด้าน

ก. ระยะเวลาในการดำเนินการ

ข. ค่าใช้จ่ายหรือการลงทุนที่เกี่ยวข้อง

ค. ศักยภาพของบุคลากร (ทำได้เอง/ต้องใช้บุคคลภายนอก)

ง. ผลกระทบที่อาจเกิดขึ้นต่อการปฏิบัติงานปัจจุบัน

6. หน้าที่ความรับผิดชอบ

การดำเนินงานตามแผนปฏิบัติการการป้องกันและแก้ไขปัญหาด้านความมั่นคงปลอดภัยทางไซเบอร์ของ กทท. ประจำปี 2565 มีผู้รับผิดชอบหลักในการดำเนินงานดังนี้

(1) **กองแผนและมาตรฐานเทคโนโลยีสารสนเทศ** รับผิดชอบในการติดตาม ประเมินผลการดำเนินงาน และนำไปปรับปรุงแผนการดำเนินงานในปีถัดไป

(2) **กองปฏิบัติการด้านคอมพิวเตอร์** รับผิดชอบในการปิดจุดอ่อนหรือช่องโหว่ที่เกี่ยวข้องระบบคอมพิวเตอร์แม่ข่าย ระบบเครือข่าย เครื่องคอมพิวเตอร์และอุปกรณ์ดิจิทัลที่มีใช้งานใน กทท.

(3) กองพัฒนาระบบงาน รับผิดชอบในการปิดจุดอ่อนหรือช่องโหว่ที่เกิดจากการพัฒนาโปรแกรม การทดสอบโปรแกรม หรือการนำโปรแกรมออกใช้งาน

7. แผนปฏิบัติการประจำปี 2565

แผนการดำเนินงานในแต่ละฟังก์ชันตามกรอบแนวทาง NIST Framework จะแบ่งเป็น 3 ด้านคือ ด้านบุคลากร (People) ด้านกระบวนการ (Process) และด้านเทคโนโลยี (Technology) จำนวนทั้งสิ้น 10 แผนงาน ดังนี้

ด้านการระบุความเสี่ยง (Identity)

ลำดับ	แผนงาน	ผลลัพธ์/ตัวชีวัด
1.	จ้างผู้ตรวจประเมินภายนอกด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ **ผู้รับผิดชอบ** ผู้อำนวยการกองแผนและมาตรฐานเทคโนโลยีสารสนเทศ	**ผลลัพธ์** รายงานผลการตรวจสอบและประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ **ตัวชี้วัด** ความสำเร็จในการปฏิบัติตามข้อกำหนดของพ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.2562
2.	การทบทวนนโยบายและมาตรการการรักษาความมั่นคงปลอดภัยทางไซเบอร์ของ กทท. **ผู้รับผิดชอบ** ผู้อำนวยการกองแผนและมาตรฐานเทคโนโลยีสารสนเทศ	**ผลลัพธ์** นโยบายและมาตรการการรักษาความมั่นคงปลอดภัยทางไซเบอร์ของ กทท. (ฉบับทบทวน) **ตัวชี้วัด** ความสำเร็จในการปฏิบัติตามข้อกำหนดของพ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.2562
3.	การจัดทำรายการทรัพย์สินเทคโนโลยีสารสนเทศที่ระบุวัตถุประสงค์ในการใช้งาน การเชื่อมโยงระหว่างทรัพย์สินประเภทต่างๆ ผู้รับผิดชอบทรัพย์สิน และรายละเอียดที่จำเป็น **ผู้รับผิดชอบ** ผู้อำนวยการกองปฏิบัติการด้านคอมพิวเตอร์	**ผลลัพธ์** รายการทรัพย์สินด้านเทคโนโลยีสารสนเทศ **ตัวชี้วัด** คุณภาพของรายการทรัพย์สิน

ลำดับ	แผนงาน	ผลลัพธ์/ตัวชี้วัด
	ผู้อำนวยการกองพัฒนาระบบงาน	

ด้านการป้องกันความเสี่ยง (Protect)

