

## เอกสารรับฟังความคิดเห็น

เลขที่ อตท. 37/2567

เรื่อง

ร่างประกาศสำนักงานคณะกรรมการกำกับหลักทรัพย์  
และตลาดหลักทรัพย์ ที่ สธ. /2567 เรื่อง ข้อกำหนดในรายละเอียด  
เกี่ยวกับการจัดให้มีระบบเทคโนโลยีสารสนเทศ (ฉบับที่ )

เผยแพร่เมื่อวันที่ 12 กันยายน 2567

สำนักงานได้จัดทำเอกสารฉบับนี้ขึ้นเพื่อสำรวจความคิดเห็นจากผู้เกี่ยวข้อง  
ท่านสามารถ download เอกสารเผยแพร่ฉบับนี้ได้จาก  
เว็บไซต์ของสำนักงาน ([www.sec.or.th](http://www.sec.or.th)) และระบบกลางทางกฎหมาย ([law.go.th](http://law.go.th))

วันสุดท้ายของการแสดงความคิดเห็น วันที่ 15 ตุลาคม 2567

ท่านสามารถส่งความเห็นหรือข้อเสนอแนะหรือติดต่อสอบถามข้อมูลเพิ่มเติมได้จาก  
เจ้าหน้าที่ของสำนักงาน ดังนี้

- ฝ่ายกำกับและตรวจสอบความเสี่ยงด้านเทคโนโลยีสารสนเทศ อีเมล [cyberteam@sec.or.th](mailto:cyberteam@sec.or.th)
- นายวรนาถ หมั่นวิจิตร โทรศัพท์ 0-2033-9541 อีเมล [wornat@sec.or.th](mailto:wornat@sec.or.th)
- นายกฤษฎา ตูลารักษ์ โทรศัพท์ 0-2033-9653 อีเมล [kritsadat@sec.or.th](mailto:kritsadat@sec.or.th)
- นางสาวณัชชา จารุณนศ โทรศัพท์ 0-2033-9985 อีเมล [natchac@sec.or.th](mailto:natchac@sec.or.th)

สำนักงานขอขอบคุณทุกท่านที่เข้าร่วมแสดงความคิดเห็น  
และให้ข้อเสนอแนะมา ณ โอกาสนี้

สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์  
เลขที่ 333/3 ถนนวิภาวดีรังสิต แขวงจอมพล เขตจตุจักร กรุงเทพฯ 10900  
โทรศัพท์ 1207 หรือ 0-2033-9999 โทรสาร: 0-2033-9660 email: [info@sec.or.th](mailto:info@sec.or.th)

## 1. ที่มา

สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ (“สำนักงาน ก.ล.ต.”) เห็นชอบการออกประกาศสำนักงานคณะกรรมการ ก.ล.ต. ที่ สธ. 38/2565 เรื่อง ข้อกำหนดในรายละเอียดเกี่ยวกับการจัดให้มีระบบเทคโนโลยีสารสนเทศ ลงวันที่ 28 กันยายน พ.ศ. 2565 (“หลักเกณฑ์ฯ”) เพื่อให้ผู้ประกอบการจัดให้มี (1) การกำกับดูแลและบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ (2) การรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ และ (3) การตรวจสอบด้านเทคโนโลยีสารสนเทศ (“ตรวจสอบด้าน IT”) เพื่อให้มั่นใจว่า ระบบเทคโนโลยีสารสนเทศที่ผู้ประกอบการนำมาใช้นั้นมีความมั่นคงปลอดภัยและสามารถให้บริการได้อย่างต่อเนื่อง สอดคล้องกับระดับความเสี่ยงที่ยอมรับได้ รวมทั้งรักษาไว้ซึ่งความน่าเชื่อถือของภาคตลาดทุน ทั้งนี้ หลักเกณฑ์ฯ ได้กำหนดให้ผู้ประกอบการถือปฏิบัติในการจัดให้มีมาตรการควบคุมความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ ตามระดับผลการประเมินระดับความเสี่ยงเกี่ยวกับระบบเทคโนโลยีสารสนเทศซึ่งส่งผลต่อการดำเนินธุรกิจของผู้ประกอบการตามแบบ RLA (Risk Level Assessment) โดยแบ่งผู้ประกอบการออกเป็น 4 กลุ่ม ได้แก่ ผู้ประกอบการที่มีความเสี่ยง (1) ระดับสูง (2) ระดับปานกลาง (3) ระดับต่ำ และ (4) ผู้ประกอบการขนาดเล็ก

ภายหลังจากที่หลักเกณฑ์ฯ มีผลบังคับใช้ตั้งแต่วันที่ 1 กรกฎาคม 2566 เป็นต้นมา สำนักงาน ก.ล.ต. ได้รับข้อเสนอแนะจากผู้ประกอบการ เพื่อประโยชน์ต่อการพิจารณาปรับปรุงหลักเกณฑ์ฯ ให้ผู้ประกอบการสามารถปฏิบัติได้สอดคล้องตามเจตนารมณ์ของข้อกำหนดได้อย่างเหมาะสม และมีประสิทธิผลมากยิ่งขึ้น

ตามที่สำนักงาน ก.ล.ต. ได้เปิดรับฟังความคิดเห็นจากผู้ที่เกี่ยวข้องต่อหลักการปรับปรุงหลักเกณฑ์ฯ ตามเอกสารรับฟังความคิดเห็นเลขที่ อตท. 75/2567 ระหว่างวันที่ 14 มิถุนายน ถึง 15 กรกฎาคม 2566 นั้น สำนักงาน ก.ล.ต. ได้นำความคิดเห็นและข้อเสนอแนะพิจารณาในรายละเอียดและนำไปใช้ประกอบการยกร่างประกาศ (ฉบับแก้ไขเพิ่มเติม) และแนวปฏิบัติที่เกี่ยวข้องแล้ว ดังนี้

1. ร่างประกาศสำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ ที่ สธ. /2567 เรื่อง ข้อกำหนดในรายละเอียดเกี่ยวกับการจัดให้มีระบบเทคโนโลยีสารสนเทศ (ฉบับที่ ) (เอกสารแนบ 1) พร้อมกับภาคผนวกแนบท้ายประกาศ ดังนี้

(1) ภาคผนวก 1 คำศัพท์ (เอกสารแนบ 1.1)

- (2) ภาคผนวก 2 การกำกับดูแลและบริหารจัดการด้านเทคโนโลยีสารสนเทศ (เอกสารแนบ 1.2)
- (3) ภาคผนวก 3 การรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (เอกสารแนบ 1.3)
- (4) ภาคผนวก 4 การตรวจสอบด้านเทคโนโลยีสารสนเทศ (เอกสารแนบ 1.4)

2. ร่างประกาศแนวปฏิบัติ ที่ นป. /2567 เรื่อง แนวปฏิบัติในการจัดให้มีระบบเทคโนโลยีสารสนเทศ (เอกสารแนบ 2) พร้อมกับภาคผนวกแนบท้ายประกาศแนวปฏิบัติ ดังนี้

- (1) ภาคผนวกแนบท้ายประกาศแนวปฏิบัติ ที่ นป. 7/2567 (เอกสารแนบ 2.1) ทั้งนี้ เพื่อให้ประกาศมีความสอดคล้องเหมาะสมกับผู้ประกอบธุรกิจยิ่งขึ้น สำนักงาน ก.ล.ต. จึงเห็นควรจัดให้มีการรับฟังความคิดเห็นร่างประกาศหลักเกณฑ์ฯ และเอกสารที่เกี่ยวข้องเพื่อขอรับฟังความเห็นจากผู้ประกอบธุรกิจและบุคคลทั่วไป

## 2. เป้าหมายที่ต้องการบรรลุ (Intended Outcome)

เพื่อให้ผู้ประกอบธุรกิจสามารถบริหารจัดการความเสี่ยงในการใช้เทคโนโลยีสารสนเทศได้อย่างมีประสิทธิภาพ และมีความพร้อมในการรับมือต่อภัยคุกคามทางไซเบอร์ที่เพิ่มขึ้นอย่างต่อเนื่อง พร้อมทั้งสร้างความเชื่อมั่นให้กับผู้ลงทุนในการใช้บริการและผลิตภัณฑ์ของภาคตลาดทุน ซึ่งมีระบบเทคโนโลยีสารสนเทศเป็นส่วนสำคัญ โดยไม่ก่อให้เกิดภาระกับผู้ประกอบธุรกิจเกินสมควร

## 3. สรุปสาระสำคัญของร่างประกาศ

สำนักงาน ก.ล.ต. ได้ปรับปรุงหลักเกณฑ์การจัดให้มีระบบเทคโนโลยีสารสนเทศ จึงขอเปิดรับฟังความคิดเห็นต่อร่างประกาศ โดยสรุปสาระสำคัญได้ดังนี้

### 3.1 การปรับปรุงขอบเขตการบังคับใช้ประกาศฯ สำหรับผู้ประกอบธุรกิจ การเป็นที่ปรึกษาการลงทุน และการเป็นที่ปรึกษาสัญญาซื้อขายล่วงหน้า

ปรับปรุงจาก “การเป็นที่ปรึกษาการลงทุนที่มีการวางแผนการลงทุนให้แก่ลูกค้า หรือใช้โปรแกรมสำเร็จรูปประกอบการให้บริการแก่ลูกค้า” และ “การเป็นที่ปรึกษาสัญญาซื้อขายล่วงหน้าที่มีการวางแผนการลงทุนให้แก่ลูกค้า หรือใช้โปรแกรมสำเร็จรูปประกอบการให้บริการแก่ลูกค้า” เป็น “การเป็นที่ปรึกษาการลงทุนที่มีการใช้เทคโนโลยีเพื่อการติดต่อหรือให้บริการแก่

