สิ่งที่ส่งมาด้วย 1

แนวปฏิบัติในการกำกับดูแลและการตรวจสอบ
ด้านเทคโนโลยีสารสนเทศ (Information Technology)
สำหรับสำนักงานสอบบัญชี

สารบัญ

หน้า

หมวดที่ 1 การกำกับดูแลและบริหารจัดการด้านเทคโนโลยีสารสนเทศ (Information Technology Governance)

ข้อกำหนด	แนวปฏิบัติ
1.1 บทบาทหน้าที่และความรับผิดชอบของหัวหน้าสำนักงานสอบบัญชี หรือคณะกรรมการบริหารของสำนักงานสอบบัญชี	
ส่วนที่ 1 บทบาทหน้าที่และความรับผิดชอบของหัวหน้าสำนักงานสอบบัญชี หรือคณะกรรมการบริหารของสำนักงานสอบบัญชี หัวหน้าสำนักงานสอบบัญชี หรือคณะกรรมการบริหารของสำนักงานสอบบัญชีควรมีการควบคุมดูแลและบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ (“IT”) ให้สอดคล้องกับระดับความเสี่ยงที่สำนักงานสอบบัญชียอมรับได้ โดยคำนึงถึงการบริหารและจัดการความเสี่ยงขององค์กร (enterprise risk) โดยควรครอบคลุมเนื้อหาอย่างน้อยในเรื่องดังต่อไปนี้	
1.1 ควรมีการกำหนดกรอบการกำกับดูแลด้าน IT (IT governance framework) และการกำกับดูแลแผนงานด้าน IT ให้สอดคล้องกับแผนธุรกิจ และมีความเหมาะสมเพียงพอที่จะรองรับการเปลี่ยนแปลงด้าน IT และการเปลี่ยนแปลงการดำเนินธุรกิจในอนาคต	1. สำนักงานสอบบัญชีควรมีการกำหนดกรอบการกำกับดูแลด้าน IT (IT governance framework) โดยควรครอบคลุมเนื้อหาอย่างน้อยในเรื่องดังต่อไปนี้ (1) โครงสร้างการกำกับดูแล บทบาทหน้าที่และความรับผิดชอบของหัวหน้าสำนักงานสอบบัญชี หรือคณะกรรมการบริหารของสำนักงานสอบบัญชี และฝ่ายงานที่เกี่ยวข้อง สำหรับการกำกับดูแลด้าน IT ของสำนักงานสอบบัญชี (2) กระบวนการที่เกี่ยวข้องกับการกำกับดูแลด้าน IT โดยควรครอบคลุมเนื้อหาอย่างน้อยในเรื่องดังต่อไปนี้ (2.1) การจัดทำและขออนุมัติแผนงานด้าน IT (2.2) การจัดทำแผนและการบริหารจัดการทรัพยากรด้าน IT (2.3) การติดตามและรายงานผลการดำเนินการด้าน IT 2. สำนักงานสอบบัญชีควรมีการจัดทำแผนงานด้าน IT ประจำปี เพื่อให้การใช้ IT สอดรับกับกลยุทธ์ในการดำเนินธุรกิจ
1.2 ควรมีการจัดสรรทรัพยากรทางด้าน IT และทรัพยากรบุคคลที่ปฏิบัติงานด้าน IT ให้มีความเหมาะสมเพียงพอต่อการดำเนินธุรกิจ	1. สำนักงานสอบบัญชีควรมีการจัดสรรทรัพยากรทางด้าน IT และทรัพยากรบุคคลที่ปฏิบัติงานด้าน IT ให้สอดคล้องกับเป้าหมายตามภารกิจ กลยุทธ์ นโยบาย และแผนการดำเนินงานที่กำหนดไว้

ข้อกำหนด	แนวปฏิบัติ
1.3 ควรมีการกำหนดนโยบายที่เกี่ยวข้องกับการกำกับดูแลความเสี่ยงด้าน IT อย่างเป็นลายลักษณ์อักษร โดยควรครอบคลุมเนื้อหาอย่างน้อยในเรื่องนโยบายตามที่กำหนดในหมวดที่ 1 ส่วนที่ 2 ข้อ 2.2.1 และ 2.2.2	1. สำนักงานสอบบัญชีควรมีการกำหนดนโยบายที่เกี่ยวข้องกับการกำกับดูแลความเสี่ยงด้าน IT อย่างเป็นลายลักษณ์อักษร โดยควรครอบคลุมเนื้อหาอย่างน้อยในเรื่องนโยบายตามที่กำหนดในหมวดที่ 1 ส่วนที่ 2 ข้อ 2.2.1 และ 2.2.2 และควรมีการทบทวนความเหมาะสมของนโยบายดังกล่าวทุกปีเป็นอย่างน้อยเพื่อให้สอดคล้องกับความเสี่ยงของสำนักงานสอบบัญชีในปัจจุบัน ในกรณีที่สำนักงานสอบบัญชีพิจารณาเรื่องการบริหารจัดการความเสี่ยงด้าน IT ตามหมวดที่ 1 ส่วนที่ 2 ข้อ 2.2.1 แล้วพบว่าสำนักงานสอบบัญชีไม่มีกิจกรรมที่อาจจะก่อให้เกิดความเสี่ยงด้าน IT ในบางหัวข้อที่ระบุไว้ในหมวดที่ 1 ส่วนที่ 2 ข้อ 2.2.2 ได้แก่ (2) การบริหารจัดการบุคลากรเฉพาะเรื่องการบริหารจัดการบุคคลภายนอก (6) การควบคุมการเข้ารหัส (cryptographic control) (8) การรักษาความมั่นคงปลอดภัยในการปฏิบัติงานด้าน IT เฉพาะเรื่องการประเมินช่องโหว่ทางเทคนิค (technical vulnerability assessment) (10) การบริหารจัดการโครงการด้าน IT และการจัดหา พัฒนา และบำรุงรักษาระบบงาน IT สำนักงานสอบบัญชีสามารถยกเว้นการกำหนดนโยบายการกำกับดูแลความเสี่ยงด้าน IT ในเรื่องนั้น ๆ ได้ อย่างไรก็ดี สำหรับหัวข้ออื่นนอกเหนือจากที่กล่าวข้างต้นนั้น เป็นหัวข้อที่โดยปกติมีความเกี่ยวข้องกับทุกสำนักงานสอบบัญชี จึงควรมีการกำหนดนโยบายให้ครบถ้วน ทั้งนี้ หากสำนักงานสอบบัญชีมีกิจกรรมที่อาจจะก่อให้เกิดความเสี่ยงด้าน IT แต่มีข้อจำกัดในการดำเนินการตามแนวปฏิบัติฉบับนี้ สำนักงานสอบบัญชีควรหาวิธีการควบคุมอื่นทดแทน เพื่อลดระดับความเสี่ยงดังกล่าวให้อยู่ในระดับที่ยอมรับได้
1.4 ควรมีการกำหนดขั้นตอนและวิธีปฏิบัติงานในการบริหารจัดการความเสี่ยงด้าน IT และการรักษาความมั่นคงปลอดภัยด้าน IT เพื่อให้เป็นไปตามนโยบายในข้อ 1.3 รวมถึงกำกับดูแลให้มีการนำไปปฏิบัติอย่างเหมาะสม	[ไม่มีการกำหนดแนวปฏิบัติไว้เป็นการเฉพาะ]
1.5 ควรมีการสร้างความรู้และความตระหนักด้านความเสี่ยงด้าน IT แก่บุคลากรอย่างต่อเนื่องและมีประสิทธิผล	[ไม่มีการกำหนดแนวปฏิบัติไว้เป็นการเฉพาะ]

ข้อกำหนด	แนวปฏิบัติ
1.6 ควรมีการติดตาม ตรวจสอบ และรายงานผลการปฏิบัติงานเพื่อให้เป็นไปตามนโยบายในข้อ 1.3 ต่อหัวหน้าสำนักงานสอบบัญชี หรือคณะกรรมการบริหารของสำนักงานสอบบัญชี โดยควรมีการรายงานอย่างน้อยปีละ 1 ครั้ง และในกรณีที่มีเหตุการณ์หรือการเปลี่ยนแปลงใด ๆ ซึ่งอาจส่งผลกระทบอย่างมีนัยสำคัญต่อการปฏิบัติงาน เพื่อให้เป็นไปตามนโยบายดังกล่าว ควรมีการรายงานให้หัวหน้าสำนักงานสอบบัญชี หรือคณะกรรมการบริหารของสำนักงานสอบบัญชีทราบโดยไม่ชักช้าด้วย	1. สำนักงานสอบบัญชีควรจัดให้มีกระบวนการติดตาม ตรวจสอบ และควบคุมการจัดทำรายงานผลการปฏิบัติงานเพื่อให้มั่นใจว่าสามารถจัดทำรายงานได้อย่างครบถ้วนถูกต้อง 2. สำนักงานสอบบัญชีควรกำหนดให้มีการรายงานผลการปฏิบัติตามนโยบายที่เกี่ยวข้องกับการกำกับดูแลและบริหารจัดการความเสี่ยงด้าน IT ต่อหัวหน้าสำนักงานสอบบัญชี หรือคณะกรรมการบริหารของสำนักงานสอบบัญชี โดยควรครอบคลุมเนื้อหาอย่างน้อยในเรื่องดังต่อไปนี้ (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 (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
1.2 โครงสร้างการกำกับดูแล	
ส่วนที่ 2 การกำกับดูแลและบริหารจัดการความเสี่ยงด้าน IT ในระดับองค์กร 2.1 สำนักงานสอบบัญชีควรจัดให้มีโครงสร้างการกำกับดูแลและบริหารจัดการความเสี่ยงด้าน IT โดยอย่างน้อยควรมีลักษณะดังนี้ 2.1.1 ทำให้เกิดการถ่วงดุลอย่างเป็นอิสระ 2.1.2 สอดคล้องตามหลักการแบ่งแยกหน้าที่ 3 ระดับ	สำนักงานสอบบัญชีควรจัดให้มีโครงสร้างการกำกับดูแลและบริหารจัดการความเสี่ยงด้าน IT ที่มีการถ่วงดุลอำนาจ (check and balance) และมีการแบ่งแยกหน้าที่ (segregation of duties) อย่างเหมาะสม ตามหลักการแบ่งแยกหน้าที่ 3 ระดับ ได้แก่ 1. การปฏิบัติงาน (first line of defense) หมายถึง หน่วยงานหรือบุคลากรที่ปฏิบัติงานด้าน IT และผู้ที่ใช้ระบบงาน IT ปฏิบัติงาน (1.1) หน่วยงานหรือบุคลากรที่ปฏิบัติงานด้าน IT มีหน้าที่ปฏิบัติงานตามหน้าที่ความรับผิดชอบ ประเมินความเสี่ยงและควบคุมความเสี่ยงด้าน IT ติดตามและรายงานการปฏิบัติงานด้าน IT ต่อหัวหน้าสำนักงานสอบบัญชี หรือคณะกรรมการ

