คำอธิบายสรุปหลักเกณฑ์ IT ที่ได้รับการแก้ไขเพิ่มเติม

ตามที่สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ (“สำนักงาน ก.ล.ต.”) ได้ปรับปรุงหลักเกณฑ์ของประกาศสำนักงาน ก.ล.ต. ที่ สธ. 38/2565 เรื่อง ข้อกำหนดในรายละเอียดเกี่ยวกับการจัดให้มีระบบเทคโนโลยีสารสนเทศ (“ประกาศที่ สธ. 38/2565”) และประกาศแนวปฏิบัติ ที่ นป. 7/2565 เรื่อง แนวปฏิบัติในการจัดให้มีระบบเทคโนโลยีสารสนเทศ (“หลักเกณฑ์ IT”) นั้น

สำนักงาน ก.ล.ต. ได้ออกประกาศและแนวปฏิบัติฉบับแก้ไขเพิ่มเติมสำหรับหลักเกณฑ์ IT ดังกล่าว ซึ่งจะมีผลบังคับใช้ตั้งแต่วันที่ 1 มกราคม พ.ศ. 2568 เป็นต้นไป ได้แก่

1. ประกาศสำนักงาน ก.ล.ต. ที่ สธ. 33/2567 เรื่อง ข้อกำหนดในรายละเอียดเกี่ยวกับการจัดให้มีระบบเทคโนโลยีสารสนเทศ (ฉบับที่ 2) ลงวันที่ 21 พฤศจิกายน พ.ศ. 2567 และภาคผนวกแนบท้าย (“ประกาศที่ สธ. 33/2567”) ซึ่งแก้ไขเพิ่มเติมประกาศที่ สธ. 38/2565
2. ประกาศแนวปฏิบัติ ที่ นป. 6/2567 เรื่อง แนวปฏิบัติในการจัดให้มีระบบเทคโนโลยีสารสนเทศ ลงวันที่ 21 พฤศจิกายน พ.ศ. 2567 และภาคผนวกแนบท้าย (“ประกาศที่ นป. 6/2567”) ซึ่งจะใช้แทน ประกาศแนวปฏิบัติ ที่ นป. 7/2565 ซึ่งจะถูกยกเลิก

ประกาศที่มีผลใช้บังคับ ตั้งแต่วันที่ 1 กรกฎาคม 2566 เป็นต้นมา	**ประกาศที่จะมีผลใช้บังคับ ตั้งแต่วันที่ 1 มกราคม 2568 เป็นต้นไป**
ประกาศสำนักงาน ก.ล.ต. ที่ สธ. 38/2565 เรื่อง ข้อกำหนดในรายละเอียดเกี่ยวกับการจัดให้มีระบบเทคโนโลยีสารสนเทศ	ประกาศสำนักงาน ก.ล.ต. ที่ **สธ. 38/2565** เรื่อง ข้อกำหนดในรายละเอียดเกี่ยวกับการจัดให้มีระบบเทคโนโลยีสารสนเทศ ซึ่งแก้ไขเพิ่มเติมโดยประกาศสำนักงาน ก.ล.ต. ที่ **สธ. 33/2567** เรื่อง ข้อกำหนดในรายละเอียดเกี่ยวกับการจัดให้มีระบบเทคโนโลยีสารสนเทศ (ฉบับที่ 2)
ประกาศแนวปฏิบัติ ที่ นป. 7/2565 เรื่อง แนวปฏิบัติในการจัดให้มีระบบเทคโนโลยีสารสนเทศ ***(ยกเลิก)***	ประกาศแนวปฏิบัติ ที่ นป. 6/2567 เรื่อง แนวปฏิบัติในการจัดให้มีระบบเทคโนโลยีสารสนเทศ

<u>สรุปหลักเกณฑ์ IT ที่ได้รับการแก้ไขเพิ่มเติม</u>

1. ปรับปรุงขอบเขตการบังคับใช้ประกาศสำหรับผู้ประกอบธุรกิจการเป็นที่ปรึกษาการลงทุน และผู้ประกอบธุรกิจการเป็นที่ปรึกษาสัญญาซื้อขายล่วงหน้า ที่มีการใช้เทคโนโลยีเพื่อการประกอบธุรกิจ

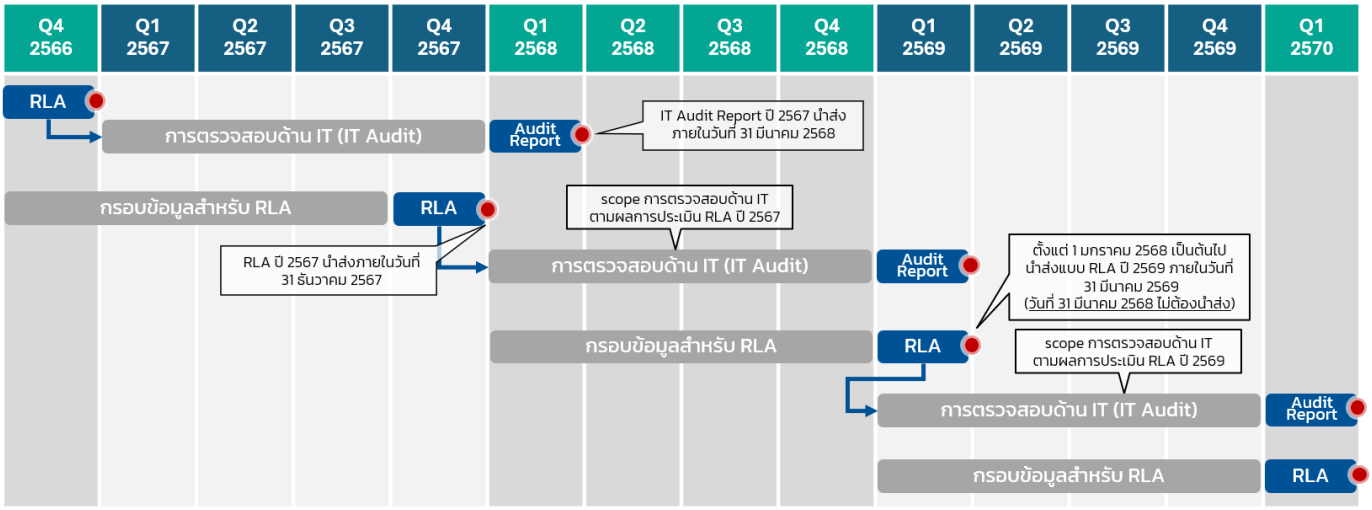
เพื่อให้ขอบเขตการบังคับใช้ของประกาศมีความเหมาะสมกับบริบทของผู้ประกอบธุรกิจประเภทดังกล่าวมากยิ่งขึ้น หลักเกณฑ์ IT ได้ปรับปรุงขอบเขตให้ผู้ประกอบธุรกิจ “การเป็นที่ปรึกษาการลงทุนที่มีการใช้เทคโนโลยีเพื่อการติดต่อหรือให้บริการแก่ลูกค้า” และ

"การเป็นที่ปรึกษาสัญญาซื้อขายล่วงหน้าที่มีการใช้เทคโนโลยีเพื่อการติดต่อหรือให้บริการแก่ลูกค้า" มีหน้าที่ปฏิบัติตามข้อกำหนดการจัดให้มีระบบเทคโนโลยีสารสนเทศ และได้เพิ่มเติมนิยาม "เทคโนโลยีเพื่อการติดต่อหรือให้บริการแก่ลูกค้า" เพื่อความความชัดเจนในการบังคับใช้

2. ปรับปรุงกำหนดการจัดทำและนำส่งแบบรายงานที่เกี่ยวข้อง

เพื่อให้ลดโอกาสเกิดความเข้าใจคลาดเคลื่อนในการนำส่ง (1) ผลการประเมินตามแบบ RLA (Risk Level Assessment) และ (2) รายงานผลการตรวจสอบด้านเทคโนโลยีสารสนเทศและแผนการปรับปรุงแก้ไขข้อบกพร่อง ("การตรวจสอบด้าน IT") ต่อสำนักงานภายในระยะเวลาที่กำหนด ทั้งนี้ หลักเกณฑ์ IT ได้แก้ไขให้ผู้ประกอบธุรกิจนำส่งแบบรายงานทั้ง 2 รายการดังกล่าว เป็นช่วงเวลาเดียวกัน ภายในวันที่ 31 มีนาคม ของทุกปีปฏิทิน โดยมีรายละเอียดดังนี้