ลูกค้า” และ “การเป็นที่ปรึกษาสัญญาซื้อขายล่วงหน้าที่มีการใช้เทคโนโลยีเพื่อการติดต่อหรือให้บริการแก่ลูกค้า” รวมทั้งเพิ่มคำจำกัดความ “เทคโนโลยีเพื่อการติดต่อหรือให้บริการแก่ลูกค้า” หมายความว่า “เทคโนโลยีหรือคอมพิวเตอร์ที่มีการใช้งานเพื่อดำเนินการอย่างหนึ่งอย่างใด ดังนี้ (1) เพื่อการติดต่อลูกค้า (2) เพื่อการจัดทำหรือนำส่งข้อมูลบริการหรือผลิตภัณฑ์ให้แก่ลูกค้า (3) เพื่อการประมวลผล วิเคราะห์ ออกผลลัพธ์หรือคำแนะนำ เพื่อให้ลูกค้าใช้ประกอบการตัดสินใจลงทุน”

### 3.2 การปรับปรุงข้อกำหนดสำหรับผู้ประกอบธุรกิจที่เป็นสาขาของธนาคารพาณิชย์ต่างประเทศ

ปรับปรุงข้อกำหนด ดังนี้

ข้อกำหนดประกาศที่ สธ. 38/2565	ข้อกำหนดของร่างประกาศ (ฉบับแก้ไขเพิ่มเติม)
<p><b>ภาคผนวก 2 ข้อ 1.6</b></p> <p>1.6 การติดตาม ตรวจสอบ และรายงานผลการปฏิบัติงานเพื่อให้เป็นไปตามนโยบายในข้อ 1.3 ต่อคณะกรรมการของผู้ประกอบธุรกิจ โดยมีการรายงานอย่างน้อยปีละ 1 ครั้ง และในกรณีที่มีเหตุการณ์ หรือการเปลี่ยนแปลงใด ๆ ซึ่งอาจส่งผลกระทบต่อการทำงานเพื่อให้เป็นไปตามนโยบายดังกล่าว ต้องมีการรายงานให้คณะกรรมการของผู้ประกอบธุรกิจทราบโดยไม่ชักช้าด้วย</p>	<p><b>ปรับปรุงข้อกำหนด ดังนี้</b></p> <p>1.6 การติดตาม ตรวจสอบ และรายงานผลการปฏิบัติงานเพื่อให้เป็นไปตามนโยบายในข้อ 1.3 ต่อคณะกรรมการของผู้ประกอบธุรกิจ <b><u>หรือคณะกรรมการที่ได้รับมอบหมายจากคณะกรรมการของผู้ประกอบธุรกิจ เฉพาะกรณีเป็นสาขาของธนาคารพาณิชย์ต่างประเทศ</u></b> โดยมีการรายงานอย่างน้อยปีละ 1 ครั้ง และในกรณีที่มีเหตุการณ์หรือการเปลี่ยนแปลงใด ๆ ซึ่งอาจส่งผลกระทบต่อการทำงานเพื่อให้เป็นไปตามนโยบายดังกล่าว ต้องมีการรายงานให้คณะกรรมการของผู้ประกอบธุรกิจ <b><u>หรือคณะกรรมการที่ได้รับมอบหมายจากคณะกรรมการของผู้ประกอบธุรกิจ เฉพาะกรณีเป็นสาขาของธนาคารพาณิชย์ต่างประเทศ</u></b> ทราบโดยไม่ชักช้าด้วย</p>
<p><b>ภาคผนวก 4 ข้อ 5</b></p> <p>5.1 เสนอรายงานผลการตรวจสอบตามข้อ 3. และแผนการปรับปรุงแก้ไขข้อบกพร่องต่อคณะกรรมการของผู้ประกอบธุรกิจหรือคณะกรรมการ</p>	<p><b>ปรับปรุงข้อกำหนด ดังนี้</b></p> <p>5.1 เสนอรายงานผลการตรวจสอบตามข้อ 3. และแผนการปรับปรุงแก้ไขข้อบกพร่องต่อคณะกรรมการของผู้ประกอบธุรกิจ <b><u>หรือคณะกรรมการตรวจสอบของผู้ประกอบธุรกิจ หรือคณะกรรมการที่ได้รับมอบหมายจากคณะกรรมการของผู้ประกอบธุรกิจ</u></b></p>

ข้อกำหนดประกาศที่ สร. 38/2565	ข้อกำหนดของร่างประกาศ (ฉบับแก้ไขเพิ่มเติม)
<p>ตรวจสอบของผู้ประกอบธุรกิจโดย ไม่ชักช้า</p> <p>5.2 รายงานผลการตรวจสอบและ แผนการปรับปรุงแก้ไขข้อบกพร่อง ที่ผ่านการพิจารณาจากคณะกรรมการ ของผู้ประกอบธุรกิจหรือคณะกรรมการ ตรวจสอบของผู้ประกอบธุรกิจตาม ข้อ 5.1 ต่อสำนักงานตามรูปแบบ และวิธีการที่กำหนดไว้บนเว็บไซต์ ของสำนักงาน ...</p>	<p><b>เฉพาะกรณีเป็นสาขาของธนาคารพาณิชย์ต่างประเทศ</b> โดยไม่ชักช้า</p> <p>5.2 รายงานผลการตรวจสอบและแผนการปรับปรุง แก้ไขข้อบกพร่องที่ผ่านการพิจารณาจากคณะกรรมการ ของผู้ประกอบธุรกิจหรือคณะกรรมการตรวจสอบของ ผู้ประกอบธุรกิจ <b>หรือคณะกรรมการที่ได้รับมอบหมาย จากคณะกรรมการของผู้ประกอบธุรกิจเฉพาะกรณี เป็นสาขาของธนาคารพาณิชย์ต่างประเทศ</b> ตามข้อ 5.1 ต่อสำนักงานตามรูปแบบและวิธีการที่กำหนดไว้บน เว็บไซต์ของสำนักงาน ...</p>

### 3.3 การตรวจสอบด้านเทคโนโลยีสารสนเทศ

ยกเลิกข้อกำหนดให้ผู้ประกอบธุรกิจขนาดเล็ก และผู้ประกอบธุรกิจที่มีความเสี่ยงระดับต่ำ ดำเนินการตรวจสอบด้าน IT อย่างน้อยปีละ 1 ครั้ง และให้ดำเนินการ ดังนี้

(1) กรณีผู้ประกอบธุรกิจขนาดเล็ก ต้องจัดให้มีการตรวจสอบด้าน IT ที่ครอบคลุมหลักเกณฑ์ทั้งหมดที่บังคับใช้กับผู้ประกอบธุรกิจขนาดเล็ก แบบเต็มรูปแบบ (full scope) อย่างน้อยทุก 3 ปี ตามรอบปีที่สำนักงานกำหนด หรือเมื่อเกิดเหตุการณ์ด้านความมั่นคงปลอดภัยของระบบ IT อย่างมีนัยสำคัญ<sup>1</sup> (ตามรูปที่ 1)

(2) กรณีผู้ประกอบธุรกิจที่มีความเสี่ยงระดับต่ำ ต้องจัดให้มีการตรวจสอบด้าน IT ที่ครอบคลุมหลักเกณฑ์ทั้งหมดที่บังคับใช้กับผู้ประกอบธุรกิจที่มีความเสี่ยงระดับต่ำ แบบเต็มรูปแบบ (full scope) อย่างน้อยทุก 3 ปี ตามรอบปีที่สำนักงานกำหนด หรือเมื่อเกิดเหตุการณ์ด้านความมั่นคงปลอดภัยของระบบ IT อย่างมีนัยสำคัญ (ตามรูปที่ 1)

กรณีที่มีเหตุจำเป็นทำให้ผู้ประกอบธุรกิจขนาดเล็ก หรือผู้ประกอบธุรกิจที่มีความเสี่ยงระดับต่ำ ไม่สามารถดำเนินการตรวจสอบด้าน IT แบบเต็มรูปแบบ (full scope)

<sup>1</sup> เหตุการณ์ด้านความมั่นคงปลอดภัยของระบบ IT อย่างมีนัยสำคัญ ครอบคลุมถึง เหตุการณ์ที่เกี่ยวข้องกับภัยคุกคามทางไซเบอร์ (cyber incident) และเหตุการณ์ที่ไม่เกี่ยวข้องกับภัยคุกคามทางไซเบอร์ (non-cyber incident) ซึ่งส่งผลกระทบต่อทรัพย์สิน หรือข้อมูลของลูกค้าในวงกว้าง

ภายในปีที่เกิดเหตุการณ์ด้านความมั่นคงปลอดภัยของระบบ IT อย่างมีนัยสำคัญ ผู้ประกอบธุรกิจต้องดำเนินการ ดังต่อไปนี้

(1) รายงานเหตุจำเป็นที่ทำให้ไม่สามารถดำเนินการตรวจสอบด้าน IT ได้ภายในปีที่เกิดเหตุการณ์ดังกล่าว และแผนการตรวจสอบด้าน IT ต่อคณะกรรมการของผู้ประกอบธุรกิจ หรือคณะกรรมการที่ได้รับมอบหมายจากคณะกรรมการของผู้ประกอบธุรกิจ เฉพาะกรณีเป็นสาขาของธนาคารพาณิชย์ต่างประเทศ รวมทั้งรายงานเหตุจำเป็นดังกล่าว ต่อสำนักงาน และ

