

**แนวทางการตรวจราชการกระทรวงสาธารณสุข ประจำปีงบประมาณ พ.ศ. 2569**  
**(Inspection Guideline)**

- ยุทธศาสตร์      ☐ PP & P Excellence                      ☐ Service Excellence  
                         ☐ People Excellence                      ☒ Governance Excellence  
                         ☐ Health-Related Economy Excellence

**ข้อตัวชีวิต :** ร้อยละของหน่วยงานที่ผ่านเกณฑ์มาตรฐานความมั่นคงปลอดภัยไซเบอร์ระดับสูง

ตัวชี้วัดย่อย : (ถ้ามี) -

**คำนิยาม :**

๑. หน่วยงาน หมายถึง โรงพยาบาลสังกัดสำนักงานปลัดกระทรวงสาธารณสุข ได้แก่ โรงพยาบาลศูนย์/ทั่วไป/ชุมชนที่เปิดให้บริการแล้ว และ สำนักงานสาธารณสุขจังหวัด และ สำนักงานเขตสุขภาพ ที่ ๑-๑๒

๒. มาตรฐานความมั่นคงปลอดภัยไซเบอร์ หมายถึง เกณฑ์การประเมินระดับการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Technical Assessment Matrix Plus: CTAM+)

๓. ผ่านเกณฑ์มาตรฐานความมั่นคงปลอดภัยไซเบอร์ระดับสูง หมายถึง ผลการประเมินผ่านเกณฑ์มาตรฐานความมั่นคงปลอดภัยไซเบอร์ (CTAM+) ตามที่กำหนดครบทุกข้อ ดังนี้

- ๑) Backup
- ๒) Antivirus Software
- ๓) Access Control (Public และ Private)
- ๔) Privileged Access Management (PAM)
- ๕) Business Continuity Plan (BCP) และ Disaster Recovery Plan (DRP)
- ๖) OS Patching
- ๗) Multi-Factor Authentication (๒FA)
- ๘) Web Application Firewall (WAF)
- ๙) Log Management
- ๑๐) Security Information & Event Management (SIEM)
- ๑๑) Vulnerability Assessment (VA Scan)
- ๑๒) สำรวจและปิดระบบงานที่ไม่ได้ใช้งานเพื่อป้องกันการเข้าถึงข้อมูล
- ๑๓) อัปเดตซอฟต์แวร์หรือแพตช์ ด้านความปลอดภัย
- ๑๔) Network Segmentation
- ๑๕) ใช้ซอฟต์แวร์กักกันภัยคุกคาม
- ๑๖) Penetration Testing
- ๑๗) มีนโยบายด้านการรักษาความมั่นคงปลอดภัยไซเบอร์และการคุ้มครองข้อมูลส่วนบุคคล รวมถึง การส่งเสริมให้เกิดการพัฒนาบุคลากรด้านดังกล่าว

**ตารางที่ 1 ค่าเป้าหมาย : ร้อยละของหน่วยงานที่ผ่านเกณฑ์มาตรฐานความมั่นคงปลอดภัยไซเบอร์ระดับสูง**

ปีงบประมาณ 67	ปีงบประมาณ 68	ปีงบประมาณ 69	ปีงบประมาณ 70
-	ร้อยละ 100 ของ หน่วยงานผ่านเกณฑ์ฯ ระดับสูง (ตุลาคม 2567 – กันยายน 2568)	ร้อยละ 100 ของ หน่วยงานผ่านเกณฑ์ฯ ระดับสูง (ตุลาคม 2568 – กันยายน 2569)	ร้อยละ 100 ของ หน่วยงานผ่านเกณฑ์ฯ ระดับสูง (ตุลาคม 2569 – กันยายน 2569)

**วัตถุประสงค์ :** 1. เพื่อให้หน่วยงานมีความพร้อมรับมือเหตุการณ์ฉุกเฉินทางคอมพิวเตอร์ ด้วยระบบป้องกัน  
ตรวจจับ วิเคราะห์ และโต้ตอบต่อภัยคุกคามทางไซเบอร์

2. เพื่อลดความรุนแรงของผลกระทบกรณีหน่วยงานถูกคุกคามทางไซเบอร์ที่ส่งผลต่อการ  
ให้บริการประชาชน และอาจส่งผลต่อการคุ้มครองข้อมูลส่วนบุคคล

