



หลักเกณฑ์ วิธีการ และเงื่อนไขการตรวจประเมินระบบการจัดการ

18 กันยายน 2569

ประวัติการปรับปรุงเอกสาร

[illegible]

คำนำ

ตามที่พระราชบัญญัติสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2562 กำหนดให้สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ หรือ สพธอ. มีหน้าที่และอำนาจในการวิเคราะห์และรับรองความสอดคล้องและความถูกต้องตามมาตรฐาน หรือตามมาตรการ หรือกลไกการกำกับดูแลที่เกี่ยวข้องกับการทำธุรกรรมทางอิเล็กทรอนิกส์และพาณิชย์อิเล็กทรอนิกส์

ดังนั้น สพธอ. จึงได้จัดทำเอกสารข้อกำหนดเกี่ยวกับหลักเกณฑ์ วิธีการ และเงื่อนไขการตรวจประเมินระบบการจัดการเพื่อให้หน่วยงาน องค์กร หรือบุคคลที่ประสงค์จะยื่นขอรับการตรวจประเมินเพื่อรับรองระบบการจัดการจาก สพธอ. รับทราบหลักเกณฑ์ วิธีการ และเงื่อนไขสำหรับการดำเนินการตรวจประเมินเพื่อรับรองความสอดคล้องของระบบการจัดการตามมาตรฐานตามที่ สพธอ. กำหนด

สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์

18 กันยายน 2569

สารบัญ

	หน้า
1. บทนำ	5
1.1 ขอบข่าย	5
1.2 คำนินยาม	5
2. หลักเกณฑ์ วิธีการ และเงื่อนไข	9
2.1 ขั้นตอนการตรวจประเมิน.....	9
2.1.1 ทั่วไป.....	9
2.1.2 การกำหนดคณะผู้ตรวจประเมิน.....	11
2.1.3 การตรวจประเมินเพื่อการรับรอง ประกอบด้วยการตรวจประเมิน 2 ขั้นตอน คือ การตรวจประเมินขั้นตอนที่ 1 และการตรวจประเมินขั้นตอนที่ 2	11
2.1.4 การตรวจติดตามผล.....	17
2.1.5 การตรวจประเมินเพื่อต่ออายุ.....	19
2.2 การตรวจกรณีองค์กรหลายสาขา.....	20
2.3 การตรวจประเมินกรณีองค์กรที่มีสถานที่ดำเนินชั่วคราว	25
2.4 การตรวจประเมินแบบบูรณาการและแบบรวมระบบ	25

หลักเกณฑ์ วิธีการ และเงื่อนไขการตรวจประเมินระบบการจัดการ

1. บทนำ

1.1 ขอบข่าย

เอกสารนี้กำหนดหลักเกณฑ์ วิธีการ และเงื่อนไขการตรวจประเมินระบบการจัดการ ในการดำเนินการตรวจประเมินความสอดคล้องของระบบการจัดการ ซึ่งจะครอบคลุมรายละเอียดการตรวจประเมินขั้นตอนที่ 1 ขั้นตอนที่ 2 การตรวจกรณีองค์กรหลายสาขา การตรวจประเมินกรณีที่มีสถานที่ดำเนินชั่วคราว การตรวจประเมินแบบบูรณาการและแบบรวมระบบ การตรวจติดตามผล และการตรวจประเมินเพื่อต่ออายุ

1.2 คำนิยาม

- ความหมายของคำที่ใช้ในเอกสารนี้ให้เป็นไปตามคำนิยามต่อไปนี้
- **สำนักงาน** หมายถึง สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์
 - **ผู้ยื่นคำขอ (Applicant)** หมายถึง บุคคลธรรมดาหรือนิติบุคคลที่ประสงค์ขอให้มีการตรวจประเมินเพื่อการรับรอง
 - **ผู้รับการตรวจประเมิน (Auditee)** หมายถึง ผู้ยื่นคำขอหรือผู้ได้รับการรับรองที่เข้ารับการตรวจประเมิน
 - **ผู้ได้รับการรับรอง** หมายถึง ผู้ยื่นคำขอที่ผ่านการตรวจประเมิน และได้รับการรับรองจากสำนักงาน
 - **ผู้ตรวจประเมิน (Auditor)** หมายถึง พนักงานของสำนักงานที่มีคุณสมบัติเป็นผู้เชี่ยวชาญหรือมีประสบการณ์ที่เกี่ยวข้องกับการตรวจประเมินความสอดคล้องของกระบวนการหรือระบบให้บริการตามมาตรฐาน ที่ดำเนินการตรวจประเมินอย่างเป็นระบบ เป็นอิสระ เพื่อให้ได้มาซึ่งหลักฐานการตรวจประเมิน และผลการตรวจประเมินอย่างเป็นรูปธรรม สำหรับการตัดสินใจระดับการบรรลุผลตามความสอดคล้องของเกณฑ์การตรวจประเมิน ทั้งนี้ รวมถึงผู้ตรวจประเมินภายนอกที่ได้รับการขึ้นทะเบียนเป็นผู้ตรวจประเมินภายนอกกับสำนักงาน
 - **ผู้เชี่ยวชาญด้านเทคนิค (Technical Expert)** หมายถึง บุคคลผู้ให้ความรู้หรือความเชี่ยวชาญเฉพาะด้านแก่คณะผู้ตรวจประเมิน แต่ไม่ได้ปฏิบัติหน้าที่ในฐานะผู้ตรวจประเมิน
 - **ผู้สังเกตการณ์ (Observer)** หมายถึง บุคคลผู้ติดตามคณะผู้ตรวจประเมิน แต่ไม่ได้ดำเนินการตรวจประเมิน และไม่มีอิทธิพลในการแทรกแซงการดำเนินการตรวจประเมิน ซึ่งผู้สังเกตการณ์ อาจมาจากผู้รับการตรวจประเมิน หรือหน่วยงานควบคุมกฎระเบียบ หรือผู้มีส่วนได้เสียอื่น
 - **คณะผู้ตรวจประเมิน (Audit Team)** หมายถึง ผู้ตรวจประเมินซึ่งเป็นหัวหน้าผู้ตรวจประเมิน หรือผู้ตรวจประเมินซึ่งประกอบด้วยหัวหน้าผู้ตรวจประเมินและผู้ตรวจประเมิน ที่ได้รับมอบหมายให้รับผิดชอบตรวจประเมินกระบวนการหรือระบบให้บริการตามมาตรฐานที่สำนักงานกำหนด นอกจากนี้ อาจมีผู้เชี่ยวชาญด้านเทคนิค หรือจะมอบหมายหัวหน้าผู้ตรวจประเมินคนใดคนหนึ่งให้รับผิดชอบตรวจประเมินกระบวนการหรือระบบให้บริการตามมาตรฐานที่สำนักงานกำหนด เข้าร่วมสนับสนุนการตรวจประเมินด้วยก็ได้
 - **ผู้ตัดสินใจการรับรอง** หมายถึง ผู้ที่ได้รับการแต่งตั้งจากผู้อำนวยการสำนักงานเพื่อพิจารณาตัดสินใจให้การรับรอง การคงไว้ เพิ่ม/ลดขอบข่าย การต่ออายุ ยกเลิกการรับรอง

- **คณะกรรมการพักใช้ เพิกถอน** หมายถึง คณะกรรมการที่ได้รับการแต่งตั้งจากผู้อำนวยการสำนักงานเพื่อพิจารณาการพักใช้ การเพิกถอนการรับรอง
- **ระบบการจัดการ** หมายถึง ระบบการจัดการที่องค์กรผู้ยื่นคำขอเข้าไปปฏิบัติ ซึ่งได้แก่ ระบบการจัดการความมั่นคงปลอดภัยด้านสารสนเทศ ระบบ ISMS ตามมาตรฐาน ISO/IEC 27001 และระบบการจัดการอื่น ๆ ที่สำนักงานจะให้การรับรองในอนาคต
- **องค์กรหลายสาขา (Multi site organization)** หมายถึง องค์กรที่ดำเนินธุรกิจมีเครือข่ายหรือสาขาที่เป็นนิติบุคคลเดียวกันหรือไม่ก็ได้ โดยมีสำนักงานส่วนกลางเป็นผู้ดำเนินการวางแผน ควบคุม จัดการหน่วยงานเครือข่ายหรือสาขา ในกรณีที่เครือข่ายหรือสาขาไม่เป็นนิติบุคคลเดียวกับสำนักงานส่วนกลาง ต้องมีสัญญาหรือนิติกรรมใด ๆ ที่แสดงว่าสำนักงานส่วนกลางมีอำนาจในการตรวจติดตาม และดำเนินการแก้ไขในเครือข่ายหรือสาขาต่าง ๆ ได้
- **สถานที่ดำเนินการชั่วคราว (Temporary site)** หมายถึง สถานที่ชั่วคราวที่อยู่ในขอบข่ายการรับรอง และสถานที่อื่นนอกเหนือจากสถานที่ที่ระบุในเอกสารการรับรอง ซึ่งกิจกรรมต่าง ๆ ภายในขอบข่ายการรับรองถูกนำไปปฏิบัติเป็นระยะเวลาหนึ่ง โดยสถานที่เหล่านี้จะมีตั้งแต่สถานที่จัดการโครงการขนาดใหญ่ไปจนถึงสถานที่ให้บริการหรือติดตั้งขนาดเล็ก
- **หนังสือรับรอง (Certificate)** หมายถึง หนังสือรับรองที่สำนักงานออกให้ผู้ได้รับการรับรอง
- **การตรวจประเมินขั้นตอนที่ 1 (Stage 1 audit)** หมายถึง การตรวจประเมินเบื้องต้นและการประเมินเอกสาร โดยมีวัตถุประสงค์เพื่อตรวจประเมินความพร้อมขององค์กรทั้งทางด้านเอกสาร ความรู้ ความเข้าใจในข้อกำหนดของระบบการจัดการที่ขอรับการรับรอง รวมถึงการนำไปปฏิบัติ เพื่อประกอบการนัดหมายการตรวจประเมินขั้นตอนที่ 2
- **การตรวจประเมินขั้นตอนที่ 2 (Stage 2 audit)** หมายถึง การตรวจประเมินเพื่อการรับรอง ซึ่งจะดำเนินการตรวจประเมิน ณ สถานที่ประกอบการ โดยมีวัตถุประสงค์เพื่อประเมินความสอดคล้องและประสิทธิผลของการนำระบบที่ขอรับการรับรองไปปฏิบัติ
- **การตรวจติดตามผล (Surveillance Audit)** หมายถึง การตรวจประเมินเพื่อติดตามการดำเนินการในช่วงอายุการรับรอง เพื่อให้เกิดความมั่นใจว่าระบบการจัดการยังคงเป็นไปตามเกณฑ์การตรวจประเมินที่กำหนด
- **การตรวจประเมินเพื่อต่ออายุ (Re-Certification Audit)** หมายถึง การตรวจประเมินเพื่อต่ออายุการรับรอง โดยมีวัตถุประสงค์เพื่อการทบทวนระบบการจัดการของผู้ได้รับการรับรองอีกครั้งว่าผู้ได้รับการรับรองมีการนำเกณฑ์การตรวจประเมินไปปฏิบัติ และยังมีประสิทธิภาพอยู่ซึ่งการตรวจประเมินเพื่อต่ออายุดังกล่าวจะดำเนินการก่อนหนังสือรับรองสิ้นอายุ
- **การตรวจประเมินกรณีพิเศษ** หมายถึง การตรวจประเมินเพื่อขยายขอบข่ายการรับรองหรือการตรวจประเมินแบบเร่งด่วนหาระยะเวลาสั้น ๆ เพื่อสืบสวนข้อร้องเรียน ติดตามการเปลี่ยนแปลงของลูกค้า หรือติดตามสถานะการถูกพักใช้
- **การตรวจประเมินทางไกล (Remote Audit)** หมายถึง การอำนวยความสะดวกในการตรวจประเมินของหน่วยตรวจสอบรับรองจากสถานที่อื่นนอกเหนือจากการเข้าตรวจประเมินด้วยตัวบุคคล ณ สถานที่ประกอบการ/สถานที่ที่จะตรวจประเมิน ด้วยการใช้เทคโนโลยีในการเก็บข้อมูล ทบทวนข้อมูล สัมภาษณ์ผู้รับการตรวจประเมิน รวมถึงการสุ่มตรวจพื้นที่ปฏิบัติงานที่สนใจและการสังเกตการณ์พนักงาน