(2) ดำเนินการตรวจสอบด้าน IT แบบเต็มรูปแบบ (full scope) ในปีถัดไป ทั้งนี้ การดำเนินการในข้อ (1) และ (2) ต้องอยู่ภายในกรอบระยะเวลา 4 เดือน นับแต่วันที่ทราบเหตุการณ์ด้านความมั่นคงปลอดภัยของระบบ IT อย่างมีนัยสำคัญ เพื่อให้ผู้ประกอบธุรกิจมีการตอบสนองต่อเหตุการณ์ด้านความมั่นคงปลอดภัยของระบบ IT อย่างมีนัยสำคัญ เช่น การตรวจสอบสาเหตุ (investigate) การแก้ไข และการปรับปรุง ข้อบกพร่องได้ภายในระยะเวลาที่เหมาะสม เป็นต้น

**ส. 38/2565**

	2568	2569	2570	2571	2572	2573	2574
ความเสี่ยงระดับปานกลาง / สูง	Full	Full	Full	Full	Full	Full	Full
ขนาดเล็ก / ความเสี่ยงระดับต่ำ	Partial	Full	Partial	Full	Partial	Full	Partial

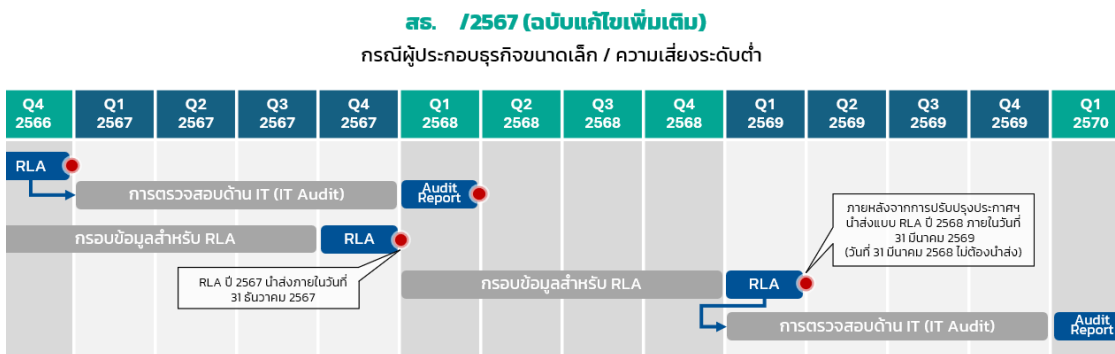
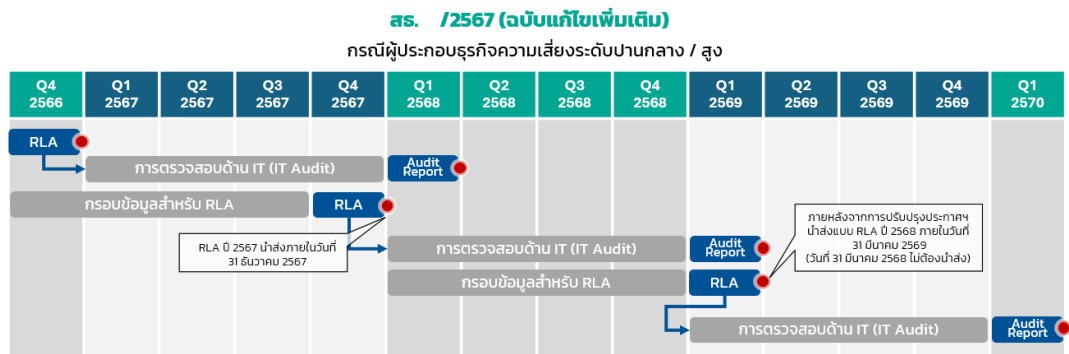
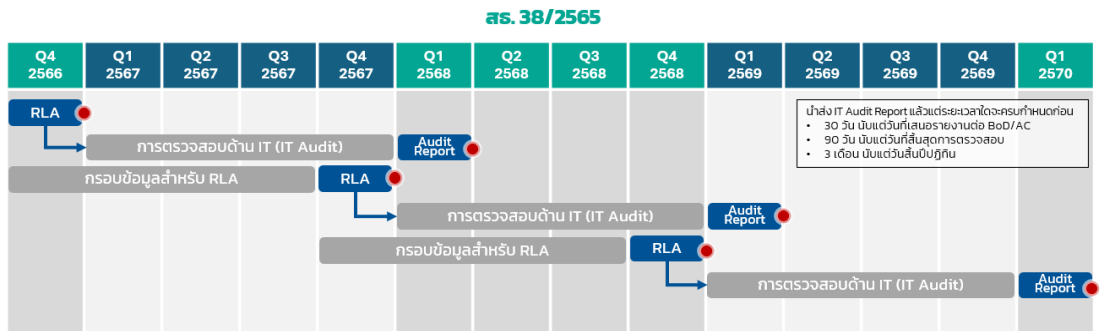
**ส. /2567 (ฉบับแก้ไขเพิ่มเติม)**

	2568	2569	2570	2571	2572	2573	2574
ความเสี่ยงระดับปานกลาง / สูง	Full	Full	Full	Full	Full	Full	Full
ขนาดเล็ก / ความเสี่ยงระดับต่ำ		Full			Full		
ขนาดเล็ก / ความเสี่ยงระดับต่ำ (กรณีเกิดเหตุการณ์ด้านความมั่นคงปลอดภัยของระบบ IT อย่างมีนัยสำคัญ)		Full	⚠ Full เนื่องจากเกิด Major IT Security Incident		Full		⚠ Full เนื่องจากเกิด Major IT Security Incident

รูปที่ 1 การตรวจสอบด้าน IT ของผู้ประกอบธุรกิจแต่ละระดับความเสี่ยง ตามผลการประเมินแบบ Risk Level Assessment (“RLA”)

### 3.4 การจัดส่งรายงานผลการตรวจสอบด้านเทคโนโลยีสารสนเทศ

กำหนดให้ผู้ประกอบธุรกิจรายงานผลการตรวจสอบด้าน IT และแผนการปรับปรุงแก้ไขข้อบกพร่องที่ผ่านการพิจารณาจากคณะกรรมการของผู้ประกอบธุรกิจ<sup>2</sup> หรือคณะกรรมการตรวจสอบของผู้ประกอบธุรกิจต่อสำนักงาน ก.ล.ต. ตามรูปแบบและวิธีการที่กำหนดไว้บนเว็บไซต์ของสำนักงานภายใน 3 เดือน นับแต่วันสิ้นปีปฏิทินของปีที่เริ่มตรวจสอบ (ตามรูปที่ 2)



รูปที่ 2 การจัดส่งแบบ RLA และรายงานผลการตรวจสอบด้าน IT

<sup>2</sup> คณะกรรมการที่ได้รับมอบหมายจากคณะกรรมการของผู้ประกอบธุรกิจเฉพาะกรณีเป็นสาขาของธนาคารพาณิชย์ต่างประเทศ (ภายหลังมีการปรับปรุงประกาศ ที่ สธ. 38/2565)

### 3.5 การจัดส่งแบบ RLA

ปรับปรุงรอบการจัดส่งแบบ RLA โดยกำหนดให้จัดส่งผลการประเมินดังกล่าว ต่อสำนักงาน ก.ล.ต. ภายในไตรมาสที่ 1 ของทุกปีปฏิทิน โดยข้อมูลที่ใช้ประเมินได้มาจากข้อมูล ระหว่างวันที่ 1 มกราคม ถึง 31 ธันวาคม ของปีก่อนหน้าปีที่ต้องนำเสนอ รายละเอียดตามรูปที่ 2 ข้างต้น

### 3.6 การรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ สำหรับผู้ประกอบธุรกิจขนาดเล็ก

#### (1) การทดสอบการเจาะระบบ (penetration test)

กำหนดให้ผู้ประกอบธุรกิจขนาดเล็ก จัดให้มีการทดสอบการเจาะระบบ (penetration test) บนระบบงาน (application system) และระบบเครือข่ายที่มีการเชื่อมต่อกับเครือข่ายสาธารณะ (internet facing) อย่างน้อยทุก 3 ปี และทุกครั้งที่มีการเปลี่ยนแปลงระบบดังกล่าวอย่างมีนัยสำคัญ<sup>3</sup>

#### (2) การควบคุมการเข้าถึงข้อมูลและระบบ IT (access control)

กำหนดให้ผู้ประกอบธุรกิจขนาดเล็ก จัดให้มีการควบคุมการเข้าถึงข้อมูลและระบบ IT (access control) เทียบเท่ากับผู้ประกอบธุรกิจระดับความเสี่ยงอื่น ๆ โดยไม่จำกัดเฉพาะการควบคุมเพียงแค่อุปกรณ์ privileged user (privileged user management)

#### (3) การบริหารจัดการเหตุการณ์ผิดปกติด้าน IT

กำหนดให้ผู้ประกอบธุรกิจขนาดเล็ก จัดให้มีการดำเนินการดังนี้ กรณีที่เกิดเหตุการณ์ผิดปกติด้าน IT

ก. รายงานเหตุการณ์ผิดปกติด้าน IT ต่อผู้มีหน้าที่รับผิดชอบเหตุการณ์และสำนักงานโดยไม่ชักช้าเมื่อทราบเหตุการณ์ดังกล่าว

ข. วิเคราะห์สาเหตุที่แท้จริง (root cause) ของเหตุการณ์ผิดปกติด้าน IT เพื่อกำหนดแนวทางการแก้ไขและป้องกันไม่ให้เกิดเหตุการณ์ซ้ำในอนาคต

