# หลักเกณฑ์ในการกำกับดูแลและการตรวจสอบ
# ด้านเทคโนโลยีสารสนเทศ (Information Technology)
# สำหรับสำนักงานสอบบัญชี

**สารบัญ**

**หน้า**

**หมวดที่ 1 การกำกับดูแลและบริหารจัดการด้านเทคโนโลยีสารสนเทศ (Information Technology Governance)**

| ข้อกำหนด | แนวปฏิบัติ |
|---|---|
| **1.1 บทบาทหน้าที่และความรับผิดชอบของคณะกรรมการของสำนักงานสอบบัญชี** | |
| **ส่วนที่ 1 บทบาทหน้าที่และความรับผิดชอบของหัวหน้าสำนักงานสอบบัญชี หรือคณะกรรมการบริหารของสำนักงานสอบบัญชี**<br>หัวหน้าสำนักงานสอบบัญชี หรือคณะกรรมการบริหารของสำนักงานสอบบัญชีต้องควบคุมดูแลและบริหารจัดการความเสี่ยงด้าน IT ให้สอดคล้องกับระดับความเสี่ยงที่สำนักงานสอบบัญชียอมรับได้ โดยคำนึงถึงการบริหารและจัดการความเสี่ยงขององค์กร (enterprise risk) ซึ่งอย่างน้อยต้องครอบคลุมในเรื่องดังนี้ | |
| 1.1 การกำหนดกรอบการกำกับดูแลด้าน IT (IT governance framework) และการกำกับดูแลแผนงานด้าน IT ให้สอดคล้องกับแผนธุรกิจ และมีความเหมาะสมเพียงพอที่จะรองรับการเปลี่ยนแปลงด้าน IT และการเปลี่ยนแปลงการดำเนินธุรกิจในอนาคต | 1. สำนักงานสอบบัญชีควรกำหนดกรอบการกำกับดูแลด้าน IT (IT governance framework) ที่ครอบคลุมรายละเอียดดังนี้<br>(1) โครงสร้างการกำกับดูแล บทบาทหน้าที่และความรับผิดชอบของหัวหน้าสำนักงานสอบบัญชี หรือคณะกรรมการบริหารของสำนักงานสอบบัญชี และฝ่ายงานที่เกี่ยวข้อง สำหรับการกำกับดูแลด้าน IT ของสำนักงานสอบบัญชี<br>(2) กระบวนการที่เกี่ยวข้องกับการกำกับดูแลด้าน IT อย่างน้อยให้ครอบคลุม<br>(2.1) การจัดทำและขออนุมัติแผนงานด้าน IT<br>(2.2) การจัดทำแผนและและการบริหารจัดการทรัพยากรด้าน IT<br>(2.3) การติดตามและรายงานผลการดำเนินการด้าน IT เป็นต้น<br>2. สำนักงานสอบบัญชีควรจัดให้มีแผนงานด้าน IT ประจำปี เพื่อให้การใช้ IT สอดรับกับกลยุทธ์ในการดำเนินธุรกิจ |
| 1.2 การจัดสรรทรัพยากรทางด้าน IT และทรัพยากรบุคคลที่ปฏิบัติงานด้าน IT ให้มีความเหมาะสมเพียงพอต่อการดำเนินธุรกิจ | สำนักงานสอบบัญชีควรจัดสรรทรัพยากรทางด้าน IT และทรัพยากรบุคคลที่ปฏิบัติงานด้าน IT ให้สอดคล้องกับเป้าหมายตามภารกิจ กลยุทธ์ นโยบาย และแผนการดำเนินงานที่กำหนดไว้ |
| 1.3 การกำหนดนโยบายที่เกี่ยวข้องกับการกำกับดูแลความเสี่ยงด้าน IT อย่างเป็นลายลักษณ์อักษร โดยอย่างน้อยต้องครอบคลุมนโยบายตามที่กำหนดในส่วนที่ 2 ข้อ 2.2 | [ไม่มีการกำหนดแนวปฏิบัติไว้เป็นการเฉพาะ] |
| 1.4 การกำหนดขั้นตอนและวิธีปฏิบัติงานในการบริหารจัดการความเสี่ยงด้าน IT และการรักษาความมั่นคงปลอดภัยด้าน IT เพื่อให้เป็นไปตามนโยบายในข้อ 1.3 รวมถึงกำกับดูแลให้มีการนำไปปฏิบัติ | [ไม่มีการกำหนดแนวปฏิบัติไว้เป็นการเฉพาะ] |

| ข้อกำหนด | แนวปฏิบัติ |
|---|---|
| อย่างเหมาะสม | |
| 1.5 การสร้างความรู้และความตระหนักด้านความเสี่ยงด้าน IT แก่บุคลากรอย่างต่อเนื่องและมีประสิทธิผล | [ไม่มีการกำหนดแนวปฏิบัติไว้เป็นการเฉพาะ] |
| 1.6 การติดตาม ตรวจสอบ และรายงานผลการปฏิบัติงานเพื่อให้เป็นไปตามนโยบายในข้อ 1.3 ต่อหัวหน้าสำนักงานสอบบัญชี หรือคณะกรรมการบริหารของสำนักงานสอบบัญชี โดยมีการรายงานอย่างน้อยปีละ 1 ครั้ง และในกรณีที่มีเหตุการณ์หรือการเปลี่ยนแปลงใด ๆ ซึ่งอาจส่งผลกระทบอย่างมีนัยสำคัญต่อการปฏิบัติงานเพื่อให้เป็นไปตามนโยบายดังกล่าว ต้องมีการรายงานให้หัวหน้าสำนักงานสอบบัญชี หรือคณะกรรมการบริหารของสำนักงานสอบบัญชีทราบโดยไม่ชักช้าด้วย | 1. สำนักงานสอบบัญชีควรจัดให้มีกระบวนการติดตาม ตรวจสอบ และควบคุมการจัดทำรายงานผลการปฏิบัติงานเพื่อให้มั่นใจว่าสามารถจัดทำรายงานได้อย่างครบถ้วนถูกต้อง<br>2. สำนักงานสอบบัญชีควรกำหนดให้การรายงานผลการปฏิบัติตามนโยบายที่เกี่ยวข้องกับการกำกับดูแลและบริหารจัดการความเสี่ยงด้าน IT ต่อหัวหน้าสำนักงานสอบบัญชี หรือคณะกรรมการบริหารของสำนักงานสอบบัญชี มีเนื้อหาครอบคลุมถึงเรื่องดังนี้<br>(1) ผลการประเมินความเสี่ยงด้าน IT การติดตามความเสี่ยง และแนวทางการควบคุมที่เกี่ยวข้อง โดยหน่วยงานที่ทำหน้าที่บริหารความเสี่ยงด้าน IT หรือหน่วยงานที่เกี่ยวข้อง<br>(2) ผลการปฏิบัติตามกฎระเบียบ ข้อบังคับ หรือนโยบายการรักษาความมั่นคงปลอดภัยด้าน IT ในภาพรวมขององค์กร โดยหน่วยงานที่ทำหน้าที่กำกับดูแลการปฏิบัติงานด้าน IT หรือหน่วยงานที่เกี่ยวข้อง<br>(3) ผลการตรวจสอบด้าน IT (IT audit) และความคืบหน้าในการดำเนินการแก้ไขข้อบกพร่อง โดยหน่วยงานที่ทำหน้าที่ตรวจสอบด้าน IT หรือหน่วยงานที่เกี่ยวข้อง<br>(4) ผลการปฏิบัติงานด้าน IT ที่สำคัญ เช่น<br>(4.1) เหตุการณ์ผิดปกติ หรือปัญหาด้าน IT ที่สำคัญ<br>(4.2) ความเพียงพอของทรัพยากรด้าน IT (capacity and system utilization)<br>(4.3) ความคืบหน้าของโครงการด้าน IT ในภาพรวม และโครงการที่สำคัญ<br>(4.4) การปฏิบัติงานด้าน IT ของบุคคลภายนอก เช่น ผลการดำเนินการตามข้อตกลงการให้บริการ (service level agreement) เป็นต้น<br>(4.5) ผลการทดสอบแผนฉุกเฉินด้าน IT และการใช้งานแผน (ถ้ามี) |
| **1.2 โครงสร้างการกำกับดูแล** | |
| **ส่วนที่ 2 การกำกับดูแลและบริหารจัดการความเสี่ยงด้าน IT ในระดับองค์กร**<br>2.1 สำนักงานสอบบัญชีต้องจัดให้มีโครงสร้างการกำกับดูแลและ | สำนักงานสอบบัญชีควรจัดให้มีโครงสร้างการกำกับดูแลและบริหารจัดการความเสี่ยงด้าน IT ที่มีการถ่วงดุลอำนาจ (check and balance) และมีการแบ่งแยกหน้าที่ (segregation of duties) อย่างเหมาะสม ตามหลักการแบ่งแยกหน้าที่ 3 ระดับ ได้แก่<br>(1) การปฏิบัติงาน (first line of defense) หมายถึง หน่วยงาน หรือ บุคลากรที่ปฏิบัติงานด้าน IT และผู้ที่ใช้ระบบ IT ปฏิบัติงาน |

| ข้อกำหนด | แนวปฏิบัติ |
|---|---|
| บริหารจัดการความเสี่ยงด้าน IT โดยอย่างน้อยต้องมีลักษณะดังนี้<br>2.1.1 ทำให้เกิดการถ่วงดุลอย่างเป็นอิสระ<br>2.1.2 สอดคล้องตามหลักการแบ่งแยกหน้าที่ 3 ระดับ (3 Lines of Defense : 3 LoDs) โดยมีการแบ่งแยกหน้าที่อย่างชัดเจนระหว่างการทำหน้าที่ด้าน IT ดังนี้<br><u>ระดับที่ 1</u> (first line of defense) : การปฏิบัติงาน<br><u>ระดับที่ 2</u> (second line of defense) : การบริหารความเสี่ยงและกำกับดูแลการปฏิบัติตามกฎหมายและหลักเกณฑ์ที่เกี่ยวข้อง<br><u>ระดับที่ 3</u> (third line of defense) : การตรวจสอบ | (1.1) หน่วยงาน หรือ บุคลากรที่ปฏิบัติงานด้าน IT มีหน้าที่ปฏิบัติงานตามหน้าที่ความรับผิดชอบ ประเมินความเสี่ยงและควบคุมความเสี่ยงด้าน IT ติดตามและรายงานการปฏิบัติงานด้าน IT ต่อหัวหน้าสำนักงานสอบบัญชี หรือคณะกรรมการบริหารของสำนักงานสอบบัญชีที่ได้รับมอบหมาย<br>(1.2) ผู้ที่ใช้ระบบ IT ปฏิบัติงาน มีหน้าที่ปฏิบัติตามนโยบายและระเบียบปฏิบัติที่เกี่ยวข้องกับความมั่นคงปลอดภัยด้าน IT รวมทั้งมีส่วนร่วมรับผิดชอบในการประเมินและจัดการความเสี่ยงด้าน IT ที่เกี่ยวข้องกับการใช้งานระบบ<br>(2) การบริหารความเสี่ยงและกำกับดูแลการปฏิบัติตามกฎหมายและหลักเกณฑ์ที่เกี่ยวข้องในการปฏิบัติงานด้าน IT (second line of defense) หมายถึง หน่วยงาน หรือ บุคลากรที่บริหารความเสี่ยงด้าน IT และหน่วยงาน หรือบุคลากรที่กำกับดูแลการปฏิบัติตามกฎหมายและหลักเกณฑ์ด้าน IT<br>(2.1) หน่วยงาน หรือ บุคลากรบริหารความเสี่ยงด้าน IT (IT risk function) มีหน้าที่กำหนดกรอบนโยบาย และกระบวนการบริหารความเสี่ยงด้าน IT สนับสนุนให้มีการประเมินความเสี่ยงเป็นไปตามกรอบการบริหารความเสี่ยงที่กำหนด พร้อมทั้งให้คำปรึกษา ติดตามความเสี่ยง และทบทวนการควบคุมความเสี่ยงด้าน IT ให้อยู่ในระดับความเสี่ยงที่ยอมรับได้ โดยมีการรวบรวมและเชื่อมโยงความเสี่ยงด้าน IT กับความเสี่ยงด้านอื่น และนำเสนอผลการบริหารความเสี่ยงต่อหัวหน้าสำนักงานสอบบัญชี หรือคณะกรรมการบริหารของสำนักงานสอบบัญชีที่ได้รับมอบหมาย<br>(2.2) หน่วยงาน หรือ บุคลากร ที่กำกับดูแลการปฏิบัติตามกฎหมายและหลักเกณฑ์ด้าน IT (IT compliance function) มีหน้าที่ในการกำกับดูแลให้มีการปฏิบัติตามกฎหมายและหลักเกณฑ์ที่เกี่ยวข้อง รวมถึงติดตาม ให้คำปรึกษา และสอบทานด้านการปฏิบัติตามกฎหมายและหลักเกณฑ์ที่เกี่ยวข้อง<br>(3) การตรวจสอบด้าน IT (third line of defense) หมายถึง หน่วยงานตรวจสอบด้าน IT ซึ่งมีหน้าที่ในการตรวจสอบการปฏิบัติงานของหน่วยงานที่ทำหน้าที่ first line และ second line of defense เพื่อให้มั่นใจว่ามีการปฏิบัติตามนโยบาย มาตรฐาน และกฎหมายทางด้าน IT ที่เกี่ยวข้อง หน่วยงานในระดับนี้อาจเป็นผู้ตรวจสอบภายใน หรือผู้ตรวจสอบภายนอกที่มีความเป็นอิสระจากหน่วยงานที่ทำหน้าที่ first line และ second line of defense |
| **1.3 นโยบายที่เกี่ยวข้องกับการกำกับดูแลความเสี่ยงด้าน IT** | |
| **ส่วนที่ 2 การกำกับดูแลและบริหารจัดการความเสี่ยงด้าน IT ในระดับองค์กร**<br>2.2 สำนักงานสอบบัญชีต้องจัดให้มีนโยบายที่เกี่ยวข้องกับการกำกับดูแลความเสี่ยงด้าน IT เป็นลายลักษณ์อักษร โดยต้องได้รับ | |

| ข้อกำหนด | แนวปฏิบัติ |
|---|---|
| ความเห็นชอบจากหัวหน้าสำนักงานสอบบัญชี หรือคณะกรรมการบริหารของสำนักงานสอบบัญชี หรือคณะกรรมการที่ได้รับมอบหมายจากหัวหน้าสำนักงานสอบบัญชี ดังนี้ | |
| 2.2.1 <u>นโยบายการบริหารจัดการความเสี่ยงด้าน IT (IT risk management policy)</u> มีเรื่องที่ต้องครอบคลุม ดังนี้<br>(1) บทบาทหน้าที่ของผู้ที่เกี่ยวข้องในการบริหารจัดการความเสี่ยงด้าน IT<br>(2) การจัดให้มีกระบวนการบริหารจัดการความเสี่ยงด้าน IT เพื่อให้อยู่ในระดับที่องค์กรยอมรับได้ | กระบวนการบริหารจัดการความเสี่ยงด้าน IT ควรมีรายละเอียด ดังนี้<br>1. เกณฑ์ความเสี่ยง (risk criteria) ควรครอบคลุมถึงโอกาสหรือความถี่ที่จะเกิดเหตุการณ์ความเสี่ยง และความมีนัยสำคัญหรือผลกระทบที่จะเกิดขึ้นเพื่อจัดลำดับความสำคัญในการบริหารจัดการความเสี่ยง<br>2. ระดับความเสี่ยงที่ยอมรับได้ (IT risk appetite) ควรผ่านการพิจารณาโดยคณะกรรมการบริหารความเสี่ยง (ถ้ามี) และได้รับการอนุมัติจากหัวหน้าสำนักงานสอบบัญชี หรือคณะกรรมการบริหารของสำนักงานสอบบัญชี ทั้งนี้ ระดับความเสี่ยงที่ยอมรับได้ควรสอดคล้องกับการบริหารและจัดการความเสี่ยงขององค์กร (enterprise risk management) (ถ้ามี)<br>3. การประเมินความเสี่ยง (risk assessment) ควรมีการประเมินความเสี่ยงอย่างน้อยปีละ 1 ครั้ง และเมื่อมีการเปลี่ยนแปลงระบบ IT อย่างมีนัยสำคัญ โดยมีกระบวนการครอบคลุมอย่างน้อย ดังนี้<br>(1) การระบุความเสี่ยง (risk identification)<br>จัดให้มีการระบุเหตุการณ์ความเสี่ยง (risk scenario) ด้าน IT ที่อาจจะเกิดขึ้นหรือที่เคยเกิดขึ้นจริงกับสำนักงานสอบบัญชีเอง หรือเกิดกับผู้อื่นที่ใช้งานเทคโนโลยีในลักษณะเดียวกัน รวมถึงภัยคุกคามทางไซเบอร์และช่องโหว่ต่าง ๆ ที่ส่งผลกระทบต่อการดำเนินธุรกิจ โดยเหตุการณ์ความเสี่ยงดังกล่าวอาจมีสาเหตุมาจากปัจจัยภายใน (internal factor) เช่น กระบวนการปฏิบัติงาน ระบบงาน บุคลากร เป็นต้น รวมถึงปัจจัยภายนอกอื่น ๆ (external factor) เช่น การปฏิบัติตามกฎหมาย การใช้บริการ การเชื่อมต่อ หรือการเข้าถึงข้อมูลจากบุคคลภายนอก เป็นต้น<br>(2) การวิเคราะห์ความเสี่ยง (risk analysis)<br>จัดให้มีการวิเคราะห์ความเสี่ยงด้าน IT เพื่อหาแนวทางในการจัดการความเสี่ยงอย่างเหมาะสม โดยครอบคลุมการดำเนินการอย่างน้อย ดังนี้<br>(2.1) กำหนดผู้รับผิดชอบต่อความเสี่ยง หรือเจ้าของความเสี่ยง (risk owner)<br>(2.2) ระบุการควบคุมที่มีอยู่ในปัจจุบัน (existing control)<br>(2.3) วิเคราะห์โอกาสหรือความถี่ที่จะเกิดเหตุการณ์ความเสี่ยง (likelihood) และความมีนัยสำคัญหรือผลกระทบที่จะเกิดขึ้น (potential impact) จากเหตุการณ์ดังกล่าว<br>(3) การประเมินค่าความเสี่ยง (risk evaluation) |

| ข้อกำหนด | แนวปฏิบัติ |
|---|---|
| | จัดให้มีประเมินค่าความเสี่ยงด้าน IT เพื่อจัดลำดับในการบริหารความเสี่ยงอย่างเหมาะสม โดยครอบคลุมการดำเนินการอย่างน้อย ดังนี้<br>(3.1) ประเมินผลลัพธ์ที่ได้จากการวิเคราะห์ความเสี่ยง ได้แก่ ค่าโอกาสและผลกระทบ (likelihood และ potential impact) กับเกณฑ์ความเสี่ยง (risk criteria) ที่กำหนดไว้ เพื่อระบุระดับค่าความเสี่ยงของแต่ละเหตุการณ์ความเสี่ยงด้าน IT<br>(3.2) จัดลำดับความเสี่ยงด้าน IT<br>4. การจัดการความเสี่ยง (risk treatment) ควรกำหนดให้มีแนวทางในการจัดการความเสี่ยงด้าน IT อย่างเหมาะสมและสอดคล้องกับผลการประเมินความเสี่ยง (risk assessment) เพื่อให้ความเสี่ยงที่เหลืออยู่ (residual risk) อยู่ในระดับความเสี่ยงที่ยอมรับได้ (risk appetite) โดยครอบคลุมการดำเนินการอย่างน้อย ดังนี้<br>(1) การกำหนดแนวทางในการจัดการความเสี่ยง โดยพิจารณาถึงความคุ้มค่าและวิธีการที่เหมาะสมกับสำนักงานสอบบัญชี เช่น การหยุดหรือหลีกเลี่ยงความเสี่ยง (risk avoidance) การลดหรือบรรเทาความเสี่ยง (risk mitigation) การโอนย้ายความเสี่ยงให้กับผู้อื่น (risk transference) และการยอมรับความเสี่ยงโดยการเสนอเหตุผลต่อหัวหน้าสำนักงานสอบบัญชี หรือคณะกรรมการบริหารของสำนักงานสอบบัญชี เพื่อตัดสินใจ (risk acceptance) เป็นต้น<br>(2) การระบุรายละเอียดของงานที่ต้องดำเนินการ ผู้รับผิดชอบ และระยะเวลาที่ใช้ในการดำเนินการ<br>(3) การประเมินระดับค่าความเสี่ยงที่เหลืออยู่ (residual risk) ว่าอยู่ในระดับความเสี่ยงที่ยอมรับได้<br>(4) การขออนุมัติแผนการบริหารจัดการความเสี่ยงจากหัวหน้าสำนักงานสอบบัญชี หรือคณะกรรมการบริหารของสำนักงานสอบบัญชีที่ได้รับมอบหมาย<br>(5) การสื่อสารแผนการบริหารจัดการความเสี่ยงให้ผู้ที่เกี่ยวข้องรับทราบ<br>5. การจัดทำทะเบียนความเสี่ยง (risk register) ควรจัดให้มีทะเบียนความเสี่ยง (risk register) เพื่อบันทึกผลการประเมินความเสี่ยง และแนวทางในการจัดการความเสี่ยง โดยมีตัวอย่างรายละเอียด ดังนี้<br>(1) วันที่ประเมินความเสี่ยง<br>(2) รายละเอียดเหตุการณ์ความเสี่ยง<br>(3) โอกาสหรือความถี่ที่จะเกิดเหตุการณ์ความเสี่ยง (likelihood)<br>(4) ความมีนัยสำคัญหรือผลกระทบที่จะเกิดขึ้น (potential impact)<br>(5) ระดับค่าความเสี่ยงก่อนการควบคุม (inherent risk) |

| ข้อกำหนด | แนวปฏิบัติ |
|---|---|
| | (6) แนวทางจัดการความเสี่ยง (risk treatment)<br>(7) เจ้าของความเสี่ยง (risk owner)<br>(8) ระดับความเสี่ยงที่เหลืออยู่ (residual risk)<br>(9) สถานะของการจัดการความเสี่ยง (status of risk treatment)<br>6. การติดตามและทบทวนความเสี่ยง (risk monitor and review) ควรจัดให้มีกระบวนการติดตามและทบทวนความเสี่ยงด้าน IT โดยครอบคลุมการดำเนินการดังนี้<br>(1) การกำหนดผู้รับผิดชอบในการติดตามและทบทวนความเสี่ยง<br>(2) การกำหนดดัชนีชี้วัดความเสี่ยงด้าน IT ที่สำคัญ (IT key risk indicator) เพื่อให้สามารถติดตามแนวโน้มของความเสี่ยง และสามารถทบทวนมาตรการควบคุมความเสี่ยงได้อย่างมีประสิทธิภาพ<br>(3) การติดตามความคืบหน้าของการดำเนินงานตามแผนการบริหารจัดการความเสี่ยงด้าน IT<br>7. การรายงานความเสี่ยง (risk reporting) ควรจัดให้มีการรายงานความเสี่ยง และผลการบริหารจัดการความเสี่ยงด้าน IT ต่อหัวหน้าสำนักงานสอบบัญชี หรือคณะกรรมการบริหารของสำนักงานสอบบัญชีอย่างน้อยปีละ 1 ครั้ง โดยครอบคลุมรายละเอียดอย่างน้อย ดังนี้<br>(1) ผลการประเมินและจัดการความเสี่ยงด้าน IT<br>(2) แนวโน้มความเสี่ยงด้าน IT ที่อาจมีผลกระทบกับสำนักงานสอบบัญชี<br>(3) ความคืบหน้าของการดำเนินงานตามแผนการบริหารจัดการความเสี่ยงด้าน IT |
| 2.2.2 <u>นโยบายการรักษาความมั่นคงปลอดภัยด้าน IT (IT security policy)</u> มีเรื่องที่ต้องครอบคลุม ดังนี้<br>(1) โครงสร้างการบริหารงานเพื่อการรักษาความมั่นคงปลอดภัยด้าน IT<br>(2) การบริหารจัดการบุคลากร และบุคคลภายนอก<br>(3) การบริหารจัดการทรัพย์สินด้าน IT<br>(4) การรักษาความมั่นคงปลอดภัยของข้อมูล<br>(5) การควบคุมการเข้าถึงข้อมูลและระบบ IT<br>(6) การควบคุมการเข้ารหัส | [ไม่มีการกำหนดแนวปฏิบัติไว้เป็นการเฉพาะ] |

| ข้อกำหนด | แนวปฏิบัติ |
|---|---|
| (7) การรักษาความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อม<br>(8) การรักษาความมั่นคงปลอดภัยในการปฏิบัติงานด้าน IT<br>(9) การรักษาความมั่นคงปลอดภัยเกี่ยวกับระบบเครือข่ายสื่อสาร<br>(10) การบริหารจัดการโครงการด้าน IT และการจัดหา พัฒนา และบำรุงรักษาระบบ IT<br>(11) การบริหารจัดการเหตุการณ์ผิดปกติด้าน IT<br>(12) แผนฉุกเฉินด้าน IT | |
| 2.3 สำนักงานสอบบัญชีต้องจัดให้มีการดำเนินการตามนโยบายในข้อ 2.2 ดังนี้<br>2.3.1 สื่อสารนโยบายตามข้อ 2.2 ให้แก่บุคลากรของสำนักงานสอบบัญชีและบุคคลภายนอกที่เกี่ยวข้องรับทราบตามบทบาทหน้าที่ ความรับผิดชอบ และสิทธิการเข้าถึงข้อมูล ในลักษณะที่สามารถเข้าถึงได้ง่าย เพื่อให้บุคคลที่เกี่ยวข้องดังกล่าวเข้าใจและสามารถปฏิบัติตามนโยบายได้อย่างถูกต้อง | 1. ในการสื่อสารนโยบายให้กับบุคคลภายนอกที่เกี่ยวข้อง สำนักงานสอบบัญชีควรพิจารณาถึงรายละเอียดที่บุคคลภายนอกควรรู้เพื่อให้สามารถปฏิบัติงานได้สอดคล้องกับนโยบายของสำนักงานสอบบัญชี โดยคำนึงถึงความลับของข้อมูลด้วย |
| 2.3.2 กำหนดขั้นตอนและวิธีปฏิบัติงานให้เป็นไปตามนโยบายตามข้อ 2.2 | 1. สำนักงานสอบบัญชีควรกำหนดขั้นตอนการปฏิบัติงานที่เกี่ยวข้องกับระบบ IT เป็นลายลักษณ์อักษร เพื่อให้เจ้าหน้าที่ผู้ปฏิบัติงานด้าน IT สามารถปฏิบัติงานได้อย่างถูกต้องและเป็นไปตามนโยบายที่เกี่ยวข้องกับการกำกับดูแลความเสี่ยงด้าน IT<br>2. สำนักงานสอบบัญชีควรกำหนดวิธีปฏิบัติสำหรับการอนุมัติยกเว้น (exception) กรณีที่มีความจำเป็นให้ไม่สามารถปฏิบัติตามขั้นตอนและวิธีปฏิบัติงานที่สำนักงานสอบบัญชีกำหนดไว้ โดยจัดให้มีการประเมินความเสี่ยง ควบคุมความเสี่ยงอย่างเพียงพอเหมาะสม และขออนุมัติยกเว้นจากผู้มีอำนาจก่อนดำเนินการต่อไป พร้อมนี้ ควรจัดเก็บหลักฐานการอนุมัติยกเว้นดังกล่าวอย่างเป็นลายลักษณ์อักษร<br>3. สำนักงานสอบบัญชีควรจัดให้มีการสอบทานความเหมาะสมของรายการขออนุมัติยกเว้น ตลอดจนแนวทางการควบคุมความเสี่ยงอย่างน้อยปีละ 1 ครั้ง เพื่อทบทวนแนวทางการดำเนินการให้มีความเหมาะสมต่อความเสี่ยงที่อาจมีการเปลี่ยนแปลงไปตามสภาพแวดล้อมการประกอบธุรกิจและการใช้งานเทคโนโลยีสารสนเทศในการประกอบธุรกิจ |

| ข้อกำหนด | แนวปฏิบัติ |
|---|---|
| 2.3.3 ในกรณีที่มีการเปลี่ยนแปลงนโยบายตามข้อ 2.2 ต้องสื่อสารให้บุคคลที่เกี่ยวข้องได้รับทราบอย่างทั่วถึง และต้องปรับปรุงขั้นตอนและวิธีปฏิบัติงานให้สอดคล้องกับการเปลี่ยนแปลงดังกล่าว | [ไม่มีการกำหนดแนวปฏิบัติไว้เป็นการเฉพาะ] |
| 2.4 สำนักงานสอบบัญชีต้องทบทวนหรือปรับปรุงนโยบายตามข้อ 2.2 อย่างน้อยปีละ 1 ครั้ง และโดยไม่ชักช้าเมื่อมีเหตุการณ์ใด ๆ ซึ่งอาจส่งผลกระทบต่อการกำกับดูแลและบริหารจัดการความเสี่ยงด้าน IT อย่างมีนัยสำคัญ | [ไม่มีการกำหนดแนวปฏิบัติไว้เป็นการเฉพาะ] |

