

ภาคผนวก 1 ของประกาศแนวปฏิบัติ ที่ นป. /2567

การกำกับดูแลและการตรวจสอบด้านเทคโนโลยีสารสนเทศ
(Information Technology) สำหรับสำนักงานสอบบัญชี

สารบัญ

หน้า

หมวดที่ 1 การกำกับดูแลและบริหารจัดการด้านเทคโนโลยีสารสนเทศ (Information Technology Governance)	4
1.1 บทบาทหน้าที่และความรับผิดชอบของหัวหน้าสำนักงานสอบบัญชี หรือคณะกรรมการบริหารของสำนักงานสอบบัญชี	4
1.2 โครงสร้างการกำกับดูแล	6
1.3 นโยบายที่เกี่ยวข้องกับการกำกับดูแลความเสี่ยงด้าน IT.....	7
หมวดที่ 2 การรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (Information Technology Security).....	13
2.1 โครงสร้างการบริหารงานเพื่อการรักษาความมั่นคงปลอดภัยด้าน IT (organization of information technology security)	13
2.2 การบริหารจัดการบุคลากร และบุคคลภายนอก	13
2.2.1 การบริหารจัดการบุคลากร.....	13
2.2.2 การบริหารจัดการบุคคลภายนอก (third-party management) (ถ้ามี)	15
2.3 การบริหารจัดการทรัพย์สินด้าน IT (IT asset management).....	20
2.4 การรักษาความมั่นคงปลอดภัยของข้อมูล (data security)	22
2.5 การควบคุมการเข้าถึงข้อมูลและระบบงาน IT (access control).....	24
2.6 การควบคุมการเข้ารหัส (cryptographic control) (ถ้ามี).....	27
2.7 การรักษาความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อม (physical and environmental security)	29
2.8 การรักษาความมั่นคงปลอดภัยในการปฏิบัติงานด้าน IT (IT operations security).....	30
2.8.1 การบริหารจัดการการตั้งค่าระบบ (system configuration management).....	30
2.8.2 การบริหารจัดการการเปลี่ยนแปลง (change management)	31
2.8.3 การบริหารจัดการขีดความสามารถของระบบงาน IT (capacity management).....	32
2.8.4 การรักษาความมั่นคงปลอดภัยของเครื่องแม่ข่าย (server) และอุปกรณ์ที่ใช้ปฏิบัติงาน (endpoint).....	32
2.8.5 การรักษาความปลอดภัยสำหรับการปฏิบัติงานจากเครื่องข่ายภายนอก (teleworking) การใช้งานอุปกรณ์เคลื่อนที่ (mobile device) และการใช้งานอุปกรณ์ส่วนตัว (bring your own device : BYOD).....	33
2.8.6 การสำรองข้อมูล (data backup).....	34
2.8.7 การจัดเก็บข้อมูลบันทึกเหตุการณ์การใช้งานเกี่ยวกับระบบงาน IT (log).....	35
2.8.8 การติดตามดูแลระบบและเฝ้าระวังภัยคุกคามทางไซเบอร์ (security monitoring)	36
2.8.9 การประเมินช่องโหว่ทางเทคนิค (technical vulnerability assessment) (ถ้ามี).....	36
2.8.10 การบริหารจัดการโปรแกรมแก้ไขช่องโหว่ (patch management).....	36
2.9 การรักษาความมั่นคงปลอดภัยเกี่ยวกับระบบเครือข่ายสื่อสาร (communication system security)	37

2.10	การบริหารจัดการโครงการด้าน IT (IT project management) และการจัดหา พัฒนา และบำรุงรักษาระบบงาน IT (system acquisition, development and maintenance) (ถ้ามี).....	38
2.10.1	การบริหารจัดการโครงการด้าน IT (IT project management).....	39
2.10.2	การจัดหาระบบงาน IT (system acquisition).....	41
2.10.3	การพัฒนาระบบงาน IT (system development).....	41
2.10.4	การแก้ไขเปลี่ยนแปลงระบบงาน IT (system change).....	44
2.11	การบริหารจัดการเหตุการณ์ผิดปกติด้าน IT (IT incident management).....	45
2.12	แผนฉุกเฉินด้าน IT (IT contingency plan).....	48
	หมวดที่ 3 การตรวจสอบด้านเทคโนโลยีสารสนเทศ (Information Technology Audit).....	51
	คำจำกัดความ	55

หมวดที่ 1 การกำกับดูแลและบริหารจัดการด้านเทคโนโลยีสารสนเทศ (Information Technology Governance)

ข้อกำหนด	แนวปฏิบัติ
1.1 บทบาทหน้าที่และความรับผิดชอบของหัวหน้าสำนักงานสอบบัญชี หรือคณะกรรมการบริหารของสำนักงานสอบบัญชี	
<p>ส่วนที่ 1 บทบาทหน้าที่และความรับผิดชอบของหัวหน้าสำนักงานสอบบัญชี หรือคณะกรรมการบริหารของสำนักงานสอบบัญชี</p> <p>หัวหน้าสำนักงานสอบบัญชี หรือคณะกรรมการบริหารของสำนักงานสอบบัญชีต้องควบคุมดูแลและบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ (“ระบบงาน IT”) ให้สอดคล้องกับระดับความเสี่ยงที่สำนักงานสอบบัญชียอมรับได้ โดยคำนึงถึงการบริหารและจัดการความเสี่ยงขององค์กร (enterprise risk) ซึ่งอย่างน้อยต้องครอบคลุมในเรื่องดังนี้</p>	
<p>1.1 การกำหนดกรอบการกำกับดูแลด้าน IT (IT governance framework) และการกำกับดูแลแผนงานด้าน IT ให้สอดคล้องกับแผนธุรกิจ และมีความเหมาะสมเพียงพอที่จะรองรับการเปลี่ยนแปลงด้าน IT และการเปลี่ยนแปลงการดำเนินธุรกิจในอนาคต</p>	<p>1. สำนักงานสอบบัญชีควรกำหนดกรอบการกำกับดูแลด้าน IT (IT governance framework) ที่ครอบคลุมรายละเอียดดังนี้</p> <p>(1) โครงสร้างการกำกับดูแล บทบาทหน้าที่และความรับผิดชอบของหัวหน้าสำนักงานสอบบัญชี หรือคณะกรรมการบริหารของสำนักงานสอบบัญชี และฝ่ายงานที่เกี่ยวข้อง สำหรับการกำกับดูแลด้าน IT ของสำนักงานสอบบัญชี</p> <p>(2) กระบวนการที่เกี่ยวข้องกับการกำกับดูแลด้าน IT อย่างน้อยให้ครอบคลุม</p> <p>(2.1) การจัดทำและขออนุมัติแผนงานด้าน IT</p> <p>(2.2) การจัดทำแผนและและการบริหารจัดการทรัพยากรด้าน IT</p> <p>(2.3) การติดตามและรายงานผลการดำเนินการด้าน IT</p> <p>2. สำนักงานสอบบัญชีควรจัดให้มีแผนงานด้าน IT ประจำปี เพื่อให้การใช้ IT สอดรับกับกลยุทธ์ในการดำเนินธุรกิจ</p>
<p>1.2 การจัดสรรทรัพยากรทางด้าน IT และทรัพยากรบุคคลที่ปฏิบัติงานด้าน IT ให้มีความเหมาะสมเพียงพอต่อการดำเนินธุรกิจ</p>	<p>สำนักงานสอบบัญชีควรจัดสรรทรัพยากรทางด้าน IT และทรัพยากรบุคคลที่ปฏิบัติงานด้าน IT ให้สอดคล้องกับเป้าหมายตามภารกิจ กลยุทธ์ นโยบาย และแผนการดำเนินงานที่กำหนดไว้</p>

ข้อกำหนด	แนวปฏิบัติ
1.3 การกำหนดนโยบายที่เกี่ยวข้องกับการกำกับดูแลความเสี่ยงด้าน IT อย่างเป็นลายลักษณ์อักษร โดยอย่างน้อยต้องครอบคลุมนโยบายตามที่กำหนดในหมวดที่ 1 ส่วนที่ 2 ข้อ 2.2.1 และ 2.2.2	<p>หากสำนักงานสอบบัญชีพิจารณาเรื่องการบริหารจัดการความเสี่ยงด้าน IT ตามหมวดที่ 1 ส่วนที่ 2 ข้อ 2.2.1 แล้วพบว่าสำนักงานสอบบัญชีไม่มีกิจกรรมที่อาจจะก่อให้เกิดความเสี่ยงด้าน IT ในหัวข้อเรื่องที่ระบุไว้ในหมวดที่ 1 ส่วนที่ 2 ข้อ 2.2.2 ดังนี้</p> <ul style="list-style-type: none">(2) เฉพาะเรื่องการบริหารจัดการบุคคลภายนอก(6) การควบคุมการเข้ารหัส (cryptographic control)(8) เฉพาะเรื่องการประเมินช่องโหว่ทางเทคนิค (technical vulnerability assessment)(10) การบริหารจัดการโครงการด้าน IT และการจัดหา พัฒนา และบำรุงรักษาระบบงาน IT <p>สำนักงานสอบบัญชีสามารถยกเว้นการกำหนดนโยบายการกำกับดูแลความเสี่ยงด้าน IT ในเรื่องนั้น ๆ ได้</p> <p>ทั้งนี้ หากสำนักงานสอบบัญชีมีกิจกรรมที่อาจจะก่อให้เกิดความเสี่ยงด้าน IT แต่มีข้อจำกัดในการดำเนินการตามหลักเกณฑ์และแนวปฏิบัติฉบับนี้ สำนักงานสอบบัญชีจำเป็นต้องหาวิธีการควบคุมอื่นทดแทน เพื่อลดระดับความเสี่ยงดังกล่าวให้อยู่ในระดับที่ยอมรับได้</p> <p>อย่างไรก็ดี สำนักงานสอบบัญชีควรทบทวนความเหมาะสมของนโยบายดังกล่าวทุกปีเพื่อให้สอดคล้องกับความเสี่ยงของสำนักงานสอบบัญชีในปัจจุบัน</p>
1.4 การกำหนดขั้นตอนและวิธีปฏิบัติงานในการบริหารจัดการความเสี่ยงด้าน IT และการรักษาความมั่นคงปลอดภัยด้าน IT เพื่อให้เป็นไปตามนโยบายในข้อ 1.3 รวมถึงกำกับดูแลให้มีการนำไปปฏิบัติอย่างเหมาะสม	[ไม่มีการกำหนดแนวปฏิบัติไว้เป็นการเฉพาะ]
1.5 การสร้างความรู้และความตระหนักด้านความเสี่ยงด้าน IT แก่บุคลากรอย่างต่อเนื่องและมีประสิทธิผล	[ไม่มีการกำหนดแนวปฏิบัติไว้เป็นการเฉพาะ]
1.6 การติดตาม ตรวจสอบ และรายงานผลการปฏิบัติงานเพื่อให้เป็นไปตามนโยบายในข้อ 1.3 ต่อหัวหน้าสำนักงานสอบบัญชี หรือคณะกรรมการบริหารของสำนักงานสอบบัญชี โดยมีการรายงานอย่างน้อยปีละ 1 ครั้ง และในกรณีที่มีเหตุการณ์หรือการเปลี่ยนแปลงใด ๆ ซึ่งอาจส่งผลกระทบต่ออย่างมีนัยสำคัญต่อการปฏิบัติงานเพื่อให้	<ol style="list-style-type: none">1. สำนักงานสอบบัญชีควรจัดให้มีกระบวนการติดตาม ตรวจสอบ และควบคุมการจัดทำรายงานผลการปฏิบัติงานเพื่อให้มั่นใจว่าสามารถจัดทำรายงานได้อย่างครบถ้วนถูกต้อง2. สำนักงานสอบบัญชีควรกำหนดให้การรายงานผลการปฏิบัติตามนโยบายที่เกี่ยวข้องกับการกำกับดูแลและบริหารจัดการความเสี่ยงด้าน IT ต่อหัวหน้าสำนักงานสอบบัญชี หรือคณะกรรมการบริหารของสำนักงานสอบบัญชี มีเนื้อหาครอบคลุมถึงเรื่องดังนี้

ข้อกำหนด	แนวปฏิบัติ
<p>เป็นไปตามนโยบายดังกล่าว ต้องมีการรายงานให้หัวหน้าสำนักงานสอบบัญชี หรือคณะกรรมการบริหารของสำนักงานสอบบัญชีทราบ โดยไม่ชักช้าด้วย</p>	<ol style="list-style-type: none"> (1) ผลการประเมินความเสี่ยงด้าน IT การติดตามความเสี่ยง และแนวทางการควบคุมที่เกี่ยวข้อง โดยหน่วยงานที่ทำหน้าที่บริหารความเสี่ยงด้าน IT หรือหน่วยงานที่เกี่ยวข้อง (2) ผลการปฏิบัติตามกฎระเบียบ ข้อบังคับ หรือนโยบายการรักษาความมั่นคงปลอดภัยด้าน IT ในภาพรวมขององค์กร โดยหน่วยงานที่ทำหน้าที่กำกับดูแลการปฏิบัติงานด้าน IT หรือหน่วยงานที่เกี่ยวข้อง (3) ผลการตรวจสอบด้าน IT (IT audit) และความคืบหน้าในการดำเนินการแก้ไขข้อบกพร่อง โดยหน่วยงานที่ทำหน้าที่ตรวจสอบด้าน IT หรือหน่วยงานที่เกี่ยวข้อง (4) ผลการปฏิบัติงานด้าน IT ที่สำคัญ เช่น <ol style="list-style-type: none"> (4.1) เหตุการณ์ผิดปกติ หรือปัญหาด้าน IT ที่สำคัญ (4.2) ความเพียงพอของทรัพยากรด้าน IT (capacity and system utilization) (4.3) ความคืบหน้าของโครงการด้าน IT ในภาพรวม และโครงการที่สำคัญ (4.4) การปฏิบัติงานด้าน IT ของบุคคลภายนอก เช่น ผลการดำเนินการตามข้อตกลงการให้บริการ (service level agreement) เป็นต้น (4.5) ผลการทดสอบแผนฉุกเฉินด้าน IT และการใช้งานแผน (ถ้ามี)
<p>1.2 โครงสร้างการกำกับดูแล</p>	
<p>ส่วนที่ 2 การกำกับดูแลและบริหารจัดการความเสี่ยงด้าน IT ในระดับองค์กร</p> <p>2.1 สำนักงานสอบบัญชีต้องจัดให้มีโครงสร้างการกำกับดูแลและบริหารจัดการความเสี่ยงด้าน IT โดยอย่างน้อยต้องมีลักษณะดังนี้</p> <p>2.1.1 ทำให้เกิดการถ่วงดุลอย่างเป็นอิสระ</p> <p>2.1.2 สอดคล้องตามหลักการแบ่งแยกหน้าที่ 3 ระดับ (3 Lines of Defense: 3 LoDs) โดยมีการแบ่งแยกหน้าที่อย่างชัดเจนระหว่างการทำหน้าที่ด้าน IT ดังนี้</p> <p>ระดับที่ 1 (first line of defense): การปฏิบัติงาน</p> <p>ระดับที่ 2 (second line of defense): การบริหารความเสี่ยงที่เกี่ยวข้องกับระบบงาน IT</p>	<p>สำนักงานสอบบัญชีควรจัดให้มีโครงสร้างการกำกับดูแลและบริหารจัดการความเสี่ยงด้าน IT ที่มีการถ่วงดุลอำนาจ (check and balance) และมีการแบ่งแยกหน้าที่ (segregation of duties) อย่างเหมาะสม ตามหลักการแบ่งแยกหน้าที่ 3 ระดับ ได้แก่</p> <ol style="list-style-type: none"> (1) การปฏิบัติงาน (first line of defense) หมายถึง หน่วยงาน หรือ บุคลากรที่ปฏิบัติงานด้าน IT และผู้ใช้ระบบงาน IT ปฏิบัติงาน <ol style="list-style-type: none"> (1.1) หน่วยงาน หรือ บุคลากรที่ปฏิบัติงานด้าน IT มีหน้าที่ปฏิบัติงานตามหน้าที่ความรับผิดชอบ ประเมินความเสี่ยงและควบคุมความเสี่ยงด้าน IT ติดตามและรายงานการปฏิบัติงานด้าน IT ต่อหัวหน้าสำนักงานสอบบัญชี หรือคณะกรรมการบริหารของสำนักงานสอบบัญชีที่ได้รับมอบหมาย (1.2) ผู้ที่ใช้ระบบงาน IT ปฏิบัติงาน มีหน้าที่ปฏิบัติตามนโยบายและระเบียบปฏิบัติที่เกี่ยวข้องกับความมั่นคงปลอดภัยด้าน IT รวมทั้งมีส่วนร่วมรับผิดชอบในการประเมินและจัดการความเสี่ยงด้าน IT ที่เกี่ยวข้องกับการใช้งานระบบ (2) การบริหารความเสี่ยงที่เกี่ยวข้องกับระบบงาน IT (second line of defense) หมายถึง หน่วยงาน หรือ บุคลากรที่บริหารความเสี่ยงด้าน IT (IT risk function) มีหน้าที่กำหนดกรอบนโยบาย และกระบวนการบริหารความเสี่ยงด้าน IT สนับสนุนให้มี

ข้อกำหนด	แนวปฏิบัติ
<p>ระดับที่ 3 (third line of defense): การตรวจสอบ</p>	<p>การประเมินความเสี่ยงเป็นไปตามกรอบการบริหารความเสี่ยงที่กำหนด พร้อมทั้งให้คำปรึกษา ติดตามความเสี่ยง และทบทวน การควบคุมความเสี่ยงด้าน IT ให้อยู่ในระดับความเสี่ยงที่ยอมรับได้ โดยมีการรวบรวมและเชื่อมโยงความเสี่ยงด้าน IT กับ ความเสี่ยงด้านอื่น และนำเสนอผลการบริหารความเสี่ยงต่อหัวหน้าสำนักงานสอบบัญชี หรือคณะกรรมการบริหารของ สำนักงานสอบบัญชีที่ได้รับมอบหมาย</p> <p>(3) การตรวจสอบด้าน IT (third line of defense) หมายถึง หน่วยงาน หรือบุคลากรที่ทำหน้าที่ตรวจสอบด้าน IT ซึ่งมีหน้าที่ใน การตรวจสอบการปฏิบัติงานของหน่วยงานที่ทำหน้าที่ first line และ second line of defense เพื่อให้มั่นใจว่าการปฏิบัติ ตามนโยบาย มาตรฐาน และกฎหมายทางด้าน IT ที่เกี่ยวข้อง หน่วยงาน หรือบุคลากรในระดับนี้อาจเป็นผู้ตรวจสอบภายใน หรือผู้ตรวจสอบภายนอกผู้ซึ่งมีความเป็นอิสระจากหน่วยงานที่ทำหน้าที่ first line และ second line of defense</p>
<p>1.3 นโยบายที่เกี่ยวข้องกับการกำกับดูแลความเสี่ยงด้าน IT</p>	
<p>ส่วนที่ 2 การกำกับดูแลและบริหารจัดการความเสี่ยงด้าน IT ในระดับองค์กร</p> <p>2.2 สำนักงานสอบบัญชีต้องจัดให้มีนโยบายที่เกี่ยวข้องกับการกำกับ ดูแลความเสี่ยงด้าน IT เป็นลายลักษณ์อักษร โดยต้องได้รับความเห็นชอบจากหัวหน้าสำนักงานสอบบัญชี หรือคณะกรรมการ บริหารของสำนักงานสอบบัญชี หรือคณะกรรมการที่ได้รับมอบหมาย จากหัวหน้าสำนักงานสอบบัญชี ดังนี้</p>	
<p>2.2.1 <u>นโยบายการบริหารจัดการความเสี่ยงด้าน IT (IT risk management policy)</u> มีเรื่องที่ต้องครอบคลุม ดังนี้</p> <p>(1) บทบาทหน้าที่ของผู้ที่เกี่ยวข้องในการบริหาร จัดการความเสี่ยงด้าน IT</p> <p>(2) การจัดให้มีกระบวนการบริหารจัดการความเสี่ยง ด้าน IT เพื่อให้อยู่ในระดับที่องค์กรยอมรับได้</p>	<p>กระบวนการบริหารจัดการความเสี่ยงด้าน IT ควร มีรายละเอียดและจัดทำเป็นลายลักษณ์อักษร ดังนี้</p> <ol style="list-style-type: none"> 1. เกณฑ์ความเสี่ยง (risk criteria) ควรครอบคลุมถึงโอกาสหรือความถี่ที่จะเกิดเหตุการณ์ความเสี่ยง และความมีนัยสำคัญหรือ ผลกระทบที่จะเกิดขึ้นเพื่อจัดลำดับความสำคัญในการบริหารจัดการความเสี่ยง 2. ระดับความเสี่ยงที่ยอมรับได้ (IT risk appetite) ควรผ่านการพิจารณาโดยคณะกรรมการบริหารความเสี่ยง (ถ้ามี) และได้รับการอนุมัติจากหัวหน้าสำนักงานสอบบัญชี หรือคณะกรรมการบริหารของสำนักงานสอบบัญชี ทั้งนี้ ระดับความเสี่ยงที่ยอมรับ ได้ควรสอดคล้องกับการบริหารและจัดการความเสี่ยงขององค์กร (enterprise risk management) (ถ้ามี)

ข้อกำหนด	แนวปฏิบัติ
	<p>3. การประเมินความเสี่ยง (risk assessment) ควรมีการประเมินความเสี่ยงอย่างน้อยปีละ 1 ครั้ง และเมื่อมีการเปลี่ยนแปลงระบบงาน IT อย่างมีนัยสำคัญ¹ โดยมีกระบวนการครอบคลุมอย่างน้อย ดังนี้</p> <ul style="list-style-type: none">(1) การระบุความเสี่ยง (risk identification) จัดให้มีการระบุเหตุการณ์ความเสี่ยง (risk scenario) ด้าน IT ที่อาจจะเกิดขึ้นหรือที่เคยเกิดขึ้นจริงกับสำนักงาน สอบบัญชีเอง หรือเกิดกับผู้อื่นที่ใช้งานเทคโนโลยีในลักษณะเดียวกัน รวมถึงภัยคุกคามทางไซเบอร์และช่องโหว่ต่าง ๆ ที่ส่งผลกระทบต่อการดำเนินธุรกิจ โดยเหตุการณ์ความเสี่ยงดังกล่าวอาจมีสาเหตุมาจากปัจจัยภายใน (internal factor) เช่น มีการเปลี่ยนแปลงกระบวนการปฏิบัติงาน ระบบงาน บุคลากร เป็นต้น รวมถึงปัจจัยภายนอกอื่น ๆ (external factor) เช่น การปฏิบัติตามกฎหมาย การใช้บริการ การเชื่อมต่อ หรือการเข้าถึงข้อมูลจากบุคคลภายนอก เป็นต้น รวมถึงให้นำข้อสังเกตที่ได้จากการตรวจสอบรอบก่อน โดยผู้ตรวจสอบด้านเทคโนโลยีสารสนเทศที่มีคุณสมบัติตามหมวดที่ 3 ข้อที่ 1 มาประกอบการพิจารณาในการระบุความเสี่ยงด้วย(2) การวิเคราะห์ความเสี่ยง (risk analysis) จัดให้มีการวิเคราะห์ความเสี่ยงด้าน IT เพื่อหาแนวทางในการจัดการความเสี่ยงอย่างเหมาะสม โดยครอบคลุมการดำเนินการอย่างน้อย ดังนี้<ul style="list-style-type: none">(2.1) กำหนดผู้รับผิดชอบต่อความเสี่ยง หรือเจ้าของความเสี่ยง (risk owner)(2.2) ระบุการควบคุมที่มีอยู่ในปัจจุบัน (existing control)(2.3) วิเคราะห์โอกาสหรือความถี่ที่จะเกิดเหตุการณ์ความเสี่ยง (likelihood) และความมีนัยสำคัญหรือผลกระทบที่จะเกิดขึ้น (potential impact) จากเหตุการณ์ดังกล่าว(3) การประเมินค่าความเสี่ยง (risk evaluation) จัดให้มีการประเมินค่าความเสี่ยงด้าน IT เพื่อจัดลำดับในการบริหารความเสี่ยงอย่างเหมาะสม โดยครอบคลุมการดำเนินการอย่างน้อย ดังนี้<ul style="list-style-type: none">(3.1) ประเมินผลลัพธ์ที่ได้จากการวิเคราะห์ความเสี่ยง ได้แก่ ค่าโอกาสและผลกระทบ (likelihood และ potential impact) กับเกณฑ์ความเสี่ยง (risk criteria) ที่กำหนดไว้ เพื่อระบุระดับค่าความเสี่ยงของแต่ละเหตุการณ์ ความเสี่ยงด้าน IT

¹ อ้างอิงจากหลักเกณฑ์การประเมินระดับความเสี่ยงด้านเทคโนโลยีสารสนเทศของสำนักงานสอบบัญชี (IT Risk Assessment: ITRA) หัวข้อแนวปฏิบัติสำหรับปีสำหรับสำนักงานสอบบัญชีไม่ได้ถูกกำหนดให้ดำเนินการตรวจแบบ full-scope