<sup>3</sup> ผู้ประกอบธุรกิจสามารถพิจารณา “ความมีนัยสำคัญ” โดยคำนึงถึงกรอบหลักการของความเสียหาย (inherent risk) และผลกระทบต่อ การให้บริการหรือดำเนินธุรกิจ ในวงกว้าง (enterprise-wide impact) โดยยังไม่นำมาตรการควบคุม (controls) มาประกอบการพิจารณาความเสี่ยงนั้น ทั้งนี้ ตัวอย่างของการเปลี่ยนแปลงระบบที่มีนัยสำคัญ เช่น (1) การเปลี่ยนโครงสร้างพื้นฐานจาก on-premise เป็นระบบคลาวด์ (2) การนำระบบงานใหม่มาใช้งาน และ (3) การเปลี่ยนแปลงระบบที่มีผลต่อความมั่นคงปลอดภัย เป็นต้น



ค. บันทึกข้อมูลที่เกี่ยวข้องกับการบริหารจัดการเหตุการณ์ผิดปกติด้าน IT และจัดเก็บข้อมูลดังกล่าวเป็นระยะเวลาไม่น้อยกว่า 2 ปี นับแต่วันที่เกิดเหตุการณ์นั้น โดยต้องจัดเก็บไว้ในลักษณะที่พร้อมให้สำนักงานสามารถเรียกดูและตรวจสอบได้โดยไม่ชักช้า

### 3.7 แนวปฏิบัติข้อกำหนดการจัดทำและนำส่งบันทึกการทำธุรกรรมเพิ่มเติม (additional transaction log) เมื่อสำนักงานร้องขอ

ร่างประกาศยังคงไว้ซึ่งรายละเอียดของ transaction log ตามข้อกำหนดของประกาศที่ สร. 38/2565 อย่างไรก็ตาม เพื่อให้ผู้ปฏิบัติหน้าที่ market surveillance ได้รับข้อมูลที่จำเป็นต่อการปฏิบัติหน้าที่ในการพิจารณาการกระทำอันไม่เป็นธรรมเกี่ยวกับการซื้อขายหลักทรัพย์ได้อย่างเหมาะสม ร่างประกาศได้เพิ่มเติมข้อกำหนดในแนวปฏิบัติ ให้ผู้ประกอบการธุรกิจดำเนินการจัดทำและนำส่งข้อมูลเพิ่มเติม (additional transaction log) ต่อสำนักงาน ก.ล.ต. ตามรูปแบบและวิธีการที่กำหนด โดยไม่ชักช้า เมื่อมีการร้องขอ ดังนี้

แนวปฏิบัติที่ นป. 7/2565	ร่างแนวปฏิบัติ (ฉบับแก้ไขเพิ่มเติม)
<p>(5) บันทึกการทำธุรกรรม (transaction log) ควรมีระยะเวลาจัดเก็บขั้นต่ำ 1 ปี โดยในกรณีที่เป็นระบบ IT เพื่อการซื้อขายหลักทรัพย์ (trading system) ให้บันทึก บัญชีผู้ใช้งาน / ข้อมูลรายละเอียดซื้อขายหลักทรัพย์ (securities symbol) / หมายเลขบริษัทสมาชิก (broker No. 4 หลัก : xxxx) / เลขที่คำสั่งซื้อขายหลักทรัพย์ (SET order ID) / เลขที่บัญชีซื้อขายหลักทรัพย์ (account ID) / วันและเวลาในการส่งคำสั่งซื้อขายหลักทรัพย์ (yyyy/mm/dd – hh:mm:ss:sss) / หมายเลข public และ local IP address ต้นทาง (source) / หมายเลข IP address ปลายทาง (destination) / ที่อยู่ของเว็บไซต์ปลายทาง (full URL) / terminal type (ถ้ามี) เช่น mobile, PC, iPad, iPhone เป็นต้น</p>	<p><u>เพิ่มเติมแนวปฏิบัติ ดังนี้</u></p> <p>(5) บันทึกการทำธุรกรรม (transaction log) ควรมีระยะเวลาจัดเก็บขั้นต่ำ 1 ปี โดยในกรณีที่เป็นระบบ IT เพื่อการซื้อขายหลักทรัพย์ (trading system) ให้บันทึก บัญชีผู้ใช้งาน / ข้อมูลรายละเอียดซื้อขายหลักทรัพย์ (securities symbol) / หมายเลขบริษัทสมาชิก (broker No. 4 หลัก : xxxx) / เลขที่คำสั่งซื้อขายหลักทรัพย์ (SET order ID) / เลขที่บัญชีซื้อขายหลักทรัพย์ (account ID) / วันและเวลาในการส่งคำสั่งซื้อขายหลักทรัพย์ (yyyy/mm/dd – hh:mm:ss:sss) / หมายเลข public และ local IP address ต้นทาง (source) / หมายเลข IP address ปลายทาง (destination) / ที่อยู่ของเว็บไซต์ปลายทาง (full URL) / terminal type (ถ้ามี) เช่น mobile, PC, iPad, iPhone เป็นต้น</p>

	<p>ทั้งนี้ ให้ผู้ประกอบการจัดทำและนำส่งข้อมูลเพิ่มเติมต่อสำนักงาน ตามรูปแบบและวิธีการที่สำนักงานกำหนดโดยไม่ชักช้าเมื่อสำนักงานร้องขอ โดยข้อมูลบันทึกการทำธุรกรรมเพิ่มเติม (additional transaction log) ที่ผู้ประกอบการควรพร้อมจัดทำและนำส่งต่อสำนักงานเมื่อสำนักงานร้องขอ ควรมีรายละเอียดขั้นต่ำ ดังนี้</p> <ul style="list-style-type: none"> <li>(ก) บัญชีผู้ใช้งาน (user ID)</li> <li>(ข) เลขบัตรประจำตัวประชาชนหรือเลขทะเบียนนิติบุคคลของลูกค้า</li> <li>(ค) ชื่อ-นามสกุลของลูกค้า</li> <li>(ง) วันที่จับคู่คำสั่งซื้อขายได้ (matched date : yyyy/mm/dd)</li> <li>(จ) กรณีส่งคำสั่งจากอุปกรณ์ของบริษัทหลักทรัพย์ ให้จัดเก็บข้อมูลที่สามารถระบุได้ว่า คำสั่งซื้อขายจัดส่งจากอุปกรณ์ใด และใครเป็นผู้ใช้งานอุปกรณ์ในขณะที่ส่งคำสั่งนั้น</li> </ul>
--	---

### 3.8 การแก้ไขรายละเอียดอื่น ๆ ของประกาศ ที่ สธ. 38/2565

ข้อกำหนดประกาศที่ สธ. 38/2565	ข้อกำหนดของร่างประกาศ (ฉบับแก้ไขเพิ่มเติม)
<p><b>ภาคผนวก 1 คำศัพท์</b></p> <p>บุคคลภายนอก (third party) หมายถึง บุคคล ภายนอกที่มีความเกี่ยวข้องกับผู้ประกอบการธุรกิจดังนี้ แต่ไม่รวมถึงลูกค้าที่ใช้บริการหรือผลิตภัณฑ์ของผู้ประกอบการ</p> <ul style="list-style-type: none"> <li>(1) ผู้ให้บริการงานด้าน IT</li> <li>(2) ผู้ที่มีการเชื่อมต่อกับระบบ IT ของผู้ประกอบการ</li> </ul>	<p><u>ปรับปรุงข้อกำหนด ดังนี้</u></p> <p>บุคคลภายนอก (third party) หมายถึงบุคคล ภายนอกที่มีความเกี่ยวข้องกับผู้ประกอบการธุรกิจดังนี้ แต่ไม่รวมถึงลูกค้าที่ใช้บริการหรือผลิตภัณฑ์ของผู้ประกอบการ</p> <ul style="list-style-type: none"> <li>(1) ผู้ให้บริการงานด้าน IT</li> <li>(2) ผู้ที่มีการเชื่อมต่อกับระบบ IT ของผู้ประกอบการ</li> </ul>

ข้อกำหนดประกาศที่ สธ. 38/2565	ข้อกำหนดของร่างประกาศ (ฉบับแก้ไขเพิ่มเติม)
<p>(3) ผู้ที่สามารถเข้าถึงข้อมูลสำคัญของผู้ประกอบการธุรกิจหรือข้อมูลของลูกค้าที่อยู่ภายใต้การควบคุมดูแลของผู้ประกอบการธุรกิจ</p>	<p>(3) ผู้ที่สามารถเข้าถึงข้อมูลสำคัญของผู้ประกอบการธุรกิจหรือข้อมูลของลูกค้าที่อยู่ในรูปแบบอิเล็กทรอนิกส์และอยู่ภายใต้การควบคุมดูแลของผู้ประกอบการธุรกิจ</p>
<p><b>ภาคผนวก 1 คำศัพท์</b>  <b>เพิ่มข้อกำหนด ดังนี้</b>          “เหตุการณ์ด้านความมั่นคงปลอดภัยของระบบ IT อย่างมีนัยสำคัญ”</p>	<p>เหตุการณ์ด้านความมั่นคงปลอดภัยของระบบ IT ที่เกิดขึ้นแล้วส่งผลกระทบต่อ</p> <p>(1) ทำให้ระบบ IT หรือข้อมูลที่จัดเก็บ ประมวลผล หรือส่งต่อ สูญเสียคุณสมบัติด้านความถูกต้อง ครบถ้วน (integrity) สภาพพร้อมใช้งาน (availability) หรือการรั่วไหลซึ่งความลับ (confidentiality) อย่างมีนัยสำคัญ หรือ</p> <p>(2) ทำให้เกิดการละเมิดหรือมีความเสี่ยงที่อาจทำให้เกิดการละเมิดต่อข้อกำหนดขององค์กรหรือกฎหมาย เช่น</p> <ul style="list-style-type: none"> <li>- ระบบ IT ของผู้ประกอบการถูกบุกรุกหรือโจมตีสำเร็จ (successfully attacked หรือ system compromised)</li> <li>- เหตุการณ์ DDoS ที่ส่งผลให้ระบบของผู้ประกอบการเกิดการหยุดชะงัก</li> <li>- ระบบ IT หยุดชะงัก ไม่สามารถให้บริการได้เป็นระยะเวลาจนส่งผลกระทบต่อลูกค้าของผู้ประกอบการในวงกว้าง</li> <li>- เหตุการณ์ข้อมูลสำคัญของผู้ประกอบการหรือข้อมูลส่วนบุคคลที่อยู่ภายใต้การควบคุมดูแลของผู้ประกอบการรั่วไหล (data breach) ซึ่งส่งผลกระทบต่ออย่างมีนัยสำคัญ</li> </ul>