**หมวดที่ 2 การรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (Information Technology Security)**

| ข้อกำหนด | แนวปฏิบัติ |
|---|---|
| **2.1 โครงสร้างการบริหารงานเพื่อการรักษาความมั่นคงปลอดภัยด้าน IT (organization of information technology security)** | |
| **ส่วนที่ 1 โครงสร้างการบริหารงานเพื่อการรักษาความมั่นคงปลอดภัยด้าน IT (organization of information technology security)**<br>สำนักงานสอบบัญชีต้องดำเนินการจัดให้มีโครงสร้างดังกล่าว โดยมีลักษณะอย่างน้อยดังนี้ | |
| 1.1 กำหนดโครงสร้างภายในองค์กร (organizational structure) ในการปฏิบัติงานด้าน IT โดยมีรายละเอียดหน้าที่และความรับผิดชอบของบุคลากรเป็นลายลักษณ์อักษร | สำหรับสำนักงานสอบบัญชีที่ไม่ได้จัดตั้งหน่วยงานที่ปฏิบัติงานด้าน IT ภายใน แต่มีการว่าจ้างบุคลากรภายนอกมาปฏิบัติงานด้าน IT ให้กับสำนักงานสอบบัญชี หรือ บุคลากรที่ปฏิบัติงานด้าน IT เป็นพนักงานของสำนักงานสอบบัญชีเครือข่าย โครงสร้างภายในองค์กรในการปฏิบัติงานด้าน IT ควรมีลักษณะอย่างน้อยดังนี้<br>● มีการระบุหน้าที่และความรับผิดชอบของบุคลากรที่ทำหน้าที่กำกับดูแลและสอบทานการปฏิบัติงานของบุคลากรภายนอก หรือพนักงานของสำนักงานสอบบัญชีเครือข่ายที่มาปฏิบัติงานด้าน IT |
| 1.2 มีการสอบทานการปฏิบัติงานเพื่อป้องกันความเสี่ยงในการรักษาความมันคงปลอดภัยของระบบ IT ที่อาจเกิดขึ้นในการปฏิบัติงาน | สำนักงานสอบบัญชีควรจัดให้มีการแบ่งแยกหน้าที่ในการปฏิบัติงานด้านต่าง ๆ ที่เกี่ยวกับความมั่นคงปลอดภัยของระบบ IT อย่างชัดเจน เพื่อให้มีการสอบทานการปฏิบัติงานระหว่างกัน เพื่อลดข้อผิดพลาดในการปฏิบัติงานและลดโอกาสการกระทำผิด (fraud) เช่น แบ่งแยกผู้พัฒนาระบบงาน (developer) ออกจากผู้มีสิทธิในการนำระบบขึ้นใช้งานจริง เป็นต้น<br>ทั้งนี้ กรณีที่ไม่สามารถแบ่งแยกหน้าที่ความรับผิดชอบได้เนื่องจากข้อจำกัดทางด้านขนาดของธุรกิจหรือบุคลากร สำนักงานสอบบัญชีควรจัดให้มีมาตรการควบคุมทดแทน เช่น การจัดให้มีกระบวนการติดตามและตรวจสอบการปฏิบัติงานของบุคลากรที่เกี่ยวข้องอย่างใกล้ชิดและสม่ำเสมอ หรือ ทุก ๆ การเปลี่ยนแปลงทางด้าน IT ต้องได้รับความเห็นชอบจากผู้มีอำนาจ เป็นต้น |
| **2.2 การบริหารจัดการบุคลากร และบุคคลภายนอก** | |
| **ส่วนที่ 2 การบริหารจัดการบุคลากร และบุคคลภายนอก** | |
| **2.2.1 การบริหารจัดการบุคลากร** | |
| <u>บุคลากรที่ต้องบริหารจัดการ</u><br>2.1 บุคลากรที่เกี่ยวข้องหรือที่ใช้ระบบ IT ปฏิบัติงาน | |

| ข้อกำหนด | แนวปฏิบัติ |
|---|---|
| <u>การบริหารจัดการ</u><br>สำนักงานสอบบัญชีต้องบริหารจัดการบุคลากรตามข้อ 2.1 อย่างเหมาะสม โดยดำเนินการอย่างน้อยดังนี้<br>(1) มีกระบวนการคัดเลือกบุคลากรในการปฏิบัติหน้าที่ดังนี้<br>(1.1) คำนึงถึงความรู้ ความสามารถ และความเพียงพอในการปฏิบัติงาน<br>(1.2) มีการตรวจสอบข้อมูลของบุคลากรก่อนการว่าจ้างอย่างเพียงพอและสอดคล้องกับความเสี่ยงของตำแหน่งงานและหน้าที่ความรับผิดชอบ | [ไม่มีการกำหนดแนวปฏิบัติไว้เป็นการเฉพาะ] |
| (2) มีข้อกำหนดให้บุคลากรทำความเข้าใจ รับทราบและลงนามยอมรับในเรื่องดังนี้<br>(2.1) บทบาทหน้าที่และความรับผิดชอบของบุคลากรดังกล่าวเกี่ยวกับการรักษาความมั่นคงปลอดภัยด้าน IT<br>(2.2) non-disclosure agreement | 1. สำนักงานสอบบัญชีควรให้บุคลากรที่ได้รับการว่าจ้างทำความเข้าใจ รับทราบ และลงนามยอมรับเงื่อนไขการว่าจ้างงานหรือระเบียบข้อบังคับภายในองค์กร นโยบายการรักษาความมั่นคงปลอดภัยด้าน IT และข้อตกลงการไม่เปิดเผยข้อมูล (non-disclosure agreement) ก่อนเริ่มปฏิบัติงาน<br>2. non-disclosure agreement ควรมีเนื้อหาขั้นต่ำ ดังนี้<br>(1) ความเป็นเจ้าของข้อมูลสำคัญทางธุรกิจ ทรัพย์สินทางปัญญา และการป้องกันการรั่วไหลของข้อมูล<br>(2) ความรับผิดชอบในการเก็บรักษาความลับ และไม่เปิดเผยข้อมูลโดยไม่ได้รับอนุญาต<br>(3) การแจ้งเตือนและรายงานผู้เกี่ยวข้องหากพบการรั่วไหลหรือเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต<br>(4) การดำเนินการกรณีละเมิดหรือยกเลิกข้อตกลง รวมทั้งข้อกำหนดในการคืนหรือทำลายข้อมูลที่มีความสำคัญเมื่อสิ้นสุดข้อตกลง |
| (3) สร้างความตระหนักรู้ถึงความเสี่ยงด้าน IT ให้แก่บุคลากรที่ปฏิบัติงาน ซึ่งสามารถเข้าถึงข้อมูลหรือระบบงานภายในองค์กร เพื่อให้บุคลากรดังกล่าวสามารถใช้งานระบบ IT ได้อย่างปลอดภัย | 1. สำนักงานสอบบัญชีควรส่งเสริมและพัฒนาความรู้ด้าน IT ให้แก่บุคลากรอย่างสม่ำเสมอ เช่น การจัดการอบรมภายในองค์กร หรือส่งบุคลากรเข้าร่วมฝึกอบรมภายนอกองค์กร เป็นต้น เพื่อให้บุคลากรมีความรู้ความเข้าใจถึงการใช้งาน IT ที่ถูกต้องปลอดภัย และลดความเสี่ยงที่อาจเกิดขึ้นจากการใช้งาน IT โดยมีเนื้อหา เช่น<br>(1) การรักษาความมั่นคงปลอดภัยด้าน IT<br>(2) ความเสี่ยงด้าน IT และภัยคุกคามทางไซเบอร์<br>(3) หลักเกณฑ์และกฎหมายที่เกี่ยวข้องกับ IT เป็นต้น |

| ข้อกำหนด | แนวปฏิบัติ |
|---|---|
| | 2. สำนักงานสอบบัญชีควรทบทวนแผนการส่งเสริมและพัฒนาความรู้ด้าน IT (training program) อย่างน้อยปีละ 1 ครั้ง เพื่อให้มั่นใจว่าเนื้อหาและรายละเอียดของแผนงานที่เกี่ยวข้องยังคงเพียงพอเหมาะสมกับแนวโน้มความเสี่ยงด้าน IT ในปัจจุบัน<br>3. สำนักงานสอบบัญชีควรจัดให้มีการเสริมสร้างความตระหนักเรื่องการรักษาความมั่นคงปลอดภัยด้าน IT และความเสี่ยงด้าน IT อย่างสม่ำเสมอ ให้แก่บุคลากร (user) ที่สามารถเข้าถึงข้อมูลที่มีความสำคัญของสำนักงานสอบบัญชีหรือข้อมูลของลูกค้า เช่น การทดสอบเรื่องอีเมลหลอกลวง (phishing) การทดสอบเรื่องวิศวกรรมสังคม (social engineering) และการซักซ้อมแผนเพื่อเตรียมความพร้อมรับมือกับการโจมตีทางไซเบอร์ เป็นต้น |
| (4) กำหนดให้บุคลากรงดเว้นการใช้งานระบบ IT ในลักษณะที่อาจก่อให้เกิดความเสียหายแก่สำนักงานสอบบัญชี หรือที่เป็นการกระทำผิดกฎหมาย หรือข้อกำหนดและจรรยาบรรณที่สำนักงานสอบบัญชีกำหนดไว้ | 1. สำนักงานสอบบัญชีควรจัดให้มีนโยบายการใช้งาน IT ที่ยอมรับได้ (acceptable use policy) โดยมีรายละเอียดครอบคลุมขอบเขตความรับผิดชอบของผู้ใช้งาน IT สิ่งที่ผู้ใช้งานพึงปฏิบัติ และสิ่งที่ผู้ใช้งานห้ามปฏิบัติ<br>2. สำนักงานสอบบัญชีควรสื่อสารนโยบายการใช้งาน IT ที่ยอมรับได้ (acceptable use policy) ให้ผู้ใช้งานรับทราบ และลงนามยอมรับนโยบายดังกล่าว |
| (5) กำหนดมาตรการในการลงโทษบุคลากรที่มีพฤติกรรมฝ่าฝืนหรือไม่ปฏิบัติตามนโยบายและมาตรการรักษาความมั่นคงปลอดภัยในการปฏิบัติงานด้าน IT | [ไม่มีการกำหนดแนวปฏิบัติไว้เป็นการเฉพาะ] |
| (6) กำหนดขั้นตอนปฏิบัติเมื่อสิ้นสุดการจ้างงาน หรือเมื่อมีการเปลี่ยนแปลงตำแหน่งงาน เพื่อป้องกันการละเมิดหรือความเสียหายที่อาจเกิดขึ้นต่อทรัพย์สินด้าน IT | 1. สำนักงานสอบบัญชีควรจัดให้มีกระบวนการรองรับเมื่อมีการเปลี่ยนแปลงตำแหน่งงาน และสิ้นสุดการจ้างงาน เช่น การคืนทรัพย์สินขององค์กร การปรับปรุงสิทธิให้เป็นปัจจุบัน การยกเลิกสิทธิเมื่อหมดหน้าที่และความรับผิดชอบ เป็นต้น รวมทั้งมีการสื่อสารให้ผู้ที่เกี่ยวข้องรับทราบถึงการเปลี่ยนแปลงสิทธิ หน้าที่ และความรับผิดชอบ |
| **2.2.2 การบริหารจัดการบุคคลภายนอก (third-party management)** | |
| <u>บุคลากรที่ต้องบริหารจัดการ</u><br>2.2 บุคคลภายนอก ในกรณีที่สำนักงานสอบบัญชีมีการดำเนินการอย่างใดอย่างหนึ่งดังนี้<br>● ใช้บริการงานด้าน IT จากบุคคลภายนอก<br>● เชื่อมต่อระบบ IT กับบุคคลภายนอก | แม้ในปัจจุบัน สำนักงานสอบบัญชียังไม่มีการว่าจ้างบุคคลภายนอกมาดำเนินการอย่างใดอย่างหนึ่งดังนี้<br>● ใช้บริการงานด้าน IT จากบุคคลภายนอก<br>● เชื่อมต่อระบบ IT กับบุคคลภายนอก<br>● อนุญาตให้บุคคลภายนอกสามารถเข้าถึงข้อมูลสำคัญหรือข้อมูลของลูกค้าของสำนักงานสอบบัญชีได้ |

| ข้อกำหนด | แนวปฏิบัติ |
|---|---|
| • อนุญาตให้บุคคลภายนอกสามารถเข้าถึงข้อมูลสำคัญหรือข้อมูลของลูกค้าของสำนักงานสอบบัญชีได้ | อย่างไรก็ดี สำนักงานสอบบัญชีต้องจัดทำนโยบายและแนวปฏิบัติสำหรับการว่าจ้างบุคคลภายนอกอย่างเป็นลายลักษณ์อักษร ให้ครอบคลุมรายละเอียดอย่างน้อย ดังนี้ |
| <u>การบริหารจัดการ</u><br>สำนักงานสอบบัญชีต้องบริหารจัดการบุคคลภายนอกตามข้อ 2.2 ดังนี้<br>(1) ประเมินความเสี่ยงจากการใช้บริการ การเชื่อมต่อหรือการเข้าถึงข้อมูลจากบุคคลภายนอก รวมถึงผู้รับดำเนินการช่วง (subcontract) จากบุคคลภายนอก | 1. สำนักงานสอบบัญชีควรประเมินความเสี่ยงและผลกระทบในเรื่องดังต่อไปนี้ก่อน<br>• การใช้บริการงานด้าน IT จากบุคคลภายนอก<br>• การเชื่อมต่อระบบ IT กับบุคคลภายนอก<br>• การอนุญาตให้บุคคลภายนอกสามารถเข้าถึงข้อมูลสำคัญหรือข้อมูลของลูกค้าที่ควบคุมดูแลโดยสำนักงานสอบบัญชีได้<br>โดยคำนึงถึงความเสี่ยง ดังนี้<br>(1) ความเสี่ยงด้านกฎหมาย และกฎเกณฑ์ที่เกี่ยวข้องทั้งในประเทศและต่างประเทศ เช่น กฎหมายเกี่ยวกับการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ กฎหมายเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล กฎหมายเกี่ยวกับธุรกรรมทางอิเล็กทรอนิกส์ และ The EU General Data Protection Regulation (GDPR) เป็นต้น<br>(2) ความเสี่ยงจากการกำกับดูแลและบริหารจัดการบุคคลภายนอกที่ไม่รัดกุมเพียงพอ เช่น การไม่สามารถตรวจสอบการดำเนินงานของบุคคลภายนอกได้ด้วยตนเอง เป็นต้น<br>(3) ความเสี่ยงจากการพึ่งพาบุคคลภายนอกรายใดรายหนึ่งเป็นหลัก (third party/vendor locked-in) ซึ่งทำให้มีข้อจำกัดในการเปลี่ยนแปลงเทคโนโลยี ผู้ให้บริการ หรือข้อจำกัดในการนำระบบหรือข้อมูลกลับมาดำเนินการเอง<br>(4) ความเสี่ยงด้าน IT และภัยทางไซเบอร์ เช่น ระบบที่ให้บริการโดยบุคคลภายนอกเกิดขัดข้อง ระบบของบุคคลภายนอกมีช่องโหว่ทำให้ข้อมูลเกิดการสูญหายหรือรั่วไหล เป็นต้น<br>(5) ความเสี่ยงกรณีบุคคลภายนอกให้ผู้อื่นดำเนินการแทน (sub-contracting) เช่น subcontractor ปฏิบัติงานบกพร่อง เป็นต้น<br>2. สำนักงานสอบบัญชีควรจัดให้มีการกำหนดระดับความมีนัยสำคัญของบุคคลภายนอกแต่ละราย |
| (2) กำหนดวิธีปฏิบัติและหลักเกณฑ์ในการคัดเลือกบุคคลภายนอก | 1. สำนักงานสอบบัญชีควรกำหนดกระบวนการและหลักเกณฑ์ในการคัดเลือกบุคคลภายนอกอย่างชัดเจน และเป็นลายลักษณ์อักษร เพื่อให้มั่นใจว่าผู้ให้บริการภายนอกจะสามารถให้บริการได้ตรงตามความต้องการของสำนักงานสอบบัญชี ทั้งนี้ ในการตัดสินใจใช้บริการ การเชื่อมต่อ หรือการเข้าถึงข้อมูลจากบุคคลภายนอก ที่มีความเสี่ยงหรือมีนัยสำคัญควรได้รับความเห็นชอบจากหัวหน้าสำนักงานสอบบัญชีหรือคณะกรรมการบริหารของสำนักงานสอบบัญชีที่ได้รับมอบหมาย<br>2. สำนักงานสอบบัญชีควรประเมินศักยภาพบุคคลภายนอก (due diligence) ให้สอดคล้องกับระดับความเสี่ยง และความมีนัยสำคัญ |

| ข้อกำหนด | แนวปฏิบัติ |
|---|---|
| | ของบุคคลภายนอก โดยคำนึงถึงเรื่องดังต่อไปนี้<br>(1) ฐานะทางการเงิน ชื่อเสียง ความรู้ความเชี่ยวชาญ ประสบการณ์ และความสามารถในการให้บริการในช่วงที่ผ่านมา<br>(2) การบริหารจัดการความเสี่ยง การควบคุมภายใน การตรวจสอบภายใน และการติดตามผลการปฏิบัติงาน<br>(3) การรักษาความมั่นคงปลอดภัยด้าน IT<br>(4) การบริหารจัดการความต่อเนื่องทางธุรกิจ และความพร้อมรับมือภัยหรือเหตุการณ์ต่าง ๆ<br>(5) การปฏิบัติตามกฎหมายและกฎเกณฑ์ที่เกี่ยวข้อง เช่น การขอตรวจสอบเอกสารหลักฐานหรือใบรับรองจากบุคคลภายนอกในการดำเนินการตามกฎหมายและกฎเกณฑ์ที่เกี่ยวข้อง หรือการตรวจสอบประวัติด้านการกระทำความผิด เป็นต้น<br>(6) การปฏิบัติตามมาตรฐานสากลด้าน IT เช่น การตรวจสอบเอกสารหลักฐานการได้รับการรองรับตามมาตรฐาน ISO 27001 เป็นต้น โดยในการรับรองการปฏิบัติตามมาตรฐานสากล สำนักงานสอบบัญชีควรพิจารณาว่า บุคคลภายนอกได้รับการรับรองในระบบที่สำคัญ หรือระบบที่สำนักงานสอบบัญชีใช้บริการ เชื่อมต่อ หรือเข้าถึงข้อมูล หรือได้รับการรับรองครอบคลุมทั้งองค์กร<br>(7) การใช้เทคโนโลยีแบบเปิด (open technology) เพื่อให้สามารถนำระบบหรือข้อมูลไปใช้งานหรือเชื่อมโยงกับระบบอื่นได้ (interoperability) และลดข้อจำกัดในการย้ายหรือเปลี่ยนแปลงเทคโนโลยี ผู้ให้บริการ หรือพันธมิตร รวมถึงข้อจำกัดในการนำระบบหรือข้อมูลกลับมาดำเนินการเอง<br>(8) กรณีที่บุคคลภายนอกมอบหมายการปฏิบัติงานที่สำคัญให้กับบุคคลอื่นต่อ (sub-contracting to another supplier) สำนักงานสอบบัญชีควรพิจารณารายละเอียดด้านความมั่นคงปลอดภัยสารสนเทศของบุคคลดังกล่าวด้วย |
| (3) กำหนดบทบาท หน้าที่ และความรับผิดชอบของสำนักงานสอบบัญชีและบุคคลภายนอกอย่างชัดเจนและเป็นลายลักษณ์อักษร | 1. สำนักงานสอบบัญชีควรจัดทำสัญญาหรือข้อตกลงการใช้บริการ การเชื่อมต่อ หรือการเข้าถึงข้อมูลจากบุคคลภายนอกอย่างเป็นลายลักษณ์อักษร โดยมีการลงนามร่วมกันระหว่างสำนักงานสอบบัญชีและบุคคลภายนอก เพื่อให้มั่นใจได้ว่าบุคคลภายนอกมีหน้าที่รับผิดชอบในการรักษาความมั่นคงปลอดภัยของระบบ IT ในระดับที่เหมาะสม โดยมีรายละเอียดสอดคล้องกับความเสี่ยง และความมีนัยสำคัญของบุคคลภายนอก ดังนี้<br>(1) ขอบเขตการให้บริการ การเชื่อมต่อ และการเข้าถึงข้อมูลจากบุคคลภายนอก<br>(2) บทบาท หน้าที่ และความรับผิดชอบของบุคคลภายนอกและสำนักงานสอบบัญชี<br>(3) มาตรฐานขั้นต่ำในการปฏิบัติงานของบุคคลภายนอก เช่น การรักษาความปลอดภัยของระบบ IT การรักษาความลับของข้อมูล และการไม่นำข้อมูลไปใช้นอกเหนือจากที่ระบุไว้ในสัญญาหรือข้อตกลงการให้บริการ เป็นต้น<br>(4) ข้อตกลงระดับการให้บริการด้าน IT (service level agreement: SLA) สำหรับการใช้บริการจากบุคคลภายนอก<br>(5) การติดตามและรายงานผลการปฏิบัติงานของบุคคลภายนอก ซึ่งครอบคลุมถึงการแจ้งการเปลี่ยนแปลงหรือปัญหาที่สำคัญ และ |

