Version ใช้สำหรับตรวจสอบรอบปี 2569

คำอธิบายประกอบการจัดทำแบบรายงานผลการตรวจสอบด้านเทคโนโลยีสารสนเทศ และแผนการปรับปรุงแก้ไขข้อบกพร่อง

สำนักงาน ก.ล.ต. ได้กำหนดแบบรายงานผลการตรวจสอบด้านเทคโนโลยีสารสนเทศ และแผนการปรับปรุงแก้ไขข้อบกพร่อง (“แบบรายงานผล IT Audit”) เพื่อให้ผู้ประกอบธุรกิจสามารถตรวจประเมินการควบคุมด้านการบริหารจัดการความเสี่ยงทาง IT (IT risk management) และการตอบสนองต่อภัยไซเบอร์อย่างเป็นระบบและมีมาตรฐาน โดยการควบคุมที่ใช้ในการตรวจสอบอ้างอิงตามประกาศสำนักงาน ก.ล.ต. ที่ สธ. 38/2565 (ที่แก้ไขเพิ่มเติมโดยประกาศสำนักงาน ก.ล.ต. ที่ สธ. 33/2567) และแนวปฏิบัติที่ นป. 6/2567 (“ประกาศฯ”)

หัวข้อ **หน้า**

1. โครงสร้างของแบบรายงาน

แบบรายงานผล IT Audit (Excel file) ประกอบด้วยข้อมูลสำคัญ 6 ส่วน ให้ผู้ประกอบธุรกิจกรอกข้อมูลลงใน cell ที่มีสีเหลืองอ่อน (☐) โดยมีรายละเอียด ดังนี้

ส่วนที่	แผ่นงาน (Sheet)	รายละเอียด
1	Basic info	**ข้อมูลพื้นฐานเกี่ยวกับการตรวจสอบ** กรอกข้อมูลเกี่ยวกับการตรวจสอบ ผู้ตรวจสอบ และการรายงานผลการตรวจสอบต่อคณะกรรมการของบริษัทหรือคณะกรรมการตรวจสอบของบริษัท
2	Systems	**ระบบ IT ที่ใช้ในการประกอบธุรกิจ** กรอกข้อมูลเกี่ยวกับผู้ให้บริการ Cloud และ Infrastructure พร้อมทั้งระบบงานและเครื่องมือด้าน IT ที่สนับสนุนฟังก์ชันทางธุรกิจที่สำคัญ หรือมีการใช้งานปริมาณมากสูงสุด 3 อันดับแรก โดยมีวัตถุประสงค์เพื่อให้สำนักงานมีข้อมูลในการติดตามและวิเคราะห์ความเสี่ยงด้าน IT ในภาพรวมของตลาดทุน (เช่น concentration risk เป็นต้น) ตลอดจนสามารถแจ้งเตือนข้อมูลเกี่ยวกับภัยคุกคามทางไซเบอร์ได้มีประสิทธิภาพยิ่งขึ้น
3	Scope	**ระบบ IT ที่อยู่ในขอบเขตของการตรวจสอบ** กรอกข้อมูลรายชื่อระบบ IT ที่อยู่ในขอบเขตของการตรวจสอบครั้งนี้ (IT systems in the audit scope) ทั้งนี้ เพื่อให้การตรวจสอบครอบคลุมถึงระบบ IT ที่สำคัญ สำนักงานได้กำหนดรายชื่อระบบ IT ขั้นต่ำที่ผู้ประกอบธุรกิจแต่ละประเภทต้องพิจารณากำหนดเป็นขอบเขตของการตรวจสอบ (รายละเอียดตามข้อ 3 ขอบเขตของการตรวจสอบ (Audit scope))
4	D1-D3	**ผลการตรวจสอบ** กรอกข้อมูลผลการตรวจสอบการควบคุมตามแต่ละรายการ โดยการตรวจสอบมี 2 รูปแบบ ได้แก่ (1) การวัดการปฏิบัติตามข้อกำหนด (compliance check) (2) การวัดระดับความพร้อม (maturity level) (รายละเอียดตามข้อ 4 การตรวจสอบ)
5	Finding	**สรุปประเด็นข้อตรวจพบ/ข้อบกพร่อง** กรอกข้อมูลประเด็นข้อตรวจพบ/ข้อบกพร่อง พร้อมกับแผนการแก้ไข โดยแบ่งระดับความสำคัญของข้อตรวจพบ/ข้อบกพร่อง เป็น 3 ระดับ ได้แก่ (1) ความสำคัญระดับสูง (2) ความสำคัญระดับปานกลาง (3) ความสำคัญระดับต่ำ (รายละเอียดตามข้อ 5 การสรุปประเด็นข้อตรวจพบ/ข้อบกพร่อง (Finding))
6	Result	**สรุปผลการตรวจสอบในภาพรวม** (ไม่ต้องกรอกข้อมูล) Excel จะประมวลผลการตรวจสอบในภาพรวมอัตโนมัติ โดยเชื่อมโยงข้อมูลผลการตรวจสอบใน Sheet D1-D3 และแสดงผลในรูปแบบตารางและกราฟ เพื่อให้ผู้ประกอบธุรกิจสามารถนำไปใช้ประยุกต์ใช้ประโยชน์ได้ (รายละเอียดตามข้อ 6 การสรุปผลการตรวจสอบในภาพรวม)

2. หลักเกณฑ์ที่ใช้ในการตรวจสอบ (Audit criteria)

แผ่นงาน D1-D3 ประกอบด้วย column “H” “M” “L” และ “S” ซึ่งใช้กำหนดว่า ผู้ประกอบธุรกิจในแต่ละระดับความเสี่ยงต้องมีการตรวจประเมินการควบคุม (control) ในข้อใดบ้าง

- Column “H” ที่มีเครื่องหมาย “x” หมายถึง การควบคุมสำหรับผู้ประกอบธุรกิจที่มีความเสี่ยงระดับสูง
- Column “M” ที่มีเครื่องหมาย “x” หมายถึง การควบคุมสำหรับผู้ประกอบธุรกิจที่มีความเสี่ยงระดับปานกลาง
- Column “L” ที่มีเครื่องหมาย “x” หมายถึง การควบคุมสำหรับผู้ประกอบธุรกิจที่มีความเสี่ยงระดับต่ำ
- Column “S” ที่มีเครื่องหมาย “x” หมายถึง การควบคุมสำหรับผู้ประกอบธุรกิจขนาดเล็ก

[New] ผู้ประกอบธุรกิจต้องจัดให้มีการตรวจสอบแบบเต็มรูปแบบ (full scope) ตามรอบดังต่อไปนี้

ระดับความเสี่ยงที่ได้จากการประเมินแบบ RLA	Audit criteria
ระดับความเสี่ยงสูง	ตรวจสอบการปฏิบัติตาม control ของผู้ประกอบธุรกิจที่มีความเสี่ยงระดับสูงทุกปี
ระดับความเสี่ยงปานกลาง	ตรวจสอบการปฏิบัติตาม control ของผู้ประกอบธุรกิจที่มีความเสี่ยงระดับปานกลางทุกปี
ระดับความเสี่ยงต่ำ	ตรวจสอบการปฏิบัติตาม control ของผู้ประกอบธุรกิจที่มีความเสี่ยงระดับต่ำ อย่างน้อยทุก 3 ปี ตามรอบปีที่สำนักงานกำหนด*
ผู้ประกอบธุรกิจขนาดเล็ก	ตรวจสอบการปฏิบัติตาม control ของผู้ประกอบธุรกิจขนาดเล็ก อย่างน้อยทุก 3 ปี ตามรอบปีที่สำนักงานกำหนด*

หมายเหตุ *

[1] รอบปีที่สำนักงานกำหนด ให้อ้างอิง หนังสือเวียน ที่ กลต.ตท.(ว) 5225/2567 เรื่อง ซักซ้อมความเข้าใจเกี่ยวกับประกาศข้อกำหนด การจัดให้มีระบบเทคโนโลยีสารสนเทศ (ฉบับแก้ไขเพิ่มเติม) และเอกสารแนบของหนังสือเวียนซักซ้อมดังกล่าว (เข้าถึงได้ที่ Link) ซึ่งได้กำหนดให้รอบปี 2569 เป็นรอบปีเริ่มต้นที่ผู้ประกอบธุรกิจขนาดเล็ก และผู้ประกอบที่มีความเสี่ยงระดับต่ำ ต้องจัดให้มีการตรวจสอบด้าน IT ตามข้อกำหนดของประกาศ (จัดให้มีการตรวจสอบรอบปีแรก ระหว่างวันที่ 1 มกราคม 2569 – 31 ธันวาคม 2569) และให้จัดให้มีการตรวจสอบทุกรอบ 3 ปี ดังนี้