ข้อกำหนดประกาศที่ สธ. 38/2565	ข้อกำหนดของร่างประกาศ (ฉบับแก้ไขเพิ่มเติม)
	<ul style="list-style-type: none"> <li>- เหตุการณ์ insider threat ทั้งด้วยเจตนาและไม่เจตนา จนเป็นเหตุให้ทรัพย์สินหรือข้อมูลของลูกค้าเสียหายหรือสูญหาย</li> <li>- หน้าเว็บไซต์ของบริษัทโดนปลอมแปลง (website defacement) เป็นต้น</li> </ul>
<p><b>ภาคผนวก 3 ข้อ 2.2</b></p> <p>(7) รักษาความมั่นคงปลอดภัยด้าน IT จากการให้บริการ การเชื่อมต่อหรือการเข้าถึงข้อมูลจากบุคคลภายนอกที่สอดคล้องกับ<b>มาตรฐาน</b>การรักษาความมั่นคงปลอดภัยด้าน IT ของผู้ประกอบการธุรกิจ</p>	<p><u>ปรับปรุงข้อกำหนด ดังนี้</u></p> <p>(7) รักษาความมั่นคงปลอดภัยด้าน IT จากการให้บริการ การเชื่อมต่อหรือการเข้าถึงข้อมูลจากบุคคลภายนอก ที่สอดคล้องกับ<b>การรักษาความมั่นคงปลอดภัยด้าน IT ของผู้ประกอบการธุรกิจ หรือสอดคล้องกับมาตรฐานสากลที่ได้รับการยอมรับโดยทั่วไป</b></p>
<p><b>ภาคผนวก 3 ข้อ 8.4</b></p> <p>การรักษาความมั่นคงปลอดภัยของเครื่องแม่ข่าย (server) และอุปกรณ์ที่ใช้ปฏิบัติงาน (endpoint) เพื่อไม่ให้ถูกใช้เป็นช่องทางที่ทำให้ข้อมูลสำคัญรั่วไหลหรือมีการเข้าใช้งานระบบ IT โดยไม่ได้รับอนุญาต</p>	<p><u>ปรับปรุงข้อกำหนด ดังนี้</u></p> <p>การรักษาความมั่นคงปลอดภัยของเครื่องแม่ข่าย (server) และอุปกรณ์ที่ใช้ปฏิบัติงาน (endpoint) <b>ให้สามารถป้องกันการโจมตีด้วยรูปแบบต่าง ๆ หรือภัยจากโปรแกรมไม่ประสงค์ดี (malware) เพื่อลดความเสี่ยงจากการถูกโจมตีระบบ IT ขององค์กร หรือถูกใช้เป็นช่องทางในการโจมตีหน่วยงานอื่น และป้องกันการรั่วไหลของข้อมูลสำคัญหรือการเข้าใช้งานระบบ IT โดยไม่ได้รับอนุญาต</b></p>
<p><b>ภาคผนวก 3 ข้อ 8.8</b></p> <p>การติดตามดูแลระบบและเฝ้าระวังภัยคุกคามทางไซเบอร์ (security monitoring) โดยมีกระบวนการหรือเครื่องมือป้องกันและตรวจจับเหตุการณ์ผิดปกติด้าน IT</p>	<p><u>ปรับปรุงข้อกำหนด ดังนี้</u></p> <p>การติดตามดูแลระบบและเฝ้าระวังภัยคุกคามทางไซเบอร์ (security monitoring) โดยมีกระบวนการหรือเครื่องมือป้องกันและตรวจจับเหตุการณ์ผิดปกติด้าน IT หรือ</p>

ข้อกำหนดประกาศที่ สธ. 38/2565	ข้อกำหนดของร่างประกาศ (ฉบับแก้ไขเพิ่มเติม)
โปรแกรมไม่ประสงค์ดี (malware) หรือภัยคุกคามทางไซเบอร์ที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยต่อระบบ IT ที่มีนัยสำคัญ	ภัยคุกคามทางไซเบอร์ที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยต่อระบบ IT ที่มีนัยสำคัญ
<p>ภาคผนวก 3 ข้อ 11.3</p> <p>รายงานเหตุการณ์ผิดปกติด้าน IT เหตุการณ์การละเมิดต่อข้อมูลส่วนบุคคล และเหตุการณ์ที่ส่งผลให้ทรัพย์สินของผู้ใช้งานสูญหายหรือเสียหายอันเกิดจากเหตุการณ์ด้านความมั่นคงปลอดภัยของระบบ IT ต่อผู้มีหน้าที่รับผิดชอบเหตุการณ์ และสำนักงาน โดยไม่ชักช้าเมื่อทราบเหตุการณ์ดังกล่าว</p>	<p>ปรับปรุงข้อกำหนด ดังนี้</p> <p>รายงานเหตุการณ์ผิดปกติด้าน IT ต่อผู้มีหน้าที่รับผิดชอบเหตุการณ์ และสำนักงาน โดยไม่ชักช้าเมื่อทราบเหตุการณ์ดังกล่าว</p>

### 3.9 การแก้ไขแนวปฏิบัติในการจัดให้มีระบบเทคโนโลยีสารสนเทศ

ปรับปรุงแนวปฏิบัติให้สอดคล้องกับประกาศ ที่ สธ. 38/2565 ที่เปลี่ยนแปลงไปตามข้อ 3.1 – 3.8 และแนวปฏิบัติอื่น ๆ ดังนี้

แนวปฏิบัติที่ นป. 7/2565	ร่างแนวปฏิบัติ (ฉบับแก้ไขเพิ่มเติม)
ภาคผนวก 2 ข้อ 1.5 การสร้างความรู้และความตระหนักด้านความเสี่ยงด้าน IT แก่กรรมการและบุคลากรอย่างต่อเนื่องและมีประสิทธิผล [ไม่มีการกำหนดแนวปฏิบัติเรื่องนี้]	<p>เพิ่มเติมแนวปฏิบัติ</p> <p>“กรรมการของผู้ประกอบธุรกิจควรได้รับการสร้างความรู้และความตระหนักด้านความเสี่ยงด้าน IT อย่างเพียงพอ ตามระยะเวลาที่เหมาะสม เพื่อให้เท่าทันกับภัยคุกคามใหม่ และสภาพแวดล้อมด้าน IT ที่เปลี่ยนแปลงไป”</p>

แนวปฏิบัติที่ นป. 7/2565	ร่างแนวปฏิบัติ (ฉบับแก้ไขเพิ่มเติม)
<p>ภาคผนวก 2 ข้อ 2.3.2 การกำหนดขั้นตอนและวิธีปฏิบัติงานให้เป็นไปตามนโยบายที่เกี่ยวข้องกับการกำกับดูแลความเสี่ยงด้าน IT</p> <p>2. ผู้ประกอบธุรกิจควรกำหนดวิธีปฏิบัติสำหรับการอนุมัติยกเว้น (exception) กรณีที่มีความจำเป็นให้ไม่สามารถปฏิบัติตามขั้นตอนและวิธีปฏิบัติงานที่ผู้ประกอบธุรกิจกำหนดไว้ โดยจัดให้มีการประเมินความเสี่ยง ควบคุมความเสี่ยงอย่างเพียงพอเหมาะสม และขออนุมัติยกเว้นจากผู้มีอำนาจก่อนดำเนินการต่อไป พร้อมทั้ง ควรจัดเก็บหลักฐานการอนุมัติยกเว้นดังกล่าวอย่างเป็นลายลักษณ์อักษร</p>	<p><u>เพิ่มเติมข้อความ</u></p> <p>“ทั้งนี้ ผู้มีอำนาจในการอนุมัติยกเว้น ไม่ควรเป็นบุคคลที่อาจก่อให้เกิดความขัดแย้งทางผลประโยชน์ (conflict of interest) และการกำหนดผู้มีอำนาจอนุมัติยกเว้น ควรเป็นไปตามหลักการบริหารจัดการความเสี่ยงที่ดี (good governance) อย่างไรก็ดี ผู้ประกอบธุรกิจสามารถให้ผู้บริหารของฝ่ายงาน เช่น Head of IT เป็นต้น เป็นผู้อนุมัติยกเว้นได้ กรณีที่การอนุมัติยกเว้นนั้น ได้รับการประเมินแล้วว่ามีความเสี่ยงต่ำ และผู้บริหารของฝ่ายงานดังกล่าว ได้รับการอนุมัติจากคณะกรรมการหรือผู้บริหารระดับสูงของผู้ประกอบธุรกิจเป็นการล่วงหน้า (pre-authorized) ให้เป็นผู้ที่สามารถอนุมัติยกเว้นข้อกำหนดที่มีความเสี่ยงต่ำได้ โดยผู้ประกอบธุรกิจควรรายงานการอนุมัติยกเว้นดังกล่าวให้คณะกรรมการหรือผู้บริหารระดับสูงที่เกี่ยวข้องทราบ ตามกรอบระยะเวลาที่เหมาะสม”</p>
<p>ภาคผนวก 3 ข้อ 2.2 (3) กำหนดบทบาท หน้าที่ และความรับผิดชอบของผู้ประกอบธุรกิจและบุคคลภายนอกอย่างชัดเจนและเป็นลายลักษณ์อักษร</p> <p>1. ผู้ประกอบธุรกิจควรจัดทำสัญญาหรือข้อตกลงการใช้บริการ การเชื่อมต่อ หรือการเข้าถึงข้อมูลจากบุคคลภายนอกเป็นลายลักษณ์อักษร โดยมีการลงนาม</p>	<p><u>ปรับปรุงแนวปฏิบัติ ดังนี้</u></p> <p>1.ผู้ประกอบธุรกิจควรจัดทำสัญญาหรือข้อตกลงการใช้บริการ การเชื่อมต่อ หรือการเข้าถึงข้อมูลจากบุคคลภายนอกเป็นลายลักษณ์อักษร โดยมีการลงนามร่วมกันระหว่างผู้ประกอบธุรกิจและบุคคลภายนอก</p>