ข้อกำหนด	แนวปฏิบัติ
(3 Lines of Defense : 3 LoDs) โดยควรมีการแบ่งแยกหน้าที่อย่างชัดเจนระหว่างการทำหน้าที่ด้าน IT ดังนี้ <u>ระดับที่ 1</u> (first line of defense) : การปฏิบัติงาน <u>ระดับที่ 2</u> (second line of defense) : การบริหารความเสี่ยงที่เกี่ยวข้องกับระบบงาน IT <u>ระดับที่ 3</u> (third line of defense) : การตรวจสอบ	บริหารของสำนักงานสอบบัญชีที่ได้รับมอบหมาย (1.2) ผู้ที่ใช้ระบบงาน IT ปฏิบัติงาน มีหน้าที่ปฏิบัติตามนโยบายและระเบียบปฏิบัติที่เกี่ยวข้องกับความมั่นคงปลอดภัยด้าน IT รวมทั้งมีส่วนร่วมรับผิดชอบในการประเมินและจัดการความเสี่ยงด้าน IT ที่เกี่ยวข้องกับการใช้งานระบบ 2. การบริหารความเสี่ยงที่เกี่ยวข้องกับระบบงาน IT (second line of defense) หมายถึง หน่วยงานหรือบุคลากรที่บริหารความเสี่ยงด้าน IT (IT risk function) มีหน้าที่กำหนดกรอบนโยบาย และกระบวนการบริหารความเสี่ยงด้าน IT สนับสนุนให้มีการประเมินความเสี่ยงตามกรอบการบริหารความเสี่ยงที่กำหนด พร้อมทั้งให้คำปรึกษา ติดตามความเสี่ยง และทบทวนการควบคุมความเสี่ยงด้าน IT ให้อยู่ในระดับความเสี่ยงที่ยอมรับได้ โดยมีการรวบรวมและเชื่อมโยงความเสี่ยงด้าน IT กับความเสี่ยงด้านอื่น และนำเสนอผลการบริหารความเสี่ยงต่อหัวหน้าสำนักงานสอบบัญชี หรือคณะกรรมการบริหารของสำนักงานสอบบัญชีที่ได้รับมอบหมาย 3. การตรวจสอบด้าน IT (third line of defense) หมายถึง หน่วยงาน หรือบุคลากรที่ทำหน้าที่ตรวจสอบด้าน IT ซึ่งมีหน้าที่ในการตรวจสอบการปฏิบัติงานของหน่วยงานที่ทำหน้าที่ first line และ second line of defense เพื่อให้มั่นใจว่ามีการปฏิบัติตามนโยบาย มาตรฐาน และกฎหมายทางด้าน IT ที่เกี่ยวข้อง หน่วยงาน หรือบุคลากรในระดับนี้อาจเป็นผู้ตรวจสอบภายในหรือผู้ตรวจสอบภายนอกผู้ซึ่งมีความเป็นอิสระจากหน่วยงานที่ทำหน้าที่ first line และ second line of defense
1.3 นโยบายที่เกี่ยวข้องกับการกำกับดูแลความเสี่ยงด้าน IT	
ส่วนที่ 2 การกำกับดูแลและบริหารจัดการความเสี่ยงด้าน IT ในระดับองค์กร 2.2 สำนักงานสอบบัญชีควรจัดให้มีนโยบายที่เกี่ยวข้องกับการกำกับดูแลความเสี่ยงด้าน IT เป็นลายลักษณ์อักษร โดยได้รับความเห็นชอบจากหัวหน้าสำนักงานสอบบัญชี หรือคณะกรรมการบริหารของสำนักงานสอบบัญชี หรือคณะกรรมการที่ได้รับมอบหมายจากหัวหน้าสำนักงานสอบบัญชี ดังนี้	
2.2.1 <u>นโยบายการบริหารจัดการความเสี่ยงด้าน IT (IT risk management policy)</u> โดยควรครอบคลุมเนื้อหาอย่างน้อยในเรื่องดังต่อไปนี้ (1) บทบาทหน้าที่ของผู้ที่เกี่ยวข้องในการบริหาร	กระบวนการบริหารจัดการความเสี่ยงด้าน IT ควรมีรายละเอียดและจัดทำเป็นลายลักษณ์อักษร ดังนี้ 1. เกณฑ์ความเสี่ยง (risk criteria) โดยควรครอบคลุมเนื้อหาอย่างน้อยในเรื่องโอกาสหรือความถี่ที่จะเกิดเหตุการณ์ความเสี่ยงและความมีนัยสำคัญหรือผลกระทบที่จะเกิดขึ้นเพื่อจัดลำดับความสำคัญในการบริหารจัดการความเสี่ยง

ข้อกำหนด	แนวปฏิบัติ
จัดการความเสี่ยงด้าน IT (2) การจัดให้มีกระบวนการบริหารจัดการความเสี่ยงด้าน IT เพื่อให้อยู่ในระดับที่องค์กรยอมรับได้	2. ระดับความเสี่ยงที่ยอมรับได้ (IT risk appetite) ควรผ่านการพิจารณาโดยคณะกรรมการบริหารความเสี่ยง (ถ้ามี) และควรได้รับการอนุมัติจากหัวหน้าสำนักงานสอบบัญชี หรือคณะกรรมการบริหารของสำนักงานสอบบัญชี ทั้งนี้ ระดับความเสี่ยงที่ยอมรับได้ควรสอดคล้องกับการบริหารและจัดการความเสี่ยงขององค์กร (enterprise risk management) 3. การประเมินความเสี่ยง (risk assessment) ควรมีการประเมินความเสี่ยงอย่างน้อยปีละ 1 ครั้ง และเมื่อมีการเปลี่ยนแปลงระบบงาน IT อย่างมีนัยสำคัญ โดยควรครอบคลุมเนื้อหาอย่างน้อยในเรื่องดังต่อไปนี้ (1) การระบุความเสี่ยง (risk identification) ควรจัดให้มีการระบุเหตุการณ์ความเสี่ยง (risk scenario) ด้าน IT ที่อาจจะเกิดขึ้นหรือที่เคยเกิดขึ้นจริงกับสำนักงานสอบบัญชีเอง หรือเกิดกับผู้อื่นที่ใช้งานเทคโนโลยีในลักษณะเดียวกัน รวมถึงภัยคุกคามทางไซเบอร์และช่องโหว่ต่าง ๆ ที่ส่งผลกระทบต่อการดำเนินธุรกิจ โดยเหตุการณ์ความเสี่ยงดังกล่าวอาจมีสาเหตุมาจากปัจจัยภายใน (internal factor) เช่น มีการเปลี่ยนแปลงกระบวนการปฏิบัติงาน ระบบงาน บุคลากร เป็นต้น รวมถึงปัจจัยภายนอกอื่น ๆ (external factor) เช่น การปฏิบัติตามกฎหมาย การใช้บริการ การเชื่อมต่อ หรือการเข้าถึงข้อมูลจากบุคคลภายนอก เป็นต้น รวมถึงควรนำข้อสังเกตที่ได้จากการตรวจสอบรอบก่อน โดยผู้ตรวจสอบด้านเทคโนโลยีสารสนเทศที่มีคุณสมบัติ ตามหมวดที่ 3 ข้อที่ 1 มาประกอบการพิจารณาในการระบุความเสี่ยงด้วย (2) การวิเคราะห์ความเสี่ยง (risk analysis) ควรจัดให้มีการวิเคราะห์ความเสี่ยงด้าน IT เพื่อหาแนวทางในการจัดการความเสี่ยงอย่างเหมาะสม โดยควรครอบคลุมเนื้อหาอย่างน้อยในเรื่องดังต่อไปนี้ (2.1) กำหนดผู้รับผิดชอบต่อความเสี่ยง หรือเจ้าของความเสี่ยง (risk owner) (2.2) ระบุการควบคุมที่มีอยู่ในปัจจุบัน (existing control) (2.3) วิเคราะห์โอกาสหรือความถี่ที่จะเกิดเหตุการณ์ความเสี่ยง (likelihood) และความมีนัยสำคัญหรือผลกระทบที่จะเกิดขึ้น (potential impact) จากเหตุการณ์ดังกล่าว (3) การประเมินค่าความเสี่ยง (risk evaluation) ควรจัดให้มีการประเมินค่าความเสี่ยงด้าน IT เพื่อจัดลำดับในการบริหารความเสี่ยงอย่างเหมาะสม โดยควรครอบคลุมเนื้อหาอย่างน้อยในเรื่องดังต่อไปนี้ (3.1) การประเมินผลลัพธ์ที่ได้จากการวิเคราะห์ความเสี่ยง ได้แก่ ค่าโอกาสและผลกระทบ (likelihood และ potential impact) กับเกณฑ์ความเสี่ยง (risk criteria) ที่กำหนดไว้ เพื่อระบุระดับค่าความเสี่ยงของแต่ละ

ข้อกำหนด	แนวปฏิบัติ
	เหตุการณ์ความเสี่ยงด้าน IT (3.2) การจัดลำดับความเสี่ยงด้าน IT 4. การจัดการความเสี่ยง (risk treatment) ควรจัดให้มีแนวทางในการจัดการความเสี่ยงด้าน IT อย่างเหมาะสมและสอดคล้องกับผลการประเมินความเสี่ยง (risk assessment) เพื่อให้ความเสี่ยงที่เหลืออยู่ (residual risk) อยู่ในระดับความเสี่ยงที่ยอมรับได้ (risk appetite) โดยควรครอบคลุมเนื้อหาอย่างน้อยในเรื่องดังต่อไปนี้ (1) การกำหนดแนวทางในการจัดการความเสี่ยง โดยควรพิจารณาถึงความคุ้มค่าและวิธีการที่เหมาะสมกับสำนักงานสอบบัญชี 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 5. การจัดทำทะเบียนความเสี่ยง (risk register) ควรจัดให้มีทะเบียนความเสี่ยง (risk register) เพื่อบันทึกผลการประเมินความเสี่ยง และแนวทางในการจัดการความเสี่ยง โดยมีตัวอย่างรายละเอียด ดังนี้ (1) วันที่ประเมินความเสี่ยง (2) รายละเอียดเหตุการณ์ความเสี่ยง (3) โอกาสหรือความถี่ที่จะเกิดเหตุการณ์ความเสี่ยง (likelihood) (4) ความมีนัยสำคัญหรือผลกระทบที่จะเกิดขึ้น (potential impact) (5) ระดับค่าความเสี่ยงก่อนการควบคุม (inherent risk) (6) แนวทางจัดการความเสี่ยง (risk treatment) (7) เจ้าของความเสี่ยง (risk owner)