พ.ศ.	ปีที่กำหนดให้มีการตรวจสอบด้าน IT
2568	-
2569	จัดให้มีการตรวจสอบด้าน IT
2570	-
2571	-
2572	จัดให้มีการตรวจสอบด้าน IT
2573	-
2574	-

[New] หมายถึง ข้อมูลได้รับการปรับปรุงภายให้เป็นไปตามประกาศสำนักงานคณะกรรมการ ก.ล.ต. ที่ สธ. 33/2567 เรื่อง ข้อกำหนดในรายละเอียดเกี่ยวกับการจัดให้มีระบบเทคโนโลยีสารสนเทศ (ฉบับที่ 2)

พ.ศ.	ปีที่กำหนดให้มีการตรวจสอบด้าน IT
2575	จัดให้มีการตรวจสอบด้าน IT
2576	-
2577	-
2578	จัดให้มีการตรวจสอบด้าน IT
...	...

[2] **กรณีที่เกิดเหตุการณ์ด้านความมั่นคงปลอดภัยของระบบ IT อย่างมีนัยสำคัญ** ผู้ประกอบธุรกิจที่มีความเสี่ยงระดับต่ำ หรือผู้ประกอบธุรกิจขนาดเล็ก ต้องจัดให้มีการดำเนินการตรวจสอบด้าน IT แบบเต็มรูปแบบ (full scope) ภายในปีที่เกิดเหตุการณ์ดังกล่าว กรณีที่มีเหตุจำเป็นทำให้ผู้ประกอบธุรกิจขนาดเล็กหรือผู้ประกอบธุรกิจที่มีความเสี่ยงระดับต่ำ ไม่สามารถดำเนินการตรวจสอบด้าน IT แบบเต็มรูปแบบ (full scope) ภายในปีที่เกิดเหตุการณ์ด้านความมั่นคงปลอดภัยของระบบ IT อย่างมีนัยสำคัญ[2] ผู้ประกอบธุรกิจต้องดำเนินการดังต่อไปนี้ ภายใน 4 เดือน นับแต่วันที่ทราบเหตุการณ์ดังกล่าว

(1) รายงานเหตุจำเป็นที่ทำให้ไม่สามารถดำเนินการตรวจสอบด้าน IT แบบเต็มรูปแบบ (full scope) ได้ภายในปีที่เกิดเหตุการณ์ดังกล่าว และแผนการตรวจสอบด้าน IT ต่อคณะกรรมการของผู้ประกอบธุรกิจหรือคณะกรรมการที่ได้รับมอบหมายจากคณะกรรมการของผู้ประกอบธุรกิจเฉพาะกรณีเป็นสาขาของธนาคารพาณิชย์ต่างประเทศ รวมทั้งรายงานเหตุจำเป็นดังกล่าวต่อสำนักงาน *และ*

(2) ดำเนินการตรวจสอบด้าน IT แบบเต็มรูปแบบ (full scope)

<u>ตัวอย่าง</u> ในปีที่สำนักงาน<u>ไม่ได้</u>กำหนดให้มีการตรวจสอบด้าน IT สำหรับ "ผู้ประกอบธุรกิจที่มีความเสี่ยงระดับต่ำ" หรือ "ผู้ประกอบธุรกิจขนาดเล็ก"

- ผู้ประกอบธุรกิจประเมินแบบ RLA รอบปี 2567 เป็น "ผู้ประกอบธุรกิจที่มีความเสี่ยงระดับต่ำ" หรือ "ผู้ประกอบธุรกิจขนาดเล็ก" ดังนั้น ในปี 2568 ผู้ประกอบธุรกิจไม่ต้องจัดให้มีการตรวจสอบด้าน IT อ้างอิงตามตารางรอบปีที่สำนักงานกำหนดในหนังสือเวียนซักซ้อม
- อย่างไรก็ดี กรณีระหว่างปี 2568 "ผู้ประกอบธุรกิจที่มีความเสี่ยงระดับต่ำ" หรือ "ผู้ประกอบธุรกิจขนาดเล็ก" ดังกล่าวเกิดเหตุการณ์ด้านความมั่นคงปลอดภัยของระบบ IT อย่างมีนัยสำคัญ ผู้ประกอบธุรกิจจำเป็นต้องดำเนินการตรวจสอบในปี 2568 และต้องนำส่งรายงานผลการตรวจสอบดังกล่าวต่อสำนักงาน ภายในวันที่ 31 มีนาคม 2569 ด้วย

[2] เหตุการณ์ด้านความมั่นคงปลอดภัยของระบบ IT อย่างมีนัยสำคัญ อ้างอิงตามภาคผนวก 1 แนบท้ายประกาศที่ สธ. 38/2565 (ที่แก้ไขเพิ่มเติมโดยประกาศที่ สธ. 33/2567)

<u>ตัวอย่าง</u> ในปีที่สำนักงานกำหนดให้<u>มี</u>การตรวจสอบด้าน IT สำหรับ "ผู้ประกอบธุรกิจที่มีความเสี่ยงระดับต่ำ" หรือ "ผู้ประกอบธุรกิจขนาดเล็ก"

- ผู้ประกอบธุรกิจประเมินแบบ RLA รอบปี 2569 (กำหนดการนำส่ง RLA ภายใน 31 มีนาคม 2569) เป็น "ผู้ประกอบธุรกิจที่มีความเสี่ยงระดับต่ำ" หรือ "ผู้ประกอบธุรกิจขนาดเล็ก" ในปี 2569 <u>ต้องจัดให้มีการตรวจสอบด้าน IT รอบปี 2569</u> เนื่องด้วยเป็นรอบปีที่สำนักงานกำหนดให้มีการตรวจสอบ โดยรายงานผลการตรวจสอบ IT รอบปี 2569 ดังกล่าว ต้องนำส่งสำนักงาน ภายในวันที่ 31 มีนาคม 2570

หมายเหตุ : ผู้ประกอบธุรกิจสินทรัพย์ดิจิทัล ยังคงต้องปฏิบัติตามข้อกำหนดของประกาศ กธ. 19/2561
ผู้ประกอบธุรกิจสินทรัพย์ดิจิทัล (เช่น ที่ปรึกษาคริปโทเคอร์เรนซี ที่ปรึกษาโทเคนดิจิทัล เป็นต้น) ยังคงมีหน้าที่ปฏิบัติตามข้อกำหนดของประกาศ กธ. 19/2561 เรื่อง หลักเกณฑ์ เงื่อนไข และวิธีการประกอบธุรกิจสินทรัพย์ดิจิทัล ซึ่งกำหนดให้ "ผู้ประกอบธุรกิจสินทรัพย์ดิจิทัลต้องจัดให้มีการตรวจสอบด้านเทคโนโลยีสารสนเทศ (IT audit) ก่อนเริ่มให้บริการและภายหลังเริ่มให้บริการแล้วอย่างน้อยปีละ 1 ครั้งโดยผู้ที่มีความรู้ ความสามารถและเป็นอิสระ และรายงานผลต่อสำนักงาน ก.ล.ต. ภายใน 30 วันนับจากวันที่ได้รับผลการทดสอบอย่างเป็นทางการ แต่ไม่เกิน 90 วันนับจากวันที่สิ้นสุดกระบวนการทดสอบ" แม้ผลการประเมินแบบ RLA ผู้ประกอบธุรกิจสินทรัพย์ดิจิทัลจะเป็นผู้ประกอบธุรกิจขนาดเล็ก ผู้ประกอบธุรกิจสินทรัพย์ดิจิทัลยังคงมีหน้าที่ในการตรวจสอบปีละ 1 ครั้ง และต้องนำส่งสำนักงาน ตามเงื่อนไขของประกาศ กธ. 19/2561

3. ขอบเขตในการตรวจสอบ (Audit scope)

ขอบเขตในการตรวจสอบต้องครอบคลุมระบบ IT ที่มีนัยสำคัญ[3] ซึ่งใช้เพื่อการประกอบธุรกิจที่ได้รับใบอนุญาตจากสำนักงาน ก.ล.ต. และอยู่ภายใต้การบังคับใช้ตามประกาศฯ