ข้อกำหนด	แนวปฏิบัติ
	<p>(3.2) จัดลำดับความเสี่ยงด้าน IT</p> <p>4. การจัดการความเสี่ยง (risk treatment) ควรกำหนดให้มีแนวทางในการจัดการความเสี่ยงด้าน IT อย่างเหมาะสมและสอดคล้องกับผลการประเมินความเสี่ยง (risk assessment) เพื่อให้ความเสี่ยงที่เหลืออยู่ (residual risk) อยู่ในระดับความเสี่ยงที่ยอมรับได้ (risk appetite) โดยครอบคลุมการดำเนินการอย่างน้อย ดังนี้</p> <ol style="list-style-type: none">(1) การกำหนดแนวทางในการจัดการความเสี่ยง โดยพิจารณาถึงความคุ้มค่าและวิธีการที่เหมาะสมกับสำนักงานสอบบัญชี เช่น การหยุดหรือหลีกเลี่ยงความเสี่ยง (risk avoidance) การลดหรือบรรเทาความเสี่ยง (risk mitigation) การโอนย้ายความเสี่ยงให้กับผู้อื่น (risk transference) และการยอมรับความเสี่ยงโดยการเสนอเหตุผลต่อหัวหน้าสำนักงานสอบบัญชี หรือคณะกรรมการบริหารของสำนักงานสอบบัญชี เพื่อตัดสินใจ (risk acceptance) เป็นต้น(2) การระบุรายละเอียดของงานที่ต้องดำเนินการ ผู้รับผิดชอบ และระยะเวลาที่ใช้ในการดำเนินการ(3) การประเมินระดับค่าความเสี่ยงที่เหลืออยู่ (residual risk) ว่าอยู่ในระดับความเสี่ยงที่ยอมรับได้(4) การขออนุมัติแผนการบริหารจัดการความเสี่ยงจากหัวหน้าสำนักงานสอบบัญชี หรือคณะกรรมการบริหารของสำนักงานสอบบัญชีที่ได้รับมอบหมาย(5) การสื่อสารแผนการบริหารจัดการความเสี่ยงให้ผู้ที่เกี่ยวข้องรับทราบ <p>5. การจัดทำทะเบียนความเสี่ยง (risk register) ควรจัดทำมีทะเบียนความเสี่ยง (risk register) เพื่อบันทึกผลการประเมินความเสี่ยง และแนวทางในการจัดการความเสี่ยง โดยมีตัวอย่างรายละเอียด ดังนี้</p> <ol style="list-style-type: none">(1) วันที่ประเมินความเสี่ยง(2) รายละเอียดเหตุการณ์ความเสี่ยง(3) โอกาสหรือความถี่ที่จะเกิดเหตุการณ์ความเสี่ยง (likelihood)(4) ความมีนัยสำคัญหรือผลกระทบที่จะเกิดขึ้น (potential impact)(5) ระดับค่าความเสี่ยงก่อนการควบคุม (inherent risk)(6) แนวทางจัดการความเสี่ยง (risk treatment)(7) เจ้าของความเสี่ยง (risk owner)(8) ระดับความเสี่ยงที่เหลืออยู่ (residual risk)(9) สถานะของการจัดการความเสี่ยง (status of risk treatment)

ข้อกำหนด	แนวปฏิบัติ
	<p>6. การติดตามและทบทวนความเสี่ยง (risk monitor and review) ควรจัดให้มีกระบวนการติดตามและทบทวนความเสี่ยงด้าน IT โดยครอบคลุมการดำเนินการดังนี้</p> <ul style="list-style-type: none">(1) การกำหนดผู้รับผิดชอบในการติดตามและทบทวนความเสี่ยง(2) การกำหนดดัชนีชี้วัดความเสี่ยงด้าน IT ที่สำคัญ (IT key risk indicator) เพื่อให้สามารถติดตามแนวโน้มของความเสี่ยง และสามารถทบทวนมาตรการควบคุมความเสี่ยงได้อย่างมีประสิทธิภาพ(3) การติดตามความคืบหน้าของการดำเนินงานตามแผนการบริหารจัดการความเสี่ยงด้าน IT <p>7. การรายงานความเสี่ยง (risk reporting) ควรจัดให้มีการรายงานความเสี่ยง และผลการบริหารจัดการความเสี่ยงด้าน IT ต่อหัวหน้าสำนักงานสอบบัญชี หรือคณะกรรมการบริหารของสำนักงานสอบบัญชีอย่างน้อยปีละ 1 ครั้ง โดยครอบคลุมรายละเอียดอย่างน้อย ดังนี้</p> <ul style="list-style-type: none">(1) ผลการประเมินและจัดการความเสี่ยงด้าน IT(2) แนวโน้มความเสี่ยงด้าน IT ที่อาจมีผลกระทบต่อสำนักงานสอบบัญชี(3) ความคืบหน้าของการดำเนินงานตามแผนการบริหารจัดการความเสี่ยงด้าน IT
<p>2.2.2 นโยบายการรักษาความมั่นคงปลอดภัยด้าน IT (IT security policy) มีเรื่องที่ต้องครอบคลุม ดังนี้</p> <ul style="list-style-type: none">(1) โครงสร้างการบริหารงานเพื่อการรักษาความมั่นคงปลอดภัยด้าน IT(2) การบริหารจัดการบุคลากร และบุคคลภายนอก(3) การบริหารจัดการทรัพย์สินด้าน IT(4) การรักษาความมั่นคงปลอดภัยของข้อมูล(5) การควบคุมการเข้าถึงข้อมูลและระบบงาน IT(6) การควบคุมการเข้ารหัส(7) การรักษาความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อม(8) การรักษาความมั่นคงปลอดภัยในการปฏิบัติงานด้าน IT	<p>[ไม่มีการกำหนดแนวปฏิบัติไว้เป็นการเฉพาะ]</p>

ข้อกำหนด	แนวปฏิบัติ
<p>(9) การรักษาความมั่นคงปลอดภัยเกี่ยวกับระบบเครือข่าย สื่อสาร</p> <p>(10) การบริหารจัดการโครงการด้าน IT และการจัดหา พัฒนา และบำรุงรักษาระบบงาน IT</p> <p>(11) การบริหารจัดการเหตุการณ์ผิดปกติด้าน IT</p> <p>(12) แผนฉุกเฉินด้าน IT</p>	
<p>2.3 สำนักงานสอบบัญชีต้องจัดให้มีการดำเนินการตามนโยบาย ในข้อ 2.2 ดังนี้</p> <p>2.3.1 สื่อสารนโยบายตามข้อ 2.2 ให้แก่บุคลากรของ สำนักงานสอบบัญชีและบุคคลภายนอกที่เกี่ยวข้องรับทราบตาม บทบาทหน้าที่ ความรับผิดชอบ และสิทธิการเข้าถึงข้อมูล ในลักษณะ ที่สามารถเข้าถึงได้ง่าย เพื่อให้บุคคลที่เกี่ยวข้องดังกล่าวเข้าใจและ สามารถปฏิบัติตามนโยบายได้อย่างถูกต้อง</p>	<p>1. ในการสื่อสารนโยบายให้กับบุคคลภายนอกที่เกี่ยวข้อง สำนักงานสอบบัญชีควรพิจารณาถึงรายละเอียดที่บุคคลภายนอกควรรู้ เพื่อให้สามารถปฏิบัติงานได้สอดคล้องกับนโยบายของสำนักงานสอบบัญชี โดยคำนึงถึงความลับของข้อมูลด้วย</p>
<p>2.3.2 กำหนดขั้นตอนและวิธีปฏิบัติงานให้เป็นไปตาม นโยบายตามข้อ 2.2</p>	<p>1. สำนักงานสอบบัญชีควรกำหนดขั้นตอนการปฏิบัติงานที่เกี่ยวข้องกับระบบงาน IT เป็นลายลักษณ์อักษร เพื่อให้เจ้าหน้าที่ ผู้ปฏิบัติงานด้าน IT สามารถปฏิบัติงานได้อย่างถูกต้องและเป็นไปตามนโยบายที่เกี่ยวข้องกับการกำกับดูแลความเสี่ยงด้าน IT</p> <p>2. สำนักงานสอบบัญชีควรกำหนดวิธีปฏิบัติสำหรับการอนุมัติยกเว้น (exception) กรณีที่มีความจำเป็นที่ไม่สามารถปฏิบัติตาม ขั้นตอนและวิธีปฏิบัติงานที่สำนักงานสอบบัญชีกำหนดไว้ สำนักงานสอบบัญชีต้องจัดให้มีการประเมินความเสี่ยง ควบคุม ความเสี่ยงอย่างเพียงพอเหมาะสม และขออนุมัติยกเว้นจากผู้มีอำนาจก่อนดำเนินการต่อไป พร้อมทั้ง ต้องจัดเก็บหลักฐาน การอนุมัติยกเว้นดังกล่าวอย่างเป็นลายลักษณ์อักษร</p> <p>3. สำนักงานสอบบัญชีควรจัดให้มีการสอบทานความเหมาะสมของรายการขออนุมัติยกเว้น ตลอดจนแนวทางการควบคุม ความเสี่ยงอย่างน้อยปีละ 1 ครั้ง เพื่อทบทวนแนวทางการดำเนินการให้มีความเหมาะสมต่อความเสี่ยงที่อาจมีการเปลี่ยนแปลง ไปตามสภาพแวดล้อมการประกอบธุรกิจและการใช้งานเทคโนโลยีสารสนเทศในการประกอบธุรกิจ</p>
<p>2.3.3 ในกรณีที่มีการเปลี่ยนแปลงนโยบายตามข้อ 2.2 ต้องสื่อสารให้บุคคลที่เกี่ยวข้องได้รับทราบอย่างทั่วถึง และต้องปรับปรุง ขั้นตอนและวิธีปฏิบัติงานให้สอดคล้องกับการเปลี่ยนแปลงดังกล่าว</p>	<p>[ไม่มีการกำหนดแนวปฏิบัติไว้เป็นการเฉพาะ]</p>

ข้อกำหนด	แนวปฏิบัติ
2.4 สำนักงานสอบบัญชีต้องทบทวนหรือปรับปรุงนโยบายตามข้อ 2.2 อย่างน้อยปีละ 1 ครั้ง และโดยไม่ชักช้าเมื่อมีเหตุการณ์ใด ๆ ซึ่งอาจส่งผลกระทบต่อการทำงานกับดูแลและบริหารจัดการความเสี่ยงด้าน IT อย่างมีนัยสำคัญ	[ไม่มีการกำหนดแนวปฏิบัติไว้เป็นการเฉพาะ]

หมวดที่ 2 การรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (Information Technology Security)

ข้อกำหนด	แนวปฏิบัติ
2.1 โครงสร้างการบริหารงานเพื่อการรักษาความมั่นคงปลอดภัยด้าน IT (organization of information technology security)	
<p>ส่วนที่ 1 โครงสร้างการบริหารงานเพื่อรักษาความมั่นคงปลอดภัยด้าน IT (organization of information technology security)</p> <p>สำนักงานสอบบัญชีต้องดำเนินการจัดให้มีโครงสร้างดังกล่าว โดยมีลักษณะอย่างน้อยดังนี้</p>	
<p>1.1 กำหนดโครงสร้างภายในองค์กร (organizational structure) ในการปฏิบัติงานด้าน IT โดยมีรายละเอียดหน้าที่และความรับผิดชอบของบุคลากรเป็นลายลักษณ์อักษร</p>	<p>สำหรับสำนักงานสอบบัญชีที่ไม่ได้จัดตั้งหน่วยงานที่ปฏิบัติงานด้าน IT ภายใน แต่มีการว่าจ้างบุคลากรภายนอกมาปฏิบัติงานด้าน IT ให้กับสำนักงานสอบบัญชี หรือ บุคลากรที่ปฏิบัติงานด้าน IT เป็นพนักงานของสำนักงานสอบบัญชีเครือข่าย โครงสร้างภายในองค์กรในการปฏิบัติงานด้าน IT ควรมีลักษณะอย่างน้อยดังนี้</p> <ul style="list-style-type: none"> ● มีการระบุหน้าที่และความรับผิดชอบของบุคลากรที่ทำหน้าที่กำกับดูแลและสอบทานการปฏิบัติงานของบุคลากรภายนอก หรือ พนักงานของสำนักงานสอบบัญชีเครือข่ายที่มาปฏิบัติงานด้าน IT
<p>1.2 มีการสอบทานการปฏิบัติงานเพื่อป้องกันความเสี่ยงในการรักษาความมั่นคงปลอดภัยของระบบงาน IT ที่อาจเกิดขึ้นในการปฏิบัติงาน</p>	<p>สำนักงานสอบบัญชีควรจัดให้มีการแบ่งแยกหน้าที่ในการปฏิบัติงานด้านต่าง ๆ ที่เกี่ยวกับความมั่นคงปลอดภัยของระบบงาน IT อย่างชัดเจน เพื่อให้มีการสอบทานการปฏิบัติงานระหว่างกัน เพื่อลดข้อผิดพลาดในการปฏิบัติงานและลดโอกาสการกระทำผิด (fraud) เช่น แบ่งแยกผู้พัฒนาระบบงาน (developer) ออกจากผู้มีสิทธิในการนำระบบขึ้นใช้งานจริง เป็นต้น</p> <p>ทั้งนี้ กรณีที่ไม่สามารถแบ่งแยกหน้าที่ความรับผิดชอบได้เนื่องจากข้อจำกัดทางด้านขนาดของธุรกิจหรือบุคลากร สำนักงานสอบบัญชีควรจัดให้มีมาตรการควบคุมทดแทน เช่น การจัดให้มีกระบวนการติดตามและตรวจสอบการปฏิบัติงานของบุคลากรที่เกี่ยวข้องอย่างใกล้ชิดและสม่ำเสมอ หรือทุก ๆ การเปลี่ยนแปลงทางด้าน IT ต้องได้รับความเห็นชอบจากผู้มีอำนาจ เป็นต้น</p>
2.2 การบริหารจัดการบุคลากร และบุคคลภายนอก	
<p>ส่วนที่ 2 การบริหารจัดการบุคลากร และบุคคลภายนอก</p>	
2.2.1 การบริหารจัดการบุคลากร	
<p>บุคลากรที่ต้องบริหารจัดการ</p> <p>2.1 บุคลากรที่เกี่ยวข้องหรือที่ใช้ระบบงาน IT ปฏิบัติงาน</p>	

ข้อกำหนด	แนวปฏิบัติ
<p>การบริหารจัดการ</p> <p>สำนักงานสอบบัญชีต้องบริหารจัดการบุคลากรตามข้อ 2.1 อย่างเหมาะสม โดยดำเนินการอย่างน้อยดังนี้</p> <p>(1) มีกระบวนการคัดเลือกบุคลากรในการปฏิบัติหน้าที่ ดังนี้</p> <p>(1.1) คำนึงถึงความรู้ ความสามารถ และ ความเพียงพอในการปฏิบัติงาน</p> <p>(1.2) มีการตรวจสอบข้อมูลของบุคลากรก่อนการว่าจ้างอย่างเพียงพอและสอดคล้องกับความเสี่ยงของตำแหน่งงานและหน้าที่ความรับผิดชอบ</p>	<p>[ไม่มีการกำหนดแนวปฏิบัติไว้เป็นการเฉพาะ]</p>
<p>(2) มีข้อกำหนดให้บุคลากรทำความเข้าใจ รับทราบ และลงนามยอมรับในเรื่องดังนี้</p> <p>(2.1) บทบาทหน้าที่และความรับผิดชอบของบุคลากรดังกล่าวเกี่ยวกับการรักษาความมั่นคงปลอดภัยด้าน IT</p> <p>(2.2) non-disclosure agreement</p>	<ol style="list-style-type: none">1. สำนักงานสอบบัญชีควรให้บุคลากรที่ได้รับทราบว่าจ้างทำความเข้าใจ รับทราบ และลงนามยอมรับเงื่อนไขการว่าจ้างงานหรือระเบียบข้อบังคับภายในองค์กร นโยบายการรักษาความมั่นคงปลอดภัยด้าน IT และข้อตกลงการไม่เปิดเผยข้อมูล (non-disclosure agreement) ก่อนเริ่มปฏิบัติงาน2. non-disclosure agreement ควรมีเนื้อหาขั้นต่ำ ดังนี้<ol style="list-style-type: none">(1) ความเป็นเจ้าของข้อมูลสำคัญทางธุรกิจ ทรัพย์สินทางปัญญา และการป้องกันการรั่วไหลของข้อมูล(2) ความรับผิดชอบในการเก็บรักษาความลับ และไม่เปิดเผยข้อมูลโดยไม่ได้รับอนุญาต(3) การแจ้งเตือนและรายงานผู้เกี่ยวข้องหากพบการรั่วไหลหรือเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต(4) การดำเนินการกรณีละเมิดหรือยกเลิกข้อตกลง รวมทั้งข้อกำหนดในการคืนหรือทำลายข้อมูลที่มีความสำคัญเมื่อสิ้นสุดข้อตกลง
<p>(3) สร้างความตระหนักรู้ถึงความเสี่ยงด้าน IT ให้แก่บุคลากรที่ปฏิบัติงาน ซึ่งสามารถเข้าถึงข้อมูลหรือระบบงานภายในองค์กร เพื่อให้บุคลากรดังกล่าวสามารถใช้งานระบบงาน IT ได้อย่างปลอดภัย</p>	<ol style="list-style-type: none">1. สำนักงานสอบบัญชีควรส่งเสริมและพัฒนาความรู้ด้าน IT ให้แก่บุคลากรอย่างสม่ำเสมอ เช่น การจัดการอบรมภายในองค์กร หรือส่งบุคลากรเข้าร่วมฝึกอบรมภายนอกองค์กร เป็นต้น เพื่อให้บุคลากรมีความรู้ความเข้าใจถึงการใช้งาน IT ที่ถูกต้องปลอดภัย และลดความเสี่ยงที่อาจเกิดขึ้นจากการใช้งาน IT โดยมีเนื้อหา เช่น<ol style="list-style-type: none">(1) การรักษาความมั่นคงปลอดภัยด้าน IT(2) ความเสี่ยงด้าน IT และภัยคุกคามทางไซเบอร์(3) หลักเกณฑ์และกฎหมายที่เกี่ยวข้องกับ IT เป็นต้น

ข้อกำหนด	แนวปฏิบัติ
	<ol style="list-style-type: none"> 2. สำนักงานสอบบัญชีควรทบทวนแผนการส่งเสริมและพัฒนาความรู้ด้าน IT (training program) อย่างน้อยปีละ 1 ครั้ง เพื่อให้มั่นใจว่าเนื้อหาและรายละเอียดของแผนงานที่เกี่ยวข้องยังคงเพียงพอเหมาะสมกับแนวโน้มความเสี่ยงด้าน IT ในปัจจุบัน 3. สำนักงานสอบบัญชีควรจัดให้มีการเสริมสร้างความตระหนักรู้เรื่องการรักษาความมั่นคงปลอดภัยด้าน IT และความเสี่ยงด้าน IT อย่างสม่ำเสมอให้แก่บุคลากร (user) ที่สามารถเข้าถึงข้อมูลที่มีความสำคัญของสำนักงานสอบบัญชีหรือข้อมูลของลูกค้า เช่น การทดสอบเรื่องอีเมลหลอกลวง (phishing) การทดสอบเรื่องวิศวกรรมสังคม (social engineering) และการซุกซอมแผนเพื่อเตรียมความพร้อมรับมือกับการโจมตีทางไซเบอร์ เป็นต้น
<p>(4) กำหนดให้บุคลากรงดเว้นการใช้งานระบบงาน IT ในลักษณะที่อาจก่อให้เกิดความเสียหายแก่สำนักงานสอบบัญชี หรือที่เป็นการกระทำผิดกฎหมายหรือข้อกำหนดและจรรยาบรรณที่สำนักงานสอบบัญชีกำหนดไว้</p>	<ol style="list-style-type: none"> 1. สำนักงานสอบบัญชีควรจัดให้มีนโยบายการใช้งาน IT ที่ยอมรับได้ (acceptable use policy) โดยมีรายละเอียดครอบคลุมขอบเขตความรับผิดชอบของผู้ใช้งาน IT สิ่งที่ผู้ใช้งานพึงปฏิบัติ และสิ่งที่ไม่ควรปฏิบัติ 2. สำนักงานสอบบัญชีควรสื่อสารนโยบายการใช้งาน IT ที่ยอมรับได้ (acceptable use policy) ให้ผู้ใช้งานรับทราบ และลงนามยอมรับนโยบายดังกล่าว
<p>(5) กำหนดมาตรการในการลงโทษบุคลากรที่มีพฤติกรรมฝ่าฝืนหรือไม่ปฏิบัติตามนโยบายและมาตรการรักษาความมั่นคงปลอดภัยในการปฏิบัติงานด้าน IT</p>	<p>[ไม่มีการกำหนดแนวปฏิบัติไว้เป็นการเฉพาะ]</p>
<p>(6) กำหนดขั้นตอนปฏิบัติเมื่อสิ้นสุดการจ้างงาน หรือเมื่อมีการเปลี่ยนแปลงตำแหน่งงาน เพื่อป้องกันการละเมิดหรือความเสียหายที่อาจเกิดขึ้นต่อทรัพย์สินด้าน IT</p>	<ol style="list-style-type: none"> 1. สำนักงานสอบบัญชีควรจัดให้มีกระบวนการรองรับเมื่อมีการเปลี่ยนแปลงตำแหน่งงาน และสิ้นสุดการจ้างงาน เช่น การคืนทรัพย์สินขององค์กร การปรับปรุงสิทธิให้เป็นปัจจุบัน การยกเลิกสิทธิเมื่อหมดหน้าที่และความรับผิดชอบ เป็นต้น รวมทั้งมีการสื่อสารให้ผู้ที่เกี่ยวข้องรับทราบถึงการเปลี่ยนแปลงสิทธิ หน้าที่ และความรับผิดชอบ
<p>2.2.2 การบริหารจัดการบุคคลภายนอก (third-party management) (ถ้ามี)</p>	
<p><u>บุคลากรที่ต้องบริหารจัดการ</u></p> <p>2.2 บุคคลภายนอก ให้รวมถึงพนักงานของสำนักงานเครือข่ายหรือบริษัทในเครือของสำนักงานสอบบัญชี ในกรณีที่สำนักงานสอบบัญชีมีการดำเนินการอย่างใดอย่างหนึ่งดังนี้</p> <ul style="list-style-type: none"> ● ใช้บริการงานด้าน IT จากบุคคลภายนอก 	

ข้อกำหนด	แนวปฏิบัติ
<ul style="list-style-type: none">• เชื่อมต่อระบบงาน IT กับบุคคลภายนอก• อนุญาตให้บุคคลภายนอกสามารถเข้าถึงข้อมูลสำคัญหรือข้อมูลของลูกค้าของสำนักงานสอบบัญชีได้	
<p><u>การบริหารจัดการ</u></p> <p>สำนักงานสอบบัญชีต้องบริหารจัดการบุคคลภายนอกตามข้อ 2.2 ดังนี้</p> <p>(1) ประเมินความเสี่ยงจากการใช้บริการ การเชื่อมต่อหรือการเข้าถึงข้อมูลจากบุคคลภายนอก รวมถึงผู้รับดำเนินการช่วง (subcontract) จากบุคคลภายนอก</p>	<p>1. สำนักงานสอบบัญชีควรประเมินความเสี่ยงและผลกระทบในเรื่องดังต่อไปนี้ก่อน</p> <ul style="list-style-type: none">• การใช้บริการงานด้าน IT จากบุคคลภายนอก• การเชื่อมต่อระบบงาน IT กับบุคคลภายนอก• การอนุญาตให้บุคคลภายนอกสามารถเข้าถึงข้อมูลสำคัญหรือข้อมูลของลูกค้าที่ควบคุมดูแลโดยสำนักงานสอบบัญชีได้ <p>โดยคำนึงถึงความเสี่ยง ดังนี้</p> <ol style="list-style-type: none">(1) ความเสี่ยงด้านกฎหมาย และกฎเกณฑ์ที่เกี่ยวข้องทั้งในประเทศและต่างประเทศ เช่น กฎหมายเกี่ยวกับการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ กฎหมายเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล กฎหมายเกี่ยวกับธุรกรรมทางอิเล็กทรอนิกส์ และ The EU General Data Protection Regulation (GDPR) เป็นต้น(2) ความเสี่ยงจากการกำกับดูแลและบริหารจัดการบุคคลภายนอกที่ไม่รัดกุมเพียงพอ เช่น การไม่สามารถตรวจสอบการดำเนินงานของบุคคลภายนอกได้ด้วยตนเอง เป็นต้น(3) ความเสี่ยงจากการพึ่งพาศักยภาพบุคคลภายนอกรายใดรายหนึ่งเป็นหลัก (third party/vendor locked-in) ซึ่งทำให้มีข้อจำกัดในการเปลี่ยนแปลงเทคโนโลยี ผู้ให้บริการ หรือข้อจำกัดในการนำระบบหรือข้อมูลกลับมาดำเนินการเอง(4) ความเสี่ยงด้าน IT และภัยทางไซเบอร์ เช่น ระบบที่ให้บริการโดยบุคคลภายนอกเกิดขัดข้อง ระบบของบุคคลภายนอกมีช่องโหว่ทำให้ข้อมูลเกิดการสูญหายหรือรั่วไหล เป็นต้น(5) ความเสี่ยงกรณีบุคคลภายนอกให้ผู้อื่นดำเนินการแทน (sub-contracting) เช่น subcontractor ปฏิบัติงานบกพร่อง เป็นต้น <p>2. สำนักงานสอบบัญชีควรจัดให้มีการกำหนดระดับความมีนัยสำคัญของบุคคลภายนอกแต่ละราย</p>
<p>(2) กำหนดวิธีปฏิบัติและหลักเกณฑ์ในการคัดเลือกบุคคลภายนอก</p>	<p>1. สำนักงานสอบบัญชีควรกำหนดกระบวนการและหลักเกณฑ์ในการคัดเลือกบุคคลภายนอกอย่างชัดเจน และเป็นลายลักษณ์อักษร เพื่อให้มั่นใจว่าผู้ให้บริการภายนอกจะสามารถให้บริการได้ตรงตามความต้องการของสำนักงานสอบบัญชี ทั้งนี้ ในการตัดสินใจใช้บริการ การเชื่อมต่อ หรือการเข้าถึงข้อมูลจากบุคคลภายนอก ที่มีความเสี่ยงหรือมีนัยสำคัญควรได้รับความเห็นชอบจากหัวหน้าสำนักงานสอบบัญชี หรือคณะกรรมการบริหารของสำนักงานสอบบัญชีที่ได้รับมอบหมาย</p>