ข้อกำหนด	แนวปฏิบัติ
	(8) ระดับความเสี่ยงที่เหลืออยู่ (residual risk) (9) สถานะของการจัดการความเสี่ยง (status of risk treatment) 6. การติดตามและทบทวนความเสี่ยง (risk monitoring and review) ควรจัดให้มีกระบวนการติดตามและทบทวนความเสี่ยงด้าน IT โดยควรครอบคลุมการดำเนินการอย่างน้อยในเรื่องดังต่อไปนี้ (1) การกำหนดผู้รับผิดชอบในการติดตามและทบทวนความเสี่ยง (2) การกำหนดดัชนีชี้วัดความเสี่ยงด้าน IT ที่สำคัญ (IT key risk indicator) เพื่อให้สามารถติดตามแนวโน้มของความเสี่ยง และสามารถทบทวนมาตรการควบคุมความเสี่ยงได้อย่างมีประสิทธิภาพ (3) การติดตามความคืบหน้าของการดำเนินงานตามแผนการบริหารจัดการความเสี่ยงด้าน IT 7. การรายงานความเสี่ยง (risk reporting) ควรจัดให้มีการรายงานความเสี่ยง และผลการบริหารจัดการความเสี่ยงด้าน IT ต่อหัวหน้าสำนักงานสอบบัญชี หรือคณะกรรมการบริหารของสำนักงานสอบบัญชีอย่างน้อยปีละ 1 ครั้ง โดยควรครอบคลุมเนื้อหาอย่างน้อยในเรื่องดังต่อไปนี้ (1) ผลการประเมินและจัดการความเสี่ยงด้าน IT (2) แนวโน้มความเสี่ยงด้าน IT ที่อาจมีผลกระทบกับสำนักงานสอบบัญชี (3) ความคืบหน้าของการดำเนินงานตามแผนการบริหารจัดการความเสี่ยงด้าน IT
2.2.2 <u>นโยบายการรักษาความมั่นคงปลอดภัยด้าน IT (IT security policy)</u> ควรครอบคลุมเนื้อหาอย่างน้อยในเรื่องดังต่อไปนี้ (1) โครงสร้างการบริหารงานเพื่อการรักษาความมั่นคงปลอดภัยด้าน IT (2) การบริหารจัดการบุคลากร และบุคคลภายนอก (3) การบริหารจัดการทรัพย์สินด้าน IT (4) การรักษาความมั่นคงปลอดภัยของข้อมูล (5) การควบคุมการเข้าถึงข้อมูลและระบบงาน IT (6) การควบคุมการเข้ารหัส (Cryptographic Control)	[ไม่มีการกำหนดแนวปฏิบัติไว้เป็นการเฉพาะ]

ข้อกำหนด	แนวปฏิบัติ
(7) การรักษาความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อม (8) การรักษาความมั่นคงปลอดภัยในการปฏิบัติงานด้าน IT (9) การรักษาความมั่นคงปลอดภัยเกี่ยวกับระบบเครือข่ายสื่อสาร (10) การบริหารจัดการโครงการด้าน IT และการจัดหาพัฒนา และบำรุงรักษาระบบงาน IT (11) การบริหารจัดการเหตุการณ์ผิดปกติด้าน IT (12) แผนฉุกเฉินด้าน IT	
2.3 สำนักงานสอบบัญชีควรจัดให้มีการดำเนินการตามนโยบายในข้อ 2.2 ดังนี้ 2.3.1 ควรสื่อสารนโยบายตามข้อ 2.2 ให้แก่บุคลากรของสำนักงานสอบบัญชีและบุคคลภายนอกที่เกี่ยวข้องรับทราบตามบทบาทหน้าที่ ความรับผิดชอบ และสิทธิการเข้าถึงข้อมูล ในลักษณะที่สามารถเข้าถึงได้ง่าย เพื่อให้บุคคลที่เกี่ยวข้องดังกล่าวเข้าใจและสามารถปฏิบัติตามนโยบายได้อย่างถูกต้อง	1. ในการสื่อสารนโยบายให้กับบุคคลภายนอกที่เกี่ยวข้อง สำนักงานสอบบัญชีควรมีการพิจารณาถึงรายละเอียดที่บุคคลภายนอกควรรู้เพื่อให้สามารถปฏิบัติงานได้สอดคล้องกับนโยบายของสำนักงานสอบบัญชี โดยควรคำนึงถึงความลับของข้อมูลด้วย
2.3.2 ควรกำหนดขั้นตอนและวิธีปฏิบัติงานให้เป็นไปตามนโยบายตามข้อ 2.2	1. สำนักงานสอบบัญชีควรกำหนดขั้นตอนการปฏิบัติงานที่เกี่ยวข้องกับระบบงาน IT เป็นลายลักษณ์อักษร เพื่อให้เจ้าหน้าที่ผู้ปฏิบัติงานด้าน IT สามารถปฏิบัติงานได้อย่างถูกต้องและเป็นไปตามนโยบายที่เกี่ยวข้องกับการกำกับดูแลความเสี่ยงด้าน IT 2. สำนักงานสอบบัญชีควรกำหนดวิธีปฏิบัติสำหรับการอนุมัติยกเว้น (exception) กรณีที่มีความจำเป็นให้ไม่สามารถปฏิบัติตามขั้นตอนและวิธีปฏิบัติงานที่สำนักงานสอบบัญชีกำหนดไว้ สำนักงานสอบบัญชีควรจัดให้มีการประเมินความเสี่ยง ควบคุมความเสี่ยงอย่างเพียงพอเหมาะสม และขออนุมัติยกเว้นจากผู้มีอำนาจก่อนดำเนินการต่อไป พร้อมนี้ ควรจัดเก็บหลักฐานการอนุมัติยกเว้นดังกล่าวอย่างเป็นลายลักษณ์อักษร 3. สำนักงานสอบบัญชีควรจัดให้มีการสอบทานความเหมาะสมของรายการขออนุมัติยกเว้น ตลอดจนแนวทางการควบคุมความเสี่ยงอย่างน้อยปีละ 1 ครั้ง เพื่อทบทวนแนวทางการดำเนินการให้มีความเหมาะสมต่อความเสี่ยงที่อาจมีการเปลี่ยนแปลงไปตามสภาพแวดล้อมการประกอบธุรกิจและการใช้งานเทคโนโลยีสารสนเทศในการประกอบธุรกิจ

ข้อกำหนด	แนวปฏิบัติ
2.3.3 ในกรณีที่มีการเปลี่ยนแปลงนโยบายตามข้อ 2.2 ควรมีการสื่อสารให้บุคคลที่เกี่ยวข้องได้รับทราบอย่างทั่วถึง และปรับปรุงขั้นตอนและวิธีปฏิบัติงานให้สอดคล้องกับการเปลี่ยนแปลงดังกล่าว	[ไม่มีการกำหนดแนวปฏิบัติไว้เป็นการเฉพาะ]
2.4 สำนักงานสอบบัญชีควรทบทวนหรือปรับปรุงนโยบายตามข้อ 2.2 อย่างน้อยปีละ 1 ครั้ง และโดยไม่ชักช้าเมื่อมีเหตุการณ์ใด ๆ ซึ่งอาจส่งผลกระทบต่อการกำกับดูแลและบริหารจัดการความเสี่ยงด้าน IT อย่างมีนัยสำคัญ	[ไม่มีการกำหนดแนวปฏิบัติไว้เป็นการเฉพาะ]

หมวดที่ 2 การรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (Information Technology Security)

ข้อกำหนด	แนวปฏิบัติ
2.1 โครงสร้างการบริหารงานเพื่อการรักษาความมั่นคงปลอดภัยด้าน IT (organization of information technology security)	
ส่วนที่ 1 โครงสร้างการบริหารงานเพื่อการรักษาความมั่นคงปลอดภัยด้าน IT (organization of information technology security) สำนักงานสอบบัญชีควรดำเนินการจัดให้มีโครงสร้างดังกล่าว โดยควรมีลักษณะอย่างน้อยดังนี้	
1.1 ควรมีการกำหนดโครงสร้างภายในองค์กร (organizational structure) ในการปฏิบัติงานด้าน IT โดยมีรายละเอียดหน้าที่และความรับผิดชอบของบุคลากรเป็นลายลักษณ์อักษร	1. สำหรับสำนักงานสอบบัญชีที่ไม่ได้จัดตั้งหน่วยงานที่ปฏิบัติงานด้าน IT ภายใน แต่มีการว่าจ้างบุคลากรภายนอกมาปฏิบัติงานด้าน IT ให้กับสำนักงานสอบบัญชีหรือบุคลากรที่ปฏิบัติงานด้าน IT เป็นพนักงานของสำนักงานสอบบัญชีเครือข่าย โครงสร้างภายในองค์กรในการปฏิบัติงานด้าน IT อย่างน้อยควรระบุหน้าที่และความรับผิดชอบของบุคลากรที่ทำหน้าที่กำกับดูแลและสอบทานการปฏิบัติงานของบุคลากรภายนอกหรือพนักงานของสำนักงานสอบบัญชีเครือข่ายที่มาปฏิบัติงานด้าน IT
1.2 ควรมีการสอบทานการปฏิบัติงานเพื่อป้องกันความเสี่ยงในการรักษาความมั่นคงปลอดภัยของระบบงาน IT ที่อาจเกิดขึ้นในการปฏิบัติงาน	1. สำนักงานสอบบัญชีควรจัดให้มีการแบ่งแยกหน้าที่ในการปฏิบัติงานด้านต่าง ๆ ที่เกี่ยวกับความมั่นคงปลอดภัยของระบบงาน IT อย่างชัดเจนเพื่อให้มีการสอบทานการปฏิบัติงานระหว่างกัน เพื่อลดข้อผิดพลาดในการปฏิบัติงานและลดโอกาสการกระทำผิด เช่น แบ่งแยกผู้พัฒนาระบบงาน (developer) ออกจากผู้มีสิทธิในการนำระบบขึ้นใช้งานจริง เป็นต้น ทั้งนี้ กรณีที่ไม่สามารถแบ่งแยกหน้าที่ความรับผิดชอบได้เนื่องจากข้อจำกัดทางด้านขนาดของธุรกิจหรือบุคลากร สำนักงานสอบบัญชีควรจัดให้มีมาตรการควบคุมทดแทน เช่น การจัดให้มีกระบวนการติดตามและตรวจสอบการปฏิบัติงานของบุคลากรที่เกี่ยวข้องอย่างใกล้ชิดและสม่ำเสมอ หรือ ทุก ๆ การเปลี่ยนแปลงทางด้าน IT ควรได้รับความเห็นชอบจากผู้มีอำนาจ เป็นต้น
2.2 การบริหารจัดการบุคลากร และบุคคลภายนอก	
ส่วนที่ 2 การบริหารจัดการบุคลากร และบุคคลภายนอก	
2.2.1 การบริหารจัดการบุคลากร	
<u>บุคลากรที่ควรบริหารจัดการ</u> 2.1 บุคลากรที่เกี่ยวข้องหรือที่ใช้ระบบงาน IT ปฏิบัติงาน	