ชื่อแบบ	แบบ RLA	รายงานผลการตรวจสอบด้าน IT และแผนการปรับปรุงแก้ไขข้อบกพร่อง
คำอธิบาย	แบบประเมินระดับความเสี่ยงเพื่อกำหนด scope การบังคับใช้ข้อกำหนดของประกาศ การจัดให้มีมาตรการควบคุมด้าน IT และ scope เพื่อการตรวจสอบด้าน IT	รายงานผลการตรวจสอบด้าน IT และแผนการปรับปรุงแก้ไขข้อบกพร่องที่ผู้ประกอบธุรกิจได้จัดทำประจำปี
การดำเนินการ	การประเมิน โดยใช้ข้อมูลระหว่างวันที่ 1 ม.ค. – 31 ธ.ค. ของปีก่อนหน้า	การตรวจสอบ โดยดำเนินการภายในวันที่ 1 ม.ค. – 31 ธ.ค. ของปีปัจจุบัน
ผู้ที่สามารถอนุมัติรายงานก่อนจัดส่งสำนักงาน ก.ล.ต.	• คณะกรรมการของผู้ประกอบธุรกิจ • ผู้ที่ได้รับมอบหมายจากคณะกรรมการของผู้ประกอบธุรกิจให้รับผิดชอบในการพิจารณาผลการประเมิน RLA	• คณะกรรมการของผู้ประกอบธุรกิจ • คณะกรรมการตรวจสอบของผู้ประกอบธุรกิจ (audit committee) • *[เฉพาะผู้ประกอบธุรกิจที่เป็นสาขาของธนาคารพาณิชย์ต่างประเทศ]* คณะกรรมการที่ได้รับมอบหมายจากคณะกรรมการของผู้ประกอบธุรกิจ
กำหนดส่ง	ภายใน 31 มีนาคม ของปีปัจจุบัน	ภายใน 31 มีนาคม ของปีถัดไป (Y+1 of audit year)



ภาพประกอบที่ 1 ความสัมพันธ์ของการประเมินแบบ RLA และการตรวจสอบด้าน IT

ผู้ประกอบธุรกิจสามารถตรวจสอบรายละเอียดและตัวอย่างกำหนดการการจัดให้มีการตรวจสอบด้าน IT และการประเมินแบบ RLA ได้ที่ภาคผนวก ก. ของเอกสาร

3. ปรับปรุงรอบการตรวจสอบด้าน IT สำหรับผู้ประกอบธุรกิจขนาดเล็กและผู้ประกอบธุรกิจที่มีความเสี่ยงระดับต่ำ

ปรับปรุงรอบการตรวจสอบด้าน IT ของผู้ประกอบธุรกิจที่มีผลการประเมินตามแบบ RLA เป็น “ผู้ประกอบธุรกิจขนาดเล็ก” หรือ “ผู้ประกอบธุรกิจที่มีความเสี่ยงระดับต่ำ” ให้มีการตรวจสอบด้าน IT “อย่างน้อยทุก 3 ปี ตามรอบปีที่สำนักงานกำหนด”

ทั้งนี้ สำนักงาน ก.ล.ต. กำหนดให้รอบปี 2569 เป็นรอบปีเริ่มต้นที่ผู้ประกอบธุรกิจขนาดเล็ก และผู้ประกอบที่มีความเสี่ยงระดับต่ำ ต้องจัดให้มีการตรวจสอบด้าน IT ตามข้อกำหนดของประกาศ (จัดให้มีการตรวจสอบรอบปีแรก ระหว่างวันที่ 1 มกราคม 2569 – 31 ธันวาคม 2569) และให้จัดให้มีการตรวจสอบทุกรอบ 3 ปี ดังนี้

พ.ศ.	ปีที่กำหนดให้มีการตรวจสอบด้าน IT	พ.ศ.	ปีที่กำหนดให้มีการตรวจสอบด้าน IT
2568	-	2577	-
2569	จัดให้มีการตรวจสอบด้าน IT	2578	จัดให้มีการตรวจสอบด้าน IT
2570	-	2579	-
2571	-	2580	-
2572	จัดให้มีการตรวจสอบด้าน IT	2581	จัดให้มีการตรวจสอบด้าน IT
2573	-	2582	-
2574	-	2583	-
2575	จัดให้มีการตรวจสอบด้าน IT	2584	จัดให้มีการตรวจสอบด้าน IT
2576	-	...	...

อย่างไรก็ดี หลักเกณฑ์ IT กำหนดเพิ่มเติมให้ผู้ประกอบธุรกิจขนาดเล็ก และผู้ประกอบที่มีความเสี่ยงระดับต่ำ **ต้องจัดให้มีการตรวจสอบด้าน IT ในรอบปีที่เกิดเหตุการณ์ด้านความมั่นคงปลอดภัยของระบบ IT อย่างมีนัยสำคัญด้วย** ดังนี้

ข้อกำหนดภาคผนวก 4 แนบท้ายประกาศที่ สธ. 33/2567
ทั้งนี้ กรณีที่เกิดเหตุการณ์ด้านความมั่นคงปลอดภัยของระบบ IT อย่างมีนัยสำคัญ ผู้ประกอบธุรกิจขนาดเล็กและผู้ประกอบธุรกิจที่มีความเสี่ยงระดับต่ำ ต้องจัดให้มีการดำเนินการตรวจสอบด้าน IT แบบเต็มรูปแบบ (full scope) ภายในปีที่เกิดเหตุการณ์ดังกล่าว กรณีที่มีเหตุจำเป็นทำให้ผู้ประกอบธุรกิจขนาดเล็กหรือผู้ประกอบธุรกิจที่มีความเสี่ยงระดับต่ำ ไม่สามารถดำเนินการตรวจสอบด้าน IT แบบเต็มรูปแบบ (full scope) ภายในปีที่เกิดเหตุการณ์ด้านความมั่นคงปลอดภัยของระบบ IT อย่างมีนัยสำคัญ ผู้ประกอบธุรกิจต้องดำเนินการดังต่อไปนี้ ภายใน 4 เดือน นับแต่วันที่ทราบเหตุการณ์ดังกล่าว (1) รายงานเหตุจำเป็นที่ทำให้ไม่สามารถดำเนินการตรวจสอบด้าน IT แบบเต็มรูปแบบ (full scope) ได้ภายในปีที่เกิดเหตุการณ์ดังกล่าว และแผนการตรวจสอบด้าน IT ต่อคณะกรรมการของผู้ประกอบธุรกิจ หรือคณะกรรมการที่ได้รับมอบหมายจากคณะกรรมการของผู้ประกอบธุรกิจเฉพาะกรณีเป็นสาขาของธนาคารพาณิชย์ต่างประเทศ รวมทั้งรายงานเหตุจำเป็นดังกล่าวต่อสำนักงาน *และ* (2) ดำเนินการตรวจสอบด้าน IT แบบเต็มรูปแบบ (full scope)

ผู้ประกอบธุรกิจสามารถตรวจสอบรายละเอียดและตัวอย่างกำหนดการการจัดให้มีการตรวจสอบด้าน IT และการประเมินแบบ RLA ได้ที่ภาคผนวก ก. ของเอกสาร

4. ปรับปรุงข้อกำหนดการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศสำหรับผู้ประกอบธุรกิจขนาดเล็ก

ปรับปรุงข้อกำหนดแนวปฏิบัติขั้นต้น (cyber hygiene) ดังนี้

ภาคผนวกแนบท้ายประกาศที่ นป. 6/2567	
เรื่อง	**ข้อกำหนดสำหรับผู้ประกอบธุรกิจขนาดเล็ก**
การทดสอบการเจาะระบบ (penetration test)	***[แก้ไข]*** จัดให้มี**การทดสอบการเจาะระบบ** (penetration test) บนระบบงาน (application system) และระบบเครือข่ายที่มีการเชื่อมต่อกับเครือข่ายสาธารณะ (internet facing) “**อย่างน้อยทุก 3 ปี และทุกครั้งที่มีการเปลี่ยนแปลงระบบดังกล่าวอย่างมีนัยสำคัญ**” จากเดิม “อย่างน้อยปีละ 1 ครั้ง และทุกครั้งที่มีการเปลี่ยนแปลงระบบดังกล่าวอย่างมีนัยสำคัญ”
การควบคุมการเข้าถึงข้อมูลและระบบ IT (access control)	***[เพิ่มเติม]*** **จัดให้มีการควบคุมการเข้าถึงข้อมูลและระบบ IT (access control) ทุกข้อของหัวข้อการควบคุม access control** จากเดิม กำหนดเพียงเฉพาะการเข้าถึงบัญชีสิทธิสูง (privileged user)