ข้อกำหนด	แนวปฏิบัติ
	<p>2. สำนักงานสอบบัญชีควรประเมินศักยภาพบุคคลภายนอก (due diligence) ให้สอดคล้องกับระดับความเสี่ยง และความมีนัยสำคัญของบุคคลภายนอก โดยคำนึงถึงเรื่องดังต่อไปนี้</p> <ol style="list-style-type: none">(1) ฐานะทางการเงิน ชื่อเสียง ความรู้ความเชี่ยวชาญ ประสบการณ์ และความสามารถในการให้บริการในช่วงที่ผ่านมา(2) การบริหารจัดการความเสี่ยง การควบคุมภายใน การตรวจสอบภายใน และการติดตามผลการปฏิบัติงาน(3) การรักษาความมั่นคงปลอดภัยด้าน IT(4) การบริหารจัดการความต่อเนื่องทางธุรกิจ และความพร้อมรับมือภัยหรือเหตุการณ์ต่าง ๆ(5) การปฏิบัติตามกฎหมายและกฎเกณฑ์ที่เกี่ยวข้อง เช่น การขอตรวจสอบเอกสารหลักฐานหรือใบรับรองจากบุคคลภายนอก ในการดำเนินการตามกฎหมายและกฎเกณฑ์ที่เกี่ยวข้อง หรือการตรวจสอบประวัติด้านการกระทำความผิด เป็นต้น(6) การปฏิบัติตามมาตรฐานสากลด้าน IT เช่น การตรวจสอบเอกสารหลักฐานการได้รับการรับรองรับตามมาตรฐาน ISO 27001 เป็นต้น โดยในการรับรองการปฏิบัติตามมาตรฐานสากล สำนักงานสอบบัญชีควรพิจารณาว่า บุคคลภายนอกได้รับการรับรองในระบบที่สำคัญ หรือระบบที่สำนักงานสอบบัญชีใช้บริการ เชื่อมต่อ หรือเข้าถึงข้อมูล หรือได้รับการรับรองครอบคลุมทั้งองค์กร(7) การใช้เทคโนโลยีแบบเปิด (open technology) เพื่อให้สามารถนำระบบหรือข้อมูลไปใช้งานหรือเชื่อมโยงกับระบบอื่นได้ (interoperability) และลดข้อจำกัดในการย้ายหรือเปลี่ยนแปลงเทคโนโลยี ผู้ให้บริการ หรือพันธมิตร รวมถึงข้อจำกัดในการนำระบบหรือข้อมูลกลับมาดำเนินการเอง(8) กรณีที่บุคคลภายนอกมอบหมายการปฏิบัติงานที่สำคัญให้กับบุคคลอื่นต่อ (sub-contracting to another supplier) สำนักงานสอบบัญชีควรพิจารณารายละเอียดด้านความมั่นคงปลอดภัยสารสนเทศของบุคคลดังกล่าวด้วย
<p>(3) กำหนดบทบาท หน้าที่ และความรับผิดชอบของสำนักงานสอบบัญชีและบุคคลภายนอกอย่างชัดเจนและเป็นลายลักษณ์อักษร</p>	<p>1. สำนักงานสอบบัญชีควรจัดทำสัญญาหรือข้อตกลงการใช้บริการ การเชื่อมต่อ หรือการเข้าถึงข้อมูลจากบุคคลภายนอกอย่างเป็นลายลักษณ์อักษร โดยมีการลงนามร่วมกันระหว่างสำนักงานสอบบัญชีและบุคคลภายนอก เพื่อให้มั่นใจได้ว่าบุคคลภายนอกมีหน้าที่รับผิดชอบในการรักษาความมั่นคงปลอดภัยของระบบงาน IT ในระดับที่เหมาะสม โดยมีรายละเอียดสอดคล้องกับความเสี่ยง และความมีนัยสำคัญของบุคคลภายนอก ดังนี้</p> <ol style="list-style-type: none">(1) ขอบเขตการให้บริการ การเชื่อมต่อ และการเข้าถึงข้อมูลจากบุคคลภายนอก(2) บทบาท หน้าที่ และความรับผิดชอบของบุคคลภายนอกและสำนักงานสอบบัญชี(3) มาตรฐานขั้นต่ำในการปฏิบัติงานของบุคคลภายนอก เช่น การรักษาความปลอดภัยของระบบงาน IT การรักษาความลับของข้อมูล และการไม่นำข้อมูลไปใช้นอกเหนือจากที่ระบุไว้ในสัญญาหรือข้อตกลงการใช้บริการ เป็นต้น(4) ข้อตกลงระดับการให้บริการด้าน IT (service level agreement: SLA) สำหรับการใช้บริการจากบุคคลภายนอก

ข้อกำหนด	แนวปฏิบัติ
	<p>(5) การติดตามและรายงานผลการปฏิบัติงานของบุคคลภายนอก ซึ่งครอบคลุมถึงการแจ้งการเปลี่ยนแปลงหรือปัญหาที่สำคัญ และการรายงานเหตุการณ์ผิดปกติอย่างทันการณ์</p> <p>(6) รายชื่อ และช่องทางการติดต่อในกรณีเกิดปัญหาเกี่ยวกับการรักษาความมั่นคงปลอดภัยของระบบงาน IT</p> <p>(7) การทำลายข้อมูลเมื่อสิ้นสุดหรือยกเลิกการใช้บริการ การเชื่อมต่อ และการเข้าถึงข้อมูลจากบุคคลภายนอก</p> <p>(8) เงื่อนไขหรือสิทธิของสำนักงานสอบบัญชีในการเปลี่ยนแปลง ยุติ หรือยกเลิกสัญญาหรือข้อตกลงกับบุคคลภายนอก เช่น กรณีที่บุคคลภายนอกมีการละเมิดสัญญาหรือข้อตกลง เป็นต้น</p> <p>(9) การจัดให้มีแผนฉุกเฉินด้าน IT (IT contingency plan) ที่สอดคล้องกับแผนฉุกเฉินด้าน IT ของสำนักงานสอบบัญชี</p> <p>(10) ความรับผิดชอบต่อความเสียหายที่เกิดจากบุคคลภายนอก เช่น กรณีการให้บริการไม่เป็นไปตาม SLA ที่กำหนดไว้ เป็นต้น</p> <p>อย่างไรก็ดี หากมีข้อจำกัดในการระบุรายละเอียดและกำหนดเงื่อนไขที่สำคัญลงในข้อตกลงหรือสัญญาที่ทำกับบุคคลภายนอก สำนักงานสอบบัญชีควรมีการประเมินความเสี่ยงและพิจารณาแนวทางควบคุมความเสี่ยงที่เพียงพอเหมาะสม พร้อมทั้งขออนุมัติยกเว้น (exception) จากผู้มีอำนาจ</p>
<p>(4) กรณีบุคคลภายนอกซึ่งเป็นผู้ให้บริการงานด้าน IT รายที่มีนัยสำคัญตามผลการประเมินความเสี่ยงในข้อ 2.2 (1) ข้อตกลงหรือสัญญาการให้บริการต้องระบุสิทธิให้สำนักงานสอบบัญชี สำนักงานก.ล.ต. และผู้ตรวจสอบที่ได้รับการแต่งตั้งจากสำนักงานสอบบัญชีหรือสำนักงานก.ล.ต. สามารถเข้าตรวจสอบการดำเนินงานและการควบคุมภายในของบุคคลภายนอกดังกล่าวได้</p> <p>หากมีเหตุจำเป็นทำให้สำนักงานสอบบัญชีไม่สามารถระบุสิทธิในการเข้าตรวจสอบตามวรรคหนึ่งไว้ในข้อตกลงหรือสัญญา สำนักงานสอบบัญชีต้องมีมาตรการประเมินหรือติดตามการดำเนินงานและการควบคุมภายในของบุคคลภายนอกให้รัดกุมเพียงพอและสอดคล้องกับความเสี่ยงและความมีนัยสำคัญของการใช้บริการ การเชื่อมต่อ หรือการเข้าถึงข้อมูล</p>	<p>1. สำนักงานสอบบัญชีควรกำหนดสิทธิให้สำนักงานสอบบัญชี สำนักงานก.ล.ต. และผู้ตรวจสอบที่ได้รับการแต่งตั้งจากสำนักงานสอบบัญชี หรือ สำนักงานก.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</p>

ข้อกำหนด	แนวปฏิบัติ
<p>(5) มี non-disclosure agreement สำหรับบุคคลภายนอกหรือผู้รับดำเนินการช่วงของบุคคลภายนอก ในกรณีที่บุคคลดังกล่าวสามารถเข้าถึงข้อมูลสำคัญของสำนักงานสอบบัญชีหรือข้อมูลของลูกค้า</p>	<p>1. non-disclosure agreement ควรมีรายละเอียดครอบคลุมขอบเขตความรับผิดชอบในการเก็บรักษาความลับ การไม่เปิดเผยข้อมูลโดยไม่ได้รับอนุญาต การรายงานสำนักงานสอบบัญชีเมื่อพบการรั่วไหลหรือเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต และการทำลายข้อมูลที่มีความสำคัญเมื่อสิ้นสุดข้อตกลงหรือสัญญา</p>
<p>(6) กำกับดูแล ติดตาม และบริหารจัดการความเสี่ยงจากการใช้บริการ การเชื่อมต่อหรือการเข้าถึงข้อมูลจากบุคคลภายนอก โดยต้องสอดคล้องกับระดับความเสี่ยงและระดับความสำคัญของบุคคลภายนอก</p>	<p>1. สำนักงานสอบบัญชีควรกำกับดูแล ติดตาม และบริหารจัดการความเสี่ยงจากการใช้บริการ การเชื่อมต่อ หรือการเข้าถึงข้อมูลจากบุคคลภายนอกให้สอดคล้องกับความเสี่ยง และความมีนัยสำคัญของบุคคลภายนอก โดยครอบคลุมการดำเนินการอย่างน้อย ดังนี้</p> <ol style="list-style-type: none">(1) กำหนดผู้รับผิดชอบในการติดตามผลการปฏิบัติงานของบุคคลภายนอกอย่างต่อเนื่อง โดยพิจารณาตามขอบเขตระดับความเสี่ยงและความมีนัยสำคัญของใช้บริการ การเชื่อมต่อ หรือการเข้าถึงข้อมูลจากบุคคลภายนอก(2) จัดให้มีทะเบียนบุคคลภายนอก เพื่อให้สามารถใช้ในการบริหารจัดการความเสี่ยง ติดตาม และตรวจสอบการปฏิบัติงานของบุคคลภายนอกได้อย่างครบถ้วนต่อเนื่อง โดยมีรายละเอียดครอบคลุม<ul style="list-style-type: none">- ชื่อบุคคลภายนอก- รายละเอียดของใช้บริการ การเชื่อมต่อ หรือการเข้าถึงข้อมูลจากบุคคลภายนอก- ระดับความเสี่ยงและระดับความมีนัยสำคัญ- วันเริ่มต้นและสิ้นสุดสัญญาหรือข้อตกลง(3) จัดให้มีมาตรการควบคุมและติดตามสิทธิการเข้าถึงข้อมูลสารสนเทศของบุคคลภายนอกอย่างสม่ำเสมอ เพื่อให้สิทธิดังกล่าวเป็นไปตามหลักความจำเป็นต้องรู้ (need-to-know basis)(4) กำหนดให้บุคคลภายนอกรายงานเหตุการณ์ผิดปกติที่เกิดขึ้นระหว่างการดำเนินงานที่เกี่ยวข้องให้สำนักงานสอบบัญชีได้รับทราบอย่างทันการณ(5) ประเมินผลการปฏิบัติงานหรือผลการให้บริการของบุคคลภายนอก ทั้งในด้านประสิทธิภาพของบริการ การรักษาความมั่นคงปลอดภัยด้าน IT และการปฏิบัติตามกฎหมายที่เกี่ยวข้อง เมื่อจะต่อสัญญาหรือเมื่อถึงรอบระยะเวลาที่สำนักงานสอบบัญชีกำหนด(6) ทบทวนคุณสมบัติบุคคลภายนอกอย่างสม่ำเสมอ เพื่อให้มั่นใจว่าบุคคลภายนอกยังคงมีคุณสมบัติที่เหมาะสม(7) หากสำนักงานสอบบัญชีมีการใช้บริการจาก cloud service provider สำนักงานสอบบัญชีต้องกำหนดนโยบายและวิธีปฏิบัติเพิ่มเติมในเรื่องการโอนย้ายหรือการเข้าถึงข้อมูล เมื่อเกิดการยุติสัญญาหรือข้อตกลงการให้บริการ ทั้งนี้ สำนักงานสอบบัญชีควรกำหนดเงื่อนไขเกี่ยวกับสิทธิในการขอโอนย้ายหรือเข้าถึงข้อมูลดังกล่าวในสัญญาหรือข้อตกลงการให้บริการอย่างเป็นทางการ

ข้อกำหนด	แนวปฏิบัติ
	<p>ลายลักษณ์อักษร เพื่อให้มั่นใจว่า สำนักงานสอบบัญชีจะสามารถได้รับการโอนย้ายข้อมูลหรือเข้าถึงข้อมูลได้อย่างครบถ้วน ถูกต้องและทันเวลา</p>
<p>(7) รักษาความมั่นคงปลอดภัยด้าน IT จากการใช้บริการ การเชื่อมต่อ หรือการเข้าถึงข้อมูลจากบุคคลภายนอก ที่สอดคล้องกับมาตรฐานการรักษาความมั่นคงปลอดภัยด้าน IT ของสำนักงานสอบบัญชี</p>	<p>1. สำนักงานสอบบัญชีควรมีแนวทางการดูแลให้มั่นใจว่าการใช้บริการ การเชื่อมต่อ หรือการเข้าถึงข้อมูลจากบุคคลภายนอกมีการรักษาความมั่นคงปลอดภัยด้าน IT ตามกรอบหลักการที่สำคัญ 3 ประการ คือ การดำรงไว้ซึ่งความลับ (confidentiality) ความถูกต้อง ครบถ้วน (integrity) และสภาพพร้อมใช้งาน (availability) ของระบบและข้อมูล และสอดคล้องกับนโยบายและมาตรการรักษาความมั่นคงปลอดภัยด้าน IT ของสำนักงานสอบบัญชีหรือมาตรฐานสากลที่เกี่ยวข้อง เช่น ISO/IEC 27001 หรือ หลักเกณฑ์ในการกำกับดูแลด้านเทคโนโลยีสารสนเทศของสำนักงาน ก.ล.ต. เป็นต้น โดยพิจารณาให้สอดคล้องกับระดับความเสี่ยง และความมีนัยสำคัญของบุคคลภายนอก</p>
<p>(8) เตรียมความพร้อมรับมือต่อเหตุการณ์ผิดปกติด้าน IT ที่อาจเกิดขึ้นและมีผลกระทบอย่างมีนัยสำคัญเพื่อให้สามารถให้บริการหรือดำเนินธุรกิจได้อย่างต่อเนื่อง</p>	<p>1. สำนักงานสอบบัญชีควรจัดให้มีแผนรองรับในกรณีที่บุคคลภายนอกเกิดเหตุการณ์ผิดปกติด้าน IT (incident response plan) ซึ่งมีผลกระทบกับการดำเนินการของสำนักงานสอบบัญชีโดยครอบคลุมเหตุการณ์ที่เกี่ยวข้องกับเหตุการณ์ความปลอดภัยทางไซเบอร์ และเหตุการณ์การละเมิดต่อข้อมูลส่วนบุคคล</p>
<p>2.3 การบริหารจัดการทรัพย์สินด้าน IT (IT asset management)</p>	
<p>ส่วนที่ 3 การบริหารจัดการทรัพย์สินด้าน IT (IT asset management) สำนักงานสอบบัญชีต้องจัดให้มีการบริหารจัดการทรัพย์สินด้าน IT เพื่อนำไปใช้ดำเนินการเกี่ยวกับการรักษาความมั่นคงปลอดภัยด้าน IT ได้อย่างเหมาะสม ครบถ้วนและเป็นปัจจุบัน ดังนี้</p>	
<p>3.1 จัดทำทะเบียนรายการทรัพย์สินด้าน IT ประเภท ฮาร์ดแวร์ ซอฟต์แวร์ รวมถึงสิทธิในการใช้งานฮาร์ดแวร์ และซอฟต์แวร์</p>	<p>1. สำนักงานสอบบัญชีควรกำหนดระเบียบปฏิบัติเกี่ยวกับการบริหารจัดการทรัพย์สินด้าน IT ครอบคลุมการจัดทำทะเบียนรายการทรัพย์สิน การปรับปรุงทะเบียนรายการทรัพย์สิน การยกเลิกและเรียกคืนทรัพย์สิน</p> <p>2. สำนักงานสอบบัญชีควรจัดทำทะเบียนรายการทรัพย์สินด้าน IT ประเภทอุปกรณ์ (hardware) รวมถึง virtual machine ให้ครบถ้วน และเป็นปัจจุบัน โดยมีตัวอย่างของรายละเอียด ดังนี้</p> <ol style="list-style-type: none"> (1) เลขทะเบียนทรัพย์สิน (2) ประเภทฮาร์ดแวร์ (3) รายละเอียดทางเทคนิค ยี่ห้อ รุ่น

ข้อกำหนด	แนวปฏิบัติ																													
	(4) ระบบปฏิบัติการและเวอร์ชัน (5) เจ้าของทรัพย์สิน (6) ผู้ดูแลทรัพย์สิน (7) สถานที่ตั้ง (8) วันที่เริ่มใช้งาน/วันที่ติดตั้ง (9) วันที่สิ้นสุดการรับประกัน หรือสิ้นสุดการใช้งานตามสัญญา (10) ประเภทการครอบครอง (ซื้อ หรือเช่า)																													
	ตัวอย่างเช่น																													
	<table border="1"> <thead> <tr> <th>เลขทะเบียนทรัพย์สิน</th> <th>ประเภท</th> <th>รายละเอียด</th> <th>ระบบปฏิบัติการ/เวอร์ชัน</th> <th>เจ้าของทรัพย์สิน</th> <th>ผู้ดูแลทรัพย์สิน</th> <th>สถานที่ตั้ง</th> <th>วันที่เริ่มใช้งาน</th> <th>วันที่สิ้นสุดประกัน</th> <th>การครอบครอง</th> </tr> </thead> <tbody> <tr> <td>RT123456</td> <td>Switch</td> <td>ยี่ห้อ CC รุ่น 1000 48 ports</td> <td>A-OS 1.0.2</td> <td>ฝ่าย IT</td> <td>บริษัท A</td> <td>สำนักงาน</td> <td>1 มี.ค. 64</td> <td>1 มี.ค. 67</td> <td>ซื้อ</td> </tr> <tr> <td>SV212224</td> <td>Router</td> <td>ยี่ห้อ JP รุ่น 3700 8 ports</td> <td>13.2B</td> <td>ฝ่าย IT</td> <td>ฝ่าย IT</td> <td>สำนักงาน</td> <td>5 พ.ค. 64</td> <td>5 พ.ค. 66</td> <td>เช่า</td> </tr> </tbody> </table>	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
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 <ol style="list-style-type: none"> (1) เลขทะเบียนทรัพย์สิน (2) ชื่อซอฟต์แวร์ (3) รายละเอียดทางเทคนิค/การใช้งาน (4) ระบบปฏิบัติการและเวอร์ชัน (5) หน่วยงานภายในผู้เป็นเจ้าของซอฟต์แวร์ 																													

ข้อกำหนด	แนวปฏิบัติ																
	<p>(6) วันที่ลงทะเบียนซอฟต์แวร์</p> <p>(7) วันที่สิ้นสุดการใช้บริการ</p> <p>(8) เลขทะเบียนทรัพย์สินฮาร์ดแวร์ที่อ้างอิง</p> <p><u>ตัวอย่างเช่น</u></p> <table border="1" data-bbox="721 443 2078 837"> <thead> <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> </thead> <tbody> <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> </tbody> </table> <p>4. สำนักงานสอบบัญชีควรปรับปรุงทะเบียนทรัพย์สินสารสนเทศต่าง ๆ ให้ครบถ้วนและเป็นปัจจุบันอยู่อย่างสม่ำเสมอ อย่างน้อยปีละ 1 ครั้ง และทุกครั้งที่มีการเปลี่ยนแปลงระบบงาน IT อย่างมีนัยสำคัญ</p>	เลขทะเบียนทรัพย์สิน	ชื่อซอฟต์แวร์	รายละเอียดทางเทคนิค / การใช้งาน	ระบบปฏิบัติการและเวอร์ชัน	หน่วยงานภายในผู้เป็นเจ้าของซอฟต์แวร์	วันที่ลงทะเบียนซอฟต์แวร์	วันที่สิ้นสุดการใช้บริการ	เลขทะเบียนทรัพย์สินฮาร์ดแวร์ (เพื่อใช้อ้างอิง)	SP123456	Sheet processor pro	Software ประมวลผล sheet/excel	10.2.3A	IT	1 พ.ค. 64	1 ธ.ค. 69	SV123456
เลขทะเบียนทรัพย์สิน	ชื่อซอฟต์แวร์	รายละเอียดทางเทคนิค / การใช้งาน	ระบบปฏิบัติการและเวอร์ชัน	หน่วยงานภายในผู้เป็นเจ้าของซอฟต์แวร์	วันที่ลงทะเบียนซอฟต์แวร์	วันที่สิ้นสุดการใช้บริการ	เลขทะเบียนทรัพย์สินฮาร์ดแวร์ (เพื่อใช้อ้างอิง)										
SP123456	Sheet processor pro	Software ประมวลผล sheet/excel	10.2.3A	IT	1 พ.ค. 64	1 ธ.ค. 69	SV123456										
3.2 กำหนดบุคคลหรือหน่วยงานซึ่งรับผิดชอบทรัพย์สินด้าน IT แต่ละรายการ	1. สำนักงานสอบบัญชีควรกำหนดบุคคลหรือหน่วยงานที่รับผิดชอบในการจัดทำและปรับปรุงทะเบียนรายการทรัพย์สินด้าน IT รวมถึงบำรุงรักษาทรัพย์สินด้าน IT อย่างสม่ำเสมอตลอดอายุการใช้งานของทรัพย์สินดังกล่าว																
3.3 จัดให้มีการบำรุงรักษาทรัพย์สินด้าน IT อย่างสม่ำเสมอ	1. สำนักงานสอบบัญชีควรบำรุงรักษาทรัพย์สินด้าน IT ให้มีสภาพพร้อมใช้งานและรองรับการดำเนินงานอย่างต่อเนื่อง พร้อมทั้งวางแผนรองรับทรัพย์สินด้าน IT ที่ใกล้จะสิ้นสุดอายุการใช้งาน (end of life) หรือสิ้นสุดการสนับสนุนหรือให้บริการจากผู้ผลิต (end of support) ได้อย่างเหมาะสมทันการณ์ ทั้งนี้ ในกรณีที่มีความจำเป็นต้องใช้ทรัพย์สินที่สิ้นสุดอายุการใช้งานหรือสิ้นสุดการสนับสนุนหรือให้บริการจากผู้ผลิต สำนักงานสอบบัญชีควรประเมินความเสี่ยงและจัดให้มีมาตรการควบคุมความเสี่ยงอย่างเหมาะสม																
2.4 การรักษาความมั่นคงปลอดภัยของข้อมูล (data security)																	
<p>ส่วนที่ 4 การรักษาความมั่นคงปลอดภัยของข้อมูล (data security)</p> <p>สำนักงานสอบบัญชีต้องจัดให้มีการรักษาความมั่นคงปลอดภัยของข้อมูลเพื่อให้ข้อมูลมีความถูกต้องครบถ้วน</p>																	

ข้อกำหนด	แนวปฏิบัติ
และมีสภาพพร้อมใช้งาน รวมถึงสามารถรักษาความลับของข้อมูลได้อย่างเหมาะสม ดังนี้	
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 2. สำนักงานสอบบัญชีควรจัดให้มีการรักษาความปลอดภัยของข้อมูลที่อยู่บนสื่อบันทึกข้อมูล โดยดำเนินการ ดังนี้ (1) คำนึงถึงความเสี่ยงที่สื่อบันทึกข้อมูลอาจเสื่อมสภาพ รวมทั้งวิธีการนำข้อมูลกลับมาใช้งานใหม่ ในกรณีที่จัดเก็บข้อมูลเป็นระยะเวลานาน (2) จัดเก็บสื่อบันทึกข้อมูลในพื้นที่ที่มีความมั่นคงปลอดภัย และเป็นไปตามคำแนะนำของผู้ผลิต (ถ้ามี) (3) จัดให้มีมาตรการรักษาความปลอดภัยของการขนส่งสื่อบันทึกข้อมูล (physical media transfer)
4.3 การจัดให้มีแนวทางในการนำเข้า ประมวลผล และทำลายข้อมูลอย่างปลอดภัย	1. สำนักงานสอบบัญชีควรกำหนดระเบียบปฏิบัติในการทำลายข้อมูล (data disposal) ซึ่งครอบคลุมหน้าที่ความรับผิดชอบของเจ้าของข้อมูล หน่วยงานที่เกี่ยวข้อง และวิธีการทำลายข้อมูลที่เหมาะสมกับชั้นความลับของข้อมูล 2. สำนักงานสอบบัญชีควรจัดให้มีกระบวนการควบคุมการทำลายข้อมูลที่ครอบคลุมการขออนุมัติจากเจ้าของข้อมูลก่อนดำเนินการ การควบคุมและสอบทานการปฏิบัติงาน และการจัดทำทะเบียนการทำลายข้อมูลสำคัญ
4.4 การจัดทำทะเบียนทรัพย์สินด้าน IT ประเภทข้อมูล (data inventory) ให้ครบถ้วนและเป็นปัจจุบัน	1. สำนักงานสอบบัญชีควรจัดทำทะเบียนทรัพย์สินประเภทข้อมูล (data inventory) ให้ครบถ้วนและเป็นปัจจุบัน โดยมีตัวอย่างของรายละเอียด ดังนี้ (1) เลขทะเบียนข้อมูล (2) ชื่อข้อมูลหรือชุดข้อมูล (3) รายละเอียดลักษณะ และประเภทของข้อมูล (4) ระดับชั้นความลับและระดับความสำคัญของข้อมูล (5) เจ้าของข้อมูลและผู้ดูแลข้อมูล (data owner) (6) สถานที่ หรือเครื่องแม่ข่ายที่จัดเก็บ