3. เพื่อลดปัจจัยเสี่ยงของโอกาสเกิดช่องโหว่ภัยคุกคามทางไซเบอร์

4. เพื่อให้ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ของหน่วยงานโครงสร้าง  
พื้นฐานสำคัญทางสารสนเทศด้านสาธารณสุข (HealthCERT) ได้รับการประสานงานอย่างรวดเร็ว และโต้ตอบ  
ภัยคุกคามทางไซเบอร์ได้ทันเวลา

**ประชากรกลุ่มเป้าหมาย :** -

**หน่วยงานที่เกี่ยวข้องกับตัวชี้วัดนี้ :** โรงพยาบาลสังกัดสำนักงานปลัดกระทรวงสาธารณสุข ได้แก่ โรงพยาบาล  
ศูนย์/ทั่วไป/ชุมชนที่เปิดให้บริการแล้ว และ สำนักงานสาธารณสุขจังหวัด และ สำนักงานเขตสุขภาพ ที่ 1-12

**รูปแบบการจัดเก็บข้อมูล :** (เลือกได้ 1 รูปแบบ)

☐ HDC

☐ ฐานข้อมูลกรม/ กอง/ หน่วยงาน

☐ ข้อมูลจากการตรวจราชการ

☒ อื่น ระบุ หน่วยงานส่งมาให้ ศทส.ส.สธ. ตามช่องทางที่กำหนด

ดังนี้

1) หน่วยงานดำเนินการให้ระบบเครือข่ายคอมพิวเตอร์และสารสนเทศตามเกณฑ์มาตรฐานความมั่นคง  
ปลอดภัยไซเบอร์ และประเมินตนเอง หรือให้ผู้เชี่ยวชาญที่เป็นผู้ตรวจประเมิน (หากเป็นเอกชนต้องมีใบรับรอง  
มาตรฐาน)

2) หน่วยงานส่งผลยืนยันผลการประเมินพร้อมหลักฐานให้คณะทำงานควบคุมคุณภาพการตรวจประเมิน  
ความมั่นคงปลอดภัยไซเบอร์ระดับจังหวัดและระดับเขตสุขภาพตามลำดับ (ชื่อและคุณสมบัติของคณะกรรมการ/  
คณะทำงาน ทั้งระดับจังหวัดและระดับเขต แล้วแต่เขตสุขภาพจะพิจารณาอาจใช้ชื่ออื่นๆ ได้ โดยกรรมการระดับ  
จังหวัดและเขตสุขภาพอย่างน้อย 1 ท่าน ควรผ่านการอบรม MOPH CISO หรือ MOPH DPO ที่จัดโดยศูนย์เทคโนโลยี

สารสนเทศและการสื่อสาร (ศทส.สป.สธ.) มาก่อน ) และคณะกรรมการ/คณะทำงานส่งผลการประเมินมายัง ศทส.สป.สธ. ที่อีเมล cyberaudit@moph.go.th ทุกวันพฤหัสบดี หรือ ช่องทางอื่น ๆ ตามที่ ศทส.สป.สธ. แจ้งเพิ่มเติม

3) ศทส.สป.สธ. จะยืนยันผลการประเมินของหน่วยงานทุกศุภกร์โดยแสดงผลที่ <https://ict.moph.go.th/th/extension/1763>

4) ศทส.สป.สธ. ได้จัดทำคู่มือการตรวจประเมินระดับการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Technical Assessment Matrix Plus: CTAM+) ประจำปี พ.ศ. 2569 ตาม QR Code และ ลิงก์ด้านล่าง



<https://moph.link/Zj43wyXWJ>

ลิงก์ดาวน์โหลดคู่มือ

ระยะเวลาการเก็บรวบรวมและตัดข้อมูล :

- ข้อมูลการตรวจราชการระดับจังหวัด ใช้ข้อมูล ณ ปัจจุบันก่อนลงพื้นที่ตรวจราชการ
- สรุปตรวจราชการรอบที่ 1 (ตุลาคม 2568 - มีนาคม 2569) : ใช้ข้อมูล ณ วันที่ 31 มีนาคม 2569
- สรุปตรวจราชการรอบที่ 2 (ตุลาคม 2568 - กรกฎาคม 2569) : ใช้ข้อมูล ณ วันที่ 31 กรกฎาคม 2569