ภาคผนวกแนบท้ายประกาศที่ นป. 6/2567	
เรื่อง	**ข้อกำหนดสำหรับผู้ประกอบธุรกิจขนาดเล็ก**
การบริหารจัดการเหตุการณ์ผิดปกติด้าน IT	กรณีที่เกิดเหตุการณ์ผิดปกติด้าน IT ผู้ประกอบธุรกิจขนาดเล็กควรจัดให้มีการดำเนินการ ดังต่อไปนี้ ก. รายงานเหตุการณ์ผิดปกติด้าน IT ต่อผู้มีหน้าที่รับผิดชอบเหตุการณ์และสำนักงานโดยไม่ชักช้าเมื่อทราบเหตุการณ์ดังกล่าว ข. ***[เพิ่มเติม]*** วิเคราะห์สาเหตุที่แท้จริง (root cause) ของเหตุการณ์ผิดปกติด้าน IT เพื่อกำหนดแนวทางการแก้ไขและป้องกันไม่ให้เกิดเหตุการณ์ซ้ำในอนาคต ค. ***[เพิ่มเติม]*** บันทึกข้อมูลที่เกี่ยวข้องกับการบริหารจัดการเหตุการณ์ผิดปกติด้าน IT และจัดเก็บข้อมูลดังกล่าวเป็นระยะเวลาไม่น้อยกว่า 2 ปี นับแต่วันที่เกิดเหตุการณ์นั้น โดยต้องจัดเก็บไว้ในลักษณะที่พร้อมให้สำนักงานสามารถเรียกดูและตรวจสอบได้โดยไม่ชักช้า

5. เพิ่มเติมแนวปฏิบัติข้อกำหนดการจัดทำและนำส่งบันทึกการทำธุรกรรมเพิ่มเติม (additional transaction log) เมื่อสำนักงานร้องขอ

หลักเกณฑ์ IT ยังคงไว้ซึ่งรายละเอียดของ transaction log ตามข้อกำหนดของประกาศที่ นป. 7/2565 อย่างไรก็ดี เพื่อให้ผู้ปฏิบัติหน้าที่ market surveillance ได้รับข้อมูลที่จำเป็นต่อการปฏิบัติหน้าที่ในการพิจารณาการกระทำอันไม่เป็นธรรมเกี่ยวกับการซื้อขายหลักทรัพย์ได้อย่างเหมาะสม ทั้งนี้ หลักเกณฑ์ IT ได้เพิ่มเติมข้อกำหนดให้ผู้ประกอบธุรกิจภายใต้ประกาศดำเนินการจัดทำและนำส่งข้อมูลเพิ่มเติม (additional transaction log) ต่อสำนักงาน ก.ล.ต. ตามรูปแบบและวิธีการที่กำหนด โดยไม่ชักช้าเมื่อมีการร้องขอ ดังนี้

ข้อกำหนดที่ 8.7.1(5) ภาคผนวกแนบท้ายประกาศที่ นป. 6/2567
(5) บันทึกการทำธุรกรรม (transaction log) ควรมีระยะเวลาจัดเก็บขั้นต่ำ 1 ปี โดยในกรณีที่เป็นระบบ IT เพื่อการซื้อขายหลักทรัพย์ (trading system) ให้บันทึกบัญชีผู้ใช้งาน / ข้อมูลรายละเอียดชื่อย่อหลักทรัพย์ (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 ***[เพิ่มเติม]*** ทั้งนี้ ให้ผู้ประกอบธุรกิจจัดทำและนำส่งข้อมูลเพิ่มเติมต่อสำนักงาน ตามรูปแบบและวิธีการที่สำนักงานกำหนดโดยไม่ชักช้าเมื่อสำนักงานร้องขอ โดยข้อมูลบันทึกการทำธุรกรรมเพิ่มเติม (additional transaction log) ที่ผู้ประกอบธุรกิจควรพร้อมจัดทำและนำส่งต่อสำนักงานเมื่อสำนักงานร้องขอ ควรมีรายละเอียดขั้นต่ำ ดังนี้

ข้อกำหนดที่ 8.7.1(5) ภาคผนวกแนบท้ายประกาศที่ นป. 6/2567
(ก) บัญชีผู้ใช้งาน (user ID) (ข) เลขบัตรประจำตัวประชาชนหรือเลขทะเบียนนิติบุคคลของลูกค้า (ค) ชื่อ-นามสกุลของลูกค้า (ง) วันและเวลาที่จับคู่คำสั่งซื้อขายได้ (matched date : yyyy/mm/dd – hh:mm:ss:sss) (จ) กรณีส่งคำสั่งจากอุปกรณ์ของบริษัทหลักทรัพย์ ให้จัดเก็บข้อมูลที่สามารถระบุได้ว่าคำสั่งซื้อขายจัดส่งจากอุปกรณ์ใด และใครเป็นผู้ใช้งานอุปกรณ์ในขณะที่ส่งคำสั่งนั้น

6. ปรับปรุงข้อกำหนดสำหรับผู้ประกอบธุรกิจที่เป็นสาขาของธนาคารพาณิชย์ต่างประเทศ

เฉพาะผู้ประกอบธุรกิจที่เป็นสาขาของธนาคารพาณิชย์ต่างประเทศ สามารถให้คณะกรรมการที่ได้รับมอบหมายจากคณะกรรมการของผู้ประกอบธุรกิจ ทำหน้าที่ในการกำกับดูแลและบริหารจัดการด้านเทคโนโลยีสารสนเทศ การติดตาม และการพิจารณารายงานผลการปฏิบัติงานและแผนการปรับปรุงแก้ไขข้อบกพร่องได้

รายละเอียดของข้อกำหนดปรากฏตาม ภาคผนวก 2 ข้อ 1.6 และ ภาคผนวก 4 ข้อ 5 แนบท้ายประกาศ สธ. 38/2565 ซึ่งแก้ไขเพิ่มเติมโดยประกาศ สธ. 33/2567

7. แก้ไขรายละเอียดอื่น ๆ ของหลักเกณฑ์ IT

เพื่อให้ผู้ประกอบธุรกิจเข้าใจในเจตนารมณ์ของหลักเกณฑ์ IT และสามารถจัดให้มีมาตรการควบคุมที่ครบถ้วนและมีประสิทธิภาพมากยิ่งขึ้น จึงปรับปรุงและเพิ่มเติมแนวปฏิบัติเพื่อขยายความข้อกำหนดของหลักเกณฑ์ IT ให้ชัดเจนมากยิ่งขึ้น ทั้งนี้ ผู้ประกอบธุรกิจสามารถตรวจสอบรายละเอียดการแก้ไขได้ที่ภาคผนวก ข. ของเอกสาร