ข้อกำหนด	แนวปฏิบัติ
<u>การบริหารจัดการ</u> สำนักงานสอบบัญชีควรบริหารจัดการบุคลากรตามข้อ 2.1 อย่างเหมาะสม โดยควรดำเนินการอย่างน้อยดังนี้ (1) ควรมีกระบวนการคัดเลือกบุคลากรในการปฏิบัติหน้าที่ดังนี้ (1.1) ควรคำนึงถึงความรู้ ความสามารถ และความเพียงพอในการปฏิบัติงาน (1.2) ควรมีการตรวจสอบข้อมูลของบุคลากรก่อนการว่าจ้างอย่างเพียงพอและสอดคล้องกับความเสี่ยงของตำแหน่งงานและหน้าที่ความรับผิดชอบ	[ไม่มีการกำหนดแนวปฏิบัติไว้เป็นการเฉพาะ]
(2) ควรมีข้อกำหนดให้บุคลากรทำความเข้าใจ รับทราบ และลงนามยอมรับในเรื่องดังนี้ (2.1) บทบาทหน้าที่และความรับผิดชอบของบุคลากรดังกล่าวเกี่ยวกับการรักษาความมั่นคงปลอดภัยด้าน IT (2.2) ข้อตกลงการไม่เปิดเผยข้อมูล (non-disclosure agreement)	1. สำนักงานสอบบัญชีควรกำหนดให้บุคลากรที่ได้รับการว่าจ้างทำความเข้าใจ รับทราบ และลงนามยอมรับเงื่อนไขการว่าจ้างงานหรือระเบียบข้อบังคับภายในองค์กร นโยบายการรักษาความมั่นคงปลอดภัยด้าน IT และข้อตกลงการไม่เปิดเผยข้อมูล (non-disclosure agreement) ก่อนเริ่มปฏิบัติงาน 2. ข้อตกลงการไม่เปิดเผยข้อมูล non-disclosure agreement ควรครอบคลุมเนื้อหาอย่างน้อยในเรื่องดังต่อไปนี้ (1) ความเป็นเจ้าของข้อมูลสำคัญทางธุรกิจ ทรัพย์สินทางปัญญา และการป้องกันการรั่วไหลของข้อมูล (2) ความรับผิดชอบในการเก็บรักษาความลับ และไม่เปิดเผยข้อมูลโดยไม่ได้รับอนุญาต (3) การแจ้งเตือนและรายงานผู้เกี่ยวข้องหากพบการรั่วไหลหรือเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต (4) การดำเนินการกรณีละเมิดหรือยกเลิกข้อตกลง รวมทั้งข้อกำหนดในการคืนหรือทำลายข้อมูลที่มีความสำคัญเมื่อสิ้นสุดข้อตกลง
(3) ควรสร้างความตระหนักรู้ถึงความเสี่ยงด้าน IT ให้แก่บุคลากรที่ปฏิบัติงาน ซึ่งสามารถเข้าถึงข้อมูลหรือระบบงานภายในองค์กร เพื่อให้บุคลากรดังกล่าวสามารถใช้งานระบบงาน IT ได้อย่างปลอดภัย	1. สำนักงานสอบบัญชีควรส่งเสริมและพัฒนาความรู้ด้าน IT ให้แก่บุคลากรอย่างสม่ำเสมอ เช่น การจัดการอบรมภายในองค์กร หรือส่งบุคลากรเข้าร่วมฝึกอบรมภายนอกองค์กร เป็นต้น เพื่อให้บุคลากรมีความรู้ความเข้าใจถึงการใช้งาน IT ที่ถูกต้องปลอดภัย และลดความเสี่ยงที่อาจเกิดขึ้นจากการใช้งาน IT โดยมีเนื้อหา เช่น (1) การรักษาความมั่นคงปลอดภัยด้าน IT (2) ความเสี่ยงด้าน IT และภัยคุกคามทางไซเบอร์ (3) หลักเกณฑ์และกฎหมายที่เกี่ยวข้องกับ IT เป็นต้น

ข้อกำหนด	แนวปฏิบัติ
	2. สำนักงานสอบบัญชีควรทบทวนแผนการส่งเสริมและพัฒนาความรู้ด้าน IT (training program) อย่างน้อยปีละ 1 ครั้ง เพื่อให้มั่นใจว่าเนื้อหาและรายละเอียดของแผนงานที่เกี่ยวข้องยังคงเพียงพอเหมาะสมกับแนวโน้มความเสี่ยงด้าน IT ในปัจจุบัน 3. สำนักงานสอบบัญชีควรจัดให้มีการเสริมสร้างความตระหนักเรื่องการรักษาความมั่นคงปลอดภัยด้าน IT และความเสี่ยงด้าน IT อย่างสม่ำเสมอ ให้แก่บุคลากร (user) ที่สามารถเข้าถึงข้อมูลที่มีความสำคัญของสำนักงานสอบบัญชีหรือข้อมูลของลูกค้า เช่น การทดสอบเรื่องอีเมลหลอกลวง (phishing) การทดสอบเรื่องวิศวกรรมสังคม (social engineering) และการซักซ้อมแผนเพื่อเตรียมความพร้อมรับมือกับการโจมตีทางไซเบอร์ เป็นต้น
(4) ควรกำหนดให้บุคลากรงดเว้นการใช้งานระบบงาน IT ในลักษณะที่อาจก่อให้เกิดความเสียหายแก่สำนักงานสอบบัญชี หรือที่เป็นการกระทำผิดกฎหมาย หรือไม่เป็นไปตามข้อกำหนดและจรรยาบรรณที่สำนักงานสอบบัญชีกำหนดไว้	1. สำนักงานสอบบัญชีควรจัดให้มีนโยบายการใช้งาน IT ที่ยอมรับได้ (acceptable use policy) โดยควรครอบคลุมเนื้อหาอย่างน้อยในเรื่องขอบเขตความรับผิดชอบของผู้ใช้งาน IT สิ่งที่ผู้ใช้งานพึงปฏิบัติ และสิ่งที่ผู้ใช้งานห้ามปฏิบัติ 2. สำนักงานสอบบัญชีควรสื่อสารนโยบายการใช้งาน IT ที่ยอมรับได้ (acceptable use policy) ให้ผู้ใช้งานรับทราบ และลงนามยอมรับนโยบายดังกล่าว
(5) ควรกำหนดมาตรการในการลงโทษบุคลากรที่มีพฤติกรรมฝ่าฝืนหรือไม่ปฏิบัติตามนโยบายและมาตรการรักษาความมั่นคงปลอดภัยในการปฏิบัติงานด้าน IT	[ไม่มีการกำหนดแนวปฏิบัติไว้เป็นการเฉพาะ]
(6) ควรกำหนดขั้นตอนปฏิบัติเมื่อสิ้นสุดการจ้างงาน หรือเมื่อมีการเปลี่ยนแปลงตำแหน่งงาน เพื่อป้องกันการละเมิดหรือความเสียหายที่อาจเกิดขึ้นต่อทรัพย์สินด้าน IT	1. สำนักงานสอบบัญชีควรจัดให้มีกระบวนการรองรับเมื่อมีการเปลี่ยนแปลงตำแหน่งงาน และสิ้นสุดการจ้างงาน เช่น การคืนทรัพย์สินขององค์กร การปรับปรุงสิทธิให้เป็นปัจจุบัน การยกเลิกสิทธิเมื่อหมดหน้าที่และความรับผิดชอบ เป็นต้น รวมทั้งควรมีการสื่อสารให้ผู้ที่เกี่ยวข้องรับทราบถึงการเปลี่ยนแปลงสิทธิ หน้าที่ และความรับผิดชอบ
2.2.2 การบริหารจัดการบุคคลภายนอก (third-party management)	
<u>บุคลากรที่ควรบริหารจัดการ</u> 2.2 บุคคลภายนอก ควรรวมถึงพนักงานของสำนักงานสอบบัญชีเครือข่ายหรือบริษัทในเครือของสำนักงานสอบบัญชีในกรณีที่สำนักงานสอบบัญชีมีการดำเนินการอย่างใดอย่างหนึ่งดังนี้ ● ใช้บริการงานด้าน IT จากบุคคลภายนอก	

ข้อกำหนด	แนวปฏิบัติ
• เชื่อมต่อระบบงาน IT กับบุคคลภายนอก • อนุญาตให้บุคคลภายนอกสามารถเข้าถึงข้อมูลสำคัญหรือข้อมูลของลูกค้าของสำนักงานสอบบัญชีได้	
<u>การบริหารจัดการ</u> สำนักงานสอบบัญชีควรบริหารจัดการบุคคลภายนอกตามข้อ 2.2 ดังนี้ (1) ควรประเมินความเสี่ยงจากการใช้บริการการเชื่อมต่อหรือการเข้าถึงข้อมูลจากบุคคลภายนอก รวมถึงผู้รับดำเนินการช่วง (subcontract) จากบุคคลภายนอก	1. สำนักงานสอบบัญชีควรประเมินความเสี่ยงและผลกระทบในเรื่องดังต่อไปนี้ก่อน • การใช้บริการงานด้าน IT จากบุคคลภายนอก • การเชื่อมต่อระบบงาน IT กับบุคคลภายนอก • การอนุญาตให้บุคคลภายนอกสามารถเข้าถึงข้อมูลสำคัญหรือข้อมูลของลูกค้าที่ควบคุมดูแลโดยสำนักงานสอบบัญชีได้ โดยควรคำนึงถึงความเสี่ยง ดังนี้ (1) ความเสี่ยงด้านกฎหมาย และกฎเกณฑ์ที่เกี่ยวข้องทั้งในประเทศและต่างประเทศ เช่น กฎหมายเกี่ยวกับการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ กฎหมายเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล กฎหมายเกี่ยวกับธุรกรรมทางอิเล็กทรอนิกส์ และ The EU General Data Protection Regulation (GDPR) เป็นต้น (2) ความเสี่ยงจากการกำกับดูแลและบริหารจัดการบุคคลภายนอกที่ไม่รัดกุมเพียงพอ เช่น การไม่สามารถตรวจสอบการดำเนินงานของบุคคลภายนอกได้ด้วยตนเอง เป็นต้น (3) ความเสี่ยงจากการพึ่งพาบุคคลภายนอกรายใดรายหนึ่งเป็นหลัก (third party/vendor locked-in) ซึ่งทำให้มีข้อจำกัดในการเปลี่ยนแปลงเทคโนโลยี ผู้ให้บริการ หรือข้อจำกัดในการนำระบบหรือข้อมูลกลับมาดำเนินการเอง (4) ความเสี่ยงด้าน IT และภัยทางไซเบอร์ เช่น ระบบที่ให้บริการโดยบุคคลภายนอกเกิดขัดข้อง ระบบของบุคคลภายนอกมีช่องโหว่ทำให้ข้อมูลเกิดการสูญหายหรือรั่วไหล เป็นต้น (5) ความเสี่ยงกรณีบุคคลภายนอกให้ผู้อื่นดำเนินการแทน (sub-contracting) เช่น subcontractor ปฏิบัติงานบกพร่อง เป็นต้น 2. สำนักงานสอบบัญชีควรจัดให้มีการกำหนดระดับความมีนัยสำคัญของบุคคลภายนอกแต่ละราย
(2) ควรกำหนดวิธีปฏิบัติและหลักเกณฑ์ในการคัดเลือกบุคคลภายนอก	1. สำนักงานสอบบัญชีควรกำหนดกระบวนการและหลักเกณฑ์ในการคัดเลือกบุคคลภายนอกอย่างชัดเจน และเป็นลายลักษณ์อักษร เพื่อให้มั่นใจว่าผู้ให้บริการภายนอกจะสามารถให้บริการได้ตรงตามความต้องการของสำนักงานสอบบัญชี ทั้งนี้ ในการตัดสินใจใช้บริการการเชื่อมต่อ หรือการเข้าถึงข้อมูลจากบุคคลภายนอก ที่มีความเสี่ยงหรือมีนัยสำคัญได้รับความเห็นชอบจากหัวหน้าสำนักงานสอบบัญชี หรือคณะกรรมการบริหารของสำนักงานสอบบัญชีที่ได้รับมอบหมาย