| ข้อกำหนด | แนวปฏิบัติ |
|---|---|
| | การรายงานเหตุการณ์ผิดปกติอย่างทันการณ์<br>(6) รายชื่อ และช่องทางการติดต่อในกรณีเกิดปัญหาเกี่ยวกับการรักษาความมั่นคงปลอดภัยของระบบ IT<br>(7) การทำลายข้อมูลเมื่อสิ้นสุดหรือยกเลิกการใช้บริการ การเชื่อมต่อ และการเข้าถึงข้อมูลจากบุคคลภายนอก<br>(8) เงื่อนไขหรือสิทธิของสำนักงานสอบบัญชีในการเปลี่ยนแปลง ยุติ หรือยกเลิกสัญญาหรือข้อตกลงกับบุคคลภายนอก เช่น กรณีที่บุคคลภายนอกมีการละเมิดสัญญาหรือข้อตกลง เป็นต้น<br>(9) การจัดให้มีแผนฉุกเฉินด้าน IT (IT contingency plan) ที่สอดคล้องกับแผนฉุกเฉินด้าน IT ของสำนักงานสอบบัญชี<br>(10) ความรับผิดชอบต่อความเสียหายที่เกิดจากบุคคลภายนอก เช่น กรณีการให้บริการไม่เป็นไปตาม SLA ที่กำหนดไว้ เป็นต้น<br>หากมีข้อจำกัดในการระบุรายละเอียดและกำหนดเงื่อนไขที่สำคัญลงในข้อตกลงหรือสัญญาที่ทำกับบุคคลภายนอก สำนักงานสอบบัญชีควรมีการประเมินความเสี่ยงและพิจารณาแนวทางควบคุมความเสี่ยงที่เพียงพอเหมาะสม พร้อมทั้งขออนุมัติยกเว้น (exception) จากผู้มีอำนาจ |
| (4) กรณีบุคคลภายนอกซึ่งเป็นผู้ให้บริการงานด้าน IT รายที่มีนัยสำคัญตามผลการประเมินความเสี่ยงในข้อ 2.2 (1) ข้อตกลงหรือสัญญาการให้บริการต้องระบุสิทธิให้สำนักงานสอบบัญชี สำนักงาน ก.ล.ต. และผู้ตรวจสอบภายนอกที่ได้รับการแต่งตั้งจากสำนักงานสอบบัญชีหรือสำนักงาน ก.ล.ต. สามารถเข้าตรวจสอบการดำเนินงานและการควบคุมภายในของบุคคลภายนอกดังกล่าวได้<br>หากมีเหตุจำเป็นทำให้สำนักงานสอบบัญชีไม่สามารถระบุสิทธิในการเข้าตรวจสอบตามวรรคหนึ่งไว้ในข้อตกลงหรือสัญญา สำนักงานสอบบัญชีต้องมีมาตรการประเมินหรือติดตามการดำเนินงานและการควบคุมภายในของบุคคลภายนอกให้รัดกุมเพียงพอสอดคล้องกับความเสี่ยงและความมีนัยสำคัญของการใช้บริการ การเชื่อมต่อ หรือการเข้าถึงข้อมูล | 1. สำนักงานสอบบัญชีควรกำหนดสิทธิให้สำนักงานสอบบัญชี สำนักงาน ก.ล.ต. และผู้ตรวจสอบภายนอกที่ได้รับการแต่งตั้งจากสำนักงานสอบบัญชี หรือ สำนักงาน ก.ล.ต. สามารถเข้าตรวจสอบการดำเนินงานด้าน IT และการควบคุมภายในของบุคคลภายนอกที่ให้บริการงานด้าน IT รายที่มีนัยสำคัญ โดยระบุไว้เป็นส่วนหนึ่งของข้อตกลงหรือสัญญาการให้บริการ ในกรณีที่ไม่สามารถระบุสิทธิดังกล่าวได้ สำนักงานสอบบัญชีควรพิจารณาเลือกใช้บุคคลภายนอกที่มีการดำเนินการตรวจสอบด้าน IT โดยผู้ตรวจสอบภายนอกที่มีความเป็นอิสระและได้มาตรฐานสากล เช่น ผลการตรวจสอบตามมาตรฐาน SSAE 18 (SOC 2 Type 2 Report : ความสามารถในการรักษาข้อมูลที่ sensitive สำหรับ cloud-based service provider) เป็นต้น นอกจากนี้ สำนักงานสอบบัญชีควรพิจารณารายละเอียดของผลการตรวจสอบที่จัดทำโดยผู้ตรวจสอบภายนอกอย่างเหมาะสม |

| ข้อกำหนด | แนวปฏิบัติ |
|---|---|
| (5) มี non-disclosure agreement สำหรับบุคคลภายนอกหรือผู้รับดำเนินการช่วงของบุคคลภายนอก ในกรณีที่บุคคลดังกล่าวสามารถเข้าถึงข้อมูลสำคัญของสำนักงานสอบบัญชีหรือข้อมูลของลูกค้า | 1. non-disclosure agreement ควรมีรายละเอียดครอบคลุมขอบเขตความรับผิดชอบในการเก็บรักษาความลับ การไม่เปิดเผยข้อมูลโดยไม่ได้รับอนุญาต การรายงานสำนักงานสอบบัญชีเมื่อพบการรั่วไหลหรือเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต และการทำลายข้อมูลที่มีความสำคัญเมื่อสิ้นสุดข้อตกลงหรือสัญญา |
| (6) กำกับดูแล ติดตาม และบริหารจัดการความเสี่ยงจากการใช้บริการ การเชื่อมต่อหรือการเข้าถึงข้อมูลจากบุคคลภายนอก โดยต้องสอดคล้องกับระดับความเสี่ยงและระดับความมีนัยสำคัญของบุคคลภายนอก | 1. สำนักงานสอบบัญชีควรกำกับดูแล ติดตาม และบริหารจัดการความเสี่ยงจากการใช้บริการ การเชื่อมต่อ หรือการเข้าถึงข้อมูลจากบุคคลภายนอกให้สอดคล้องกับความเสี่ยง และความมีนัยสำคัญของบุคคลภายนอก โดยครอบคลุมการดำเนินการอย่างน้อย ดังนี้<br>(1) กำหนดผู้รับผิดชอบในการติดตามผลการปฏิบัติงานของบุคคลภายนอกอย่างต่อเนื่อง โดยพิจารณาตามขอบเขต ระดับความเสี่ยงและความมีนัยสำคัญของการใช้บริการ การเชื่อมต่อ หรือการเข้าถึงข้อมูลจากบุคคลภายนอก<br>(2) จัดให้มีทะเบียนบุคคลภายนอก เพื่อให้สามารถใช้ในการบริหารจัดการความเสี่ยง ติดตาม และตรวจสอบการปฏิบัติงานของบุคคลภายนอกได้อย่างครบถ้วนต่อเนื่อง โดยมีรายละเอียดครอบคลุม<br>- ชื่อบุคคลภายนอก<br>- รายละเอียดของการใช้บริการ การเชื่อมต่อ หรือการเข้าถึงข้อมูลจากบุคคลภายนอก<br>- ระดับความเสี่ยงและระดับความมีนัยสำคัญ<br>- วันเริ่มต้นและสิ้นสุดสัญญาหรือข้อตกลง<br>(3) จัดให้มีมาตรการควบคุมและติดตามสิทธิการเข้าถึงข้อมูลสารสนเทศของบุคคลภายนอกอย่างสม่ำเสมอ เพื่อให้สิทธิดังกล่าวเป็นไปตามหลักความจำเป็นต้องรู้ (need-to-know basis)<br>(4) กำหนดให้บุคคลภายนอกรายงานเหตุการณ์ผิดปกติที่เกิดขึ้นระหว่างการดำเนินงานที่เกี่ยวข้องให้สำนักงานสอบบัญชีได้รับทราบอย่างทันการณ์<br>(5) ประเมินผลการปฏิบัติงานหรือผลการให้บริการของบุคคลภายนอก ทั้งในด้านประสิทธิภาพของบริการ การรักษาความมั่นคงปลอดภัยด้าน IT และการปฏิบัติตามกฎหมายที่เกี่ยวข้อง เมื่อจะต่อสัญญาหรือเมื่อถึงรอบระยะเวลาที่สำนักงานสอบบัญชีกำหนด<br>(6) ทบทวนคุณสมบัติบุคคลภายนอกอย่างสม่ำเสมอ เพื่อให้มั่นใจว่าบุคคลภายนอกยังคงมีคุณสมบัติที่เหมาะสม |
| (7) รักษาความมั่นคงปลอดภัยด้าน IT จากการใช้บริการการเชื่อมต่อ หรือการเข้าถึงข้อมูลจากบุคคลภายนอก | 1. สำนักงานสอบบัญชีควรมีแนวทางการดูแลให้มั่นใจว่าการใช้บริการ การเชื่อมต่อ หรือการเข้าถึงข้อมูลจากบุคคลภายนอกมีการรักษาความมั่นคงปลอดภัยด้าน IT ตามกรอบหลักการที่สำคัญ 3 ประการ คือ การธำรงไว้ซึ่งความลับ (confidentiality) ความถูกต้องครบถ้วน (integrity) และสภาพพร้อมใช้งาน (availability) ของระบบและข้อมูล และสอดคล้องกับนโยบายและมาตรการรักษา |

| ข้อกำหนด | แนวปฏิบัติ |
|---|---|
| ที่สอดคล้องกับมาตรฐานการรักษาความมั่นคงปลอดภัยด้าน IT ของสำนักงานสอบบัญชี | ความมั่นคงปลอดภัยด้าน IT ของสำนักงานสอบบัญชีหรือมาตรฐานสากลที่เกี่ยวข้อง เช่น ISO/IEC 27001 หรือ เกณฑ์ในการกำกับดูแลด้านเทคโนโลยีสารสนเทศของสำนักงานก.ล.ต เป็นต้น โดยพิจารณาให้สอดคล้องกับระดับความเสี่ยง และความมีนัยสำคัญของบุคคลภายนอก |
| (8) เตรียมความพร้อมรับมือต่อเหตุการณ์ผิดปกติด้าน IT ที่อาจเกิดขึ้นและมีผลกระทบอย่างมีนัยสำคัญเพื่อให้สามารถให้บริการหรือดำเนินธุรกิจได้อย่างต่อเนื่อง | 1. สำนักงานสอบบัญชีควรจัดให้มีแผนรองรับในกรณีที่บุคคลภายนอกเกิดเหตุการณ์ผิดปกติด้าน IT (incident response plan) ซึ่งมีผลกระทบกับการดำเนินการของสำนักงานสอบบัญชีโดยครอบคลุมเหตุการณ์ที่เกี่ยวข้องกับเหตุการณ์ความปลอดภัยทางไซเบอร์และเหตุการณ์การละเมิดต่อข้อมูลส่วนบุคคล |
| **2.3 การบริหารจัดการทรัพย์สินด้าน IT (IT asset management)** | |
| **ส่วนที่ 3 การบริหารจัดการทรัพย์สินด้าน IT (IT asset management)**<br>สำนักงานสอบบัญชีต้องจัดให้มีการบริหารจัดการทรัพย์สินด้าน IT เพื่อนำไปใช้ดำเนินการเกี่ยวกับการรักษาความมั่นคงปลอดภัยด้าน IT ได้อย่างเหมาะสม ครบถ้วนและเป็นปัจจุบัน ดังนี้ | |
| 3.1 จัดทำทะเบียนรายการทรัพย์สินด้าน IT ประเภทฮาร์ดแวร์ ซอฟต์แวร์ รวมถึงสิทธิในการใช้งานฮาร์ดแวร์และซอฟต์แวร์ | 1. สำนักงานสอบบัญชีควรกำหนดระเบียบปฏิบัติเกี่ยวกับการบริหารจัดการทรัพย์สินด้าน IT ครอบคลุมการจัดทำทะเบียนรายการทรัพย์สิน การปรับปรุงทะเบียนรายการทรัพย์สิน การยกเลิกและเรียกคืนทรัพย์สิน<br>2. สำนักงานสอบบัญชีควรจัดทำทะเบียนรายการทรัพย์สินด้าน IT ประเภทอุปกรณ์ (hardware) รวมถึง virtual machine ให้ครบถ้วนและเป็นปัจจุบัน โดยมีตัวอย่างของรายละเอียด ดังนี้<br>(1) เลขทะเบียนทรัพย์สิน<br>(2) ประเภทฮาร์ดแวร์<br>(3) รายละเอียดทางเทคนิค ยี่ห้อ รุ่น<br>(4) ระบบปฏิบัติการและเวอร์ชัน<br>(5) เจ้าของทรัพย์สิน<br>(6) ผู้ดูแลทรัพย์สิน<br>(7) สถานที่ตั้ง<br>(8) วันที่เริ่มใช้งาน/วันที่ติดตั้ง |

| ข้อกำหนด | แนวปฏิบัติ |
|---|---|

(9) วันที่สิ้นสุดการรับประกัน หรือสิ้นสุดการใช้งานตามสัญญา

(10) ประเภทการครอบครอง (ซื้อ หรือเช่า)

<u>ตัวอย่างเช่น</u>

| เลขทะเบียนทรัพย์สิน | ประเภท | รายละเอียด | ระบบปฏิบัติการ/เวอร์ชัน | เจ้าของทรัพย์สิน | ผู้ดูแลทรัพย์สิน | สถานที่ตั้ง | วันที่เริ่มใช้งาน | วันที่สิ้นสุดประกัน | การครอบครอง |
|---|---|---|---|---|---|---|---|---|---|
| RT123456 | Switch | ยี่ห้อ CC รุ่น 1000 48 ports | A-OS 1.0.2 | ฝ่าย IT | บริษัท A | สำนักงาน | 1 มี.ค. 64 | 1 มี.ค. 67 | ซื้อ |
| SV212224 | Router | ยี่ห้อ JP รุ่น 3700 8 ports | 13.2B | ฝ่าย IT | ฝ่าย IT | สำนักงาน | 5 พ.ค. 64 | 5 พ.ค. 66 | เช่า |

3. สำนักงานสอบบัญชีควรจัดทำทะเบียนรายการทรัพย์สินด้าน IT ประเภทซอฟต์แวร์ (software) ให้ครบถ้วนและเป็นปัจจุบัน โดยมีตัวอย่างของรายละเอียด ดังนี้

(1) เลขทะเบียนทรัพย์สิน

(2) ชื่อซอฟต์แวร์

(3) รายละเอียดทางเทคนิค/การใช้งาน

(4) ระบบปฏิบัติการและเวอร์ชัน

(5) หน่วยงานภายในผู้เป็นเจ้าของซอฟต์แวร์

(6) วันที่ลงทะเบียนซอฟต์แวร์

(7) วันที่สิ้นสุดการใช้บริการ

(8) เลขทะเบียนทรัพย์สินฮาร์ดแวร์ที่อ้างอิง

<table>
<tr><th>ข้อกำหนด</th><th>แนวปฏิบัติ</th></tr>
<tr><td></td><td>ตัวอย่างเช่น
<table>
<tr><th>เลขทะเบียนทรัพย์สิน</th><th>ชื่อซอฟต์แวร์</th><th>รายละเอียดทางเทคนิค / การใช้งาน</th><th>ระบบปฏิบัติการและเวอร์ชัน</th><th>หน่วยงานภายในผู้เป็นเจ้าของซอฟต์แวร์</th><th>วันที่ลงทะเบียนซอฟต์แวร์</th><th>วันที่สิ้นสุดการใช้บริการ</th><th>เลขทะเบียนทรัพย์สินฮาร์ดแวร์ (เพื่อใช้อ้างอิง)</th></tr>
<tr><td>SP123456</td><td>Sheet processor pro</td><td>Software ประมวลผล sheet/excel</td><td>10.2.3A</td><td>IT</td><td>1 พ.ค. 64</td><td>1 ธ.ค. 69</td><td>SV123456</td></tr>
</table>
4. สำนักงานสอบบัญชีควรปรับปรุงทะเบียนทรัพย์สินสารสนเทศต่าง ๆ ให้ครบถ้วนและเป็นปัจจุบันอยู่อย่างสม่ำเสมอ อย่างน้อยปีละ 1 ครั้ง และทุกครั้งที่มีการเปลี่ยนแปลงระบบ IT อย่างมีนัยสำคัญ</td></tr>
<tr><td>3.2 กำหนดบุคคลหรือหน่วยงานซึ่งรับผิดชอบทรัพย์สินด้าน IT แต่ละรายการ</td><td>1. สำนักงานสอบบัญชีควรกำหนดบุคคลหรือหน่วยงานที่รับผิดชอบในการจัดทำและปรับปรุงทะเบียนรายการทรัพย์สินด้าน IT รวมถึงบำรุงรักษาทรัพย์สินด้าน IT อย่างสม่ำเสมอตลอดอายุการใช้งานของทรัพย์สินดังกล่าว</td></tr>
<tr><td>3.3 จัดให้มีการบำรุงรักษาทรัพย์สินด้าน IT อย่างสม่ำเสมอ</td><td>1. สำนักงานสอบบัญชีควรบำรุงรักษาทรัพย์สินด้าน IT ให้มีสภาพพร้อมใช้งานและรองรับการดำเนินธุรกิจอย่างต่อเนื่อง พร้อมทั้งวางแผนรองรับทรัพย์สินด้าน IT ที่ใกล้จะสิ้นสุดอายุการใช้งาน (end of life) หรือสิ้นสุดการสนับสนุนหรือให้บริการจากผู้ผลิต (end of support) ได้อย่างเหมาะสมทันการณ์ ทั้งนี้ ในกรณีที่มีความจำเป็นต้องใช้ทรัพย์สินที่สิ้นสุดอายุการใช้งานหรือสิ้นสุดการสนับสนุนหรือให้บริการจากผู้ผลิต สำนักงานสอบบัญชีควรประเมินความเสี่ยงและจัดให้มีมาตรการควบคุมความเสี่ยงอย่างเหมาะสม</td></tr>
<tr><td colspan="2">2.4 การรักษาความมั่นคงปลอดภัยของข้อมูล (data security)</td></tr>
<tr><td>ส่วนที่ 4 การรักษาความมั่นคงปลอดภัยของข้อมูล (data security)<br>สำนักงานสอบบัญชีต้องจัดให้มีการรักษาความมั่นคงปลอดภัยของข้อมูลเพื่อให้ข้อมูลมีความถูกต้องครบถ้วนและมีสภาพพร้อมใช้งาน รวมถึงสามารถรักษาความลับของข้อมูลได้อย่างเหมาะสม ดังนี้</td><td></td></tr>
</table>

| ข้อกำหนด | แนวปฏิบัติ |
|---|---|
| 4.1 การกำหนดบุคคลหรือหน่วยงานซึ่งเป็นเจ้าของข้อมูล | 1. สำนักงานสอบบัญชีควรกำหนดบุคคลหรือหน่วยงานซึ่งเป็นเจ้าของข้อมูล (data owner) เพื่อรับผิดชอบในการกำหนดผู้ใช้งาน สิทธิการเข้าถึงและแก้ไขเปลี่ยนแปลงข้อมูล และวิธีปฏิบัติในการใช้งานข้อมูลอย่างปลอดภัย |
| 4.2 การจัดชั้นความลับของข้อมูล (data classification) และแนวทางการรักษาความปลอดภัยของข้อมูลที่สอดคล้องตามชั้นความลับ | 1. สำนักงานสอบบัญชีควรกำหนดหลักเกณฑ์การจัดชั้นความลับของข้อมูล (data classification) และวิธีการจัดการข้อมูล (data handling) ตามชั้นความลับ ให้ครอบคลุมตลอดวงจรชีวิตของข้อมูล (data life cycle) ตั้งแต่การสร้างหรือการได้มาซึ่งข้อมูล การประมวลผล การจัดเก็บ การใช้งาน ไปจนถึงการทำลายข้อมูล รวมทั้งระบุชั้นความลับของข้อมูล (labeling) อย่างชัดเจน<br>2. สำนักงานสอบบัญชีควรจัดให้มีการรักษาความปลอดภัยของข้อมูลที่อยู่บนสื่อบันทึกข้อมูล โดยดำเนินการ ดังนี้<br>(1) คำนึงถึงความเสี่ยงที่สื่อบันทึกข้อมูลอาจเสื่อมสภาพ รวมทั้งวิธีการนำข้อมูลกลับมาใช้งานใหม่ ในกรณีที่จัดเก็บข้อมูลเป็นระยะเวลานาน<br>(2) จัดเก็บสื่อบันทึกข้อมูลในพื้นที่ที่มีความมั่นคงปลอดภัย และเป็นไปตามคำแนะนำของผู้ผลิต (ถ้ามี)<br>(3) จัดให้มีมาตรการรักษาความปลอดภัยของการขนส่งสื่อบันทึกข้อมูล (physical media transfer) |
| 4.3 การจัดให้มีแนวทางในการนำเข้า ประมวลผล และทำลายข้อมูลอย่างปลอดภัย | 1. สำนักงานสอบบัญชีควรกำหนดระเบียบปฏิบัติในการทำลายข้อมูล (data disposal) ซึ่งครอบคลุมหน้าที่ความรับผิดชอบของเจ้าของข้อมูล หน่วยงานที่เกี่ยวข้อง และวิธีการทำลายข้อมูลที่เหมาะสมกับชั้นความลับของข้อมูล<br>2. สำนักงานสอบบัญชีควรจัดให้มีกระบวนการควบคุมการทำลายข้อมูลที่ครอบคลุมการขออนุมัติจากเจ้าของข้อมูลก่อนดำเนินการ การควบคุมและสอบทานการปฏิบัติงาน และการจัดทำทะเบียนการทำลายข้อมูลสำคัญ |
| 4.4 การจัดทำทะเบียนทรัพย์สินด้าน IT ประเภทข้อมูล (data inventory) ให้ครบถ้วนและเป็นปัจจุบัน | 1. สำนักงานสอบบัญชีควรจัดทำทะเบียนทรัพย์สินประเภทข้อมูล (data inventory) ให้ครบถ้วนและเป็นปัจจุบัน โดยมีตัวอย่างของรายละเอียด ดังนี้<br>(1) เลขทะเบียนข้อมูล<br>(2) ชื่อข้อมูลหรือชุดข้อมูล<br>(3) รายละเอียดลักษณะ และประเภทของข้อมูล<br>(4) ระดับชั้นความลับและระดับความสำคัญของข้อมูล<br>(5) เจ้าของข้อมูลและผู้ดูแลข้อมูล (data owner) |

<table>
<tr><th>ข้อกำหนด</th><th>แนวปฏิบัติ</th></tr>
<tr><td></td><td>(6) สถานที่ หรือเครื่องแม่ข่ายที่จัดเก็บ<br><u>ตัวอย่างเช่น</u>
<table>
<tr><th>เลขทะเบียนข้อมูล</th><th>ชื่อข้อมูล/ชุดข้อมูล</th><th>รายละเอียด</th><th>ระดับชั้นความลับ</th><th>เจ้าของข้อมูล</th><th>ผู้ดูแลข้อมูล</th><th>สถานที่จัดเก็บ</th></tr>
<tr><td>ABC-IT-001</td><td>IT security policy</td><td>นโยบายด้าน IT</td><td>Internal</td><td>ฝ่าย IT</td><td>ฝ่าย IT</td><td>ระบบ Intranet</td></tr>
<tr><td>ABC-Data-002</td><td>Customer information</td><td>ข้อมูลของลูกค้า ได้แก่ ชื่อ สกุล วันเดือนปีเกิด</td><td>Confidential</td><td>ฝ่ายปฏิบัติการหลักทรัพย์</td><td>ฝ่าย IT</td><td>- DB server 015<br>- DB backup 012</td></tr>
</table></td></tr>
<tr><td colspan="2">2.5 การควบคุมการเข้าถึงข้อมูลและระบบ IT (access control)</td></tr>
<tr><td>ส่วนที่ 5 การควบคุมการเข้าถึงข้อมูลและระบบ IT (access control)<br>สำนักงานสอบบัญชีต้องจัดให้มีการควบคุมการเข้าถึงข้อมูลและระบบ IT อย่างมีประสิทธิภาพ เพื่อให้สามารถป้องกันการเข้าถึง และเปลี่ยนแปลงแก้ไขโดยผู้ไม่มีสิทธิหรือไม่ได้รับอนุญาต ดังนี้</td><td></td></tr>
<tr><td>5.1 จัดให้มีแนวทางการบริหารจัดการบัญชีผู้ใช้งานและสิทธิการเข้าถึง โดยมีการทบทวนปรับปรุงสิทธิให้เหมาะสมอย่างสม่ำเสมอ สอดคล้องกับหน้าที่ความรับผิดชอบ รวมถึงมีกระบวนการเพิกถอนสิทธิเมื่อสิ้นสุดความจำเป็นต้องใช้งาน<br>ทั้งนี้ หากสำนักงานสอบบัญชีไม่สามารถกำหนดแนวทางการบริหารจัดการบัญชีและสิทธิการเข้าถึงข้อมูลและระบบ IT ตามลักษณะขั้นต่ำของแนวปฏิบัตินี้ทุกข้อได้</td><td>1. แนวทางการบริหารจัดการบัญชีผู้ใช้งาน ควรครอบคลุมอย่างน้อย ดังนี้<br>(1) หน่วยงาน หรือบุคลากร ที่รับผิดชอบในการบริหารจัดการบัญชีผู้ใช้งาน<br>(2) ขั้นตอนการสร้างบัญชีผู้ใช้งาน โดยบัญชีผู้ใช้งาน (user ID) ควรระบุตัวตนผู้ใช้งานได้ และหลีกเลี่ยงการใช้บัญชีผู้ใช้งานที่มีผู้ใช้งานมากกว่า 1 ราย (shared ID)<br>(3) การจำกัดหรือหลีกเลี่ยงใช้งานบัญชีผู้ใช้งานที่มาพร้อมกับระบบ (default user account)<br>(4) การทบทวนบัญชีผู้ใช้งานอย่างน้อยปีละ 1 ครั้ง<br>(5) การระงับหรือลบบัญชีผู้ใช้งานเมื่อ (1) ผู้ใช้งานสิ้นสุดสภาพการเป็นพนักงาน และ (2) ไม่มีความจำเป็นต้องใช้งาน<br>2. แนวทางการบริหารจัดการสิทธิการเข้าถึงข้อมูลและระบบ IT ควรครอบคลุมอย่างน้อย ดังนี้</td></tr>
</table>