ข้อกำหนด	แนวปฏิบัติ																											
	<p style="text-align: center;">ตัวอย่างเช่น</p> <table border="1" data-bbox="719 293 2085 643"> <thead> <tr> <th data-bbox="719 293 898 395">เลขทะเบียนข้อมูล</th> <th data-bbox="898 293 1095 395">ชื่อข้อมูล/ชุดข้อมูล</th> <th data-bbox="1095 293 1335 395">รายละเอียด</th> <th data-bbox="1335 293 1498 395">ระดับชั้นความลับ</th> <th data-bbox="1498 293 1740 395">เจ้าของข้อมูล</th> <th data-bbox="1740 293 1868 395">ผู้ดูแลข้อมูล</th> <th data-bbox="1868 293 2085 395">สถานที่จัดเก็บ</th> </tr> </thead> <tbody> <tr> <td data-bbox="719 395 898 491">ABC-IT-001</td> <td data-bbox="898 395 1095 491">IT security policy</td> <td data-bbox="1095 395 1335 491">นโยบายด้าน IT</td> <td data-bbox="1335 395 1498 491">Internal</td> <td data-bbox="1498 395 1740 491">ฝ่าย IT</td> <td data-bbox="1740 395 1868 491">ฝ่าย IT</td> <td data-bbox="1868 395 2085 491">ระบบ Intranet</td> </tr> <tr> <td data-bbox="719 491 898 643">ABC-Data-002</td> <td data-bbox="898 491 1095 643">Customer information</td> <td data-bbox="1095 491 1335 643">ข้อมูลของลูกค้า ได้แก่ ชื่อ สกุล วันเดือนปีเกิด</td> <td data-bbox="1335 491 1498 643">Confidential</td> <td data-bbox="1498 491 1740 643">ฝ่ายปฏิบัติการหลักทรัพย์</td> <td data-bbox="1740 491 1868 643">ฝ่าย IT</td> <td data-bbox="1868 491 2085 643">- DB server 015 - DB backup 012</td> </tr> </tbody> </table>							เลขทะเบียนข้อมูล	ชื่อข้อมูล/ชุดข้อมูล	รายละเอียด	ระดับชั้นความลับ	เจ้าของข้อมูล	ผู้ดูแลข้อมูล	สถานที่จัดเก็บ	ABC-IT-001	IT security policy	นโยบายด้าน IT	Internal	ฝ่าย IT	ฝ่าย IT	ระบบ Intranet	ABC-Data-002	Customer information	ข้อมูลของลูกค้า ได้แก่ ชื่อ สกุล วันเดือนปีเกิด	Confidential	ฝ่ายปฏิบัติการหลักทรัพย์	ฝ่าย IT	- DB server 015 - DB backup 012
เลขทะเบียนข้อมูล	ชื่อข้อมูล/ชุดข้อมูล	รายละเอียด	ระดับชั้นความลับ	เจ้าของข้อมูล	ผู้ดูแลข้อมูล	สถานที่จัดเก็บ																						
ABC-IT-001	IT security policy	นโยบายด้าน IT	Internal	ฝ่าย IT	ฝ่าย IT	ระบบ Intranet																						
ABC-Data-002	Customer information	ข้อมูลของลูกค้า ได้แก่ ชื่อ สกุล วันเดือนปีเกิด	Confidential	ฝ่ายปฏิบัติการหลักทรัพย์	ฝ่าย IT	- DB server 015 - DB backup 012																						
2.5 การควบคุมการเข้าถึงข้อมูลและระบบงาน IT (access control)																												
<p>ส่วนที่ 5 การควบคุมการเข้าถึงข้อมูลและระบบงาน IT (access control)</p> <p>สำนักงานสอบบัญชีต้องจัดให้มีการควบคุมการเข้าถึงข้อมูลและระบบงาน IT อย่างมีประสิทธิภาพ เพื่อให้สามารถป้องกันการเข้าถึง และเปลี่ยนแปลงแก้ไขโดยผู้ไม่มีสิทธิหรือไม่ได้รับอนุญาต ดังนี้</p>																												
<p>5.1 จัดให้มีแนวทางการบริหารจัดการบัญชีผู้ใช้งาน และสิทธิการเข้าถึง โดยมีการทบทวนปรับปรุงสิทธิให้เหมาะสมอย่างสม่ำเสมอ สอดคล้องกับหน้าที่ความรับผิดชอบ รวมถึงมีกระบวนการเพิกถอนสิทธิเมื่อสิ้นสุดความจำเป็นต้องใช้งาน</p> <p>ทั้งนี้ หากสำนักงานสอบบัญชีไม่สามารถกำหนดแนวทางการบริหารจัดการบัญชีและสิทธิการเข้าถึงข้อมูลและระบบงาน IT ตามลักษณะขั้นต่ำของแนวปฏิบัตินี้ทุกข้อได้ สำนักงานสอบบัญชีต้องกำหนดให้มีการควบคุม</p>	<ol style="list-style-type: none"> 1. แนวทางการบริหารจัดการบัญชีผู้ใช้งาน ควรครอบคลุมอย่างน้อย ดังนี้ <ol style="list-style-type: none"> (1) หน่วยงาน หรือบุคลากร ที่รับผิดชอบในการบริหารจัดการบัญชีผู้ใช้งาน (2) ขั้นตอนการสร้างบัญชีผู้ใช้งาน โดยบัญชีผู้ใช้งาน (user ID) ควรระบุตัวตนผู้ใช้งานได้ และหลีกเลี่ยงการใช้บัญชีผู้ใช้งานที่มีผู้ใช้งานมากกว่า 1 ราย (shared ID) (3) การจำกัดหรือหลีกเลี่ยงใช้งานบัญชีผู้ใช้งานที่มาพร้อมกับระบบ (default user account) (4) การทบทวนบัญชีผู้ใช้งานอย่างน้อยปีละ 1 ครั้ง (5) การระงับหรือลบบัญชีผู้ใช้งานเมื่อ (1) ผู้ใช้งานสิ้นสุดสภาพการเป็นพนักงาน และ (2) ไม่มีความจำเป็นต้องใช้งาน 2. แนวทางการบริหารจัดการสิทธิการเข้าถึงข้อมูลและระบบงาน IT ควรครอบคลุมอย่างน้อย ดังนี้ <ol style="list-style-type: none"> (1) หน่วยงานหรือบุคลากรที่รับผิดชอบในการบริหารจัดการสิทธิการเข้าถึงข้อมูลและระบบงาน IT (2) ขั้นตอนการขออนุมัติสิทธิในการเข้าถึงข้อมูลและระบบงาน IT จากผู้มีอำนาจ เช่น เจ้าของระบบ หรือเจ้าของข้อมูล เป็นต้น 																											

ข้อกำหนด	แนวปฏิบัติ
<p>อินทแดนเพื่อตอบสนองต่อความเสี่ยงที่อาจเกิดขึ้นจากบัญชีผู้ใช้งานและสิทธิการเข้าถึงที่ไม่เหมาะสม</p>	<p>(3) ขั้นตอนการปรับปรุงสิทธิของผู้ใช้งานเมื่อมีการเปลี่ยนแปลงหน้าที่ความรับผิดชอบหรือตำแหน่งงาน</p> <p>(4) ขั้นตอนการเพิกถอนสิทธิของผู้ใช้งาน โดยเพิกถอนสิทธิทันทีเมื่อผู้ใช้งานสิ้นสุดสภาพการเป็นพนักงาน และเมื่อไม่มี ความจำเป็นต้องใช้งาน</p> <p>(5) การแบ่งแยกบทบาทหน้าที่ของบุคคลที่เกี่ยวข้องในการจัดสรรสิทธิ เช่น ผู้ร้องขอ (access request) ผู้มีอำนาจอนุมัติ (access authorization) และผู้ดูแลสิทธิการเข้าถึง (access administration) เป็นต้น เพื่อให้สอดคล้องตามหลักการถ่วงดุล (check and balance) ที่ดี</p> <p>(6) กำหนดสิทธิของผู้ใช้งานโดยคำนึงถึงความจำเป็นต้องรู้ (need-to-know) ความจำเป็นต้องใช้งาน (need-to-use) และหลักการแบ่งแยกหน้าที่ความรับผิดชอบ (segregation of duties)</p> <p>(7) จัดทำตารางควบคุมการให้สิทธิ (authorization matrix) ของผู้ใช้งานที่สอดคล้องกับตำแหน่งหน้าที่และความรับผิดชอบ เพื่อใช้เป็นแนวทางการกำหนดสิทธิอย่างถูกต้องเหมาะสม</p> <p>(8) ทบทวนสิทธิการเข้าถึงอย่างสม่ำเสมอ อย่างน้อยปีละ 1 ครั้ง โดยกำหนดรอบระยะเวลาในการทบทวนสิทธิให้สอดคล้องกับ ความเสี่ยงและความสำคัญของสิทธิ</p>
<p>5.2 จัดให้มีกระบวนการยืนยันตัวตนผู้ใช้งาน (authentication) ที่เหมาะสมกับความเสี่ยง ทั้งนี้ หากสำนักงานสอบบัญชีไม่สามารถกำหนด กระบวนการยืนยันตัวตนผู้ใช้งาน (authentication) ที่เหมาะสมตามลักษณะขั้นต่ำของแนวปฏิบัตินี้ทุกข้อได้ สำนักงานสอบบัญชีต้องกำหนดให้มีการควบคุมอื่น ทดแทนเพื่อตอบสนองต่อความเสี่ยงที่อาจเกิดขึ้นจาก การเข้าถึงระบบโดยไม่ได้รับอนุญาต</p>	<p>1. สำนักงานสอบบัญชีควรจัดให้มีกระบวนการยืนยันตัวตนผู้ใช้งาน (authentication) ที่มีประสิทธิภาพเหมาะสมกับความเสี่ยงของ การเข้าถึงระบบโดยไม่ได้รับอนุญาต โดยครอบคลุมอย่างน้อย ดังนี้</p> <p>(1) กำหนดวิธีการยืนยันตัวตนผู้ใช้งานที่เหมาะสมกับความเสี่ยง</p> <p>(2) กรณีที่มีการสร้างรหัสผ่านครั้งแรกสำหรับผู้ใช้งาน ให้มีการจัดส่งรหัสผ่านให้แก่ผู้ใช้งานด้วยวิธีการที่รัดกุมและปลอดภัย และให้ ผู้ใช้งานเปลี่ยนแปลงรหัสผ่านทันทีที่ได้รับรหัสดังกล่าว</p> <p>(3) กำหนดให้ผู้ใช้งานตั้งรหัสผ่านที่ซับซ้อนและยากต่อการคาดเดา โดยมีความยาวขั้นต่ำ 8 อักขระ (8 characters) และ ประกอบด้วยตัวเลขและตัวอักษร ทั้งนี้ สำนักงานสอบบัญชีอาจพิจารณาเพิ่มความซับซ้อนโดยกำหนดให้รหัสผ่านประกอบด้วย ตัวเลข ตัวอักษรพิมพ์ใหญ่ ตัวอักษรพิมพ์เล็ก และอักขระพิเศษ (เช่น “#”)</p> <p>(4) กำหนดจำนวนครั้งที่ยอมให้ผู้ใช้งานใส่รหัสผ่านผิดพลาดติดต่อกัน ก่อนระงับการเข้าสู่ระบบชั่วคราวหรือวิธีการอื่น ๆ ที่เทียบเท่า เพื่อป้องกันการเข้าใช้งานโดยวิธีเดาสุ่ม (brute force) ทั้งนี้ ในทางปฏิบัติไม่ควรยอมให้ผู้ใช้งานยืนยันตัวตน ผิดพลาดติดต่อกันเกิน 10 ครั้ง</p> <p>(5) กำหนดให้การเปลี่ยนรหัสผ่านใหม่ไม่ซ้ำกับรหัสที่ใช้งานอย่างน้อย 4 ครั้งล่าสุด หรือไม่ซ้ำกับรหัสผ่านที่ใช้งานในช่วง 1 ปี ที่ผ่านมา</p>

ข้อกำหนด	แนวปฏิบัติ
	<p>(6) กำหนดการตั้งค่าปกติ (default) ให้ไม่แสดงรหัสผ่านบนหน้าจอ ระหว่างที่ผู้ใช้งานใส่รหัสผ่าน</p> <p>(7) มีวิธีจัดเก็บข้อมูลรหัสผ่านที่ปลอดภัย เพื่อป้องกันการลวงรู้หรือแก้ไขเปลี่ยนแปลง รวมทั้งไม่จัดเก็บข้อมูลรหัสผ่านใน folder เดียวกันกับ folder ที่จัดเก็บข้อมูลของแอปพลิเคชัน</p> <p>(8) กำหนดให้ผู้ใช้งานรับผิดชอบการใช้งานบัญชีผู้ใช้งาน (user ID) และการรักษาความปลอดภัยสิ่งที่ยืนยันตัวตน (authenticator) เช่น รหัสผ่าน รหัสที่ใช้ครั้งเดียว (one-time password) เป็นต้น รวมทั้งข้อมูลส่วนบุคคลที่อาจนำมาใช้เพื่อขอเปลี่ยนแปลงข้อมูลบัญชีผู้ใช้งาน เพื่อป้องกันการใช้งานจากผู้ไม่หวังดี</p>
<p>5.3 กำหนดมาตรการควบคุม จำกัด และติดตามการใช้งานบัญชี privileged user (privileged user management) ดังนี้ (ถ้ามี)</p> <p>5.3.1 มี Multi-Factor Authentication (“MFA”) หรือ วิธีการยืนยันตัวตนเพิ่มเติมหลังจากทำการยืนยันตัวตนโดยการใส่รหัสผ่าน เพื่ออนุญาตเข้าใช้งานระบบงาน IT และเมื่อเข้าใช้งานและเปลี่ยนรหัสผ่านสำหรับระบบปฏิบัติการและระบบฐานข้อมูลที่เกี่ยวข้องกับระบบงาน IT ที่มีนัยสำคัญ</p> <p>5.3.2 กรณีสำนักงานสอบบัญชีมีข้อจำกัดสำหรับ MFA สามารถใช้วิธีการอื่นใดที่เทียบเท่าทดแทน และจัดให้มีการประเมินความเสี่ยงและพิจารณาแนวทางการควบคุมความเสี่ยงก่อนดำเนินการเพื่อขออนุมัติยกเว้น (exception)</p>	<p>หากสำนักงานสอบบัญชีมีการใช้งานบัญชี privileged user ต้องมีการดำเนินการตามข้อ 5.3.1 ถึง 5.3.3 เป็นอย่างน้อย</p>
<p>5.3.3 มีการควบคุมและติดตามตรวจสอบการใช้งานบัญชี privileged user</p>	<p>1. สำนักงานสอบบัญชีควรจัดให้มีการควบคุมและติดตามการใช้บัญชี privileged user ดังนี้</p> <p>(1) ควบคุมดูแลการให้สิทธิโดยจำกัดตามบทบาทหน้าที่ และความจำเป็นในการใช้งาน</p> <p>(2) จำกัดจำนวนบัญชี privileged user ให้มีจำนวนน้อยที่สุดหรือเท่าที่จำเป็น</p> <p>(3) มีกระบวนการขอใช้งานบัญชี privileged user และการอนุมัติโดยผู้มีอำนาจ</p> <p>(4) ทบทวนบัญชีผู้ใช้งาน privileged user อย่างสม่ำเสมออย่างน้อยปีละ 1 ครั้ง</p>

ข้อกำหนด	แนวปฏิบัติ
	<p>(5) กำหนดนโยบายหรือมาตรการยืนยันตัวตนของบัญชี privileged user ที่เข้มงวดกว่าบัญชีผู้ใช้งานทั่วไป</p> <p>(6) จัดเก็บบันทึกการยืนยันตัวตนและการเข้าถึง (authentication log และ access log) และการดำเนินงาน (activity log) ของบัญชี privileged user อย่างเหมาะสม</p> <p>(7) สอบทานบันทึกการยืนยันตัวตนและการเข้าถึง (authentication log และ access log) และการดำเนินงาน (activity log) ของบัญชี privileged user หลังเสร็จสิ้นการใช้งาน หรือสอบทานสม่ำเสมอตามรอบระยะเวลาที่เหมาะสมกับความเสี่ยง หรือ อย่างน้อยปีละ 1 ครั้ง เพื่อให้มั่นใจได้ว่าการใช้งานสิทธิเป็นไปตามขอบเขตและหน้าที่ที่ได้รับมอบหมาย</p>
<p>2.6 การควบคุมการเข้ารหัส (cryptographic control) (ถ้ามี)</p>	
<p>ส่วนที่ 6 การควบคุมการเข้ารหัส (cryptographic control)</p> <p>หากสำนักงานสอบบัญชีมีการเข้ารหัสข้อมูล สำนักงานสอบบัญชีต้องจัดให้มีการควบคุมการเข้ารหัสที่เชื่อถือได้และเป็นไปตามมาตรฐานสากลโดยกำหนดวิธีการเข้ารหัสข้อมูล (encryption) และการบริหารจัดการกุญแจเข้ารหัส (key management) อย่างปลอดภัยเพื่อให้มั่นใจได้ว่า การอ้างไว้ซึ่งความลับ (confidentiality) ความถูกต้องครบถ้วน (integrity) และความถูกต้องแท้จริง (authenticity) ของข้อมูล มีความเหมาะสมและมีประสิทธิภาพ ดังนี้</p>	
<p>6.1 กำหนดวิธีการเข้ารหัสที่ปลอดภัย</p>	<p>ในการกำหนดวิธีการเข้ารหัสที่ปลอดภัย สำนักงานสอบบัญชีควรดำเนินการอย่างน้อย ดังนี้</p> <ol style="list-style-type: none"> กำหนดความรับผิดชอบของหน่วยงานหรือบุคลากรที่เกี่ยวข้อง กำหนดมาตรฐานวิธีการเข้ารหัสข้อมูล (cryptographic algorithm) ให้เป็นไปตามมาตรฐานสากล และมีความมั่นคงปลอดภัยเหมาะสมกับระดับความสำคัญของข้อมูล การกำหนดกรอบระยะเวลาในการทบทวนมาตรฐานวิธีการเข้ารหัสข้อมูล เพื่อให้มั่นใจว่าวิธีการเข้ารหัสข้อมูลที่ใช้กันอยู่ ยังมีความมั่นคงเพียงพอในการรักษาความปลอดภัยของข้อมูล
<p>6.2 กำหนดการบริหารจัดการกุญแจเข้ารหัส โดยจัดให้มี</p>	<ol style="list-style-type: none"> การสร้างและติดตั้งกุญแจเข้ารหัส สำนักงานสอบบัญชีควรดำเนินการอย่างน้อย ดังนี้

ข้อกำหนด	แนวปฏิบัติ
<p>มาตรการการควบคุมตั้งแต่การสร้างและติดตั้งกุญแจเข้ารหัส การจัดเก็บและสำรองกุญแจเข้ารหัส ไปจนถึงการเพิกถอนหรือทำลายกุญแจเข้ารหัส</p>	<p>(1) ควบคุมสภาพแวดล้อมและกระบวนการในการสร้างกุญแจเข้ารหัสที่รัดกุมปลอดภัย เช่น เลือกใช้ผู้ให้บริการออกใบรับรอง (certification authority) ที่น่าเชื่อถือ และมีการทำลายข้อมูลที่อาจหลงเหลือภายหลังการสร้างกุญแจเข้ารหัสแล้วเสร็จ เพื่อป้องกันเข้าถึงหรือกู้คืนกุญแจเข้ารหัสข้อมูลโดยไม่ได้รับอนุญาต เป็นต้น</p> <p>(2) กำหนดสิทธิการเข้าถึงกุญแจเข้ารหัสให้สามารถเข้าถึงได้โดยผู้ที่ได้รับอนุญาตเท่านั้น</p> <p>(3) กำหนดความยาวของกุญแจเข้ารหัสที่เพียงพอในการป้องกันการถอดรหัส (decrypt) โดยผู้ไม่หวังดี เช่น การโจมตีแบบ brute force เป็นต้น</p> <p>(4) แลกเปลี่ยนกุญแจเข้ารหัส (key exchange) ผ่านกระบวนการและช่องทางที่ปลอดภัย</p> <p>2. การจัดเก็บและการสำรองกุญแจเข้ารหัส สำนักงานสอบบัญชีควรดำเนินการอย่างน้อย ดังนี้</p> <p>(1) มีการรักษาความปลอดภัยในการจัดเก็บกุญแจเข้ารหัสทั้งด้าน physical และ logical เช่น การใช้อุปกรณ์ Hardware Security Module (HSM) หรืออุปกรณ์ที่ทำหน้าที่ในลักษณะเดียวกัน เป็นต้น</p> <p>(2) มีการสำรองข้อมูลกุญแจเข้ารหัส โดยวิธีการเก็บรักษาข้อมูลกุญแจเข้ารหัสชุดสำรองต้องมีการรักษาความปลอดภัยในระดับเดียวกับกุญแจเข้ารหัสชุดหลัก</p> <p>3. การเพิกถอนหรือทำลายกุญแจเข้ารหัส สำนักงานสอบบัญชีควรดำเนินการอย่างน้อย ดังนี้</p> <p>(1) กำหนดเกณฑ์และแนวทางในการเปลี่ยนและเพิกถอนกุญแจเข้ารหัส เช่น กรณีกุญแจเข้ารหัสหมดอายุการใช้งาน หรือไม่ปลอดภัย เป็นต้น</p> <p>(2) กำหนดกระบวนการทำลายกุญแจ เพื่อให้มั่นใจว่าจะไม่สามารถนำกุญแจนั้นมาใช้งานได้อีก</p> <p>4. สำนักงานสอบบัญชีควรจัดเก็บข้อมูลบันทึกเหตุการณ์กิจกรรมสำคัญที่เกี่ยวกับกุญแจเข้ารหัส เช่น การสร้างกุญแจ การสำรองกุญแจ การเข้าถึงหรือใช้งานกุญแจ และการเพิกถอนกุญแจ เป็นต้น</p>
<p>6.3 กำหนดมาตรการการควบคุมกุญแจเข้ารหัสที่ให้บริการโดยบุคคลภายนอก ซึ่งต้องตรวจสอบเพื่อให้มั่นใจได้ว่ากุญแจการเข้ารหัสที่สร้างขึ้นไม่มีการนำมาใช้ร่วมกับบุคคลอื่น</p>	<p>1. กรณีที่สำนักงานสอบบัญชีไม่สามารถสร้างกุญแจเข้ารหัสด้วยตนเองได้ หรือมีความจำเป็นต้องใช้กุญแจเข้ารหัสที่ให้บริการโดยบุคคลภายนอก สำนักงานสอบบัญชีควรดำเนินการเพื่อให้มั่นใจได้ว่ากุญแจเข้ารหัสที่ให้บริการโดยบุคคลภายนอกไม่มีการนำมาใช้งานร่วมกับผู้ใช้บริการรายอื่นและมีความมั่นคงปลอดภัย โดยพิจารณาเงื่อนไขหรือรายละเอียดของการให้บริการ ดังนี้</p> <p>(1) ประเภทของกุญแจเข้ารหัส</p> <p>(2) รายละเอียดของระบบ และกระบวนการบริหารจัดการกุญแจเข้ารหัส</p> <p>(3) ข้อเสนอการใช้งานและการควบคุมการเข้ารหัสข้อมูล</p>
<p>6.4 กำหนดกระบวนการรองรับกรณีเกิดการรั่วไหลของ</p>	<p>1. สำนักงานสอบบัญชีควรกำหนดกิจกรรมที่ต้องดำเนินการเมื่อเกิดการรั่วไหลของกุญแจเข้ารหัส เช่น การติดต่อหน่วยงานและ</p>

ข้อกำหนด	แนวปฏิบัติ
<p>กฎแฉเข้ารหัส</p>	<p>ผู้ที่เกี่ยวข้องกับชุดข้อมูลที่ใช้กฎแฉเข้ารหัสชุดดังกล่าว การตรวจสอบชุดข้อมูลที่มีความเสี่ยงในการรั่วไหล การเปลี่ยนหรือเพิกถอน กฎแฉการเข้ารหัสข้อมูล เป็นต้น</p>
<p>2.7 การรักษาความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อม (physical and environmental security)</p>	
<p>ส่วนที่ 7 การรักษาความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อม (physical and environmental security)</p> <p>สำนักงานสอบบัญชีต้องจัดให้มีการรักษาความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อมของทรัพย์สินด้าน IT พร้อมทั้งมีระบบการป้องกัน และกระบวนการบำรุงรักษาฮาร์ดแวร์และระบบสารสนเทศ (facilities) ที่เกี่ยวข้องกับ IT เพื่อให้สามารถป้องกันความเสียหายต่อทรัพย์สินด้าน IT ซึ่งรวมถึงอุปกรณ์ที่จัดเก็บอยู่ในศูนย์คอมพิวเตอร์หลัก ศูนย์คอมพิวเตอร์สำรอง หรือ ศูนย์คอมพิวเตอร์จากบุคคลภายนอก (co-location) (ถ้ามี)</p>	<ol style="list-style-type: none"> 1. สำนักงานสอบบัญชีควรรออกแบบศูนย์คอมพิวเตอร์ และพื้นที่ที่เกี่ยวข้องกับระบบงาน IT ที่มีนัยสำคัญ โดยคำนึงถึงความเสี่ยงจากภัยธรรมชาติและภัยคุกคามจากมนุษย์ เช่น มีกำแพงหรือรั้วที่มั่นคง และมีระยะห่างของศูนย์คอมพิวเตอร์สำรองและศูนย์คอมพิวเตอร์หลักที่เพียงพอ เป็นต้น 2. สำนักงานสอบบัญชีควรมีการบริหารจัดการสิทธิการเข้าถึงศูนย์คอมพิวเตอร์ และพื้นที่ที่เกี่ยวข้องกับระบบงาน IT ที่มีนัยสำคัญ โดยครอบคลุมการดำเนินการอย่างน้อย ดังนี้ <ol style="list-style-type: none"> (1) ให้สิทธิการเข้าถึงตามหลักความจำเป็น (2) อนุมัติสิทธิการเข้าถึงโดยผู้มีอำนาจ (3) ปรับปรุง/ยกเลิกสิทธิการเข้าถึง ทันทีที่พนักงานลาออกหรือเปลี่ยนหน้าที่ความรับผิดชอบ (4) ทบทวนสิทธิการเข้าถึงอย่างสม่ำเสมออย่างน้อยปีละ 1 ครั้ง 3. สำนักงานสอบบัญชีควรจัดให้มีวิธีการยืนยันตัวตนผู้เข้า-ออกศูนย์คอมพิวเตอร์ และพื้นที่ที่เกี่ยวข้องกับระบบงาน IT ที่มีนัยสำคัญ เช่น การใช้ access card door หรือ ลงชื่อในใบลงชื่อเข้า-ออก เป็นต้น ทั้งนี้ สำหรับพื้นที่ที่มีความเสี่ยงสูง สำนักงานสอบบัญชีอาจพิจารณาใช้วิธีการยืนยันตัวตนแบบ MFA เช่น ใช้ access card door ร่วมกับรหัสผ่านส่วนตัว (PIN) เป็นต้น 4. สำนักงานสอบบัญชีควรมีมาตรการควบคุมการเข้า-ออกศูนย์คอมพิวเตอร์ และพื้นที่ที่เกี่ยวข้องกับระบบงาน IT ที่มีนัยสำคัญ สำหรับพนักงานที่ไม่ได้มีหน้าที่ปฏิบัติงานประจำหรือผู้ที่เข้าถึงแบบชั่วคราว โดยจัดให้มีการอนุมัติจากผู้มีอำนาจ การบันทึกเหตุการณ์เข้า-ออก และมีการติดตามและควบคุม (escort) อย่างใกล้ชิด ตลอดระยะเวลาปฏิบัติงานในพื้นที่ดังกล่าว 5. สำนักงานสอบบัญชีควรจัดให้มีระบบรักษาความมั่นคงปลอดภัยให้กับศูนย์คอมพิวเตอร์ เช่น ระบบกล้องวงจรปิด ระบบแจ้งเตือนและระงับอัคคีภัย ระบบควบคุมแรงดันและกระแสไฟฟ้า ระบบสำรองไฟฟ้า (uninterrupted power supply) และระบบควบคุมอุณหภูมิและความชื้น เป็นต้น พร้อมทั้งมีการบำรุงรักษาอย่างสม่ำเสมอ 6. สำนักงานสอบบัญชีควรจัดให้มีมาตรการรองรับการทำงานผิดพลาดของระบบสารสนเทศของศูนย์คอมพิวเตอร์ เช่น ระบบไฟฟ้า ระบบโทรคมนาคมและระบบปรับอากาศ เป็นต้น 7. สำนักงานสอบบัญชีควรจัดเก็บอุปกรณ์คอมพิวเตอร์ที่สำคัญ เช่น เครื่องแม่ข่าย และอุปกรณ์เครือข่าย เป็นต้น ไว้ในพื้นที่ที่มีการควบคุม