- **การตรวจประเมินแบบบูรณาการ (Integrated Audit)** หมายถึง การตรวจประเมินแบบบูรณาการระหว่างมาตรฐานต่าง ๆ ที่สำนักงานเปิดให้บริการแก่ลูกค้า และต้องมีการดำเนินการกิจกรรมร่วมกันในระบบการจัดการที่ขอรับการรับรองตามที่สำนักงานกำหนด
- **การตรวจประเมินแบบรวมระบบ (Combined Audit)** หมายถึง การตรวจประเมินรวมระบบระหว่างมาตรฐานต่าง ๆ ที่สำนักงานเปิดให้บริการแก่ลูกค้า และลูกค้ามีความประสงค์ให้สำนักงานดำเนินการตรวจประเมินพร้อมกันในทุกกระบวนที่ลูกค้าดำเนินการ
- **ระบบการจัดการแบบบูรณาการ (Integrated Management System)** หมายถึง ระบบการจัดการที่มีการนำข้อกำหนดของมาตรฐานระบบการจัดการมากกว่า 1 ระบบ ไปปฏิบัติ โดยมีการดำเนินการในกิจกรรมร่วมกัน ได้แก่ นโยบายและวัตถุประสงค์ การประชุมทบทวนของฝ่ายบริหาร การตรวจประเมินภายใน การปฏิบัติการแก้ไขและป้องกัน การควบคุมเอกสารและข้อมูล และมีหน้าที่ความรับผิดชอบและสนับสนุนการจัดการร่วมกัน
- **ระบบการจัดการแบบรวมระบบ (Combined Management System)** หมายถึง ระบบการจัดการที่มีการนำข้อกำหนดของมาตรฐานระบบการจัดการมากกว่า 1 ระบบ ไปปฏิบัติแต่ไม่มีการดำเนินการในกิจกรรมร่วมกัน
- **แผนการตรวจประเมิน (Audit Plan)** หมายถึง แผนกิจกรรม และการเตรียมการที่เกี่ยวข้องกับการดำเนินการตรวจประเมินตามกระบวนการที่จัดทำขึ้นอย่างเป็นระบบ
- **ความไม่สอดคล้อง (Nonconformity)** หมายถึง ความล้มเหลวที่ไม่บรรลุตามเกณฑ์การตรวจประเมินและรับรอง
- **ความไม่สอดคล้องสำคัญ (Major Nonconformity)** หมายถึง กรณีที่ผู้รับการตรวจประเมินยังไม่ได้จัดทำตามเกณฑ์การตรวจประเมินและรับรอง หรือจัดทำแต่ไม่สอดคล้องตามเกณฑ์การตรวจประเมินและรับรอง หรือจัดทำแล้วแต่ไม่ได้นำไปปฏิบัติ หรือกรณีที่มีความไม่สอดคล้องย่อยหลาย ๆ จุดรวมกัน ซึ่งพิจารณาแล้วอาจมีผลกระทบต่อระบบการจัดการโดยรวม หรือการดำเนินการไม่เป็นไปตามกฎหมายที่เกี่ยวข้อง
- **ความไม่สอดคล้องย่อย (Minor Nonconformity)** หมายถึง กรณีที่ผู้รับการตรวจประเมินจัดทำตามเกณฑ์การตรวจประเมินและรับรองแล้ว และนำไปปฏิบัติบ้างไม่ปฏิบัติบ้าง แต่ไม่มีผลกระทบต่อระบบการจัดการ
- **ข้อเสนอแนะเพื่อการปรับปรุง (Opportunity for Improvement)** หมายถึง ข้อเสนอแนะหรือโอกาสเพื่อการปรับปรุง เช่น ข้อเสนอแนะเพื่อปรับปรุงเพิ่มประสิทธิภาพในการปฏิบัติงานให้ดียิ่งขึ้น หรือเพื่อป้องกันความไม่สอดคล้อง เป็นต้น
- **เกณฑ์การตรวจประเมิน (Audit Criteria)** หมายถึง มาตรฐาน กฎหมาย หรือชุดของนโยบาย ขั้นตอนการดำเนินการ หรือข้อกำหนดที่ใช้อ้างอิง หลักเกณฑ์ วิธีการ และเงื่อนไข และระเบียบอื่น ๆ เพื่อนำไปเปรียบเทียบกับหลักฐานการตรวจประเมินเพื่อการรับรอง
- **หลักฐานการตรวจประเมิน (Audit Evidence)** หมายถึง บันทึกข้อมูล ข้อเท็จจริงหรือข้อมูลอื่นที่เกี่ยวข้องกับเกณฑ์การตรวจประเมินและสามารถทวนสอบได้
- **สิ่งที่พบจากการตรวจประเมิน (Audit Findings)** หมายถึง ผลจากการประเมินหลักฐานการตรวจประเมินที่เก็บรวบรวมได้ แล้วนำมาเปรียบเทียบกับเกณฑ์การตรวจประเมิน เพื่อประเมินบ่งชี้ถึงระดับความสอดคล้อง ความไม่สอดคล้อง ความไม่สอดคล้องย่อย ความไม่สอดคล้องสำคัญ และโอกาสในการปรับปรุงกับเกณฑ์การตรวจประเมิน

2. หลักเกณฑ์ วิธีการ และเงื่อนไข

2.1 ขั้นตอนการตรวจประเมิน

2.1.1 ทั่วไป

- (1) การตรวจประเมินจะดำเนินการตามขอบข่าย ภาษา และพื้นที่ที่เปิดให้บริการ
- (2) การตรวจประเมินเพื่อการรับรอง ประกอบด้วย
 - การตรวจประเมินขั้นตอนที่ 1
 - การตรวจประเมินขั้นตอนที่ 2
- (3) ระยะเวลาในการตรวจประเมินขึ้นอยู่กับจำนวนพนักงานในขอบข่ายการตรวจประเมิน ขนาดกิจกรรม เทคโนโลยีที่ใช้ กฎระเบียบที่เกี่ยวข้อง การว่าจ้างหน่วยงานภายนอกในการดำเนินกิจกรรม ภายใต้ขอบข่ายการตรวจประเมิน จำนวนสถานประกอบการ จำนวนสาขาที่ขอรับการตรวจประเมินเพื่อการรับรอง และจำนวนสมาชิกในคณะผู้ตรวจประเมิน
- (4) ผู้รับการตรวจประเมินต้องยินยอมให้ผู้แทนจากสำนักงาน หรือบุคคลอื่นใดที่สำนักงานแจ้งรายชื่อเข้าร่วมสังเกตการณ์การตรวจประเมินของคณะผู้ตรวจประเมินของสำนักงาน ภายใต้ขอบข่ายที่ขอรับรองได้ตลอดระยะเวลาการตรวจประเมินเมื่อสำนักงานร้องขอ
- (5) ผู้รับการตรวจประเมินต้องให้ความร่วมมือแก่สำนักงานในการตรวจประเมินทุกครั้ง รวมทั้งต้องจัดเตรียมเอกสารและบันทึกที่เกี่ยวข้องกับการดำเนินงานเพื่อการตรวจสอบ และให้การอำนวยความสะดวกในการเข้าถึงอุปกรณ์ สถานที่ พื้นที่ บุคลากร และผู้รับจ้างของผู้รับการตรวจประเมิน ตลอดจนการสืบสวนข้อร้องเรียน
- (6) รูปแบบการตรวจประเมิน อาจใช้รูปแบบการตรวจประเมินอื่นนอกเหนือจากการเข้าตรวจประเมินด้วยตัวบุคคล ณ สถานประกอบการ/สถานที่ที่จะตรวจประเมินได้ตามความจำเป็นและความเหมาะสม เช่น การตรวจประเมินทางไกล การตรวจประเมิน ณ สถานประกอบการร่วมกับการตรวจประเมินทางไกล

สำนักงานอาจพิจารณาตรวจประเมินทางไกล ในกรณีต่อไปนี้

- ผู้ยื่นคำขอไม่มีการดำเนินกิจกรรมใด ๆ ขององค์กรภายในขอบข่ายการรับรอง ณ สถานที่ทางกายภาพ
- การเดินทางของคณะผู้ตรวจประเมินไปยังสถานประกอบการ/สถานที่ที่จะตรวจประเมินของผู้ยื่นคำขอมีเหตุผลที่ไม่สมควร/เหมาะสม เช่น เหตุผลด้านความปลอดภัย ข้อจำกัดในการเดินทาง
- แผนการตรวจประเมินมีการเปลี่ยนแปลงที่ไม่สามารถหลีกเลี่ยงได้ เช่น ประเด็นส่วนตัว การเปลี่ยนแปลงลำดับความสำคัญทางธุรกิจ
- จำนวนของสถานประกอบการที่จะตรวจประเมินยากที่จะครบถ้วนภายในระยะเวลาที่กำหนด
- ผู้ยื่นคำขอมีการนำระบบการจัดการไปปฏิบัติอย่างเป็นระบบ ที่บันทึก ข้อมูล และอื่น ๆ สามารถทบทวน ณ สถานที่ใด ๆ ได้ แม้ว่าจะมีการดำเนินงานนั้นอยู่สถานที่ใดก็ตาม
- การตรวจประเมินสำหรับการขยายขอบข่ายการรับรองจากเดิมเพียงเล็กน้อย
- ผู้ยื่นคำขอมีบันทึกความสอดคล้องที่ตรวจสอบแล้วว่าสามารถทวนสอบย้อนหลัง ณ สถานที่ที่ทำการตรวจประเมินทางไกลได้

- ระดับความเสี่ยงของการตรวจประเมินที่สำนักงานประเมินอยู่ในระดับต่ำ
- กิจกรรมที่วางแผนไว้สำหรับการตรวจประเมิน ณ สถานประกอบการไม่สามารถดำเนินการได้ครบถ้วน และการขยายเวลาตรวจประเมิน ณ สถานประกอบการไม่ใช่ทางเลือก/การแก้ปัญหาที่ดีที่สุด
- สถานการณ์ที่จำเป็นต้องให้คณะผู้ตรวจประเมินตรวจติดตามผลการแก้ไขความไม่สอดคล้อง แต่ไม่สามารถตรวจติดตามผล ณ สถานประกอบการได้ภายในกรอบเวลาที่จำกัด
- ผู้ตรวจประเมินหรือคณะผู้ตรวจประเมินของสำนักงานมีความคุ้นเคยกับระบบการจัดการและแนวปฏิบัติของผู้ยื่นคำขอ

ก่อนการตรวจประเมินทางไกล สำนักงานจะทำการประเมินความเสี่ยงและโอกาสที่อาจมีผลต่อประสิทธิภาพของการตรวจประเมินทุกครั้งที่มีการใช้เทคโนโลยีสารสนเทศและการสื่อสารในการตรวจประเมินภายใต้สภาวะเดียวกัน รวมถึงการเลือกใช้เทคโนโลยีและวิธีการจัดการกับความเสี่ยงและโอกาส