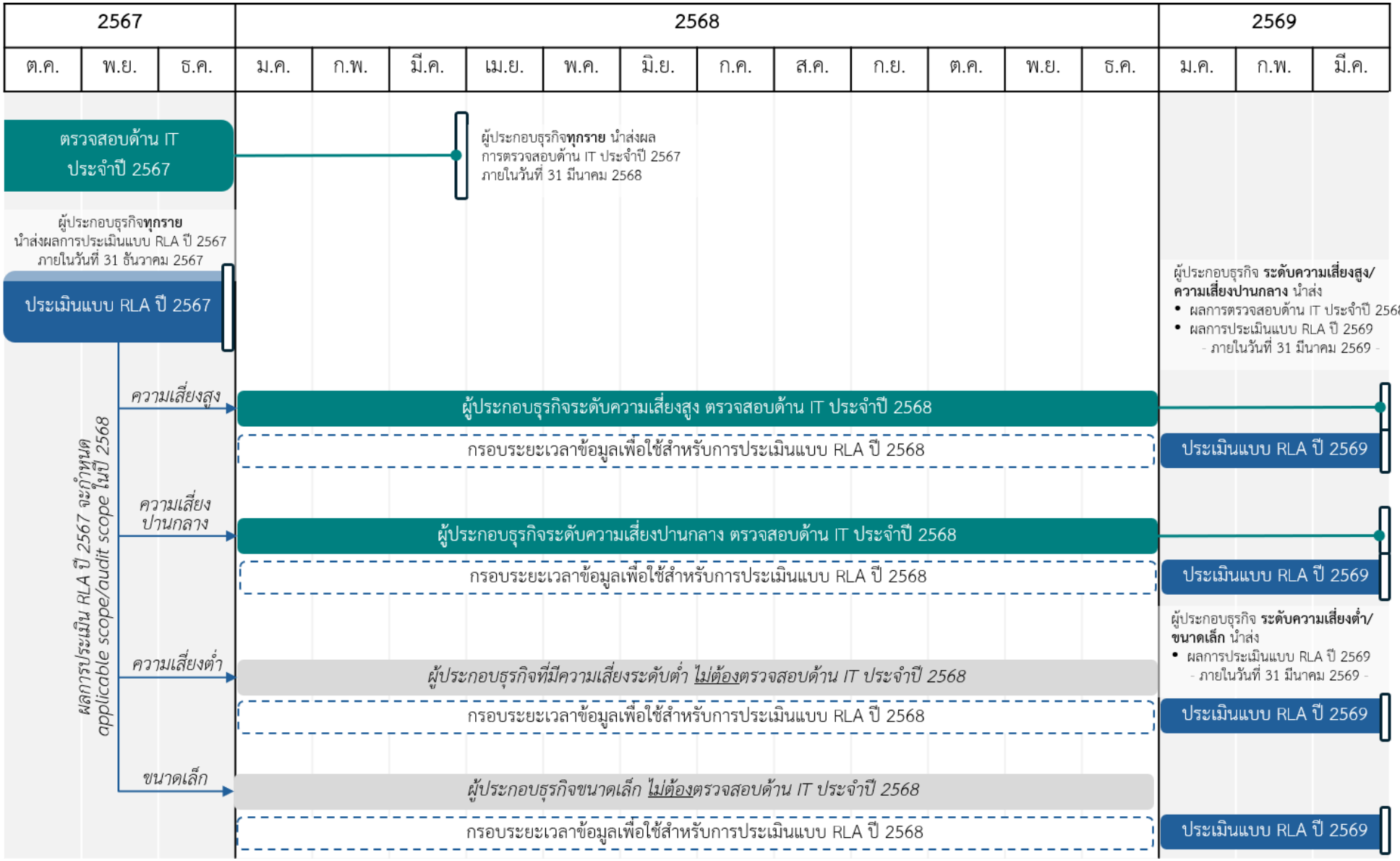
กรณีต้องการติดต่อสอบถามเรื่องข้อกำหนดในรายละเอียดการจัดให้มีระบบเทคโนโลยีสารสนเทศ สามารถติดต่อได้ที่ ฝ่ายกำกับและตรวจสอบความเสี่ยงด้านเทคโนโลยีสารสนเทศ อีเมล cyberteam@sec.or.th

ข้อกำหนดในรายละเอียดการจัดให้มีระบบเทคโนโลยีสารสนเทศ และเอกสารที่เกี่ยวข้อง
สามารถดาวน์โหลดเอกสารทั้งหมดได้ที่ Link
(1) ประกาศสำนักงาน ก.ล.ต. ที่ สธ. 38/2565 ฉบับประมวล ประกาศสำนักงาน ก.ล.ต. ที่ สธ. 38/2565 เรื่อง ข้อกำหนดในรายละเอียดเกี่ยวกับการจัดให้มีระบบเทคโนโลยีสารสนเทศ ซึ่งแก้ไขเพิ่มเติมโดยประกาศสำนักงาน ก.ล.ต. ที่ สธ. 33/2567 เรื่อง ข้อกำหนดในรายละเอียดเกี่ยวกับการจัดให้มีระบบเทคโนโลยีสารสนเทศ (ฉบับที่ 2) ● ประกาศสำนักงาน ก.ล.ต. ที่ สธ. 38/2565 เรื่อง ข้อกำหนดในรายละเอียดเกี่ยวกับการจัดให้มีระบบเทคโนโลยีสารสนเทศ ● ประกาศสำนักงาน ก.ล.ต. ที่ สธ. 33/2567 เรื่อง ข้อกำหนดในรายละเอียดเกี่ยวกับการจัดให้มีระบบเทคโนโลยีสารสนเทศ (ฉบับที่ 2)
● ภาคผนวก 1 : คำศัพท์ (แนบท้ายประกาศที่ สธ. 33/2567)
● ภาคผนวก 2 : การกำกับดูแลและบริหารจัดการด้านเทคโนโลยีสารสนเทศ (Information Technology Governance) (แนบท้ายประกาศที่ สธ. 33/2567)
● ภาคผนวก 3 : การรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (Information Technology Security) (แนบท้ายประกาศที่ สธ. 33/2567)
● ภาคผนวก 4 : การตรวจสอบด้านเทคโนโลยีสารสนเทศ (Information Technology Audit) (แนบท้ายประกาศที่ สธ. 33/2567)
(2) ประกาศแนวปฏิบัติ ที่ นป. 6/2567 เรื่อง แนวปฏิบัติในการจัดให้มีระบบเทคโนโลยีสารสนเทศ ● ภาคผนวกแนบท้ายประกาศที่ นป. 6/2567
(3) หนังสือเวียน ที่ กลต.ตท.(ว) 8/2566 เรื่อง ซักซ้อมความเข้าใจเกี่ยวกับการจัดส่งข้อมูล ตามข้อกำหนดในรายละเอียดเกี่ยวกับการจัดให้มีระบบเทคโนโลยีสารสนเทศ หมายเหตุ : รอบการจัดส่ง (1) แบบ RLA และ (2) รายงานผลการตรวจสอบด้าน IT และแผนการปรับปรุงแก้ไขข้อบกพร่อง เป็นไปตามข้อกำหนดของประกาศฉบับแก้ไขเพิ่มเติม คือ ภายในวันที่ 31 มีนาคม ของทุกปี ทั้งนี้ รูปแบบและวิธีการจัดส่งข้อมูล การแจ้งเตือน และการดำเนินการ กรณีที่ผู้ประกอบธุรกิจไม่สามารถจัดส่งข้อมูลภายในระยะเวลาที่กำหนด ยังคงเป็นไปตามที่หนังสือเวียน ที่ กลต.ตท.(ว) 8/2566 กำหนด
(4) ประเด็นคำถามที่ถามบ่อย (FAQ)
(5) แบบ RLA (Risk Level Assessment) ● คำอธิบายประกอบการจัดทำแบบ RLA หมายเหตุ : สำนักงานจะมีการปรับปรุงแบบ RLA ปีละ 1 ครั้ง ขอให้ผู้ประกอบธุรกิจติดตามแบบ RLA ประจำปีเมื่อถึงรอบการประเมิน
(6) แบบรายงานผลการตรวจสอบด้านเทคโนโลยีสารสนเทศและแผนการปรับปรุงแก้ไขข้อบกพร่อง (แบบรายงานผล IT Audit) ● คำอธิบายประกอบการจัดทำแบบรายงานผล IT Audit ● เอกสารแนบ คำอธิบายประกอบการจัดทำแบบรายงานผล IT Audit หมายเหตุ : สำนักงานจะมีการปรับปรุงแบบรายงานผล IT Audit ปีละ 1 ครั้ง ขอให้ผู้ประกอบธุรกิจติดตามแบบรายงานผล IT Audit ประจำปีเมื่อถึงรอบการตรวจสอบ