ข้อกำหนด	แนวปฏิบัติ
	<p>อย่างปลอดภัย</p> <p>8. สำนักงานสอบบัญชีควรจัดให้มีมาตรการป้องกันสายเคเบิลและสายไฟของศูนย์คอมพิวเตอร์จากการขัดขวางการทำงาน หรือการทำให้เสียหาย และบำรุงรักษาอย่างสม่ำเสมอ</p> <p>9. สำนักงานสอบบัญชีควรจัดให้มีการดูแลและบำรุงรักษาทรัพย์สินด้าน IT ประเภทฮาร์ดแวร์อย่างถูกวิธี เพื่อให้อยู่ในสภาพครบถ้วนสมบูรณ์และพร้อมใช้งาน</p> <p>10. สำนักงานสอบบัญชีควรควบคุมมิให้มีการนำทรัพย์สินด้าน IT ประเภทฮาร์ดแวร์ออกนอกพื้นที่โดยมิได้รับอนุญาต</p> <p>11. ก่อนการยกเลิกการใช้งานหรือจำหน่ายทรัพย์สินด้าน IT ประเภทฮาร์ดแวร์ เช่น hard disk, switch, firewall และ router เป็นต้น สำนักงานสอบบัญชีควรจัดเก็บทรัพย์สินในพื้นที่ปลอดภัย และตรวจสอบให้มั่นใจว่าได้มีการลบ ย้าย ทำลายข้อมูลสำคัญและข้อมูลการปรับแต่ง (configuration) หรือปรับค่าดังกล่าวกลับไปสู่ค่าตั้งต้น (factory reset) ด้วยวิธีการที่ไม่สามารถกู้คืนได้อีก</p>
<p>2.8 การรักษาความมั่นคงปลอดภัยในการปฏิบัติงานด้าน IT (IT operations security)</p>	
<p>ส่วนที่ 8 การรักษาความมั่นคงปลอดภัยในการปฏิบัติงานด้าน IT (IT operations security)</p> <p>สำนักงานสอบบัญชีต้องมีมาตรการรักษาความมั่นคงปลอดภัยในการปฏิบัติงานด้าน IT เพื่อให้การปฏิบัติงานเกี่ยวกับการประมวลผลข้อมูลมีความถูกต้องและมั่นคงปลอดภัย โดยต้องครอบคลุมการบริหารจัดการอย่างน้อยในเรื่องดังนี้</p>	
<p>2.8.1 การบริหารจัดการการตั้งค่าระบบ (system configuration management)</p>	
<p>8.1 การบริหารจัดการการตั้งค่าระบบ (system configuration management) โดยมีกระบวนการในการควบคุมการตั้งค่าระบบ และสอบทานการตั้งค่าระบบอย่างสม่ำเสมอ เพื่อให้การตั้งค่าระบบเป็นไปอย่างถูกต้อง และปลอดภัย</p>	<p>1. สำนักงานสอบบัญชีควรกำหนดมาตรฐานการตั้งค่าด้านความมั่นคงปลอดภัย (security configuration standard) หรือ security based line อย่างเป็นลายลักษณ์อักษร เพื่อใช้ในการตั้งค่าระบบปฏิบัติการ ระบบฐานข้อมูล และอุปกรณ์เครือข่าย โดยคำนึงถึงเรื่องดังนี้</p> <p>(1) การลบบัญชีผู้ใช้งานตั้งต้น (default user) หรือการเปลี่ยนแปลงรหัสผ่านตั้งต้น (default password)</p> <p>(2) การใช้วิธีการยืนยันตัวตนที่มีความรัดกุมปลอดภัย</p> <p>(3) การกำหนดบริการ แอปพลิเคชัน และพอร์ตการเชื่อมต่อเท่าที่จำเป็น</p> <p>(4) การจัดเก็บข้อมูลบันทึกเหตุการณ์ (log)</p>

ข้อกำหนด	แนวปฏิบัติ
	<p>(5) การปรับปรุงเวอร์ชันของซอฟต์แวร์หรือ firmware ให้เป็นปัจจุบัน</p> <ol style="list-style-type: none"> 2. สำนักงานสอบบัญชีควรทบทวนและปรับปรุงมาตรฐานการตั้งค่าด้านความมั่นคงปลอดภัย (security configuration standard) หรือ security based line ให้เป็นปัจจุบันอย่างสม่ำเสมอ 3. สำนักงานสอบบัญชีควรตั้งค่าด้านความมั่นคงปลอดภัยของระบบปฏิบัติการ ระบบฐานข้อมูล และอุปกรณ์เครือข่ายตามมาตรฐานที่สำนักงานสอบบัญชีกำหนดไว้ ก่อนการนำไปใช้งาน 4. สำนักงานสอบบัญชีควรสอบทานการตั้งค่าด้านความมั่นคงปลอดภัยของระบบปฏิบัติการ ระบบฐานข้อมูล และอุปกรณ์เครือข่ายอย่างสม่ำเสมอ และทุกครั้งที่มีการเปลี่ยนแปลงระบบและอุปกรณ์ดังกล่าวอย่างมีนัยสำคัญ เพื่อให้สอดคล้องกับมาตรฐานที่สำนักงานสอบบัญชีกำหนดไว้
2.8.2 การบริหารจัดการการเปลี่ยนแปลง (change management)	
<p>8.2 การบริหารจัดการการเปลี่ยนแปลง (change management) อย่างรัดกุมเพียงพอเพื่อให้การเปลี่ยนแปลงเป็นไปตามวัตถุประสงค์ที่กำหนดไว้ อย่างถูกต้องครบถ้วน และป้องกันการเปลี่ยนแปลงโดยที่ไม่ได้รับอนุญาต</p>	<ol style="list-style-type: none"> 1. สำนักงานสอบบัญชีควรกำหนดกระบวนการบริหารจัดการการเปลี่ยนแปลงอย่างเป็นลายลักษณ์อักษรเพื่อควบคุมการเปลี่ยนแปลงโครงสร้างพื้นฐานด้าน IT ระบบงาน IT และขั้นตอนการปฏิบัติงานที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัย 2. สำนักงานสอบบัญชีควรกำหนดบุคคลหรือคณะกรรมการบริหารของสำนักงานสอบบัญชีที่ทำหน้าที่อนุมัติการเปลี่ยนแปลง 3. สำนักงานสอบบัญชีควรแบ่งแยกหน้าที่ (segregation of duties) ผู้ที่เกี่ยวข้องในกระบวนการการเปลี่ยนแปลง เพื่อไม่ให้บุคคลใดบุคคลหนึ่งสามารถปฏิบัติงานได้ตั้งแต่เริ่มต้นจนจบกระบวนการการเปลี่ยนแปลง เช่น ผู้มีสิทธิร้องขอ ผู้ที่มีอำนาจในการอนุมัติการเปลี่ยนแปลง ผู้ที่สามารถดำเนินการเปลี่ยนแปลงระบบ เป็นต้น 4. สำนักงานสอบบัญชีควรจัดให้มีคำขอการเปลี่ยนแปลง (change request) และการอนุมัติการเปลี่ยนแปลง เป็นลายลักษณ์อักษร เพื่อเป็นหลักฐานแสดงให้เห็นว่าการเปลี่ยนแปลงได้ผ่านการพิจารณาจากเจ้าของข้อมูล เจ้าของระบบ หรือผู้มีอำนาจตามสิทธิที่กำหนดไว้ โดยคำขอการเปลี่ยนแปลงควรระบุเหตุผลความจำเป็นและผลกระทบที่อาจเกิดขึ้นจากการเปลี่ยนแปลง 5. สำนักงานสอบบัญชีควรจัดให้มีระบบหรือทะเบียนในการจัดเก็บคำขอเปลี่ยนแปลงและเอกสารรายละเอียดที่เกี่ยวข้อง เพื่อใช้ควบคุมการปฏิบัติงานตั้งแต่ต้นจนจบกระบวนการ และสามารถใช้ในการติดตามและสอบทานการปฏิบัติงาน 6. กรณีที่การเปลี่ยนแปลงมีผลกระทบต่อการทำงาน สำนักงานสอบบัญชีควรสื่อสารให้ผู้เกี่ยวข้องรับทราบการเปลี่ยนแปลงเพื่อให้สามารถปฏิบัติงานได้อย่างถูกต้อง 7. สำนักงานสอบบัญชีควรจัดให้มีแผนการถอยกลับสู่สภาพเดิม (fallback procedure) หากเกิดข้อผิดพลาดจากการเปลี่ยนแปลง เช่น การจัดเก็บเวอร์ชันของระบบก่อนการเปลี่ยนแปลงไว้ เป็นต้น

ข้อกำหนด	แนวปฏิบัติ
2.8.3 การบริหารจัดการขีดความสามารถของระบบงาน IT (capacity management)	
<p>8.3 การบริหารจัดการขีดความสามารถของระบบงาน IT (capacity management) โดยจัดให้มีมาตรฐานและวิธีปฏิบัติเรื่องการจัดการขีดความสามารถ การติดตามประสิทธิภาพการทำงานของระบบ และการประเมินแนวโน้มการใช้ทรัพยากรด้าน IT เพื่อให้สามารถรองรับการดำเนินธุรกิจในปัจจุบัน และสามารถวางแผนการจัดสรรทรัพยากรให้รองรับการใช้งานในอนาคตได้อย่างมีประสิทธิภาพ</p>	<ol style="list-style-type: none"> 1. สำนักงานสอบบัญชีควรกำหนดมาตรฐานและระเบียบวิธีปฏิบัติในการบริหารจัดการขีดความสามารถของระบบ เพื่อประเมินและติดตามดูแลความเพียงพอของโครงสร้างพื้นฐานด้าน IT ที่ครอบคลุมถึงระบบคอมพิวเตอร์ ระบบฐานข้อมูล ระบบเครือข่ายสื่อสาร และระบบสาธารณูปโภคที่เกี่ยวข้องกับงานด้าน IT 2. สำนักงานสอบบัญชีควรจัดทำรายงานความเพียงพอของทรัพยากรด้าน IT นำเสนอต่อหัวหน้าสำนักงานสอบบัญชี หรือคณะกรรมการบริหารของสำนักงานสอบบัญชีรับทราบอย่างสม่ำเสมอ เพื่อให้มีการกำกับดูแลความพร้อมใช้และความเพียงพอของระบบในการรองรับการให้บริการทางธุรกิจได้อย่างต่อเนื่อง และสามารถพิจารณาแนวทางลดความเสี่ยงได้อย่างทันการณ์
2.8.4 การรักษาความมั่นคงปลอดภัยของเครื่องแม่ข่าย (server) และอุปกรณ์ที่ใช้ปฏิบัติงาน (endpoint)	
<p>8.4 การรักษาความมั่นคงปลอดภัยของเครื่องแม่ข่าย (server) และอุปกรณ์ที่ใช้ปฏิบัติงาน (endpoint) เพื่อให้ไม่ถูกใช้เป็นช่องทางที่ทำให้ข้อมูลสำคัญรั่วไหล หรือมีการเข้าใช้งานระบบงาน IT โดยไม่ได้รับอนุญาต</p>	<ol style="list-style-type: none"> 1. สำนักงานสอบบัญชีควรกำหนดมาตรการรักษาความปลอดภัยของเครื่องแม่ข่าย และอุปกรณ์ที่ใช้ในการปฏิบัติงาน เพื่อให้สามารถป้องกันและตรวจจับโปรแกรมไม่ประสงค์ดี (malware) และภัยคุกคามทางไซเบอร์ โดยครอบคลุมการดำเนินการอย่างน้อย ดังนี้ <ol style="list-style-type: none"> (1) มีกระบวนการหรือเครื่องมือในการควบคุมและติดตามไม่ให้เกิดการติดตั้งซอฟต์แวร์ที่ไม่ได้รับอนุญาต (2) ติดตั้งเครื่องมือในการป้องกันและตรวจจับโปรแกรมไม่ประสงค์ดี เช่น anti-virus, anti-malware และ intrusion prevention system เป็นต้น โดยปรับปรุง (update) เครื่องมือที่ใช้งานให้เป็นปัจจุบันอย่างสม่ำเสมอ เพื่อให้เท่าทันในการป้องกันภัยคุกคามใหม่ ๆ (3) ควบคุมการใช้งานหรือการเชื่อมต่อสื่อบันทึกข้อมูลพกพา (removable media) เช่น กำหนดแนวทางการควบคุมการใช้งาน universal serial bus (USB) หรือ external hard disk เป็นต้น 2. สำนักงานสอบบัญชีควรจัดให้มีการควบคุมป้องกันทรัพย์สินด้าน IT ประเภทฮาร์ดแวร์ระหว่างที่ไม่มีผู้ใช้งาน (unattended user equipment) ให้มีความปลอดภัย โดยครอบคลุมการดำเนินการอย่างน้อย ดังนี้ <ol style="list-style-type: none"> (1) ควบคุมเอกสาร อุปกรณ์ที่ใช้ปฏิบัติงาน หรือสื่อบันทึกข้อมูลต่าง ๆ ที่มีการจัดเก็บข้อมูลสำคัญหรือข้อมูลลับ ไม่ให้วางทิ้งไว้บนโต๊ะทำงานหรือสถานที่ไม่ปลอดภัยในขณะที่ไม่ได้ใช้งาน (clear desk) (2) ควบคุมหน้าจอคอมพิวเตอร์ไม่ให้มีข้อมูลสำคัญปรากฏในขณะที่ไม่ได้ใช้งาน (clear screen) เช่น การตัดออกจากระบบ (session time out) หรือการล็อกหน้าจอ (lock screen) อัตโนมัติ เมื่อไม่มีการใช้งานถึงระยะเวลาที่กำหนด เป็นต้น

ข้อกำหนด	แนวปฏิบัติ
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	<ol style="list-style-type: none">1. ในกรณีที่มีการปฏิบัติงานจากเครือข่ายภายนอก (teleworking) เพื่อเข้าถึงระบบงาน IT ที่มียุทธศาสตร์สำคัญ สำนักงานสอบบัญชีควรจัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่รัดกุมเพียงพอเหมาะสมกับระบบงาน IT และข้อมูลที่ถูกเข้าถึง โดยครอบคลุมอย่างน้อยดังนี้<ol style="list-style-type: none">(1) มาตรการรักษาความมั่นคงปลอดภัยด้านกายภาพที่เหมาะสม รัดกุมเพียงพอกับขอบเขตการปฏิบัติงาน สำหรับพื้นที่ปฏิบัติงานนอกองค์กร(2) การอนุมัติการปฏิบัติงานจากเครือข่ายภายนอกโดยผู้มีอำนาจหรือผู้บริหารที่เกี่ยวข้อง(3) การกำหนดสิทธิการเข้าถึงข้อมูลและระบบงาน IT จากเครือข่ายภายนอกเท่าที่จำเป็น พร้อมทั้งมีการทบทวนสิทธิอย่างสม่ำเสมอ(4) การยืนยันตัวตน (authentication) ของพนักงานที่ปฏิบัติงานจากเครือข่ายภายนอกด้วยวิธีการที่รัดกุมปลอดภัย เช่น การใช้วิธียืนยันตัวตนแบบหลายปัจจัย (multi-factor authentication) และการใช้งานผ่านอุปกรณ์ที่อนุญาตเท่านั้น เป็นต้น(5) มาตรการป้องกันความเสี่ยงจากการใช้อุปกรณ์ที่ใช้ในการปฏิบัติงานจากเครือข่ายภายนอก เป็นช่องทางในการแพร่กระจายของโปรแกรมไม่ประสงค์ดี (malware) และการรั่วไหลของข้อมูลสำคัญ(6) มาตรการป้องกันข้อมูลที่เป็นความลับหรือมีความสำคัญ (sensitive data) เช่น การยืนยันตัวตนก่อนใช้งานอุปกรณ์ (lock screen) การเข้ารหัสข้อมูลบนอุปกรณ์ที่ใช้ในการปฏิบัติงาน หรือการลบข้อมูลจากระยะไกล (remote wipe-out) เป็นต้น2. ในการปฏิบัติงานที่มีการใช้อุปกรณ์เคลื่อนที่ (mobile device) เพื่อเข้าถึงระบบงาน IT ที่มียุทธศาสตร์สำคัญ สำนักงานสอบบัญชีควรจัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่รัดกุมเพียงพอ เหมาะสมกับระบบงาน IT และข้อมูลที่ถูกเข้าถึง เช่น<ol style="list-style-type: none">(1) การลงทะเบียนอุปกรณ์เคลื่อนที่ก่อนการใช้งานโดยมีการอนุมัติโดยผู้มีอำนาจที่เกี่ยวข้อง และมีกรทบทวนทะเบียนดังกล่าวอย่างน้อยปีละ 1 ครั้ง และเมื่อมีการเปลี่ยนอุปกรณ์ พร้อมทั้งมีการยกเลิกสิทธิการใช้งานของอุปกรณ์เดิม เพื่อให้มั่นใจได้ว่าอุปกรณ์เคลื่อนที่ดังกล่าวมีความความมั่นคงปลอดภัยเพียงพอ ทั้งนี้ สำนักงานสอบบัญชีอาจใช้ระบบหรือเทคโนโลยีการลงทะเบียนอื่นทดแทนได้ หากพิจารณาแล้วเห็นว่าเหมาะสม(2) มาตรการป้องกันข้อมูลที่เป็นความลับหรือมีความสำคัญ (sensitive data) เช่น การยืนยันตัวตนก่อนใช้งานอุปกรณ์ (lock screen) การเข้ารหัสข้อมูลบนอุปกรณ์ที่ใช้ปฏิบัติงาน หรือการลบข้อมูลจากระยะไกล (remote wipe-out) เป็นต้น

ข้อกำหนด	แนวปฏิบัติ
	<p>3. กรณีที่อนุญาตให้พนักงานสามารถใช้อุปกรณ์ส่วนตัวของพนักงาน (bring your own device : BYOD) สำนักงานสอบบัญชีควรพิจารณาความเสี่ยงที่เกี่ยวข้อง และจัดให้มีมาตรการควบคุมความเสี่ยงอย่างเหมาะสม โดยครอบคลุมอย่างน้อยดังนี้</p> <ol style="list-style-type: none"> (1) การกำหนดหลักเกณฑ์การอนุญาตให้ใช้งาน BYOD (2) การควบคุมการใช้ BYOD ให้สามารถเข้าถึงเครือข่ายสื่อสาร ข้อมูล และระบบงาน IT เท่าที่จำเป็น (3) การยืนยันตัวตนเพื่อปลอดภัยในการเข้าถึง BYOD เช่น การใช้รหัสผ่าน และการสแกนลายนิ้วมือ เป็นต้น (4) ในกรณีเครื่องคอมพิวเตอร์ส่วนตัวของพนักงาน (personal computer, notebook) สามารถเชื่อมต่อเข้าสู่ระบบเครือข่ายภายในหรือข้อมูลสำคัญ ควรจัดให้มีการติดตั้งซอฟต์แวร์ป้องกันโปรแกรมไม่ประสงค์ดี (anti-virus/ anti-malware) และปรับปรุงให้ทันสมัย (update) อยู่เสมอ (5) ห้ามการใช้อุปกรณ์เคลื่อนที่ (tablet, smartphone) ที่ถูกปรับแต่ง (rooted หรือ jailbroken) เข้าถึงระบบงาน IT
2.8.6 การสำรองข้อมูล (data backup)	
<p>8.6 การสำรองข้อมูล (data backup) ที่สำคัญด้วยวิธีการและความถี่ที่เหมาะสม เพื่อให้ข้อมูลสำรองมีสภาพพร้อมใช้งานสอดคล้องกับเป้าหมายการกู้คืนระบบงาน IT ในกรณีที่ระบบงาน IT และข้อมูลหลักเกิดเหตุขัดข้องหรือได้รับความเสียหาย โดยต้องมีการทดสอบข้อมูลสำรองและกระบวนการกู้คืนข้อมูลอย่างน้อยปีละ 1 ครั้ง</p>	<ol style="list-style-type: none"> 1. สำนักงานสอบบัญชีควรกำหนดมาตรฐานหรือวิธีปฏิบัติในการสำรองข้อมูลที่สอดคล้องกับระยะเวลาเป้าหมายในการกู้คืนระบบงาน IT (Recovery Time Objective: RTO) และระยะเวลาเป้าหมายสูงสุดที่ยอมให้ข้อมูลเสียหาย (Recovery Point Objective: RPO) โดยอย่างน้อยควรมีรายละเอียดครอบคลุม <ol style="list-style-type: none"> (1) ข้อมูลที่ต้องสำรอง (2) ความถี่หรือรอบเวลาในการสำรองข้อมูล (3) ขั้นตอนและวิธีการสำรองข้อมูล (4) ขั้นตอนและวิธีการกู้คืนข้อมูล (5) สถานที่และวิธีการเก็บรักษาสื่อบันทึกข้อมูล 2. สำนักงานสอบบัญชีควรจัดเก็บสื่อบันทึกข้อมูลสำรอง พร้อมทั้งสำเนาขั้นตอนหรือวิธีปฏิบัติงานต่าง ๆ ไว้นอกศูนย์คอมพิวเตอร์หลักหรือนอกสถานที่ปฏิบัติงานหลัก โดยสถานที่ดังกล่าวควรจัดให้มีมาตรการรักษาความปลอดภัยอย่างเหมาะสมตามนโยบายของสำนักงานสอบบัญชี หรือ เทียบเคียงกับศูนย์คอมพิวเตอร์หลักหรือสถานที่ปฏิบัติงานหลัก 3. สำนักงานสอบบัญชีควรจัดให้มีการสอบทานการสำรองข้อมูล และทดสอบข้อมูลสำรองอย่างน้อยปีละ 1 ครั้ง เพื่อให้มั่นใจว่ามีการสำรองข้อมูลมีความครบถ้วนถูกต้อง พร้อมใช้งาน และปลอดภัย 4. ในกรณีที่จำเป็นต้องจัดเก็บข้อมูลเป็นระยะเวลานาน สำนักงานสอบบัญชีควรคำนึงถึงวิธีการนำข้อมูลกลับมาใช้งานในอนาคตด้วยหากมี

