รายงานการตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์ (Audit Report)

ชื่อหน่วยงานที่รับการตรวจประเมิน : ใส่ชื่อหน่วยงานที่เราไปตรวจ

ประเภทของหน่วยงาน : **CII | Regulator | Gov**

วันที่ประเมิน: วันที่ 29 – 30 พฤศจิกายน 2567

ชื่อผู้ตรวจสอบ: 1. ใส่ชื่อของเรา (Lead Auditor), 2. ใส่ชื่อของเพื่อนในกลุ่ม (Auditor)

Audit Objective : เพื่อแน่ใจว่าหน่วยงาน ..... ได้ปฏิบัติตาม พรบ ไซเบอร์ **2562** และกฎหมายลำดับรอง **15** ฉบับ

Audit Scope : ชื่อหน่วยงานที่เราไปตรวจ

Audit Criteria : พรบ ไซเบอร์ **2562** และกฎหมายลำดับรอง **15** ฉบับ

ผลการประเมินก่อนหน้า: ประเมินล่าสุดเมื่อเดือนธันวาคม 2566, อ้างอิงถึงเอกสาร ประเมิน-001 : รายงานการตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์ (Audit Report) , ดูเอกสารแนบท้าย

สรุปผลการประเมินโดยภาพรวม (Executive Summary)

1. ผ่านการประเมินโดยรวม
2. คะแนนรวมที่ได้จากการประเมิน : 98 % – คิดตามสัดส่วน (จำนวนข้อที่สอดคล้อง / จำนวนข้อทั้งหมด) เช่น (96 / 98)*100 = 97.95 %
3. จำนวนตัวควบคุมทั้งหมดที่ใช้ในการตรวจประเมิน = 98 ตัวควบคุม
4. จำนวนตัวควบคุมที่ไม่ผ่านการประเมิน = 2 ตัวควบคุม

	รายการการตรวจประเมิน	จำนวนตัวควบคุม/ คะแนนเต็ม	ผลการประเมิน	% Score ที่ได้รับ
1	พรบ ไซเบอร์ 2562	12	S	12
2	นโยบายฯ ไซเบอร์แห่งชาติ (2565-2570)	13	S	13

3	**ประมวลแนวทางปฏิบัติและกรอบมาตรฐาน**	**73**	**2 NC**	**71**
3.1	**ประมวลแนวทางปฏิบัติ**			
3.1.1	แผนการตรวจสอบ		O (1)	
3.1.2	การประเมินความเสี่ยง		**S**	
3.1.3	แผนการรับมือภัยคุกคามทางไซเบอร์		**S**	
3.2	**กรอบมาตรฐาน**			
3.2.1	Govern		S	
3.2.2	Identify		S	
3.2.3	Protect		S	
3.2.4	Detect		S	
3.2.5	Respond		S	
3.2.6	Recover		O (1)	
	ผลรวม	**98**		**96**

S – Satisfied = Conformity

O – Non Satisfied = NC (Non Conformity)

N/A - Not Applicable

รายละเอียดการตรวจสอบ

ข้อดี (Strong Point) :

1. หน่วยงานดังกล่าวได้มีการจัดทำเอกสารต่างๆ โดยรวมได้เป็นอย่างดี ตรงตามที่ พรบ ไซเบอร์ ได้กำหนดไว้
2. โดยส่วนมาก บุคลากรที่ได้รับการสัมภาษณ์มีความรู้ในส่วนที่เกี่ยวข้องได้ดี

ข้อที่ควรทำการแก้ไข (Weak Point) :

1.ตัวควบคุม: Domain 3 : ประมวลและกรอบฯ | แผนการตรวจสอบ | ข้อ 17.1

วัตถุประสงค์: ต้องมีการตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์ โดยผู้ตรวจสอบด้านความมั่นคงปลอดภัยสารสนเทศทั้งโดยผู้ตรวจสอบภายใน หรือผู้ตรวจสอบอิสระภายนอก อย่างน้อยปีละ 1 ครั้ง

วิธีการประเมิน:

1. Interview : สัมภาษณ์ผู้ตรวจสอบภายใน
2. Review Document : ร้องขอดูเอกสารรายงานการตรวจสอบ

อธิบายการดำเนินการของผู้ตรวจ :

ทางผู้ตรวจสอบ ได้ดำเนินการตรวจสอบเอกสารและบันทึกการรายงานต่างๆ รวมถึงการสัมภาษณ์ผู้ที่เกี่ยวข้อง ตามหลักการณ์ ISO 19011 พบว่าไม่มีหลักฐานในการทำการตรวจสอบภายใน ภายในปี ตามที่ระบุไว้

ผลการประเมิน:

ไม่ผ่านการประเมิน (O) : พบว่า ไม่มีการทำการตรวจสอบภายใน ภายในปี ตามที่ระบุไว้

ความคิดเห็นของผู้ประเมิน: เนื่องจากการตรวจสอบภายในมีความสำคัญเป็นอย่างยิ่ง ในการปรับปรุงพัฒนาอย่างต่อเนื่องของระบบ ดังนั้น จึงถือว่าข้อนี้ ไม่สอดคล้องตามเกณฑ์ของ พรบ ไซเบอร์

คำแนะนำ: ผู้รับการตรวจสอบ กระทำตามที่กำหนดไว้

……..