เทคโนโลยีสารสนเทศและการสื่อสารที่ใช้ในการตรวจประเมินทางไกล ต้องได้รับการยินยอม/มีการตกลงกันเป็นลายลักษณ์อักษรจากสำนักงานและผู้ยื่นคำขอก่อน

สำนักงานอาจจำกัดหรือไม่ดำเนินการตรวจประเมินทางไกลในกรณีต่อไปนี้

- 1) กรณีที่ข้อกำหนดอันเนื่องมาจากเงื่อนไขด้านกฎหมาย กฎระเบียบที่เกี่ยวข้องได้ระบุไว้ว่าต้องดำเนินการตรวจประเมิน ณ สถานประกอบการเท่านั้น หรือห้ามมิให้ดำเนินการตรวจประเมินทางไกล
- 2) มีความเสี่ยงที่จะไม่สามารถตรวจประเมินให้เป็นไปตามวัตถุประสงค์
- 3) สำนักงานอาจพิจารณาไม่ตรวจประเมินทางไกล เช่น กรณีที่ผู้ยื่นคำขอมีประวัติความไม่สอดคล้อง ณ สถานที่ที่จะตรวจประเมิน ในระหว่างการตรวจประเมินเพื่อการรับรอง ผู้ยื่นคำขอมีสิ่งอำนวยความสะดวกใหม่ ขอบข่ายและการเปลี่ยนแปลงที่มีนัยสำคัญ การไม่ได้รับการตรวจประเมิน ณ สถานประกอบการภายในช่วงเวลาที่ยื่นคำขอได้ขยายระยะเวลาให้ ทั้งนี้ สำนักงานจะมีการพิจารณาเป็นกรณี ๆ ไป

(7) กรณีที่ไม่สามารถตรวจประเมินหลังพระอาทิตย์ตกดินได้ ให้ดำเนินการตรวจสอบผลการปฏิบัติตามบันทึกคุณภาพของผู้ยื่นคำขอในระหว่างการตรวจประเมินในเวลาปกติ

2.1.2 การกำหนดคณะผู้ตรวจประเมิน

(1) คณะผู้ตรวจประเมินที่ดำเนินการตรวจประเมินในแต่ละครั้งอย่างเป็นทางการ ต้องเป็นผู้ตรวจประเมินซึ่งเป็นหัวหน้าผู้ตรวจประเมิน หรือเป็นผู้ตรวจประเมินซึ่งประกอบด้วยหัวหน้าผู้ตรวจประเมินและผู้ตรวจประเมิน ที่สำนักงานมอบหมาย ทั้งนี้ คณะผู้ตรวจประเมินให้มีจำนวนตามความเหมาะสม และอาจมีผู้เชี่ยวชาญด้านเทคนิคเข้าร่วมในคณะผู้ตรวจประเมินด้วยก็ได้ ซึ่งต้องกำหนดอำนาจหน้าที่ให้ชัดเจน และแจ้งให้ผู้ยื่นคำขอทราบ

(2) คณะผู้ตรวจประเมินต้องมีคุณสมบัติและไม่มีลักษณะต้องห้าม ดังนี้

- (2.1) เป็นบุคคลที่มีคุณสมบัติตามที่สำนักงานกำหนด
- (2.2) มีความรู้เกี่ยวกับเกณฑ์การตรวจประเมิน และเกณฑ์การรับรอง
- (2.3) มีความรู้ความเข้าใจในวิธีการตรวจประเมิน และเอกสารการตรวจประเมิน
- (2.4) มีความรู้ความสามารถทางเทคนิคตามเกณฑ์การตรวจประเมินที่ขอรับการรับรอง

(2.5) มีความสามารถในการสื่อความ

(2.6) ปราศจากผลประโยชน์ที่อาจทำให้สมาชิกในคณะผู้ตรวจประเมิน ปฏิบัติตนอย่างไม่เป็นกลาง ไม่น่าเชื่อถือ หรืออย่างไม่เสมอภาค รวมทั้ง

(2.6.1) ผู้ตรวจประเมินต้องไม่เคยให้คำปรึกษา หรือเป็นวิทยากรภายใน (In-house Training) หรือทำหน้าที่เป็นที่ปรึกษาให้แก่ผู้ยื่นคำขอภายในระยะเวลา 2 ปี ที่ผ่านมา ซึ่งอาจมีผลต่อกระบวนการตรวจประเมินและการตัดสินใจให้การรับรอง

(2.6.2) ผู้ตรวจประเมินต้องไม่เป็นผู้ร่วมลงทุน ผู้ถือหุ้น หรือหุ้นส่วนในหน่วยงานของผู้ยื่นคำขอ

(2.6.3) ผู้ตรวจประเมินต้องเป็นอิสระไม่ถูกกดดันจากผู้ขอรับการตรวจประเมิน และผู้ตรวจประเมินต้องไม่มีแรงกดดันหรือมีอำนาจเหนือผู้ขอรับการตรวจประเมิน เพื่อให้เกิดความโปร่งใส และเป็นกลาง

(2.6.4) ผู้ตรวจประเมินต้องไม่เป็นผู้ที่เข้าข่ายอย่างใดอย่างหนึ่ง ได้แก่ ผู้จัดหา ผู้ออกแบบผลิตภัณฑ์ ผู้ให้บริการ ผู้พัฒนาบริการ ผู้ประกอบการ หรือ ผู้พัฒนา กระบวนการหรือระบบ ทั้งในส่วนของตนเองและนายจ้าง ในระยะเวลา 2 ปีที่ผ่านมา

(3) สำนักงานต้องแจ้งชื่อคณะผู้ตรวจประเมินให้ผู้ยื่นคำขอทราบและยืนยันข้อมูลก่อนการตรวจประเมิน

2.1.3 การตรวจประเมินเพื่อการรับรอง ประกอบด้วย การตรวจประเมินขั้นตอนที่ 1 และการตรวจประเมินขั้นตอนที่ 2

- การตรวจประเมินขั้นตอนที่ 1

เพื่อตรวจประเมินความพร้อมขององค์กรทั้งทางด้านเอกสาร ความรู้ความเข้าใจในข้อกำหนดของระบบการจัดการที่ขอรับการรับรอง รวมถึงการนำไปปฏิบัติ เพื่อประกอบการนัดหมายการตรวจประเมินขั้นตอนที่ 2

การตรวจประเมินในขั้นตอนนี้ มีวัตถุประสงค์ ดังต่อไปนี้

(1) เพื่อรวบรวมข้อมูลที่เกี่ยวข้องกับระบบการจัดการ และกิจกรรม กระบวนการ เครื่องมือ กฎหมาย ที่ตั้ง ที่ครอบคลุมตามระบบการจัดการ เอกสารในระบบการจัดการและเอกสารประกอบอื่น ๆ ที่เกี่ยวข้อง

(2) เพื่อประเมินเอกสารในระบบการจัดการที่ขอรับการรับรอง

(3) เพื่อประเมินความเพียงพอเกี่ยวกับการออกแบบระบบการจัดการในบริบทขององค์กร ประเมินความเสี่ยงและการจัดการความเสี่ยง ระบบการควบคุม นโยบาย วัตถุประสงค์ด้านความปลอดภัยของข้อมูลสารสนเทศ

(4) เพื่อทบทวนสถานะและความเข้าใจของผู้ยื่นคำขอในส่วนที่เกี่ยวข้องกับข้อกำหนดมาตรฐานของระบบการจัดการที่ขอรับการรับรอง โดยเฉพาะอย่างยิ่งในส่วนที่เกี่ยวข้องกับสมรรถนะหลักหรือลักษณะปัญหาที่มีนัยสำคัญ กระบวนการวัตถุประสงค์และการดำเนินการของระบบการจัดการที่ขอรับการรับรอง

(5) เพื่อยืนยันขอบข่ายและขอบเขตการรับรอง รวมถึงรวบรวมข้อมูลที่จำเป็นที่เกี่ยวข้องกับขอบข่ายของระบบการจัดการ กระบวนการ ที่ตั้งและจำนวนสถาน

ประกอบการที่ขอรับการรับรอง กฎหมายและระเบียบที่เกี่ยวข้องและมีผลกระทบ ต่อระบบที่ขอรับการรับรอง และการปฏิบัติตามกฎหมายและกฎระเบียบที่เกี่ยวข้อง ดังกล่าว

- (6) เพื่อพิจารณาความพร้อมสำหรับการตรวจประเมินขั้นตอนที่ 2
- (7) เพื่อทบทวนการจัดสรรทรัพยากร และตกลงกับผู้ยื่นคำขอเกี่ยวกับรายละเอียดในการตรวจประเมินขั้นตอนที่ 2
- (8) เพื่อนำข้อมูลเกี่ยวกับความเข้าใจในระบบการจัดการของผู้ยื่นคำขอ และการดำเนินการของสถานประกอบการในหัวข้อที่มีโอกาสเกิดผลกระทบที่มีนัยสำคัญ ไปใช้ในการวางแผนการตรวจประเมินขั้นตอนที่ 2
- (9) เพื่อประเมินว่าผู้ยื่นคำขอมีการตรวจประเมินภายในและการทบทวนของฝ่ายบริหาร รวมถึงความพร้อมสำหรับการตรวจประเมินขั้นตอนที่ 2
- (10) เพื่อหารือกับผู้ยื่นคำขอเกี่ยวกับช่วงเวลาที่จะดำเนินการแก้ไขประเด็นที่พบจากการตรวจประเมินสำหรับขั้นตอนนี้ เพื่อประกอบการนัดหมายกำหนดเวลาในการตรวจประเมินขั้นตอนที่ 2 ต่อไป

การตรวจประเมินขั้นตอนที่ 1 สำนักงานจะดำเนินการตรวจประเมิน ณ สถานประกอบการ ซึ่งผลจากการตรวจประเมินในขั้นตอนนี้ สำนักงานจะจัดทำรายงานสิ่งที่ตรวจพบจากการตรวจประเมินเป็นลายลักษณ์อักษร และแจ้งให้ผู้ยื่นคำขอทราบ โดยประเด็นที่รายงานนี้จะครอบคลุมประเด็นความไม่สอดคล้องที่มีโอกาสตรวจพบในการตรวจประเมินขั้นตอนที่ 2

กรณีผู้ยื่นคำขอได้รับการตรวจประเมินขั้นตอนที่ 1 แล้ว และพบประเด็นที่ตรวจพบเป็นจำนวนมากและส่วนใหญ่เป็นประเด็นความไม่สอดคล้องที่มีโอกาสตรวจพบในการตรวจประเมินขั้นตอนที่ 2 ซึ่งส่งผลให้ความพร้อมสำหรับการนัดหมายเพื่อตรวจประเมินขั้นตอนที่ 2 ใช้เวลานาน สำนักงานอาจดำเนินการตรวจประเมินขั้นตอนที่ 1 ใหม่ ณ สถานประกอบการได้อีก 1 ครั้ง กรณีตรวจประเมินขั้นตอนที่ 1 เกิน 2 ครั้ง ให้เสนอผู้ตัดสินการรับรอง พิจารณาไม่ให้การรับรอง ทั้งนี้ หากผู้ยื่นคำขอประสงค์เข้ารับการตรวจประเมินต่อไปให้ผู้ยื่นคำขอการรับรองใหม่