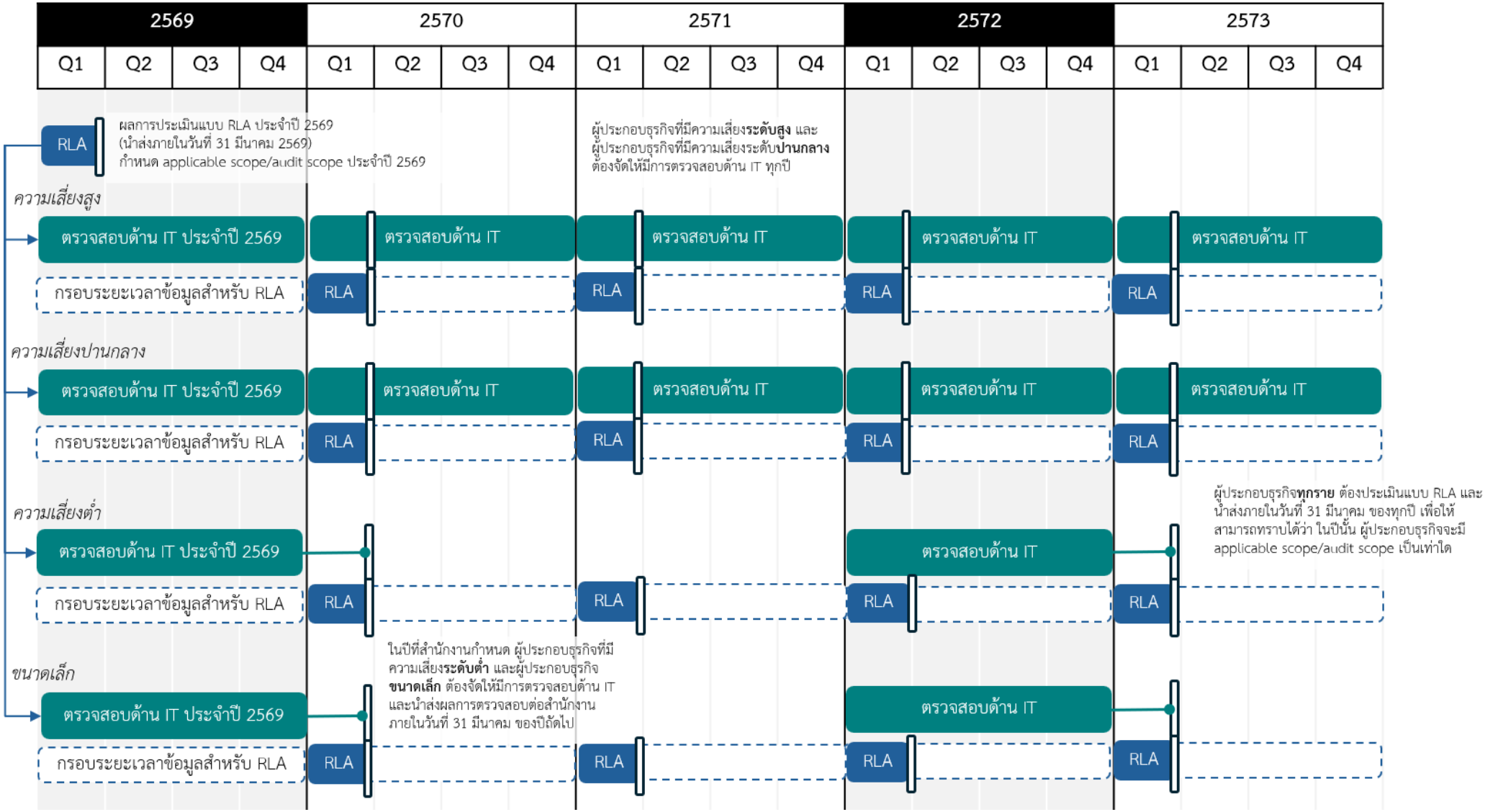
ภาคผนวก ก.

ข้อกำหนดที่ผู้ประกอบธุรกิจต้องปฏิบัติและจัดให้มีการตรวจสอบด้าน IT

ผลการประเมินแบบ RLA	การประเมินแบบ RLA	การตรวจสอบด้าน IT	ข้อกำหนดแนวปฏิบัติขั้นต้น (cyber hygiene)	ข้อกำหนดทุกข้อ **ยกเว้น**ข้อที่ระบุว่า [ความเสี่ยงสูง]	ข้อกำหนดที่ระบุว่า [ความเสี่ยงสูง]
ผู้ประกอบธุรกิจขนาดเล็ก	ทุกปี	อย่างน้อยทุก 3 ปี **	✓		
ผู้ประกอบธุรกิจที่มีความเสี่ยงระดับต่ำ	ทุกปี	อย่างน้อยทุก 3 ปี **	✓	✓	
ผู้ประกอบธุรกิจที่มีความเสี่ยงระดับปานกลาง	ทุกปี	อย่างน้อยปีละ 1 ครั้ง	✓	✓	
ผู้ประกอบธุรกิจที่มีความเสี่ยงระดับสูง	ทุกปี	อย่างน้อยปีละ 1 ครั้ง	✓	✓	✓
หมายเหตุ ** กรณีที่เกิดเหตุการณ์ด้านความมั่นคงปลอดภัยของระบบ IT อย่างมีนัยสำคัญผู้ประกอบธุรกิจขนาดเล็กและผู้ประกอบธุรกิจที่มีความเสี่ยงระดับต่ำ ต้องจัดให้มีการดำเนินการตรวจสอบด้าน IT แบบเต็มรูปแบบ (full scope) ภายในปีที่เกิดเหตุการณ์ดังกล่าว					



ภาพประกอบที่ 2 กำหนดการประเมินแบบ RLA และการตรวจสอบด้าน IT สำหรับปี 2568



ภาพประกอบที่ 3 ตัวอย่างการนับปีที่ต้องจัดให้มีการตรวจสอบด้าน IT
กรณีผู้ประกอบธุรกิจประเมินแบบ RLA ในแต่ละปีและไม่มีการเปลี่ยนแปลงระดับความเสี่ยง

ภาคผนวก ข.

สรุปการแก้ไขรายละเอียดอื่น ๆ ของหลักเกณฑ์ IT

หัวข้อ	ข้อ	รายละเอียดที่แก้ไข	การแก้ไข
ประกาศที่ สธ. 38/2565 ซึ่งแก้ไขเพิ่มเติมโดยประกาศที่ สธ. 33/2567			
ปรับปรุงขอบเขตการบังคับใช้หลักเกณฑ์ IT สำหรับผู้ประกอบธุรกิจการเป็นที่ปรึกษาการลงทุนและผู้ประกอบธุรกิจการเป็นที่ปรึกษาสัญญาซื้อขายล่วงหน้า (บลป.)	1-3	● การเป็นที่ปรึกษาสัญญาซื้อขายล่วงหน้าที่มีการใช้เทคโนโลยีเพื่อการติดต่อหรือให้บริการแก่ลูกค้า ● การเป็นที่ปรึกษาการลงทุนที่มีการใช้เทคโนโลยีเพื่อการติดต่อหรือให้บริการแก่ลูกค้า “เทคโนโลยีเพื่อการติดต่อหรือให้บริการแก่ลูกค้า” หมายความว่า เทคโนโลยีหรือคอมพิวเตอร์ที่มีการใช้งานเพื่อดำเนินการอย่างหนึ่งอย่างใดดังต่อไปนี้ (1) การติดต่อลูกค้า (2) การจัดทำหรือนำส่งข้อมูลบริการหรือผลิตภัณฑ์ให้แก่ลูกค้า (3) การประมวลผล วิเคราะห์ ออกผลลัพธ์หรือคำแนะนำ เพื่อให้ลูกค้าใช้ประกอบการตัดสินใจลงทุน	แก้ไขขอบเขตและเพิ่มนิยาม
กำหนดการประเมินและนำส่งแบบ RLA	4	เพื่อประโยชน์ในการปฏิบัติตามหลักเกณฑ์ที่กำหนดในประกาศนี้ ให้ผู้ประกอบธุรกิจประเมินระดับความเสี่ยงเกี่ยวกับระบบเทคโนโลยีสารสนเทศซึ่งส่งผลต่อการดำเนินธุรกิจของผู้ประกอบธุรกิจตามแบบ RLA (Risk Level Assessment) และจัดส่งผลการประเมินดังกล่าวต่อสำนักงาน ภายในไตรมาสที่ 1 ของทุกปีปฏิทิน ทั้งนี้ ตามแบบและวิธีการที่กำหนดไว้บนเว็บไซต์ของสำนักงาน	แก้ไขรอบวันที่นำส่ง
ภาคผนวก 1 คำศัพท์			
นิยาม “บุคคลภายนอก”	-	หมายความว่า บุคคลภายนอกที่มีความเกี่ยวข้องกับผู้ประกอบธุรกิจดังนี้ แต่ไม่รวมถึงลูกค้าที่ใช้บริการหรือผลิตภัณฑ์ของผู้ประกอบธุรกิจ (1) ผู้ให้บริการงานด้าน IT (2) ผู้ที่มีการเชื่อมต่อกับระบบ IT ของผู้ประกอบธุรกิจ (3) ผู้ที่สามารถเข้าถึงข้อมูลสำคัญของผู้ประกอบธุรกิจหรือข้อมูลของลูกค้าที่อยู่ในรูปแบบอิเล็กทรอนิกส์และอยู่ภายใต้การควบคุมดูแลของผู้ประกอบธุรกิจ	แก้ไข