ข้อกำหนด	แนวปฏิบัติ
	2. สำนักงานสอบบัญชีควรประเมินศักยภาพบุคคลภายนอก (due diligence) ให้สอดคล้องกับระดับความเสี่ยง และความมีนัยสำคัญของบุคคลภายนอก โดยควรคำนึงถึงเรื่องดังต่อไปนี้ (1) ฐานะทางการเงิน ชื่อเสียง ความรู้ความเชี่ยวชาญ ประสบการณ์ และความสามารถในการให้บริการในช่วงที่ผ่านมา (2) การบริหารจัดการความเสี่ยง การควบคุมภายใน การตรวจสอบภายใน และการติดตามผลการปฏิบัติงาน (3) การรักษาความมั่นคงปลอดภัยด้าน IT (4) การบริหารจัดการความต่อเนื่องทางธุรกิจ และความพร้อมรับมือภัยหรือเหตุการณ์ต่าง ๆ (5) การปฏิบัติตามกฎหมายและกฎเกณฑ์ที่เกี่ยวข้อง เช่น การขอตรวจสอบเอกสารหลักฐานหรือใบรับรองจากบุคคลภายนอกในการดำเนินการตามกฎหมายและกฎเกณฑ์ที่เกี่ยวข้อง หรือการตรวจสอบประวัติด้านการกระทำความผิด เป็นต้น (6) การปฏิบัติตามมาตรฐานสากลด้าน IT เช่น การตรวจสอบเอกสารหลักฐานการได้รับการรองรับตามมาตรฐาน ISO/IEC 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) สำนักงานสอบบัญชีควรมีการพิจารณารายละเอียดด้านความมั่นคงปลอดภัยสารสนเทศของบุคคลดังกล่าวด้วย
(3) ควรกำหนดบทบาท หน้าที่ และความรับผิดชอบของสำนักงานสอบบัญชีและบุคคลภายนอกอย่างชัดเจนและเป็นลายลักษณ์อักษร	1. สำนักงานสอบบัญชีควรจัดทำสัญญาหรือข้อตกลงการใช้บริการ การเชื่อมต่อ หรือการเข้าถึงข้อมูลจากบุคคลภายนอกอย่างเป็นลายลักษณ์อักษร โดยควรมีการลงนามร่วมกันระหว่างสำนักงานสอบบัญชีและบุคคลภายนอก เพื่อให้มั่นใจได้ว่าบุคคลภายนอกมีหน้าที่รับผิดชอบในการรักษาความมั่นคงปลอดภัยของระบบงาน IT ในระดับที่เหมาะสม โดยควรมีรายละเอียดสอดคล้องกับความเสี่ยง และความมีนัยสำคัญของบุคคลภายนอก ดังนี้ (1) ขอบเขตการให้บริการ การเชื่อมต่อ และการเข้าถึงข้อมูลจากบุคคลภายนอก (2) บทบาท หน้าที่ และความรับผิดชอบของบุคคลภายนอกและสำนักงานสอบบัญชี (3) มาตรฐานขั้นต่ำในการปฏิบัติงานของบุคคลภายนอก เช่น การรักษาความปลอดภัยของระบบงาน IT การรักษาความลับของข้อมูล และการไม่นำข้อมูลไปใช้นอกเหนือจากที่ระบุไว้ในสัญญาหรือข้อตกลงการให้บริการ เป็นต้น (4) ข้อตกลงระดับการให้บริการด้าน IT (service level agreement: SLA) สำหรับการใช้บริการจากบุคคลภายนอก

ข้อกำหนด	แนวปฏิบัติ
	(5) การติดตามและรายงานผลการปฏิบัติงานของบุคคลภายนอก โดยควรครอบคลุมเนื้อหาอย่างน้อยในเรื่องการแจ้งการเปลี่ยนแปลงหรือปัญหาที่สำคัญ และการรายงานเหตุการณ์ผิดปกติอย่างทันการณ์ (6) รายชื่อ และช่องทางการติดต่อในกรณีเกิดปัญหาเกี่ยวกับการรักษาความมั่นคงปลอดภัยของระบบงาน IT (7) การทำลายข้อมูลเมื่อสิ้นสุดหรือยกเลิกการใช้บริการ การเชื่อมต่อ และการเข้าถึงข้อมูลจากบุคคลภายนอก (8) เงื่อนไขหรือสิทธิของสำนักงานสอบบัญชีในการเปลี่ยนแปลง ยุติ หรือยกเลิกสัญญาหรือข้อตกลงกับบุคคลภายนอก เช่น กรณีที่บุคคลภายนอกมีการละเมิดสัญญาหรือข้อตกลง เป็นต้น (9) การจัดให้มีแผนฉุกเฉินด้าน IT (IT contingency plan) ที่สอดคล้องกับแผนฉุกเฉินด้าน IT ของสำนักงานสอบบัญชี (10) ความรับผิดชอบต่อความเสียหายที่เกิดจากบุคคลภายนอก เช่น กรณีการให้บริการไม่เป็นไปตาม SLA ที่กำหนดไว้ เป็นต้น อย่างไรก็ดี หากมีข้อจำกัดในการระบุรายละเอียดและกำหนดเงื่อนไขที่สำคัญลงในข้อตกลงหรือสัญญาที่ทำกับบุคคลภายนอก สำนักงานสอบบัญชีควรมีการประเมินความเสี่ยงและพิจารณาแนวทางควบคุมความเสี่ยงที่เพียงพอเหมาะสม พร้อมทั้งขออนุมัติยกเว้น (exception) จากผู้มีอำนาจ
(4) กรณีบุคคลภายนอกซึ่งเป็นผู้ให้บริการงานด้าน IT รายที่มีนัยสำคัญตามผลการประเมินความเสี่ยงในหมวดที่ 2 ส่วนที่ 2.2 ข้อ 2.2 (1) ข้อตกลงหรือสัญญาการให้บริการควรระบุสิทธิให้สำนักงานสอบบัญชีและผู้ตรวจสอบที่ได้รับการแต่งตั้งจากสำนักงานสอบบัญชี สามารถเข้าตรวจสอบการดำเนินงานและการควบคุมภายในของบุคคลภายนอกดังกล่าวได้ หากมีเหตุจำเป็นทำให้สำนักงานสอบบัญชีไม่สามารถระบุสิทธิในการเข้าตรวจสอบตามวรรคหนึ่งไว้ในข้อตกลงหรือสัญญา สำนักงานสอบบัญชีควรมีมาตรการประเมินหรือติดตามการดำเนินงานและการควบคุมภายในของบุคคลภายนอกให้รัดกุมเพียงพอและสอดคล้องกับความเสี่ยงและความมีนัยสำคัญของการใช้บริการ การเชื่อมต่อ หรือการเข้าถึงข้อมูล	1. สำนักงานสอบบัญชีควรกำหนดสิทธิให้สำนักงานสอบบัญชี และผู้ตรวจสอบที่ได้รับการแต่งตั้งจากสำนักงานสอบบัญชี สามารถเข้าตรวจสอบการดำเนินงานด้าน IT และการควบคุมภายในของบุคคลภายนอกที่ให้บริการงานด้าน IT รายที่มีนัยสำคัญ โดยระบุไว้เป็นส่วนหนึ่งของข้อตกลงหรือสัญญาการให้บริการ ในกรณีที่ไม่สามารถระบุสิทธิดังกล่าวได้ สำนักงานสอบบัญชีควรพิจารณาเลือกใช้บุคคลภายนอกที่มีการดำเนินการตรวจสอบด้าน IT โดยผู้ตรวจสอบภายนอกที่มีความเป็นอิสระและได้มาตรฐานสากล เช่น ผลการตรวจสอบตามมาตรฐาน SSAE 18 (SOC 2 Type 2 Report : ความสามารถในการรักษาข้อมูลที่ sensitive สำหรับ cloud-based service provider) เป็นต้น นอกจากนี้ สำนักงานสอบบัญชีควรพิจารณารายละเอียดของผลการตรวจสอบที่จัดทำโดยผู้ตรวจสอบภายนอกอย่างเหมาะสม

ข้อกำหนด	แนวปฏิบัติ
(5) ควรมี non-disclosure agreement สำหรับบุคคลภายนอกหรือผู้รับดำเนินการช่วงของบุคคลภายนอก ในกรณีที่บุคคลดังกล่าวสามารถเข้าถึงข้อมูลสำคัญของสำนักงานสอบบัญชีหรือข้อมูลของลูกค้า	1. non-disclosure agreement ควรครอบคลุมเนื้อหาอย่างน้อยในเรื่องขอบเขตความรับผิดชอบในการเก็บรักษาความลับ การไม่เปิดเผยข้อมูลโดยไม่ได้รับอนุญาต การรายงานสำนักงานสอบบัญชีเมื่อพบการรั่วไหลหรือเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต และการทำลายข้อมูลที่มีความสำคัญเมื่อสิ้นสุดข้อตกลงหรือสัญญา
(6) ควรกำกับดูแล ติดตาม และบริหารจัดการความเสี่ยงจากการใช้บริการ การเชื่อมต่อ หรือการเข้าถึงข้อมูลจากบุคคลภายนอกให้สอดคล้องกับระดับความเสี่ยงและระดับความมีนัยสำคัญของบุคคลภายนอก	1. สำนักงานสอบบัญชีควรกำกับดูแล ติดตาม และบริหารจัดการความเสี่ยงจากการใช้บริการ การเชื่อมต่อ หรือการเข้าถึงข้อมูลจากบุคคลภายนอกให้สอดคล้องกับความเสี่ยง และความมีนัยสำคัญของบุคคลภายนอก โดยควรครอบคลุมการดำเนินการอย่างน้อย ดังนี้ (1) ควรกำหนดผู้รับผิดชอบในการติดตามผลการปฏิบัติงานของบุคคลภายนอกอย่างต่อเนื่อง โดยพิจารณาตามขอบเขต ระดับความเสี่ยงและความมีนัยสำคัญของการใช้บริการ การเชื่อมต่อ หรือการเข้าถึงข้อมูลจากบุคคลภายนอก (2) ควรจัดให้มีทะเบียนบุคคลภายนอก เพื่อให้สามารถใช้ในการบริหารจัดการความเสี่ยง ติดตาม และตรวจสอบการปฏิบัติงานของบุคคลภายนอกได้อย่างครบถ้วนต่อเนื่อง โดยควรครอบคลุมเนื้อหาอย่างน้อยในเรื่องดังต่อไปนี้ - ชื่อบุคคลภายนอก - รายละเอียดของการใช้บริการ การเชื่อมต่อ หรือการเข้าถึงข้อมูลจากบุคคลภายนอก - ระดับความเสี่ยงและระดับความมีนัยสำคัญ - วันเริ่มต้นและสิ้นสุดสัญญาหรือข้อตกลง (3) ควรจัดให้มีมาตรการควบคุมและติดตามสิทธิการเข้าถึงข้อมูลสารสนเทศของบุคคลภายนอกอย่างสม่ำเสมอ เพื่อให้สิทธิดังกล่าวเป็นไปตามหลักความจำเป็นต้องรู้ (need-to-know basis) (4) ควรกำหนดให้บุคคลภายนอกรายงานเหตุการณ์ผิดปกติที่เกิดขึ้นระหว่างการดำเนินงานที่เกี่ยวข้องให้สำนักงานสอบบัญชีได้รับทราบอย่างทันการณ์ (5) ควรประเมินผลการปฏิบัติงานหรือผลการให้บริการของบุคคลภายนอก ทั้งในด้านประสิทธิภาพของบริการ การรักษาความมั่นคงปลอดภัยด้าน IT และการปฏิบัติตามกฎหมายที่เกี่ยวข้อง เมื่อจะต่อสัญญาหรือเมื่อถึงรอบระยะเวลาที่สำนักงานสอบบัญชีกำหนด (6) ควรทบทวนคุณสมบัติบุคคลภายนอกอย่างสม่ำเสมอ เพื่อให้มั่นใจว่าบุคคลภายนอกยังคงมีคุณสมบัติที่เหมาะสม (7) หากสำนักงานสอบบัญชีมีการใช้บริการจาก cloud service provider สำนักงานสอบบัญชีควรกำหนดนโยบายและวิธีปฏิบัติเพิ่มเติมในเรื่องการโอนย้ายหรือการเข้าถึงข้อมูล เมื่อเกิดการยุติสัญญาหรือข้อตกลงการให้บริการ ทั้งนี้ สำนักงานสอบบัญชีควรกำหนดเงื่อนไขเกี่ยวกับสิทธิในการขอโอนย้ายหรือเข้าถึงข้อมูลดังกล่าวในสัญญาหรือข้อตกลงการให้บริการอย่างเป็น