กรณีผู้ยื่นคำขอมีการเปลี่ยนแปลงระบบการจัดการอย่างมีนัยสำคัญ สำนักงานอาจพิจารณาให้มีการตรวจประเมินขั้นตอนที่ 1 ใหม่ ทั้งหมดหรือบางส่วน ณ สถานประกอบการอีกครั้ง ก่อนการตรวจประเมินขั้นตอนที่ 2

กรณีผู้ยื่นคำขอแจ้งความประสงค์ และกรณีถ้ามีการนัดหมายการตรวจประเมินขั้นตอนที่ 2 เกิน 180 วัน นับจากวันตรวจประเมินขั้นตอนที่ 1 สำนักงานอาจพิจารณาให้มีการตรวจประเมินขั้นตอนที่ 1 ใหม่ ณ สถานประกอบการอีกครั้ง หรือทำการประเมินเอกสารก่อนการตรวจประเมินขั้นตอนที่ 2 โดยไม่ต้องยื่นคำขอใหม่

- การตรวจประเมินขั้นตอนที่ 2

การตรวจประเมินเพื่อการรับรอง ซึ่งจะดำเนินการตรวจประเมิน ณ สถานประกอบการ หรือการตรวจประเมินทางไกล โดยมีวัตถุประสงค์เพื่อประเมินความสอดคล้องและประสิทธิผลของการนำระบบที่ขอรับการรับรองไปปฏิบัติ อันมีรายละเอียด ดังต่อไปนี้

- (1) พิจารณาความเป็นผู้นำของผู้บริหารระดับสูง และความมุ่งมั่นของผู้ยื่นคำขอที่มีต่อวัตถุประสงค์ด้านความปลอดภัยของสารสนเทศ
- (2) ประเมินความเสี่ยงที่เกี่ยวข้องด้านความปลอดภัยของสารสนเทศ เพื่อพิจารณาผลลัพธ์ที่สอดคล้อง ถูกต้อง เป็นไปตามเกณฑ์การประเมินความเสี่ยงที่กำหนด
- (3) พิจารณามาตรการควบคุมว่าสอดคล้องตามผลประเมินความเสี่ยงและการจัดการความเสี่ยงด้านความปลอดภัยของสารสนเทศ
- (4) ประเมินความสอดคล้องและประสิทธิผลของการนำระบบที่ขอรับการรับรองไปปฏิบัติ
- (5) พิจารณาประสิทธิภาพและประสิทธิผลของระบบการจัดการ เทียบกับวัตถุประสงค์ด้านความปลอดภัยของสารสนเทศ
- (6) เพื่อพิจารณาความสอดคล้องระหว่างมาตรการควบคุมที่กำหนดใน Statement of Applicability (SoA) ผลการประเมินความเสี่ยง กระบวนการจัดการความเสี่ยง และนโยบายและวัตถุประสงค์ด้านความปลอดภัยของสารสนเทศ
- (7) เพื่อพิจารณาการนำการควบคุมไปปฏิบัติ โดยคำนึงถึงบริบทภายนอกและภายใน ความเสี่ยงที่เกี่ยวข้อง การติดตาม การวัดผล และวิเคราะห์กระบวนการ และการควบคุมด้านความปลอดภัยของสารสนเทศ เพื่อพิจารณาการควบคุมที่จัดทำได้ ดำเนินการ และมีประสิทธิภาพ
- (8) เพื่อให้โปรแกรม กระบวนการ ขั้นตอนการปฏิบัติงาน บันทึก การตรวจประเมิน ภายใน การทบทวนประสิทธิผลของระบบการจัดการ ได้รับการตัดสินใจจากผู้บริหารสูงสุด
- (9) เพื่อพิจารณาว่ามีการกำหนดนโยบาย และวัตถุประสงค์ด้านความปลอดภัยของสารสนเทศ
- (10) เพื่อให้ข้อมูลและหลักฐานของการเป็นไปตามข้อกำหนดของระบบที่ขอรับการรับรองทั้งหมด
- (11) เพื่อให้ระบบและสมรรถนะการดำเนินการว่าสอดคล้องตามกฎหมาย
- (12) เพื่อให้มีการควบคุมกระบวนการ
- (13) เพื่อกำหนดความรับผิดชอบของฝ่ายบริหารที่มีหน้าที่ความรับผิดชอบสำหรับนโยบายของลูกค้า ซึ่งต้องมีการจัดเตรียมรายการตรวจประเมิน (Check list) และแผนการตรวจประเมิน โดยสำนักงานจะจัดส่งแผนการตรวจประเมินให้ผู้ยื่นคำขอ เพื่อให้ความเห็นชอบก่อนการตรวจประเมินการตรวจประเมิน ณ สถานที่ประกอบการ ประกอบด้วย 6 ขั้นตอนย่อย
 - 1) การประชุมเปิดการตรวจประเมิน (Opening meeting)
หัวหน้าผู้ตรวจประเมินประชุมเปิดการตรวจประเมินร่วมกับผู้บริหารระดับสูงหรือผู้แทนผู้บริหารของผู้ยื่นคำขอ
 - 2) การดำเนินการการตรวจประเมิน
การดำเนินการการตรวจประเมินประกอบด้วย การสัมภาษณ์ การตรวจเอกสาร และการสังเกตกิจกรรม และสถานะของพื้นที่ที่ตรวจ ซึ่งอาจรวมถึงสถานที่อื่น ๆ ขึ้นอยู่กับโครงสร้างองค์กรของผู้ยื่นคำขอ และหน้าที่

ความรับผิดชอบ ขอบข่ายการดำเนินงานของสถานที่ต่าง ๆ เหล่านั้น ให้บันทึกสิ่งที่อาจเป็นเหตุนำไปสู่ความไม่สอดคล้องตามข้อกำหนด การตรวจประเมินอาจตรวจประเมินรายละเอียดที่ไม่ได้เขียนไว้ในรายการตรวจประเมินก็ได้ ข้อมูลที่ได้จากการสัมภาษณ์จะต้องยืนยันจากแหล่งข้อมูลอิสระอื่น ๆ เช่น การสังเกต การวัด และการบันทึก

ในระหว่างการตรวจประเมิน หัวหน้าคณะผู้ตรวจประเมินอาจเปลี่ยนแปลงแผนตรวจประเมินได้ตามความเหมาะสมโดยความเห็นชอบของผู้ยื่นคำขอ เพื่อให้การตรวจประเมินเป็นไปอย่างมีประสิทธิภาพและบรรลุวัตถุประสงค์ของการตรวจประเมิน

ทั้งนี้ ในระหว่างการตรวจประเมินขั้นตอนที่ 2 หากพบความไม่สอดคล้องสำคัญจำนวนมากที่แสดงให้เห็นว่าผู้ยื่นคำขอยังไม่ได้ดำเนินการตามมาตรฐานที่ขอการรับรองอย่างมีประสิทธิภาพเพียงพอ และผู้ยื่นคำขอมีความประสงค์ที่จะขอยุติการตรวจประเมินเพื่อให้มีการตรวจประเมินทั้งระบบใหม่ทั้งหมดภายใน 180 วันนับจากวันที่แจ้งยุติการตรวจประเมิน ทั้งนี้ สำนักงานจะดำเนินการตามความประสงค์ดังกล่าวได้ ผู้ยื่นคำขอต้องเป็นผู้รับผิดชอบค่าธรรมเนียมการตรวจประเมินใหม่ตามที่สำนักงานกำหนด โดยไม่ต้องยื่นคำขอใหม่

3) การบันทึกสิ่งที่พบจากการตรวจประเมิน

สิ่งที่พบจากการตรวจประเมินทั้งหมดต้องบันทึกไว้ และหลังจากเสร็จสิ้นการตรวจประเมิน คณะผู้ตรวจประเมินต้องประชุมร่วมกันเพื่อวิเคราะห์ข้อมูลและหลักฐานการตรวจประเมินทั้งหมดที่รวบรวมได้ในระหว่างการตรวจประเมินขั้นตอนที่ 1 และการตรวจประเมินขั้นตอนที่ 2 เพื่อทบทวนสิ่งที่ตรวจพบและสรุปผลการตรวจประเมิน รวมทั้งการสรุปว่าสิ่งที่ตรวจพบรายการใดถือเป็นความไม่สอดคล้อง การเขียนรายงานความไม่สอดคล้องต้องกระชับ มีหลักฐานสนับสนุนที่เป็นรูปธรรม และให้อ้างอิงข้อกำหนดในมาตรฐานให้ชัดเจน โดยบันทึกความไม่สอดคล้องในรายงานความไม่สอดคล้อง

สำหรับการตรวจประเมินขั้นตอนที่ 1 คณะผู้ตรวจประเมินจะรายงานสิ่งที่ตรวจพบจากการตรวจประเมินโดยไม่ระบุรายการใดเป็นความไม่สอดคล้อง

4) การประชุมปิดการตรวจประเมิน

หลังจากการตรวจประเมินแล้วเสร็จ คณะผู้ตรวจประเมินดำเนินการประชุมปิดการตรวจประเมิน เพื่อรายงานผลการตรวจประเมิน และสิ่งที่ตรวจพบจากการตรวจประเมินขั้นตอนที่ 1 หรือความไม่สอดคล้องที่พบจากการตรวจประเมินขั้นตอนที่ 2 (ถ้ามี) ต่อผู้บริหารระดับสูงของผู้รับการตรวจประเมิน เพื่อทำความเข้าใจผลของการตรวจประเมินให้ถูกต้องตรงกัน และผู้บริหาร/ผู้แทนของผู้รับการตรวจประเมินลงชื่อรับทราบความไม่สอดคล้อง (ถ้ามี) และจากนั้นจัดส่งให้ผู้แทนองค์กร 1 ชุดและคณะผู้ตรวจประเมินเก็บไว้ 1 ชุด

ในกรณีที่พบความไม่สอดคล้อง คณะผู้ตรวจประเมินจะแจ้งให้ผู้ยื่นคำขอจัดทำแนวทางการแก้ไขและป้องกันความไม่สอดคล้องให้สำนักงานพิจารณาภายใน 30 วันนับจากวันที่ออกรายงานความไม่สอดคล้อง

หากไม่จัดส่งแนวทางการแก้ไขและป้องกันความไม่สอดคล้องให้สำนักงานภายในระยะเวลาที่กำหนด สำนักงานอาจนำเสนอผู้ตัดสินการรับรองเพื่อพิจารณาตรวจประเมินขั้นตอนที่ 2 ใหม่

5) การเขียนรายงานการตรวจประเมินให้ผู้ยื่นคำขอทราบ

หลังจากตรวจประเมินแล้วเสร็จ หัวหน้าคณะผู้ตรวจประเมิน/ผู้ตรวจประเมินจะจัดทำรายงานผลการตรวจประเมิน และเสนอผู้ตัดสินการรับรอง เพื่อพิจารณาให้การรับรอง เพื่อแจ้งผลการตรวจประเมินให้ผู้ยื่นคำขอทราบ

โดยเอกสารที่ส่งให้ผู้ยื่นคำขอ ประกอบด้วย

- รายงานผลการตรวจประเมิน
- รายงานสิ่งที่ตรวจพบจากการตรวจประเมินขั้นตอนที่ 1 หรือรายงานความไม่สอดคล้องที่พบจากการตรวจประเมิน (ถ้ามี)