สูตรคำนวณตัวชี้วัดเชิงปริมาณ :  $(A/B) \times 100$

รายการข้อมูล 1 A = หน่วยงานผ่านเกณฑ์มาตรฐานความมั่นคงปลอดภัยไซเบอร์ (CTAM+) ตามที่กำหนดครบทุกข้อ

รายการข้อมูล 2 B = 990 (หน่วยงานตามที่กำหนดไว้ในคำนิยาม)

ตัวชี้วัดนี้สามารถวัดเชิงคุณภาพได้แบบใด โปรดเลือก (สามารถเลือกได้มากกว่า 1 ข้อ)

- ☐ 1) เชิงคุณภาพ (ด้านผลลัพธ์)
- |   |   |
|---|---|
| <input type="radio"/> 1. การให้บริการสุขภาพ             | <input type="radio"/> 2. กำลังคนที่ให้บริการ                    |
| <input type="radio"/> 3. ระบบงานและการจัดการข้อมูล      | <input type="radio"/> 4. การเข้าถึงยาช่วยชีวิตและอุปกรณ์ฉุกเฉิน |
| <input type="radio"/> 5. การเงินการคลังด้านการให้บริการ | <input type="radio"/> 6.ภาวะผู้นำและธรรมาภิบาลระบบสุขภาพ        |

หมายเหตุ : ขอให้จัดทำเกณฑ์การประเมินผลเชิงคุณภาพ ด้านผลลัพธ์ (Outcome) ตามกรอบแนวคิด

6 Building Blocks ขององค์การอนามัยโลก (WHO) ตามตารางที่ 4

☒ 2) เชิงคุณภาพ (ด้านผลกระทบ)

- |   |  |
|---|--|
| <input type="radio"/> 1. การเข้าถึงบริการ | <input type="radio"/> 2.ความครอบคลุมการรักษา |
|---|--|

- 3. การรักษาตามมาตรฐานคุณภาพบริการ      ○ 4. ประสิทธิภาพของการรักษา
- ◎ 5. ความปลอดภัยของผู้ป่วยและข้อมูล

หมายเหตุ : ขอให้จัดทำเกณฑ์การประเมินผลเชิงคุณภาพ ด้านผลกระทบ (Impact) ตามองค์การอนามัยโลก (WHO) ตามตารางที่ 6

### ตามตารางที่ 8

**มาตรการหลัก/กระบวนการที่สำคัญ** (เฉพาะมาตรการหลัก (3-5 ข้อ) ไม่ควรนำกิจกรรมมาใส่)

1) หน่วยงานส่งบุคลากรเข้าร่วมอบรม หลักสูตรต่างๆ ที่ ศทส.สป. จัดขึ้น หรือหน่วยงานที่น่าเชื่อถือ และเสริมแรงจูงใจเพื่อรักษาคนไข้อีที่มีทักษะด้านไซเบอร์ให้อยู่กับหน่วยงาน รวมถึง HealthCERT โดย ศทส.สป.สร เป็น ศูนย์กลางประสานให้ความช่วยเหลือหน่วยงานด้านไซเบอร์ ผ่านช่องทางไลน์ @health-cirt

2) มีคณะทำงานดำเนินงานความมั่นคงปลอดภัยไซเบอร์ในระดับจังหวัด ทำหน้าที่ให้ความช่วยเหลือหน่วยงานในพื้นที่ ตรวจสอบ และการรับรองได้เทียบเท่าเอกชน โดยมีคณะทำงานระดับเขตสุขภาพ เป็นเครือข่าย กำกับดูแลหน่วยงานในพื้นที่ รวมถึง ดำเนินการกำกับดูแลจากส่วนกลางโดยมีการสุ่มตรวจ (Audit) หน่วยงาน

3) ภายในจังหวัด หรือ ภายในเขตสุขภาพ สามารถดูแลกันเองได้ด้วยตัวเอง ลดการพึ่งพาหน่วยงานเอกชน โดยใช้ซอฟต์แวร์แบบ Opensource ในการดำเนินงาน รวมถึงช่วยกันต่อรองในส่วนที่จำเป็นต้องใช้งบประมาณ เช่น Firewall , Server , ค่า MA หรือ ค่าใช้จ่ายอื่นๆ เป็นต้น