| ข้อกำหนด | แนวปฏิบัติ |
|---|---|
| สำนักงานสอบบัญชีต้องกำหนดให้มีการควบคุมอื่นทดแทนเพื่อตอบสนองต่อความเสี่ยงที่อาจจะเกิดขึ้นจากบัญชีผู้ใช้งานและสิทธิการเข้าถึงที่ไม่เหมาะสม | (1) หน่วยงานหรือบุคลากรที่รับผิดชอบในการบริหารจัดการสิทธิการเข้าถึงข้อมูลและระบบ IT<br>(2) ขั้นตอนการขออนุมัติสิทธิในการเข้าถึงข้อมูลและระบบ IT จากผู้มีอำนาจ เช่น เจ้าของระบบ หรือเจ้าของข้อมูล เป็นต้น<br>(3) ขั้นตอนการปรับปรุงสิทธิของผู้ใช้งานเมื่อมีการเปลี่ยนแปลงหน้าที่ความรับผิดชอบหรือตำแหน่งงาน<br>(4) ขั้นตอนการเพิกถอนสิทธิของผู้ใช้งาน โดยเพิกถอนสิทธิทันทีเมื่อผู้ใช้งานสิ้นสุดสภาพการเป็นพนักงาน และเมื่อไม่มีความจำเป็นต้องใช้งาน<br>(5) การแบ่งแยกบทบาทหน้าที่ของบุคคลที่เกี่ยวข้องในการจัดสรรสิทธิ เช่น ผู้ร้องขอ (access request) ผู้มีอำนาจอนุมัติ (access authorization) และผู้ดูแลสิทธิการเข้าถึง (access administration) เป็นต้น เพื่อให้สอดคล้องตามหลักการถ่วงดุล (check and balance) ที่ดี<br>(6) กำหนดสิทธิของผู้ใช้งานโดยคำนึงถึงความจำเป็นต้องรู้ (need-to-know) ความจำเป็นต้องใช้งาน (need-to-use) และหลักการแบ่งแยกหน้าที่ความรับผิดชอบ (segregation of duties)<br>(7) จัดทำตารางควบคุมการให้สิทธิ (authorization matrix) ของผู้ใช้งานที่สอดคล้องกับตำแหน่งหน้าที่และความรับผิดชอบเพื่อใช้เป็นแนวทางการกำหนดสิทธิอย่างถูกต้องเหมาะสม<br>(8) ทบทวนสิทธิการเข้าถึงอย่างสม่ำเสมอ อย่างน้อยปีละ 1 ครั้ง โดยกำหนดรอบระยะเวลาในการทบทวนสิทธิให้สอดคล้องกับความเสี่ยงและความสำคัญของสิทธิ |
| 5.2 จัดให้มีกระบวนการยืนยันตัวตนผู้ใช้งาน (authentication) ที่เหมาะสมกับความเสี่ยง<br>ทั้งนี้ หากสำนักงานสอบบัญชีไม่สามารถกำหนดกระบวนการยืนยันตัวตนผู้ใช้งาน (authentication) ที่เหมาะสมตามลักษณะขั้นต่ำของแนวปฏิบัตินี้ทุกข้อได้ สำนักงานสอบบัญชีต้องกำหนดให้มีการควบคุมอื่นทดแทนเพื่อตอบสนองต่อความเสี่ยงที่อาจจะเกิดขึ้นจากการเข้าถึงระบบโดยไม่ได้รับอนุญาต | 1. สำนักงานสอบบัญชีควรจัดให้มีกระบวนการยืนยันตัวตนผู้ใช้งาน (authentication) ที่มีประสิทธิภาพเหมาะสมกับความเสี่ยงของการเข้าถึงระบบโดยไม่ได้รับอนุญาต โดยครอบคลุมอย่างน้อย ดังนี้<br>(1) กำหนดวิธีการยืนยันตัวตนผู้ใช้งานที่เหมาะสมกับความเสี่ยง<br>(2) กรณีที่มีการสร้างรหัสผ่านครั้งแรกสำหรับผู้ใช้งาน ให้มีการจัดส่งรหัสผ่านให้แก่ผู้ใช้งานด้วยวิธีการที่รัดกุมและปลอดภัย และให้ผู้ใช้งานเปลี่ยนแปลงรหัสผ่านทันทีที่ได้รับรหัสดังกล่าว<br>(3) กำหนดให้ผู้ใช้งานตั้งรหัสผ่านที่ซับซ้อนและยากต่อการคาดเดา โดยมีความยาวขั้นต่ำ 8 อักขระ (8 characters) และประกอบด้วยตัวเลขและตัวอักษร ทั้งนี้ สำนักงานสอบบัญชีอาจพิจารณาเพิ่มความซับซ้อนโดยกำหนดให้รหัสผ่านประกอบด้วยตัวเลข ตัวอักษรพิมพ์ใหญ่ ตัวอักษรพิมพ์เล็ก และอักขระพิเศษ (เช่น “#”)<br>(4) กำหนดจำนวนครั้งที่ยอมให้ผู้ใช้งานใส่รหัสผ่านผิดพลาดติดต่อกัน ก่อนระงับการเข้าสู่ระบบชั่วคราวหรือวิธีการอื่น ๆ ที่เทียบเท่า เพื่อป้องกันการเข้าใช้งานโดยวิธีเดาสุ่ม (brute force) ทั้งนี้ ในทางปฏิบัติไม่ควรยอมให้ผู้ใช้งานยืนยันตัวตนผิดพลาดติดต่อกันเกิน 10 ครั้ง |

| ข้อกำหนด | แนวปฏิบัติ |
|---|---|
| | (5) กำหนดให้การเปลี่ยนรหัสผ่านใหม่ไม่ซ้ำกับรหัสที่ใช้งานอย่างน้อย 4 ครั้งล่าสุด หรือไม่ซ้ำกับรหัสผ่านที่ใช้งานในช่วง 1 ปีที่ผ่านมา<br>(6) กำหนดการตั้งค่าปกติ (default) ให้ไม่แสดงรหัสผ่านบนหน้าจอ ระหว่างที่ผู้ใช้งานใส่รหัสผ่าน<br>(7) มีวิธีจัดเก็บข้อมูลรหัสผ่านที่ปลอดภัย เพื่อป้องกันการล่วงรู้หรือแก้ไขเปลี่ยนแปลง รวมทั้งไม่จัดเก็บข้อมูลรหัสผ่านใน folder เดียวกันกับ folder ที่จัดเก็บข้อมูลของแอปพลิเคชัน<br>(8) กำหนดให้ผู้ใช้งานรับผิดชอบการใช้งานบัญชีผู้ใช้งาน (user ID) และการรักษาความปลอดภัยสิ่งที่ใช้ยืนยันตัวตน (authenticator) เช่น รหัสผ่าน รหัสที่ใช้ครั้งเดียว (one-time password) เป็นต้น รวมทั้งข้อมูลส่วนบุคคลที่อาจนำมาใช้เพื่อขอเปลี่ยนแปลงข้อมูลบัญชีผู้ใช้งาน เพื่อป้องกันการใช้งานจากผู้ไม่หวังดี |
| 5.3 กำหนดมาตรการควบคุม จำกัด และติดตามการใช้งานบัญชี privileged user (privileged user management) ดังนี้ (ถ้ามี)<br>5.3.1 มี Multi-Factor Authentication (“MFA”) หรือ วิธีการยืนยันตัวตนเพิ่มเติมหลังจากทำการยืนยันตัวตนโดยการใช้รหัสผ่าน เพื่ออนุญาตเข้าใช้งานระบบเทคโนโลยีสารสนเทศ เมื่อเข้าใช้งานและเปลี่ยนรหัสผ่าน สำหรับระบบปฏิบัติการและระบบฐานข้อมูลที่เกี่ยวข้องกับระบบ IT ที่มีนัยสำคัญ<br>5.3.2 กรณีสำนักงานสอบบัญชีมีข้อจำกัดสำหรับ MFA สามารถใช้วิธีการอื่นใดที่เทียบเท่าทดแทน และจัดให้มีการประเมินความเสี่ยงและพิจารณาแนวทางควบคุมความเสี่ยงก่อนดำเนินการเพื่อขออนุมัติยกเว้น (exception) | หากสำนักงานสอบบัญชีมีการใช้งานบัญชี privileged user ต้องมีการดำเนินการตามข้อ 5.3.1 ถึง 5.3.3 เป็นอย่างน้อย |
| 5.3.3 มีการควบคุมและติดตามตรวจสอบการใช้งานบัญชี privileged user | 1. สำนักงานสอบบัญชีควรจัดให้มีการควบคุมและติดตามการใช้บัญชี privileged user ดังนี้<br>(1) ควบคุมดูแลการให้สิทธิโดยจำกัดตามบทบาทหน้าที่ และความจำเป็นในการใช้งาน |

| ข้อกำหนด | แนวปฏิบัติ |
|---|---|
| | (2) จำกัดจำนวนบัญชี privileged user ให้มีจำนวนน้อยที่สุดหรือเท่าที่จำเป็น<br>(3) มีกระบวนการขอใช้งานบัญชี privileged user และการอนุมัติโดยผู้มีอำนาจ<br>(4) ทบทวนบัญชีผู้ใช้งาน privileged user อย่างสม่ำเสมออย่างน้อยปีละ 1 ครั้ง<br>(5) กำหนดนโยบายหรือมาตรการยืนยันตัวตนของบัญชี privileged user ที่เข้มงวดกว่าบัญชีผู้ใช้งานทั่วไป<br>(6) จัดเก็บบันทึกการยืนยันตัวตนและการเข้าถึง (authentication log และ access log) และการดำเนินงาน (activity log) ของบัญชี privileged user อย่างเหมาะสม<br>(7) สอบทานบันทึกการยืนยันตัวตนและการเข้าถึง (authentication log และ access log) และการดำเนินงาน (activity log) ของบัญชี privileged user หลังเสร็จสิ้นการใช้งาน หรือสอบทานสม่ำเสมอตามรอบระยะเวลาที่เหมาะสมกับความเสี่ยง หรือ อย่างน้อยปีละ 1 ครั้ง เพื่อให้มั่นใจได้ว่าการใช้งานสิทธิเป็นไปตามขอบเขตและหน้าที่ที่ได้รับมอบหมาย |
| **2.6 การควบคุมการเข้ารหัส (cryptographic control)** | |
| **ส่วนที่ 6 การควบคุมการเข้ารหัส (cryptographic control)**<br>หากสำนักงานสอบบัญชีมีการเข้ารหัสข้อมูล สำนักงานสอบบัญชีต้องจัดให้มีการควบคุมการเข้ารหัสที่เชื่อถือได้และเป็นไปตามมาตรฐานสากลโดยกำหนดวิธีการเข้ารหัสข้อมูล (encryption) และการบริหารจัดการกุญแจเข้ารหัส (key management) อย่างปลอดภัยเพื่อให้มั่นใจได้ว่า การธำรงไว้ซึ่งความลับ (confidentiality) ความถูกต้องครบถ้วน (integrity) และความถูกต้องแท้จริง (authenticity) ของข้อมูลมีความเหมาะสมและมีประสิทธิภาพ ดังนี้ | หากสำนักงานสอบบัญชีมีข้อจำกัดในการดำเนินการตามส่วนที่ 6 การควบคุมการเข้ารหัส สำนักงานสอบบัญชีต้องกำหนดวิธีการควบคุมอื่นทดแทนเพื่อสกัดกั้นการเข้าถึงข้อมูลโดยบุคคลที่ไม่ได้รับอนุญาตเพื่อให้มั่นใจได้ว่า การธำรงไว้ซึ่งความลับ (confidentiality) ความถูกต้องครบถ้วน (integrity) และความถูกต้องแท้จริง (authenticity) ของข้อมูลมีความเหมาะสมกับระดับชั้นความลับและเป็นไปอย่างมีประสิทธิภาพ เช่น ล็อคไฟล์เอกสารชั้นความลับเพื่อป้องกันบุคคลที่ไม่ได้รับอนุญาตเปิดก่อนจัดส่งทาง email และส่งรหัสผ่านของไฟล์ดังกล่าวผ่านช่องทางอื่นที่ไม่ใช่ทาง email เป็นต้น |
| 6.1 กำหนดวิธีการเข้ารหัสที่ปลอดภัย | ในการกำหนดวิธีการเข้ารหัสที่ปลอดภัย สำนักงานสอบบัญชีควรดำเนินการอย่างน้อย ดังนี้<br>1. กำหนดความรับผิดชอบของหน่วยงานหรือบุคลากรที่เกี่ยวข้อง<br>2. กำหนดมาตรฐานวิธีการเข้ารหัสข้อมูล (cryptographic algorithm) ให้เป็นไปตามมาตรฐานสากล และมีความมั่นคงปลอดภัยเหมาะสมกับระดับความสำคัญของข้อมูล |

| ข้อกำหนด | แนวปฏิบัติ |
|---|---|
| | 3. การกำหนดรอบระยะเวลาในการทบทวนมาตรฐานวิธีการเข้ารหัสข้อมูล เพื่อให้มั่นใจว่าวิธีการเข้ารหัสข้อมูลที่ใช้งานอยู่ยังมีความมั่นคงเพียงพอในการรักษาความปลอดภัยของข้อมูล |
| 6.2 กำหนดการบริหารจัดการกุญแจเข้ารหัส โดยจัดให้มีมาตรการการควบคุมตั้งแต่การสร้างและติดตั้งกุญแจเข้ารหัส การจัดเก็บและสำรองกุญแจเข้ารหัส ไปจนถึงการเพิกถอนหรือทำลายกุญแจเข้ารหัส | 1. การสร้างและติดตั้งกุญแจเข้ารหัส สำนักงานสอบบัญชีควรดำเนินการอย่างน้อย ดังนี้<br>(1) ควบคุมสภาพแวดล้อมและกระบวนการในการสร้างกุญแจเข้ารหัสที่รัดกุมปลอดภัย เช่น เลือกใช้ผู้ให้บริการออกใบรับรอง (certification authority) ที่น่าเชื่อถือ และมีการทำลายข้อมูลที่อาจหลงเหลือภายหลังการสร้างกุญแจเข้ารหัสแล้วเสร็จ เพื่อป้องกันเข้าถึงหรือกู้คืนกุญแจเข้ารหัสข้อมูลโดยไม่ได้รับอนุญาต เป็นต้น<br>(2) กำหนดสิทธิการเข้าถึงกุญแจเข้ารหัสให้สามารถเข้าถึงได้โดยผู้ที่ได้รับอนุญาตเท่านั้น<br>(3) กำหนดความยาวของกุญแจเข้ารหัสที่เพียงพอในการป้องกันการถูกถอดรหัส (decrypt) โดยผู้ไม่หวังดี เช่น การโจมตีแบบ brute force เป็นต้น<br>(4) แลกเปลี่ยนกุญแจเข้ารหัส (key exchange) ผ่านกระบวนการและช่องทางที่ปลอดภัย<br>2. การจัดเก็บและการสำรองกุญแจเข้ารหัส สำนักงานสอบบัญชีควรดำเนินการอย่างน้อย ดังนี้<br>(1) มีการรักษาความปลอดภัยในการจัดเก็บกุญแจเข้ารหัสทั้งด้าน physical และ logical เช่น การใช้อุปกรณ์ Hardware Security Module (HSM) หรืออุปกรณ์ที่ทำหน้าที่ในลักษณะเดียวกัน เป็นต้น<br>(2) มีการสำรองข้อมูลกุญแจเข้ารหัส โดยวิธีการเก็บรักษาข้อมูลกุญแจเข้ารหัสชุดสำรองต้องมีการรักษาความปลอดภัยในระดับเดียวกับกุญแจเข้ารหัสชุดหลัก<br>3. การเพิกถอนหรือทำลายกุญแจเข้ารหัส สำนักงานสอบบัญชีควรดำเนินการอย่างน้อย ดังนี้<br>(1) กำหนดเกณฑ์และแนวทางในการเปลี่ยนและเพิกถอนกุญแจเข้ารหัส เช่น กรณีกุญแจเข้ารหัสหมดอายุการใช้งาน หรือไม่ปลอดภัย เป็นต้น<br>(2) กำหนดกระบวนการทำลายกุญแจ เพื่อให้มั่นใจว่าจะไม่สามารถนำกุญแจนั้นมาใช้งานได้อีก<br>4. สำนักงานสอบบัญชีควรจัดเก็บข้อมูลบันทึกเหตุการณ์กิจกรรมสำคัญที่เกี่ยวกับกุญแจเข้ารหัส เช่น การสร้างกุญแจ การสำรองกุญแจ การเข้าถึงหรือใช้งานกุญแจ และการเพิกถอนกุญแจ เป็นต้น |
| 6.3 กำหนดมาตรการการควบคุมกุญแจเข้ารหัสที่ให้บริการโดยบุคคลภายนอก ซึ่งต้องตรวจสอบเพื่อให้มั่นใจได้ว่ากุญแจการเข้ารหัสที่สร้างขึ้นไม่มีการนำมาใช้ร่วมกับบุคคลอื่น | 1. กรณีที่สำนักงานสอบบัญชีไม่สามารถสร้างกุญแจเข้ารหัสด้วยตนเองได้ หรือมีความจำเป็นต้องใช้กุญแจเข้ารหัสที่ให้บริการโดยบุคคลภายนอก สำนักงานสอบบัญชีควรดำเนินการเพื่อให้มั่นใจได้ว่ากุญแจเข้ารหัสที่ให้บริการโดยบุคคลภายนอกไม่มีการนำมาใช้งานร่วมกับผู้ใช้บริการรายอื่นและมีความมั่นคงปลอดภัย โดยพิจารณาเงื่อนไขหรือรายละเอียดของการให้บริการ ดังนี้<br>(1) ประเภทของกุญแจเข้ารหัส |

| ข้อกำหนด | แนวปฏิบัติ |
|---|---|
| | (2) รายละเอียดของระบบ และกระบวนการบริหารจัดการกุญแจเข้ารหัส<br>(3) ข้อแนะนำการใช้งานและการควบคุมการเข้ารหัสข้อมูล |
| 6.4 กำหนดกระบวนการรองรับกรณีเกิดการรั่วไหลของกุญแจเข้ารหัส | 1. สำนักงานสอบบัญชีควรกำหนดกิจกรรมที่ต้องดำเนินการเมื่อเกิดการรั่วไหลของกุญแจเข้ารหัส เช่น การติดต่อหน่วยงานและผู้ที่เกี่ยวข้องกับชุดข้อมูลที่ใช้กุญแจเข้ารหัสชุดดังกล่าว การตรวจสอบชุดข้อมูลที่มีความเสี่ยงในการรั่วไหล การเปลี่ยนหรือเพิกถอนกุญแจการเข้ารหัสข้อมูล เป็นต้น |
| **2.7 การรักษาความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อม (physical and environmental security)** | |
| **ส่วนที่ 7 การรักษาความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อม (physical and environmental security)**<br>สำนักงานสอบบัญชีต้องจัดให้มีการรักษาความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อมของทรัพย์สินด้าน IT พร้อมทั้งมีระบบการป้องกัน และกระบวนการบำรุงรักษาฮาร์ดแวร์และระบบสาธารณูปโภค (facilities) ที่เกี่ยวข้องกับ IT เพื่อให้สามารถป้องกันความเสียหายต่อทรัพย์สินด้าน IT ซึ่งรวมถึงอุปกรณ์ที่จัดเก็บอยู่ในศูนย์คอมพิวเตอร์หลัก ศูนย์คอมพิวเตอร์สำรอง หรือ ศูนย์คอมพิวเตอร์จากบุคคลภายนอก (co-location) (ถ้ามี)<br>อย่างไรก็ดี หากศูนย์คอมพิวเตอร์ และพื้นที่ที่เกี่ยวข้องกับระบบ IT ที่มีนัยสำคัญของสำนักงานสอบบัญชีอยู่ในการควบคุมของบุคคลภายนอก ทำให้สำนักงานสอบบัญชีมีข้อจำกัดในการปฏิบัติตามแนวปฏิบัตินี้ สำนักงานสอบบัญชีต้องประเมินความสามารถในการรักษาความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อมของทรัพย์สินด้าน IT ของบุคคลภายนอก | 1. สำนักงานสอบบัญชีควรออกแบบศูนย์คอมพิวเตอร์ และพื้นที่ที่เกี่ยวข้องกับระบบ IT ที่มีนัยสำคัญ โดยคำนึงถึงความเสี่ยงจากภัยธรรมชาติและภัยคุกคามจากมนุษย์ เช่น มีกำแพงหรือรั้วที่มั่นคง และมีระยะห่างของศูนย์คอมพิวเตอร์สำรองและศูนย์คอมพิวเตอร์หลักที่เพียงพอ เป็นต้น<br>2. สำนักงานสอบบัญชีควรมีการบริหารจัดการสิทธิการเข้าถึงศูนย์คอมพิวเตอร์ และพื้นที่ที่เกี่ยวข้องกับระบบ IT ที่มีนัยสำคัญ โดยครอบคลุมการดำเนินการอย่างน้อย ดังนี้<br>(1) ให้สิทธิการเข้าถึงตามหลักความจำเป็น<br>(2) อนุมัติสิทธิการเข้าถึงโดยผู้มีอำนาจ<br>(3) ปรับปรุง/ยกเลิกสิทธิการเข้าถึง ทันทีที่พนักงานลาออกหรือเปลี่ยนหน้าที่ความรับผิดชอบ<br>(4) ทบทวนสิทธิการเข้าถึงอย่างสม่ำเสมออย่างน้อยปีละ 1 ครั้ง<br>3. สำนักงานสอบบัญชีควรจัดให้มีวิธีการยืนยันตัวตนผู้เข้า-ออกศูนย์คอมพิวเตอร์ และพื้นที่ที่เกี่ยวข้องกับระบบ IT ที่มีนัยสำคัญ เช่น การใช้ access card door หรือ ลงชื่อในใบลงชื่อเข้า-ออก เป็นต้น<br>ทั้งนี้ สำหรับพื้นที่ที่มีความเสี่ยงสูง สำนักงานสอบบัญชีอาจพิจารณาใช้วิธีการยันตัวตนแบบ MFA เช่น ใช้ access card door ร่วมกับรหัสผ่านส่วนตัว (PIN) เป็นต้น<br>4. สำนักงานสอบบัญชีควรมีมาตรการควบคุมการเข้า-ออกศูนย์คอมพิวเตอร์ และพื้นที่ที่เกี่ยวข้องกับระบบ IT ที่มีนัยสำคัญ สำหรับพนักงานที่ไม่ได้มีหน้าที่ปฏิบัติงานประจำหรือผู้ที่เข้าถึงแบบชั่วคราว โดยจัดให้มีการอนุมัติจากผู้มีอำนาจ การบันทึกเหตุการณ์เข้า-ออก และมีการติดตามและควบคุม (escort) อย่างใกล้ชิด ตลอดระยะเวลาปฏิบัติงานในพื้นที่ดังกล่าว<br>5. สำนักงานสอบบัญชีควรจัดให้มีระบบรักษาความมั่นคงปลอดภัยให้กับศูนย์คอมพิวเตอร์ เช่น ระบบกล้องวงจรปิด ระบบแจ้งเตือนและระงับอัคคีภัย ระบบควบคุมแรงดันและกระแสไฟฟ้า ระบบสำรองไฟฟ้า (uninterrupted power supply) และระบบควบคุมอุณหภูมิและความชื้น เป็นต้น พร้อมทั้งมีการบำรุงรักษาอย่างสม่ำเสมอ |

| ข้อกำหนด | แนวปฏิบัติ |
|---|---|
| และกำหนดแนวทางการกำกับดูแลตามระดับความเสี่ยงอย่างเหมาะสม | 6. สำนักงานสอบบัญชีควรจัดให้มีมาตรการรองรับการทำงานผิดพลาดของระบบสาธารณูปโภคของศูนย์คอมพิวเตอร์ เช่น ระบบไฟฟ้า ระบบโทรคมนาคมและระบบปรับอากาศ เป็นต้น<br>7. สำนักงานสอบบัญชีควรจัดเก็บอุปกรณ์คอมพิวเตอร์ที่สำคัญ เช่น เครื่องแม่ข่าย และอุปกรณ์เครือข่าย เป็นต้น ไว้ในพื้นที่ที่มีการควบคุมอย่างปลอดภัย<br>8. สำนักงานสอบบัญชีควรจัดให้มีมาตรการป้องกันสายเคเบิลและสายไฟของศูนย์คอมพิวเตอร์จากการขัดขวางการทำงาน หรือการทำให้เสียหาย และบำรุงรักษาอย่างสม่ำเสมอ<br>9. สำนักงานสอบบัญชีควรจัดให้มีการดูแลและบำรุงรักษาทรัพย์สินด้าน IT ประเภทฮาร์ดแวร์อย่างถูกวิธี เพื่อให้อยู่ในสภาพครบถ้วนสมบูรณ์และพร้อมใช้งาน<br>10. สำนักงานสอบบัญชีควรควบคุมมิให้มีการนำทรัพย์สินด้าน IT ประเภทฮาร์ดแวร์ออกนอกพื้นที่โดยมิได้รับอนุญาต<br>11. ก่อนการยกเลิกการใช้งานหรือจำหน่ายทรัพย์สินด้าน IT ประเภทฮาร์ดแวร์ เช่น hard disk, switch, firewall และ router เป็นต้น สำนักงานสอบบัญชีควรจัดเก็บทรัพย์สินในพื้นที่ปลอดภัย และตรวจสอบให้มั่นใจว่าได้มีการลบ ย้าย ทำลายข้อมูลสำคัญและข้อมูลการปรับแต่ง (configuration) หรือปรับค่าดังกล่าวกลับไปสู่ค่าตั้งต้น (factory reset) ด้วยวิธีการที่ไม่สามารถกู้คืนได้อีก |
| **2.8 การรักษาความมั่นคงปลอดภัยในการปฏิบัติงานด้าน IT (IT operations security)** | |
| **ส่วนที่ 8 การรักษาความมั่นคงปลอดภัยในการปฏิบัติงานด้าน IT (IT operations security)**<br>สำนักงานสอบบัญชีต้องมีมาตรการรักษาความมั่นคงปลอดภัยในการปฏิบัติงานด้าน IT เพื่อให้การปฏิบัติงานเกี่ยวกับการประมวลผลข้อมูลมีความถูกต้องและมั่นคงปลอดภัย โดยต้องครอบคลุมการบริหารจัดการอย่างน้อยในเรื่องดังนี้ | |
| **2.8.1 การบริหารจัดการการตั้งค่าระบบ (system configuration management)** | |
| 8.1 การบริหารจัดการการตั้งค่าระบบ (system configuration management) โดยมีกระบวนการในการควบคุมการตั้งค่าระบบ และสอบทานการตั้งค่าระบบอย่างสม่ำเสมอ เพื่อให้การตั้งค่าระบบเป็นไปอย่าง | 1. สำนักงานสอบบัญชีควรกำหนดมาตรฐานการตั้งค่าด้านความมั่นคงปลอดภัย (security configuration standard) หรือ security based line อย่างเป็นลายลักษณ์อักษร เพื่อใช้ในการตั้งค่าระบบปฏิบัติการ ระบบฐานข้อมูล และอุปกรณ์เครือข่าย โดยคำนึงถึงเรื่องดังนี้<br>(1) การลบบัญชีผู้ใช้งานตั้งต้น (default user) หรือการเปลี่ยนแปลงรหัสผ่านตั้งต้น (default password) |