6) การพิจารณาผล

- กรณีไม่พบความไม่สอดคล้อง คณะผู้ตรวจประเมินสามารถสรุปรายงานเสนอผู้ตัดสินการรับรองพิจารณาตัดสินให้การรับรองได้
- กรณีพบเฉพาะความไม่สอดคล้องย่อย คณะผู้ตรวจประเมินสามารถสรุปรายงานเสนอผู้ตัดสินการรับรองพิจารณาให้การรับรองได้ หลังจากที่คุณคณะผู้ตรวจประเมินพิจารณาแนวทางการแก้ไขและป้องกันความไม่สอดคล้องที่เกิดขึ้นตามที่ผู้ยื่นคำขอเสนอแล้วเห็นว่าเป็นแนวทางที่ยอมรับได้
- กรณีพบความไม่สอดคล้องสำคัญตั้งแต่ 1 รายการขึ้นไป คณะผู้ตรวจประเมินจะยังไม่สามารถสรุปรายงานเสนอผู้ตัดสินการรับรองพิจารณาให้การรับรองได้ และต้องมีการดำเนินการดังต่อไปนี้

- (1) นัดหมายผู้รับการตรวจประเมินเพื่อตกลงช่วงเวลาที่ดำเนินการตรวจติดตามการแก้ไขความไม่สอดคล้อง (Follow up audit) ซึ่งช่วงระยะเวลาการแก้ไขความไม่สอดคล้องต้องไม่เกิน 180 วันนับจากวันที่ตรวจประเมินเสร็จสิ้น หากระยะเวลาการแก้ไขเกิน 180 วัน ให้ดำเนินการตรวจประเมินใหม่ทั้งระบบ และผู้ยื่นคำขอต้องยื่นแบบยื่นคำขอใหม่

ในกรณีที่อยู่ในช่วงระยะเวลาการแก้ไขความไม่สอดคล้อง 180 วัน มีการปรับปรุงเปลี่ยนแปลงระบบการจัดการที่เกี่ยวข้องกับการรับรอง หรือเอกสารที่เกี่ยวข้องที่ตรวจประเมินนั้น ๆ เป็นจำนวนมาก และผู้ยื่นคำขอมีความประสงค์ขอให้ตรวจประเมินใหม่ทั้งระบบโดยยกเลิกความไม่สอดคล้องเดิม สำนักงานสามารถ

ดำเนินการตามความประสงค์ของผู้ยื่นคำขอได้ โดยผู้ยื่นคำขอต้องยื่นแบบยื่นคำขอใหม่

- (2) ในการตรวจติดตามการแก้ไขความไม่สอดคล้องสำคัญ คณะผู้ตรวจประเมินจะตรวจติดตามเฉพาะรายการที่เป็นความไม่สอดคล้องสำคัญเท่านั้น และอาจสุ่มตรวจที่หน่วยงาน/กิจกรรมใด ๆ ที่เกี่ยวข้องได้
- ทั้งนี้ หากพบว่าการแก้ไขความไม่สอดคล้องสำคัญไม่มีประสิทธิผล และได้พ้นระยะเวลา 180 วันนับจากวันที่ตรวจประเมินเสร็จสิ้น สำนักงานจะดำเนินการตรวจประเมินใหม่ทั้งระบบ โดยผู้ยื่นคำขอต้องยื่นแบบยื่นคำขอใหม่

2.1.4 การตรวจติดตามผล

- หลังจากผู้ยื่นคำขอผ่านการตรวจประเมินและได้รับการรับรองแล้ว สำนักงานจะตรวจติดตามผลอย่างสม่ำเสมอ โดยสำนักงานจะจัดทำแผนการตรวจเพื่อตรวจติดตามผลอย่างน้อยปีละ 1 ครั้ง นับจากวันที่ตัดสินใจให้การรับรอง โดยการตรวจติดตามผลจะดำเนินการตรวจประเมินจนครบทุกข้อกำหนด ภายในกำหนดระยะเวลาของหนังสือรับรองหรือก่อนครบกำหนดระยะเวลาให้การรับรอง
- การตรวจติดตามผล สำนักงานจะดำเนินการตรวจประเมินการประเมินความเสี่ยงด้านความปลอดภัยของสารสนเทศ ระบบควบคุม การตรวจประเมินภายใน การทบทวนโดยฝ่ายบริหาร การดำเนินการแก้ไข การสื่อสารจากผู้มีส่วนได้เสียภายนอก ประสิทธิภาพของระบบการจัดการ การบรรลุวัตถุประสงค์ของนโยบายความมั่นคงปลอดภัยสารสนเทศของลูกค้า ขั้นตอนการประเมินและการทบทวนการปฏิบัติตามกฎหมายและข้อบังคับด้านความมั่นคงปลอดภัยสารสนเทศ การเปลี่ยนแปลงการควบคุม การเปลี่ยนแปลง SoA การแก้ไขความไม่สอดคล้องที่พบจากการตรวจประเมินครั้งก่อน การดำเนินการต่อข้อร้องเรียน แนวทางการพัฒนาอย่างต่อเนื่อง การใช้เครื่องหมายรับรอง เครื่องหมายรับรองระบบงาน (ถ้ามี) และ/หรือการอ้างอิงถึงการรับรอง เพื่อใช้ประกอบการพิจารณาการตรวจติดตามผล
- ผู้ได้รับการรับรองต้องรักษาและปฏิบัติตามขั้นตอนการดำเนินงานขององค์กร ให้เป็นไปตามข้อกำหนดทั่วไปว่าด้วยหลักเกณฑ์ วิธีการ และเงื่อนไขในการรับรองระบบการจัดการ (RE-01) หากผู้ได้รับการรับรองไม่สามารถปฏิบัติตามได้อาจมีผลให้ต้อง ลดขอบข่าย พักใช้ หรือเพิกถอนการรับรองที่รับการรับรองได้
- กิจกรรมการตรวจติดตามผล ต้องรวมถึงการตรวจประเมิน ณ สถานที่ประกอบการที่ได้รับ การรับรองว่ายังคงเป็นไปตามระบบที่ได้รับการรับรองหรือไม่ นอกจากนี้ การตรวจติดตามผลอาจรวมถึงกิจกรรมการตรวจติดตามผลอื่น ๆ ด้วย เช่น
 - (1) การสอบถามผู้ได้รับการรับรองเกี่ยวกับการรับรอง
 - (2) การทบทวนเอกสาร ข้อมูลของผู้ได้รับการรับรองที่มีการดำเนินการ เช่น เอกสารประชาสัมพันธ์ เว็บไซต์ (website) เป็นต้น
 - (3) การขอเอกสารและบันทึกจากผู้ได้รับการรับรอง
 - (4) วิธีการอื่น ๆ ในการเฝ้าระวังสมรรถนะของผู้ได้รับการรับรอง

แผนการตรวจติดตามผลที่ระบุไว้อย่างน้อยปีละ 1 ครั้ง อาจปรับแผนการตรวจติดตามผล ให้มีการตรวจเยี่ยมบ่อยครั้งขึ้นได้ เพื่อตรวจประเมินทั้งระบบโดยไม่ต้องแจ้งให้ทราบล่วงหน้า ในกรณีดังต่อไปนี้

- (1) มีเหตุอันทำให้สงสัยว่าสมรรถนะลดหย่อนลง
- (2) เมื่อมีการวิเคราะห์ข้อร้องเรียนหรือข้อมูลแล้วเห็นว่า ผู้ได้รับการรับรองไม่เป็นไปตามข้อกำหนด
- (3) ผลการตรวจประเมินครั้งก่อนในบางส่วนไม่เพียงพอ

สำนักงานขอสงวนสิทธิ์ในการดำเนินการตรวจประเมินกรณีพิเศษ โดยจะแจ้งให้ทราบล่วงหน้าในระยะเวลาอันสั้น (Short notice audit) สำหรับผู้ได้รับการรับรองในบางกรณีที่มีความจำเป็น เช่น

- (1) ต้องมีการสืบสวนข้อร้องเรียนของผู้ได้รับการรับรอง
 - (2) ทบทวนหรือติดตามผลกระทบที่เกิดจากการเปลี่ยนแปลงในสาระที่สำคัญ เช่น การเปลี่ยนแปลงสถานะทางกฎหมาย สถานะทางการค้า องค์กรหรือเจ้าของฝ่ายบริหาร ชื่อ ที่อยู่สถานประกอบการ ขอบข่ายที่ได้รับการรับรอง และการเปลี่ยนแปลงที่สำคัญของระบบและกระบวนการ
 - (3) ติดตามผลการพักใช้การรับรอง
- การตรวจติดตามผลที่กำหนดแผนไว้นี้ ให้ปฏิบัติตามขั้นตอนการตรวจประเมินขั้นตอนที่ 2 หรือการตรวจประเมินเพื่อต่ออายุ โดยอนุโลม โดยกรณีที่พบความไม่สอดคล้องย่อยให้ผู้ได้รับการรับรองเสนอแนวทางการแก้ไขและป้องกันความไม่สอดคล้องให้สำนักงานพิจารณาภายใน 30 วัน นับจากวันที่ออกรายงานความไม่สอดคล้อง หากพบว่าเป็นแนวทางที่ยอมรับได้ สำนักงานจะนำเสนอผู้ตัดสินใจการรับรองเพื่อทราบและคงไว้ซึ่งการรับรอง หรือในกรณีพบความไม่สอดคล้องสำคัญ (Major Nonconformity) ให้นัดหมายผู้ได้รับการรับรองเพื่อตกลงเวลาในการตรวจติดตามผลการแก้ไขความไม่สอดคล้องต่อไป หากผู้ได้รับการรับรองไม่สามารถดำเนินการได้ภายใน 180 วันนับจากวันที่ตรวจประเมินเสร็จสิ้น สำนักงานอาจแจ้งเตือนและ/หรืออาจนำเสนอคณะกรรมการเพื่อพิจารณาพักใช้ หรือเพิกถอนการรับรองต่อไป แล้วแต่กรณี หากผู้ได้รับการตรวจประเมินมีเหตุผลความจำเป็นหรือเหตุฉุกเฉินที่ไม่สามารถหลีกเลี่ยงได้ ให้สำนักงานพิจารณาดำเนินการและ/หรือนำเสนอผู้ตัดสินใจการรับรองเพื่อทราบหรือพิจารณาแล้วแต่กรณี
 - ในการตรวจติดตามการแก้ไขความไม่สอดคล้องสำคัญ คณะผู้ตรวจประเมินจะตรวจติดตามเฉพาะรายการที่เป็นความไม่สอดคล้องสำคัญเท่านั้น แต่อาจสุ่มตรวจที่หน่วยงาน/กิจกรรมใด ๆ ที่เกี่ยวข้องได้

ทั้งนี้หากพบว่าการแก้ไขความไม่สอดคล้องสำคัญไม่มีประสิทธิผล และเกินระยะเวลา 180 วัน นับจากวันที่ตรวจประเมินเสร็จสิ้น สำนักงานจะดำเนินการเสนอคณะกรรมการเพื่อพิจารณาพักใช้ หรือเพิกถอนการรับรอง ต่อไป