ข้อกำหนด	แนวปฏิบัติ
	ลายลักษณ์อักษร เพื่อให้มั่นใจว่า สำนักงานสอบบัญชีจะสามารถได้รับการโอนย้ายข้อมูลหรือเข้าถึงข้อมูลได้อย่างครบถ้วน ถูกต้องและทันเวลา
(7) ควรมีการรักษาความมั่นคงปลอดภัยด้าน IT จากการใช้บริการ การเชื่อมต่อ หรือการเข้าถึงข้อมูลจากบุคคลภายนอกให้สอดคล้องกับมาตรฐานการรักษาความมั่นคงปลอดภัยด้าน IT ของสำนักงานสอบบัญชี	1. สำนักงานสอบบัญชีควรมีแนวทางการดูแลให้มั่นใจว่าการใช้บริการ การเชื่อมต่อ หรือการเข้าถึงข้อมูลจากบุคคลภายนอกมีการรักษาความมั่นคงปลอดภัยด้าน IT ตามกรอบหลักการที่สำคัญ 3 ประการ คือ การธำรงไว้ซึ่งความลับ (confidentiality) ความถูกต้องครบถ้วน (integrity) และสภาพพร้อมใช้งาน (availability) ของระบบและข้อมูล และสอดคล้องกับนโยบายและมาตรการรักษาความมั่นคงปลอดภัยด้าน IT ของสำนักงานสอบบัญชีหรือมาตรฐานสากลที่เกี่ยวข้อง เช่น ISO/IEC 27001 หรือแนวปฏิบัติในการกำกับดูแลด้าน IT ของสำนักงาน ก.ล.ต เป็นต้น โดยควรพิจารณาให้สอดคล้องกับระดับความเสี่ยง และความมีนัยสำคัญของบุคคลภายนอก
(8) ควรมีการเตรียมความพร้อมรับมือต่อเหตุการณ์ผิดปกติด้าน IT ที่อาจเกิดขึ้นและมีผลกระทบอย่างมีนัยสำคัญเพื่อให้สามารถให้บริการหรือดำเนินธุรกิจได้อย่างต่อเนื่อง	1. สำนักงานสอบบัญชีควรจัดให้มีแผนรองรับในกรณีที่บุคคลภายนอกเกิดเหตุการณ์ผิดปกติด้าน IT (incident response plan) ซึ่งมีผลกระทบกับการดำเนินการของสำนักงานสอบบัญชีโดยควรครอบคลุมเนื้อหาอย่างน้อยในเรื่องเหตุการณ์ความปลอดภัยทางไซเบอร์และเหตุการณ์การละเมิดต่อข้อมูลส่วนบุคคล
2.3 การบริหารจัดการทรัพย์สินด้าน IT (IT asset management)	
ส่วนที่ 3 การบริหารจัดการทรัพย์สินด้าน IT (IT asset management) สำนักงานสอบบัญชีควรจัดให้มีการบริหารจัดการทรัพย์สินด้าน IT เพื่อนำไปใช้ดำเนินการเกี่ยวกับการรักษาความมั่นคงปลอดภัยด้าน IT ได้อย่างเหมาะสม ครบถ้วนและเป็นปัจจุบัน ดังนี้	
3.1 ควรจัดทำทะเบียนรายการทรัพย์สินด้าน IT ประเภทฮาร์ดแวร์ ซอฟต์แวร์ รวมถึงสิทธิในการใช้งานฮาร์ดแวร์และซอฟต์แวร์	1. สำนักงานสอบบัญชีควรกำหนดระเบียบปฏิบัติเกี่ยวกับการบริหารจัดการทรัพย์สินด้าน IT โดยควรครอบคลุมเนื้อหาอย่างน้อยในเรื่องการจัดทำทะเบียนรายการทรัพย์สิน การปรับปรุงทะเบียนรายการทรัพย์สิน การยกเลิกและเรียกคืนทรัพย์สิน 2. สำนักงานสอบบัญชีควรจัดทำทะเบียนรายการทรัพย์สินด้าน IT ประเภทอุปกรณ์ (hardware) รวมถึง virtual machine ให้ครบถ้วนและเป็นปัจจุบัน โดยมีตัวอย่างของรายละเอียด ดังนี้ (1) เลขทะเบียนทรัพย์สิน (2) ประเภทฮาร์ดแวร์ (3) รายละเอียดทางเทคนิค ยี่ห้อ รุ่น

<table>
<tr><th>ข้อกำหนด</th><th>แนวปฏิบัติ</th></tr>
<tr><td></td><td>
(4) ระบบปฏิบัติการและเวอร์ชัน
(5) เจ้าของทรัพย์สิน
(6) ผู้ดูแลทรัพย์สิน
(7) สถานที่ตั้ง
(8) วันที่เริ่มใช้งาน/วันที่ติดตั้ง
(9) วันที่สิ้นสุดการรับประกัน หรือสิ้นสุดการใช้งานตามสัญญา
(10) ประเภทการครอบครอง (ซื้อ หรือเช่า)
<u>ตัวอย่างเช่น</u>
<table>
<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>
<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>
</table>
3. สำนักงานสอบบัญชีควรจัดทำทะเบียนรายการทรัพย์สินด้าน IT ประเภทซอฟต์แวร์ (software) ให้ครบถ้วนและเป็นปัจจุบัน โดยมีตัวอย่างของรายละเอียด ดังนี้
(1) เลขทะเบียนทรัพย์สิน
(2) ชื่อซอฟต์แวร์
(3) รายละเอียดทางเทคนิค/การใช้งาน
(4) ระบบปฏิบัติการและเวอร์ชัน
(5) หน่วยงานภายในผู้เป็นเจ้าของซอฟต์แวร์
</td></tr>
</table>

<table>
<tr><th>ข้อกำหนด</th><th>แนวปฏิบัติ</th></tr>
<tr><td></td><td>(6) วันที่ลงทะเบียนซอฟต์แวร์
(7) วันที่สิ้นสุดการใช้บริการ
(8) เลขทะเบียนทรัพย์สินฮาร์ดแวร์ที่อ้างอิง
<u>ตัวอย่างเช่น</u>
<table>
<tr><th>เลขทะเบียนทรัพย์สิน</th><th>ชื่อซอฟต์แวร์</th><th>รายละเอียดทางเทคนิค / การใช้งาน</th><th>ระบบปฏิบัติการและเวอร์ชัน</th><th>หน่วยงานภายในผู้เป็นเจ้าของซอฟต์แวร์</th><th>วันที่ลงทะเบียนซอฟต์แวร์</th><th>วันที่สิ้นสุดการใช้บริการ</th><th>เลขทะเบียนทรัพย์สินฮาร์ดแวร์ (เพื่อใช้อ้างอิง)</th></tr>
<tr><td>SP123456</td><td>Sheet processor pro</td><td>Software ประมวลผล sheet/excel</td><td>10.2.3A</td><td>ฝ่าย IT</td><td>1 พ.ค. 64</td><td>1 ธ.ค. 69</td><td>SV123456</td></tr>
</table>
4. สำนักงานสอบบัญชีควรปรับปรุงทะเบียนทรัพย์สินสารสนเทศต่าง ๆ ให้ครบถ้วนและเป็นปัจจุบันอย่างสม่ำเสมอ อย่างน้อยปีละ 1 ครั้ง และทุกครั้งที่มีการเปลี่ยนแปลงระบบงาน IT อย่างมีนัยสำคัญ</td></tr>
<tr><td>3.2 ควรกำหนดบุคคลหรือหน่วยงานซึ่งรับผิดชอบทรัพย์สินด้าน IT แต่ละรายการ</td><td>1. สำนักงานสอบบัญชีควรกำหนดบุคคลหรือหน่วยงานที่รับผิดชอบในการจัดทำและปรับปรุงทะเบียนรายการทรัพย์สินด้าน IT รวมถึงบำรุงรักษาทรัพย์สินด้าน IT อย่างสม่ำเสมอตลอดอายุการใช้งานของทรัพย์สินดังกล่าว</td></tr>
<tr><td>3.3 ควรจัดให้มีการบำรุงรักษาทรัพย์สินด้าน IT อย่างสม่ำเสมอ</td><td>1. สำนักงานสอบบัญชีควรจัดให้มีการบำรุงรักษาทรัพย์สินด้าน IT ให้มีสภาพพร้อมใช้งานและรองรับการดำเนินธุรกิจอย่างต่อเนื่อง พร้อมทั้งวางแผนรองรับทรัพย์สินด้าน IT ที่ใกล้จะสิ้นสุดอายุการใช้งาน (end of life) หรือสิ้นสุดการสนับสนุนหรือให้บริการจากผู้ผลิต (end of support) ได้อย่างเหมาะสมทันการณ์ ทั้งนี้ ในกรณีที่มีความจำเป็นต้องใช้ทรัพย์สินที่สิ้นสุดอายุการใช้งานหรือสิ้นสุดการสนับสนุนหรือให้บริการจากผู้ผลิต สำนักงานสอบบัญชีควรมีการประเมินความเสี่ยงและจัดให้มีมาตรการควบคุมความเสี่ยงอย่างเหมาะสม</td></tr>
</table>