ข้อกำหนด	แนวปฏิบัติ
	<p>ความจำเป็น เช่น เมื่อมีการจัดเก็บข้อมูลลงในสื่อบันทึกข้อมูลใด ให้มีการจัดเก็บอุปกรณ์และโปรแกรมที่ใช้อ่านสื่อบันทึกข้อมูลนั้นด้วย เป็นต้น</p>
<p>2.8.7 การจัดเก็บข้อมูลบันทึกเหตุการณ์การใช้งานเกี่ยวกับระบบงาน IT (log)</p>	
<p>8.7 การจัดเก็บข้อมูลบันทึกเหตุการณ์การใช้งานเกี่ยวกับระบบงาน IT (log) อย่างครบถ้วนและเพียงพอ เพื่อให้สามารถใช้เป็นหลักฐานการทำการธุรกรรมทางอิเล็กทรอนิกส์ และสามารถติดตามและตรวจสอบการเข้าถึงและใช้งานข้อมูลและระบบงาน IT ย้อนหลังได้ตามที่กฎหมายกำหนด</p>	<ol style="list-style-type: none"> 1. สำนักงานสอบบัญชีควรจัดเก็บข้อมูลบันทึกเหตุการณ์ (log) ด้วยวิธีการที่ปลอดภัย โดยมีรายละเอียดครบถ้วนเพียงพอที่จะใช้เป็นหลักฐานในการตรวจสอบที่สามารถระบุตัวบุคคลผู้กระทำได้ และจัดเก็บเป็นระยะเวลาอย่างน้อย 90 วัน หรือจัดเก็บตามกฎหมายที่เกี่ยวข้องกำหนด ประกอบด้วยรายการหลักฐานอย่างน้อย ดังนี้ <ol style="list-style-type: none"> (1) บันทึกเหตุการณ์การเข้า-ออกศูนย์คอมพิวเตอร์ และพื้นที่ที่เกี่ยวข้องกับระบบงาน IT ที่มีนัยสำคัญ (physical access log) (2) บันทึกการยืนยันตัวตนและการเข้าถึง (authentication log และ access log) ของเครื่องแม่ข่าย ระบบงาน อุปกรณ์เครือข่าย และข้อมูลที่มีความสำคัญ โดยรวมถึงความพยายามในการเข้าถึง (log-in attempt) (3) บันทึกการดำเนินงาน (activity log) ที่สำคัญ โดยอย่างน้อยครอบคลุม <ol style="list-style-type: none"> (3.1) การเปลี่ยนแปลงแก้ไขโครงสร้างข้อมูล (3.2) การเปลี่ยนแปลงแก้ไข และลบข้อมูลสำคัญ (3.3) การเปลี่ยนแปลงแก้ไขการตั้งค่าของระบบ (system configuration) (3.4) การเปลี่ยนแปลงแก้ไขบัญชี และสิทธิของผู้ใช้งาน (3.5) การใช้งานอินเทอร์เน็ตผ่านระบบเครือข่ายของสำนักงานสอบบัญชี (3.6) การทำงานของ firewall (network firewall log) 2. สำนักงานสอบบัญชีควรจัดเก็บ log ที่เกี่ยวข้องกับข้อมูลส่วนบุคคล เพื่อใช้ตรวจสอบกิจกรรมของผู้ใช้งานและใช้เป็นหลักฐานหากเกิดเหตุการณ์การเข้าถึง ใช้งาน แก้ไขเปลี่ยนแปลง หรือเปิดเผยข้อมูลส่วนบุคคลที่ไม่เหมาะสม โดยสอดคล้องกับกฎหมายและหลักเกณฑ์ที่เกี่ยวข้อง เช่น กฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ และกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล เป็นต้น 3. สำนักงานสอบบัญชีควรจัดเก็บ log ของอุปกรณ์สำคัญไว้ที่เครื่องแม่ข่ายที่ใช้จัดเก็บ log (logging server) ที่แยกเฉพาะ หรือใช้วิธีการที่เทียบเคียงซึ่งสามารถป้องกันการเปลี่ยนแปลง แก้ไข หรือทำลาย log ได้ โดยมีมาตรการรักษาความปลอดภัยอย่างน้อย ดังนี้ <ol style="list-style-type: none"> (1) กำหนดหน้าที่และความรับผิดชอบผู้ที่สามารถเข้าถึง log ตามความจำเป็น (2) มีกระบวนการยืนยันตัวตนและตรวจสอบสิทธิในการเข้าถึง log (3) ติดตั้งเครื่องแม่ข่าย หรืออุปกรณ์ที่ใช้จัดเก็บ log ให้อยู่ในโซนเครือข่ายที่มีความมั่นคงปลอดภัย

ข้อกำหนด	แนวปฏิบัติ
2.8.8 การติดตามดูแลระบบและเฝ้าระวังภัยคุกคามทางไซเบอร์ (security monitoring)	
<p>8.8 การติดตามดูแลระบบและเฝ้าระวังภัยคุกคามทางไซเบอร์ (security monitoring) โดยมีกระบวนการหรือเครื่องมือป้องกันและตรวจจับเหตุการณ์ผิดปกติด้าน IT โปรแกรมไม่ประสงค์ดี (malware) หรือภัยคุกคามทางไซเบอร์ที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยต่อระบบงาน IT ที่มีนัยสำคัญ</p>	<ol style="list-style-type: none"> 1. สำนักงานสอบบัญชีควรจัดให้มีกระบวนการหรือเครื่องมือในการตรวจจับเหตุการณ์ผิดปกติที่อาจส่งผลกระทบต่อความปลอดภัยของระบบ IT ที่มีนัยสำคัญอย่างทั่วถึงที่ เช่น กระบวนการหรือเครื่องมือในการสอบทาน log เป็นต้น เพื่อให้รับทราบความผิดปกติหรือภัยคุกคาม และสามารถดำเนินการป้องกันหรือรับมือได้อย่างเหมาะสม 2. สำนักงานสอบบัญชีควรจัดให้มีกระบวนการหรือเครื่องมือในการรับข้อมูลข่าวสารเกี่ยวกับภัยคุกคาม (cyber threat intelligence) เพื่อให้สามารถติดตามและวิเคราะห์ภัยคุกคามทางไซเบอร์ที่อาจเกิดขึ้น และสามารถดำเนินการป้องกันหรือรับมือได้อย่างเหมาะสม
2.8.9 การประเมินช่องโหว่ทางเทคนิค (technical vulnerability assessment) (ถ้ามี)	
<p>8.9 การประเมินช่องโหว่ทางเทคนิค (technical vulnerability assessment) ของระบบงาน IT ที่เหมาะสมกับระดับความเสี่ยงเพื่อให้ทราบถึงช่องโหว่ และสามารถดำเนินการแก้ไขและป้องกันภัยคุกคามทางไซเบอร์ที่อาจเกิดขึ้นได้อย่างทั่วถึง โดยการประเมินช่องโหว่ทางเทคนิคครอบคลุมระบบงาน IT ที่มีนัยสำคัญและระบบงาน IT ที่เชื่อมต่อกับเครือข่ายสาธารณะ (internet facing) ทุกระบบอย่างน้อยตามรอบระยะเวลาที่ได้จากการประเมินระดับความเสี่ยงด้านเทคโนโลยีสารสนเทศของสำนักงานสอบบัญชี (IT Risk Assessment: ITRA) และทุกครั้งที่มีการเปลี่ยนแปลงอย่างมีนัยสำคัญของระบบดังกล่าว เช่น การเปลี่ยนแปลงโครงสร้างพื้นฐานของระบบงาน IT หรือการเพิ่มเติมฟังก์ชันสำคัญของระบบงาน IT เป็นต้น</p>	<ol style="list-style-type: none"> 1. สำนักงานสอบบัญชีควรกำหนดขอบเขตและความถี่ของการประเมินช่องโหว่ทางเทคนิคให้ครอบคลุมทุกระบบงานตามระดับความเสี่ยง ทั้งนี้ สำหรับระบบงาน IT ที่มีนัยสำคัญและระบบงาน IT ที่เชื่อมต่อกับเครือข่ายสาธารณะทุกระบบต้องได้รับการประเมินช่องโหว่อย่างน้อยตามรอบระยะเวลาที่ได้จากการประเมินระดับความเสี่ยงด้านเทคโนโลยีสารสนเทศของสำนักงานสอบบัญชี (IT Risk Assessment: ITRA) และทุกครั้งที่มีการเปลี่ยนแปลงระบบดังกล่าวอย่างมีนัยสำคัญ 2. สำนักงานสอบบัญชีควรประเมินความเสี่ยงของช่องโหว่ที่ตรวจพบและกำหนดระยะเวลาแก้ไขที่เหมาะสมกับความเสี่ยง 3. สำนักงานสอบบัญชีควรรายงานผลการประเมินช่องโหว่ไปยังผู้รับผิดชอบ รวมถึงติดตามให้มีการแก้ไขช่องโหว่ภายในระยะเวลาที่กำหนดไว้ โดยนำเสนอความคืบหน้าของการดำเนินการต่อหัวหน้าสำนักงานสอบบัญชี หรือคณะกรรมการบริหารของสำนักงานสอบบัญชีที่ได้รับมอบหมาย
2.8.10 การบริหารจัดการโปรแกรมแก้ไขช่องโหว่ (patch management)	
<p>8.10 การบริหารจัดการโปรแกรมแก้ไขช่องโหว่ (patch management) โดยจัดให้มีกระบวนการควบคุม</p>	<ol style="list-style-type: none"> 1. สำนักงานสอบบัญชีควรมีการกำหนดมาตรฐานและระเบียบวิธีปฏิบัติในการบริหารจัดการโปรแกรมแก้ไขช่องโหว่ (patch) ที่ครอบคลุมการดำเนินการอย่างน้อย ดังนี้

ข้อกำหนด	แนวปฏิบัติ
<p>การติดตั้งโปรแกรมแก้ไขช่องโหว่บนระบบและอุปกรณ์ เพื่อลดความเสี่ยงที่จะถูกโจมตีในอนาคต</p>	<ol style="list-style-type: none"> (1) การประเมินความเสี่ยงและความจำเป็นในการติดตั้ง patch (2) การกำหนดกรอบระยะเวลาการติดตั้ง patch โดยคำนึงถึงความจำเป็นและความเสี่ยงจากการถูกโจมตีจากช่องโหว่ (3) การตรวจสอบความถูกต้องและการทดสอบ patch ก่อนการดำเนินการติดตั้งบนระบบที่ให้บริการจริง เพื่อป้องกันผลกระทบที่ไม่พึงประสงค์จากการติดตั้ง patch ทั้งนี้ ในกรณีที่มีข้อจำกัดในการทดสอบ patch สำนักงานสอบบัญชีอาจพิจารณาการควบคุมอื่น ๆ ทดแทน 2. การติดตั้ง patch บนระบบงานจริง ควรดำเนินการตามกระบวนการบริหารจัดการการเปลี่ยนแปลง (change management) ที่กำหนดไว้ เพื่อป้องกันความเสี่ยงและข้อผิดพลาดจากการปฏิบัติงาน 3. กรณีมีเหตุที่ผู้ผลิตระบบงานหรืออุปกรณ์ยังไม่แจ้งการปรับปรุง security patch อย่างเป็นทางการเพื่อปิดช่องโหว่ใหม่ ๆ ที่เพิ่งค้นพบ สำนักงานสอบบัญชีควรปฏิบัติตามคำแนะนำของผู้พัฒนาระบบ เจ้าของผลิตภัณฑ์ หรือผู้เชี่ยวชาญด้านความมั่นคงปลอดภัย หรือจัดให้มีมาตรการควบคุมทดแทน เพื่อลดความเสี่ยงจากการถูกโจมตีผ่านช่องโหว่นั้น ๆ 4. สำนักงานสอบบัญชีควรมอบหมายผู้รับผิดชอบ หรือจัดให้มีเครื่องมือที่ใช้ติดตาม patch ด้านการรักษาความปลอดภัย (patch monitoring tool) ที่ยังไม่มีติดตั้งบนระบบปฏิบัติการ (operation system) และระบบฐานข้อมูล (database system) ที่สำคัญ ของสำนักงานสอบบัญชี
<p>2.9 การรักษาความมั่นคงปลอดภัยเกี่ยวกับระบบเครือข่ายสื่อสาร (communication system security)</p>	
<p>ส่วนที่ 9 การรักษาความมั่นคงปลอดภัยเกี่ยวกับระบบเครือข่ายสื่อสาร (communication system security)</p> <p>สำนักงานสอบบัญชีต้องมีการรักษาความมั่นคงปลอดภัยเกี่ยวกับระบบเครือข่ายสื่อสารอย่างเหมาะสม เพื่อให้ระบบเครือข่ายสื่อสารและข้อมูลที่ได้รับส่งผ่านระบบเครือข่ายสื่อสารมีความมั่นคงปลอดภัย สามารถป้องกันการบุกรุกหรือภัยคุกคามทางไซเบอร์ที่อาจเกิดขึ้น รวมทั้งพร้อมใช้งานได้อย่างต่อเนื่อง</p>	<ol style="list-style-type: none"> 1. สำนักงานสอบบัญชีควรจัดให้มีการรักษาความมั่นคงปลอดภัยของระบบเครือข่ายสื่อสาร โดยมีการดำเนินการอย่างน้อย ดังนี้ <ol style="list-style-type: none"> (1) ออกแบบเครือข่ายสื่อสารที่มีการแบ่งแยกเครือข่ายอย่างเหมาะสม โดยคำนึงถึงระดับความสำคัญของระบบงาน (application system) ระดับความสำคัญของข้อมูล รวมถึงความจำเป็นในการเชื่อมต่อจากระบบงานอื่น ๆ หรือจากภายนอกองค์กร (2) จัดให้มีการควบคุมการเชื่อมต่อของระบบงาน (application system) ที่สำคัญ (3) การแบ่งแยกเครือข่ายให้มีความรัดกุมปลอดภัย เช่น <ol style="list-style-type: none"> (3.1) แบ่งแยกเครือข่ายภายใน (private network) และเครือข่ายภายนอก (public network) ออกจากกัน (3.2) แบ่งแยกเครือข่ายของระบบงาน IT ที่มีนัยสำคัญ เครือข่ายสำหรับการปฏิบัติงานของพนักงาน และเครือข่ายสำหรับการใช้งานทั่วไป/เครือข่ายสำหรับบุคคลภายนอก (guest network) ออกจากกัน (3.3) จุดที่มีการแบ่งแยกเครือข่ายที่มีความสำคัญและมีความเสี่ยง ควรติดตั้งอุปกรณ์รักษาความปลอดภัยเครือข่ายที่มีความสามารถในการควบคุมและคัดกรองข้อมูล (traffic) ที่รับส่งผ่านเครือข่าย เพื่อป้องกันและตรวจจับการบุกรุกของไวรัสหรือมัลแวร์ต่าง ๆ

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

ข้อกำหนด	แนวปฏิบัติ
<p>สำหรับสำนักงานสอบบัญชีมีการบริหารจัดการโครงการด้าน IT (IT project management) และการจัดหาพัฒนา และบำรุงรักษาระบบงาน IT ในปัจจุบัน หรือวางแผนว่าจะมีในอนาคต สำนักงานสอบบัญชีต้องจัดทำนโยบายและแนวปฏิบัติสำหรับการบริหารจัดการโครงการด้าน IT การจัดหา พัฒนา รวมถึงบำรุงรักษาระบบงาน IT เป็นลายลักษณ์อักษร เพื่อให้มั่นใจได้ว่าเมื่อใดก็ตามที่มีการดำเนินโครงการด้าน IT สำนักงานสอบบัญชีจะมีกรอบและแนวทางที่จะช่วยรักษาความมั่นคงปลอดภัยตลอดวงจรชีวิตของระบบงาน IT (entire life cycle) โดยให้ครอบคลุมรายละเอียดอย่างน้อย ดังนี้</p>	
<p>2.10.1 การบริหารจัดการโครงการด้าน IT (IT project management)</p>	
<p><u>10.1 บริหารจัดการโครงการด้าน IT (IT project management)</u> กำหนดกรอบการบริหารจัดการโครงการ (project management framework) เพื่อให้การบริหารจัดการโครงการด้าน IT ที่มีนัยสำคัญเป็นไปอย่างมีประสิทธิภาพสามารถส่งมอบโครงการได้อย่างถูกต้อง ครบถ้วนตามแผนงานและบรรลุวัตถุประสงค์ตามเป้าหมายที่กำหนดไว้ ไม่ว่างงานโครงการนั้นจะดำเนินการโดยสำนักงานสอบบัญชีเอง หรือ บุคคลภายนอก</p>	<p>1. สำนักงานสอบบัญชีควรกำหนดกรอบการบริหารจัดการโครงการ (project management framework) เป็นลายลักษณ์อักษร โดยมีรายละเอียดขั้นต่ำ ดังนี้</p> <p>(1) โครงสร้างการควบคุมและกำกับดูแลโครงการ (project governance) ที่ชัดเจน เพื่อให้มีการควบคุมดูแลโครงการให้สำเร็จเป็นไปตามแผนงานที่กำหนด โดยพิจารณาการจัดให้มีผู้รับผิดชอบในบทบาทหน้าที่ตามความจำเป็นและความเหมาะสม เช่น</p> <p>(1.1) คณะกรรมการกำกับดูแลโครงการ (project steering committee) มีบทบาทหน้าที่และความรับผิดชอบในการกำกับดูแลและติดตามความคืบหน้าของโครงการ รวมทั้งให้คำแนะนำ และพิจารณาตัดสินใจการดำเนินงานในโครงการที่สำคัญ เพื่อให้โครงการสามารถดำเนินการได้ตามแผนที่กำหนดไว้ โดยควรประกอบด้วยผู้บริหารจากหน่วยงานที่เกี่ยวข้อง และเจ้าของโครงการหรือผู้สนับสนุนโครงการ (project owner/project sponsor)</p> <p>(1.2) ผู้จัดการโครงการ (project manager) มีบทบาทหน้าที่และความรับผิดชอบในการบริหารจัดการโครงการให้เป็นไปตามระเบียบขั้นตอนการบริหารจัดการโครงการ เพื่อให้โครงการสามารถส่งมอบได้อย่างถูกต้องครบถ้วนสำเร็จตามแผนงานที่กำหนด</p> <p>(2) แนวทางการบริหารจัดการโครงการ โดยมีรายละเอียดขั้นต่ำ ดังนี้</p>

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

ข้อกำหนด	แนวปฏิบัติ
	<p>4. การปิดโครงการ สำนักงานสอบบัญชีควรดำเนินการอย่างน้อย ดังนี้</p> <ol style="list-style-type: none"> (1) สรุปประโยชน์ที่ได้รับจากโครงการเปรียบเทียบกับเป้าหมายที่กำหนด (2) รวบรวมปัญหา อุปสรรคจากการบริหารจัดการโครงการ เพื่อนำมาเป็นที่ได้เรียนรู้ (lesson learned) ใช้สำหรับวิเคราะห์ปรับปรุง และพัฒนากระบวนการหรือเครื่องมือในการบริหารจัดการโครงการต่อไปให้มีประสิทธิภาพมากขึ้น <p>5. สำนักงานสอบบัญชีควรสอบทานโครงการที่มีนัยสำคัญ เพื่อให้มั่นใจได้ว่าโครงการสอดคล้องกับเป้าหมายของโครงการ นโยบายมาตรฐาน ระเบียบและวิธปฏิบัติของสำนักงานสอบบัญชี รวมทั้งกฎหมายและหลักเกณฑ์ที่เกี่ยวข้อง</p>
2.10.2 การจัดหาระบบงาน IT (system acquisition)	
<p><u>10.2 จัดหาระบบงาน IT (system acquisition)</u> จัดให้มีหลักเกณฑ์ในการจัดหาระบบงาน IT และผู้ให้บริการ เพื่อให้มั่นใจว่าระบบที่จัดหาสามารถตอบสนองความต้องการทางธุรกิจและความต้องการด้านความมั่นคงปลอดภัย IT โดยคำนึงถึงความยืดหยุ่นในการเปลี่ยนแปลงผู้ให้บริการ การเปลี่ยนแปลงเทคโนโลยี รวมถึงการเปลี่ยนแปลงต่าง ๆ ที่เกี่ยวข้องกับการดำเนินธุรกิจอย่างมีนัยสำคัญ</p>	<ol style="list-style-type: none"> 1. สำนักงานสอบบัญชีควรจัดให้มีหลักเกณฑ์การคัดเลือกระบบงาน IT และผู้ให้บริการ เพื่อให้มั่นใจว่าระบบที่จัดหาสามารถตอบสนองความต้องการทางธุรกิจและความต้องการด้านความมั่นคงปลอดภัยสารสนเทศ ซึ่งควรคำนึงถึงเรื่องดังนี้ <ol style="list-style-type: none"> (1) รายละเอียดทั่วไป เช่น เทคโนโลยีที่ใช้ สิทธิการใช้งานซอฟต์แวร์ (software license) ฟังก์ชันการทำงานของระบบ เป็นต้น (2) ความมั่นคงปลอดภัยของระบบ (3) ความน่าเชื่อถือของระบบงาน IT และผู้ให้บริการ เช่น ฐานะการเงิน ชื่อเสียง และความสามารถด้านเทคนิค เป็นต้น (4) การได้รับการรับรองตามมาตรฐานสากลหรือมาตรฐานด้าน IT ที่เกี่ยวข้องที่ได้รับการยอมรับโดยทั่วไป (certificate) (5) การสนับสนุนและการบำรุงรักษาระบบ (6) การทดสอบการทำงานขั้นต้น (proof of concept) ในกรณีที่เป็นระบบงาน IT ที่มีนัยสำคัญ (7) มาตรการรองรับหรือการบริหารความเสี่ยง ในกรณีที่ผู้พัฒนาระบบหรือผู้ให้บริการซอฟต์แวร์ไม่ปฏิบัติตามข้อตกลงในการบำรุงรักษาระบบหรือให้การสนับสนุนการดำเนินงานตามที่ตกลงไว้ เช่น จัดให้มีข้อตกลงการรับฝากโค้ดต้นฉบับ (source-code escrow agreement) เพื่อให้มั่นใจว่าสำนักงานสอบบัญชีจะมีสิทธิในการเข้าถึง source code ของระบบหรือซอฟต์แวร์ดังกล่าว เป็นต้น
2.10.3 การพัฒนาระบบงาน IT (system development)	
<p><u>10.3 พัฒนาระบบงาน IT (system development)</u> จัดให้มีมาตรการควบคุมเกี่ยวกับการพัฒนาระบบงาน IT ในการออกแบบ พัฒนา ทดสอบระบบ และนำระบบขึ้นใช้งานจริง เพื่อให้มั่นใจว่าระบบมีความถูกต้อง มั่นคง ปลอดภัย เชื่อถือได้ พร้อมใช้งาน และมีความยืดหยุ่น</p>	<p>[ไม่มีการกำหนดแนวปฏิบัติไว้เป็นการเฉพาะ]</p>

ข้อกำหนด	แนวปฏิบัติ
<p>เพียงพอจะรองรับการใช้งานได้ สอดคล้องกับแผนการดำเนินธุรกิจ โดยต้องดำเนินการอย่างน้อย ดังนี้</p>	
<p>(1) มีการกำหนดรายละเอียดความต้องการของระบบ (requirement) และคุณสมบัติทางเทคนิค (technical specification) ของระบบที่พัฒนา ดังนี้</p> <p>(1.1) ความมั่นคงปลอดภัย (security)</p> <p>(1.2) สภาพพร้อมใช้งาน (availability)</p> <p>(1.3) ชีตความสามารถที่รองรับ (capacity)</p>	<p><u>การออกแบบระบบ</u></p> <ol style="list-style-type: none"> 1. สำนักงานสอบบัญชีควรกำหนดให้หน่วยงานอื่นที่เกี่ยวข้องมีส่วนร่วมในการกำหนดรายละเอียดความต้องการของระบบ 2. สำนักงานสอบบัญชีควรจัดทำเอกสารระบุรายละเอียดความต้องการของระบบ (functional requirement และ non-functional requirement) และคุณสมบัติทางเทคนิค (technical specification) ที่ครอบคลุมเรื่อง ดังนี้ <ol style="list-style-type: none"> (1) ความมั่นคงปลอดภัย (security) ตามนโยบายหรือมาตรฐานที่สำนักงานสอบบัญชีกำหนด เช่น การควบคุมการเข้าถึง และการเข้ารหัสข้อมูล เป็นต้น (2) ความพร้อมใช้งาน (availability) เช่น การออกแบบให้มีระบบทดแทน high availability หรือ redundancy รวมถึงมีระบบสำรอง (Disaster Recovery strategy) เป็นต้น เพื่อให้ระบบสามารถทำงานได้อย่างต่อเนื่อง และลดความเสี่ยงที่จุดใดจุดหนึ่งทำให้ระบบเกิดปัญหาหรือล้มเหลวทั้งหมด (single point of failure) (3) ชีตความสามารถที่รองรับ (capacity) ตามอัตรากำลังคนของสำนักงานสอบบัญชีที่วางแผนไว้ในปัจจุบัน ทั้งนี้ เอกสารข้างต้นควรผ่านการสอบทานความถูกต้องครบถ้วนและได้รับอนุมัติจากผู้เกี่ยวข้องก่อนเริ่มพัฒนาระบบ
<p>(2) มีการแบ่งแยกบทบาทหน้าที่และความรับผิดชอบของผู้ที่เกี่ยวข้องในการพัฒนาระบบ เพื่อให้มีการสอบทานก่อนนำระบบขึ้นไปให้บริการจริง ทั้งนี้ หากระบบถูกพัฒนาโดยบุคคลภายนอก และมีข้อจำกัดในการแบ่งแยกหน้าที่ที่สำนักงานสอบบัญชีต้องจัดการควบคุมอื่นทดแทนเพื่อตอบสนองต่อความเสี่ยงจากการแบ่งแยกหน้าที่ไม่เหมาะสม</p>	<p><u>การพัฒนาระบบ</u></p> <ol style="list-style-type: none"> 1. สำนักงานสอบบัญชีควรแบ่งแยกบทบาทหน้าที่และความรับผิดชอบของผู้ที่เกี่ยวข้องในการพัฒนาระบบ (segregation of duty) เพื่อให้มีการสอบทานก่อนนำระบบขึ้นไปให้บริการจริง เช่น แยกผู้พัฒนาระบบ ออกจากผู้นำระบบขึ้นใช้งานจริง เป็นต้น
<p>(3) มีการแบ่งแยกสภาพแวดล้อมของระบบงานที่ใช้สำหรับการพัฒนา (development) และการทดสอบ (testing) ออกจากระบบงานที่ให้บริการจริง (production) เช่น</p>	<ol style="list-style-type: none"> 1. สำนักงานสอบบัญชีควรแบ่งแยกสภาพแวดล้อมของระบบงานที่ใช้สำหรับการพัฒนา (development) และการทดสอบ (testing) ออกจากระบบงานที่ให้บริการจริง (production) เพื่อควบคุมการทดสอบและลดผลกระทบที่อาจเกิดขึ้นต่อระบบงานที่ให้บริการจริง 2. สำนักงานสอบบัญชีควรจัดให้มีการรักษาความมั่นคงปลอดภัยของเครื่องที่ไม่ได้อยู่บนระบบที่ให้บริการจริง (non-production) ให้เพียงพอกับระดับความเสี่ยงของการเข้าถึงระบบและข้อมูลโดยไม่ได้รับอนุญาต และการรั่วไหลของข้อมูลที่ใช้ทดสอบ 3. สำนักงานสอบบัญชีควรจัดให้มีการควบคุมไม่ให้มีการติดตั้งเครื่องมือการพัฒนาระบบ (development tools) และเครื่องมือแปล