แนวปฏิบัติที่ นป. 7/2565	ร่างแนวปฏิบัติ (ฉบับแก้ไขเพิ่มเติม)
<p>ร่วมกันระหว่างผู้ประกอบการธุรกิจและบุคคลภายนอก เพื่อให้มั่นใจได้ว่าบุคคลภายนอกมีหน้าที่รับผิดชอบในการรักษาความมั่นคงปลอดภัยของระบบ IT ในระดับที่เหมาะสม โดยมีรายละเอียดสอดคล้องกับความเสี่ยง และความมีนัยสำคัญของบุคคลภายนอก ดังนี้</p> <p>...</p> <p>(4) ข้อตกลงระดับการให้บริการด้าน IT (service level agreement : SLA) สำหรับการให้บริการจากบุคคลภายนอก</p> <p>...</p> <p><u>(9) การจัดทำมีแผนฉุกเฉินด้าน IT (IT contingency plan) ที่สอดคล้องกับแผนฉุกเฉินด้าน IT ของผู้ประกอบการธุรกิจ</u></p> <p><u>(10) ความรับผิดชอบต่อความเสียหายที่เกิดจากบุคคลภายนอก เช่น กรณีการให้บริการไม่เป็นไปตาม SLA ที่กำหนดไว้ เป็นต้น</u></p> <p>หากมีข้อจำกัดในการระบุรายละเอียดและกำหนดเงื่อนไขที่สำคัญลงในข้อตกลงหรือสัญญาที่ทำกับบุคคลภายนอก ผู้ประกอบการธุรกิจควรมีการประเมินความเสี่ยงและพิจารณาแนวทางควบคุมความเสี่ยงที่เพียงพอเหมาะสม</p>	<p>เพื่อให้มั่นใจได้ว่าบุคคลภายนอกมีหน้าที่รับผิดชอบในการรักษาความมั่นคงปลอดภัยของระบบ IT ในระดับที่เหมาะสม โดยมีรายละเอียดสอดคล้องกับความเสี่ยง และความมีนัยสำคัญของบุคคลภายนอก ดังนี้</p> <p>...</p> <p>(4) ข้อตกลงระดับการให้บริการด้าน IT (service level agreement : SLA) สำหรับการให้บริการจากบุคคลภายนอก <u>และความรับผิดชอบต่อความเสียหายที่เกิดจากบุคคลภายนอก เช่น กรณีการให้บริการไม่เป็นไปตาม SLA ที่กำหนดไว้ เป็นต้น</u></p> <p>...</p> <p><u>(9) การจัดทำมีทรัพยากร เช่น บุคลากร ระบบงาน และเทคโนโลยี เป็นต้น ที่สอดคล้องกับแผนฉุกเฉินด้าน IT ของผู้ประกอบการธุรกิจ (Recovery Point Objective (RPO) Maximum Tolerable Downtime (MTD) และ Recovery Time Objective (RTO))</u></p> <p>หากมีข้อจำกัดในการระบุรายละเอียดและกำหนดเงื่อนไขที่สำคัญลงในข้อตกลงหรือสัญญาที่ทำกับบุคคลภายนอก ผู้ประกอบการธุรกิจควรมีการประเมินความเสี่ยงและพิจารณาแนวทางควบคุมความเสี่ยงที่เพียงพอเหมาะสม พร้อมทั้งขออนุมัติยกเว้น (exception) จากผู้มีอำนาจ</p>

แนวปฏิบัติที่ นป. 7/2565	ร่างแนวปฏิบัติ (ฉบับแก้ไขเพิ่มเติม)
พร้อมทั้งขออนุมัติยกเว้น (exception) จากผู้มีอำนาจ	
<p><b>ภาคผนวก 3 ข้อ 2.2 (5) การบริหารจัดการบุคคลภายนอก</b></p> <p>1. non-disclosure agreement ควรมีรายละเอียดครอบคลุมขอบเขตความรับผิดชอบในการเก็บรักษาความลับ การไม่เปิดเผยข้อมูลโดยไม่ได้รับอนุญาต การรายงานผู้ประกอบการธุรกิจเมื่อพบการรั่วไหลหรือเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต และการทำลายข้อมูลที่มีความสำคัญเมื่อสิ้นสุดข้อตกลงหรือสัญญา</p>	<p><u>เพิ่มเติมข้อความ</u></p> <p>“... ทั้งนี้ non-disclosure agreement อาจกำหนดไว้เป็นส่วนหนึ่งของสัญญาหรือข้อตกลงกับบุคคลภายนอกได้”</p>
<p><b>ภาคผนวก 3 ข้อ 4.4 การจัดทำทะเบียนทรัพย์สินด้าน IT ประเภทข้อมูล (data inventory) ให้ครบถ้วนและเป็นปัจจุบัน</b></p> <p>1. ผู้ประกอบการธุรกิจควรจัดทำทะเบียนทรัพย์สินประเภทข้อมูล (data inventory) ให้ครบถ้วนและเป็นปัจจุบัน โดยมีตัวอย่างของรายละเอียด ดังนี้ ...</p>	<p><u>เพิ่มเติมแนวปฏิบัติ</u></p> <p>1. ผู้ประกอบการธุรกิจควรจัดทำทะเบียนทรัพย์สินประเภทข้อมูล (data inventory) ให้ครบถ้วนและเป็นปัจจุบัน โดยมีตัวอย่างของรายละเอียด ดังนี้ ...</p> <p><u>2. ผู้ประกอบการธุรกิจควรปรับปรุงทะเบียนทรัพย์สินด้าน IT ประเภทข้อมูล (data inventory) ให้ครบถ้วนและเป็นปัจจุบันอยู่อย่างสม่ำเสมอ อย่างน้อยปีละ 1 ครั้ง และทุกครั้งที่มีการเปลี่ยนแปลงระบบ IT อย่างมีนัยสำคัญ</u></p>



แนวปฏิบัติที่ นป. 7/2565	ร่างแนวปฏิบัติ (ฉบับแก้ไขเพิ่มเติม)
<p>ภาคผนวก 3 ข้อ 8.7 การจัดเก็บข้อมูลบันทึกเหตุการณ์การใช้งานเกี่ยวกับระบบ IT (log)</p> <p>1. ผู้ประกอบธุรกิจควรจัดเก็บข้อมูลบันทึกเหตุการณ์ (log) ด้วยวิธีการที่ปลอดภัย โดยมีรายละเอียดครบถ้วนเพียงพอที่จะใช้เป็นหลักฐานในการตรวจสอบที่สามารถระบุตัวบุคคลผู้กระทำได้ และจัดเก็บเป็นระยะเวลาอย่างน้อย 90 วัน หรือจัดเก็บตามกฎหมายที่เกี่ยวข้องกำหนด ประกอบด้วยรายการหลักฐานอย่างน้อย ดังนี้</p> <p>...</p> <p>(2) บันทึกการยืนยันตัวตนและการเข้าถึง (<u>authentication log และ access log</u>) ของเครื่องแม่ข่าย ระบบงาน อุปกรณ์ เครือข่าย และข้อมูลที่มีความสำคัญ โดยรวมถึงความพยายามในการเข้าถึง (log-in attempt)</p> <p>(3) บันทึกการดำเนินงาน (activity log) ที่สำคัญ โดยอย่างน้อยครอบคลุม</p> <p><u>(ก) การเปลี่ยนแปลงแก้ไขโครงสร้างข้อมูล</u></p> <p><u>(ข) การเปลี่ยนแปลงแก้ไข และลบข้อมูลสำคัญ</u></p> <p>(ค) การเปลี่ยนแปลงแก้ไขการตั้งค่าของระบบ (system configuration)</p>	<p><u>ปรับปรุงแนวปฏิบัติ ดังนี้</u></p> <p>1. ผู้ประกอบธุรกิจควรจัดเก็บข้อมูลบันทึกเหตุการณ์ (log) ด้วยวิธีการที่ปลอดภัย โดยมีรายละเอียดครบถ้วนเพียงพอที่จะใช้เป็นหลักฐานในการตรวจสอบที่สามารถระบุตัวบุคคลผู้กระทำได้ และจัดเก็บเป็นระยะเวลาอย่างน้อย 90 วัน หรือจัดเก็บตามกฎหมายที่เกี่ยวข้องกำหนด ประกอบด้วยรายการหลักฐานอย่างน้อย ดังนี้</p> <p>...</p> <p>(2) บันทึกการเข้าถึง (access log) ของเครื่องแม่ข่าย ระบบงาน อุปกรณ์ เครือข่าย และข้อมูลที่มีความสำคัญ โดยรวมถึงความพยายามในการเข้าสู่ระบบ (log-in attempt)</p> <p>(3) บันทึกการดำเนินงาน (activity log) ที่สำคัญ โดยอย่างน้อยครอบคลุม</p> <p><u>(ก) การเปลี่ยนแปลงแก้ไขโครงสร้างฐานข้อมูล (database schema log) เช่น DDL operation (create/modify or alter/ drop) ที่ส่งผลกระทบต่อ database object เช่น table, index หรือ view เป็นต้น และการเปลี่ยนแปลงแก้ไขข้อมูล (update/insert/delete) ในตารางที่สำคัญ</u></p> <p>(ข) การเปลี่ยนแปลงแก้ไขการตั้งค่าของระบบ (system configuration)</p>