ทั้งนี้ เพื่อให้ผู้ประกอบธุรกิจมีการตรวจสอบระบบ IT ที่มีนัยสำคัญได้อย่างครอบคลุมและมีมาตรฐาน สำนักงาน ก.ล.ต. จึงได้กำหนดรายชื่อระบบ IT ที่ผู้ประกอบธุรกิจแต่ละประเภทควรพิจารณากำหนดไว้เป็นขอบเขตในการตรวจสอบในแต่ละปี โดยมีรายละเอียด ดังนี้

ประเภทผู้ประกอบธุรกิจ	ระบบงานสำคัญที่ควรอยู่ในขอบเขตการตรวจสอบ	คำอธิบาย
[บล.] นายหน้าซื้อขาย / ค้า /จัดจำหน่ายหลักทรัพย์	ระบบรับส่งคำสั่งซื้อขาย (Front Office : OMS)	ระบบสำหรับรับส่งคำสั่งซื้อขายหลักทรัพย์จากลูกค้าไปยังศูนย์ซื้อขายหลักทรัพย์ (Trading Venue) และตัวแทนซื้อขายในต่างประเทศ (oversea brokers & dealers)
	ระบบ Back Office	ระบบที่เกี่ยวข้องกับการจัดการข้อมูลลูกค้า ข้อมูลการซื้อขาย การชำระราคาและส่งมอบหลักทรัพย์ระหว่างบริษัท ธุรกรรมกับลูกค้าและบุคคลอื่น เช่น TCH TSD รวมถึงการดูแลทรัพย์สินของลูกค้า เช่น การฝากถอนเงิน และการวางหลักประกันของลูกค้า เป็นต้น
[บล.] ตัวแทนซื้อขายสัญญาซื้อขายล่วงหน้า	ระบบรับส่งคำสั่งซื้อขาย (Front Office : OMS)	ระบบสำหรับรับส่งคำสั่งซื้อขายสัญญาซื้อขายล่วงหน้าจากลูกค้าไปยังศูนย์ซื้อขายสัญญาซื้อขายล่วงหน้า (Trading Venue) และตัวแทนซื้อขายในต่างประเทศ (oversea brokers & dealers)
	ระบบ Back Office	ระบบที่เกี่ยวข้องกับการจัดการข้อมูลลูกค้า ข้อมูลการซื้อขาย การวางหลักประกันระหว่างบริษัท ธุรกรรมกับลูกค้าและบุคคลอื่น เช่น TCH รวมถึงการดูแลทรัพย์สินของลูกค้า เช่น การฝากถอนเงิน เป็นต้น
[บลจ.] การจัดการกองทุนรวม / การจัดการกองทุนส่วนบุคคล	ระบบรับคำสั่งซื้อขายหน่วยลงทุน (Selling Agent)	ระบบที่เกี่ยวข้องกับการรับคำสั่งซื้อขายหน่วยลงทุนจากลูกค้า
	ระบบจัดการกองทุน (Portfolio Management)	ระบบที่เกี่ยวข้องกับการบริหารจัดการกองทุน
	ระบบ Back Office	ระบบที่เกี่ยวข้องกับการชำระราคา การจัดสรรหน่วยลงทุน การเก็บรักษาทรัพย์สินของผู้ลงทุน และการคำนวณมูลค่าทรัพย์สิน
[บลน. / LBDU] นายหน้าซื้อขาย / ค้า /จัด	ระบบรับคำสั่งซื้อขายหน่วยลงทุน (Selling Agent)	ระบบที่เกี่ยวข้องกับการรับคำสั่งซื้อขายหน่วยลงทุนจากลูกค้า

[3] ระบบคอมพิวเตอร์หรือระบบเครือข่ายที่หากมีการหยุดชะงักจะส่งผลกระทบอย่างมีนัยสำคัญต่อการดำเนินงานหรือความต่อเนื่องในการดำเนินงาน ชื่อเสียง หรือฐานะของผู้ประกอบธุรกิจ หรือการใช้บริการของลูกค้า

ประเภทผู้ประกอบธุรกิจ	ระบบงานสำคัญที่ควรอยู่ในขอบเขตการตรวจสอบ	คำอธิบาย
จำหน่ายหลักทรัพย์ ที่เป็นหน่วยลงทุน	ระบบ Back Office	ระบบที่เกี่ยวข้องกับการชำระราคา การจัดสรรหน่วยหน่วยลงทุน การเก็บรักษาทรัพย์สินของผู้ลงทุน และการจัดทำทะเบียนผู้ถือหน่วยลงทุน (กรณี omnibus)
[Digital Asset Exchange] ศูนย์ซื้อขายสินทรัพย์ดิจิทัล	ระบบซื้อขายสินทรัพย์ดิจิทัล	ระบบสำหรับการซื้อขาย ระบบงานที่ช่วยเสริมสร้างและรักษากลไกการทำงานของระบบซื้อขาย ให้มีความเป็นระเบียบเรียบร้อย (market surveillance) ระบบชำระราคาและส่งมอบสินทรัพย์ดิจิทัล
	ระบบการรับลูกค้า การพิสูจน์ยืนยันตัวของลูกค้า	ระบบการรับลูกค้า (customer onboarding) และระบบการพิสูจน์ตัวตนของลูกค้า (KYC)
	ระบบเก็บรักษาสินทรัพย์ดิจิทัลของลูกค้า	ระบบสำหรับดูแลรักษาสินทรัพย์ของลูกค้า ซึ่งรวมถึงระบบรับฝากและถอนทรัพย์สินที่เป็นสินทรัพย์ดิจิทัล
[Digital Asset Broker] นายหน้าซื้อขายสินทรัพย์ดิจิทัล	ระบบรับส่งคำสั่งซื้อขายสินทรัพย์ดิจิทัล	ระบบสำหรับให้บริการรับคำสั่งซื้อหรือขายสินทรัพย์ดิจิทัลจากลูกค้า เพื่อส่งผ่านไปยังศูนย์ซื้อขายสินทรัพย์ดิจิทัลปลายทางที่นายหน้าซื้อขายสินทรัพย์ดิจิทัลไปเชื่อมต่อระบบด้วย
	ระบบการรับลูกค้า การพิสูจน์ยืนยันตัวของลูกค้า	ระบบการรับลูกค้า (customer onboarding) และระบบการพิสูจน์ตัวตนของลูกค้า (KYC)
	ระบบเก็บรักษาสินทรัพย์ดิจิทัลของลูกค้า	ระบบสำหรับดูแลรักษาสินทรัพย์ของลูกค้า ซึ่งรวมถึงระบบรับฝากและถอนทรัพย์สินที่เป็นสินทรัพย์ดิจิทัล
[Digital Asset Dealer] ผู้ค้าสินทรัพย์ดิจิทัล	ระบบค้าสินทรัพย์ดิจิทัล	ระบบสำหรับการค้า แลกเปลี่ยน ชำระ ส่งมอบสินทรัพย์ดิจิทัล
	ระบบการรับลูกค้า การพิสูจน์ยืนยันตัวของลูกค้า	ระบบการรับลูกค้า (customer onboarding) และระบบการพิสูจน์ตัวตนของลูกค้า (KYC)
[Digital Asset Fund Manager] ผู้จัดการเงินทุนสินทรัพย์ดิจิทัล	ระบบรับคำสั่งเพิ่มทุนหรือลดทุน	ระบบที่เกี่ยวข้องกับการรับคำสั่งเพิ่มทุนหรือลดทุนจากลูกค้า
	ระบบจัดการกองทุน (Portfolio Management)	ระบบที่เกี่ยวข้องกับการบริหารจัดการกองทุน
	ระบบการรับลูกค้า การพิสูจน์ยืนยันตัวของลูกค้า	ระบบการรับลูกค้า (customer onboarding) และระบบการพิสูจน์ตัวตนของลูกค้า (KYC)
	ระบบคำนวณ NAV	ระบบที่เกี่ยวข้องกับการคำนวณมูลค่าทรัพย์สิน
[Digital Asset Custodial Wallet Provider] ผู้ให้บริการรับฝากสินทรัพย์ดิจิทัล	ระบบเก็บรักษาสินทรัพย์ดิจิทัลของลูกค้า	ระบบสำหรับดูแลรักษาสินทรัพย์ของลูกค้า ซึ่งรวมถึงระบบรับฝากและถอนทรัพย์สินที่เป็นสินทรัพย์ดิจิทัล
[Crowd Funding] ผู้ให้บริการระบบคราวด์ฟันดิง	ระบบการเสนอขายและการจองจัดสรรหลักทรัพย์คราวด์ฟันดิง	ระบบที่เกี่ยวข้องกับการให้บริการเสนอขาย การจองและจัดสรรหลักทรัพย์คราวด์ฟันดิง