ข้อกำหนด	แนวปฏิบัติ
(4) มีกระบวนการหรือเครื่องมือควบคุมการพัฒนาชุดคำสั่งคอมพิวเตอร์ให้มีความปลอดภัย เช่น	<p>โปรแกรม (compilers) ไว้บนระบบที่ให้บริการจริง เพื่อป้องกันความเสี่ยงที่อาจถูกปรับเปลี่ยนหรือติดตั้งโปรแกรมโดยไม่ได้รับอนุญาต</p> <ol style="list-style-type: none">1. สำนักงานสอบบัญชีควรกำหนดมาตรฐานและระเบียบวิธีปฏิบัติในการออกแบบและพัฒนาระบบอย่างปลอดภัย (secure coding) สอดคล้องกับมาตรฐานสากล รวมทั้งควบคุมให้ผู้พัฒนาระบบปฏิบัติตามมาตรฐานและระเบียบวิธีปฏิบัติดังกล่าว2. สำนักงานสอบบัญชีควรมีกระบวนการหรือเครื่องมือควบคุมเวอร์ชันของชุดคำสั่งคอมพิวเตอร์ (source code version control)3. สำนักงานสอบบัญชีควรสอบทานคำสั่งในการเขียนโปรแกรม (source code review) โดยใช้ระบบอัตโนมัติ (automated review) หรือแบบ manual review ซึ่งดำเนินการโดยบุคคลที่ไม่ใช่ผู้พัฒนาโปรแกรม เมื่อมีการพัฒนาหรือแก้ไขเปลี่ยนแปลงระบบงาน IT ที่มีนัยสำคัญ และมีความเสี่ยงด้านความมั่นคงปลอดภัย เพื่อให้สามารถระบุข้อบกพร่องด้านความมั่นคงปลอดภัย และแก้ไขก่อนนำระบบไปใช้งานจริง
(5) มีการทดสอบระบบงาน IT ที่ได้รับการพัฒนาหรือแก้ไขเปลี่ยนแปลง เพื่อให้มั่นใจได้ว่าระบบดังกล่าวสามารถประมวลผลได้อย่างถูกต้องครบถ้วน และเป็นไปตามความต้องการของผู้ใช้งาน	<p><u>การทดสอบระบบ</u></p> <ol style="list-style-type: none">1. สำนักงานสอบบัญชีต้องจัดให้มีการทดสอบระบบก่อนนำไปใช้งานหรือให้บริการจริง เพื่อให้มั่นใจได้ว่าระบบดังกล่าวสามารถทำงานได้อย่างถูกต้อง ปลอดภัย มีประสิทธิภาพ และเป็นไปตามความต้องการของผู้ใช้งาน โดยครอบคลุมอย่างน้อย ดังนี้<ol style="list-style-type: none">(1) ทดสอบการทำงานของแต่ละหน่วย (unit test)(2) ทดสอบการทำงานของระบบและการเชื่อมต่อ (system and integration test)(3) ทดสอบความต้องการของผู้ใช้งาน (user acceptance test)(4) ทดสอบการรักษาความปลอดภัย (security test) ได้แก่ การประเมินช่องโหว่ (vulnerabilities assessment) และการทดสอบการเจาะระบบ (penetration test) ตามความจำเป็น สำหรับระบบใหม่ใด ๆ ที่มีการเชื่อมต่อกับระบบงาน IT ที่มีนัยสำคัญ เพื่อให้สามารถตรวจพบช่องโหว่และดำเนินการปรับปรุงแก้ไขอย่างเหมาะสมก่อนเริ่มให้บริการจริง2. สำนักงานสอบบัญชีควรกำหนดสถานการณ์ที่ใช้ทดสอบ (test scenario) หรือกรณีที่ใช้ทดสอบ (test case) แบบ end-to-end และมีกระบวนการสอบทาน test scenario หรือ test case เพื่อให้มั่นใจว่ามีความครอบคลุมเพียงพอและตรงกับความต้องการของสำนักงานสอบบัญชี3. สำนักงานสอบบัญชีควรทดสอบระบบบนสภาพแวดล้อม (test environment) ที่ใกล้เคียงระบบที่ให้บริการจริง เพื่อลดความเสี่ยงที่อาจเกิดขึ้นจากการเปลี่ยนแปลงบนระบบงานที่ให้บริการจริง4. สำนักงานสอบบัญชีต้องมีการจัดการข้อบกพร่อง (defect) ของระบบที่พบในการทดสอบ โดยพิจารณาแนวทางปรับปรุง หรือลดความเสี่ยงและผลกระทบของข้อบกพร่องดังกล่าว5. 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 สำนักงานสอบบัญชีควรจัดให้มีแนวทางการรักษาความมั่นคงและความลับของข้อมูลดังกล่าว เช่น การทำ data masking เป็นต้น เพื่อป้องกันความเสี่ยงในการรั่วไหลของข้อมูล
(8) ในกรณีที่มีการมอบให้มอบหมายให้บุคคลภายนอกเป็นผู้พัฒนาหรือแก้ไขเปลี่ยนแปลงระบบงาน IT สำนักงานสอบบัญชีต้องจัดให้มีการติดตาม และควบคุมการดำเนินการให้ไปตามข้อตกลงในการมอบหมายงาน	[ไม่มีการกำหนดแนวปฏิบัติไว้เป็นการเฉพาะ]
(9) มีกระบวนการขออนุมัติหัวหน้าสำนักงานสอบบัญชีหรือคณะกรรมการบริหารของสำนักงานสอบบัญชีก่อนนำระบบขึ้นใช้งานจริง	<p><u>การนำระบบขึ้นใช้งานจริง</u></p> <ol style="list-style-type: none"> 1. สำนักงานสอบบัญชีควรดำเนินการนำระบบขึ้นใช้งานจริง โดยผ่านกระบวนการบริหารจัดการการเปลี่ยนแปลงที่กำหนดไว้ 2. สำนักงานสอบบัญชีควรเตรียมความพร้อมในการนำระบบขึ้นใช้งานจริง โดยจัดเก็บระบบเวอร์ชันก่อนการเปลี่ยนแปลงให้พร้อมนำกลับมาใช้งานได้ 3. สำนักงานสอบบัญชีควรกำหนดแผนหรือเงื่อนไขการนำระบบใหม่เข้าไปทดแทน (cutover หรือ go-live technique) ที่เหมาะสมกับระดับความเสี่ยง เช่น การเปลี่ยนแปลงไปยังระบบใหม่ทันที (direct changeover) การเปลี่ยนแปลงระบบโดยการใช้งานคู่ขนาน (parallel changeover) หรือ การเปลี่ยนแปลงระบบทีละเฟส (phased changeover) เป็นต้น
2.10.4 การแก้ไขเปลี่ยนแปลงระบบงาน IT (system change)	
<u>10.4 แก้ไขเปลี่ยนแปลงระบบงาน IT (system change)</u>	1. การแก้ไขเปลี่ยนแปลงระบบงาน IT (system change) ควรพิจารณาดำเนินการตามแนวปฏิบัติเรื่องการบริหารจัดการการเปลี่ยนแปลง (change management) และแนวปฏิบัติเรื่องการพัฒนาาระบบ
(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) เมื่อมีการแก้ไขเปลี่ยนแปลงระบบงาน IT เพื่อให้เป็นปัจจุบันอยู่เสมอ นอกจากนี้ ควรสื่อสารการเปลี่ยนแปลงให้บุคคลที่เกี่ยวข้องได้รับทราบเพื่อให้สามารถปฏิบัติงานได้อย่างถูกต้อง
2.11 การบริหารจัดการเหตุการณ์ผิดปกติด้าน IT (IT incident management)	
ส่วนที่ 11 การบริหารจัดการเหตุการณ์ผิดปกติด้าน IT (IT incident management) สำนักงานสอบบัญชีต้องมีการบริหารจัดการเหตุการณ์ผิดปกติด้าน IT อย่างเหมาะสมและทันทั่วทั้งที่ดังนี้	
11.1 จัดให้มีช่องทางรับแจ้งเหตุการณ์ผิดปกติด้าน IT จากบุคลากร ผู้ใช้บริการ และผู้ที่เกี่ยวข้อง	1. สำนักงานสอบบัญชีควรจัดให้มีหน่วยงานหรือบุคลากรที่มีหน้าที่รับแจ้งเหตุการณ์ (point of contact) โดยทำหน้าที่ในการบันทึกข้อมูลแก้ไขในเบื้องต้น หรือส่งต่อเหตุการณ์ผิดปกติไปยังหน่วยงานด้าน IT ที่เกี่ยวข้อง
11.2 กำหนดแผน หรือขั้นตอนการบริหารจัดการ	1. สำนักงานสอบบัญชีควรจัดให้มีแผนการบริหารจัดการ หรือแผนการรับมือกับเหตุการณ์ผิดปกติ (incident response plan)

ข้อกำหนด	แนวปฏิบัติ
เหตุการณ์ผิดปกติด้าน IT	<p>ตามความสำคัญของเหตุการณ์ เพื่อให้สามารถรับมือและตอบสนองต่อเหตุการณ์ได้อย่างรวดเร็วและทันการณ์ โดยมีรายละเอียดครอบคลุมอย่างน้อย ดังนี้</p> <ol style="list-style-type: none">(1) การตรวจสอบความถูกต้องข้อมูลที่รับแจ้ง(2) การจัดประเภท และความเร่งด่วนของเหตุการณ์ เพื่อดำเนินการแก้ไขปัญหาภายในระยะเวลาที่เหมาะสม(3) การแก้ไขเหตุการณ์ ได้แก่ การวิเคราะห์ข้อมูล (analysis) การจำกัดความเสียหาย (containment) การจัดเก็บหลักฐานอย่างปลอดภัย (evidence gathering) การหาแนวทางแก้ไข (resolution research) และการแก้ไขปัญหาและฟื้นฟูระบบ (eradication and recovery) ตลอดจนการจัดให้มีช่องทางประสานงานจากผู้เชี่ยวชาญทั้งภายในและภายนอก(4) แนวทางการรายงานเหตุการณ์ผิดปกติ (incident escalation) และรายงานความคืบหน้าของเหตุการณ์ต่อหัวหน้าสำนักงาน สอบบัญชี และคณะกรรมการของสำนักงานสอบบัญชีให้รับทราบ ตามระดับความรุนแรงของเหตุการณ์(5) การแจ้งหรือสื่อสารลูกค้า โดยกำหนดผู้รับผิดชอบในการสื่อสารไปยังลูกค้า และช่องทางการสื่อสาร เพื่อให้ลูกค้ารับทราบผลกระทบ และความคืบหน้าการแก้ไขเหตุการณ์ผิดปกติ(6) การตรวจพิสูจน์พยานหลักฐานทางดิจิทัล (digital forensic) ในกรณีภัยคุกคามทางไซเบอร์ซึ่งส่งผลกระทบต่อทรัพย์สินและข้อมูลของลูกค้า โดยผู้ที่มีความเชี่ยวชาญเพื่อให้ทราบสาเหตุหรือช่องโหว่ของระบบ และสามารถดำเนินการปิดช่องโหว่ได้อย่างปลอดภัย
11.3 รายงานเหตุการณ์ผิดปกติด้าน IT เหตุการณ์การละเมิดต่อข้อมูลส่วนบุคคล และเหตุการณ์ที่ส่งผลให้ทรัพย์สินของผู้ใช้งานเสียหายอันเกิดจากเหตุการณ์ด้านความมั่นคงปลอดภัยของระบบงาน IT ต่อผู้มีหน้าที่รับผิดชอบเหตุการณ์ และหน่วยงานที่เกี่ยวข้องโดยไม่ชักช้า ตามที่กฎหมายกำหนด เช่น สำนักงาน ก.ล.ต. และ สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เป็นต้น	<ol style="list-style-type: none">1. สำนักงานสอบบัญชีควรรายงานเหตุการณ์ที่มีการละเมิดกฎหมาย กฎ และระเบียบที่เกี่ยวข้องกับสำนักงานสอบบัญชี ต่อหน่วยงานที่เกี่ยวข้องโดยไม่ชักช้า ตามที่กฎหมายกำหนด เช่น มาตรา 37 (4) พรบ.คุ้มครองข้อมูลส่วนบุคคลฯ แจ้งให้รายงานเหตุการณ์ละเมิดข้อมูลส่วนบุคคลแก่สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลภายใน 72 ชั่วโมงนับแต่ทราบเหตุเท่าที่สามารถกระทำได้ ทั้งนี้ การแจ้งดังกล่าวและข้อยกเว้นให้เป็นไปตามหลักเกณฑ์และวิธีการที่คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลประกาศกำหนด เป็นต้น รวมทั้ง สำนักงานสอบบัญชีต้องรายงานเหตุการณ์ดังกล่าวแก่สำนักงาน ก.ล.ต. ภายใน 72 ชั่วโมงนับแต่ทราบเหตุเท่าที่สามารถกระทำได้ด้วยเช่นกัน ตามหลักเกณฑ์ในการกำกับดูแลและการตรวจสอบด้าน IT สำหรับสำนักงานสอบบัญชี2. สำนักงานสอบบัญชีควรรายงานสำนักงาน ก.ล.ต. ในกรณีที่มีเหตุการณ์ด้าน IT ซึ่งอาจส่งผลกระทบต่อการใช้งาน ธุรกิจ ชื่อเสียง ฐานะ ผลการดำเนินงานของสำนักงานสอบบัญชีอย่างมาก หรือลูกค้าในวงกว้าง โดยครอบคลุมเหตุการณ์ ดังนี้<ol style="list-style-type: none">(1) การละเมิดต่อข้อมูลส่วนบุคคลที่เกิดจากเหตุการณ์ผิดปกติด้าน IT(2) ทรัพย์สินของผู้ใช้งานสูญหาย หรือเสียหาย(3) การบุกรุก เข้าถึง หรือใช้งานระบบโดยไม่ได้รับอนุญาต (system compromised)

ข้อกำหนด	แนวปฏิบัติ
	<p>(4) เหตุการณ์ที่ส่งผลกระทบต่อชื่อเสียงของสำนักงานสอบบัญชี (harm to reputation) เช่น ถูกปลอมแปลงหน้าเว็บไซต์ของบริษัท (website defacement) เป็นต้น</p> <p>3. สำนักงานสอบบัญชีควรรายงานเหตุการณ์ต่อสำนักงาน ก.ล.ต. ภายในกรอบระยะเวลา ดังนี้</p> <ul style="list-style-type: none">(1) รายงานโดยไม่ชักช้า ภายใน 72 ชั่วโมงนับแต่ทราบเหตุเท่าที่สามารถกระทำได้ โดยมีเนื้อหาครอบคลุมถึงวันเวลา ประเภทเหตุการณ์ เหตุการณ์ และผลกระทบที่คาดว่าจะเกิดขึ้น ทั้งนี้ สามารถแจ้งโดยวาจาหรือรายงานผ่านช่องทางอิเล็กทรอนิกส์ตามที่สำนักงาน ก.ล.ต. กำหนดตามความเหมาะสม(2) รายงานความคืบหน้าเป็นลายลักษณ์อักษรทุก ๆ 14 วัน หรือ ตามความเหมาะสมจนกว่าระบบงาน IT จะกลับสู่การให้บริการได้อย่างเป็นปกติ โดยมีเนื้อหาครอบคลุมถึงวันเวลา ประเภทเหตุการณ์ เหตุการณ์ ผลกระทบที่เกิดขึ้น และความคืบหน้าในการแก้ไขปัญหา ทั้งนี้ ให้รายงานผ่านช่องทางอิเล็กทรอนิกส์ที่สำนักงาน ก.ล.ต. กำหนด(3) รายงานเมื่อเหตุการณ์ยุติหรือแก้ไขปัญหาแล้วเสร็จ โดยมีเนื้อหาครอบคลุมถึงวันเวลา ประเภทเหตุการณ์ เหตุการณ์ ผลกระทบที่เกิดขึ้น การดำเนินการแก้ไขปัญหา ผลการแก้ไขปัญหา ระยะเวลาในการแก้ไข สาเหตุที่เกิดปัญหา และแนวทางป้องกันในอนาคต ทั้งนี้ ให้รายงานผ่านช่องทางอิเล็กทรอนิกส์ที่สำนักงาน ก.ล.ต. กำหนด
11.4 วิเคราะห์สาเหตุที่แท้จริง (root cause) ของเหตุการณ์ผิดปกติด้าน IT เพื่อกำหนดแนวทางการแก้ไข และป้องกันไม่ให้เกิดเหตุการณ์ซ้ำในอนาคต	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) และจัดให้มีการรายงานผลการทดสอบ	1. สำนักงานสอบบัญชีควรทดสอบและทบทวนขั้นตอนปฏิบัติหรือแผนการบริหารจัดการเหตุการณ์ผิดปกติ อย่างน้อยปีละ 1 ครั้ง เพื่อให้สามารถจัดการแก้ไขเหตุการณ์ให้กลับสู่สภาพปกติได้อย่างรวดเร็วและจำกัดความเสียหายที่ส่งผลกระทบต่อธุรกิจ โดยดำเนินการ ดังนี้ <ul style="list-style-type: none">(1) จัดให้มีการจำลองสถานการณ์เสี่ยง (risk scenario) ด้านเหตุการณ์ภัยคุกคามทางไซเบอร์ที่มีความเป็นไปได้ที่จะเกิดขึ้น สอดคล้องกับลักษณะ ขอบเขต และความซับซ้อนในการประกอบธุรกิจ และสอดคล้องกับแนวโน้มภัยคุกคามไซเบอร์ที่อาจเกิดขึ้นกับสำนักงานสอบบัญชีโดยสถานการณ์ดังกล่าวควรเป็นสถานการณ์ที่เกิดขึ้นแล้วส่งผลกระทบต่อระบบงาน IT

ข้อกำหนด	แนวปฏิบัติ
<p>และทบทวนต่อหัวหน้าสำนักงานสอบบัญชี หรือ คณะกรรมการบริหารของสำนักงานสอบบัญชี</p>	<p>อย่างมีนัยสำคัญ</p> <p>(2) จัดเก็บเอกสารที่เกี่ยวข้องกับการทดสอบให้ครบถ้วนและเป็นปัจจุบัน ดังนี้</p> <p>(2.1) สถานการณ์ความเสี่ยง (risk scenario) รูปแบบการทดสอบ วัน เวลา สถานที่ในการทดสอบ บทบาทหน้าที่ของผู้ที่เกี่ยวข้องที่ใช้ในการทดสอบ</p> <p>(2.2) สรุปผลการทดสอบ และผลการทบทวนขั้นตอนการบริหารจัดการเหตุการณ์</p> <p>(3) จัดให้มีการรายงานผลการทดสอบและทบทวนต่อหัวหน้าสำนักงานสอบบัญชี หรือคณะกรรมการบริหารของสำนักงานสอบบัญชี</p>
<p>2.12 แผนฉุกเฉินด้าน IT (IT contingency plan)</p>	
<p>ส่วนที่ 12 แผนฉุกเฉินด้าน IT (IT contingency plan)</p> <p>สำนักงานสอบบัญชีต้องจัดให้มีแผนฉุกเฉินด้าน IT เพื่อรองรับเหตุการณ์ผิดปกติด้าน IT ซึ่งส่งผลกระทบต่อการใช้งานได้ตามปกติ หรือไม่สามารถดำเนินธุรกิจอย่างต่อเนื่อง โดยต้องกู้คืนระบบให้กลับคืนสู่สภาพปกติภายในระยะเวลาที่เหมาะสมได้ ดังนี้</p>	
<p>12.1 จัดให้มีคณะทำงานหรือหน่วยงานที่รับผิดชอบในการจัดทำแผนฉุกเฉินด้าน IT</p>	<p>1. สำนักงานสอบบัญชีควรจัดให้มีคณะทำงานหรือหน่วยงานที่รับผิดชอบในการจัดทำแผนฉุกเฉินด้าน IT ไว้อย่างเป็นลายลักษณ์อักษร โดยมีผู้บริหารและบุคลากรของหน่วยงานด้านต่าง ๆ ที่เกี่ยวข้องเข้าร่วมด้วย เช่น ด้าน IT ด้านธุรกิจ และด้านสื่อสารองค์กร เป็นต้น</p>
<p>12.2 กระบวนการจัดทำแผนฉุกเฉินด้าน IT ต้องครอบคลุมการดำเนินการ ดังนี้</p> <p>12.2.1 ประเมินความเสี่ยง (risk analysis) เพื่อให้สามารถระบุเหตุการณ์ความเสี่ยงที่อาจทำให้กระบวนการและระบบงาน IT หยุดชะงัก ไม่สามารถให้บริการได้ตามปกติ หรือไม่สามารถดำเนินธุรกิจอย่างต่อเนื่อง</p>	<p>สำนักงานสอบบัญชีควรประเมินความเสี่ยง (risk analysis) เพื่อให้สามารถระบุเหตุการณ์ความเสี่ยงซึ่งส่งผลกระทบต่อการทำงานของกระบวนการและระบบงาน IT โดยมีแนวทางดำเนินการ ดังนี้</p> <ol style="list-style-type: none"> 1. ระบุเหตุการณ์ความเสี่ยง (risk scenarios) ที่อาจทำให้กระบวนการและระบบงาน IT หยุดชะงัก ทั้งจากภายในและภายนอก เช่น การโจมตีด้านไซเบอร์ ไฟไหม้ เป็นต้น 2. ประเมินความเสี่ยงโดยพิจารณาผลกระทบและโอกาสที่จะเกิดขึ้น รวมถึงการควบคุมที่มีอยู่ 3. จัดให้มีกระบวนการและทรัพยากรที่จำเป็นในการควบคุมความเสี่ยงให้อยู่ในระดับที่ยอมรับได้
<p>12.2.2 วิเคราะห์ผลกระทบทางธุรกิจ (business impact analysis) จากเหตุการณ์ความเสี่ยง</p>	<p>1. สำนักงานสอบบัญชีควรวิเคราะห์ผลกระทบทางธุรกิจ (business impact analysis) เพื่อให้ทราบถึงความสำคัญของระบบงาน IT ที่มีผลต่อการดำเนินธุรกิจ โดยมีแนวทางการดำเนินการ ดังนี้</p>

ข้อกำหนด	แนวปฏิบัติ
<p>ตาม 12.2.1 เพื่อกำหนดระยะเวลาเป้าหมายในการกู้คืนระบบงาน IT (Recovery Time Objective: RTO) ระยะเวลาเป้าหมายสูงสุดที่ยอมให้ข้อมูลเสียหาย (Recovery Point Objective: RPO) และระยะเวลาสูงสุดที่ยอมให้กระบวนการทางธุรกิจหยุดชะงัก (Maximum Tolerable Downtime: MTD) อย่างเหมาะสม</p>	<ol style="list-style-type: none"> (1) ระบุรายการกระบวนการทางธุรกิจ (business process) และระบบงาน IT ที่กระบวนการทางธุรกิจพึ่งพา (2) วิเคราะห์ผลกระทบที่เกิดจากการหยุดชะงักของระบบงาน IT เพื่อกำหนดระยะเวลา RTO, RPO และ MTD ตามความเหมาะสม (3) ระบุระบบงาน IT และทรัพยากรที่จำเป็นต่อกระบวนการทางธุรกิจที่สำคัญ (ฮาร์ดแวร์ ซอฟต์แวร์ ข้อมูล และทรัพยากรอื่น ๆ) พร้อมทั้งรายละเอียดคุณสมบัติ (specification) ขั้นต่ำของระบบงาน IT และทรัพยากรดังกล่าว (4) จัดลำดับความสำคัญของระบบงาน IT เพื่อให้ระบบงาน IT ที่สนับสนุนกระบวนการทางธุรกิจที่สำคัญสูงได้รับการกู้คืนเป็นลำดับแรก
<p>12.2.3 จัดทำแผนฉุกเฉินด้าน IT อย่างเป็นลายลักษณ์อักษร ซึ่งได้รับความเห็นชอบจากหัวหน้าสำนักงานสอบบัญชี หรือคณะกรรมการบริหารของสำนักงานสอบบัญชี</p>	<ol style="list-style-type: none"> 1. สำนักงานสอบบัญชีควรจัดให้มีแผนฉุกเฉินด้าน IT ที่ได้รับความเห็นชอบจากหัวหน้าสำนักงานสอบบัญชี หรือคณะกรรมการบริหารของสำนักงานสอบบัญชีซึ่งมีรายละเอียดของกระบวนการหรือขั้นตอนการปฏิบัติงานที่ชัดเจน เพื่อให้สามารถดำเนินการได้อย่างรวดเร็วและง่ายต่อการปฏิบัติ โดยครอบคลุมรายละเอียดอย่างน้อย ดังนี้ <ol style="list-style-type: none"> (1) หน้าที่ และความรับผิดชอบของผู้บริหารระดับสูง และผู้ที่เกี่ยวข้องในการดำเนินการตามแผน (2) รายละเอียดของระบบงาน IT เช่น โครงสร้างสถาปัตยกรรม แผนภาพแสดงระบบเครือข่ายสื่อสาร เป็นต้น (3) เงื่อนไขและขั้นตอนในการประกาศใช้แผนฉุกเฉินด้าน IT การตอบสนองต่อเหตุการณ์ฉุกเฉิน และแผนการสื่อสารให้ผู้ที่เกี่ยวข้องรับทราบ (4) ขั้นตอนการกู้คืนระบบและข้อมูล โดยมีรายละเอียดที่ชัดเจนและเพียงพอที่ผู้ปฏิบัติงานสามารถใช้เป็นขั้นตอนปฏิบัติได้อย่างถูกต้อง และเป็นไปตามเป้าหมายเวลาที่กำหนดไว้ โดยอาจจัดทำในรูปแบบรายการตรวจสอบขั้นตอนปฏิบัติ (checklist) (5) ขั้นตอนการตรวจสอบความถูกต้องครบถ้วนของระบบงาน IT และข้อมูลที่กู้คืน ก่อนกลับสู่การดำเนินกระบวนการทางธุรกิจอย่างปกติ (return to normal) (6) ขั้นตอนการประกาศยกเลิกแผนฉุกเฉินด้าน IT (7) การจัดเก็บแผนฉุกเฉินด้าน IT ไว้ในสถานที่ปลอดภัยและมีความพร้อมใช้งานในสถานที่ปฏิบัติงานหลักและสถานที่สำรอง 2. สำนักงานสอบบัญชีควรจัดให้มีรายชื่อของบุคลากรและช่องทางการติดต่อ เพื่อใช้ในการสื่อสารกรณีเกิดภาวะวิกฤตหรือมีเหตุจำเป็นเร่งด่วนได้
<p>12.3 จัดให้มีระบบงาน IT สำรอง และทรัพยากรที่จำเป็น เพื่อให้สามารถกู้คืนระบบได้ตามระยะเวลาเป้าหมายที่กำหนดไว้</p>	<ol style="list-style-type: none"> 1. สำนักงานสอบบัญชีควรจัดให้มีระบบงาน IT สำรอง และทรัพยากรที่จำเป็นเพื่อให้สามารถกู้คืนระบบงาน IT ได้ตามระยะเวลาเป้าหมายที่กำหนดไว้ โดยกรณีที่สำนักงานสอบบัญชีมีศูนย์คอมพิวเตอร์สำรอง ควรระบุรายละเอียดเกี่ยวกับศูนย์คอมพิวเตอร์สำรองให้ชัดเจน เช่น ทรัพยากรที่มี สถานที่ตั้งและแผนที่ เป็นต้น