ส่วนของผู้รับการตรวจ

ทำการวิเคราะห์หาสาเหตุ (Root Cause Analyst) : พบว่าทางเจ้าหน้าที่ที่เกี่ยวข้องละเลยไม่ได้จัดทำการตรวจสอบ เนื่องจากไม่มีเวลา

วิธีการแก้ไขเพื่อไม่ให้ปัญหาเกิดขึ้นอีก (Corrective Action) : ทางหน่วยงานได้มีการทบทวนแผนการตรวจสอบใหม่ทั้งหมด และมอบหมายให้ผู้บังคับบัญชาโดยตรง รับผิดชอบในการควบคุมหรือตรวจตราตามเวลาที่กำหนด โดยมี Timeline ดังต่อไปนี้

1. ทบทวนแผนการตรวจสอบใหม่ทั้งหมด | วันที่ดำเนินการคือ 15 มีนาคม 2569, ผู้รับผิดชอบ คือ นาย A

2.ตัวควบคุม: Domain 3 : ประมวลและกรอบฯ | Recover - Cybersecurity Resilience and Recovery | ข้อ 25.1.1

วัตถุประสงค์: ต้องมีการจัดทำแผนความต่อเนื่องทางธุรกิจ Business Continuity Plan : BCP) เพื่อให้หน่วยงานสามารถกลับมาดำเนินการได้อย่างต่อเนื่อง

วิธีการประเมิน:

1. Review Document : ตรวจสอบเอกสารที่ได้จัดทำในส่วนที่เป็นกรอบมาตรฐาน (Recover > Cybersecurity Resilience and Recovery)
2. Interview : สัมภาษณ์ผู้ดูแลระบบ (พรบ ไซเบอร์ 2562)
3. Observation : จากการสังเกตุการรี ไม่พบหลักฐานใดๆ ที่แสดงถึงการทำแผนความต่อเนื่องทางธุรกิจ

อธิบายการดำเนินการของผู้ตรวจ :

ทางผู้ตรวจสอบ ได้ดำเนินการตรวจสอบเอกสารและบันทึกการรายงานต่างๆ รวมถึงการสัมภาษณ์ผู้ที่เกี่ยวข้อง และการสังเกตการณ์ ตามหลักการณ์ ISO 19011 พบว่าไม่มีหลักฐานในการทำจัดทำแผนความต่อเนื่องทางธุรกิจ Business Continuity Plan : BCP) ตามที่ระบุไว้

ผลการประเมิน:

ไม่ผ่านการประเมิน (O): พบว่าไม่ได้มีการจัดทำแผนความต่อเนื่องทางธุรกิจ Business Continuity Plan

ความคิดเห็นของผู้ประเมิน: ทางหน่วยงานดังกล่าวได้มีการจัดทำเอกสารที่เป็นขั้นตอนการปฏิบัติงาน (Procedure)ได้เป็นอย่างดี ตรงตามที่ พรบ ไซเบอร์ ได้กำหนด แต่จากการตรวจสอบเอกสารโดยละเอียดแล้ว รวมถึงหาหลักฐานประกอบ พบว่า ทางหน่วยงาน ไม่ได้มีการจัดทำแผนความต่อเนื่อง ซึ่งแผนดังกล่าว มีความสำคัญ ต่อผู้บริหารหรือหน่วยควบคุมการกำกับดูแล

คำแนะนำ: ควรต้องมีการจัดทำแผนความต่อเนื่อง รวมถึงมีการฝึกซ้อม BCP ด้วย

……..

<u>ส่วนของผู้รับการตรวจ</u>

ทำการวิเคราะห์หาสาเหตุ (Root Cause Analyst) : พบว่าทางเจ้าหน้าที่ที่เกี่ยวข้องไม่ได้จัดทำแผนความต่อเนื่อง ในปีดังกล่าว เนื่องจากเป็นเจ้าหน้าที่ใหม่ ซึ่งไม่ทราบว่าจะต้องมีการจัดทำ

วิธีการแก้ไขเพื่อไม่ให้ปัญหาเกิดขึ้นอีก (Corrective Action) : ทางหน่วยงานได้มีการทบทวนแผนการอบรม พรบ ไซเบอร์ ให้กับพนักงานที่เกี่ยวข้องให้รับทราบ โดยมี Timeline ดังต่อไปนี้

1.ทำการอบรมเจ้าหน้าที่ที่เกี่ยวข้อง ทั้งหมด พร้อม Post test หลังการอบรม โดยเน้นในส่วนของการจัดทำแผนความต่อเนื่องทางธุรกิจ | วันที่ดำเนินการคือ 15 มีนาคม 2569, ผู้รับผิดชอบคือ นาย A