ประเภทผู้ประกอบธุรกิจ	ระบบงานสำคัญที่ควรอยู่ในขอบเขตการตรวจสอบ	คำอธิบาย
[ICO Portal] ผู้ให้บริการระบบเสนอขายโทเคนดิจิทัล	ระบบการเสนอขายและการจองจัดสรรโทเคนดิจิทัล	ระบบที่เกี่ยวข้องกับการให้บริการเสนอขาย การจองและจัดสรรโทเคนดิจิทัล
ตลาดหลักทรัพย์แห่งประเทศไทย	ระบบซื้อขายหลักทรัพย์	ระบบที่เกี่ยวข้องกับการซื้อขายหลักทรัพย์
	ระบบงานกำกับการซื้อขาย (Market Surveillance System)	ระบบที่เกี่ยวข้องกับการรักษากลไกการทำงานของระบบซื้อขายหลักทรัพย์ให้มีความเป็นระเบียบเรียบร้อย (market surveillance)
	ระบบเผยแพร่ข้อมูลซื้อขาย	ระบบที่เกี่ยวข้องกับการเปิดเผยข้อมูลซื้อขายหลักทรัพย์
ศูนย์ซื้อขายสัญญาซื้อขายล่วงหน้า	ระบบซื้อขายสัญญาซื้อขายล่วงหน้า	ระบบที่เกี่ยวข้องกับการซื้อขายสัญญาซื้อขายล่วงหน้า
	ระบบงานกำกับการซื้อขาย (Market Surveillance System)	ระบบที่เกี่ยวข้องกับการรักษากลไกการทำงานของระบบซื้อขายสัญญาซื้อขายล่วงหน้าให้มีความเป็นระเบียบเรียบร้อย (market surveillance)
	ระบบเผยแพร่ข้อมูลซื้อขาย	ระบบที่เกี่ยวข้องกับการเปิดเผยข้อมูลซื้อขายสัญญาซื้อขายล่วงหน้า
สำนักหักบัญชีหลักทรัพย์/สำนักหักบัญชีสัญญาซื้อขายล่วงหน้า	ระบบชำระราคาซื้อขายหลักทรัพย์	ระบบที่เกี่ยวข้องกับการชำระราคาซื้อขายหลักทรัพย์
	ระบบชำระราคาซื้อขายสัญญาซื้อขายล่วงหน้า	ระบบที่เกี่ยวข้องกับการชำระราคาซื้อขายสัญญาซื้อขายล่วงหน้า
ศูนย์รับฝากหลักทรัพย์	ระบบนายทะเบียนหลักทรัพย์ (Registrar)	ระบบที่เกี่ยวข้องกับการจัดทำทะเบียนหลักทรัพย์ให้กับหลักทรัพย์ที่จดทะเบียนใน SET และ mai รวมทั้งหลักทรัพย์ที่ไม่ได้จดทะเบียน
	ระบบรับฝากหลักทรัพย์ (Depository)	ระบบที่เกี่ยวข้องกับการรับฝากหลักทรัพย์ทั้งตราสารทุนและตราสารหนี้
ผู้ให้บริการระบบสนับสนุนงานที่เกี่ยวข้องกับการซื้อขายหน่วยลงทุนและการจัดการกองทุน (เช่น Fund Connext เป็นต้น)	ระบบ Order Routing	ระบบที่ให้บริการเกี่ยวกับการรับส่งคำสั่งซื้อขายหน่วยลงทุน
ผู้ให้บริการระบบชำระเงินซื้อขายหลักทรัพย์ (เช่น Finnet เป็นต้น)	ระบบจัดการข้อมูลในการชำระเงินซื้อขายหลักทรัพย์	ระบบที่เกี่ยวข้องกับการบริหารจัดการข้อมูลและการชำระเงินซื้อขายหลักทรัพย์

สำหรับธุรกิจซึ่งไม่ได้มีการกำหนดรายชื่อของระบบขั้นต่ำในตารางข้างต้น ผู้ประกอบธุรกิจสามารถประเมินความเสี่ยง และพิจารณากำหนดขอบเขตในการตรวจสอบเพิ่มเติมเพื่อให้ครอบคลุมระบบ IT ที่มีนัยสำคัญได้ด้วยตนเอง

4. การตรวจสอบ

4.1 วิธีการเก็บหลักฐาน

วิธีการเก็บหลักฐาน (methods of obtaining audit evidence) ที่แนะนำสำหรับการควบคุมแต่ละข้อมีรายละเอียดตาม**เอกสารแนบ** ผู้ตรวจสอบสามารถเลือกใช้วิธีการเก็บหลักฐานสำหรับตรวจสอบการควบคุมแต่ละข้อได้ตามความเหมาะสม โดยคำนึงถึงการสรุปผลการประเมินอย่างสมเหตุสมผล (reasonable assurance) โดยใช้ทรัพยากรด้านการตรวจสอบที่อาจมีอยู่อย่างจำกัดได้อย่างมีประสิทธิภาพ และพึงกระทำด้วยความเชี่ยวชาญและความระมัดระวังเยี่ยงวิชาชีพ

ทั้งนี้ ตัวอย่างของวิธีการเก็บหลักฐานที่สามารถใช้ดำเนินการตรวจสอบมีดังนี้

วิธีการเก็บหลักฐาน	คำอธิบาย
การสังเกตการณ์ (observation)	สังเกตขั้นตอนหรือวิธีปฏิบัติงานของผู้ปฏิบัติงานของบริษัทที่รับการตรวจสอบ
การสัมภาษณ์/สอบถาม (inquiry)	สอบถามข้อมูลจากบุคลากรของบริษัทที่รับการตรวจสอบ
การสอบทาน/ตรวจสอบ (Inspection)	ตรวจสอบบันทึก (record) เอกสาร และข้อมูล ทั้งในรูปแบบกระดาษและรูปแบบอิเล็กทรอนิกส์ รวมถึงการตั้งค่าบนระบบงาน (configuration)
การยืนยันโดยบุคคลภายนอก (third-party confirmation)	ตรวจสอบข้อมูลที่ได้รับการยืนยันจากบุคคลภายนอกที่เป็นอิสระจากบริษัทที่รับการตรวจสอบ
การคำนวณซ้ำ (recalculation)	คำนวณซ้ำโดยผู้สอบเพื่อสอบทานความถูกต้องของตัวเลขในเชิงคณิตศาสตร์
การปฏิบัติซ้ำ (reperformance)	ทดสอบการปฏิบัติหรือทดสอบการควบคุมโดยผู้ตรวจสอบ
การเรียกข้อมูลจากระบบ (system query)	ตรวจสอบความถูกต้องของ output จาก input ที่กำหนด

4.2 แนวทางการสุ่มตัวอย่าง

การสุ่มตัวอย่างในการตรวจสอบ (audit sampling) มีวัตถุประสงค์เพื่อให้ผู้ตรวจสอบมีข้อมูลเพียงพอในการสรุปผลการประเมิน ในขณะที่ลดเวลาและค่าใช้จ่ายของการตรวจสอบจากประชากร (population) ทั้งหมด ดังนั้น ผู้ตรวจสอบควรพิจารณากรอบระยะเวลา (sample period) และจำนวนของกลุ่มตัวอย่าง (sample size) ที่เพียงพอสำหรับการสรุปผลการประเมินการควบคุมที่เกิดขึ้นในรอบ 1 ปีที่ผ่านมา โดยให้ความเชื่อมั่นอย่างสมเหตุสมผล (reasonable assurance)

ในการนี้ ผู้ตรวจสอบสามารถใช้ตารางการกำหนดจำนวนของกลุ่มตัวอย่างด้านล่างนี้เป็นแนวทางในการกำหนดกลุ่มตัวอย่างในการตรวจสอบ อย่างไรก็ดี ผู้ตรวจสอบสามารถใช้วิธีการทางสถิติอื่น ๆ ในการกำหนดจำนวนของกลุ่มตัวอย่างได้ตามดุลยพินิจของผู้ตรวจสอบ