แนวปฏิบัติที่ นป. 7/2565	ร่างแนวปฏิบัติ (ฉบับแก้ไขเพิ่มเติม)
<p>(ง) การเปลี่ยนแปลงแก้ไขบัญชี และสิทธิของผู้ใช้งาน</p> <p>(จ) การใช้งานอินเทอร์เน็ตผ่านระบบเครือข่ายของผู้ประกอบธุรกิจ</p> <p>(ฉ) การทำงานของ firewall (network firewall log) ...</p>	<p>(ค) การเปลี่ยนแปลงแก้ไขบัญชี และสิทธิของผู้ใช้งาน</p> <p>(ง) การใช้งานอินเทอร์เน็ตผ่านระบบเครือข่ายของผู้ประกอบธุรกิจ (<b>internet traffic log</b>)</p> <p>(จ) การทำงานของ firewall (network firewall log) ...</p>
<p><b>ภาคผนวก 3 ข้อ 11.3 การรายงานเหตุการณ์ผิดปกติด้าน IT</b></p> <p>2. ผู้ประกอบธุรกิจควรรายงานสำนักงานในกรณีที่มีเหตุการณ์ด้าน IT <b>ซึ่งอาจส่งผลกระทบต่อ</b>การดำเนินงาน ธุรกิจ ชื่อเสียง ฐานะ ผลการดำเนินงานของผู้ประกอบธุรกิจ หรือลูกค้าในวงกว้าง <b>โดยครอบคลุมเหตุการณ์ ดังนี้</b></p>	<p><u>ปรับปรุงแนวปฏิบัติ ดังนี้</u></p> <p>2. ผู้ประกอบธุรกิจควรรายงานสำนักงานในกรณีที่มีเหตุการณ์ผิดปกติด้าน IT <b>โดยไม่จำกัดเพียง (including but not limited to) สถานการณ์ที่มีสาเหตุหรือส่งผลกระทบต่อ</b>การดำเนินงาน ธุรกิจ ชื่อเสียง ฐานะ ผลการดำเนินงานของผู้ประกอบธุรกิจ หรือลูกค้าในวงกว้าง <b>อย่างน้อยดังต่อไปนี้ ...</b></p>
<p><b>ภาคผนวก 4 ข้อ 5 การจัดทำและรายงานผลการตรวจสอบ</b></p> <p>[ไม่มีการกำหนดตัวอย่างสำหรับกำหนดการนำส่งแบบใหม่]</p>	<p><u>ปรับปรุงตัวอย่างในแนวปฏิบัติ เพื่อสื่อสารกำหนดการนำส่งแบบใหม่ (ตามหลักเกณฑ์ฯ ฉบับแก้ไขปรับปรุง)</u></p> <p>1. กรณีที่ผู้ประกอบธุรกิจจัดทำ และรายงานผลการตรวจสอบและแผนการปรับปรุงแก้ไขข้อบกพร่องต่อคณะกรรมการของผู้ประกอบธุรกิจ คณะกรรมการตรวจสอบของผู้ประกอบธุรกิจ หรือคณะกรรมการที่ได้รับมอบหมายจากคณะกรรมการของผู้ประกอบธุรกิจเฉพาะกรณีเป็นสาขาของธนาคารพาณิชย์ต่างประเทศ เสร็จสิ้นภายในปีที่เริ่มตรวจสอบ ผู้ประกอบธุรกิจสามารถนำส่งสำนักงานได้ทันที โดยต้องไม่เกินกำหนดเวลา ภายใน 3 เดือน นับแต่วันสิ้นปีปฏิทินของปีที่เริ่มตรวจสอบ ตัวอย่างเช่น</p>

แนวปฏิบัติที่ นป. 7/2565	ร่างแนวปฏิบัติ (ฉบับแก้ไขเพิ่มเติม)
	<ul style="list-style-type: none"> <li>ผู้ประกอบธุรกิจดำเนินการตรวจสอบรอบปี 2569 เสร็จสิ้นเมื่อวันที่ 1 กรกฎาคม 2569 และได้เสนอรายงานผลการตรวจสอบและแผนการปรับปรุงแก้ไขข้อบกพร่องต่อคณะกรรมการฯ เมื่อวันที่ 7 กรกฎาคม 2569 ผู้ประกอบธุรกิจสามารถรายงานสำนักงานได้ตั้งแต่วันที่ 7 กรกฎาคม 2569 จนถึงวันที่ 31 มีนาคม 2570 เป็นต้น</li> </ul>

#### 4. ช่วงเวลาที่คาดว่าจะประกาศ (ฉบับปรับปรุงแก้ไข) จะมีผลใช้บังคับ

วันที่ 1 มกราคม 2568 เป็นต้นไป

#### 5. ผู้เกี่ยวข้อง/บุคคลที่อาจได้รับผลกระทบ และผลกระทบที่อาจเกิดขึ้น

ผู้เกี่ยวข้อง	ผลกระทบเชิงบวก	ผลกระทบเชิงลบ
1. ผู้ประกอบธุรกิจ	<ul style="list-style-type: none"> <li>หลักเกณฑ์ฯ มีข้อกำหนดที่ชัดเจนยิ่งขึ้น โดยการปรับปรุงข้อกำหนดหรือรูปประโยคจะช่วยให้ผู้ประกอบธุรกิจมีความเข้าใจในจุดประสงค์ของหลักเกณฑ์ฯ ได้ครบถ้วนยิ่งขึ้น</li> <li>มีมาตรการควบคุมและบริหารจัดการด้าน IT ที่เหมาะสมและเป็นไปตามหลักการที่ดีมากยิ่งขึ้น</li> <li>ลดภาระในการติดตามและควบคุมการจัดส่งแบบรายงานต่อสำนักงาน เนื่องจากมีการกำหนดวันที่จัดส่งที่ชัดเจนยิ่งขึ้น</li> </ul>	<ul style="list-style-type: none"> <li>ผู้ประกอบธุรกิจทุกรายยังคงมีหน้าที่ในการกำกับดูแลและควบคุมความเสี่ยงด้านเทคโนโลยีสารสนเทศ ตามระดับความเสี่ยงของตน</li> <li>ผู้ประกอบธุรกิจบริษัทหลักทรัพย์ (บล.) ที่มีการใช้งานระบบ trading system อาจต้องมีการเตรียมข้อมูลและจัดเก็บข้อมูลบันทึก additional transaction log เพิ่มเติม กรณีที่ผู้ประกอบธุรกิจยังมิได้มีการจัดเก็บ</li> </ul>

ผู้เกี่ยวข้อง	ผลกระทบเชิงบวก	ผลกระทบเชิงลบ
	<ul style="list-style-type: none"> <li>● ผู้ประกอบธุรกิจสามารถจัดการความเสี่ยงด้าน IT ที่มีความเหมาะสมกับขนาดและระดับความเสี่ยงของผู้ประกอบธุรกิจมากยิ่งขึ้น ในขณะที่ยังคงมีมาตรการควบคุมด้านการรักษาความมั่นคงปลอดภัยด้าน IT ไว้เพียงพอ เช่น               <ul style="list-style-type: none"> <li>○ การลดรอบการดำเนินการทดสอบการเจาะระบบจากทุกปี เป็นทุก 3 ปี สำหรับผู้ประกอบธุรกิจขนาดเล็ก</li> <li>○ การลดรอบปีการตรวจสอบด้าน IT สำหรับผู้ประกอบธุรกิจขนาดเล็ก และผู้ประกอบธุรกิจที่มีความเสี่ยงระดับต่ำ เป็นต้น</li> </ul> </li> </ul>	<p>ข้อมูลดังกล่าวในลักษณะที่พร้อมนำมาใช้งาน และสามารถจัดทำเป็นข้อมูลพร้อมนำส่งสำนักงานเมื่อมีการร้องขอได้โดยไม่ชักช้า</p> <ul style="list-style-type: none"> <li>● ผู้ประกอบธุรกิจขนาดเล็ก: อาจต้องจัดสรรทรัพยากรเพิ่มเติม เพื่อจัดให้มีการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (cyber hygiene) เพิ่มเติม เช่น การควบคุมการเข้าถึง การวิเคราะห์สาเหตุที่แท้จริง (root cause) และการบันทึกข้อมูลที่เกี่ยวข้องกับการบริหารจัดการเหตุการณ์ผิดปกติด้าน IT เป็นต้น</li> </ul>
<p>2. สำนักงาน ก.ส.ต.</p>	<ul style="list-style-type: none"> <li>● การปรับปรุงด้านความชัดเจนในเนื้อหาของหลักเกณฑ์ฯ จะช่วยให้สำนักงาน ก.ส.ต. สามารถสื่อสารจุดประสงค์ของหลักเกณฑ์ให้ผู้ประกอบธุรกิจมีความเข้าใจ และสามารถปฏิบัติได้อย่างเหมาะสมมากยิ่งขึ้น</li> <li>● สามารถส่งเสริมให้ผู้ประกอบธุรกิจมีการบริหารจัดการด้าน IT ได้อย่างมีประสิทธิภาพมากยิ่งขึ้น ซึ่งจะเป็นการยกระดับความพร้อมด้านความมั่นคงปลอดภัยด้าน IT และเพิ่มความเชื่อมั่นต่อภาคตลาดทุนของประเทศ</li> </ul>	<ul style="list-style-type: none"> <li>● ข้อมูลผลการตรวจสอบด้าน IT ซึ่งใช้ในการวิเคราะห์ cyber landscape ของตลาดทุนสำหรับผู้ประกอบธุรกิจขนาดเล็กและผู้ประกอบธุรกิจที่มีความเสี่ยงระดับต่ำ จะไม่ได้รับการปรับปรุง (update) เป็นรายปี แต่จะปรับปรุงทุก 3 ปี จึงต้องใช้กลไกอื่น ๆ เพื่อติดตามความเสี่ยงของผู้ประกอบธุรกิจกลุ่มดังกล่าวอย่างเพียงพอ เช่น ติดตามการจัดส่งแบบ RLA ประจำปี และติดตามการรายงานเหตุการณ์ผิดปกติด้าน IT เป็นต้น</li> </ul>