| ข้อกำหนด | แนวปฏิบัติ |
|---|---|
| ถูกต้อง และปลอดภัย | (2) การใช้วิธีการยืนยันตัวตนที่มีความรัดกุมปลอดภัย<br>(3) การกำหนดบริการ แอปพลิเคชัน และพอร์ตการเชื่อมต่อเท่าที่จำเป็น<br>(4) การจัดเก็บข้อมูลบันทึกเหตุการณ์ (log)<br>(5) การปรับปรุงเวอร์ชันของซอฟต์แวร์หรือ firmware ให้เป็นปัจจุบัน<br>2. สำนักงานสอบบัญชีควรทบทวนและปรับปรุงมาตรฐานการตั้งค่าด้านความมั่นคงปลอดภัย (security configuration standard) หรือ security based line ให้เป็นปัจจุบันอย่างสม่ำเสมอ<br>3. สำนักงานสอบบัญชีควรตั้งค่าด้านความมั่นคงปลอดภัยของระบบปฏิบัติการ ระบบฐานข้อมูล และอุปกรณ์เครือข่ายตามมาตรฐานที่สำนักงานสอบบัญชีกำหนดไว้ ก่อนการนำไปใช้งาน<br>4. สำนักงานสอบบัญชีควรสอบทานการตั้งค่าด้านความมั่นคงปลอดภัยของระบบปฏิบัติการ ระบบฐานข้อมูล และอุปกรณ์เครือข่ายอย่างสม่ำเสมอ และทุกครั้งที่มีการเปลี่ยนแปลงระบบและอุปกรณ์ดังกล่าวอย่างมีนัยสำคัญ เพื่อให้สอดคล้องกับมาตรฐานที่สำนักงานสอบบัญชีกำหนดไว้ |
| **2.8.2 การบริหารจัดการการเปลี่ยนแปลง (change management)** | |
| 8.2 การบริหารจัดการการเปลี่ยนแปลง (change management) อย่างรัดกุมเพียงพอเพื่อให้การเปลี่ยนแปลงเป็นไปตามวัตถุประสงค์ที่กำหนดไว้อย่างถูกต้องครบถ้วน และป้องกันการเปลี่ยนแปลงโดยที่ไม่ได้รับอนุญาต | 1. สำนักงานสอบบัญชีควรกำหนดกระบวนการบริหารจัดการการเปลี่ยนแปลงอย่างเป็นลายลักษณ์อักษรเพื่อควบคุมการเปลี่ยนแปลงโครงสร้างพื้นฐานด้าน IT ระบบ IT และขั้นตอนการปฏิบัติงานที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัย<br>2. สำนักงานสอบบัญชีควรกำหนดบุคคลหรือคณะกรรมการบริหารของสำนักงานสอบบัญชีที่ทำหน้าที่อนุมัติการเปลี่ยนแปลง<br>3. สำนักงานสอบบัญชีควรแบ่งแยกหน้าที่ (segregation of duties) ผู้ที่เกี่ยวข้องในกระบวนการการเปลี่ยนแปลง เพื่อไม่ให้บุคคลใดบุคคลหนึ่งสามารถปฏิบัติงานได้ตั้งแต่เริ่มต้นจนจบกระบวนการการเปลี่ยนแปลง เช่น ผู้มีสิทธิร้องขอ ผู้ที่มีอำนาจในการอนุมัติการเปลี่ยนแปลง ผู้ที่สามารถดำเนินการเปลี่ยนแปลงระบบ เป็นต้น<br>4. สำนักงานสอบบัญชีควรจัดให้มีคำขอการเปลี่ยนแปลง (change request) และการอนุมัติการเปลี่ยนแปลง เป็นลายลักษณ์อักษรเพื่อเป็นหลักฐานแสดงให้เห็นว่าการเปลี่ยนแปลงได้ผ่านการพิจารณาจากเจ้าของข้อมูล เจ้าของระบบ หรือผู้มีอำนาจตามสิทธิที่กำหนดไว้ โดยคำขอการเปลี่ยนแปลงควรระบุเหตุผลความจำเป็นและผลกระทบที่อาจเกิดขึ้นจากการเปลี่ยนแปลง<br>5. สำนักงานสอบบัญชีควรจัดให้มีระบบหรือทะเบียนในการจัดเก็บคำขอเปลี่ยนแปลงและเอกสารรายละเอียดที่เกี่ยวข้อง เพื่อใช้ควบคุมการปฏิบัติงานตั้งแต่ต้นจนจบกระบวนการ และสามารถใช้ในการติดตามและสอบทานการปฏิบัติงาน<br>6. กรณีที่การเปลี่ยนแปลงมีผลกระทบต่อการปฏิบัติงาน สำนักงานสอบบัญชีควรสื่อสารให้ผู้เกี่ยวข้องรับทราบการเปลี่ยนแปลงเพื่อให้สามารถปฏิบัติงานได้อย่างถูกต้อง |

| ข้อกำหนด | แนวปฏิบัติ |
|---|---|
| | 7. สำนักงานสอบบัญชีควรจัดให้มีแผนการถอยกลับสู่สภาพเดิม (fallback procedure) หากเกิดข้อผิดพลาดจากการเปลี่ยนแปลง เช่น การจัดเก็บเวอร์ชันของระบบก่อนการเปลี่ยนแปลงไว้ เป็นต้น |
| **2.8.3 การบริหารจัดการขีดความสามารถของระบบ IT (capacity management)** | |
| 8.3 การบริหารจัดการขีดความสามารถของระบบ IT (capacity management) โดยจัดให้มีมาตรฐานและวิธีปฏิบัติเรื่องการจัดการขีดความสามารถ การติดตามประสิทธิภาพการทำงานของระบบ และการประเมินแนวโน้มการใช้ทรัพยากรด้าน IT เพื่อให้สามารถรองรับการดำเนินธุรกิจในปัจจุบัน และสามารถวางแผนการจัดสรรทรัพยากรให้รองรับการใช้งานในอนาคตได้อย่างมีประสิทธิภาพ | 1. สำนักงานสอบบัญชีควรกำหนดมาตรฐานและระเบียบวิธีปฏิบัติในการบริหารจัดการขีดความสามารถของระบบ เพื่อประเมินและติดตามดูแลความเพียงพอของโครงสร้างพื้นฐานด้าน IT ที่ครอบคลุมถึงระบบคอมพิวเตอร์ ระบบฐานข้อมูล ระบบเครือข่ายสื่อสาร และระบบสาธารณูปโภคที่เกี่ยวข้องกับงานด้าน IT<br>2. สำนักงานสอบบัญชีควรจัดทำรายงานความเพียงพอของทรัพยากรด้าน IT นำเสนอต่อหัวหน้าสำนักงานสอบบัญชี หรือคณะกรรมการบริหารของสำนักงานสอบบัญชีรับทราบอย่างสม่ำเสมอ เพื่อให้มีการกำกับดูแลความพร้อมใช้และความเพียงพอของระบบในการรองรับการให้บริการทางธุรกิจได้อย่างต่อเนื่อง และสามารถพิจารณาแนวทางลดความเสี่ยงได้อย่างทันการณ์ |
| **2.8.4 การรักษาความมั่นคงปลอดภัยของเครื่องแม่ข่าย (server) และอุปกรณ์ที่ใช้ปฏิบัติงาน (endpoint)** | |
| 8.4 การรักษาความมั่นคงปลอดภัยของเครื่องแม่ข่าย (server) และอุปกรณ์ที่ใช้ปฏิบัติงาน (endpoint) เพื่อไม่ให้ถูกใช้เป็นช่องทางที่ทำให้ข้อมูลสำคัญรั่วไหล หรือมีการเข้าใช้งานระบบ IT โดยไม่ได้รับอนุญาต | 1. สำนักงานสอบบัญชีควรกำหนดมาตรการรักษาความปลอดภัยของเครื่องแม่ข่าย และอุปกรณ์ที่ใช้ในการปฏิบัติงาน เพื่อให้สามารถป้องกันและตรวจจับโปรแกรมไม่ประสงค์ดี (malware) และภัยคุกคามทางไซเบอร์ โดยครอบคลุมการดำเนินการอย่างน้อย ดังนี้<br>(1) มีกระบวนการหรือเครื่องมือในการควบคุมและติดตามไม่ให้มีการติดตั้งซอฟต์แวร์ที่ไม่ได้รับอนุญาต<br>(2) ติดตั้งเครื่องมือในการป้องกันและตรวจจับโปรแกรมไม่ประสงค์ดี เช่น anti-virus, anti-malware และ intrusion prevention system เป็นต้น โดยปรับปรุง (update) เครื่องมือที่ใช้งานให้เป็นปัจจุบันอย่างสม่ำเสมอ เพื่อให้เท่าทันในการป้องกันภัยคุกคามใหม่ ๆ<br>(3) ควบคุมการใช้งานหรือการเชื่อมต่อสื่อบันทึกข้อมูลพกพา (removable media) เช่น กำหนดแนวทางการควบคุมการใช้งาน universal serial bus (USB) หรือ external hard disk เป็นต้น<br>2. สำนักงานสอบบัญชีควรจัดให้มีการควบคุมป้องกันทรัพย์สินด้าน IT ประเภทฮาร์ดแวร์ระหว่างที่ไม่มีผู้ใช้งาน (unattended user equipment) ให้มีความปลอดภัย โดยครอบคลุมการดำเนินการอย่างน้อย ดังนี้<br>(1) ควบคุมเอกสาร อุปกรณ์ที่ใช้ปฏิบัติงาน หรือสื่อบันทึกข้อมูลต่าง ๆ ที่มีการจัดเก็บข้อมูลสำคัญหรือข้อมูลลับ ไม่ให้วางทิ้งไว้บนโต๊ะทำงานหรือสถานที่ไม่ปลอดภัยในขณะที่ไม่ได้ใช้งาน (clear desk)<br>(2) ควบคุมหน้าจอคอมพิวเตอร์ไม่ให้มีข้อมูลสำคัญปรากฏในขณะที่ไม่ได้ใช้งาน (clear screen) เช่น การตัดออกจากระบบ |

| ข้อกำหนด | แนวปฏิบัติ |
|---|---|
| | (session time out) หรือการล็อคหน้าจอ (lock screen) อัตโนมัติ เมื่อไม่มีการใช้งานถึงระยะเวลาที่กำหนด เป็นต้น |
| **2.8.5 การรักษาความปลอดภัยสำหรับการปฏิบัติงานจากเครือข่ายภายนอก (teleworking) การใช้งานอุปกรณ์เคลื่อนที่ (mobile device) และการใช้งานอุปกรณ์ส่วนตัว (bring your own device : BYOD)** | |
| 8.5 การกำหนดนโยบายและมาตรการรักษาความปลอดภัยสำหรับการปฏิบัติงานจากเครือข่ายภายนอก (teleworking) การใช้งานอุปกรณ์เคลื่อนที่ (mobile device) และรวมถึงการใช้งานอุปกรณ์ส่วนตัว (bring your own device : BYOD) โดยพิจารณาความเสี่ยงที่เกี่ยวข้อง และจัดให้มีมาตรการควบคุมอย่างเหมาะสม<br>ทั้งนี้ หากสำนักงานสอบบัญชีมีข้อจำกัดในการดำเนินการควบคุมและการตรวจสอบความมั่นคงปลอดภัยสำหรับการปฏิบัติงานจากเครือข่ายภายนอก (teleworking) การใช้งานอุปกรณ์เคลื่อนที่ (mobile device) และรวมถึงการใช้งานอุปกรณ์ส่วนตัว (bring your own device : BYOD) สำนักงานสอบบัญชีต้องกำหนดมาตรการควบคุมทดแทน เพื่อป้องกันการถูกโจมตีทางไซเบอร์จากการใช้งานดังกล่าวอันเนื่องมาจากการรักษาความมั่นคงปลอดภัยที่ไม่เพียงพอ เช่น กำหนดสิทธิการเข้าถึงให้อุปกรณ์ หรือการใช้งานผ่านเครือข่ายดังกล่าว ให้เข้าถึงได้เฉพาะข้อมูลทั่วไป หรือ ข้อมูลที่มีความเสี่ยงต่ำเท่านั้น เป็นต้น | 1. ในกรณีที่มีการปฏิบัติงานจากเครือข่ายภายนอก (teleworking) เพื่อเข้าถึงระบบ IT ที่มีนัยสำคัญ สำนักงานสอบบัญชีควรจัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่รัดกุมเพียงพอเหมาะสมกับระบบ IT และข้อมูลที่ถูกเข้าถึง โดยครอบคลุมอย่างน้อยดังนี้<br>(1) มาตรการรักษาความมั่นคงปลอดภัยด้านกายภาพที่เหมาะสม รัดกุมเพียงพอกับขอบเขตการปฏิบัติงาน สำหรับพื้นที่ปฏิบัติงานนอกองค์กร<br>(2) การอนุมัติการปฏิบัติงานจากเครือข่ายภายนอกโดยผู้มีอำนาจหรือผู้บริหารที่เกี่ยวข้อง<br>(3) การกำหนดสิทธิการเข้าถึงข้อมูลและระบบ IT จากเครือข่ายภายนอกเท่าที่จำเป็น พร้อมทั้งมีการทบทวนสิทธิอย่างสม่ำเสมอ<br>(4) การยืนยันตัวตน (authencitation) ของพนักงานที่ปฏิบัติงานจากเครือข่ายภายนอกด้วยวิธีการที่รัดกุมปลอดภัย เช่น การใช้วิธียืนยันตัวตนแบบหลายปัจจัย (multi-factor authentication) และการเข้าใช้งานผ่านอุปกรณ์ที่อนุญาตเท่านั้น เป็นต้น<br>(5) มาตรการป้องกันความเสี่ยงจากการใช้อุปกรณ์ที่ใช้ในการปฏิบัติงานจากเครือข่ายภายนอก เป็นช่องทางในการแพร่กระจายของโปรแกรมไม่ประสงค์ดี (malware) และการรั่วไหลของข้อมูลสำคัญ<br>(6) มาตรการป้องกันข้อมูลที่เป็นความลับหรือมีความสำคัญ (sensitive data) เช่น การยืนยันตัวตนก่อนใช้งานอุปกรณ์ (lock screen) การเข้ารหัสข้อมูลบนอุปกรณ์ที่ใช้ในการปฏิบัติงาน หรือการลบข้อมูลจากระยะไกล (remote wipe-out) เป็นต้น<br><br>2. ในการปฏิบัติงานที่มีการใช้อุปกรณ์เคลื่อนที่ (mobile device) เพื่อเข้าถึงระบบ IT ที่มีนัยสำคัญ สำนักงานสอบบัญชีควรจัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่รัดกุมเพียงพอ เหมาะสมกับระบบ IT และข้อมูลที่ถูกเข้าถึง เช่น<br>(1) การลงทะเบียนอุปกรณ์เคลื่อนที่ก่อนการใช้งาน โดยมีการทบทวนทะเบียนดังกล่าวอย่างน้อยปีละ 1 ครั้ง และเมื่อมีการเปลี่ยนอุปกรณ์ เพื่อให้มั่นใจได้ว่าอุปกรณ์เคลื่อนที่ดังกล่าวมีความความมั่นคงปลอดภัยเพียงพอ ทั้งนี้ สำนักงานสอบบัญชีอาจใช้ระบบหรือเทคโนโลยีการลงทะเบียนอื่นทดแทนได้ หากพิจารณาแล้วเห็นว่าเหมาะสม<br>(2) มาตรการป้องกันข้อมูลที่เป็นความลับหรือมีความสำคัญ (sensitive data) เช่น การยืนยันตัวตนก่อนใช้งานอุปกรณ์ (lock screen) การเข้ารหัสข้อมูลบนอุปกรณ์ที่ใช้ปฏิบัติงาน หรือการลบข้อมูลจากระยะไกล (remote wipe-out) เป็นต้น |

| ข้อกำหนด | แนวปฏิบัติ |
|---|---|
| | 3. กรณีที่อนุญาตให้พนักงานสามารถใช้อุปกรณ์ส่วนตัวของพนักงาน (bring your own device : BYOD) สำนักงานสอบบัญชีควรพิจารณาความเสี่ยงที่เกี่ยวข้อง และจัดให้มีมาตรการควบคุมความเสี่ยงอย่างเหมาะสม โดยครอบคลุมอย่างน้อยดังนี้<br>(1) การกำหนดหลักเกณฑ์การอนุญาตให้ใช้งาน BYOD<br>(2) การควบคุมการใช้ BYOD ให้สามารถเข้าถึงเครือข่ายสื่อสาร ข้อมูล และระบบ IT เท่าที่จำเป็น<br>(3) การยืนยันตัวตนเพื่อปลดล็อคในการเข้าถึง BYOD เช่น การใช้รหัสผ่าน และการสแกนลายนิ้วมือ เป็นต้น<br>(4) ในกรณีเครื่องคอมพิวเตอร์ส่วนตัวของพนักงาน (personal computer, notebook) สามารถเชื่อมต่อเข้าสู่ระบบเครือข่ายภายในหรือข้อมูลสำคัญ ควรจัดให้มีการติดตั้งซอฟต์แวร์ป้องกันโปรแกรมไม่ประสงค์ดี (anti-virus/ anti-malware) และปรับปรุงให้ทันสมัย (update) อยู่เสมอ<br>(5) ห้ามการใช้อุปกรณ์เคลื่อนที่ (tablet, smartphone) ที่ถูกปรับแต่ง (rooted หรือ jailbroken) เข้าถึงระบบ IT |
| **2.8.6 การสำรองข้อมูล (data backup)** | |
| 8.6 การสำรองข้อมูล (data backup) ที่สำคัญด้วยวิธีการและความถี่ที่เหมาะสม เพื่อให้ข้อมูลสำรองมีสภาพพร้อมใช้งานสอดคล้องกับเป้าหมายการกู้คืนระบบ IT ในกรณีที่ระบบ IT และข้อมูลหลักเกิดเหตุขัดข้องหรือได้รับความเสียหาย โดยต้องมีการทดสอบข้อมูลสำรองและกระบวนการกู้คืนข้อมูลอย่างน้อยปีละ 1 ครั้ง | 1. สำนักงานสอบบัญชีควรกำหนดมาตรฐานหรือวิธีปฏิบัติในการสำรองข้อมูลที่สอดคล้องกับระยะเวลาเป้าหมายในการกู้คืนระบบ IT (Recovery Time Objective : RTO) และระยะเวลาเป้าหมายสูงสุดที่ยอมให้ข้อมูลเสียหาย (Recovery Point Objective : RPO) โดยอย่างน้อยควรมีรายละเอียดครอบคลุม<br>(1) ข้อมูลที่ต้องสำรอง<br>(2) ความถี่หรือรอบเวลาในการสำรองข้อมูล<br>(3) ขั้นตอนและวิธีการสำรองข้อมูล<br>(4) ขั้นตอนและวิธีการกู้คืนข้อมูล<br>(5) สถานที่และวิธีการเก็บรักษาสื่อบันทึกข้อมูล<br>2. สำนักงานสอบบัญชีควรจัดเก็บสื่อบันทึกข้อมูลสำรอง พร้อมทั้งสำเนาขั้นตอนหรือวิธีปฏิบัติงานต่าง ๆ ไว้นอกศูนย์คอมพิวเตอร์หลักหรือนอกสถานที่ปฏิบัติงานหลัก โดยสถานที่ดังกล่าวควรจัดให้มีมาตรการรักษาความปลอดภัยอย่างเหมาะสมตามนโยบายของสำนักงานสอบบัญชี หรือ เทียบเคียงกับศูนย์คอมพิวเตอร์หลักหรือสถานที่ปฏิบัติงานหลัก<br>3. สำนักงานสอบบัญชีควรจัดให้มีการสอบทานการสำรองข้อมูล และทดสอบข้อมูลสำรองอย่างน้อยปีละ 1 ครั้ง เพื่อให้มั่นใจว่ามีการสำรองข้อมูลมีความครบถ้วนถูกต้อง พร้อมใช้งาน และปลอดภัย<br>4. ในกรณีที่จำเป็นต้องจัดเก็บข้อมูลเป็นระยะเวลานาน สำนักงานสอบบัญชีควรคำนึงถึงวิธีการนำข้อมูลกลับมาใช้งานในอนาคตด้วยหากมี |

| ข้อกำหนด | แนวปฏิบัติ |
|---|---|
| | ความจำเป็น เช่น เมื่อมีการจัดเก็บข้อมูลลงในสื่อบันทึกข้อมูลใด ให้มีการจัดเก็บอุปกรณ์และโปรแกรมที่ใช้อ่านสื่อบันทึกข้อมูลนั้นด้วย เป็นต้น |
| **2.8.7 การจัดเก็บข้อมูลบันทึกเหตุการณ์การใช้งานเกี่ยวกับระบบ IT (log)** | |
| 8.7 การจัดเก็บข้อมูลบันทึกเหตุการณ์การใช้งานเกี่ยวกับระบบ IT (log) อย่างครบถ้วนและเพียงพอ เพื่อให้สามารถใช้เป็นหลักฐานการทำธุรกรรมทางอิเล็กทรอนิกส์ และสามารถติดตามและตรวจสอบการเข้าถึงและใช้งานข้อมูลและระบบ IT ย้อนหลังได้ ตามที่กฎหมายกำหนด อย่างไรก็ดี หากการควบคุมการจัดเก็บข้อมูลบันทึกเหตุการณ์การใช้งานเกี่ยวกับระบบ IT (log) ของสำนักงานสอบบัญชีไม่ได้อยู่ภายใต้อำนาจการควบคุมของสำนักงานสอบบัญชี และ สำนักงานสอบบัญชีมีข้อจำกัดในการดำเนินการตามแนวปฏิบัติขั้นต่ำนี้ สำนักงานสอบบัญชีต้องจัดให้มีการควบคุมอื่นทดแทน เพื่อให้มั่นใจได้ว่าสามารถติดตามและตรวจสอบการเข้าถึงและใช้งานข้อมูลและระบบ IT ย้อนหลังได้ตามที่กฎหมายกำหนด | 1. สำนักงานสอบบัญชีควรจัดเก็บข้อมูลบันทึกเหตุการณ์ (log) ด้วยวิธีการที่ปลอดภัย โดยมีรายละเอียดครบถ้วนเพียงพอที่จะใช้เป็นหลักฐานในการตรวจสอบที่สามารถระบุตัวบุคคลผู้กระทำได้ และจัดเก็บเป็นระยะเวลาอย่างน้อย 90 วัน หรือจัดเก็บตามกฎหมายที่เกี่ยวข้องกำหนด ประกอบด้วยรายการหลักฐานอย่างน้อย ดังนี้<br>(1) บันทึกเหตุการณ์การเข้า-ออกศูนย์คอมพิวเตอร์ และพื้นที่ที่เกี่ยวข้องกับระบบ IT ที่มีนัยสำคัญ (physical access log)<br>(2) บันทึกการยืนยันตัวตนและการเข้าถึง (authentication log และ access log) ของเครื่องแม่ข่าย ระบบงาน อุปกรณ์เครือข่าย และข้อมูลที่มีความสำคัญ โดยรวมถึงความพยายามในการเข้าถึง (log-in attempt)<br>(3) บันทึกการดำเนินงาน (activity log) ที่สำคัญ โดยอย่างน้อยครอบคลุม<br>(3.1) การเปลี่ยนแปลงแก้ไขโครงสร้างข้อมูล<br>(3.2) การเปลี่ยนแปลงแก้ไข และลบข้อมูลสำคัญ<br>(3.3) การเปลี่ยนแปลงแก้ไขการตั้งค่าของระบบ (system configuration)<br>(3.4) การเปลี่ยนแปลงแก้ไขบัญชี และสิทธิของผู้ใช้งาน<br>(3.5) การใช้งานอินเทอร์เน็ตผ่านระบบเครือข่ายของสำนักงานสอบบัญชี<br>(3.6) การทำงานของ firewall (network firewall log)<br>2. สำนักงานสอบบัญชีควรจัดเก็บ log ที่เกี่ยวข้องกับข้อมูลส่วนบุคคล เพื่อใช้ตรวจสอบกิจกรรมของผู้ใช้งานและใช้เป็นหลักฐานหากเกิดเหตุการณ์การเข้าถึง ใช้งาน แก้ไขเปลี่ยนแปลง หรือเปิดเผยข้อมูลส่วนบุคคลที่ไม่เหมาะสม โดยสอดคล้องกับกฎหมายและหลักเกณฑ์ที่เกี่ยวข้อง เช่น กฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ และกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล เป็นต้น<br>3. สำนักงานสอบบัญชีควรจัดเก็บ log ของอุปกรณ์สำคัญไว้ที่เครื่องแม่ข่ายที่ใช้จัดเก็บ log (logging server) ที่แยกเฉพาะ หรือใช้วิธีการที่เทียบเคียงซึ่งสามารถป้องกันการเปลี่ยนแปลง แก้ไข หรือทำลาย log ได้ โดยมีมาตรการรักษาความปลอดภัยอย่างน้อย ดังนี้<br>(1) กำหนดหน้าที่และความรับผิดชอบผู้ที่สามารถเข้าถึง log ตามความจำเป็น<br>(2) มีกระบวนการยืนยันตัวตนและตรวจสอบสิทธิในการเข้าถึง log<br>(3) ติดตั้งเครื่องแม่ข่าย หรืออุปกรณ์ที่ใช้จัดเก็บ log ให้อยู่ในโซนเครือข่ายที่มีความมั่นคงปลอดภัย |