ความถี่ของการควบคุม (จำนวนประชากร) (Frequency and Population Size)	ลำดับความสำคัญของการควบคุม (H-High, M-medium, L-low)	จำนวนของกลุ่มตัวอย่าง (Sample Size)
Annually (1)	H	1
	M	1
	L	1
Quarterly (4)	H	2
	M	1 ถึง 2
	L	1
Monthly (12)	H	4
	M	3
	L	2
Weekly (52)	H	9
	M	7
	L	5
Daily (250)	H	25
	M	20
	L	15
Multiple times per day (มากกว่า 250)	H	45
	M	35
	L	25

ตัวอย่างการใช้งานตารางการกำหนดจำนวนของกลุ่มตัวอย่างในการตรวจสอบ มีดังนี้

- การควบคุมที่เกิดขึ้น 30 ครั้ง ในรอบ 1 ปีที่ผ่านมา จะถูกปัดขึ้นเป็น Weekly controls (52) หากมีความสำคัญสูง จำนวนของกลุ่มตัวอย่าง คือ 9
- การควบคุมที่เกิดขึ้น 55 ครั้ง ในรอบ 1 ปีที่ผ่านมา จะถูกปัดขึ้นเป็น Daily controls (250) หากมีความสำคัญปานกลาง จำนวนของกลุ่มตัวอย่าง คือ 20

4.3 การบันทึกข้อมูลเกี่ยวกับการตรวจสอบ

ผู้ตรวจสอบควรจัดให้มีวิธีการบันทึกข้อมูลเกี่ยวกับการตรวจสอบที่เป็นรูปแบบมาตรฐาน ไม่ว่าจะอยู่ในรูปของกระดาษทำการที่บันทึกด้วยมือหรืออยู่ในรูปแบบข้อมูลอิเล็กทรอนิกส์ในระบบคอมพิวเตอร์ เพื่อให้มีข้อมูลเพียงพอที่จะใช้เป็นหลักฐานแสดงที่มาของการสรุปผลการตรวจสอบ และการตั้งประเด็นข้อบกพร่อง/ข้อตรวจพบ

4.4 ประเภทของการตรวจสอบ

การตรวจสอบการควบคุมตามแบบรายงานผล IT Audit แบ่งได้ 2 ประเภท ได้แก่

(1) การตรวจสอบการควบคุมในรูปแบบ Compliance check สามารถแบ่งผลการประเมินได้ 4 รูปแบบ ดังนี้

ผลการประเมิน	ความหมาย
No	ผู้ประกอบธุรกิจไม่ได้ปฏิบัติตามการควบคุมที่พึงมี/สอดคล้องตามแนวปฏิบัติของสำนักงาน
Partial	ผู้ประกอบธุรกิจได้ปฏิบัติตามการควบคุมที่พึงมี/สอดคล้องตามแนวปฏิบัติของสำนักงานบางส่วนรวมถึงการกำหนดนโยบาย แผน กระบวนการ และขั้นตอนปฏิบัติงานที่ไม่ได้รับการอนุมัติจากผู้มีอำนาจ
Yes	ผู้ประกอบธุรกิจได้ปฏิบัติตามการควบคุมที่พึงมี/สอดคล้องตามแนวปฏิบัติของสำนักงานอย่างครบถ้วน หรือจัดให้มีการควบคุมทดแทน (compensating controls/alternative controls) ที่สามารถจัดการความเสี่ยงได้เทียบเท่ากับการควบคุมที่พึงมี
N/A	ผู้ประกอบธุรกิจไม่ได้ปฏิบัติตามการควบคุมที่พึงมี/สอดคล้องตามแนวปฏิบัติของสำนักงาน เนื่องจากไม่มีความเสี่ยงที่เกี่ยวข้อง หรือการควบคุมดังกล่าวไม่สามารถใช้ได้กับระบบ IT ของบริษัท (not-applicable) ทั้งนี้ ในการตอบ N/A ผู้ตรวจสอบต้องมั่นใจได้ว่า การไม่จัดให้มีการควบคุมนี้จะไม่ส่งผลกระทบต่อประสิทธิผลในการบริหารจัดการความเสี่ยงขององค์กร
หมายเหตุ: กรณีที่ผู้ตรวจสอบพิจารณาอย่างรอบคอบและระมัดระวัง โดยใช้ความรู้ ทักษะ และความสามารถที่จำเป็นแล้วพบว่า ผู้ประกอบธุรกิจมีการบริหารจัดการความเสี่ยง (Risk Management) และ/หรือมีการควบคุมอื่น ๆ ทดแทน (compensate controls/alternative controls) ซึ่งสามารถจัดการความเสี่ยงที่เกี่ยวข้องได้เทียบเท่ากับการควบคุมที่พึงมี/สอดคล้องตามที่สำนักงานกำหนดไว้ ผู้ตรวจสอบสามารถใช้ดุลยพินิจในการตัดสินใจให้ผลการประเมินเป็น “Yes” ได้	

ตัวอย่าง

การควบคุมที่พึงมี/สอดคล้องตามที่ประกาศฯ กำหนด

จัดให้มีผู้บริหารระดับสูง (chief information security officer : CISO) หรือผู้บริหารที่รับผิดชอบในการบริหารจัดการความมั่นคงปลอดภัยด้าน IT ที่มีคุณสมบัติและอำนาจหน้าที่เหมาะสม

แนวทางการประเมิน Yes/Partial/No

ตอบ “No” หากผู้ประกอบธุรกิจไม่ได้แต่งตั้งผู้บริหารระดับสูง (CISO) หรือผู้บริหารที่รับผิดชอบในการบริหารจัดการความมั่นคงปลอดภัยด้าน IT

ตอบ “Partial” หากผู้ประกอบธุรกิจแต่งตั้งผู้บริหารระดับสูง (CISO) หรือผู้บริหารที่รับผิดชอบในการบริหารจัดการความมั่นคงปลอดภัยด้าน IT แต่ไม่มีคุณสมบัติหรืออำนาจหน้าที่ไม่เหมาะสมหรือไม่เป็นไปตามแนวปฏิบัติของสำนักงาน

ตอบ “Yes” หากผู้ประกอบธุรกิจแต่งตั้งผู้บริหารระดับสูง (CISO) หรือผู้บริหารที่รับผิดชอบในการบริหารจัดการความมั่นคงปลอดภัยด้าน IT โดยมีคุณสมบัติและอำนาจหน้าที่เหมาะสม/เป็นตามแนวปฏิบัติของสำนักงาน

ตอบ “N/A” หากผู้ประกอบธุรกิจไม่ได้แต่งตั้งผู้บริหารระดับสูง (CISO) หรือผู้บริหารที่รับผิดชอบในการบริหารจัดการความมั่นคงปลอดภัยด้าน IT เนื่องจากลักษณะการประกอบธุรกิจไม่มีความเสี่ยงที่เกี่ยวข้องกับการบริหารจัดการความมั่นคงปลอดภัยด้าน IT หรือความเสี่ยงที่เกี่ยวข้องคุณสมบัติและอำนาจหน้าที่ของผู้บริหารระดับสูงด้าน IT (Not applicable)

(2) การตรวจสอบการควบคุมในรูปแบบ Maturity Level สามารถแบ่งผลการประเมินได้ 6 รูปแบบ ดังนี้