หัวข้อ	ข้อ	รายละเอียดที่แก้ไข	การแก้ไข
นิยาม “เหตุการณ์ด้านความมั่นคงปลอดภัยของระบบ IT อย่างมีนัยสำคัญ”	-	หมายความว่า เหตุการณ์ด้านความมั่นคงปลอดภัยของระบบ IT ที่เกิดขึ้นแล้วส่งผลกระทบดังนี้ (1) ทำให้ระบบ IT หรือข้อมูลที่จัดเก็บ ประมวลผล หรือส่งต่อ สูญเสียคุณสมบัติด้านความถูกต้องครบถ้วน (integrity) สภาพพร้อมใช้งาน (availability) หรือการธำรงไว้ซึ่งความลับ (confidentiality) อย่างมีนัยสำคัญ *หรือ* (2) ทำให้เกิดการละเมิดหรือมีความเสี่ยงที่อาจทำให้เกิดการละเมิดต่อข้อกำหนดขององค์กรหรือกฎหมาย เช่น - ระบบ IT ของผู้ประกอบธุรกิจถูกบุกรุกหรือโจมตีสำเร็จ (successfully attacked หรือ system compromised) - เหตุการณ์ DDoS ที่ส่งผลให้ระบบของผู้ประกอบธุรกิจเกิดการหยุดชะงัก - ระบบ IT หยุดชะงัก ไม่สามารถให้บริการได้เป็นระยะเวลานานจนส่งผลกระทบต่อลูกค้าของผู้ประกอบธุรกิจในวงกว้าง - เหตุการณ์ข้อมูลสำคัญของผู้ประกอบธุรกิจหรือข้อมูลส่วนบุคคลที่อยู่ภายใต้การควบคุมดูแลของผู้ประกอบธุรกิจรั่วไหล (data breach) ซึ่งส่งผลกระทบอย่างมีนัยสำคัญ - เหตุการณ์ insider threat ทั้งด้วยเจตนา และไม่เจตนา จนเป็นเหตุให้ทรัพย์สินหรือข้อมูลของลูกค้าเสียหายหรือสูญหาย - หน้าเว็บไซต์ของบริษัทโดนปลอมแปลง (website defacement) เป็นต้น	เพิ่มเติม
ภาคผนวก 2 การกำกับดูแลและบริหารจัดการด้านเทคโนโลยีสารสนเทศ (Information Technology Governance)			
ส่วนที่ 1 บทบาทหน้าที่และความรับผิดชอบของคณะกรรมการของผู้ประกอบธุรกิจ	1.5	**[แนวปฏิบัติ]** 1. กรรมการของผู้ประกอบธุรกิจควรได้รับการสร้างความรู้และความตระหนักด้านความเสี่ยงด้าน IT อย่างเพียงพอตามระยะเวลาที่เหมาะสม เพื่อให้เท่าทันกับภัยคุกคามใหม่ และสภาพแวดล้อมด้าน IT ที่เปลี่ยนแปลงไป	เพิ่มเติม
	1.6	การติดตาม ตรวจสอบ และรายงานผลการปฏิบัติงานเพื่อให้เป็นไปตามนโยบายในข้อ 1.3 ต่อคณะกรรมการของผู้ประกอบธุรกิจ <u>หรือคณะกรรมการที่ได้รับมอบหมายจากคณะกรรมการของผู้ประกอบธุรกิจเฉพาะกรณีเป็นสาขาของธนาคารพาณิชย์ต่างประเทศ</u> โดยมีการรายงานอย่างน้อยปีละ 1 ครั้ง และในกรณีที่มีเหตุการณ์หรือการเปลี่ยนแปลงใด ๆ ซึ่งอาจส่งผลกระทบอย่างมีนัยสำคัญต่อการปฏิบัติงานเพื่อให้เป็นไปตามนโยบายดังกล่าว ต้องมีการรายงานให้คณะกรรมการของผู้ประกอบธุรกิจ <u>หรือคณะกรรมการที่ได้รับมอบหมายจากคณะกรรมการของผู้ประกอบธุรกิจเฉพาะกรณีเป็นสาขาของธนาคารพาณิชย์ต่างประเทศ</u> ทราบโดยไม่ชักช้าด้วย	แก้ไข

หัวข้อ	ข้อ	รายละเอียดที่แก้ไข	การแก้ไข
ส่วนที่ 2 การกำกับดูแลและบริหารจัดการความเสี่ยงด้าน IT ในระดับองค์กร	2.3.2	**[แนวปฏิบัติ]** ทั้งนี้ ผู้มีอำนาจในการอนุมัติยกเว้น ไม่ควรเป็นบุคคลที่อาจก่อให้เกิดความขัดแย้งทางผลประโยชน์ (conflict of interest) และการกำหนดผู้มีอำนาจอนุมัติยกเว้น ควรเป็นไปตามหลักการบริหารจัดการความเสี่ยงที่ดี (good governance) อย่างไรก็ดี ผู้ประกอบธุรกิจสามารถให้ผู้บริหารของฝ่ายงาน เช่น Head of IT เป็นต้น เป็นผู้อนุมัติยกเว้นได้ กรณีที่การอนุมัติยกเว้นนั้นได้รับการประเมินแล้วว่ามีความเสี่ยงต่ำ และผู้บริหารของฝ่ายงานดังกล่าว ได้รับการอนุมัติจากคณะกรรมการหรือผู้บริหารระดับสูงของผู้ประกอบธุรกิจเป็นการล่วงหน้า (pre-authorized) ให้เป็นผู้ที่สามารถอนุมัติยกเว้นข้อกำหนดที่มีความเสี่ยงต่ำได้ โดยผู้ประกอบธุรกิจควรรายงานการอนุมัติยกเว้นดังกล่าวให้คณะกรรมการหรือผู้บริหารระดับสูงที่เกี่ยวข้องทราบ ตามกรอบระยะเวลาที่เหมาะสม	เพิ่มเติม
ภาคผนวก 3 การรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (Information Technology Security)			
ส่วนที่ 2 การบริหารจัดการบุคลากร และบุคคลภายนอก	2.2(3)	**[แนวปฏิบัติ]** (4) ข้อตกลงระดับการให้บริการด้าน IT (service level agreement : SLA) สำหรับการใช้บริการจากบุคคลภายนอก และความรับผิดชอบต่อความเสียหายที่เกิดจากบุคคลภายนอก เช่น กรณีการให้บริการที่ไม่เป็นไปตาม SLA ที่กำหนดไว้ เป็นต้น	แก้ไข (รวมข้อ)
		[แนวปฏิบัติ] (9) การจัดให้มีทรัพยากร เช่น บุคลากร ระบบงาน และเทคโนโลยี เป็นต้น ที่สอดรับกับแผนฉุกเฉินด้าน IT ของผู้ประกอบธุรกิจ (Recovery Point Objective (RPO) Maximum Tolerable Downtime (MTD) และ Recovery Time Objective (RTO))	แก้ไข
	2.2(5)	**[แนวปฏิบัติ]** 1. non-disclosure agreement ควรมีรายละเอียดครอบคลุม (1) ขอบเขตความรับผิดชอบในการเก็บรักษาความลับ การไม่เปิดเผยข้อมูลโดยไม่ได้รับอนุญาต (2) การรายงานผู้ประกอบธุรกิจเมื่อพบการรั่วไหลหรือเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต และ (3) การทำลายข้อมูลที่มีความสำคัญเมื่อสิ้นสุดข้อตกลงหรือสัญญา ทั้งนี้ non-disclosure agreement อาจกำหนดไว้เป็นส่วนหนึ่งของสัญญาหรือข้อตกลงกับบุคคลภายนอกได้	แก้ไข
	2.2(7)	รักษาความมั่นคงปลอดภัยด้าน IT จากการใช้บริการ การเชื่อมต่อ หรือการเข้าถึงข้อมูลจากบุคคลภายนอก ที่สอดคล้องกับการรักษาความมั่นคงปลอดภัยด้าน IT ของผู้ประกอบธุรกิจ หรือสอดคล้องกับมาตรฐานสากลที่ได้รับการยอมรับโดยทั่วไป	แก้ไข
ส่วนที่ 4 การรักษาความมั่นคงปลอดภัยของข้อมูล (data security)	4.4	**[แนวปฏิบัติ]** 2. ผู้ประกอบธุรกิจควรปรับปรุงทรัพย์สินด้าน IT ประเภทข้อมูล (data Inventory) ให้ครบถ้วนและเป็นปัจจุบันอย่างสม่ำเสมอ อย่างน้อยปีละ 1 ครั้ง และทุกครั้งที่มีการเปลี่ยนแปลงระบบ IT อย่างมีนัยสำคัญ	เพิ่มเติม