### ตารางที่ 2 เกณฑ์การประเมินผลเชิงปริมาณ :

วิธีการประเมินผล : เปรียบเทียบผลการดำเนินงานกับค่าเป้าหมาย

ผลการดำเนินงานเปรียบเทียบกับค่าเป้าหมาย	
รอบ 6 เดือน	รอบ 10 เดือน
1. โรงพยาบาลระดับ M1, S และ A ผ่านเกณฑ์มาตรฐานความมั่นคงปลอดภัยไซเบอร์ระดับสูง ไม่น้อยกว่าร้อยละ 80  2. สำนักงานสาธารณสุขจังหวัด และสำนักงานเขตสุขภาพ ผ่านเกณฑ์มาตรฐานความมั่นคงปลอดภัยไซเบอร์ระดับสูง ไม่น้อยกว่าร้อยละ 80	โรงพยาบาลชุมชน ผ่านเกณฑ์มาตรฐานความมั่นคงปลอดภัยไซเบอร์ระดับสูง ไม่น้อยกว่าร้อยละ 80

เอกสาร/หลักฐานสนับสนุน : -

ตารางที่ 3 เกณฑ์การให้คะแนนเชิงปริมาณในแต่ละระดับ (ข้อมูล ณ วันที่ 31 กรกฎาคม 2569) ดังนี้

[illegible]

คะแนน	เกณฑ์ผลการดำเนินงาน
3	1. โรงพยาบาลระดับ M1, S และ A ผ่านเกณฑ์มาตรฐานความมั่นคงปลอดภัยไซเบอร์ระดับสูง ไม่น้อยกว่าร้อยละ 45 2. สำนักงานสาธารณสุขจังหวัด และสำนักงานเขตสุขภาพ ผ่านเกณฑ์มาตรฐานความมั่นคงปลอดภัยไซเบอร์ระดับสูง ไม่น้อยกว่าร้อยละ 45
2	1. โรงพยาบาลระดับ M1, S และ A ผ่านเกณฑ์มาตรฐานความมั่นคงปลอดภัยไซเบอร์ระดับสูง ไม่น้อยกว่าร้อยละ 40 2. สำนักงานสาธารณสุขจังหวัด และสำนักงานเขตสุขภาพ ผ่านเกณฑ์มาตรฐานความมั่นคงปลอดภัยไซเบอร์ระดับสูง ไม่น้อยกว่าร้อยละ 40
1	1. โรงพยาบาลระดับ M1, S และ A ผ่านเกณฑ์มาตรฐานความมั่นคงปลอดภัยไซเบอร์ระดับสูง ไม่น้อยกว่าร้อยละ 35 2. สำนักงานสาธารณสุขจังหวัด และสำนักงานเขตสุขภาพ ผ่านเกณฑ์มาตรฐานความมั่นคงปลอดภัยไซเบอร์ระดับสูง ไม่น้อยกว่าร้อยละ 35

หมายเหตุ : เกณฑ์การให้คะแนนเชิงปริมาณหน่วยงานที่รับผิดชอบตัวชี้วัดเป็นผู้ออกแบบเกณฑ์ผลการดำเนินงานแต่ละระดับ โดยระบุเกณฑ์คะแนน 1-10 เปรียบเทียบผลการดำเนินงานกับค่าเป้าหมาย

ตารางที่ 4 เกณฑ์การประเมินผลเชิงคุณภาพ ด้านผลลัพธ์ (Outcome) ตามกรอบแนวคิด 6 Building Blocks ขององค์การอนามัยโลก (WHO)