ข้อกำหนด	แนวปฏิบัติ
<p>12.4 สื่อสารให้บุคลากรที่เกี่ยวข้องมีความเข้าใจและสามารถปฏิบัติตามแผนฉุกเฉินด้าน IT อย่างเหมาะสม</p>	<p>1. สำนักงานสอบบัญชีควรสื่อสารแผนฉุกเฉินด้าน IT ให้พนักงานทุกคนที่มีส่วนเกี่ยวข้องกับการปฏิบัติตามแผนฉุกเฉินด้าน IT มีความเข้าใจ และสามารถปฏิบัติตามแผนได้อย่างถูกต้อง</p>
<p>12.5 ทบทวนและทดสอบการปฏิบัติตามแผนฉุกเฉินด้าน IT อย่างน้อยปีละ 1 ครั้ง และเมื่อมีเหตุจำเป็นที่ควรได้รับการทบทวนและทดสอบดังกล่าว โดยรายงานผลการทบทวนและทดสอบต่อหัวหน้าสำนักงานสอบบัญชี หรือคณะกรรมการบริหารของสำนักงานสอบบัญชี</p>	<p>1. สำนักงานสอบบัญชีควรทบทวน (review) และทดสอบ (test) การปฏิบัติตามแผนฉุกเฉินด้าน IT อย่างน้อยปีละ 1 ครั้ง และเมื่อมีเหตุจำเป็นที่ควรได้รับการทดสอบและทบทวนดังกล่าว เช่น มีการเปลี่ยนแปลงกลยุทธ์ทางธุรกิจ นโยบายการบริหารความเสี่ยงโดยรวม สภาพแวดล้อมของการให้บริการหรือดำเนินธุรกิจ ทรัพยากร หรือโครงสร้างระบบงาน IT เป็นต้น</p> <p>2. สำนักงานสอบบัญชีควรกำหนดเหตุการณ์ที่ใช้ในการทดสอบประจำปี (test scenario) โดยเป็นเหตุการณ์ที่มีโอกาสที่จะเกิดขึ้นและอาจส่งผลกระทบต่อกระบวนการทางธุรกิจที่สำคัญหยุดชะงัก เช่น การหยุดชะงักของระบบงาน IT ที่สนับสนุนกระบวนการทางธุรกิจที่สำคัญ การหยุดชะงักของผู้ให้บริการภายนอกที่สำคัญ (รวมถึงผู้ให้บริการคลาวด์) และการโจมตีทางไซเบอร์ เป็นต้น</p> <p>3. สำนักงานสอบบัญชีควรรายงานผลการทดสอบแผนฉุกเฉินด้าน IT ต่อหัวหน้าสำนักงานสอบบัญชี หรือคณะกรรมการบริหารของสำนักงานสอบบัญชีโดยมีรายละเอียดอย่างน้อยครอบคลุมวัตถุประสงค์ ขอบเขตการทดสอบสถานการณ์จำลอง ผลการทดสอบ ข้อผิดพลาดและปัญหาหรืออุปสรรคที่พบ พร้อมทั้งแนวทางปรับปรุงแก้ไข</p>
<p>12.6 จัดให้มีรายละเอียดในการติดต่อ ดังนี้ เพื่อให้สามารถประสานงานในการรายงานเหตุการณ์ผิดปกติด้าน IT หรือขอความช่วยเหลือจากหน่วยงานภายนอกที่เกี่ยวข้องได้อย่างมีประสิทธิภาพ โดยต้องปรับปรุงข้อมูลดังกล่าวให้เป็นปัจจุบันอยู่เสมอ</p> <p>12.6.1 รายชื่อหน่วยงานกำกับดูแลและบุคคลภายนอกที่ให้บริการหรือที่มีการเชื่อมต่อกับระบบงาน IT ของสำนักงานสอบบัญชี</p> <p>12.6.2 ช่องทางในการติดต่อ และรายชื่อผู้ที่เกี่ยวข้องของหน่วยงานกำกับดูแลหรือบุคคลภายนอกตาม 12.7.1</p>	<p>[ไม่มีการกำหนดแนวปฏิบัติไว้เป็นการเฉพาะ]</p>

หมวดที่ 3 การตรวจสอบด้านเทคโนโลยีสารสนเทศ (Information Technology Audit)

ให้สำนักงานสอบบัญชีดำเนินการตามที่กำหนดในภาคผนวกนี้

ข้อกำหนด	แนวปฏิบัติ
<p>1. การจัดให้มีผู้ตรวจสอบ</p> <p>ผู้ตรวจสอบอาจเป็นได้ทั้งผู้ตรวจสอบภายในที่สังกัดสำนักงานสอบบัญชี หรือผู้ตรวจสอบจากภายนอก ซึ่งต้องมีคุณสมบัติ ดังนี้</p> <p>1.1 มีความเป็นอิสระจากผู้ที่ทำหน้าที่ด้าน IT ในระดับ ดังนี้</p> <p>1.1.1 ระดับที่ 1 (first line of defense): การปฏิบัติงาน</p> <p>1.1.2 ระดับที่ 2 (second line of defense): การบริหารความเสี่ยงในการปฏิบัติงานทางด้าน IT</p> <p>1.2 หัวหน้าทีมผู้ตรวจสอบที่เป็นผู้รับผิดชอบต่อผลการตรวจสอบด้านเทคโนโลยีสารสนเทศ ("ผลการตรวจสอบด้าน IT") ต้องผ่านการรับรองและมีวุฒิปับตรอย่างหนึ่งอย่างใดดังนี้ และมีวุฒิปับตรซึ่งยังไม่สิ้นผล</p> <p>1.2.1 Certified Information Systems Auditor (CISA)</p> <p>1.2.2 Certified Information Security Manager (CISM)</p> <p>1.2.3 Certified Information Systems Security Professional (CISSP)</p> <p>1.2.4 ISO/IEC 27001 Lead Auditor</p> <p>1.2.5 ใ้รับรองอื่นตามที่กำหนดเพิ่มเติมบนเว็บไซต์ของสำนักงาน ก.ล.ต.</p>	[ไม่มีการกำหนดแนวปฏิบัติไว้เป็นการเฉพาะ]
<p>2. การวางแผนและกำหนดขอบเขตการตรวจสอบ</p> <p>2.1 ทบทวนแผนงานและขอบเขตการตรวจสอบให้สอดคล้องกับความเสี่ยงของสำนักงานสอบบัญชีตามผลการประเมินความเสี่ยง (risk assessment) ของสำนักงานสอบบัญชีอย่างน้อยปีละ 1 ครั้ง และเมื่อมีการเปลี่ยนแปลงระบบงาน IT อย่างมีนัยสำคัญ</p> <p>2.2 สำนักงานสอบบัญชีควรกำหนดกรอบการตรวจสอบครอบคลุมระยะเวลาอย่างน้อย 12 เดือน และรอบการตรวจถัดไปควรมีวันที่เริ่มต้นและสิ้นสุดสอดคล้องกับรอบการตรวจครั้งก่อนหน้าที่เคยนำเสนอรายงานผลการตรวจสอบระบบงาน IT ให้สำนักงาน ก.ล.ต.</p> <p>ทั้งนี้ กรณีสำนักงานสอบบัญชีมีความประสงค์จะเปลี่ยนแปลงรอบการตรวจในปัจจุบัน สำนักงานสอบบัญชีต้องแจ้งการเปลี่ยนแปลงรอบการตรวจใหม่ภายใน 30 วันนับแต่มีการเปลี่ยนแปลง อย่างไรก็ตาม หากสำนักงานสอบบัญชีมีการเปลี่ยนแปลงรอบการตรวจสอบใหม่ สำนักงานสอบบัญชีต้องจัดให้มีกระบวนการตรวจสอบเพื่อให้มาซึ่งหลักฐานที่สามารถให้ความเชื่อมั่นว่าระบบทรัพยากรทางเทคโนโลยีตามมาตรฐานการบริหารคุณภาพและการควบคุมที่เกี่ยวข้องระหว่างรอบการตรวจสอบเดิมและรอบการตรวจสอบใหม่ยังคงมีอยู่ และมีประสิทธิภาพ</p>	[ไม่มีการกำหนดแนวปฏิบัติไว้เป็นการเฉพาะ]

ข้อกำหนด	แนวปฏิบัติ
<p>3. การตรวจสอบด้าน IT ตามแผนงานและขอบเขตที่กำหนด</p> <p>3.1 จัดให้มีการตรวจสอบด้าน IT ตามความถี่ที่ประเมินได้จากการประเมินระดับความเสี่ยงของสำนักงานสอบบัญชี (IT Risk Assessment: “ITRA”) และจัดทำรายงานผลการตรวจสอบ</p> <p>3.2 จัดให้มีการบันทึกและจัดเก็บข้อมูลเกี่ยวกับการตรวจสอบ เช่น กระดาษทำการ (working paper) และหลักฐานประกอบการตรวจ เป็นต้น เป็นระยะเวลาไม่น้อยกว่า 5 ปีนับแต่วันที่จัดทำรายงานและแผนดังกล่าว โดยต้องจัดเก็บไว้ในลักษณะที่พร้อมให้สำนักงาน ก.ล.ต. สามารถเรียกดูและตรวจสอบได้โดยไม่ชักช้า</p>	[ไม่มีการกำหนดแนวปฏิบัติไว้เป็นการเฉพาะ]
<p>4. กรณีผลการตรวจสอบดังกล่าวมีข้อสังเกตหรือข้อบกพร่อง</p> <p>สำนักงานสอบบัญชีต้องจัดให้มีการวิเคราะห์เชิงลึกถึงสาเหตุของข้อบกพร่อง (“root cause analysis”) และการจัดทำแผนการแก้ไข (“remediation plan”) ข้อบกพร่องหรือข้อสังเกตจากรายงานผลการตรวจสอบด้าน IT และติดตามความคืบหน้าในการดำเนินการตามแผนดังกล่าว</p>	[ไม่มีการกำหนดแนวปฏิบัติไว้เป็นการเฉพาะ]
<p>5. การนำส่งรายงานผลการตรวจสอบและเอกสารที่เกี่ยวข้อง</p> <p>5.1 เสนอรายงานผลการตรวจสอบระบบงาน IT ตามหัวข้อที่ 3. ที่จัดทำโดยผู้เชี่ยวชาญ รวมทั้ง root cause analysis และ remediation plan กรณีพบข้อสังเกตหรือข้อบกพร่อง รวมถึงผล ITRA ที่ประเมินใหม่ในปีนั้น เพื่อหารือระยะเวลาถัดไปที่จะตรวจแบบเต็มรูปแบบอีกครั้ง ต่อหัวหน้าสำนักงานสอบบัญชี แล้วนำส่งสำนักงาน ก.ล.ต. ตามรูปแบบและวิธีการที่กำหนดไว้บนเว็บไซต์ของสำนักงาน ก.ล.ต. ภายใน 5 เดือนนับแต่วันสิ้นสุดรอบการตรวจสอบ</p> <p>หมายเหตุ: หากวันที่นำส่งสำนักงาน ก.ล.ต. ตรงกับวันหยุดของสำนักงาน ก.ล.ต.ให้นำส่งวันทำการถัดไปแทน</p> <p>5.2 จัดเก็บเอกสารตาม 5.1 เป็นระยะเวลาไม่น้อยกว่า 5 ปีนับแต่วันที่จัดทำรายงานและแผนดังกล่าว โดยต้องจัดเก็บไว้ในลักษณะที่พร้อมให้สำนักงาน ก.ล.ต. สามารถเรียกดูและตรวจสอบได้โดยไม่ชักช้า</p>	
<p>6. การขอผ่อนผัน</p> <p>กรณีมีเหตุผลจำเป็นและสมควรที่ทำให้สำนักงานสอบบัญชีไม่สามารถดำเนินการตรวจสอบระบบงาน IT ได้ภายในรอบระยะเวลาตามที่ผล ITRA ล่าสุดกำหนดไว้ หรือสำนักงานสอบบัญชีไม่สามารถนำส่งเอกสารประกอบการตรวจสอบระบบงาน IT ได้ภายในระยะเวลาตามที่หัวข้อที่ “5. การนำส่งรายงานผลการตรวจสอบและเอกสารที่เกี่ยวข้อง” กำหนด สำนักงานสอบบัญชีต้องยื่นหนังสือขอผ่อนผันการดำเนินการตรวจสอบระบบงาน IT ต่อสำนักงาน ก.ล.ต. ตามคู่มือสำหรับประชาชนก่อนสิ้นสุดระยะเวลาที่กำหนดให้สำนักงานสอบบัญชีต้องจัดทำและส่งรายงานผลการตรวจสอบและเอกสารที่เกี่ยวข้องให้แก่สำนักงาน ก.ล.ต. อ้างอิงรอบการตรวจปัจจุบัน พร้อมทั้งชี้แจงเหตุผลและความจำเป็นในการขอผ่อนผันและแจ้งกำหนดระยะเวลาใหม่ที่จะดำเนินการตรวจสอบด้าน IT หรือจัดส่งเอกสารนั้น ซึ่งสำนักงาน ก.ล.ต.</p>	

ข้อกำหนด	แนวปฏิบัติ
<p>จะพิจารณาผ่อนผันเป็นรายกรณีตามความจำเป็นและสมควร</p> <p>7. วิธีปฏิบัติในช่วงเปลี่ยนแปลง (transitional period):</p> <p>สำหรับสำนักงานสอบบัญชีในตลาดทุนที่ผู้สอบบัญชีในสังกัดได้รับความเห็นชอบจากสำนักงาน ก.ล.ต. ก่อนหน้าที่ประกาศฉบับนี้จะมีผลบังคับใช้ การเริ่มใช้หลักเกณฑ์ในการกำกับดูแลและการตรวจสอบด้านเทคโนโลยีสารสนเทศ (Information Technology) เป็นครั้งแรก สำนักงานสอบบัญชีในตลาดทุนต้องดำเนินการตรวจสอบระบบงาน IT แบบเต็มรูปแบบ (“full-scope”) ภายในรอบระยะเวลาสิ้นสุด 31 ธันวาคม 2569 เป็นครั้งแรกและนำเสนอเอกสาร ได้แก่</p> <ul style="list-style-type: none"> 7.1 รายงานผลการตรวจสอบระบบงาน IT แบบ full-scope โดยผู้เชี่ยวชาญ 7.2 root cause analysis และ remediation plan กรณีผลการตรวจสอบดังกล่าวมีข้อสังเกตหรือข้อบกพร่อง 7.3 ITRA ที่ประเมินครั้งแรก เพื่อหารอบระยะเวลาถัดไปที่จะตรวจแบบเต็มรูปแบบอีกครั้ง <p>โดยสำนักงานสอบบัญชีจะต้องจัดเตรียมและนำเสนอเอกสารข้างต้น ภายใน 5 เดือนนับแต่วันสิ้นสุดรอบการตรวจสอบ และต้องไม่เกินวันที่ 31 พฤษภาคม 2570</p>	<p>สำนักงานสอบบัญชีในตลาดทุนสามารถเลือกดำเนินการตรวจสอบระบบงาน IT แบบ full-scope ภายในปีใดปีหนึ่งระหว่างปี 2567-2569 เช่น สำนักงานสอบบัญชีเลือกจะตรวจสอบ full-scope ครั้งแรกในปี 2569 (รอบระยะเวลาการตรวจ 1 มกราคม 2569 ถึง 31 ธันวาคม 2569) สำนักงานสอบบัญชีต้องนำเสนอเอกสาร ดังต่อไปนี้</p> <ul style="list-style-type: none"> - รายงานผลการตรวจสอบระบบงาน IT แบบ full-scope โดยผู้เชี่ยวชาญ - root cause analysis และ remediation plan (ถ้ามี) - ITRA ที่ประเมินครั้งแรก เพื่อหารอบระยะเวลาถัดไปที่จะตรวจแบบเต็มรูปแบบอีกครั้ง <p>โดยสำนักงานสอบบัญชีจะต้องจัดเตรียมและนำเสนอเอกสารข้างต้นภายในวันที่ 31 พฤษภาคม 2570</p>
<p>8. วิธีปฏิบัติสำหรับสำนักงานสอบบัญชีใหม่ที่จะเข้ามาปฏิบัติงานในตลาดทุนเป็นครั้งแรก ให้ดำเนินการตามข้อกำหนดด้านล่างตั้งแต่วันที่ประกาศมีผลบังคับใช้</p> <p>สำนักงานสอบบัญชีใหม่ต้องจัดให้มีการดำเนินการตรวจสอบด้านเทคโนโลยีสารสนเทศ (Information Technology) เป็นครั้งแรก และจัดส่งเอกสารตามด้านล่างมายังสำนักงาน ก.ล.ต. เพื่อเป็นเอกสารประกอบการแสดงคุณสมบัติของผู้สอบบัญชีในสังกัดสำนักงานสอบบัญชีที่จะยื่นขอความเห็นชอบเป็นผู้สอบบัญชีในตลาดทุนเป็นครั้งแรก</p> <ul style="list-style-type: none"> 8.1 รายงานผลการตรวจสอบระบบงาน IT แบบ full-scope โดยผู้เชี่ยวชาญ 8.2 root cause analysis และ remediation plan กรณีผลการตรวจสอบดังกล่าวมีข้อสังเกตหรือข้อบกพร่อง 8.3 ITRA ที่ประเมินครั้งแรก เพื่อหารอบระยะเวลาถัดไปที่จะตรวจแบบเต็มรูปแบบอีกครั้ง <p>โดยเอกสารที่นำเสนอข้างต้น ณ วันที่นำเสนอ ต้องมีอายุไม่เกิน 5 เดือนนับแต่วันสิ้นสุดรอบการตรวจสอบ</p>	

ข้อกำหนด	แนวปฏิบัติ
<p>9. วิธีปฏิบัติสำหรับสำนักงานสอบบัญชีที่มีการรวมศูนย์เทคโนโลยีสารสนเทศไว้ที่ต่างประเทศ หรือมีสำนักงานเครือข่ายในต่างประเทศ หรือได้รับการตรวจคุณภาพตามมาตรฐานสากล เช่น ISO27001</p> <p>หากสำนักงานสอบบัญชีที่มีการรวมศูนย์เทคโนโลยีสารสนเทศไว้ที่ต่างประเทศและถูกตรวจสอบโดยสำนักงานเครือข่ายในต่างประเทศ หรือได้รับการตรวจคุณภาพตามมาตรฐานสากลแล้ว สำนักงานสอบบัญชีสามารถนำข้อมูลจากรายงานผลการตรวจสอบดังกล่าวมากรอกในแบบรายงานผลการตรวจสอบระบบงานทางด้านเทคโนโลยีสารสนเทศด้าน IT แบบ full-scope ตามที่สำนักงาน ก.ล.ต. กำหนด เพื่อนำส่งสำนักงาน ก.ล.ต. ได้ หากพิจารณาแล้วพบว่า การตรวจสอบดังกล่าวมีลักษณะดังนี้</p> <p>9.1 ขอบเขตการตรวจสอบครอบคลุมระบบงาน IT ที่เกี่ยวข้องทั้งหมดตามที่มาตรฐานการบริหารคุณภาพ (TSQM1) กำหนด และเทียบเท่าได้กับหลักเกณฑ์ในการกำกับดูแลและการตรวจสอบด้านเทคโนโลยีสารสนเทศ (Information Technology) สำหรับสำนักงานสอบบัญชีฉบับนี้</p> <p>9.2 ผู้ตรวจสอบมีคุณสมบัติตามที่ประกาศหรือการกำกับดูแลและการตรวจสอบด้านเทคโนโลยีสารสนเทศ (Information Technology) สำหรับสำนักงานสอบบัญชีฉบับนี้กำหนด</p> <p>9.3 รอบการตรวจสอบของรายงานดังกล่าวตรงกับรอบการตรวจตามหลักเกณฑ์ประเมินระดับความเสี่ยงของสำนักงานสอบบัญชี (IT Risk Assessment: “ITRA”) ตามที่สำนักงาน ก.ล.ต. กำหนด เช่น หากสำนักงานสอบบัญชี A ได้มีการตรวจสอบด้านเทคโนโลยีครั้งล่าสุดในปี 2569 และทำการประเมินความเสี่ยงตาม ITRA ได้ความถี่ 2 ปีครั้ง สำนักงานสอบบัญชี A ต้องจัดให้มีการตรวจสอบอีกครั้งในปี 2571 ดังนั้น หากสำนักงานสอบบัญชี A จะนำผลการตรวจสอบทางด้านเทคโนโลยีสารสนเทศ IT ที่จัดทำขึ้นโดยสำนักงานเครือข่ายในต่างประเทศ หรือ โดยผู้เชี่ยวชาญที่ตรวจสอบคุณภาพตามมาตรฐานสากล มาอ้างอิงเพื่อนำส่งสำนักงาน ก.ล.ต. ผลการตรวจสอบดังกล่าวต้องเป็นการตรวจสอบที่ดำเนินการตรวจสอบในปี 2571 เช่นเดียวกัน ทั้งนี้ หากสำนักงานสอบบัญชี พบว่ารายงานผลการตรวจสอบที่ได้มาจาก สำนักงานเครือข่ายในต่างประเทศ หรือ จากผู้เชี่ยวชาญที่ตรวจสอบคุณภาพตามมาตรฐานสากล ไม่ครอบคลุมตามหลักเกณฑ์ในการกำกับดูแล IT ฉบับนี้ อนุโลมให้สำนักงานสอบบัญชีดำเนินการตรวจสอบเพิ่มเติมเฉพาะส่วนที่ยังไม่ครบถ้วนตามข้อกำหนดในการกำกับดูแลและการตรวจสอบด้านเทคโนโลยีสารสนเทศ (Information Technology) สำหรับสำนักงานสอบบัญชีฉบับนี้</p>	

คำจำกัดความ

เพื่อวัตถุประสงค์ของการกำกับดูแลและการตรวจสอบด้านเทคโนโลยีสารสนเทศ (Information Technology) สำหรับสำนักงานสอบบัญชีฉบับนี้

1. ระบบงานเทคโนโลยีสารสนเทศ หรือ ระบบงาน IT	<p>หมายถึง ทรัพยากรทางเทคโนโลยีของสำนักงานสอบบัญชีที่มีวัตถุประสงค์เกี่ยวข้องกับระบบการบริหารคุณภาพของสำนักงานสอบบัญชี โดยอ้างอิงตามมาตรฐานการบริหารคุณภาพ (TSQM1) ย่อหน้า 32(ฉ) ก99 ดังนี้</p> <p>(1) ทรัพยากรทางเทคโนโลยี ซึ่งใช้ในการออกแบบ การนำไปปฏิบัติ หรือการดำเนินการในระบบการบริหารคุณภาพของสำนักงานสอบบัญชีโดยตรง เช่น ระบบ timesheet และ ระบบการประเมินการรับงานสอบบัญชี เป็นต้น</p> <p>(2) ทรัพยากรทางเทคโนโลยี ซึ่งกลุ่มผู้ปฏิบัติงานใช้ในการปฏิบัติงานโดยตรง เช่น Microsoft programs โปรแกรมคำนวณขนาดตัวอย่างในการตรวจสอบ โปรแกรมที่ใช้ในการวิเคราะห์ความสัมพันธ์ของข้อมูล (Data Analytics) และระบบที่ใช้ในกระบวนการตรวจสอบและจัดเก็บกระดาษทำการ (Smart Audit Platform) เป็นต้น</p> <p>(3) ทรัพยากรทางเทคโนโลยี ซึ่งจำเป็นในการช่วยทำให้การดำเนินการข้างต้นมีประสิทธิภาพ เช่น เกี่ยวกับระบบงานเทคโนโลยีสารสนเทศ โครงสร้างทางเทคโนโลยีสารสนเทศ และกระบวนการทางเทคโนโลยีสารสนเทศที่ช่วยสนับสนุนระบบงานเทคโนโลยีสารสนเทศ เช่น ระบบปฏิบัติการคอมพิวเตอร์ (Operating System) และ ระบบฐานข้อมูล (Database) เป็นต้น</p>
2. การตรวจสอบด้าน IT แบบเต็มรูปแบบ (“full-scope”)	<p>หมายถึง การตรวจสอบระบบงานเทคโนโลยีสารสนเทศ หรือ ระบบงาน IT โดยผู้เชี่ยวชาญ โดยสำนักงานสอบบัญชีต้องจัดให้มีการตรวจระบบงานเทคโนโลยีสารสนเทศ หรือระบบงาน IT ตามผลการประเมินความเสี่ยงของสำนักงานสอบบัญชี โดยการตรวจสอบต้องครอบคลุมตามข้อกำหนดที่ระบุไว้ในเอกสาร “การกำกับดูแลและการตรวจสอบด้านเทคโนโลยีสารสนเทศ (Information Technology) สำหรับสำนักงานสอบบัญชี”</p>