หัวข้อ	ข้อ	รายละเอียดที่แก้ไข	การแก้ไข
ส่วนที่ 5 การควบคุมการเข้าถึงข้อมูลและระบบ IT (access control)	5.3.3	**[แนวปฏิบัติ]** 1. ผู้ประกอบธุรกิจควรจัดให้มีการควบคุมและติดตามการใช้งานบัญชี privileged user ดังนี้ ... (6) จัดเก็บบันทึกการเข้าถึง (access log) และการดำเนินงาน (activity log) ของบัญชี privileged user อย่างเหมาะสม (7) สอบทานบันทึกการเข้าถึง (access log) และการดำเนินงาน (activity log) ของบัญชี privileged user หลังเสร็จสิ้นการใช้งาน หรือสอบทานอย่างสม่ำเสมอตามรอบระยะเวลาที่เหมาะสมกับความเสี่ยง โดยควรสอบทานอย่างน้อยปีละ 1 ครั้ง เพื่อให้มั่นใจได้ว่าการใช้งานสิทธิเป็นไปอย่างเหมาะสม ...	แก้ไข
ส่วนที่ 8 การรักษาความมั่นคงปลอดภัยในการปฏิบัติงานด้าน IT (IT operation security)	8.4	การรักษาความมั่นคงปลอดภัยของเครื่องแม่ข่าย (server) และอุปกรณ์ที่ใช้ปฏิบัติงาน (endpoint) ให้สามารถป้องกันการโจมตีด้วยรูปแบบต่าง ๆ หรือภัยจากโปรแกรมไม่ประสงค์ดี (malware) เพื่อลดความเสี่ยงจากการถูกโจมตีระบบ IT ขององค์กร หรือถูกใช้เป็นช่องทางในการโจมตีหน่วยงานอื่น และป้องกันการรั่วไหลของข้อมูลสำคัญ หรือการเข้าใช้งานระบบ IT โดยไม่ได้รับอนุญาต	แก้ไข
	8.7	**[แนวปฏิบัติ]** 1. ผู้ประกอบธุรกิจควรจัดเก็บข้อมูลบันทึกเหตุการณ์ (log) ด้วยวิธีการที่ปลอดภัย โดยมีรายละเอียดครบถ้วนเพียงพอที่จะใช้เป็นหลักฐานในการตรวจสอบที่สามารถระบุตัวบุคคลผู้กระทำได้ และจัดเก็บเป็นระยะเวลาอย่างน้อย 90 วัน หรือจัดเก็บตามกฎหมายที่เกี่ยวข้องกำหนด ประกอบด้วยรายการหลักฐานอย่างน้อย ดังนี้ ... (2) บันทึกการเข้าถึง (access log) ของเครื่องแม่ข่าย ระบบงาน อุปกรณ์เครือข่าย และข้อมูลที่มีความสำคัญ โดยรวมถึงความพยายามในการเข้าสู่ระบบ (log-in attempt) (3) บันทึกการดำเนินงาน (activity log) ที่สำคัญ โดยอย่างน้อยครอบคลุม (ก) การเปลี่ยนแปลงแก้ไขโครงสร้างฐานข้อมูล (database schema log) และการเปลี่ยนแปลงแก้ไขข้อมูลในตารางที่สำคัญ ... (ง) การใช้งานอินเทอร์เน็ตผ่านระบบเครือข่ายของผู้ประกอบธุรกิจ (internet traffic log) ...	แก้ไข
		[แนวปฏิบัติ] (5) บันทึกการทำธุรกรรม (transaction log) ควรมีระยะเวลาจัดเก็บขั้นต่ำ 1 ปี โดยในกรณีที่เป็นระบบ IT เพื่อการซื้อขายหลักทรัพย์ (trading system) ให้บันทึกบัญชีผู้ใช้งาน / ข้อมูลรายละเอียดชื่อย่อหลักทรัพย์ (securities symbol) / หมายเลขบริษัทสมาชิก (broker No. 4 หลัก : xxxx) / เลขที่คำสั่งซื้อขายหลักทรัพย์ (SET order ID) / เลขที่บัญชีซื้อขายหลักทรัพย์ (account ID) / วันและเวลาในการส่งคำสั่งซื้อขายหลักทรัพย์ (yyyy/mm/dd – hh:mm:ss:sss) /	เพิ่มเติม

หัวข้อ	ข้อ	รายละเอียดที่แก้ไข	การแก้ไข
		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 ทั้งนี้ ให้ผู้ประกอบธุรกิจจัดทำและนำส่งข้อมูลเพิ่มเติมต่อสำนักงาน ตามรูปแบบและวิธีการที่สำนักงานกำหนดโดยไม่ชักช้าเมื่อสำนักงานร้องขอ โดยข้อมูลบันทึกการทำธุรกรรมเพิ่มเติม (additional transaction log) ที่ผู้ประกอบธุรกิจควรพร้อมจัดทำและนำส่งต่อสำนักงานเมื่อสำนักงานร้องขอ ควรมีรายละเอียดขั้นต่ำ ดังนี้ (ก) บัญชีผู้ใช้งาน (user ID) (ข) เลขบัตรประจำตัวประชาชนหรือเลขทะเบียนนิติบุคคลของลูกค้า (ค) ชื่อ-นามสกุลของลูกค้า (ง) วันและเวลาที่จับคู่คำสั่งซื้อขายได้ (matched date : yyyy/mm/dd – hh:mm:ss:sss) (จ) กรณีส่งคำสั่งจากอุปกรณ์ของบริษัทหลักทรัพย์ ให้จัดเก็บข้อมูลที่สามารถระบุได้ว่า คำสั่งซื้อขายจัดส่งจากอุปกรณ์ใด และใครเป็นผู้ใช้งานอุปกรณ์ในขณะที่ส่งคำสั่งนั้น	
	8.8	การติดตามดูแลระบบและเฝ้าระวังภัยคุกคามทางไซเบอร์ (security monitoring) โดยมีกระบวนการหรือเครื่องมือป้องกันและตรวจจับเหตุการณ์ผิดปกติด้าน IT หรือภัยคุกคามทางไซเบอร์ที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยต่อระบบ IT ที่มีนัยสำคัญ	แก้ไข (ตัดคำ)
ส่วนที่ 11 การบริหารจัดการเหตุการณ์ผิดปกติด้าน IT (IT incident management)	11.3	รายงานเหตุการณ์ผิดปกติด้าน IT ต่อผู้มีหน้าที่รับผิดชอบเหตุการณ์ และสำนักงานโดยไม่ชักช้าเมื่อทราบเหตุการณ์ดังกล่าว	แก้ไข (ตัดคำ)
		[แนวปฏิบัติ] 2. ผู้ประกอบธุรกิจควรรายงานสำนักงานในกรณีที่มีเหตุการณ์ผิดปกติด้าน IT ซึ่งอาจส่งผลกระทบต่อการดำเนินงานธุรกิจ ชื่อเสียง ฐานะ ผลการดำเนินงานของผู้ประกอบธุรกิจ หรือลูกค้าในวงกว้าง โดยครอบคลุมเหตุการณ์อย่างน้อยดังต่อไปนี้ ... (2) ทรัพย์สินของลูกค้าสูญหาย หรือเสียหาย ...	แก้ไข
ภาคผนวก 4 การตรวจสอบด้าน IT (IT audit)			
3. การตรวจสอบด้าน IT ตามแผนงานและขอบเขตที่กำหนด	3.1	จัดให้มีการตรวจสอบและรายงานผลการตรวจสอบด้าน IT โดยมีรายละเอียดดังนี้ 3.1.1 กรณีเป็นผู้ประกอบธุรกิจขนาดเล็กต้องจัดให้มีการตรวจสอบด้าน IT ที่ครอบคลุมหลักเกณฑ์ทั้งหมดที่บังคับใช้กับผู้ประกอบ	แก้ไข ข้อกำหนด