เกณฑ์การให้คะแนนเชิงคุณภาพ ด้านผลลัพธ์

Building Block	หัวข้อการประเมิน (นำมาจากมาตรการหลัก)	เกณฑ์คุณภาพ ระดับ 1 0 – 40 คะแนน	เกณฑ์คุณภาพ ระดับ 2 41 – 55 คะแนน	เกณฑ์คุณภาพ ระดับ 3 56 – 70 คะแนน	เกณฑ์คุณภาพ ระดับ 4 71- 85 คะแนน	เกณฑ์คุณภาพ ระดับ 5 86 – 100 คะแนน	เอกสารหรือหลักฐานที่ใช้ประเมิน
<input type="checkbox"/> การให้บริการสุขภาพ							
<input type="checkbox"/> กำลังคนที่ให้บริการ							
<input type="checkbox"/> ระบบงานและการจัดการข้อมูล							
<input type="checkbox"/> การเข้าถึงยาและเทคโนโลยี							
<input type="checkbox"/> การเงิน การคลังด้านการให้บริการ							
<input type="checkbox"/> ภาวะผู้นำและธรรมาภิบาลระบบสุขภาพ							

### หลักการให้คะแนนเชิงคุณภาพ

#### 1) คะแนนรวม 100 คะแนนต่อหนึ่งตัวชี้วัด

- หากตัวชี้วัดเชื่อมโยงกับหลาย Building Block (เช่น 6 ด้าน) ให้ใช้คะแนนเต็ม 100 คะแนนในการประเมินรวมทุกด้านนั้น

#### 2) คะแนนเต็มของแต่ละ Building Block = 100 คะแนน

- หากในแต่ละด้านมีหลายหัวข้อการประเมิน ให้รวมคะแนนทุกหัวข้อในส่วนนั้นให้เท่ากับ 100 คะแนน

#### 3) คำนวณคะแนนเฉลี่ยรวมของทุกด้านที่เกี่ยวข้อง

- เช่น  $(68 + 40 + 60 + 85 + 45 + 90) \div 6 = 64.7$  คะแนน
- เช่น  $(72 + 65 + 58) \div 3 = 65$

### ตารางที่ 5 การแปลผลระดับคุณภาพและระดับคะแนนการพัฒนา (5 ระดับ)

ระดับคุณภาพ	ช่วงคะแนน	การแปลผลเชิงคุณภาพ	ระดับการพัฒนา
ระดับ 5 = ดีเยี่ยม (Excellent)	86 – 100	ระบบบริการสุขภาพดีเยี่ยม เป็นแบบอย่างที่ดี ปรับปรุงต่อเนื่องอย่างเป็นระบบ	ยั่งยืนและเป็นต้นแบบ
ระดับ 4 = ดี (Good)	71 – 85	ระบบบริการสุขภาพมีความมั่นคง ครบคลุม และมีการพัฒนาต่อเนื่อง	พัฒนาอย่างมั่นคง
ระดับ 3 = พอใช้ (Fair)	56 – 70	ระบบบริการสุขภาพดำเนินการได้ตามมาตรฐานพื้นฐาน มีบางส่วนต้องปรับปรุง	กำลังพัฒนา
ระดับ 2 = ต้องพัฒนา (Developing)	41 – 55	ระบบบริการสุขภาพไม่มั่นคง ต้องเร่งปรับปรุงในหลายองค์ประกอบ	ต้องการการสนับสนุน
ระดับ 1 = ต้องเร่งแก้ไข (Critical)	ต่ำกว่าหรือเท่ากับ 40	ระบบบริการสุขภาพมีจุดอ่อนสำคัญ ต้องดำเนินการแก้ไขเร่งด่วน	ต้องการฟื้นฟูระบบ



ตารางที่ 6 เกณฑ์การประเมินผล ด้านผลกระทบ/ ผลสำเร็จเชิงยุทธศาสตร์ ตามองค์การอนามัยโลก (WHO)

ผลกระทบ	หัวข้อการประเมิน	เกณฑ์คุณภาพ ระดับ 1 0 – 40 คะแนน	เกณฑ์คุณภาพ ระดับ 2 41 – 55 คะแนน	เกณฑ์คุณภาพ ระดับ 3 56 – 70 คะแนน	เกณฑ์คุณภาพ ระดับ 4 71- 85 คะแนน	เกณฑ์คุณภาพ ระดับ 5 86 – 100 คะแนน	เอกสารหรือ หลักฐาน ที่ใช้ประเมิน
<input type="checkbox"/> การเข้าถึง บริการ							
<input type="checkbox"/> ความ ครอบคลุม การรักษา							
<input type="checkbox"/> การรักษา ตามมาตรฐาน คุณภาพ บริการ							
<input type="checkbox"/> ประสิทธิภาพของ การรักษา							