| ข้อกำหนด | แนวปฏิบัติ |
|---|---|
| **2.8.8 การติดตามดูแลระบบและเฝ้าระวังภัยคุกคามทางไซเบอร์ (security monitoring)** | |
| 8.8 การติดตามดูแลระบบและเฝ้าระวังภัยคุกคามทางไซเบอร์ (security monitoring) โดยมีกระบวนการหรือเครื่องมือป้องกันและตรวจจับเหตุการณ์ผิดปกติด้าน IT โปรแกรมไม่ประสงค์ดี (malware) หรือภัยคุกคามทางไซเบอร์ที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยต่อระบบ IT ที่มีนัยสำคัญ | 1. สำนักงานสอบบัญชีควรจัดให้มีกระบวนการหรือเครื่องมือในการตรวจจับเหตุการณ์ผิดปกติที่อาจส่งผลกระทบต่อความปลอดภัยของระบบ IT ที่มีนัยสำคัญอย่างทันท่วงที เช่น กระบวนการหรือเครื่องมือในการสอบทาน log เป็นต้น เพื่อให้รับทราบความผิดปกติหรือภัยคุกคาม และสามารถดำเนินการป้องกันหรือรับมือได้อย่างเหมาะสม<br>2. สำนักงานสอบบัญชีควรจัดให้มีกระบวนการหรือเครื่องมือในการรับข้อมูลข่าวสารเกี่ยวกับภัยคุกคาม (cyber threat intelligence) เพื่อให้สามารถติดตามและวิเคราะห์ภัยคุกคามทางไซเบอร์ที่อาจเกิดขึ้น และสามารถดำเนินการป้องกันหรือรับมือได้อย่างเหมาะสม |
| **2.8.9 การประเมินช่องโหว่ทางเทคนิค (technical vulnerability assessment)** | |
| 8.9 การประเมินช่องโหว่ทางเทคนิค (technical vulnerability assessment) ของระบบ IT ที่เหมาะสมกับระดับความเสี่ยงเพื่อให้ทราบถึงช่องโหว่ และสามารถดำเนินการแก้ไขและป้องกันภัยคุกคามทางไซเบอร์ที่อาจเกิดขึ้นได้อย่างทันท่วงที โดยการประเมินช่องโหว่ทางเทคนิคครอบคลุมระบบ IT ที่มีนัยสำคัญ และระบบ IT ที่เชื่อมต่อกับเครือข่ายสาธารณะ (internet facing) ทุกระบบอย่างน้อยตามรอบระยะเวลาที่ได้จากการประเมินระดับความเสี่ยงด้านเทคโนโลยีสารสนเทศของสำนักงานสอบบัญชี (IT Risk Assessment : ITRA) และทุกครั้งที่มีการเปลี่ยนแปลงอย่างมีนัยสำคัญของระบบดังกล่าว เช่น การเปลี่ยนแปลงโครงสร้างพื้นฐานของระบบ IT หรือการเพิ่มเติมฟังก์ชันสำคัญของระบบ IT เป็นต้น | 1. สำนักงานสอบบัญชีควรกำหนดขอบเขตและความถี่ของการประเมินช่องโหว่ทางเทคนิคให้ครอบคลุมทุกระบบงานตามระดับความเสี่ยง ทั้งนี้ สำหรับระบบ IT ที่มีนัยสำคัญและระบบ IT ที่เชื่อมต่อกับเครือข่ายสาธารณะทุกระบบต้องได้รับการประเมินช่องโหว่อย่างน้อยตามรอบระยะเวลาที่ได้จากการประเมินระดับความเสี่ยงด้านเทคโนโลยีสารสนเทศของสำนักงานสอบบัญชี (IT Risk Assessment : ITRA) และทุกครั้งที่มีการเปลี่ยนแปลงระบบดังกล่าวอย่างมีนัยสำคัญ<br>2. สำนักงานสอบบัญชีควรประเมินความเสี่ยงของช่องโหว่ที่ตรวจพบและกำหนดระยะเวลาแก้ไขที่เหมาะสมกับความเสี่ยง<br>3. สำนักงานสอบบัญชีควรรายงานผลการประเมินช่องโหว่ไปยังผู้รับผิดชอบ รวมถึงติดตามให้มีการแก้ไขช่องโหว่ภายในระยะเวลาที่กำหนดไว้ โดยนำเสนอความคืบหน้าของการดำเนินการต่อหัวหน้าสำนักงานสอบบัญชี หรือคณะกรรมการบริหารของสำนักงานสอบบัญชีที่ได้รับมอบหมาย |
| **2.8.10 การบริหารจัดการโปรแกรมแก้ไขช่องโหว่ (patch management)** | |
| 8.10 การบริหารจัดการโปรแกรมแก้ไขช่องโหว่ (patch management) โดยจัดให้มีกระบวนการควบคุม | 1. สำนักงานสอบบัญชีควรมีการกำหนดมาตรฐานและระเบียบวิธีปฏิบัติในการบริหารจัดการโปรแกรมแก้ไขช่องโหว่ (patch) ที่ครอบคลุมการดำเนินการอย่างน้อย ดังนี้ |

| ข้อกำหนด | แนวปฏิบัติ |
|---|---|
| การติดตั้งโปรแกรมแก้ไขช่องโหว่บนระบบและอุปกรณ์เพื่อลดความเสี่ยงที่จะถูกโจมตีในอนาคต | (1) การประเมินความเสี่ยงและความจำเป็นในการติดตั้ง patch<br>(2) การกำหนดกรอบระยะเวลาการติดตั้ง patch โดยคำนึงถึงความจำเป็นและความเสี่ยงจากการถูกโจมตีจากช่องโหว่<br>(3) การตรวจสอบความถูกต้องและการทดสอบ patch ก่อนการดำเนินการติดตั้งบนระบบที่ให้บริการจริง เพื่อป้องกันผลกระทบที่ไม่พึงประสงค์จากการติดตั้ง patch ทั้งนี้ ในกรณีที่มีข้อจำกัดในการทดสอบ patch สำนักงานสอบบัญชีอาจพิจารณาการควบคุมอื่น ๆ ทดแทน<br>2. การติดตั้ง patch บนระบบงานจริง ควรดำเนินการตามกระบวนการบริหารจัดการการเปลี่ยนแปลง (change management) ที่กำหนดไว้ เพื่อป้องกันความเสี่ยงและข้อผิดพลาดจากการปฏิบัติงาน<br>3. กรณีมีเหตุที่ผู้ผลิตระบบงานหรืออุปกรณ์ยังไม่แจ้งการปรับปรุง security patch อย่างเป็นทางการเพื่อปิดช่องโหว่ใหม่ ๆ ที่เพิ่งค้นพบ สำนักงานสอบบัญชีควรปฏิบัติตามคำแนะนำของผู้พัฒนาระบบ เจ้าของผลิตภัณฑ์ หรือผู้เชี่ยวชาญด้านความมั่นคงปลอดภัย หรือจัดให้มีมาตรการควบคุมทดแทน เพื่อลดความเสี่ยงจากการถูกโจมตีผ่านช่องโหว่นั้น ๆ<br>4. สำนักงานสอบบัญชีควรมอบหมายผู้รับผิดชอบ หรือจัดให้มีเครื่องมือที่ใช้ติดตาม patch ด้านการรักษาความปลอดภัย (patch monitoring tool) ที่ยังไม่มีการติดตั้งบนระบบปฏิบัติการ (operation system) และระบบฐานข้อมูล (database system) ที่สำคัญของสำนักงานสอบบัญชี |
| **2.9 การรักษาความมั่นคงปลอดภัยเกี่ยวกับระบบเครือข่ายสื่อสาร (communication system security)** | |
| **ส่วนที่ 9 การรักษาความมั่นคงปลอดภัยเกี่ยวกับระบบเครือข่ายสื่อสาร (communication system security)**<br>สำนักงานสอบบัญชีต้องมีการรักษาความมั่นคงปลอดภัยเกี่ยวกับระบบเครือข่ายสื่อสารอย่างเหมาะสม เพื่อให้ระบบเครือข่ายสื่อสารและข้อมูลที่รับส่งผ่านระบบเครือข่ายสื่อสารมีความมั่นคงปลอดภัย สามารถป้องกันการบุกรุกหรือภัยคุกคามทางไซเบอร์ที่อาจเกิดขึ้น รวมทั้งพร้อมใช้งานได้อย่างต่อเนื่อง อย่างไรก็ดี หากการรักษาความมั่นคงปลอดภัยเกี่ยวกับระบบเครือข่ายสื่อสารของสำนักงานสอบบัญชีไม่ได้อยู่ภายใต้อำนาจ | 1. สำนักงานสอบบัญชีควรจัดให้มีการรักษาความมั่นคงปลอดภัยของระบบเครือข่ายสื่อสาร โดยมีการดำเนินการอย่างน้อย ดังนี้<br>(1) ออกแบบเครือข่ายสื่อสารที่มีการแบ่งแยกเครือข่ายอย่างเหมาะสม โดยคำนึงถึงระดับความสำคัญของระบบงาน (application system) ระดับความสำคัญของข้อมูล รวมถึงความจำเป็นในการเชื่อมต่อจากระบบงานอื่น ๆ หรือจากภายนอกองค์กร<br>(2) จัดให้มีการควบคุมการเชื่อมต่อของระบบงาน (application system) ที่สำคัญ<br>(3) การแบ่งแยกเครือข่ายให้มีความรัดกุมปลอดภัย เช่น<br>(3.1) แบ่งแยกเครือข่ายภายใน (private network) และเครือข่ายภายนอก (public network) ออกจากกัน<br>(3.2) แบ่งแยกเครือข่ายของระบบ IT ที่มีนัยสำคัญ เครือข่ายสำหรับการปฏิบัติงานของพนักงาน และเครือข่ายสำหรับการใช้งานทั่วไป/เครือข่ายสำหรับบุคคลภายนอก (guest network) ออกจากกัน<br>(3.3) จุดที่มีการแบ่งแยกเครือข่ายที่มีความสำคัญและมีความเสี่ยง ควรติดตั้งอุปกรณ์รักษาความปลอดภัยเครือข่ายที่มีความสามารถในการควบคุมและคัดกรองข้อมูล (traffic) ที่รับส่งผ่านเครือข่าย เพื่อป้องกันและตรวจจับการบุกรุกของไวรัสหรือมัลแวร์ต่าง ๆ |

| ข้อกำหนด | แนวปฏิบัติ |
|---|---|
| การควบคุมของสำนักงานสอบบัญชี และสำนักงานสอบบัญชีมีข้อจำกัดในการดำเนินการตามแนวปฏิบัติขั้นต่ำนี้ สำนักงานสอบบัญชีต้องจัดให้มีการควบคุมอื่นทดแทน เพื่อให้มั่นใจได้ว่าระบบเครือข่ายสื่อสารและข้อมูลที่รับส่งผ่านระบบเครือข่ายสื่อสารมีความมั่นคงปลอดภัย สามารถป้องกันการบุกรุกหรือภัยคุกคามทางไซเบอร์ที่อาจเกิดขึ้น รวมทั้งพร้อมใช้งานได้อย่างต่อเนื่อง | (4) ควบคุม และจำกัดให้เฉพาะอุปกรณ์ที่ได้รับอนุญาตเท่านั้นที่สามารถเชื่อมต่อกับระบบเครือข่ายภายในได้<br>(5) กำหนดกระบวนการเปิดใช้งานช่องทางเชื่อมต่อ (port) ตามความจำเป็น รวมทั้งการขออนุมัติจากผู้มีอำนาจ และจัดให้มีการควบคุมอย่างเหมาะสม<br>(6) ติดตามสถานะความพร้อมใช้งานของระบบเครือข่ายให้อยู่ในระดับ service level agreement (SLA) ที่กำหนด<br>(7) จัดให้มีระบบหรือมาตรการป้องกันการโจมตีผ่านเครือข่ายสาธารณะที่เหมาะสมตามความเสี่ยง เช่น การใช้อุปกรณ์การรักษาความปลอดภัย intrusion prevention system (IPS) และการป้องกันการโจมตีแบบ Distributed Denial of Service (DDoS protection) เป็นต้น<br>2. สำนักงานสอบบัญชีควรจัดให้มีการรักษาความมั่นคงปลอดภัยของข้อมูลสารสนเทศที่รับส่งผ่านระบบเครือข่ายสื่อสาร (information transfer) เช่น<br>(1) กำหนดแนวปฏิบัติที่ดีในการรับส่งข้อมูลสารสนเทศผ่านช่องทางการสื่อสารอิเล็กทรอนิกส์ประเภทต่าง ๆ<br>(2) นำเทคนิคการเข้ารหัสข้อมูลมาใช้ในการรับส่งข้อมูลสารสนเทศที่เป็นความลับและมีความสำคัญ<br>(3) มาตรการป้องกันข้อมูลที่เป็นความลับหรือมีความสำคัญที่รับส่งในรูปแบบของไฟล์แนบ (attachment files) และการส่งต่ออีเมลแบบอัตโนมัติออกสู่ภายนอกองค์กร<br>3. สำนักงานสอบบัญชีควรจัดให้มีการรักษาความมั่นคงปลอดภัยสำหรับการใช้งานระบบรับส่งข้อมูลสารสนเทศผ่านระบบเครือข่ายสื่อสาร (ระบบ electronic messaging) โดยมีการดำเนินการอย่างน้อย ดังนี้<br>(1) กรณีที่มีการใช้งานระบบ electronic messaging ที่ให้บริการโดยบุคคลภายนอก เช่น โปรแกรมสนทนาผ่านระบบอิเล็กทรอนิกส์ (instant messaging) ระบบเครือข่ายสังคมออนไลน์ (social networking) หรือโปรแกรมเรียกใช้แฟ้มข้อมูลร่วมกัน (file sharing) เป็นต้น สำนักงานสอบบัญชีควรจัดให้มีการควบคุมดูแลอย่างเหมาะสมเพียงพอ และคำนึงถึงการปฏิบัติตามกฎหมายและหลักเกณฑ์ที่เกี่ยวข้องอย่างเคร่งครัด<br>(2) จัดให้มีมาตรการคัดกรอง (filter) อีเมลที่มีความเสี่ยงต่อการเกิดภัยคุกคามทางไซเบอร์ เช่น อีเมลที่มีไฟล์แนบชนิด .exe เป็นต้น |
| **2.10 การบริหารจัดการโครงการด้าน IT (IT project management) และการจัดหา พัฒนา และบำรุงรักษาระบบ IT (system acquisition, development and maintenance)** | |
| **ส่วนที่ 10 การบริหารจัดการโครงการด้าน IT (IT project management) และการจัดหา พัฒนา และบำรุงรักษาระบบ IT (system acquisition, development and maintenance)** | หากสำนักงานสอบบัญชีไม่มีแผนที่จะบริหารจัดการโครงการด้าน IT และการจัดหา พัฒนา และบำรุงรักษาระบบ IT หรือมีเพียงอย่างใดอย่างหนึ่ง สำนักงานสอบบัญชีสามารถเลือกที่จะจัดทำนโยบาย แนวปฏิบัติ และดำเนินการเฉพาะหัวข้อที่เกี่ยวข้องเท่านั้น |

| ข้อกำหนด | แนวปฏิบัติ |
|---|---|
| สำหรับสำนักงานสอบบัญชีมีการบริหารจัดการโครงการด้าน IT (IT project management) และการจัดหา พัฒนา และบำรุงรักษาระบบ IT ในปัจจุบัน หรือวางแผนว่าจะมีในอนาคต สำนักงานสอบบัญชีต้องจัดทำนโยบายและแนวปฏิบัติสำหรับการบริหารจัดการโครงการด้าน IT การจัดหา พัฒนา รวมถึงบำรุงรักษาระบบ IT เป็นลายลักษณ์อักษร เพื่อให้มั่นใจได้ว่า เมื่อใดก็ตามที่มีการดำเนินโครงการด้านIT สำนักงานสอบบัญชีจะมีกรอบและแนวทางที่จะช่วยรักษาความมั่นคงปลอดภัยตลอดวงจรชีวิตของระบบ IT (entire life cycle) โดยให้ครอบคลุมรายละเอียดอย่างน้อย ดังนี้ | |
| **2.10.1 การบริหารจัดการโครงการด้าน IT (IT project management)** | |
| <u>10.1 บริหารจัดการโครงการด้าน IT (IT project management)</u><br>กำหนดกรอบการบริหารจัดการโครงการ (project management framework) เพื่อให้การบริหารจัดการโครงการด้าน IT ที่มีนัยสำคัญเป็นไปอย่างมีประสิทธิภาพ สามารถส่งมอบโครงการได้อย่างถูกต้อง ครบถ้วนตามแผนงานและบรรลุวัตถุประสงค์ตามเป้าหมายที่กำหนดไว้ ไม่ว่างานโครงการนั้นจะดำเนินการโดยสำนักงานสอบบัญชีเอง หรือ บุคคลภายนอก | 1. สำนักงานสอบบัญชีควรกำหนดกรอบการบริหารจัดการโครงการ (project management framework) เป็นลายลักษณ์อักษร โดยมีรายละเอียดขั้นต่ำ ดังนี้<br>(1) โครงสร้างการควบคุมและกำกับดูแลโครงการ (project governance) ที่ชัดเจน เพื่อให้มีการควบคุมดูแลโครงการให้สำเร็จเป็นไปตามแผนงานที่กำหนด โดยพิจารณาการจัดให้มีผู้รับผิดชอบในบทบาทหน้าที่ตามความจำเป็นและความเหมาะสม เช่น<br>(1.1) คณะกรรมการกำกับดูแลโครงการ (project steering committee) มีบทบาทหน้าที่และความรับผิดชอบในการกำกับดูแลและติดตามความคืบหน้าของโครงการ รวมทั้งให้คำแนะนำ และพิจารณาตัดสินใจการดำเนินงานในโครงการที่สำคัญ เพื่อให้โครงการสามารถดำเนินการได้ตามแผนที่กำหนดไว้ โดยควรประกอบด้วยผู้บริหารจากหน่วยงานที่เกี่ยวข้อง และเจ้าของโครงการหรือผู้สนับสนุนโครงการ (project owner/project sponsor)<br>(1.2) ผู้จัดการโครงการ (project manager) มีบทบาทหน้าที่และความรับผิดชอบในการบริหารจัดการโครงการให้เป็นไปตามระเบียบขั้นตอนการบริหารจัดการโครงการ เพื่อให้โครงการสามารถส่งมอบได้อย่างถูกต้องครบถ้วนสำเร็จตามแผนงานที่กำหนด<br>(2) แนวทางการบริหารจัดการโครงการ โดยมีรายละเอียดขั้นต่ำ ดังนี้ |

| ข้อกำหนด | แนวปฏิบัติ |
|---|---|
| | (2.1) ระเบียบขั้นตอนการบริหารจัดการโครงการ ครอบคลุมตั้งแต่ก่อนเริ่มโครงการ การดำเนินการและควบคุมโครงการ การปิดโครงการ และการสอบทานโครงการ<br>(2.2) ปัจจัยและเกณฑ์ในการประเมินหรือจัดระดับความสำคัญของโครงการที่ชัดเจน รวมถึงขอบเขตอำนาจหน้าที่ในการอนุมัติและกำกับดูแลโครงการตามระดับความสำคัญของโครงการ<br>(2.3) เอกสารหรือสิ่งส่งมอบในแต่ละขั้นตอนอย่างชัดเจน เช่น แผนการดำเนินโครงการ รายงานความคืบหน้า รายงานการปิดโครงการ เป็นต้น<br>2. การเริ่มโครงการ สำนักงานสอบบัญชีควรดำเนินการอย่างน้อย ดังนี้<br>(1) ประเมินความจำเป็นและประโยชน์ที่คาดว่าจะได้รับ รวมถึงความเสี่ยงและผลกระทบที่อาจเกิดขึ้นต่อระบบและหน่วยงานที่เกี่ยวข้อง<br>(2) จัดทำแผนการดำเนินโครงการที่มีรายละเอียดครบถ้วนเพียงพอต่อการบริหารจัดการโครงการอย่างน้อยครอบคลุม<br>(2.1) เป้าหมายโครงการ<br>(2.2) ทรัพยากร และเทคโนโลยีที่ใช้<br>(2.3) บทบาทหน้าที่และความรับผิดชอบของทีมงานในการดำเนินโครงการ<br>(2.4) ขอบเขตและระยะเวลาของการดำเนินโครงการในแต่ละขั้นตอน<br>(2.5) ผลงานที่จะส่งมอบในแต่ละขั้นตอน<br>(2.6) ข้อกำหนดเงื่อนไขที่เกี่ยวข้องกับโครงการ (ถ้ามี) เช่น ข้อกำหนดของผู้ว่าจ้าง ภาระผูกพัน ข้อจำกัด เป็นต้น<br>(3) มีการนำเสนอแผนการดำเนินโครงการ เพื่อขออนุมัติโครงการต่อหัวหน้าสำนักงานสอบบัญชี หรือคณะกรรมการบริหารของสำนักงานสอบบัญชีตามขอบเขตในการอนุมัติที่กำหนดไว้<br>3. การดำเนินงานและควบคุมโครงการ สำนักงานสอบบัญชีควรดำเนินการอย่างน้อย ดังนี้<br>(1) ติดตามและประเมินการดำเนินโครงการอย่างต่อเนื่องและครอบคลุมขอบเขต ระยะเวลา และทรัพยากรที่วางแผนไว้<br>(2) ในกรณีที่มีการเปลี่ยนแปลงขอบเขต ระยะเวลาหรือทรัพยากร หรือยกเลิกโครงการ ควรมีการนำเสนอผู้มีอำนาจเพื่อขออนุมัติการเปลี่ยนแปลงหรือยกเลิกโครงการ<br>(3) รายงานความคืบหน้า ปัญหา อุปสรรคและข้อจำกัดในการดำเนินโครงการ ต่อคณะกรรมการกำกับดูแลโครงการหรือผู้บริหารระดับสูงที่ได้รับมอบหมายอย่างสม่ำเสมอ โดยโครงการที่ส่งผลกระทบต่อธุรกิจของสำนักงานสอบบัญชีอย่างมีนัยสำคัญควรมีการนำเสนอแก่หัวหน้าสำนักงานสอบบัญชี หรือคณะกรรมการบริหารของสำนักงานสอบบัญชีด้วย |

| ข้อกำหนด | แนวปฏิบัติ |
|---|---|
| | 4. การปิดโครงการ สำนักงานสอบบัญชีควรดำเนินการอย่างน้อย ดังนี้<br>(1) สรุปประโยชน์ที่ได้รับจากโครงการเปรียบเทียบกับเป้าหมายที่กำหนด<br>(2) รวบรวมปัญหา อุปสรรคจากการบริหารจัดการโครงการ เพื่อนำมาเป็นสิ่งที่ได้เรียนรู้ (lesson learned) ใช้สำหรับวิเคราะห์ ปรับปรุง และพัฒนากระบวนการหรือเครื่องมือในการบริหารจัดการโครงการต่อไปให้มีประสิทธิภาพมากขึ้น<br>5. สำนักงานสอบบัญชีควรสอบทานโครงการที่มีนัยสำคัญ เพื่อให้มั่นใจได้ว่าโครงการสอดคล้องกับเป้าหมายของโครงการ นโยบาย มาตรฐาน ระเบียบและวิธีปฏิบัติของสำนักงานสอบบัญชี รวมทั้งกฎหมายและหลักเกณฑ์ที่เกี่ยวข้อง |
| **2.10.2 การจัดหาระบบ IT (system acquisition)** | |
| 10.2 จัดหาระบบ IT (system acquisition)<br>จัดให้มีหลักเกณฑ์ในการจัดหาระบบ IT และผู้ให้บริการ เพื่อให้มั่นใจว่าระบบที่จัดหาสามารถตอบสนองความต้องการทางธุรกิจและความต้องการด้านความมั่นคงปลอดภัย IT โดยคำนึงถึงความยืดหยุ่นในการเปลี่ยนแปลงผู้ให้บริการ การเปลี่ยนแปลงเทคโนโลยี รวมถึงการเปลี่ยนแปลงต่าง ๆ ที่เกี่ยวข้องกับการดำเนินธุรกิจอย่างมีนัยสำคัญ | 1. สำนักงานสอบบัญชีควรจัดให้มีหลักเกณฑ์การคัดเลือกระบบ IT และผู้ให้บริการ เพื่อให้มั่นใจว่าระบบที่จัดหาสามารถตอบสนองความต้องการทางธุรกิจและความต้องการด้านความมั่นคงปลอดภัยสารสนเทศ ซึ่งควรคำนึงถึงเรื่องดังนี้<br>(1) รายละเอียดทั่วไป เช่น เทคโนโลยีที่ใช้ สิทธิการใช้งานซอฟต์แวร์ (software license) ฟังก์ชันการทำงานของระบบ เป็นต้น<br>(2) ความมั่นคงปลอดภัยของระบบ<br>(3) ความน่าเชื่อถือของระบบ IT และผู้ให้บริการ เช่น ฐานะการเงิน ชื่อเสียง และความสามารถด้านเทคนิค เป็นต้น<br>(4) การได้รับการรับรองตามมาตรฐานสากลหรือมาตรฐานด้าน IT ที่เกี่ยวข้องที่ได้รับการยอมรับโดยทั่วไป (certificate)<br>(5) การสนับสนุนและการบำรุงรักษาระบบ<br>(6) การทดสอบการทำงานขั้นต้น (proof of concept) ในกรณีที่เป็นระบบ IT ที่มีนัยสำคัญ<br>(7) มาตรการรองรับหรือการบริหารความเสี่ยง ในกรณีที่ผู้พัฒนาระบบหรือผู้ให้บริการซอฟต์แวร์ไม่ปฏิบัติตามข้อตกลงในการบำรุงรักษาระบบหรือให้การสนับสนุนการดำเนินงานตามที่ตกลงไว้ เช่น จัดให้มีข้อตกลงการรับฝากโค้ดต้นฉบับ (source-code escrow agreement) เพื่อให้มั่นใจว่าสำนักงานสอบบัญชีจะมีสิทธิในการเข้าถึง source code ของระบบหรือซอฟต์แวร์ดังกล่าว เป็นต้น |
| **2.10.3 การพัฒนาระบบ IT (system development))** | |
| 10.3 พัฒนาระบบ IT (system development)<br>จัดให้มีมาตรการควบคุมเกี่ยวกับการพัฒนาระบบ IT ในการออกแบบ พัฒนา ทดสอบระบบ และนำระบบขึ้นใช้งานจริง เพื่อให้มั่นใจว่าระบบมีความถูกต้อง มั่นคงปลอดภัย เชื่อถือได้ พร้อมใช้งาน และมีความยืดหยุ่น | [ไม่มีการกำหนดแนวปฏิบัติไว้เป็นการเฉพาะ] |