ข้อกำหนด	แนวปฏิบัติ
2.4 การรักษาความมั่นคงปลอดภัยของข้อมูล (data security)	
ส่วนที่ 4 การรักษาความมั่นคงปลอดภัยของข้อมูล (data security) สำนักงานสอบบัญชีควรจัดให้มีการรักษาความมั่นคงปลอดภัยของข้อมูลเพื่อให้ข้อมูลมีความถูกต้องครบถ้วนและมีสภาพพร้อมใช้งาน รวมถึงสามารถรักษาความลับของข้อมูลได้อย่างเหมาะสม ดังนี้	
4.1 ควรมีการกำหนดบุคคลหรือหน่วยงานซึ่งเป็นเจ้าของข้อมูล	1. สำนักงานสอบบัญชีควรกำหนดบุคคลหรือหน่วยงานซึ่งเป็นเจ้าของข้อมูล (data owner) เพื่อรับผิดชอบในการกำหนดผู้ใช้งาน สิทธิการเข้าถึงและแก้ไขเปลี่ยนแปลงข้อมูล และวิธีปฏิบัติในการใช้งานข้อมูลอย่างปลอดภัย
4.2 ควรมีการจัดชั้นความลับของข้อมูล (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 โดยควรครอบคลุมเนื้อหาอย่างน้อยในเรื่องดังต่อไปนี้ (1) ควรคำนึงถึงความเสี่ยงที่สื่อบันทึกข้อมูลอาจเสื่อมสภาพ รวมทั้งวิธีการนำข้อมูลกลับมาใช้งานใหม่ ในกรณีที่จัดเก็บข้อมูลเป็นระยะเวลานาน (2) ควรจัดเก็บสื่อบันทึกข้อมูลในพื้นที่ที่มีความมั่นคงปลอดภัย และเป็นไปตามคำแนะนำของผู้ผลิต (ถ้ามี) (3) ควรจัดให้มีมาตรการรักษาความปลอดภัยของการขนส่งสื่อบันทึกข้อมูล (physical media transfer)
4.3 ควรมีการจัดให้มีแนวทางในการนำเข้า ประมวลผล และทำลายข้อมูลอย่างปลอดภัย	1. สำนักงานสอบบัญชีควรกำหนดระเบียบปฏิบัติในการทำลายข้อมูล (data disposal) โดยควรครอบคลุมเนื้อหาอย่างน้อยในเรื่องหน้าที่ความรับผิดชอบของเจ้าของข้อมูล หน่วยงานที่เกี่ยวข้อง และวิธีการทำลายข้อมูลที่เหมาะสมกับชั้นความลับของข้อมูล 2. สำนักงานสอบบัญชีควรจัดให้มีกระบวนการควบคุมการทำลายข้อมูล โดยควรครอบคลุมเนื้อหาอย่างน้อยในเรื่องการขออนุมัติจากเจ้าของข้อมูลก่อนดำเนินการ การควบคุมและสอบทานการปฏิบัติงาน และการจัดทำทะเบียนการทำลายข้อมูลสำคัญ
4.4 ควรมีการจัดทำทะเบียนทรัพย์สินด้าน IT ประเภทข้อมูล (data inventory) ให้ครบถ้วนและเป็นปัจจุบัน	1. สำนักงานสอบบัญชีควรจัดทำทะเบียนทรัพย์สินประเภทข้อมูล (data inventory) ให้ครบถ้วนและเป็นปัจจุบัน โดยมีตัวอย่างของรายละเอียด ดังนี้ (1) เลขทะเบียนข้อมูล

<table>
<tr><th>ข้อกำหนด</th><th>แนวปฏิบัติ</th></tr>
<tr><td></td><td>(2) ชื่อข้อมูลหรือชุดข้อมูล
(3) รายละเอียดลักษณะ และประเภทของข้อมูล
(4) ระดับชั้นความลับและระดับความสำคัญของข้อมูล
(5) เจ้าของข้อมูลและผู้ดูแลข้อมูล (data owner)
(6) สถานที่ หรือเครื่องแม่ข่ายที่จัดเก็บ

<u>ตัวอย่างเช่น</u>
<table>
<tr><th>เลขทะเบียนข้อมูล</th><th>ชื่อข้อมูล/ชุดข้อมูล</th><th>รายละเอียด</th><th>ระดับชั้นความลับ</th><th>เจ้าของข้อมูล</th><th>ผู้ดูแลข้อมูล</th><th>สถานที่จัดเก็บ</th></tr>
<tr><td>ABC-IT-001</td><td>IT security policy</td><td>นโยบายด้าน IT</td><td>Internal</td><td>ฝ่าย IT</td><td>ฝ่าย IT</td><td>ระบบ Intranet</td></tr>
<tr><td>ABC-Data-002</td><td>Customer information</td><td>ข้อมูลของลูกค้า ได้แก่ ชื่อ สกุล วันเดือนปีเกิด</td><td>Confidential</td><td>ฝ่ายปฏิบัติการหลักทรัพย์</td><td>ฝ่าย IT</td><td>- DB server 015
- DB backup 012</td></tr>
</table>
</td></tr>
<tr><td colspan="2">2.5 การควบคุมการเข้าถึงข้อมูลและระบบงาน IT (access control)</td></tr>
<tr><td>ส่วนที่ 5 การควบคุมการเข้าถึงข้อมูลและระบบงาน IT (access control)
สำนักงานสอบบัญชีควรจัดให้มีการควบคุมการเข้าถึงข้อมูลและระบบงาน IT อย่างมีประสิทธิภาพ เพื่อให้สามารถป้องกันการเข้าถึง และเปลี่ยนแปลงแก้ไขโดยผู้ไม่มีสิทธิหรือไม่ได้รับอนุญาต ดังนี้</td><td></td></tr>
<tr><td>5.1 ควรจัดให้มีแนวทางการบริหารจัดการบัญชีผู้ใช้งานและสิทธิการเข้าถึง โดยมีการทบทวนปรับปรุงสิทธิให้เหมาะสมอย่างสม่ำเสมอ สอดคล้องกับหน้าที่ความรับผิดชอบ รวมถึงมีกระบวนการเพิกถอนสิทธิ</td><td>1. แนวทางการบริหารจัดการบัญชีผู้ใช้งาน ควรครอบคลุมเนื้อหาอย่างน้อยในเรื่องดังต่อไปนี้
(1) หน่วยงาน หรือบุคลากร ที่รับผิดชอบในการบริหารจัดการบัญชีผู้ใช้งาน
(2) ขั้นตอนการสร้างบัญชีผู้ใช้งาน โดยบัญชีผู้ใช้งาน (user ID) ควรระบุตัวตนผู้ใช้งานได้ และหลีกเลี่ยงการใช้บัญชีผู้ใช้งานที่มีผู้ใช้งานมากกว่า 1 ราย (shared ID)</td></tr>
</table>

ข้อกำหนด	แนวปฏิบัติ
เมื่อสิ้นสุดความจำเป็นต้องใช้งาน ทั้งนี้ หากสำนักงานสอบบัญชีไม่สามารถกำหนดแนวทางการบริหารจัดการบัญชีและสิทธิการเข้าถึงข้อมูลและระบบงาน IT ตามลักษณะขั้นต่ำของแนวปฏิบัตินี้ทุกข้อได้ สำนักงานสอบบัญชีควรกำหนดให้มีการควบคุมอื่นทดแทนเพื่อตอบสนองต่อความเสี่ยงที่อาจจะเกิดขึ้นจากบัญชีผู้ใช้งานและสิทธิการเข้าถึงที่ไม่เหมาะสม	(3) การจำกัดหรือหลีกเลี่ยงใช้งานบัญชีผู้ใช้งานที่มาพร้อมกับระบบ (default user account) (4) การทบทวนบัญชีผู้ใช้งานอย่างน้อยปีละ 1 ครั้ง (5) การระงับหรือลบบัญชีผู้ใช้งานเมื่อ (1) ผู้ใช้งานสิ้นสุดสภาพการเป็นพนักงาน และ (2) ไม่มีความจำเป็นต้องใช้งาน 2. แนวทางการบริหารจัดการสิทธิการเข้าถึงข้อมูลและระบบงาน IT ควรครอบคลุมเนื้อหาอย่างน้อยในเรื่องดังต่อไปนี้ (1) หน่วยงานหรือบุคลากรที่รับผิดชอบในการบริหารจัดการสิทธิการเข้าถึงข้อมูลและระบบงาน IT (2) ขั้นตอนการขออนุมัติสิทธิในการเข้าถึงข้อมูลและระบบงาน IT จากผู้มีอำนาจ เช่น เจ้าของระบบ หรือเจ้าของข้อมูล เป็นต้น (3) ขั้นตอนการปรับปรุงสิทธิของผู้ใช้งานเมื่อมีการเปลี่ยนแปลงหน้าที่ความรับผิดชอบหรือตำแหน่งงาน (4) ขั้นตอนการเพิกถอนสิทธิของผู้ใช้งาน โดยเพิกถอนสิทธิทันทีเมื่อผู้ใช้งานสิ้นสุดสภาพการเป็นพนักงาน หรือเมื่อไม่มีความจำเป็นต้องใช้งาน (5) การแบ่งแยกบทบาทหน้าที่ของบุคคลที่เกี่ยวข้องในการจัดสรรสิทธิ เช่น ผู้ร้องขอ (access request) ผู้มีอำนาจอนุมัติ (access authorization) และผู้ดูแลสิทธิการเข้าถึง (access administration) เป็นต้น เพื่อให้สอดคล้องตามหลักการถ่วงดุล (check and balance) ที่ดี (6) การกำหนดสิทธิของผู้ใช้งานโดยคำนึงถึงความจำเป็นต้องรู้ (need-to-know) ความจำเป็นต้องใช้งาน (need-to-use) และหลักการแบ่งแยกหน้าที่ความรับผิดชอบ (segregation of duties) (7) การจัดทำตารางควบคุมการให้สิทธิ (authorization matrix) ของผู้ใช้งานที่สอดคล้องกับตำแหน่งหน้าที่และความรับผิดชอบ เพื่อใช้เป็นแนวทางการกำหนดสิทธิอย่างถูกต้องเหมาะสม (8) การทบทวนสิทธิการเข้าถึงอย่างสม่ำเสมอ อย่างน้อยปีละ 1 ครั้ง โดยกำหนดรอบระยะเวลาในการทบทวนสิทธิให้สอดคล้องกับความเสี่ยงและความสำคัญของสิทธิ
5.2 ควรจัดให้มีกระบวนการยืนยันตัวตนผู้ใช้งาน (authentication) ที่เหมาะสมกับความเสี่ยง ทั้งนี้ หากสำนักงานสอบบัญชีไม่สามารถกำหนดกระบวนการยืนยันตัวตนผู้ใช้งาน (authentication) ที่เหมาะสมตามลักษณะขั้นต่ำของแนวปฏิบัตินี้ทุกข้อได้ สำนักงานสอบบัญชีควรกำหนดให้มีการควบคุมอื่นทดแทนเพื่อตอบสนองต่อความเสี่ยงที่อาจจะเกิดขึ้นจาก	1. สำนักงานสอบบัญชีควรจัดให้มีกระบวนการยืนยันตัวตนผู้ใช้งาน (authentication) ที่มีประสิทธิผลและเหมาะสมกับความเสี่ยงของการเข้าถึงระบบโดยไม่ได้รับอนุญาต โดยควรครอบคลุมเนื้อหาอย่างน้อยในเรื่องดังต่อไปนี้ (1) ควรกำหนดวิธีการยืนยันตัวตนผู้ใช้งานที่เหมาะสมกับความเสี่ยง (2) กรณีที่มีการสร้างรหัสผ่านครั้งแรกสำหรับผู้ใช้งาน ควรมีการจัดส่งรหัสผ่านให้แก่ผู้ใช้งานด้วยวิธีการที่รัดกุมและปลอดภัย และให้ผู้ใช้งานเปลี่ยนแปลงรหัสผ่านทันทีที่ได้รับรหัสดังกล่าว (3) ควรกำหนดให้ผู้ใช้งานตั้งรหัสผ่านที่ซับซ้อนและยากต่อการคาดเดา โดยมีความยาวขั้นต่ำ 8 อักขระ (8 characters) และประกอบด้วยตัวเลขและตัวอักษร ทั้งนี้ สำนักงานสอบบัญชีอาจพิจารณาเพิ่มความซับซ้อนโดยกำหนดให้รหัสผ่านประกอบด้วย