<p><input checked="" type="checkbox"/> ความปลอดภัยของผู้ป่วยและข้อมูล</p>	<p>ภายในจังหวัด หรือ ภายในเขตสุขภาพ สามารถดูแลตนเองได้ด้วยตัวเอง ลดการพึ่งพาหน่วยงานเอกชน ใช้ซอฟต์แวร์แบบ Opensource ในการดำเนินงาน รวมถึงช่วยกันต่อรองในส่วนที่จำเป็นต้องใช้งบประมาณ เช่น Firewall , Server ค่า MA หรือ ค่าใช้จ่ายอื่นๆ เป็นต้น</p>	<p>1. หน่วยบริการภายในเขตสุขภาพ เกิดเหตุการณ์การโจมตีทางไซเบอร์ของระบบ HIS หรือ Website องค์กร จนทำให้ระบบไม่สามารถให้บริการได้ โดยใช้เวลากู้คืน 73 - 96 ชั่วโมง (20 คะแนน)</p> <p>2. มีเหตุการณ์รั่วไหลของฐานข้อมูลของโรงพยาบาล ( HIS Data Breach) หรือมีเหตุการณ์ข้อมูลส่วนบุคคลรั่วไหลที่เกี่ยวข้องกับระบบสารสนเทศ และ สคส.วินิจฉัยโทษ</p>	<p>1. หน่วยบริการภายในเขตสุขภาพ เกิดเหตุการณ์การโจมตีทางไซเบอร์ของระบบ HIS หรือ Website องค์กร จนทำให้ระบบไม่สามารถให้บริการได้ โดยใช้เวลากู้คืน 49 – 72 ชั่วโมง (27.5 คะแนน)</p> <p>2. มีเหตุการณ์รั่วไหลของฐานข้อมูลของโรงพยาบาล ( HIS Data Breach) หรือมีเหตุการณ์ข้อมูลส่วนบุคคลรั่วไหลที่เกี่ยวข้องกับระบบสารสนเทศ และ สคส.วินิจฉัยโทษ</p>	<p>1. หน่วยบริการภายในเขตสุขภาพ เกิดเหตุการณ์การโจมตีทางไซเบอร์ของระบบ HIS หรือ Website องค์กร จนทำให้ระบบไม่สามารถให้บริการได้ โดยใช้เวลากู้คืน 25 – 48 ชั่วโมง (35 คะแนน)</p> <p>2. มีเหตุการณ์รั่วไหลของฐานข้อมูลของโรงพยาบาล ( HIS Data Breach) หรือมีเหตุการณ์ข้อมูลส่วนบุคคลรั่วไหลที่เกี่ยวข้องกับระบบสารสนเทศ และ สคส.วินิจฉัยโทษ</p>	<p>1. หน่วยบริการภายในเขตสุขภาพ เกิดเหตุการณ์การโจมตีทางไซเบอร์ของระบบ HIS หรือ Website องค์กร จนทำให้ระบบไม่สามารถให้บริการได้ โดยใช้เวลากู้คืนไม่เกิน 24 ชั่วโมง (42.5 คะแนน)</p> <p>2. มีเหตุการณ์รั่วไหลของฐานข้อมูลของโรงพยาบาล ( HIS Data Breach) หรือไม่มีเหตุการณ์ข้อมูลส่วนบุคคลรั่วไหลที่เกี่ยวข้องกับระบบสารสนเทศ ที่ สคส.วินิจฉัยลงโทษทางปกครอง (50 คะแนน)</p>	<p>1. หน่วยบริการภายในเขตสุขภาพ <u>ไม่เกิด</u> เหตุการณ์การโจมตีทางไซเบอร์ของระบบ HIS หรือ Website องค์กร จนทำให้ระบบไม่สามารถให้บริการได้ (50 คะแนน)</p> <p>2. <u>ไม่มี</u>เหตุการณ์รั่วไหลของฐานข้อมูลของโรงพยาบาล ( HIS Data Breach) หรือ<u>ไม่มี</u>เหตุการณ์ข้อมูลส่วนบุคคลรั่วไหลที่เกี่ยวข้องกับระบบสารสนเทศ ที่ สคส.วินิจฉัยลงโทษทางปกครอง (50 คะแนน)</p>	<p>1. หลักฐาน Log จาก Firewall, SEIM, XDR/EDR, หรืออื่นๆ ที่เกี่ยวข้อง</p> <p>2. คำตัดสินของ สคส.</p>
---	--	---	---	---	--	---	---