2.1.5 การตรวจประเมินเพื่อต่ออายุ

- ก่อนครบรอบอายุการรับรองสำนักงานจะดำเนินการตรวจสอบใหม่ทั้งกิจกรรม/ระบบเพื่อต่ออายุการรับรองสำหรับผู้ได้รับการรับรอง โดยผู้ได้รับการรับรองต้องยื่นแบบยื่นคำขอล่วงหน้าอย่างน้อย 180 วันก่อนหนังสือรับรองสิ้นอายุ
- เมื่อผู้ได้รับการรับรองแจ้งยืนยันการต่ออายุการรับรอง พร้อมยื่นแบบยื่นคำขอแล้ว สำนักงานจะดำเนินการนัดหมายและตรวจประเมินเพื่อต่ออายุทั้งระบบก่อนหนังสือรับรองสิ้นอายุ โดยขั้นตอนการตรวจประเมินเพื่อต่ออายุจะเหมือนกับการตรวจประเมินขั้นตอนที่ 2 และสำนักงานอาจยกเว้นการตรวจประเมินขั้นตอนที่ 1 โดยจะมีการทบทวนสมรรถนะระบบของผู้ได้รับการรับรองตลอดช่วงที่ได้รับการรับรอง รวมถึงทบทวนรายงานผลการตรวจติดตามผลที่ได้รับ การรับรองในรอบการรับรองที่ผ่านมา กรณีที่ผู้ได้รับการรับรองมีการเปลี่ยนแปลงใด ๆ ที่มีนัยสำคัญต่อระบบการจัดการที่ได้รับการรับรอง เช่น การเปลี่ยนแปลงข้อกำหนดกฎหมายและกฎระเบียบ เป็นต้น สำนักงานอาจพิจารณาดำเนินการตรวจประเมินขั้นตอนที่ 1 โดยการประเมินเอกสาร และ/หรือตรวจประเมินขั้นตอนที่ 1 อีกครั้งซึ่งการดำเนินการดังกล่าวสำนักงานจะมีการพิจารณาเป็นกรณี ๆ ไป
- การกำหนดวันที่มีผลให้การรับรอง สำนักงานจะกำหนดวันที่มีผลให้การรับรองต่อเนื่องจากหนังสือรับรองฉบับเดิมสำหรับกรณีที่ผู้ได้รับการรับรองมีการตรวจประเมินเพื่อต่ออายุก่อนหนังสือรับรองสิ้นอายุ รวมถึงกรณีพบความไม่สอดคล้องสำคัญ และผู้ได้รับการรับรองได้ดำเนินการแก้ไขและป้องกันความไม่สอดคล้องได้อย่างมีประสิทธิภาพก่อนหนังสือรับรองสิ้นอายุ หรือกรณีพบความไม่สอดคล้องย่อยและผู้ได้รับการรับรองจัดทำแนวทางการแก้ไขและป้องกันความไม่สอดคล้องและจัดส่งให้สำนักงานพิจารณาแล้วว่ายอมรับได้ก่อนหนังสือรับรองสิ้นอายุ หากผู้ได้รับการรับรองไม่สามารถดำเนินการตรวจประเมินเพื่อต่ออายุการรับรองได้ ก่อนหนังสือรับรองสิ้นอายุ ให้ถือว่า การตรวจประเมินดังกล่าวเป็นการตรวจประเมินเพื่อการรับรองใหม่ โดยจะกำหนดวันที่มีผลให้การรับรองนับถัดจากวันที่ผู้ตัดสินใจการรับรองมีมติให้การรับรอง

2.2 การตรวจกรณีองค์กรหลายสาขา

1. กรณีผู้ยื่นคำขอมีความประสงค์ขอการรับรองแบบหลายสาขา ต้องมีการดำเนินการ ดังนี้
 - 1) สถานประกอบการที่ขอรับการรับรองทั้งหมดดำเนินการภายใต้ระบบการจัดการเดียวกัน ซึ่งมีการบริหารจัดการและตรวจประเมินภายใน และการทบทวนโดยฝ่ายบริหารที่ส่วนกลาง
 - 2) สถานประกอบการสาขาทั้งหมดต้องรวมอยู่ในโปรแกรมการตรวจประเมินภายใน
 - 3) สถานประกอบการสาขาทั้งหมดต้องรวมอยู่ในโปรแกรมการทบทวนโดยฝ่ายบริหาร
2. สำนักงานจะดำเนินการตรวจประเมินเพื่อกำหนดหน่วยงานสาขาที่ตรวจประเมินในการตรวจประเมินขั้นตอนที่ 2 พร้อมกับการตรวจประเมินขั้นตอนที่ 1 หรือทำการตรวจเยี่ยม ณ สำนักงานส่วนกลาง และ/หรือหน่วยงานสาขา และ/หรือให้ผู้ยื่นคำขอจัดส่งข้อมูลให้สำนักงานตรวจสอบเพื่อกำหนดหน่วยงานสาขาที่จะตรวจติดตามผลหรือตรวจประเมินเพื่อต่ออายุต่อไป โดยเกณฑ์ที่ใช้กำหนดจำนวนหน่วยงานสาขาที่ตรวจประเมิน ให้ใช้เกณฑ์ดังต่อไปนี้

- 1) กลุ่มที่ 1 หน่วยงานสาขาต่าง ๆ ที่ขอรับการรับรอง/ได้รับการรับรองทั้งหมดมีกระบวนการ/กิจกรรมการดำเนินงานที่คล้ายกัน หรือสามารถจัดกลุ่มย่อยที่มีกระบวนการ/กิจกรรมการดำเนินงานที่คล้ายกัน ซึ่งสามารถสุ่มตัวอย่างเพื่อใช้เป็นตัวแทนกันได้
 - 2) กลุ่มที่ 2 หน่วยงานสาขาต่าง ๆ ที่ขอรับการรับรอง/ได้รับการรับรองทั้งหมดมีกระบวนการ/กิจกรรมการดำเนินงานที่เหมือนกันบางส่วน ซึ่งสามารถสุ่มตัวอย่างตามกลุ่มกระบวนการ/กิจกรรมที่เหมือนกันได้
 - 3) กลุ่มที่ 3 หน่วยงานสาขาต่าง ๆ ที่ขอรับการรับรอง/ได้รับการรับรองทั้งหมดมีกระบวนการ/กิจกรรมการดำเนินงานที่แตกต่างกัน ซึ่งไม่สามารถสุ่มตัวอย่างเพื่อใช้เป็นตัวแทนกันได้
3. การกำหนดจำนวนหน่วยงานสาขาและการคัดเลือกสาขาที่จะตรวจประเมิน
- 1) กลุ่มที่ 1 การพิจารณา กำหนดจำนวนหน่วยงานสาขาและการคัดเลือกสาขาที่จะตรวจประเมินให้ดำเนินการ ดังนี้
 - กรณีการตรวจประเมินเพื่อการรับรอง (การตรวจประเมินขั้นตอนที่ 2)

$$\text{สุ่มตรวจประเมินไม่น้อยกว่า } \sqrt{\text{จำนวนหน่วยงานสาขาที่ขอรับการรับรองทั้งหมด}}$$
 - กรณีการตรวจติดตามผล สุ่มตรวจประเมินในแต่ละครั้ง

$$\text{ไม่น้อยกว่า } 0.6 \sqrt{\text{จำนวนหน่วยงานสาขาที่ขอรับการรับรองทั้งหมด}}$$
 - กรณีการตรวจประเมินเพื่อต่ออายุ สุ่มตรวจประเมินในแต่ละครั้ง

$$\text{ไม่น้อยกว่า } 0.8 \sqrt{\text{จำนวนหน่วยงานสาขาที่ขอรับการรับรองใหม่ทั้งหมด}}$$
 - 2) กลุ่มที่ 2 การพิจารณา กำหนดจำนวนหน่วยงานสาขาและการคัดเลือกสาขาที่จะตรวจประเมินให้ดำเนินการ ดังนี้
 - กรณีการตรวจประเมินเพื่อการรับรอง (การตรวจประเมินขั้นตอนที่ 2)

$$\text{สุ่มตรวจประเมินไม่น้อยกว่า } \sqrt{\text{จำนวนหน่วยงานสาขาที่อยู่ในกลุ่มกระบวนการ/บริการเดียวกัน}}$$
 - กรณีการตรวจติดตามผล สุ่มตรวจประเมินในแต่ละครั้ง

$$\text{ไม่น้อยกว่า } 0.6 \sqrt{\text{จำนวนหน่วยงานสาขาที่อยู่ในกลุ่มกระบวนการ/บริการเดียวกัน}}$$
 - กรณีการตรวจประเมินเพื่อต่ออายุ สุ่มตรวจประเมินในแต่ละครั้ง

$$\text{ไม่น้อยกว่า } 0.8 \sqrt{\text{จำนวนหน่วยงานสาขาที่อยู่ในกลุ่มกระบวนการ/บริการเดียวกัน}}$$
 - 3) กลุ่มที่ 3 หน่วยงานสาขาต่าง ๆ ที่ขอรับการรับรอง/ได้รับการรับรองทั้งหมดมีกระบวนการ/กิจกรรมการดำเนินงานที่แตกต่างกัน ซึ่งไม่สามารถสุ่มตัวอย่างเพื่อใช้เป็นตัวแทนกันได้
 ให้ดำเนินการตรวจประเมินหน่วยงานสาขานั้น ๆ ทั้งหมดและกิจกรรมส่วนกลาง
4. การตรวจประเมินทุกครั้งต้องตรวจประเมินที่สำนักงานส่วนกลางด้วย และสาขาในขอบข่ายการรับรองระบบการจัดการต้องได้รับการตรวจประเมินให้ครอบคลุมทุกสาขาภายใน 3 ปี
5. คัดเลือกตัวอย่างหน่วยงานสาขาที่มีความเสี่ยงสูงโดยพิจารณาจาก
- 1) ผลการตรวจประเมินภายในสำนักงานส่วนกลาง (ถ้ามี) และสถานประกอบการสาขา
 - 2) ผลการทบทวนโดยฝ่ายบริหาร
 - 3) ความแตกต่างของขนาดสาขา เช่น บางสาขามีขนาดเล็กมาก บางสาขามีขนาดปานกลาง หรือบางสาขามีขนาดใหญ่มาก
 - 4) ความแตกต่างของวัตถุประสงค์ทางธุรกิจของสาขาต่าง ๆ
 - 5) ความซับซ้อนของระบบสารสนเทศในสาขาต่าง ๆ