ลำดับ	แผนงาน	ผลลัพธ์/ตัวชี้วัด
1.	การบริหารจัดการจุดอ่อนหรือช่องโหว่ที่ตรวจพบในระบบเทคโนโลยีสารสนเทศ **ผู้รับผิดชอบ** ผู้อำนวยการกองปฏิบัติการด้านคอมพิวเตอร์ ผู้อำนวยการกองพัฒนาระบบงาน	**ผลลัพธ์** จำนวนจุดอ่อนหรือช่องโหว่ที่มีการบริหารจัดการ **ตัวชี้วัด** ระดับคะแนนจากการประเมินความเสี่ยงตาม NIST Framework ดีขึ้น
2.	การจัดทำมาตรฐานขั้นต่ำ (Configuration Baseline) สำหรับการตั้งค่าอุปกรณ์เทคโนโลยีสารสนเทศ **ผู้รับผิดชอบ** ผู้อำนวยการกองปฏิบัติการด้านคอมพิวเตอร์	**ผลลัพธ์** คู่มือการตั้งค่าอุปกรณ์เทคโนโลยีสารสนเทศ **ตัวชี้วัด** ระดับคะแนนจากการประเมินความเสี่ยงตาม NIST Framework ดีขึ้น
3.	การอบรมสร้างความตระหนักด้านการใช้งานระบบเทคโนโลยีสารสนเทศอย่างมั่นคงปลอดภัย **ผู้รับผิดชอบ** ผู้อำนวยการกองแผนและมาตรฐานเทคโนโลยีสารสนเทศ (ร่วมกับ กองพัฒนาบุคคล)	**ผลลัพธ์** จำนวนผู้เข้ารับการอบรม **ตัวชี้วัด** อัตราส่วนของหน่วยงาน กทท. หรือผู้มีส่วนได้ส่วนเสียของกระบวนการด้านเทคโนโลยีสารสนเทศ ที่เข้ารับการอบรม

ด้านการตรวจจับภัยคุกคาม (Detect)

ลำดับ	แผนงาน	ผลลัพธ์/ตัวชี้วัด
1.	การทดสอบเจาะระบบและประเมินช่องโหว่ของระบบเทคโนโลยีสารสนเทศ (Penetration Test and Vulnerability Assessment) **ผู้รับผิดชอบ** ผู้อำนวยการกองแผนและมาตรฐานเทคโนโลยีสารสนเทศ	**ผลลัพธ์** รายงานผลการเจาะระบบและประเมินช่องโหว่ **ตัวชี้วัด** ความสำเร็จในการปฏิบัติตามข้อกำหนดของพ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.2562
2.	การทบทวนกระบวนการเฝ้าระวังเหตุการณ์ผิดปกติด้านการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ **ผู้รับผิดชอบ** ผู้อำนวยการกองปฏิบัติการด้านคอมพิวเตอร์	**ผลลัพธ์** คู่มือกระบวนการเฝ้าระวังเหตุการณ์ผิดปกติด้านการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ **ตัวชี้วัด** ระดับคะแนนจากการประเมินความเสี่ยงตาม NIST Framework ดีขึ้น

ด้านการตอบสนองต่อภัยคุกคามและการกู้คืน (Respond and Recover)

ลำดับ	แผนงาน	ผลลัพธ์/ตัวชีวัด
1.	การจัดทำแผนการรับมือภัยคุกคามทางไซเบอร์ **ผู้รับผิดชอบ** ผู้อำนวยการกองแผนและมาตรฐานเทคโนโลยีสารสนเทศ	**ผลลัพธ์** แผนการรับมือภัยคุกคามทางไซเบอร์ **ตัวชี้วัด** ความสำเร็จในการปฏิบัติตามข้อกำหนดของพ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.2562
2.	การทบทวนกระบวนการความต่อเนื่องทางธุรกิจที่รวมถึงภัยคุกคามทางไซเบอร์ **ผู้รับผิดชอบ** ผู้อำนวยการฝ่ายเทคโนโลยีสารสนเทศ	**ผลลัพธ์** แผนความต่อเนื่องทางธุรกิจด้านการให้บริการเทคโนโลยีสารสนเทศ (IT-BCP) ฉบับทบทวน **ตัวชี้วัด** ระดับคะแนนจากการประเมินความเสี่ยงตาม NIST Framework ดีขึ้น

8. การติดตามและประเมินผล

ผู้รับผิดชอบแต่ละแผนงานจัดทำแผนการดำเนินงาน (Timeline Schedule) เสนอตามสายงาน โดยกำหนดให้ต้องมีการรายงานความคืบหน้าของการดำเนินงานเป็นรายไตรมาส พร้อมนำเสนอต่อคณะอนุกรรมการกำกับดูแลการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ และคณะกรรมการบริหารจัดการความรู้ เทคโนโลยีและนวัตกรรมของ กทท.

รายการตัวชี้วัดของแผนงาน

(1) ความสำเร็จในการปฏิบัติตามข้อกำหนดของพ.ร.บ.การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.2562
ค่าเป้าหมาย ร้อยละ 80 ขึ้นไป

(2) คุณภาพของรายการทรัพย์สิน
พิจารณารายละเอียดของทรัพย์สินครบถ้วนตามมาตรฐานของการบริหารจัดการทรัพย์สินด้านเทคโนโลยีสารสนเทศ
ค่าเป้าหมาย ร้อยละ 100

(3) ระดับคะแนนจากการประเมินความเสี่ยงตาม NIST Framework
ค่าเป้าหมาย สูงขึ้นจากระดับคะแนนเดิม

(4) อัตราส่วนของหน่วยงาน กทท. หรือผู้มีส่วนได้ส่วนเสียของกระบวนการด้านเทคโนโลยีสารสนเทศ ที่เข้ารับการอบรม
ค่าเป้าหมาย ร้อยละ 80 ขึ้นไป