		ทางปกครอง ระดับ ร้ายแรง ปรับ 3 ล้านบาท – 1 ล้าน บาท (20 คะแนน)	ทางปกครองระดับ ร้ายแรง ปรับ ไม่ เกิน 1 ล้านบาท (27.5 คะแนน)	ทางปกครองระดับ ไม่ร้ายแรง และให้ แก้ไขหรือปรับปรุง กระบวนการหรือ เอกสารที่เกี่ยวข้อง (35 คะแนน)	ทางปกครองระดับ ไม่ร้ายแรง และให้ อบรมเจ้าหน้าที่ เพิ่มเติม (42.5 คะแนน)		
--	--	---	--	--	---	--	--

เกณฑ์การประเมินผลกระทบ/ผลสำเร็จเชิงยุทธศาสตร์

หลักการให้คะแนน

1) คะแนนรวม 100 คะแนนต่อหนึ่งตัวชี้วัด

ตัวอย่าง เขตสุขภาพที่ 1 มีหน่วยงานภายในเขตสุขภาพ 5 หน่วยงาน มี 1 หน่วยงาน ได้คะแนน 85 คะแนน ที่เหลืออีก 4 หน่วยงาน ได้ 100 คะแนน

การคำนวณคะแนนเฉลี่ย =  $(85 + (100 \times 4)) / 5 = 97$  คะแนน

2) พิจารณาจากผลลัพธ์เชิงประจักษ์ (Evidence of Result)

- ใช้ข้อมูลเชิงประจักษ์ เช่น สถิติ ผลสำรวจ ข้อมูลคุณภาพบริการ และผลการเปลี่ยนแปลงต่อประชาชน
- เน้นการสะท้อนผลลัพธ์ (Results-based) มากกว่ากระบวนการดำเนินงาน

3) พิจารณาจากผลลัพธ์เชิงประจักษ์ (Evidence of Result)

- ใช้ข้อมูลเชิงประจักษ์ เช่น สถิติ ผลสำรวจ ข้อมูลคุณภาพบริการ และผลการเปลี่ยนแปลงต่อประชาชน
- มีแนวโน้มการพัฒนาอย่างต่อเนื่องหรือไม่

- ส่งผลกระทบเชิงบวกต่อระบบสุขภาพและประชาชนหรือไม่

**ตารางที่ 7** การแปลผลคะแนนเพื่อสะท้อนระดับคุณภาพและระดับคะแนนของผลกระทบ

ระดับคุณภาพ	ช่วงคะแนน	ความหมายโดยสรุป
ระดับ 5 = ดีเยี่ยม (Excellent)	86 – 100	ผลลัพธ์โดดเด่น สร้างผลกระทบเชิงบวกต่อประชาชนและระบบบริการสาธารณสุขอย่างยั่งยืน
ระดับ 4 = ดี (Good)	71 – 85	ผลลัพธ์บรรลุเป้าหมายชัดเจน สร้างผลกระทบเชิงบวกต่อประชาชน แต่ควรพัฒนาระบบบริการสุขภาพอย่างต่อเนื่อง
ระดับ 3 = พอใช้ (Fair)	56 – 70	ผลลัพธ์อยู่ในระดับมาตรฐาน มีระบบบริการสุขภาพบางส่วนต้องปรับปรุง
ระดับ 2 = ต้องพัฒนา (Developing)	41 – 55	ผลลัพธ์ยังไม่บรรลุเป้าหมาย ต้องปรับกลยุทธ์หรือระบบสนับสนุน
ระดับ 1 = ต้องเร่งแก้ไข (Critical)	ต่ำกว่าหรือเท่ากับ 40	ผลลัพธ์ไม่เป็นไปตามเป้าหมาย หรือเกิดผลกระทบในทางลบต่อประชาชนและระบบบริการสุขภาพ ต้องแก้ไขเร่งด่วน