- 6) ความแตกต่างของวิธีการปฏิบัติงาน
 - 7) ความแตกต่างของกิจกรรมที่ดำเนินการ
 - 8) ความแตกต่างของการออกแบบและการดำเนินงานของระบบควบคุม
 - 9) ปฏิสัมพันธ์ที่อาจเกิดขึ้นกับระบบสารสนเทศที่สำคัญและระบบสารสนเทศที่ประมวลผลข้อมูลที่เกี่ยวข้อง
 - 10) ข้อกำหนดกฎหมายที่แตกต่างกัน
 - 11) ลักษณะทางภูมิศาสตร์และวัฒนธรรม
 - 12) สถานการณ์ความเสี่ยงของสาขา
 - 13) เหตุการณ์ด้านความปลอดภัยของสารสนเทศเฉพาะสาขา
6. ทุกสาขาที่อยู่ในระบบการจัดการที่มีความเสี่ยงสูงจะได้รับการคัดเลือกเพื่อตรวจประเมินขั้นตอนที่ 2
 7. สำนักงานส่วนกลางของผู้ขอรับการตรวจประเมินต้องเป็นศูนย์กลางของการควบคุมดูแลประสิทธิภาพของระบบซึ่งรวมถึงการรวบรวมข้อมูลและวิเคราะห์ข้อมูล และการแก้ไขความไม่สอดคล้องที่เกิดขึ้นที่สาขาต่าง ๆ เพื่อให้เกิดการแก้ไขความไม่สอดคล้องให้ครอบคลุมทั้งส่วนกลางและสาขาต่าง ๆ ในกรณีที่มีความไม่สอดคล้องมีส่วนเกี่ยวข้องกับทั้งหมด
 8. ผู้ขอรับการตรวจประเมินต้องดำเนินการทบทวนของฝ่ายบริหาร และการตรวจประเมินภายในทุกหน่วยงานสาขาทุกสาขา ก่อนการตรวจประเมินของสำนักงาน และหากพบความไม่สอดคล้องที่สาขาใดสาขาหนึ่ง ผู้ขอรับการตรวจประเมินต้องสอบสวนปัญหาและแก้ไขให้ครอบคลุมสาขาอื่นที่มีผลกระทบ รวมถึงสำนักงานส่วนกลางด้วย
 9. ในระหว่างขั้นตอนการดำเนินการเพื่อให้การรับรองหรือคงไว้ซึ่งการรับรอง ผู้รับการตรวจประเมินหรือผู้ได้รับการรับรองไม่สามารถขอละเว้นหรือยกเลิกการรับรองสาขาที่พบความไม่สอดคล้องได้ในกรณีที่ความไม่สอดคล้องนั้นเกี่ยวข้องกับทุกสาขา
 10. ผู้ขอรับการตรวจประเมินต้องแสดงให้เห็นว่า สำนักงานส่วนกลางและหน่วยงานสาขาของผู้ขอรับการตรวจประเมินได้สร้างระบบการจัดการที่สอดคล้องกับมาตรฐานและรวมถึงองค์ทั้งหมดที่เป็นไปตามมาตรฐานและข้อกำหนดของสำนักงาน
 11. ระยะเวลาทั้งหมดในการตรวจประเมินขั้นตอนที่ 1 และการตรวจประเมินขั้นตอนที่ 2 การตรวจติดตามผล และการตรวจประเมินเพื่อต่ออายุ สำหรับสำนักงานส่วนกลางและหน่วยงานสาขาจะพิจารณาจากประมาณการระยะเวลาในการตรวจประเมินตามที่สำนักงานกำหนด ซึ่งต้องไม่น้อยกว่าการตรวจประเมินขั้นตอนที่ 1 การตรวจประเมินขั้นตอนที่ 2 การตรวจติดตามผล และการตรวจประเมินเพื่อต่ออายุ สำหรับกรณีองค์กรเดียวที่มีพนักงานในองค์กรเท่านั้น
 12. กรณีที่ผู้ขอรับการตรวจประเมิน ได้รับการตรวจประเมินจากสำนักงาน และพบความไม่สอดคล้องที่สาขาใดสาขาหนึ่ง ผู้ขอรับการตรวจประเมินต้องสอบสวนปัญหาและแก้ไขให้ครอบคลุมสาขาอื่นที่มีผลกระทบ รวมถึงสำนักงานส่วนกลางด้วย
 13. เมื่อผู้ตัดสินใจการรับรองได้อนุมัติให้การรับรองแล้ว สำนักงานจะออกหนังสือรับรองโดยระบุชื่อและที่อยู่ของสำนักงานส่วนกลาง และชื่อและที่อยู่ของสาขาต่าง ๆ โดยหากไม่สามารถระบุชื่อและที่อยู่ของสาขาต่าง ๆ ได้ สำนักงานจะจัดทำใบแบบที่แสดงชื่อและที่อยู่ของสาขาเพิ่มเติม
 14. การตรวจประเมินเพื่อการรับรองให้เป็นไปตามข้อ 2.1.1-2.1.3 และพิจารณาเพิ่มเติม ดังนี้
 - 14.1 การตรวจประเมินขั้นตอนที่ 1 และการกำหนดหน่วยงานสาขาที่ตรวจประเมิน

โดยใช้วิธีการคัดเลือกและสุ่มหน่วยงานสาขาในการตรวจประเมินเพื่อการรับรองตามที
ระบุในข้อ 2-3

14.2 การตรวจประเมินขั้นตอนที่ 2

สำนักงานจะดำเนินการตรวจประเมินขั้นตอนที่ 2 ครอบคลุมสำนักงานส่วนกลางและ
หน่วยงานสาขาที่คัดเลือกไว้ใน การตรวจประเมินขั้นตอนที่ 1

กรณีที่ไม่มีพบความไม่สอดคล้องหรือพบเฉพาะความไม่สอดคล้องย่อย คณะผู้ตรวจ
ประเมินสามารถสรุปรายงานเสนอผู้ตัดสินใจเพื่อพิจารณาให้การรับรองได้หลังจากที่
คณะผู้ตรวจประเมินพิจารณาแนวทางการแก้ไขและป้องกันความไม่สอดคล้องที่เกิดขึ้น
ตามที่ยื่นคำขอเสนอแล้วเห็นว่า เป็นแนวทางที่ยอมรับได้ โดยแนวทางการแก้ไขและ
ป้องกันต้องครอบคลุมสาขาอื่นที่มีผลกระทบด้วย

ในกรณีพบความไม่สอดคล้องสำคัญตั้งแต่ 1 รายการขึ้นไปไม่ว่าที่สาขาใดหรือ
หลายสาขารวมกัน คณะผู้ตรวจประเมินจะยังไม่สามารถสรุปรายงานเสนอผู้ตัดสินใจเพื่อ
พิจารณาให้การรับรองได้ และต้องมีการดำเนินการดังต่อไปนี้

- 1) นัดหมายผู้รับการตรวจประเมินเพื่อตกลงช่วงเวลาที่ จะดำเนินการตรวจติดตาม
การแก้ไขความไม่สอดคล้อง ซึ่งช่วงระยะเวลาการแก้ไขความไม่สอดคล้องต้องไม่เกิน
180 วัน นับจากวันที่ตรวจประเมินเสร็จสิ้น หากระยะเวลาแก้ไขเกิน 180 วัน
ให้ดำเนินการตรวจประเมินใหม่ทั้งระบบ ทั้งนี้ ในการตรวจติดตามการแก้ไขความไม่
สอดคล้องสำนักงานจะพิจารณาดำเนินการตรวจประเมินในสาขาอื่นที่มีผลกระทบ
จากความไม่สอดคล้องนั้น ๆ ด้วย

ในการแก้ไขความไม่สอดคล้อง ผู้ยื่นคำขอต้องพิจารณาว่าได้แก้ไขความไม่
สอดคล้อง ครอบคลุมถึงสำนักงานส่วนกลางและสาขาต่าง ๆ ที่มีผลกระทบด้วย

ในกรณีที่อยู่ในช่วงระยะเวลาการแก้ไขความไม่สอดคล้อง 180 วัน
มีการปรับปรุงเปลี่ยนแปลงระบบการจัดการหรือเอกสารระบบการจัดการเป็น
จำนวนมาก และผู้ยื่นคำขอมีความประสงค์ขอให้ตรวจประเมินใหม่ทั้งระบบโดย
ยกเลิกความไม่สอดคล้องเดิม สำนักงานสามารถดำเนินการตามความประสงค์
ของผู้ยื่นคำขอได้ โดยผู้ยื่นคำขอต้องยื่นแบบยื่นคำขอใหม่

- 2) ในการตรวจติดตามการแก้ไขความไม่สอดคล้องสำคัญ คณะผู้ตรวจประเมิน
จะตรวจติดตาม เฉพาะรายการที่เป็นความไม่สอดคล้องเท่านั้น และอาจสุ่มตรวจที่
หน่วยงานใด ๆ ที่เกี่ยวข้องได้ โดยคณะผู้ตรวจประเมินต้องแน่ใจว่าแนวทางการแก้ไข
และป้องกันความไม่สอดคล้องเป็นการแก้ไขและป้องกันครอบคลุมสาขาอื่น ๆ ที่มี
ผลกระทบด้วย และอาจสุ่มสาขาอื่นเพิ่มเติมได้ หากพบว่าการแก้ไขความไม่สอดคล้อง
สำคัญไม่มีประสิทธิผล และได้พ้นระยะเวลา 180 วัน นับจากวันที่ตรวจประเมิน
เสร็จสิ้น สำนักงานจะดำเนินการตรวจประเมินใหม่ทั้งระบบ โดยผู้ยื่นคำขอต้องยื่น
แบบยื่นคำขอใหม่

15. การตรวจติดตามผล

- 15.1 ก่อนตรวจติดตามผล สำนักงานจะดำเนินการตรวจเยี่ยมสำนักงานส่วนกลาง
และ/หรือสาขา และ/หรือให้ผู้ได้รับการรับรองจัดส่งข้อมูลให้สำนักงานตรวจสอบ
เพื่อเป็นข้อมูลในการกำหนดหน่วยงานสาขาที่จะทำการตรวจติดตามผล โดยข้อมูล
ที่มีการนำมาพิจารณาประกอบการกำหนดสาขาที่จะทำการตรวจติดตามผล ได้แก่

กิจกรรมที่แต่ละสาขาดำเนินการ ขนาดสาขา จำนวนบุคลากรแต่ละสาขา การทบทวนของฝ่ายบริหาร ผลของการตรวจประเมินภายใน ข้อร้องเรียน ความไม่สอดคล้องที่ไม่เป็นไปตามข้อกำหนดอื่น ๆ และการแก้ไขและการป้องกันของ ส่วนกลางและแต่ละสาขา การเปลี่ยนแปลงกระบวนการจากการตรวจประเมิน ครั้งก่อน และสถานที่ตั้งของสาขาต่าง ๆ เป็นต้น

- 15.2 การตรวจติดตามผลให้ดำเนินการตรวจประเมินสำนักงานส่วนกลางทุกครั้งและคัดเลือกและสุ่มตรวจประเมินหน่วยงานสาขาเพิ่มเติม โดยการพิจารณากำหนดจำนวนหน่วยงานสาขาและการคัดเลือกสาขาที่จะตรวจประเมิน ตามข้อ 3.
 - 15.3 สำนักงานอาจตรวจประเมินมากกว่าที่กำหนดได้หากเกิดกรณีตามข้อ 2.1.4 หรือกรณีผู้ได้รับการรับรองขอเพิ่มเติมการรับรองในสาขาอื่นที่นอกเหนือจากสาขาที่ได้รับการรับรองแล้ว ให้ดำเนินการตามขั้นตอนเหมือนการยื่นคำขอใหม่ แต่ภายหลังการรับรองแล้วให้พิจารณารวมสาขาที่ได้รับการรับรองเพิ่มเติมไว้กับการรับรองเดิม เพื่อพิจารณาสุ่มตัวอย่างในการตรวจติดตามผลและการตรวจประเมินเพื่อต่ออายุต่อไปได้
 - 15.4 การตรวจติดตามผลให้เป็นไปตามข้อ 2.1.4 โดยในกรณีที่พบความไม่สอดคล้องสำคัญตั้งแต่ 1 รายการขึ้นไปไม่ว่าที่สาขาใดหรือหลายสาขารวมกัน คณะผู้ตรวจประเมินจะนัดหมายผู้รับการตรวจประเมินเพื่อตกลงช่วงเวลาที่ดำเนินการตรวจติดตามตามแก้ไขความไม่สอดคล้องซึ่งต้องไม่เกิน 180 วัน นับจากวันที่ตรวจประเมินเสร็จสิ้น หากเกิน 180 วันและ/หรือ หากผลการติดตามการแก้ไขความไม่สอดคล้องสำคัญไม่มีประสิทธิผล สำนักงานอาจแจ้งเตือนและ/หรืออาจนำเสนอคณะกรรมการเพื่อพิจารณาพักใช้ หรือเพิกถอนการรับรอง แล้วแต่กรณี
16. การตรวจประเมินเพื่อต่ออายุ