ผลการประเมิน	ความหมาย
Level 1 (M1)	ผู้ประกอบธุรกิจไม่ได้ปฏิบัติตามการควบคุมที่พึงมี/สอดคล้องตามแนวปฏิบัติของสำนักงาน
Level 2 (M2)	ผู้ประกอบธุรกิจได้ปฏิบัติตามการควบคุมที่พึงมี/สอดคล้องตามแนวปฏิบัติของสำนักงานบางส่วน รวมถึงการกำหนดนโยบาย แผน กระบวนการ และขั้นตอนปฏิบัติงานที่ไม่ได้รับการอนุมัติจากผู้มีอำนาจ
Level 3 (M3)	ผู้ประกอบธุรกิจได้ปฏิบัติตามการควบคุมที่พึงมี/สอดคล้องตามแนวปฏิบัติของสำนักงานอย่างครบถ้วน หรือจัดให้มีการควบคุมทดแทน (compensating controls/alternative controls) ที่สามารถจัดการความเสี่ยงได้เทียบเท่ากับการควบคุมที่พึงมี
Level 4 (M4)	ปฏิบัติได้ตาม Level 3 และผู้ประกอบธุรกิจมีกระบวนการสอบทาน หรือติดตามผล เช่น สอบทานการปฏิบัติงานโดย 2nd line of defense หรือ IT security ที่มีความอิสระจากผู้ปฏิบัติงาน หรือผู้ที่ไม่มีส่วนได้เสียกับการควบคุมดังกล่าว เป็นต้น เพื่อให้มั่นใจว่าได้ปฏิบัติตามการควบคุมที่พึงมี/สอดคล้องตามแนวปฏิบัติของสำนักงานได้ครบถ้วนและสม่ำเสมอ
Level 5 (M5)	ปฏิบัติได้ตาม Level 4 และผู้ประกอบธุรกิจมีการติดตามเชิงรุกต่อการเปลี่ยนทั้งภายในและภายนอกองค์กร เพื่อประเมินผลกระทบและนำมาปรับปรุงการควบคุมให้ตอบรับและสอดคล้องกับการเปลี่ยนแปลงที่เกิดขึ้น หรือ ผู้ประกอบธุรกิจมีการติดตั้งเครื่องมือในการติดตามผลหรือติดตามเชิงรุกเพื่อออกแบบและปฏิบัติตามการควบคุมด้วยวิธีอัตโนมัติเพื่อความมีประสิทธิผลของการควบคุมอย่างครบถ้วนและสม่ำเสมอ

ผลการประเมิน	ความหมาย
N/A	ผู้ประกอบธุรกิจไม่ได้ปฏิบัติตามการควบคุมที่พึงมี/สอดคล้องตามแนวปฏิบัติของสำนักงาน เนื่องจากไม่มีความเสี่ยงที่เกี่ยวข้อง หรือการควบคุมดังกล่าวไม่สามารถใช้ได้กับระบบ IT ของบริษัท (not-applicable) ทั้งนี้ ในการตอบ N/A ผู้ตรวจสอบต้องมั่นใจได้ว่า <u>การไม่จัดให้มีการควบคุมนี้จะไม่ส่งผลกระทบต่อประสิทธิผลในการบริหารจัดการความเสี่ยงขององค์กร</u>
หมายเหตุ: กรณีที่ผู้ตรวจสอบพิจารณาอย่างรอบคอบและระมัดระวัง โดยใช้ความรู้ ทักษะ และความสามารถที่จำเป็น แล้วพบว่า ผู้ประกอบธุรกิจมีการบริหารจัดการความเสี่ยง (Risk Management) และ/หรือมีการควบคุมอื่น ๆ ทดแทน (compensate controls/alternative controls) ซึ่งสามารถจัดการความเสี่ยงที่เกี่ยวข้องได้เทียบเท่ากับการควบคุมที่พึงมี/สอดคล้องตามที่สำนักงานกำหนดไว้ ผู้ตรวจสอบสามารถใช้ดุลยพินิจในการตัดสินใจให้ผลการประเมินเป็น “Level 3” ได้	

<u>ตัวอย่าง</u>

การควบคุมที่พึงมี/สอดคล้องตามที่ประกาศฯ กำหนด

มีกระบวนการจัดการเกี่ยวกับการเปลี่ยนแปลงตำแหน่งงานหรือสิ้นสุดการจ้างงาน และมอบหมายให้มีผู้รับผิดชอบอย่างชัดเจน เช่น การคืนทรัพย์สินขององค์กร การปรับปรุงสิทธิให้เป็นปัจจุบัน และยกเลิกสิทธิเมื่อสิ้นสุดการจ้างงาน รวมทั้งมีการสื่อสารให้ผู้ที่เกี่ยวข้องรับทราบถึงการเปลี่ยนแปลงสิทธิ หน้าที่ และความรับผิดชอบ

แนวทางการประเมิน Maturity Level

ตอบ “Level 1 (M1)” หากไม่มีกระบวนการจัดการเกี่ยวกับการเปลี่ยนแปลงตำแหน่งงานหรือสิ้นสุดการจ้างงาน

ตอบ “Level 2 (M2)” หากมีกระบวนการจัดการเกี่ยวกับการเปลี่ยนแปลงตำแหน่งงานหรือสิ้นสุดการจ้างงาน แต่ยังไม่มีการสื่อสารให้ผู้ที่เกี่ยวข้องทราบถึงข้อมูลกระบวนการเปลี่ยนแปลงดังกล่าวอย่างเป็นลายลักษณ์อักษร หรือการปรับปรุงสิทธิการเข้าใช้งานยังไม่เป็นปัจจุบัน หรือการเรียกคืนทรัพย์สินของบริษัทยังไม่ครบถ้วน

ตอบ “Level 3 (M3)” หากมีกระบวนการจัดการเกี่ยวกับการเปลี่ยนแปลงตำแหน่งงานหรือสิ้นสุดการจ้างงาน และสื่อสารให้ผู้ที่เกี่ยวข้องทราบถึงข้อมูลกระบวนการเปลี่ยนแปลงดังกล่าวอย่างเป็นลายลักษณ์อักษร ตลอดจนมีการปรับปรุงสิทธิให้เป็นปัจจุบันและมีการเรียกคืนทรัพย์สินของบริษัทครบถ้วน

ตอบ “Level 4 (M4)” หากปฏิบัติได้ตาม Level 3 รวมถึงมีการสอบทานการปฏิบัติตามวิธีปฏิบัติเมื่อมีการเปลี่ยนแปลงตำแหน่งงานหรือสิ้นสุดการจ้างงาน โดยหน่วยงานที่มีหน้าที่กำกับดูแลการปฏิบัติตามกฎหมายและหลักเกณฑ์ที่เกี่ยวข้องในการปฏิบัติงานทางด้าน IT (2nd line) เพื่อให้มั่นใจว่ามีการสอบทานการปฏิบัติตามวิธีปฏิบัติเมื่อมีการเปลี่ยนแปลงตำแหน่งงานหรือสิ้นสุดการจ้างงาน อย่างเหมาะสม

ตอบ "Level 5 (M5)" หากปฏิบัติได้ตาม Level 4 และใช้เครื่องมือหรือกลไกอัตโนมัติ (Monitoring mechanism) ในการตรวจจับและปรับปรุงสิทธิสำหรับพนักงานที่เปลี่ยนตำแหน่งงานหรือสิ้นสุดการจ้างงาน

ตอบ "N/A" เนื่องจากบริษัทไม่มีความเสี่ยงที่เกี่ยวข้องในการควบคุมของกระบวนการจัดการเกี่ยวกับการเปลี่ยนแปลงตำแหน่งงาน หรือสิ้นสุดการจ้างงาน และมอบหมายให้มีผู้รับผิดชอบอย่างชัดเจน

หมายเหตุ : การเว้นว่างในช่องผลการประเมิน
กรณีที่เป็นการตรวจสอบของผู้ประกอบธุรกิจขนาดเล็ก ผู้ประกอบธุรกิจที่มีความเสี่ยงระดับต่ำ หรือผู้ประกอบธุรกิจที่มีความเสี่ยงปานกลาง ซึ่งมีบางข้อการควบคุมที่ไม่ได้บังคับใช้กับระดับความเสี่ยงของตน ผู้ตรวจสอบสามารถเว้นว่างในช่องผลการประเมินสำหรับข้อการควบคุมนั้น ในกรณีที่ผู้ตรวจสอบมิได้ดำเนินการตรวจสอบข้อที่ไม่ได้บังคับใช้เหล่านั้น ทั้งนี้ กรณีที่ผู้ตรวจสอบได้ดำเนินการตรวจสอบเกินกว่าข้อการควบคุมขั้นต่ำที่กำหนดไว้ ผู้ตรวจสอบสามารถระบุผลการตรวจสอบเพิ่มเติมได้

5. การสรุปประเด็นข้อตรวจพบ/ข้อบกพร่อง (Finding)

การสรุปประเด็นข้อตรวจพบ/ข้อบกพร่อง (Finding) ในรายละเอียดนั้น ผู้ตรวจสอบสามารถพิจารณาจากผลประเมินการควบคุมในข้อที่เกี่ยวข้อง โดยหากการควบคุมดังกล่าวมีผลการประเมินเป็น **'No หรือ Level 1 (M1)' และ 'Partial หรือ Level 2 (M2)'** จะต้องถูกนำมาบันทึกไว้แถบข้อตรวจพบ (Finding)