หลักการคิดสัดส่วนผลสัมฤทธิ์ของการประเมินตัวชี้วัดการตรวจราชการ คิดอัตราส่วน 70 : 30

- สัดส่วน 70 คือ ผลสัมฤทธิ์เชิงปริมาณ
- สัดส่วน 30 คือ ผลสัมฤทธิ์เชิงคุณภาพ (Outcome หรือ Impact)

ตารางที่ 10 การคำนวณคะแนนผลการประเมินตัวชี้วัดการตรวจราชการ คิดอัตราส่วน 70 : 30

ระดับคะแนนเชิงปริมาณ (70%)	ระดับคะแนนเชิงคุณภาพ ด้านผลกระทบ (15%)
ระดับคะแนนที่ได้ $\times 0.7 = \text{Score}$	$(\text{คะแนนที่ได้} \div 10) \times 0.3$ $= \text{Score}$
Score เชิงปริมาณ + Score เชิงคุณภาพ = (คะแนนเต็ม 10)	

หมายเหตุ : 1. หากตัวชี้วัดประเมินเชิงคุณภาพด้านผลลัพธ์ ให้ใส่คะแนนตามช่องที่กำหนดและคำนวณ Score  
 2. หากตัวชี้วัดประเมินเชิงคุณภาพด้านผลกระทบ ให้ใส่คะแนนตามช่องที่กำหนดและคำนวณ Score  
 3. หากตัวชี้วัดประเมินได้เพียงด้านเดียว(ด้านผลลัพธ์หรือด้านผลกระทบ) ให้คิดสัดส่วนเชิงคุณภาพด้านเดียวเท่ากับ 30% เช่น  $(\text{คะแนนที่ได้} \div 10) \times 0.3 = \text{Score}$

หน่วยงานที่รับผิดชอบหลัก : สำนักงานปลัดกระทรวงสาธารณสุข ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

หน่วยงานที่รับผิดชอบร่วม : กรม..... สำนัก/กอง.....

ตารางที่ 11 ผู้ประสานงานตัวชี้วัด

ชื่อ-สกุล	ตำแหน่ง/หน่วยงาน	หมายเลขโทรศัพท์/e-mail address	ประเด็นที่รับผิดชอบ
แพทย์หญิงสินสุชา บุญ ตันตราภรณ์	รองผู้อำนวยการศูนย์ เทคโนโลยีสารสนเทศ และการสื่อสาร สำนัก/กอง ศูนย์เทคโนโลยี สารสนเทศและการ สื่อสาร	Tel. 09 8905 0442 e-mail : sinsucha@moph.go.th	Cybersecurity

นางสาวสุรชาติพิทย์ คล้าย เหล็ง	นักวิชาการคอมพิวเตอร์ ชำนาญการ สำนัก/กอง ศูนย์เทคโนโลยี สารสนเทศและการ สื่อสาร	Tel. 0872098757 e-mail : khlaileng@moph.mail.go.th	Cybersecurity
-----------------------------------	---	--	---------------

**ตารางที่ 12 ผู้รับผิดชอบการรายงานผลการดำเนินงาน**

ชื่อ-สกุล	ตำแหน่ง/หน่วยงาน	หมายเลขโทรศัพท์/e-mail address	ประเด็นที่ รับผิดชอบ
นางสาวสุรชาติพิทย์ คล้ายเหล็ง	ตำแหน่ง นักวิชาการ คอมพิวเตอร์ชำนาญ การ สำนัก/กอง ศูนย์เทคโนโลยี สารสนเทศและการ สื่อสาร	Tel. 0872098757 e-mail : khlaileng@moph.mail.go.th	Cybersecurity
นางสาวณัฐธิดา จันทร์ทอง	ตำแหน่ง นักวิชาการ คอมพิวเตอร์ปฏิบัติการ สำนัก/กอง ศูนย์เทคโนโลยี สารสนเทศและการ สื่อสาร	Tel. 0959485657 e-mail : natnicha-chan@moph.go.th	Cybersecurity

**หมายเหตุ** สามารถเพิ่มเติมรายละเอียดอื่น ๆ ที่สำคัญและจำเป็นได้ตามดุลยพินิจของ คกก.กำหนดประเด็นแต่ละ  
ประเด็น