การตรวจประเมินเพื่อต่ออายุให้เป็นไปตามที่กำหนดไว้ในข้อ 2.1.5 โดยมีขั้นตอนต่าง ๆ ของการตรวจประเมินเพื่อต่ออายุเหมือนกับการตรวจประเมินเพื่อการรับรอง โดยยกเว้นการตรวจประเมินขั้นตอนที่ 1 แต่ให้ดำเนินการตรวจเยี่ยม (Pre-visit) เพื่อกำหนดหน่วยงานสาขาที่ตรวจประเมินเพื่อต่ออายุ โดยการตรวจเยี่ยมอาจดำเนินการ ณ สำนักงานส่วนกลาง และ/หรือสาขา และ/หรือให้ผู้ยื่นคำขอจัดส่งข้อมูลให้สำนักงานตรวจสอบ ได้แก่ กิจกรรมที่แต่ละสาขาดำเนินการ การทบทวนของฝ่ายบริหาร ผลการตรวจประเมินภายใน และการตรวจประเมินเพื่อการรับรองครั้งก่อน (ถ้ามี) ข้อร้องเรียน ความไม่สอดคล้องที่ไม่เป็นไปตามข้อกำหนดอื่น ๆ และการแก้ไขและการป้องกันของส่วนกลางและแต่ละสาขา ขนาดสาขา การเปลี่ยนแปลงกระบวนการจากการตรวจประเมินครั้งก่อน (ถ้ามี) และสถานที่ตั้งของสาขาต่าง ๆ เพื่อกำหนดหน่วยงานสาขาที่จะตรวจประเมินเพื่อต่ออายุ โดยการตรวจประเมินเพื่อต่ออายุจะใช้เกณฑ์การคัดเลือกและสุ่มสาขาตามแนวทางที่ระบุในข้อ 3. ทั้งนี้ขึ้นอยู่กับกระบวนการ/กิจกรรมการดำเนินงานของหน่วยงานสาขาต่าง ๆ ที่ได้รับการรับรองว่าจัดอยู่ในกลุ่มที่ 1 หรือกลุ่มที่ 2 หรือกลุ่มที่ 3 และไม่มีการประเมินเอกสาร ยกเว้นกรณีที่ผู้ได้รับการรับรองแจ้งความประสงค์ขอรับการรับรองตามมาตรฐานฉบับใหม่ หรือมีการเปลี่ยนแปลงที่สำคัญ สำนักงานดำเนินการตรวจประเมินขั้นตอนที่ 1

- 17.กรณีผู้ได้รับการรับรองขอเพิ่มเติมการรับรองในสาขาอื่นที่นอกเหนือจากสาขาที่ได้รับการรับรองแล้ว ให้ดำเนินการตามขั้นตอนเหมือนการยื่นคำขอใหม่ แต่ภายหลังการรับรองแล้วให้พิจารณารวมสาขาที่ได้รับการรับรองเพิ่มเติมไว้กับการรับรองเดิม เพื่อพิจารณาสุ่มตัวอย่างในการตรวจติดตามผลและการตรวจประเมินเพื่อต่ออายุต่อไปได้

2.3 การตรวจประเมินกรณีองค์กรที่มีสถานที่ดำเนินการชั่วคราว

1. การขอรับการรับรองกรณีองค์กรที่มีสถานที่ดำเนินการชั่วคราว จะให้การรับรองได้เฉพาะสำนักงานส่วนกลาง ไม่รวมถึงการรับรองสถานที่ดำเนินการชั่วคราว การสุ่มตรวจประเมินสถานที่ดำเนินการชั่วคราวจะดำเนินการเพียงเพื่อเป็นการยืนยันระบบการจัดการของสำนักงานส่วนกลางเท่านั้น

2. ขั้นตอนการตรวจประเมิน

การตรวจประเมินเพื่อการรับรอง (ซึ่งประกอบด้วย 2 ขั้นตอน คือ การตรวจประเมินขั้นตอนที่ 1 และการตรวจประเมินขั้นตอนที่ 2) การตรวจติดตามผล และการตรวจประเมินเพื่อต่ออายุให้เป็นไปตามข้อ 2.1.1-2.1.3 ข้อ 2.1.4 ข้อ 2.1.5 โดยอนุโลม โดยดำเนินการตรวจประเมิน ณ สำนักงานส่วนกลาง และทำการสุ่มตรวจประเมินสถานที่ดำเนินการชั่วคราวโดยใช้เกณฑ์ ดังต่อไปนี้

- 1) กรณีการตรวจประเมินเพื่อการรับรอง

สุ่มตรวจประเมินไม่น้อยกว่า $\sqrt{\text{จำนวนสถานที่ดำเนินการชั่วคราวทั้งหมด}}$

- 2) กรณีการตรวจติดตามผล

สุ่มตรวจประเมินในแต่ละครั้งไม่น้อยกว่า $0.6 \sqrt{\text{จำนวนสถานที่ดำเนินการชั่วคราวทั้งหมด}}$

- 3) กรณีการตรวจประเมินเพื่อต่ออายุ

สุ่มตรวจประเมินในแต่ละครั้งไม่น้อยกว่า $0.8 \sqrt{\text{จำนวนสถานที่ดำเนินการชั่วคราวทั้งหมด}}$

2.4 การตรวจประเมินแบบบูรณาการและแบบรวมระบบ

1. ผู้ยื่นคำขอสามารถขอการรับรองแบบบูรณาการหรือแบบรวมระบบ กรณีของการรับรองแบบบูรณาการต้องมีการดำเนินการกิจกรรมร่วมกันในระบบการจัดการที่ขอรับการรับรองดังต่อไปนี้

- มีระบบการควบคุมเอกสารและบันทึกเดียวกัน
- มีการควบคุมความมั่นคงปลอดภัยของข้อมูลร่วมกัน
- มีการใช้กระบวนการหรือทรัพยากรร่วมกัน เช่น Infrastructure
- มีการทบทวนโดยฝ่ายบริหารร่วมกัน
- มีการตรวจประเมินภายในร่วมกัน
- มีการปฏิบัติการแก้ไขและป้องกันร่วมกัน
- มีนโยบายและวัตถุประสงค์ร่วมกัน
- มีกลไกการปรับปรุงร่วมกัน
- มีหน้าที่ความรับผิดชอบและสนับสนุนการจัดการร่วมกัน

2. กรณีที่พบว่าผู้ยื่นคำขอมีการดำเนินการของระบบการจัดการที่ขอรับการรับรองไม่เป็นไปตามที่ระบุในข้อ 1. ของข้อ 2.4 ข้างต้น ให้พิจารณาว่าเป็นการตรวจประเมินตามปกติหรือตรวจประเมินแบบรวมระบบ โดยการกำหนดจำนวนวันที่ใช้ในการตรวจประเมิน ให้เป็นไป

ตามเกณฑ์การตรวจประเมินนั้น ๆ ว่าเป็นการตรวจปกติหรือตรวจประเมินแบบรวมระบบ หรือตรวจประเมินแบบบูรณาการ

3. สำนักงานจะดำเนินการตรวจประเมินแบบบูรณาการและแบบรวมระบบ ตามขั้นตอนการตรวจประเมินข้อ 2.1.1-2.1.3

- 1) ในกรณีพบความไม่สอดคล้อง คณะผู้ตรวจประเมินจะแจ้งผู้ยื่นคำขอให้จัดทำแนวทางการแก้ไขและป้องกันความไม่สอดคล้อง ให้สำนักงานพิจารณาภายใน 30 วัน นับจากวันที่ออกรายงานความไม่สอดคล้องระบบการจัดการตามมาตรฐานนั้น ๆ หากผู้ยื่นคำขอไม่สามารถดำเนินการได้ภายใน 180 วัน นับจากวันที่ตรวจประเมินเสร็จสิ้น สำนักงานอาจแจ้งเตือนและ/หรืออาจนำเสนอผู้ตัดสินใจการรับรองเพื่อพิจารณาให้ตรวจประเมินใหม่ทั้งระบบ แล้วแต่กรณี
- 2) กรณีพบความไม่สอดคล้องสำคัญที่เกี่ยวข้องกับระบบการจัดการตามมาตรฐานใดตั้งแต่ 1 รายการขึ้นไป ให้ดำเนินการ ดังนี้
 - คณะผู้ตรวจประเมินจะยังไม่สามารถสรุปรายงานเสนอผู้ตัดสินใจการรับรองพิจารณาให้การรับรองสำหรับระบบการจัดการที่พบความไม่สอดคล้องสำคัญได้ และต้องให้มีการตรวจติดตามการแก้ไขและป้องกันความไม่สอดคล้องดังกล่าวตามระบบการจัดการนั้น ๆ จนพบว่ามีประสิทธิผล จึงจะสามารถนำเสนอผู้ตัดสินใจการรับรองเพื่อพิจารณาให้การรับรองได้ตามระบบการจัดการนั้น ๆ ยกเว้น กรณีการตรวจประเมินแบบบูรณาการให้เสนอผู้ตัดสินใจการรับรองพิจารณาพร้อมกันทุกระบบ
 - นัดหมายผู้รับการตรวจประเมินเพื่อตกลงช่วงเวลาที่ดำเนินการตรวจติดตามการแก้ไขความไม่สอดคล้อง (Follow up audit) ซึ่งช่วงระยะเวลาการแก้ไขความไม่สอดคล้องต้องไม่เกิน 180 วัน นับจากวันที่ตรวจประเมินเสร็จสิ้น หากระยะเวลาการแก้ไขเกิน 180 วัน ให้ดำเนินการตรวจประเมินใหม่ทั้งระบบ และผู้ยื่นคำขอต้องยื่นแบบยื่นคำขอใหม่
 - ในกรณีที่อยู่ในช่วงระยะเวลาการแก้ไขความไม่สอดคล้อง 180 วัน มีการปรับปรุงเปลี่ยนแปลงระบบการจัดการที่เกี่ยวข้องกับการรับรอง หรือเอกสารที่เกี่ยวข้องที่ตรวจประเมินนั้น ๆ เป็นจำนวนมาก และผู้ยื่นคำขอมีความประสงค์ขอให้ตรวจประเมินใหม่ทั้งระบบโดยยกเลิกความไม่สอดคล้องเดิม สำนักงานสามารถดำเนินการตามความประสงค์ของผู้ยื่นคำขอได้ โดยผู้ยื่นคำขอต้องยื่นแบบยื่นคำขอใหม่
 - ในการตรวจติดตามการแก้ไขความไม่สอดคล้องสำคัญ คณะผู้ตรวจประเมินจะตรวจติดตาม เฉพาะรายการที่เป็นความไม่สอดคล้องเท่านั้น และอาจสุ่มตรวจที่หน่วยงานใด ๆ ที่เกี่ยวข้องได้ หากพบว่าการแก้ไขความไม่สอดคล้องสำคัญไม่มีประสิทธิผล และเกินระยะเวลา 180 วัน นับจากวันที่ตรวจประเมินเสร็จสิ้น สำนักงานจะดำเนินการตรวจประเมินใหม่ทั้งระบบ โดยผู้ยื่นคำขอต้องยื่นแบบยื่นคำขอใหม่
- 3) กรณีพบเฉพาะความไม่สอดคล้องย่อย ในระบบใดระบบหนึ่ง หลังจากคณะผู้ตรวจประเมินพิจารณายอมรับแนวทางการแก้ไขและป้องกันแล้ว จะนำเสนอผู้ตัดสินใจการรับรอง

เอกสาร : หลักเกณฑ์ วิธีการ และเงื่อนไขการตรวจประเมินระบบการจัดการ	
โดย : สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์	หน้า 24

การรับรอง โดยไม่จำเป็นต้องรอเสนอให้พิจารณาพร้อมกันทุกระบบ ยกเว้นกรณี
การตรวจประเมินแบบบูรณาการจะต้องเสนอผู้ตัดสินการรับรองพิจารณาพร้อมกัน
ทุกระบบ