| ข้อกำหนด | แนวปฏิบัติ |
|---|---|
| เพียงพอจะรองรับการใช้งานได้ สอดคล้องกับแผนการดำเนินธุรกิจ โดยต้องดำเนินการอย่างน้อย ดังนี้ | |
| (1) มีการกำหนดรายละเอียดความต้องการของระบบ (requirement) และคุณสมบัติทางเทคนิค (technical specification) ของระบบที่พัฒนา ดังนี้<br>(1.1) ความมั่นคงปลอดภัย (security)<br>(1.2) สภาพพร้อมใช้งาน (availability)<br>(1.3) ขีดความสามารถที่รองรับ (capacity) | <u>การออกแบบระบบ</u><br>1. สำนักงานสอบบัญชีควรกำหนดให้หน่วยงานอื่นที่เกี่ยวข้องมีส่วนร่วมในการกำหนดรายละเอียดความต้องการของระบบ<br>2. สำนักงานสอบบัญชีควรจัดทำเอกสารระบุรายละเอียดความต้องการของระบบ (functional requirement และ non-functional requirement) และคุณสมบัติทางเทคนิค (technical specification) ที่ครอบคลุมเรื่อง ดังนี้<br>(1) ความมั่นคงปลอดภัย (security) ตามนโยบายหรือมาตรฐานที่สำนักงานสอบบัญชีกำหนด เช่น การควบคุมการเข้าถึง และการเข้ารหัสข้อมูล เป็นต้น<br>(2) ความพร้อมใช้งาน (availability) เช่น การออกแบบให้มีระบบทดแทน high availability หรือ redundancy รวมถึงมีระบบสำรอง (Disaster Recovery strategy) เป็นต้น เพื่อให้ระบบสามารถทำงานได้อย่างต่อเนื่อง และลดความเสี่ยงที่จุดใดจุดหนึ่งทำให้ระบบเกิดปัญหาหรือล้มเหลวทั้งหมด (single point of failure)<br>(3) ขีดความสามารถที่รองรับ (capacity) ตามอัตรากำลังคนของสำนักงานสอบบัญชีที่วางแผนไว้ในปัจจุบัน<br>ทั้งนี้ เอกสารข้างต้นควรผ่านการสอบทานความถูกต้องครบถ้วนและได้รับอนุมัติจากผู้เกี่ยวข้องก่อนเริ่มพัฒนาระบบ |
| (2) มีการแบ่งแยกบทบาทหน้าที่และความรับผิดชอบของผู้ที่เกี่ยวข้องในการพัฒนาระบบ เพื่อให้มีการสอบทานก่อนนำระบบขึ้นไปให้บริการจริง ทั้งนี้ หากระบบถูกพัฒนาโดยบุคคลภายนอก และมีข้อจำกัดในการแบ่งแยกหน้าที่สำนักงานสอบบัญชีต้องจัดหาการควบคุมอื่นทดแทนเพื่อตอบสนองต่อความเสี่ยงจากการแบ่งแยกหน้าที่ไม่เหมาะสม | <u>การพัฒนาระบบ</u><br>1. สำนักงานสอบบัญชีควรแบ่งแยกบทบาทหน้าที่และความรับผิดชอบของผู้ที่เกี่ยวข้องในการพัฒนาระบบ (segregation of duty) เพื่อให้มีการสอบทานก่อนนำระบบขึ้นไปให้บริการจริง เช่น แยกผู้พัฒนาระบบ ออกจากผู้นำระบบขึ้นใช้งานจริง เป็นต้น |
| (3) มีการแบ่งแยกสภาพแวดล้อมของระบบงานที่ใช้สำหรับการพัฒนา (development) และการทดสอบ (testing) ออกจากระบบงานที่ให้บริการจริง (production) เช่น | 1. สำนักงานสอบบัญชีควรแบ่งแยกสภาพแวดล้อมของระบบงานที่ใช้สำหรับการพัฒนา (development) และการทดสอบ (testing) ออกจากระบบงานที่ให้บริการจริง (production) เพื่อควบคุมการทดสอบและลดผลกระทบที่อาจเกิดขึ้นต่อระบบงานที่ให้บริการจริง<br>2. สำนักงานสอบบัญชีควรจัดให้มีการรักษาความมั่นคงปลอดภัยของเครื่องที่ไม่ได้อยู่บนระบบที่ให้บริการจริง (non-production) ให้เพียงพอกับระดับความเสี่ยงของการเข้าถึงระบบและข้อมูลโดยไม่ได้รับอนุญาต และการรั่วไหลของข้อมูลที่ใช้ทดสอบ<br>3. สำนักงานสอบบัญชีควรจัดให้มีการควบคุมไม่ให้มีการติดตั้งเครื่องมือการพัฒนาระบบ (development tools) และเครื่องมือแปล |

| ข้อกำหนด | แนวปฏิบัติ |
|---|---|
| | โปรแกรม (compilers) ไว้บนระบบที่ให้บริการจริง เพื่อป้องกันความเสี่ยงที่อาจถูกปรับเปลี่ยนหรือติดตั้งโปรแกรมโดยไม่ได้รับอนุญาต |
| (4) มีกระบวนการหรือเครื่องมือควบคุมการพัฒนาชุดคำสั่งคอมพิวเตอร์ให้มีความปลอดภัย เช่น | 1. สำนักงานสอบบัญชีควรกำหนดมาตรฐานและระเบียบวิธีปฏิบัติในการออกแบบและพัฒนาระบบอย่างปลอดภัย (secure coding) สอดคล้องกับมาตรฐานสากล รวมทั้งควบคุมให้ผู้พัฒนาระบบปฏิบัติตามมาตรฐานและระเบียบวิธีปฏิบัติดังกล่าว<br>2. สำนักงานสอบบัญชีควรมีกระบวนการหรือเครื่องมือควบคุมเวอร์ชันของชุดคำสั่งคอมพิวเตอร์ (source code version control)<br>3. สำนักงานสอบบัญชีควรสอบทานคำสั่งในการเขียนโปรแกรม (source code review) โดยใช้ระบบอัตโนมัติ (automated review) หรือแบบ manual review ซึ่งดำเนินการโดยบุคคลที่ไม่ใช่ผู้พัฒนาโปรแกรม เมื่อมีการพัฒนาหรือแก้ไขเปลี่ยนแปลงระบบ IT ที่มีนัยสำคัญ และมีความเสี่ยงด้านความมั่นคงปลอดภัย เพื่อให้สามารถระบุข้อบกพร่องด้านความมั่นคงปลอดภัย และแก้ไขก่อนนำระบบไปใช้งานจริง |
| (5) มีการทดสอบระบบ IT ที่ได้รับการพัฒนาหรือแก้ไขเปลี่ยนแปลง เพื่อให้มั่นใจได้ว่าระบบดังกล่าวสามารถประมวลผลได้อย่างถูกต้องครบถ้วน และเป็นไปตามความต้องการของผู้ใช้งาน | <u>การทดสอบระบบ</u><br>1. สำนักงานสอบบัญชีต้องจัดให้มีการทดสอบระบบก่อนนำไปใช้งานหรือให้บริการจริง เพื่อให้มั่นใจได้ว่าระบบดังกล่าวสามารถทำงานได้อย่างถูกต้อง ปลอดภัย มีประสิทธิภาพ และเป็นไปตามความต้องการของผู้ใช้งาน โดยครอบคลุมอย่างน้อย ดังนี้<br>(1) ทดสอบการทำงานของแต่ละหน่วย (unit test)<br>(2) ทดสอบการทำงานของระบบและการเชื่อมต่อ (system and integration test)<br>(3) ทดสอบความต้องการของผู้ใช้งาน (user acceptance test)<br>(4) ทดสอบการรักษาความปลอดภัย (security test) ได้แก่ การประเมินช่องโหว่ (vulnerabilities assessment) และการทดสอบการเจาะระบบ (penetration test) ตามความจำเป็น สำหรับระบบใหม่ใด ๆ ที่มีการเชื่อมต่อกับระบบ IT ที่มีนัยสำคัญ เพื่อให้สามารถตรวจพบช่องโหว่และดำเนินการปรับปรุงแก้ไขอย่างเหมาะสมก่อนเริ่มให้บริการจริง<br>2. สำนักงานสอบบัญชีควรกำหนดสถานการณ์ที่ใช้ทดสอบ (test scenario) หรือกรณีที่ใช้ทดสอบ (test case) แบบ end-to-end และมีกระบวนการสอบทาน test scenario หรือ test case เพื่อให้มั่นใจว่ามีความครอบคลุมเพียงพอและตรงกับความต้องการของสำนักงานสอบบัญชี<br>3. สำนักงานสอบบัญชีควรทดสอบระบบบนสภาพแวดล้อม (test environment) ที่ใกล้เคียงระบบที่ให้บริการจริง เพื่อลดความเสี่ยงที่อาจเกิดขึ้นจากการเปลี่ยนแปลงบนระบบงานที่ให้บริการจริง<br>4. สำนักงานสอบบัญชีต้องมีการจัดการข้อบกพร่อง (defect) ของระบบที่พบในการทดสอบ โดยพิจารณาแนวทางปรับปรุง หรือลดความเสี่ยงและผลกระทบของข้อบกพร่องดังกล่าว<br>5. สำนักงานสอบบัญชีต้องมีการขออนุมัติผลการทดสอบจากฝ่ายงานที่เกี่ยวข้อง ก่อนนำระบบขึ้นใช้งานจริง |

| ข้อกำหนด | แนวปฏิบัติ |
|---|---|
| (6) มีมาตรการควบคุมความถูกต้องครบถ้วนของการแปลงข้อมูล (data conversion) | 1. มาตรการควบคุมความถูกต้องครบถ้วนของการแปลงข้อมูล (data conversion) ควรครอบคลุมกรณีที่มีการโอนย้ายข้อมูลจากระบบเดิมไปยังระบบใหม่ (data migration) เช่น การทำ storage migration, cloud migration หรือ application migration เป็นต้น |
| (7) มีมาตรการรักษาความมั่นคงปลอดภัย และความลับของข้อมูลสำคัญที่นำไปใช้ในการทดสอบ | 1. กรณีที่มีการนำข้อมูลสำคัญจากระบบจริงมาใช้เพื่อทดสอบระบบ สำนักงานสอบบัญชีควรจัดให้มีแนวทางการรักษาความปลอดภัยและความลับของข้อมูลดังกล่าว เช่น การทำ data masking เป็นต้น เพื่อป้องกันความเสี่ยงในการรั่วไหลของข้อมูล |
| (8) ในกรณีที่มีการมอบให้มอบหมายให้บุคคลภายนอกเป็นผู้พัฒนาหรือแก้ไขเปลี่ยนแปลงระบบ IT สำนักงานสอบบัญชีต้องจัดให้มีการติดตาม และควบคุมการดำเนินการให้ไปตามข้อตกลงในการมอบหมายงาน | [ไม่มีการกำหนดแนวปฏิบัติไว้เป็นการเฉพาะ] |
| (9) มีกระบวนการขออนุมัติหัวหน้าสำนักงานสอบบัญชีหรือคณะกรรมการบริหารของสำนักงานสอบบัญชีก่อนนำระบบขึ้นใช้งานจริง | <u>การนำระบบขึ้นใช้งานจริง</u><br>1. สำนักงานสอบบัญชีควรดำเนินการนำระบบขึ้นใช้งานจริง โดยผ่านกระบวนการบริหารจัดการการเปลี่ยนแปลงที่กำหนดไว้<br>2. สำนักงานสอบบัญชีควรเตรียมความพร้อมในการนำระบบขึ้นใช้งานจริง โดยจัดเก็บระบบเวอร์ชันก่อนการเปลี่ยนแปลงให้พร้อมนำกลับมาใช้งานได้<br>3. สำนักงานสอบบัญชีควรกำหนดแผนหรือเงื่อนไขการนำระบบใหม่เข้าไปทดแทน (cutover หรือ go-live technique) ที่เหมาะสมกับระดับความเสี่ยง เช่น การเปลี่ยนแปลงไปยังระบบใหม่ทันที (direct changeover) การเปลี่ยนแปลงระบบโดยการใช้งานคู่ขนาน (parallel changeover) หรือ การเปลี่ยนแปลงระบบทีละเฟส (phased changeover) เป็นต้น |
| **2.10.4 การแก้ไขเปลี่ยนแปลงระบบ IT (system change)** | |
| <u>10.4 แก้ไขเปลี่ยนแปลงระบบ IT (system change)</u> | 1. การแก้ไขเปลี่ยนแปลงระบบ IT (system change) ควรพิจารณาดำเนินการตามแนวปฏิบัติเรื่องการบริหารจัดการการเปลี่ยนแปลง (change management) และแนวปฏิบัติเรื่องการพัฒนาระบบ |
| (1) มีการประเมินผลกระทบ และจัดลำดับความสำคัญของการเปลี่ยนแปลง | [ไม่มีการกำหนดแนวปฏิบัติไว้เป็นการเฉพาะ] |
| (2) มีกระบวนการขออนุมัติการเปลี่ยนแปลง (change request) โดยต้องได้รับการอนุมัติจากหน่วยงานเจ้าของระบบ (system owner) เป็นลายลักษณ์อักษร เพื่อให้มั่นใจได้ว่า | [ไม่มีการกำหนดแนวปฏิบัติไว้เป็นการเฉพาะ] |

| ข้อกำหนด | แนวปฏิบัติ |
|---|---|
| การเปลี่ยนแปลงได้รับการพิจารณาความจำเป็นอย่างเหมาะสมแล้ว | |
| (3) มีการทดสอบระบบก่อนนำไปตั้งค่า หรือนำไปติดตั้งบนระบบที่ให้บริการจริง เพื่อลดความเสี่ยงและผลกระทบที่อาจเกิดขึ้น | [ไม่มีการกำหนดแนวปฏิบัติไว้เป็นการเฉพาะ] |
| (4) มีกระบวนการขออนุมัติจากหัวหน้าสำนักงานสอบบัญชี หรือคณะกรรมการบริหารของสำนักงานสอบบัญชีก่อนนำระบบขึ้นใช้งานจริง | [ไม่มีการกำหนดแนวปฏิบัติไว้เป็นการเฉพาะ] |
| (5) มีกระบวนการหรือเครื่องมือควบคุมการเปลี่ยนแปลงรุ่น (version) ของชุดคำสั่งคอมพิวเตอร์ (source code version control) และรองรับการถอยกลับสู่สภาพเดิม (fallback) | [ไม่มีการกำหนดแนวปฏิบัติไว้เป็นการเฉพาะ] |
| (6) ปรับปรุงรายละเอียดประกอบระบบงานที่ได้มีการแก้ไขเปลี่ยนแปลงให้เป็นปัจจุบัน | 1. สำนักงานสอบบัญชีควรปรับปรุงขั้นตอนการปฏิบัติงาน ระบบงานสำรอง และแผนบริหารความต่อเนื่องทางธุรกิจ (business continuity plan) เมื่อมีการแก้ไขเปลี่ยนแปลงระบบ IT เพื่อให้เป็นปัจจุบันอยู่เสมอ นอกจากนี้ ควรสื่อสารการเปลี่ยนแปลงให้บุคคลที่เกี่ยวข้องได้รับทราบเพื่อให้สามารถปฏิบัติงานได้อย่างถูกต้อง |
| **2.11 การบริหารจัดการเหตุการณ์ผิดปกติด้าน IT (IT incident management)** | |
| **ส่วนที่ 11 การบริหารจัดการเหตุการณ์ผิดปกติด้าน IT (IT incident management)**<br>สำนักงานสอบบัญชีต้องมีการบริหารจัดการเหตุการณ์ผิดปกติด้าน IT อย่างเหมาะสมและทันท่วงทีดังนี้ | |
| 11.1 จัดให้มีช่องทางรับแจ้งเหตุการณ์ผิดปกติด้าน IT จากบุคลากร ผู้ใช้บริการ และผู้ที่เกี่ยวข้อง | 1. สำนักงานสอบบัญชีควรจัดให้มีหน่วยงานหรือบุคลากรที่มีหน้าที่รับแจ้งเหตุการณ์ (point of contact) โดยทำหน้าที่ในการบันทึกข้อมูลแก้ไขในเบื้องต้น หรือส่งต่อเหตุการณ์ผิดปกติไปยังหน่วยงานด้าน IT ที่เกี่ยวข้อง |
| 11.2 กำหนดแผน หรือขั้นตอนการบริหารจัดการเหตุการณ์ผิดปกติด้าน IT | 1. สำนักงานสอบบัญชีควรจัดให้มีแผนการบริหารจัดการ หรือแผนการรับมือกับเหตุการณ์ผิดปกติ (incident response plan) ตามความสำคัญของเหตุการณ์ เพื่อให้สามารถรับมือและตอบสนองต่อเหตุการณ์ได้อย่างรวดเร็วและทันการณ์ โดยมีรายละเอียด |

| ข้อกำหนด | แนวปฏิบัติ |
|---|---|
| | ครอบคลุมอย่างน้อย ดังนี้<br>(1) การตรวจสอบความถูกต้องข้อมูลที่ได้รับแจ้ง<br>(2) การจัดประเภท และความเร่งด่วนของเหตุการณ์ เพื่อดำเนินการแก้ไขปัญหาภายในระยะเวลาที่เหมาะสม<br>(3) การแก้ไขเหตุการณ์ ได้แก่ การวิเคราะห์ข้อมูล (analysis) การจำกัดความเสียหาย (containment) การจัดเก็บหลักฐานอย่างปลอดภัย (evidence gathering) การหาแนวทางแก้ไข (resolution research) และการแก้ไขปัญหาและฟื้นฟูระบบ (eradication and recovery) ตลอดจนการจัดให้มีช่องทางประสานงานจากผู้เชี่ยวชาญทั้งภายในและภายนอก<br>(4) แนวทางการรายงานเหตุการณ์ผิดปกติ (incident escalation) และรายงานความคืบหน้าของเหตุการณ์ต่อหัวหน้าสำนักงานสอบบัญชี และคณะกรรมการของสำนักงานสอบบัญชีให้รับทราบ ตามระดับความรุนแรงของเหตุการณ์<br>(5) การแจ้งหรือสื่อสารลูกค้า โดยกำหนดผู้รับผิดชอบในการสื่อสารไปยังลูกค้า และช่องทางการสื่อสาร เพื่อให้ลูกค้ารับทราบผลกระทบ และความคืบหน้าการแก้ไขเหตุการณ์ผิดปกติ<br>(6) การตรวจพิสูจน์พยานหลักฐานทางดิจิทัล (digital forensic) ในกรณีภัยคุกคามทางไซเบอร์ซึ่งส่งผลกระทบอย่างมีนัยสำคัญต่อทรัพย์สินและข้อมูลของลูกค้า โดยผู้ที่มีความเชี่ยวชาญเพื่อให้ทราบสาเหตุหรือช่องโหว่ของระบบ และสามารถดำเนินการปิดช่องโหว่ได้อย่างปลอดภัย |
| 11.3 รายงานเหตุการณ์ผิดปกติด้าน IT เหตุการณ์การละเมิดต่อข้อมูลส่วนบุคคล และเหตุการณ์ที่ส่งผลให้ทรัพย์สินของผู้ใช้งานเสียหายอันเกิดจากเหตุการณ์ด้านความมั่นคงปลอดภัยของระบบ IT ต่อผู้มีหน้าที่รับผิดชอบเหตุการณ์ และหน่วยงานที่เกี่ยวข้องโดยไม่ชักช้า ตามที่กฎหมายกำหนด เช่น สำนักงาน ก.ล.ต. และ สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เป็นต้น | 1. สำนักงานสอบบัญชีควรรายงานเหตุการณ์ที่มีการละเมิดกฎหมาย กฎ และระเบียบที่เกี่ยวข้องกับสำนักงานสอบบัญชี ต่อหน่วยงานที่เกี่ยวข้องโดยไม่ชักช้า ตามที่กฎหมายกำหนด เช่น มาตรา 37 (4) ของพรบ.คุ้มครองข้อมูลส่วนบุคคลฯ แจ้งให้รายงานเหตุการณ์ละเมิดข้อมูลส่วนบุคคลแก่สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลภายใน 72 ชั่วโมงนับแต่ทราบเหตุเท่าที่สามารถกระทำได้ ทั้งนี้การแจ้งดังกล่าวและข้อยกเว้นให้เป็นไปตามหลักเกณฑ์และวิธีการที่คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลประกาศกำหนด เป็นต้น รวมทั้ง สำนักงานสอบบัญชีต้องรายงานเหตการณ์ดังกล่าวแก่สำนักงาน ก.ล.ต. ภายใน 72 ชั่วโมงนับแต่ทราบเหตุเท่าที่สามารถกระทำได้ด้วยเช่นกัน ตามหลักเกณฑ์ในการกำกับดูแลและการตรวจสอบด้านIT สำหรับสำนักงานสอบบัญชี<br>2. สำนักงานสอบบัญชีควรรายงานสำนักงาน ก.ล.ต. ในกรณีที่มีเหตุการณ์ด้าน IT ซึ่งอาจส่งผลกระทบต่อการดำเนินงาน ธุรกิจ ชื่อเสียง ฐานะ ผลการดำเนินงานของสำนักงานสอบบัญชี หรือลูกค้าในวงกว้าง โดยครอบคลุมเหตุการณ์ ดังนี้<br>(1) การละเมิดต่อข้อมูลส่วนบุคคลที่เกิดจากเหตุการณ์ผิดปกติด้าน IT<br>(2) ทรัพย์สินของผู้ใช้งานสูญหาย หรือเสียหาย<br>(3) การบุกรุก เข้าถึง หรือใช้งานระบบโดยไม่ได้รับอนุญาต (system compromised)<br>(4) เหตุการณ์ที่ส่งผลกระทบต่อชื่อเสียงของสำนักงานสอบบัญชี (harm to reputation) เช่น ถูกปลอมแปลงหน้าเว็บไซต์ของ |

| ข้อกำหนด | แนวปฏิบัติ |
|---|---|
| | บริษัท (website defacement) เป็นต้น<br>3. สำนักงานสอบบัญชีควรรายงานเหตุการณ์ต่อสำนักงาน ก.ล.ต. ภายในกรอบระยะเวลา ดังนี้<br>(1) รายงานโดยไม่ชักช้า ภายใน 72 ชั่วโมงนับแต่ทราบเหตุเท่าที่สามารถกระทำได้ โดยมีเนื้อหาครอบคลุมถึงวันเวลา ประเภทเหตุการณ์ เหตุการณ์ และผลกระทบที่คาดว่าจะเกิดขึ้น ทั้งนี้ สามารถแจ้งโดยวาจาหรือรายงานผ่านช่องทางอิเล็กทรอนิกส์ตามที่สำนักงาน ก.ล.ต. กำหนดตามความเหมาะสม<br>(2) รายงานความคืบหน้าเป็นลายลักษณ์อักษรทุก ๆ 14 วัน หรือ ตามความเหมาะสมจนกว่าระบบ IT จะกลับสู่การให้บริการได้อย่างเป็นปกติ โดยมีเนื้อหาครอบคลุมถึงวันเวลา ประเภทเหตุการณ์ เหตุการณ์ ผลกระทบที่เกิดขึ้น และความคืบหน้าในการแก้ไขปัญหา ทั้งนี้ ให้รายงานผ่านช่องทางอิเล็กทรอนิกส์ที่สำนักงาน ก.ล.ต. กำหนด<br>(3) รายงานเมื่อเหตุการณ์ยุติหรือแก้ไขปัญหาแล้วเสร็จ โดยมีเนื้อหาครอบคลุมถึงวันเวลา ประเภทเหตุการณ์ เหตุการณ์ ผลกระทบที่เกิดขึ้น การดำเนินการแก้ไขปัญหา ผลการแก้ไขปัญหา ระยะเวลาในการแก้ไข สาเหตุที่เกิดปัญหา และแนวทางป้องกันในอนาคต ทั้งนี้ ให้รายงานผ่านช่องทางอิเล็กทรอนิกส์ที่สำนักงาน ก.ล.ต. กำหนด |
| 11.4 วิเคราะห์สาเหตุที่แท้จริง (root cause) ของเหตุการณ์ผิดปกติด้าน IT เพื่อกำหนดแนวทางการแก้ไขและป้องกันไม่ให้เกิดเหตุการณ์ซ้ำในอนาคต | 1. สำนักงานสอบบัญชีควรวิเคราะห์สาเหตุที่แท้จริงของเหตุการณ์ และนำบทเรียน (lesson learned) จากเหตุการณ์ไปป้องกันไม่ให้เกิดเหตุการณ์นี้อีกในอนาคต หรือปรับปรุงกระบวนการรับมือเหตุการณ์ผิดปกติให้มีประสิทธิภาพดีขึ้น |
| 11.5 บันทึกข้อมูลที่เกี่ยวข้องกับการบริหารจัดการเหตุการณ์ผิดปกติด้าน IT และจัดเก็บข้อมูลดังกล่าวเป็นระยะเวลาไม่น้อยกว่า 5 ปีนับแต่วันที่เกิดเหตุการณ์นั้น โดยต้องจัดเก็บไว้ในลักษณะที่พร้อมให้สำนักงาน ก.ล.ต. สามารถเรียกดูและตรวจสอบได้โดยไม่ชักช้า | 1. สำนักงานสอบบัญชีควรจัดเก็บบันทึกข้อมูลเหตุการณ์ที่เกิดขึ้นในรูปแบบที่เป็นมาตรฐาน และมีเนื้อหาขั้นต่ำประกอบด้วย วันเวลาที่เกิดเหตุการณ์ รายละเอียดเหตุการณ์ ผลกระทบ วิธีการแก้ไข วันเวลาที่สิ้นสุดเหตุการณ์ สาเหตุที่เกิดปัญหา และแนวทางการป้องกันในอนาคต โดยจัดเก็บข้อมูลดังกล่าวเป็นระยะเวลาไม่น้อยกว่า 5 ปีนับแต่วันที่เกิดเหตุการณ์นั้น โดยต้องจัดเก็บไว้ในลักษณะที่พร้อมให้สำนักงาน ก.ล.ต. สามารถเรียกดูและตรวจสอบได้โดยไม่ชักช้า |
| 11.6 ทดสอบและทบทวนขั้นตอนปฏิบัติหรือแผนการบริหารจัดการเหตุการณ์ผิดปกติด้าน IT อย่างน้อยปีละ 1 ครั้ง โดยต้องครอบคลุมถึงการทดสอบการบริหารจัดการเหตุการณ์ด้านภัยคุกคามทางไซเบอร์ (cyber security drill) และจัดให้มีการรายงานผลการทดสอบและทบทวนต่อหัวหน้าสำนักงานสอบบัญชี หรือคณะกรรมการ | 1. สำนักงานสอบบัญชีควรทดสอบและทบทวนขั้นตอนปฏิบัติหรือแผนการบริหารจัดการเหตุการณ์ผิดปกติ อย่างน้อยปีละ 1 ครั้ง เพื่อให้สามารถจัดการแก้ไขเหตุการณ์ให้กลับสู่สภาพปกติได้อย่างรวดเร็วและจำกัดความเสียหายที่ส่งผลกระทบต่อธุรกิจ โดยดำเนินการ ดังนี้<br>(1) จัดให้มีการจำลองสถานการณ์เสี่ยง (risk scenario) ด้านเหตุการณ์ภัยคุกคามทางไซเบอร์ที่มีความเป็นไปได้ที่จะเกิดขึ้น สอดคล้องกับลักษณะ ขอบเขต และความซับซ้อนในการประกอบธุรกิจ และสอดคล้องกับแนวโน้มภัยคุกคามไซเบอร์ที่อาจเกิดขึ้นกับสำนักงานสอบบัญชีโดยสถานการณ์ดังกล่าวควรเป็นสถานการณ์ที่เกิดขึ้นแล้วส่งผลกระทบต่อระบบ IT อย่างมีนัยสำคัญ<br>(2) จัดเก็บเอกสารที่เกี่ยวข้องกับการทดสอบให้ครบถ้วนและเป็นปัจจุบัน ดังนี้ |