สำหรับระดับความสำคัญของข้อบกพร่อง/ข้อตรวจพบ (Finding) นั้น จะพิจารณาจากผลกระทบที่เกิดขึ้นหรืออาจเกิดขึ้นต่อการบรรลุถึงวัตถุประสงค์ของการบริหารจัดการความเสี่ยงด้าน IT ตามที่กำหนดไว้ในหลักเกณฑ์ ดังนี้

ระดับความสำคัญของข้อบกพร่อง/ข้อตรวจพบ	ความหมาย
สูง	ข้อบกพร่อง/ข้อตรวจพบที่มีความเสี่ยงสูงที่จะก่อให้เกิดผลกระทบต่อการดำเนินธุรกิจ ทรัพย์สิน ชื่อเสียง และการปฏิบัติตามกฎหมายหรือระเบียบที่เกี่ยวข้องกับองค์กร และเป็นข้อบกพร่อง/ข้อตรวจพบซึ่งควรดำเนินการแก้ไขในทันที หรือแก้ไขให้แล้วเสร็จภายใน 3 เดือน
กลาง	ข้อบกพร่อง/ข้อตรวจพบที่มีโอกาสที่จะส่งผลกระทบ (potential impact) ต่อการดำเนินธุรกิจ ทรัพย์สิน ชื่อเสียง และการปฏิบัติตามกฎหมายหรือระเบียบที่เกี่ยวข้องกับองค์กร แต่ไม่มีความเร่งด่วนที่จะต้องแก้ไขในทันที และเป็นข้อบกพร่อง/ข้อตรวจพบซึ่งควรดำเนินการแก้ไขให้แล้วเสร็จภายใน 4-6 เดือน
ต่ำ	ข้อบกพร่อง/ข้อตรวจพบที่มีโอกาสที่จะส่งผลกระทบเพียงเล็กน้อยต่อการดำเนินธุรกิจ ทรัพย์สิน หรือชื่อเสียงขององค์กร และเป็นข้อบกพร่อง/ข้อตรวจพบซึ่งควรดำเนินการแก้ไขเมื่อมีความพร้อมทางทรัพยากร หรือภายใน 12 เดือน

หมายเหตุ: ผู้ตรวจสอบสามารถให้ข้อเสนอแนะโดยผู้ตรวจสอบ (recommendation/opportunity for improvement) ที่จะช่วยเพิ่มประสิทธิภาพในการบริหารจัดการความเสี่ยงด้าน IT ขององค์กร ซึ่งการไม่ปฏิบัติตามข้อเสนอแนะดังกล่าวไม่ได้ส่งผลกระทบต่อการบรรลุวัตถุประสงค์ด้านการรักษาความปลอดภัยทางเทคโนโลยีสารสนเทศ โดยข้อเสนอแนะดังกล่าวไม่อยู่ในขอบเขตของข้อมูลที่ต้องรายงานสำนักงาน

5.1 รายละเอียดของการบันทึกข้อสังเกต

วิธีการใส่ข้อมูลในตารางรายละเอียดข้อสังเกต ผู้ตรวจสอบควรดำเนินการตามคำอธิบายดังนี้

หัวข้อตาราง	คำอธิบาย
ลำดับ	ผู้ตรวจสอบใส่ลำดับประเด็นของหัวข้อการตรวจสอบ
หมวดที่	การควบคุมจะประกอบไป 3 หมวด ได้แก่ D1. IT Governance (การกำกับดูแลและบริหารจัดการด้าน IT D2. IT Security (การรักษาความมั่นคงปลอดภัยด้าน IT) D3. IT Audit (การตรวจสอบด้าน IT) ผู้ตรวจสอบจะต้องเลือกหมวดการควบคุมให้สอดคล้องกับข้อตรวจพบ/ข้อบกพร่องที่ปรากฏในรายงานสรุปผลการตรวจสอบและกระดาษทำการ
หมายเลขการควบคุม (Control ID)	ผู้ตรวจสอบจะต้องใส่หมายเลขรหัสการควบคุม ซึ่งจะปรากฏอยู่ในแต่ละหน้าของกระดาษทำการ (ระบุเป็นหมายเลขตาม Column A ของ Sheet D1-D3) ทั้งนี้ ผู้ตรวจสอบจะต้องนำหมายเลขรหัสการควบคุมที่เกี่ยวข้องกับข้อตรวจพบ/ข้อบกพร่องมาใส่ให้ครบถ้วน ตัวอย่างเช่น ▪ ข้อตรวจพบที่ 1 ในหมวด D1. IT Governance เกี่ยวข้องกับการควบคุมที่ D1 #2, D2 #3, D1#7 เป็นต้น
หัวข้อ (Domain)	ผู้ตรวจสอบจะต้องใส่หัวข้อให้สอดคล้องกับข้อตรวจพบ/ข้อบกพร่องที่ตรวจพบ โดยอ้างอิงจาก ‘ส่วนที่’ ในกระดาษทำการแต่ละหน้า
ข้อตรวจพบ/ข้อบกพร่อง (Audit Finding)	ผู้ตรวจสอบจะต้องใส่รายละเอียดของประเด็นที่ตรวจพบ
ระดับความสำคัญของข้อตรวจพบ (Rating)	ผู้ตรวจสอบจะต้องใส่ระดับความสำคัญของข้อตรวจพบตามที่มีการพิจารณาตามเกณฑ์ข้างต้น

หัวข้อตาราง	คำอธิบาย
แผนการแก้ไขข้อตรวจพบ/ข้อบกพร่อง (Corrective action plan)	ผู้ตรวจสอบจะต้องระบุแผนการแก้ไขที่ผู้รับตรวจได้ชี้แจ้งกลับมายังหน่วยงาน ทั้งนี้ แผนการแก้ไขจะต้องสอดคล้องกับประเด็นที่ตรวจพบ
วันที่แก้ไขแล้วเสร็จหรือคาดว่าจะแล้วเสร็จ (Close Date or Target Close Date: MM/YYYY)	ผู้ตรวจสอบจะต้องระบุวันที่แก้ไขแล้วเสร็จหรือคาดว่าแล้วเสร็จ โดยตรวจสอบจากแผนการแก้ไขที่ผู้รับตรวจได้ดำเนินการชี้แจงให้ทราบ
หมายเหตุ (ถ้ามีข้อมูลสำคัญที่จะอธิบายเพิ่มเติม)	หากมีรายละเอียดเพิ่มเติมจากข้อตรวจพบ หรือแผนการแก้ไขอื่นๆ ผู้ตรวจสอบควรบันทึกในหมายเหตุเพื่อประกอบการพิจารณาในครั้งถัดไป

6. การสรุปผลการตรวจสอบในภาพรวม

การแปลผลคะแนนเพื่อสรุปผลการตรวจสอบในภาพรวมจะประกอบไปด้วย 2 ส่วน ได้แก่ (1) การวิเคราะห์ผลการตรวจสอบในรูปแบบตารางคะแนน และ (2) การวิเคราะห์ผลการตรวจสอบในรูปแบบกราฟ

6.1 การวิเคราะห์ผลการตรวจสอบในรูปแบบตารางคะแนน

6.1.1 การควบคุมทั่วไป (Basic Controls)

ผู้ประกอบธุรกิจสามารถวิเคราะห์คะแนนที่ได้รับจากผลการประเมินในแต่ละ Domain ซึ่งประกอบด้วย การประเมินการควบคุมในรูปแบบ (1) Compliance check และ (2) Maturity Level (M1-M5) โดยในตารางคะแนนจะแสดงข้อมูลดังนี้

- คะแนนการปฏิบัติตามเกณฑ์ที่สำนักงานกำหนด (เต็ม 3 คะแนน)
- คะแนนพิเศษจากการประเมิน Maturity Level M4 และ M5 (คะแนนพิเศษ 2 คะแนน)
- คะแนนรวม (เต็ม 5 คะแนน)

6.1.2 การควบคุมเพิ่มเติมสำหรับผู้ประกอบธุรกิจที่มีความเสี่ยงสูง (Advance Controls)