**6. เหตุผลความจำเป็นของการให้มีระบบอนุญาต ระบบคณะกรรมการ หรือ การกำหนดโทษอาญา รวมทั้งหลักเกณฑ์การใช้ดุลพินิจของเจ้าหน้าที่ (ถ้ามี)**

ประกาศที่นำมารับฟังความคิดเห็น ไม่มีการกำหนดให้มีระบบอนุญาต ระบบ คณะกรรมการ หรือการกำหนดโทษอาญา และหลักเกณฑ์การใช้ดุลพินิจของเจ้าหน้าที่ขึ้นใหม่

## แบบสำรวจความคิดเห็น

เรื่อง ร่างประกาศสำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์  
ที่ สธ. /2567 เรื่อง ข้อกำหนดในรายละเอียดเกี่ยวกับการจัดให้มีระบบเทคโนโลยี  
สารสนเทศ (ฉบับที่ )

### ข้อมูลทั่วไป

ชื่อผู้ตอบ \_\_\_\_\_ ตำแหน่ง \_\_\_\_\_

ชื่อบริษัท/องค์กร \_\_\_\_\_

โทรศัพท์ \_\_\_\_\_ โทรสาร \_\_\_\_\_

อีเมล \_\_\_\_\_

### สถานะของผู้ให้ข้อคิดเห็น (ตอบได้มากกว่า 1 ข้อ)

- |  |  |
|--|--|
| <input type="checkbox"/> บริษัทหลักทรัพย์                                    | <input type="checkbox"/> ผู้ให้บริการระบบเสนอขายโทเคนดิจิทัล         |
| <input type="checkbox"/> บริษัทหลักทรัพย์จัดการกองทุนรวม/<br>กองทุนส่วนบุคคล | <input type="checkbox"/> ผู้ให้บริการระบบคราด์ฟนดิง (funding portal) |
| <input type="checkbox"/> ผู้ประกอบธุรกิจการเป็นที่ปรึกษาการลงทุน             | <input type="checkbox"/> ธนาคารพาณิชย์                               |
| <input type="checkbox"/> ผู้ประกอบธุรกิจสัญญาซื้อขายล่วงหน้า                 | <input type="checkbox"/> บริษัทประกัน                                |
| <input type="checkbox"/> ผู้ประกอบธุรกิจสินทรัพย์ดิจิทัล                     | <input type="checkbox"/> อื่น ๆ (โปรดระบุ) _____                     |

สำนักงานขอข้อมูลส่วนบุคคลของท่าน โดยมีวัตถุประสงค์เพื่อใช้พิจารณาประกอบการรับฟังความคิดเห็น และประโยชน์ในการติดต่อกลับเพื่อขอข้อมูลประกอบเอกสารรับฟังความคิดเห็นของท่านเพิ่มเติม โดยสำนักงานคำนึงถึงความสำคัญของข้อมูลและเคารพสิทธิความเป็นส่วนตัวส่วนตัวของท่าน จึงขอให้ท่านอ่านและทำความเข้าใจนโยบายการคุ้มครองข้อมูลส่วนบุคคล [privacy policy](#) แล้วจึงพิจารณาให้ความยินยอมให้สำนักงานประมวลผลข้อมูลส่วนบุคคลของท่าน

ยินยอม       ไม่ยินยอม

กรณีต้องการยกเลิกความยินยอมหรือขอใช้สิทธิ โปรดติดต่อไปที่ email: [DPO@sec.or.th](mailto:DPO@sec.or.th)

กรุณาส่งแบบสำรวจความคิดเห็นกลับไป

ฝ่ายกำกับและตรวจสอบความเสี่ยงด้านเทคโนโลยีสารสนเทศ สำนักงาน ก.ล.ต.

เลขที่ 333/3 ถนนวิภาวดีรังสิต แขวงจอมพล เขตจตุจักร กรุงเทพฯ 10900 โทรศัพท์ 1207

หรือ email: [cyberteam@sec.or.th](mailto:cyberteam@sec.or.th)

\*\*\* สำนักงานขอขอบคุณท่านที่ได้ให้ความร่วมมือในการแสดงความคิดเห็นในครั้งนี้ \*\*\*

## แบบสำรวจความคิดเห็น

ท่านเห็นด้วยหรือไม่กับร่างประกาศที่สำนักงาน ก.ล.ต. ดังต่อไปนี้

- ร่างประกาศสำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ ที่ สธ. /2567 เรื่อง ข้อกำหนดในรายละเอียดเกี่ยวกับการจัดให้มีระบบเทคโนโลยีสารสนเทศ (ฉบับที่ ) และภาคผนวกที่เกี่ยวข้อง
- ร่างประกาศแนวปฏิบัติ ที่ นป. /2565 เรื่อง แนวปฏิบัติในการจัดให้มีระบบเทคโนโลยีสารสนเทศ และภาคผนวกที่เกี่ยวข้อง

<b>1. การปรับปรุงขอบเขตการบังคับใช้สำหรับผู้ประกอบธุรกิจการเป็นที่ปรึกษาการลงทุน</b>	เห็นด้วย	ไม่เห็นด้วย
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
ข้อเสนอแนะ หรือข้อสังเกตเพิ่มเติม ..... ..... ..... .....		
<b>2. การปรับปรุงข้อกำหนดสำหรับผู้ประกอบธุรกิจที่เป็นสาขาของธนาคารพาณิชย์ต่างประเทศ</b>	เห็นด้วย	ไม่เห็นด้วย
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
ข้อเสนอแนะ หรือข้อสังเกตเพิ่มเติม ..... ..... ..... .....		
<b>3. การปรับปรุงรอบการตรวจสอบด้านเทคโนโลยีสารสนเทศ สำหรับผู้ประกอบการขนาดเล็ก และผู้ประกอบการที่มีความเสี่ยงระดับต่ำ</b>	เห็นด้วย	ไม่เห็นด้วย
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
ข้อเสนอแนะ หรือข้อสังเกตเพิ่มเติม ..... ..... ..... .....		

4. การจัดส่งรายงานผลการตรวจสอบด้านเทคโนโลยีสารสนเทศ	เห็นด้วย	ไม่เห็นด้วย
	<input type="checkbox"/>	<input type="checkbox"/>
ข้อเสนอแนะ หรือข้อสังเกตเพิ่มเติม		
.....		
.....		
.....		
.....		
5. การจัดส่งแบบ RLA (Risk Level Assessment)	เห็นด้วย	ไม่เห็นด้วย
	<input type="checkbox"/>	<input type="checkbox"/>
ข้อเสนอแนะ หรือข้อสังเกตเพิ่มเติม		
.....		
.....		
.....		
.....		
6. การรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ สำหรับ ผู้ประกอบการธุรกิจขนาดเล็ก	เห็นด้วย	ไม่เห็นด้วย
	<input type="checkbox"/>	<input type="checkbox"/>
ข้อเสนอแนะ หรือข้อสังเกตเพิ่มเติม		
.....		
.....		
.....		
.....		
7. แนวปฏิบัติข้อกำหนดการจัดทำและนำส่งบันทึกการทำธุรกรรมเพิ่มเติม (additional transaction log) เมื่อสำนักงานร้องขอ	เห็นด้วย	ไม่เห็นด้วย
	<input type="checkbox"/>	<input type="checkbox"/>
ข้อเสนอแนะ หรือข้อสังเกตเพิ่มเติม		
.....		
.....		
.....		
.....		



8. การแก้ไขรายละเอียดอื่น ๆ ของประกาศ ที่ สร. 38/2565	เห็นด้วย	ไม่เห็นด้วย
	<input type="checkbox"/>	<input type="checkbox"/>
ข้อเสนอแนะ หรือข้อสังเกตเพิ่มเติม (กรณีไม่เห็นด้วย โปรดระบุรายละเอียด/ข้อที่ท่านไม่เห็นด้วย) ..... ..... ..... ..... ..... ..... ..... .....		
9. การแก้ไขแนวปฏิบัติในการจัดให้มีระบบเทคโนโลยีสารสนเทศ	เห็นด้วย	ไม่เห็นด้วย
	<input type="checkbox"/>	<input type="checkbox"/>
ข้อเสนอแนะ หรือข้อสังเกตเพิ่มเติม (กรณีไม่เห็นด้วย โปรดระบุรายละเอียด/ข้อที่ท่านไม่เห็นด้วย) ..... ..... ..... ..... ..... ..... ..... .....		
10. ข้อเสนอแนะอื่น ๆ (ถ้ามี)		
ข้อเสนอแนะ หรือข้อสังเกตเพิ่มเติม ..... ..... ..... ..... ..... ..... ..... .....		