หัวข้อ	ข้อ	รายละเอียดที่แก้ไข	การแก้ไข
		ธุรกิจขนาดเล็ก แบบเต็มรูปแบบ (full scope) อย่างน้อยทุก 3 ปี ตามรอบปีที่สำนักงานกำหนด 3.1.2 กรณีเป็นผู้ประกอบธุรกิจที่มีความเสี่ยงระดับต่ำต้องจัดให้มีการตรวจสอบด้าน IT ที่ครอบคลุมหลักเกณฑ์ทั้งหมดที่บังคับใช้กับผู้ประกอบธุรกิจที่มีความเสี่ยงระดับต่ำ แบบเต็มรูปแบบ (full scope) อย่างน้อยทุก 3 ปี ตามรอบปีที่สำนักงานกำหนด ทั้งนี้ กรณีที่เกิดเหตุการณ์ด้านความมั่นคงปลอดภัยของระบบ IT อย่างมีนัยสำคัญ ผู้ประกอบธุรกิจขนาดเล็กและผู้ประกอบธุรกิจที่มีความเสี่ยงระดับต่ำ ต้องจัดให้มีการดำเนินการตรวจสอบด้าน IT แบบเต็มรูปแบบ (full scope) ภายในปีที่เกิดเหตุการณ์ดังกล่าว กรณีที่มีเหตุจำเป็นทำให้ผู้ประกอบธุรกิจขนาดเล็กหรือผู้ประกอบธุรกิจที่มีความเสี่ยงระดับต่ำไม่สามารถดำเนินการตรวจสอบด้าน IT แบบเต็มรูปแบบ (full scope) ภายในปีที่เกิดเหตุการณ์ด้านความมั่นคงปลอดภัยของระบบ IT อย่างมีนัยสำคัญ ผู้ประกอบธุรกิจต้องดำเนินการดังต่อไปนี้ ภายใน 4 เดือน นับแต่วันที่ทราบเหตุการณ์ดังกล่าว (1) รายงานเหตุจำเป็นที่ทำให้ไม่สามารถดำเนินการตรวจสอบด้าน IT แบบเต็มรูปแบบ (full scope) ได้ภายในปีที่เกิดเหตุการณ์ดังกล่าว และแผนการตรวจสอบด้าน IT ต่อคณะกรรมการของผู้ประกอบธุรกิจ หรือคณะกรรมการที่ได้รับมอบหมายจากคณะกรรมการของผู้ประกอบธุรกิจเฉพาะกรณีเป็นสาขาของธนาคารพาณิชย์ต่างประเทศ รวมทั้งรายงานเหตุจำเป็นดังกล่าวต่อสำนักงาน *และ* (2) ดำเนินการตรวจสอบด้าน IT แบบเต็มรูปแบบ (full scope)	และเพิ่มเติมเงื่อนไข
		3.1.3 กรณีเป็นผู้ประกอบธุรกิจที่มีความเสี่ยงระดับปานกลาง ต้องจัดให้มีการตรวจสอบด้าน IT ที่ครอบคลุมหลักเกณฑ์ทั้งหมดที่บังคับใช้กับผู้ประกอบธุรกิจที่มีความเสี่ยงระดับปานกลาง แบบเต็มรูปแบบ (full scope) อย่างน้อยปีละ 1 ครั้ง 3.1.4 กรณีเป็นผู้ประกอบธุรกิจที่มีความเสี่ยงระดับสูง ต้องจัดให้มีการตรวจสอบด้าน IT ที่ครอบคลุมหลักเกณฑ์ทั้งหมดที่บังคับใช้กับผู้ประกอบธุรกิจที่มีความเสี่ยงระดับสูง แบบเต็มรูปแบบ (full scope) อย่างน้อยปีละ 1 ครั้ง	แก้ไข
5. การจัดทำและรายงานผลการตรวจสอบ	5.1	เสนอรายงานผลการตรวจสอบตามข้อ 3. และแผนการปรับปรุงแก้ไขข้อบกพร่องต่อคณะกรรมการของผู้ประกอบธุรกิจ คณะกรรมการตรวจสอบของผู้ประกอบธุรกิจ หรือคณะกรรมการที่ได้รับมอบหมายจากคณะกรรมการของผู้ประกอบธุรกิจเฉพาะกรณีเป็นสาขาของธนาคารพาณิชย์ต่างประเทศ โดยไม่ชักช้า	แก้ไข

หัวข้อ	ข้อ	รายละเอียดที่แก้ไข	การแก้ไข
	5.2	รายงานผลการตรวจสอบและแผนการปรับปรุงแก้ไขข้อบกพร่องที่ผ่านการพิจารณาจากคณะกรรมการของผู้ประกอบธุรกิจ คณะกรรมการตรวจสอบของผู้ประกอบธุรกิจ หรือคณะกรรมการที่ได้รับมอบหมายจากคณะกรรมการของผู้ประกอบธุรกิจเฉพาะกรณีเป็นสาขาของธนาคารพาณิชย์ต่างประเทศ ตามข้อ 5.1 ต่อสำนักงาน ตามรูปแบบและวิธีการที่กำหนดไว้บนเว็บไซต์ของสำนักงาน ภายใน 3 เดือน นับแต่วันสิ้นปีปฏิทินของปีที่ดำเนินการตรวจสอบตามข้อ 3. เว้นแต่ในกรณีที่เป็นผู้ประกอบธุรกิจสินทรัพย์ดิจิทัลที่มีหน้าที่ต้องรายงานผลการตรวจสอบตามประกาศคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ ที่ กธ. 19/2561 เรื่อง หลักเกณฑ์ เงื่อนไขและวิธีการประกอบธุรกิจสินทรัพย์ดิจิทัล ลงวันที่ 3 กรกฎาคม พ.ศ. 2561 ให้ผู้ประกอบธุรกิจสินทรัพย์ดิจิทัลปฏิบัติตามประกาศดังกล่าว	แก้ไข และ เพิ่มเติม
	5.2	**[แนวปฏิบัติ]** กรณีที่ผู้ประกอบธุรกิจจัดทำ และรายงานผลการตรวจสอบและแผนการปรับปรุงแก้ไขข้อบกพร่อง ต่อคณะกรรมการของผู้ประกอบธุรกิจ คณะกรรมการตรวจสอบของผู้ประกอบธุรกิจ หรือคณะกรรมการที่ได้รับมอบหมายจากคณะกรรมการของผู้ประกอบธุรกิจเฉพาะกรณีเป็นสาขาของธนาคารพาณิชย์ต่างประเทศ เสร็จสิ้นภายในปีที่เริ่มตรวจสอบ ผู้ประกอบธุรกิจสามารถนำส่งสำนักงานได้ทันที โดยต้องไม่เกินกำหนดเวลา ภายใน 3 เดือน นับแต่วันสิ้นปีปฏิทินของปีที่เริ่มตรวจสอบ ตัวอย่างเช่น • ผู้ประกอบธุรกิจดำเนินการตรวจสอบรอบปี 2569 เสร็จสิ้นเมื่อวันที่ 1 กรกฎาคม พ.ศ. 2569 และได้เสนอรายงานผลการตรวจสอบและแผนการปรับปรุงแก้ไขข้อบกพร่องต่อคณะกรรมการฯ เมื่อวันที่ 7 กรกฎาคม พ.ศ. 2569 ผู้ประกอบธุรกิจสามารถรายงานสำนักงานได้ตั้งแต่วันที่ 7 กรกฎาคม 2569 จนถึงวันที่ 31 มีนาคม พ.ศ. 2570 เป็นต้น	แก้ไข (ตัวอย่าง)