| ข้อกำหนด | แนวปฏิบัติ |
|---|---|
| บริหารของสำนักงานสอบบัญชี | (2.1) สถานการณ์ความเสี่ยง (risk scenario) รูปแบบการทดสอบ วัน เวลา สถานที่ในการทดสอบ บทบาทหน้าที่ของผู้ที่เกี่ยวข้องที่ใช้ในการทดสอบ<br>(2.2) สรุปผลการทดสอบ และผลการทบทวนขั้นตอนการบริหารจัดการเหตุการณ์<br>(3) จัดให้มีการรายงานผลการทดสอบและทบทวนต่อหัวหน้าสำนักงานสอบบัญชี หรือคณะกรรมการบริหารของสำนักงานสอบบัญชี |
| **2.12 แผนฉุกเฉินด้าน IT (IT contingency plan)** | |
| **ส่วนที่ 12 แผนฉุกเฉินด้าน IT (IT contingency plan)**<br>สำนักงานสอบบัญชีต้องจัดให้มีแผนฉุกเฉินด้าน IT เพื่อรองรับเหตุการณ์ผิดปกติด้าน IT ซึ่งส่งผลกระทบให้ไม่สามารถให้บริการได้ตามปกติ หรือไม่สามารถดำเนินธุรกิจอย่างต่อเนื่อง โดยต้องกู้คืนระบบให้กลับคืนสู่สภาพปกติภายในระยะเวลาที่เหมาะสมได้ ดังนี้ | ทั้งนี้ หากระบบงาน IT บางอย่างไม่ได้อยู่ในการควบคุมของสำนักงานสอบบัญชี สำนักงานสอบบัญชีต้องกำหนดการควบคุมอื่นทดแทนเพื่อให้มั่นใจได้ว่าระบบงาน IT ดังกล่าว มีแนวทางรองรับเหตุการณ์ผิดปกติด้าน IT ที่อาจส่งผลกระทบให้ไม่สามารถให้บริการได้ตามปกติ หรือไม่สามารถดำเนินธุรกิจอย่างต่อเนื่อง โดยต้องกู้คืนระบบให้กลับคืนสู่สภาพปกติภายในระยะเวลาที่เหมาะสมได้ |
| 12.1 จัดให้มีคณะทำงานหรือหน่วยงานที่รับผิดชอบในการจัดทำแผนฉุกเฉินด้าน IT | 1. สำนักงานสอบบัญชีควรจัดให้มีคณะทำงานหรือหน่วยงานที่รับผิดชอบในการจัดทำแผนฉุกเฉินด้าน IT ไว้อย่างเป็นลายลักษณ์อักษร โดยมีผู้บริหารและบุคลากรของหน่วยงานด้านต่าง ๆ ที่เกี่ยวข้องเข้าร่วมด้วย เช่น ด้าน IT ด้านธุรกิจ และด้านสื่อสารองค์กร เป็นต้น |
| 12.2 กระบวนการจัดทำแผนฉุกเฉินด้าน IT ต้องครอบคลุมการดำเนินการ ดังนี้<br>12.2.1 ประเมินความเสี่ยง (risk analysis) เพื่อให้สามารถระบุเหตุการณ์ความเสี่ยงที่อาจทำให้กระบวนการและระบบ IT หยุดชะงัก ไม่สามารถให้บริการได้ตามปกติ หรือไม่สามารถดำเนินธุรกิจอย่างต่อเนื่อง | สำนักงานสอบบัญชีควรประเมินความเสี่ยง (risk analysis) เพื่อให้สามารถระบุเหตุการณ์ความเสี่ยงซึ่งส่งผลกระทบต่อการหยุดชะงักของกระบวนการและระบบ IT โดยมีแนวทางดำเนินการ ดังนี้<br>1. ระบุเหตุการณ์ความเสี่ยง (risk scenarios) ที่อาจทำให้กระบวนการและระบบ IT หยุดชะงัก ทั้งจากภายในและภายนอก เช่น การโจมตีด้านไซเบอร์ ไฟไหม้ เป็นต้น<br>2. ประเมินความเสี่ยงโดยพิจารณาผลกระทบและโอกาสที่จะเกิดขึ้น รวมถึงการควบคุมที่มีอยู่<br>3. จัดให้มีกระบวนการและทรัพยากรที่จำเป็นในการควบคุมความเสี่ยงให้อยู่ในระดับที่ยอมรับได้ |
| 12.2.2 วิเคราะห์ผลกระทบทางธุรกิจ (business impact analysis) จากเหตุการณ์ความเสี่ยงตาม 12.2.1 เพื่อกำหนดระยะเวลาเป้าหมายในการกู้คืนระบบ IT (Recovery Time Objective : RTO) | 1. สำนักงานสอบบัญชีควรวิเคราะห์ผลกระทบทางธุรกิจ (business impact analysis) เพื่อให้ทราบถึงความสำคัญของระบบ IT ที่มีผลต่อการดำเนินธุรกิจ โดยมีแนวทางการดำเนินการ ดังนี้<br>(1) ระบุรายการกระบวนการทางธุรกิจ (business process) และระบบ IT ที่กระบวนการทางธุรกิจพึ่งพา<br>(2) วิเคราะห์ผลกระทบที่เกิดจากการหยุดชะงักของระบบ IT เพื่อกำหนดระยะเวลา RTO, RPO และ MTD ตามความเหมาะสม |

| ข้อกำหนด | แนวปฏิบัติ |
|---|---|
| ระยะเวลาเป้าหมายสูงสุดที่ยอมให้ข้อมูลเสียหาย (Recovery Point Objective : RPO) และระยะเวลาสูงสุดที่ยอมให้กระบวนการทางธุรกิจหยุดชะงัก (Maximum Tolerable Downtime : MTD) อย่างเหมาะสม | (3) ระบุระบบ IT และทรัพยากรที่จำเป็นต่อกระบวนทางธุรกิจที่สำคัญ (ฮาร์ดแวร์ ซอฟต์แวร์ ข้อมูล และทรัพยากรอื่น ๆ) พร้อมทั้งรายละเอียดคุณสมบัติ (specification) ขั้นต่ำของระบบ IT และทรัพยากรดังกล่าว<br>(4) จัดลำดับความสำคัญของระบบ IT เพื่อให้ระบบ IT ที่สนับสนุนกระบวนการทางธุรกิจที่สำคัญสูงได้รับการกู้คืนเป็นลำดับแรก |
| 12.2.3 จัดทำแผนฉุกเฉินด้าน IT อย่างเป็นลายลักษณ์อักษร ซึ่งได้รับความเห็นชอบจากหัวหน้าสำนักงานสอบบัญชี หรือคณะกรรมการบริหารของสำนักงานสอบบัญชี | 1. สำนักงานสอบบัญชีควรจัดให้มีแผนฉุกเฉินด้าน IT ที่ได้รับความเห็นชอบจากหัวหน้าสำนักงานสอบบัญชี หรือคณะกรรมการบริหารของสำนักงานสอบบัญชีซึ่งมีรายละเอียดของกระบวนการหรือขั้นตอนการปฏิบัติงานที่ชัดเจน เพื่อให้สามารถดำเนินการได้อย่างรวดเร็วและง่ายต่อการปฏิบัติ โดยครอบคลุมรายละเอียดอย่างน้อย ดังนี้<br>(1) หน้าที่ และความรับผิดชอบของผู้บริหารระดับสูง และผู้ที่เกี่ยวข้องในการดำเนินการตามแผน<br>(2) รายละเอียดของระบบ IT เช่น โครงสร้างสถาปัตยกรรม แผนภาพแสดงระบบเครือข่ายสื่อสาร เป็นต้น<br>(3) เงื่อนไขและขั้นตอนในการประกาศใช้แผนฉุกเฉินด้าน IT การตอบสนองต่อเหตุการณ์ฉุกเฉิน และแผนการสื่อสารให้ผู้ที่เกี่ยวข้องรับทราบ<br>(4) ขั้นตอนการกู้คืนระบบและข้อมูล โดยมีรายละเอียดที่ชัดเจนและเพียงพอที่ผู้ปฏิบัติงานสามารถใช้เป็นขั้นตอนปฏิบัติได้อย่างถูกต้อง และเป็นไปตามเป้าหมายเวลาที่กำหนดไว้ โดยอาจจัดทำในรูปแบบรายการตรวจสอบขั้นตอนปฏิบัติ (checklist)<br>(5) ขั้นตอนการตรวจสอบความถูกต้องครบถ้วนของระบบ IT และข้อมูลที่กู้คืน ก่อนกลับสู่การดำเนินกระบวนการทางธุรกิจอย่างปกติ (return to normal)<br>(6) ขั้นตอนการประกาศยกเลิกแผนฉุกเฉินด้าน IT<br>(7) การจัดเก็บแผนฉุกเฉินด้าน IT ไว้ในสถานที่ปลอดภัยและมีความพร้อมใช้งานในสถานที่ปฏิบัติงานหลักและสถานที่สำรอง<br>2. สำนักงานสอบบัญชีควรจัดให้มีรายชื่อของบุคลากรและช่องทางการติดต่อ เพื่อใช้ในการสื่อสารกรณีเกิดภาวะวิกฤตหรือมีเหตุจำเป็นเร่งด่วนได้ |
| 12.3 จัดให้มีระบบ IT สำรอง และทรัพยากรที่จำเป็นเพื่อให้สามารถกู้คืนระบบได้ตามระยะเวลาเป้าหมายที่กำหนดไว้ ทั้งนี้ หากสำนักงานสอบบัญชีมีข้อจำกัดในการจัดให้มีระบบ IT สำรอง หรือ ทรัพยากรที่จำเป็นสำนักงานสอบบัญชีต้องจัดให้มีการควบคุมอื่นทดแทน | 1. สำนักงานสอบบัญชีควรจัดให้มีระบบ IT สำรอง และทรัพยากรที่จำเป็นเพื่อให้สามารถกู้คืนระบบ IT ได้ตามระยะเวลาเป้าหมายที่กำหนดไว้ โดยกรณีที่สำนักงานสอบบัญชีมีศูนย์คอมพิวเตอร์สำรอง ควรระบุรายละเอียดเกี่ยวกับศูนย์คอมพิวเตอร์สำรองให้ชัดเจน เช่น ทรัพยากรที่มี สถานที่ตั้งและแผนที่ เป็นต้น |

| ข้อกำหนด | แนวปฏิบัติ |
|---|---|
| อย่างเหมาะสมตามระดับความเสี่ยงที่อาจทำให้กระบวนการและระบบ IT หยุดชะงัก | |
| 12.4 สื่อสารให้บุคลากรที่เกี่ยวข้องมีความเข้าใจและสามารถปฏิบัติตามแผนฉุกเฉินด้าน IT อย่างเหมาะสม | 1. สำนักงานสอบบัญชีควรสื่อสารแผนฉุกเฉินด้าน IT ให้พนักงานทุกคนที่มีส่วนเกี่ยวข้องกับการปฏิบัติตามแผนฉุกเฉินด้าน IT มีความเข้าใจ และสามารถปฏิบัติตามแผนได้อย่างถูกต้อง |
| 12.5 ทบทวนและทดสอบการปฏิบัติตามแผนฉุกเฉินด้าน IT อย่างน้อยปีละ 1 ครั้ง และเมื่อมีเหตุจำเป็นที่ควรได้รับการทบทวนและทดสอบดังกล่าว โดยรายงานผลการทบทวนและทดสอบต่อหัวหน้าสำนักงานสอบบัญชีหรือคณะกรรมการบริหารของสำนักงานสอบบัญชี | 1. สำนักงานสอบบัญชีควรทบทวน (review) และทดสอบ (test) การปฏิบัติตามแผนฉุกเฉินด้าน IT อย่างน้อยปีละ 1 ครั้ง และเมื่อมีเหตุจำเป็นที่ควรได้รับการทดสอบและทบทวนดังกล่าว เช่น มีการเปลี่ยนแปลงกลยุทธ์ทางธุรกิจ นโยบายการบริหารความเสี่ยงโดยรวม สภาพแวดล้อมของการให้บริการหรือดำเนินธุรกิจ ทรัพยากร หรือโครงสร้างระบบ IT เป็นต้น<br>2. สำนักงานสอบบัญชีควรกำหนดเหตุการณ์ที่ใช้ในการทดสอบประจำปี (test scenario) โดยเป็นเหตุการณ์ที่มีโอกาสที่จะเกิดขึ้นและอาจส่งผลกระทบให้กระบวนการทางธุรกิจที่สำคัญหยุดชะงัก เช่น การหยุดชะงักของระบบ IT ที่สนับสนุนกระบวนการทางธุรกิจที่สำคัญ การหยุดชะงักของผู้ให้บริการภายนอกที่สำคัญ (รวมถึงผู้ให้บริการคลาวด์) และการโจมตีทางไซเบอร์ เป็นต้น<br>3. สำนักงานสอบบัญชีควรรายงานผลการทดสอบแผนฉุกเฉินด้าน IT ต่อหัวหน้าสำนักงานสอบบัญชี หรือคณะกรรมการบริหารของสำนักงานสอบบัญชีโดยมีรายละเอียดอย่างน้อยครอบคลุมวัตถุประสงค์ ขอบเขตการทดสอบสถานการณ์จำลอง ผลการทดสอบ ข้อผิดพลาดและปัญหาหรืออุปสรรคที่พบ พร้อมทั้งแนวทางปรับปรุงแก้ไข |
| 12.6 จัดให้มีรายละเอียดในการติดต่อดังนี้ เพื่อให้สามารถประสานงานในการรายงานเหตุการณ์ผิดปกติด้าน IT หรือขอความช่วยเหลือจากหน่วยงานภายนอกที่เกี่ยวข้องได้อย่างมีประสิทธิภาพ โดยต้องปรับปรุงข้อมูลดังกล่าวให้เป็นปัจจุบันอยู่เสมอ<br>12.6.1 รายชื่อหน่วยงานกำกับดูแลและบุคคลภายนอกที่ให้บริการหรือที่มีการเชื่อมต่อกับระบบ IT ของสำนักงานสอบบัญชี<br>12.6.2 ช่องทางในการติดต่อ และรายชื่อผู้ที่เกี่ยวข้องของหน่วยงานกำกับดูแลหรือบุคคลภายนอกตาม 12.7.1 | [ไม่มีการกำหนดแนวปฏิบัติไว้เป็นการเฉพาะ] |

**หมวดที่ 3 การตรวจสอบด้านเทคโนโลยีสารสนเทศ (Information Technology Audit)**

ให้สำนักงานสอบบัญชีดำเนินการตามที่กำหนดในภาคผนวกนี้

<table>
<tr><th>ข้อกำหนด</th><th>แนวปฏิบัติ</th></tr>
<tr><td>1. <u>การจัดให้มีผู้ตรวจสอบ</u><br>ผู้ตรวจสอบต้องมีลักษณะดังนี้<br>1.1 มีความเป็นอิสระจากผู้ทำหน้าที่ด้าน IT ในระดับ ดังนี้<br>1.1.1 ระดับที่ 1 (first line of defense) : การปฏิบัติงาน<br>1.1.2 ระดับที่ 2 (second line of defense) : การบริหารความเสี่ยงและกำกับดูแลการปฏิบัติตามกฎหมายและหลักเกณฑ์ที่เกี่ยวข้อง<br>1.2 ผู้ตรวจสอบต้องผ่านการรับรองและมีวุฒิบัตรอย่างหนึ่งอย่างใดดังนี้ และมีวุฒิบัตรซึ่งยังไม่สิ้นผล<br>1.2.1 Certified Information Systems Auditor (CISA)<br>1.2.2 Certified Information Security Manager (CISM)<br>1.2.3 Certified Information Systems Security Professional (CISSP)<br>1.2.4 ISO/IEC 27001 Lead Auditor<br>1.2.5 ใบรับรองอื่นตามที่กำหนดเพิ่มเติมบนเว็บไซต์ของสำนักงาน ก.ล.ต.</td><td>[ไม่มีการกำหนดแนวปฏิบัติไว้เป็นการเฉพาะ]</td></tr>
<tr><td>2. <u>การวางแผนและกำหนดขอบเขตการตรวจสอบ</u><br>ทบทวนแผนงานและขอบเขตการตรวจสอบให้สอดคล้องกับความเสี่ยงของสำนักงานสอบบัญชี ตามเกณฑ์ประเมินระดับความเสี่ยงของสำนักงานสอบบัญชี (IT Risk Assessment : “ITRA”)</td><td>[ไม่มีการกำหนดแนวปฏิบัติไว้เป็นการเฉพาะ]</td></tr>
<tr><td>3. <u>การตรวจสอบด้าน IT ตามแผนงานและขอบเขตที่กำหนด</u><br>3.1 จัดให้มีการตรวจสอบและรายงานผลการตรวจสอบด้าน IT ให้สอดคล้องกับความเสี่ยงของสำนักงานสอบบัญชี ตามเกณฑ์ประเมินระดับความเสี่ยงของสำนักงานสอบบัญชี (IT Risk Assessment : “ITRA”) โดยมีรายละเอียดดังนี้
<table>
<tr><td rowspan="2">ระดับของผลกระทบต่อตลาดทุนจากมูลค่าหลักทรัพย์ตามราคาตลาด ณ วันสิ้นปีล่าสุด</td><td colspan="3">ผลการประเมินความซับซ้อนทางเทคโนโลยีสารสนเทศของสำนักงานสอบบัญชี</td></tr>
<tr><td>ต่ำ</td><td>กลาง</td><td>สูง</td></tr>
<tr><td>ระดับสูง (H)</td><td>ทุกปี</td><td>ทุกปี</td><td>ทุกปี</td></tr>
<tr><td>ระดับกลางค่อนไปทางสูง (MH)</td><td>2 ปีครั้ง</td><td>2 ปีครั้ง</td><td>ทุกปี</td></tr>
<tr><td>ระดับกลางค่อนไปทางต่ำ (ML)</td><td>3 ปีครั้ง</td><td>3 ปีครั้ง</td><td>2 ปีครั้ง</td></tr>
<tr><td>ระดับต่ำ (Low)</td><td>3 ปีครั้ง</td><td>3 ปีครั้ง</td><td>3 ปีครั้ง</td></tr>
</table>
</td><td>[ไม่มีการกำหนดแนวปฏิบัติไว้เป็นการเฉพาะ]</td></tr>
</table>

| ข้อกำหนด | แนวปฏิบัติ |
|---|---|
| โดยรอบความถี่ของระยะเวลาที่คำนวณข้างต้น คือ ความถี่ของระยะเวลาที่สำนักงานสอบบัญชีจะต้องจัดให้มีการตรวจสอบด้าน IT แบบเต็มรูปแบบ (“full-scope”) และนำส่งผลการตรวจสอบดังกล่าวแก่สำนักงาน ก.ล.ต. ภายในปีปฏิทินดังกล่าว รวมถึงจัดให้มีการประเมิน ITRA ใหม่เพื่อหารอบระยะเวลาถัดไปที่จะตรวจแบบเต็มรูปแบบอีกครั้ง<br><u>ตัวอย่าง</u> หากสำนักงานสอบบัญชี A ได้จัดให้มีการตรวจสอบด้านเทคโนโลยีครั้งล่าสุดในปี 2569 และจัดทำการประเมินความเสี่ยงตาม ITRA ได้ความถี่ 2 ปีครั้ง ดังนั้น สำนักงานสอบบัญชี A จึงต้องจัดให้มีการตรวจสอบด้านเทคโนโลยีสารสนเทศอีกครั้งภายในปี 2571 รวมถึงรายงานผลการตรวจสอบดังกล่าว และ ITRA ต่อสำนักงาน ก.ล.ต. ภายในปี 2571<br><br>3.2 จัดให้มีการบันทึกและจัดเก็บข้อมูลเกี่ยวกับการตรวจสอบ เช่น กระดาษทำการ (working paper) และหลักฐานประกอบการตรวจ เป็นต้น เป็นระยะเวลาไม่น้อยกว่า 5 ปีนับแต่วันที่จัดทำรายงานและแผนดังกล่าว โดยต้องจัดเก็บไว้ในลักษณะที่พร้อมให้สำนักงาน ก.ล.ต. สามารถเรียกดูและตรวจสอบได้โดยไม่ชักช้า | |
| 4. จัดให้มีการวิเคราะห์เชิงลึกถึงสาเหตุของข้อบกพร่อง (“root cause analysis”) และการจัดทำแผนการแก้ไข (“remediation plan”) ข้อบกพร่องหรือข้อสังเกตจากรายงานผลการตรวจสอบด้าน IT และติดตามความคืบหน้าในการดำเนินการตามแผนดังกล่าว | [ไม่มีการกำหนดแนวปฏิบัติไว้เป็นการเฉพาะ] |
| 5. <u>การเสนอรายงานผลการตรวจสอบ</u><br>5.1 เสนอรายงานผลการตรวจสอบตาม 3. รวมทั้ง root cause analysis และ remediation plan ต่อหัวหน้าสำนักงานสอบบัญชี หรือคณะกรรมการบริหารของสำนักงานสอบบัญชี**ภายใน 30 วัน** หลังวันสุดท้ายที่สิ้นสุดการตรวจสอบ<br>5.2 นำส่งรายงานผลการตรวจสอบ รวมถึง root cause analysis และ remediation plan ที่ผ่านการพิจารณาจากหัวหน้าสำนักงานสอบบัญชี หรือคณะกรรมการบริหารของสำนักงานสอบบัญชีตาม 5.1 รวมถึง ITRA ที่ประเมินใหม่ในปีนั้น ต่อสำนักงาน ก.ล.ต. ตามรูปแบบและวิธีการที่กำหนดไว้บนเว็บไซต์ของสำนักงาน ก.ล.ต. **ภายใน 90 วัน** หลังจากวันที่เสนอรายงานและแผนดังกล่าวต่อหัวหน้าสำนักงานสอบบัญชี หรือคณะกรรมการบริหารของสำนักงานสอบบัญชี<br>5.3 จัดเก็บรายงานผลการตรวจสอบ รวมถึง root cause analysis และ remediation plan เป็นระยะเวลาไม่น้อยกว่า 5 ปีนับแต่วันที่จัดทำรายงานและแผนดังกล่าว โดยต้องจัดเก็บไว้ในลักษณะที่พร้อมให้สำนักงาน ก.ล.ต. สามารถเรียกดูและตรวจสอบได้โดยไม่ชักช้า | ตัวอย่างการนับเวลารายงานผลการตรวจสอบต่อสำนักงาน ก.ล.ต. เช่น<br>สำนักงานสอบบัญชี A มีการว่าจ้างผู้เชี่ยวชาญมาตรวจสอบด้านเทคโนโลยีสารสนเทศ (Information Technology Audit) และเสร็จสิ้น field work ณ วันที่ 31 พฤษภาคม 2571<br>● ผู้รับผิดชอบรายงานผลการตรวจสอบ root cause analysis และ remediation plan ต่อหัวหน้าสำนักงานสอบบัญชี หรือคณะกรรมการบริหารของ |

| ข้อกำหนด | แนวปฏิบัติ |
| --- | --- |
| | สำนักงานสอบบัญชี ภายในวันที่ 30 มิถุนายน 2571<br>● สำนักงานสอบบัญชี A นำส่งรายงานผลการตรวจสอบ root cause analysis และ remediation plan ที่ผ่านการเห็นชอบจากหัวหน้าสำนักงานสอบบัญชี หรือคณะกรรมการบริหารของสำนักงานสอบบัญชี รวมถึง ITRA ที่ประเมินใหม่ในปีนั้นต่อสำนักงาน ก.ล.ต. ภายในวันที่ 28 กันยายน 2571<br>หมายเหตุ: หากตรงกับวันหยุดราชการ ให้นำส่งวันทำการถัดไปแทน |