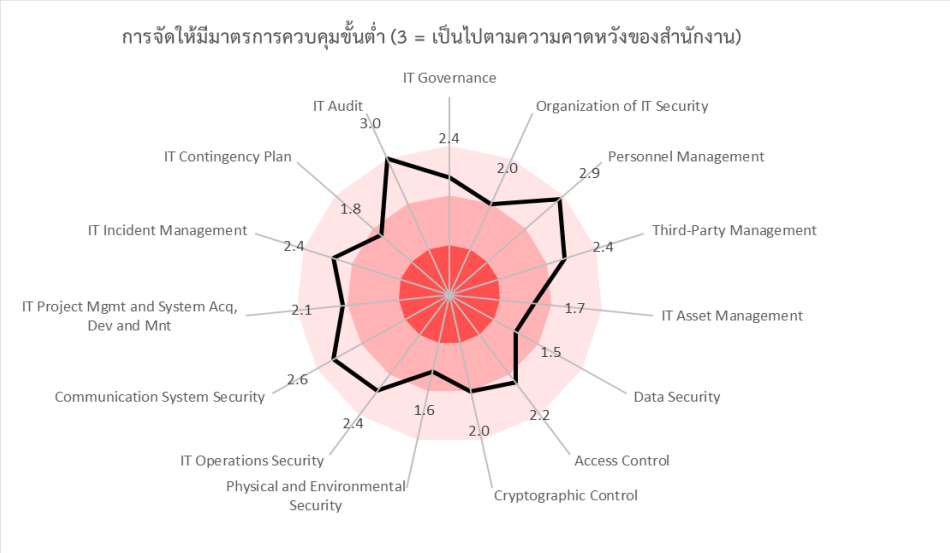
ผู้ประกอบธุรกิจสามารถวิเคราะห์การปฏิบัติตามมาตรการควบคุมเพิ่มเติมสำหรับผู้ประกอบธุรกิจที่มีความเสี่ยงสูง (Advance Controls) จากตารางซึ่งแสดงจำนวนผลมาตรการควบคุมที่มีผลตรวจเป็น N/A, No, Partial และ Yes พร้อมกับร้อยละของมาตรการควบคุมที่มีการดำเนินการ (ร้อยละของมาตรการควบคุมที่มีผลเป็น Yes)

6.2 การวิเคราะห์ผลการตรวจสอบในรูปแบบกราฟ

6.2.1 กราฟแสดงการจัดให้มีมาตรการควบคุมขั้นต่ำ

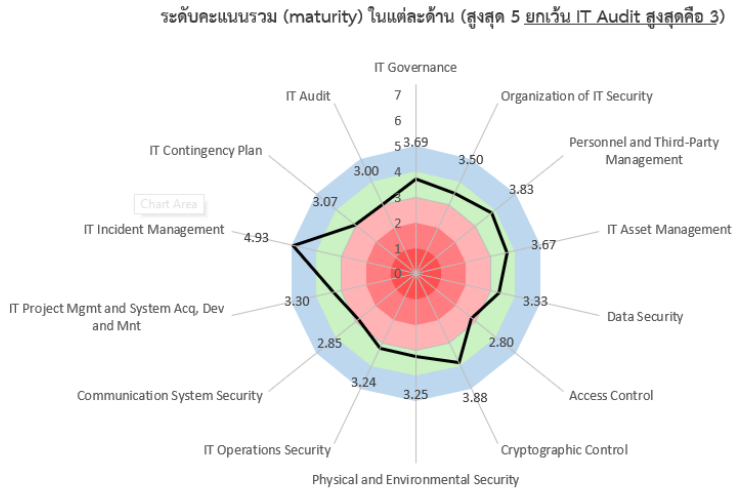
กราฟแสดงคะแนนเฉลี่ยของการจัดให้มีมาตรการควบคุมขั้นต่ำ (Basic Controls) โดยคะแนนที่สำนักงานคาดหวังคือ <u>เต็ม 3.0 คะแนนในทุก Domain</u> สำหรับ Domain ที่คะแนนต่ำกว่า 3.0 แสดงให้เห็นว่า ยังมีมาตรการควบคุมบางข้อใน Domain ดังกล่าวต้องได้รับการปรับปรุงเพื่อให้เป็นไปตามความคาดหวังของสำนักงานต่อไป

<u>ตัวอย่าง</u>



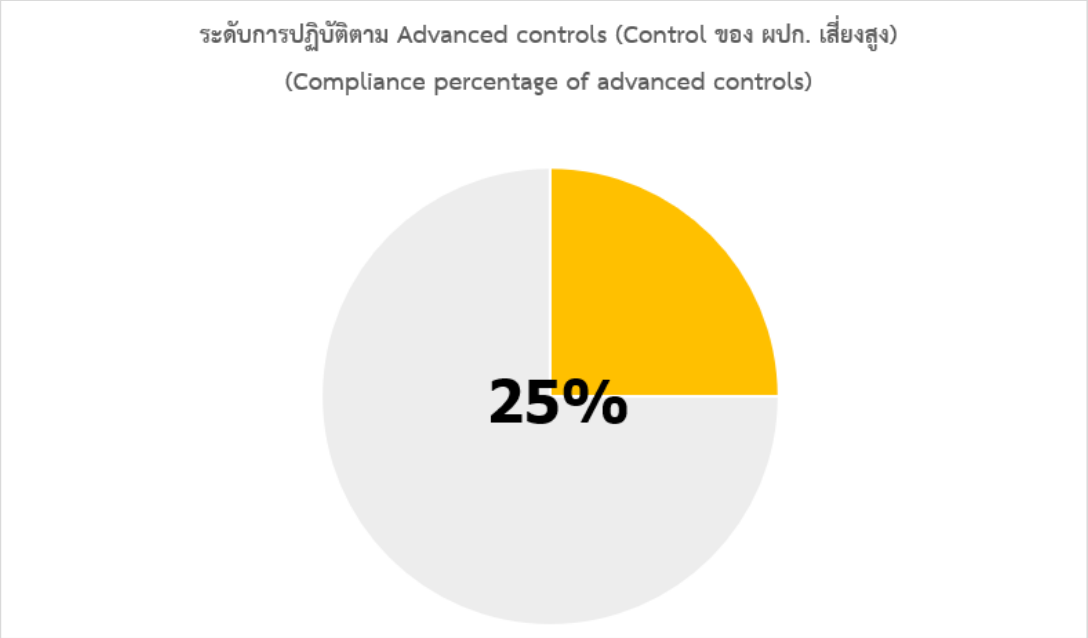
6.2.2 กราฟแสดงระดับ Maturity

กราฟแสดงคะแนนเฉลี่ยของการจัดให้มีมาตรการควบคุมในรูปแบบ Maturity โดยมีคะแนนสูงสุด 5 คะแนน สำหรับ Domain ที่มีคะแนน Maturity มากกว่า 3 คะแนน แสดงให้เห็นว่า ผู้ประกอบธุรกิจจัดให้มีมาตรการควบคุมบางส่วนได้เข้มงวดสูงกว่าความคาดหวังของสำนักงาน โดยมีกระบวนการสอนทาน ติดตามผล หรือมีเครื่องมือ/กลไกในการติดตามเชิงรุกต่อการเปลี่ยนแปลงทั้งภายในและภายนอกขององค์กร



6.2.3 กราฟแสดงระดับการปฏิบัติตาม Advanced controls

กราฟแสดงคะแนนระดับการปฏิบัติตาม Advanced control แสดงร้อยละของมาตรการควบคุมสำหรับผู้ประกอบธุรกิจที่มีความเสี่ยงระดับสูง (H) ที่มีผลการประเมินเป็น “Yes”



6.2.4 กราฟแสดงระดับคะแนนตาม function ของ NIST Cyber Security Framework

กราฟแสดงระดับคะแนนตาม function ของ NIST Cyber Security Framework 2.0 โดยข้อมูลในแต่ละแท่งแสดงเปอร์เซ็นต์ของการปฏิบัติตามมาตรการควบคุมที่เกี่ยวกับฟังก์ชันนั้น ๆ

ตัวอย่างเช่น จาก Control ทั้งหมดที่เกี่ยวข้องกับฟังก์ชัน “Protect” ของ NIST Cyber Security Framework บริษัทมีการนำไปปฏิบัติ และมีผลการประเมินเป็น Yes, M3, M4 หรือ M5 คิดเป็น 83% ของ Control ทั้งหมดในฟังก์ชันดังกล่าว