ข้อกำหนด	แนวปฏิบัติ
การเข้าถึงระบบโดยไม่ได้รับอนุญาต	ตัวเลข ตัวอักษรพิมพ์ใหญ่ ตัวอักษรพิมพ์เล็ก และอักขระพิเศษ (เช่น “#”) (4) ควรกำหนดจำนวนครั้งที่ยอมให้ผู้ใช้งานใส่รหัสผ่านผิดพลาดติดต่อกัน ก่อนระงับการเข้าสู่ระบบชั่วคราวหรือวิธีการอื่น ๆ ที่เทียบเท่า เพื่อป้องกันการเข้าใช้งานโดยวิธีเดาสุ่ม (brute force) ทั้งนี้ ในทางปฏิบัติไม่ควรยอมให้ผู้ใช้งานยืนยันตัวตนผิดพลาดติดต่อกันเกิน 10 ครั้ง (5) ควรกำหนดให้การเปลี่ยนรหัสผ่านใหม่ไม่ซ้ำกับรหัสที่ใช้งานอย่างน้อย 4 ครั้งล่าสุด หรือไม่ซ้ำกับรหัสผ่านที่ใช้งานในช่วง 1 ปีที่ผ่านมา (6) ควรกำหนดการตั้งค่าปกติ (default) ให้ไม่แสดงรหัสผ่านบนหน้าจอ ระหว่างที่ผู้ใช้งานใส่รหัสผ่าน (7) ควรมีวิธีจัดเก็บข้อมูลรหัสผ่านที่ปลอดภัย เพื่อป้องกันการล่วงรู้หรือแก้ไขเปลี่ยนแปลง รวมทั้งไม่จัดเก็บข้อมูลรหัสผ่านใน folder เดียวกันกับ folder ที่จัดเก็บข้อมูลของแอปพลิเคชัน (8) ควรกำหนดให้ผู้ใช้งานรับผิดชอบการใช้งานบัญชีผู้ใช้งาน (user ID) และการรักษาความปลอดภัยสิ่งที่ใช้ยืนยันตัวตน (authenticator) เช่น รหัสผ่าน รหัสที่ใช้ครั้งเดียว (one-time password) เป็นต้น รวมทั้งข้อมูลส่วนบุคคลที่อาจนำมาใช้เพื่อขอเปลี่ยนแปลงข้อมูลบัญชีผู้ใช้งาน เพื่อป้องกันการใช้งานจากผู้ไม่หวังดี
5.3 ควรกำหนดมาตรการควบคุม จำกัด และติดตามการใช้งานบัญชี privileged user (privileged user management) ดังนี้ (ถ้ามี) 5.3.1 ควรมี Multi-Factor Authentication (“MFA”) หรือ วิธีการยืนยันตัวตนเพิ่มเติมหลังจากทำการยืนยันตัวตนโดยการใช้รหัสผ่าน เพื่ออนุญาตเข้าใช้งานระบบงาน IT และเมื่อเข้าใช้งานและเปลี่ยนรหัสผ่าน สำหรับระบบปฏิบัติการและระบบฐานข้อมูลที่เกี่ยวข้องกับระบบงาน IT ที่มีนัยสำคัญ	หากสำนักงานสอบบัญชีมีการใช้งานบัญชี privileged user ควรมีการดำเนินการตามข้อ 5.3.1 ถึง 5.3.3 เป็นอย่างน้อย
5.3.2 กรณีสำนักงานสอบบัญชีมีข้อจำกัดสำหรับ MFA สามารถใช้วิธีการอื่นใดที่เทียบเท่าทดแทน และควรจัดให้มีการประเมินความเสี่ยงและพิจารณาแนวทางควบคุมความเสี่ยงก่อนดำเนินการเพื่อขออนุมัติ	[ไม่มีการกำหนดแนวปฏิบัติไว้เป็นการเฉพาะ]

ข้อกำหนด	แนวปฏิบัติ
ยกเว้น (exception)	
5.3.3 ควรมีการควบคุมและติดตามตรวจสอบการใช้งานบัญชี privileged user	1. สำนักงานสอบบัญชีควรจัดให้มีการควบคุมและติดตามการใช้บัญชี privileged user ดังนี้ (1) ควรควบคุมดูแลการให้สิทธิโดยจำกัดตามบทบาทหน้าที่ และความจำเป็นในการใช้งาน (2) ควรจำกัดจำนวนบัญชี privileged user ให้มีจำนวนน้อยที่สุดหรือเท่าที่จำเป็น (3) ควรมีกระบวนการขอใช้งานบัญชี privileged user และการอนุมัติโดยผู้มีอำนาจ (4) ควรทบทวนบัญชีผู้ใช้งาน privileged user อย่างสม่ำเสมออย่างน้อยปีละ 1 ครั้ง (5) ควรกำหนดนโยบายหรือมาตรการยืนยันตัวตนของบัญชี privileged user ที่เข้มงวดกว่าบัญชีผู้ใช้งานทั่วไป (6) ควรจัดเก็บบันทึกการยืนยันตัวตนและการเข้าถึง (authentication log และ access log) และการดำเนินงาน (activity log) ของบัญชี privileged user อย่างเหมาะสม (7) ควรสอบทานบันทึกการยืนยันตัวตนและการเข้าถึง (authentication log และ access log) และการดำเนินงาน (activity log) ของบัญชี privileged user หลังเสร็จสิ้นการใช้งาน หรือสอบทานอย่างสม่ำเสมอตามรอบระยะเวลาที่เหมาะสมกับความเสี่ยง หรือ อย่างน้อยปีละ 1 ครั้ง เพื่อให้มั่นใจได้ว่าการใช้งานสิทธิเป็นไปตามขอบเขตและหน้าที่ที่ได้รับมอบหมาย
2.6 การควบคุมการเข้ารหัส (cryptographic control)	
ส่วนที่ 6 การควบคุมการเข้ารหัส (cryptographic control) หากสำนักงานสอบบัญชีมีการเข้ารหัสข้อมูล สำนักงานสอบบัญชีควรจัดให้มีการควบคุมการเข้ารหัสที่เชื่อถือได้และเป็นไปตามมาตรฐานสากลโดยกำหนดวิธีการเข้ารหัสข้อมูล (encryption) และการบริหารจัดการกุญแจเข้ารหัส (key management) อย่างปลอดภัยเพื่อให้มั่นใจได้ว่า การธำรงไว้ซึ่งความลับ (confidentiality) ความถูกต้องครบถ้วน (integrity) และความถูกต้องแท้จริง (authenticity) ของข้อมูล มีความเหมาะสมและมีประสิทธิภาพ ดังนี้	

ข้อกำหนด	แนวปฏิบัติ
6.1 ควรกำหนดวิธีการเข้ารหัสที่ปลอดภัย	ในการกำหนดวิธีการเข้ารหัสที่ปลอดภัย สำนักงานสอบบัญชีควรจัดให้มีการดำเนินการอย่างน้อย ดังนี้ 1. ควรกำหนดความรับผิดชอบของหน่วยงานหรือบุคลากรที่เกี่ยวข้อง 2. ควรกำหนดมาตรฐานวิธีการเข้ารหัสข้อมูล (cryptographic algorithm) ให้เป็นไปตามมาตรฐานสากล และมีความมั่นคงปลอดภัยเหมาะสมกับระดับความสำคัญของข้อมูล 3. ควรกำหนดรอบระยะเวลาในการทบทวนมาตรฐานวิธีการเข้ารหัสข้อมูล เพื่อให้มั่นใจว่าวิธีการเข้ารหัสข้อมูลที่ใช้งานอยู่ยังมีความมั่นคงเพียงพอในการรักษาความปลอดภัยของข้อมูล
6.2 ควรกำหนดการบริหารจัดการกุญแจเข้ารหัส โดยจัดให้มีมาตรการการควบคุมตั้งแต่การสร้างและติดตั้งกุญแจเข้ารหัส การจัดเก็บและสำรองกุญแจเข้ารหัส ไปจนถึงการเพิกถอนหรือทำลายกุญแจเข้ารหัส	1. การสร้างและติดตั้งกุญแจเข้ารหัส สำนักงานสอบบัญชีควรดำเนินการอย่างน้อย ดังนี้ (1) ควรควบคุมสภาพแวดล้อมและกระบวนการในการสร้างกุญแจเข้ารหัสที่รัดกุมปลอดภัย เช่น เลือกใช้ผู้ให้บริการออกใบรับรอง (certification authority) ที่น่าเชื่อถือ และควรมีการทำลายข้อมูลที่อาจหลงเหลือภายหลังการสร้างกุญแจเข้ารหัสแล้วเสร็จ เพื่อป้องกันการเข้าถึงหรือกู้คืนกุญแจเข้ารหัสข้อมูลโดยไม่ได้รับอนุญาต เป็นต้น (2) ควรกำหนดสิทธิการเข้าถึงกุญแจเข้ารหัสให้สามารถเข้าถึงได้โดยผู้ที่ได้รับอนุญาตเท่านั้น (3) ควรกำหนดความยาวของกุญแจเข้ารหัสที่เพียงพอในการป้องกันการถูกถอดรหัส (decrypt) โดยผู้ไม่หวังดี เช่น การโจมตีแบบ brute force เป็นต้น (4) ควรแลกเปลี่ยนกุญแจเข้ารหัส (key exchange) ผ่านกระบวนการและช่องทางที่ปลอดภัย 2. การจัดเก็บและการสำรองกุญแจเข้ารหัส สำนักงานสอบบัญชีควรดำเนินการอย่างน้อย ดังนี้ (1) ควรมีการรักษาความปลอดภัยในการจัดเก็บกุญแจเข้ารหัสทั้งด้าน physical และ logical เช่น การใช้อุปกรณ์ Hardware Security Module (HSM) หรืออุปกรณ์ที่ทำหน้าที่ในลักษณะเดียวกัน เป็นต้น (2) ควรมีการสำรองข้อมูลกุญแจเข้ารหัส โดยวิธีการเก็บรักษาข้อมูลกุญแจเข้ารหัสชุดสำรองควรมีการรักษาความปลอดภัยในระดับเดียวกับกุญแจเข้ารหัสชุดหลัก 3. การเพิกถอนหรือทำลายกุญแจเข้ารหัส สำนักงานสอบบัญชีควรดำเนินการอย่างน้อย ดังนี้ (1) ควรกำหนดเกณฑ์และแนวทางในการเปลี่ยนและเพิกถอนกุญแจเข้ารหัส เช่น กรณีกุญแจเข้ารหัสหมดอายุการใช้งานหรือไม่ปลอดภัย เป็นต้น (2) ควรกำหนดกระบวนการทำลายกุญแจ เพื่อให้มั่นใจว่าจะไม่สามารถนำกุญแจนั้นมาใช้งานได้อีก 4. สำนักงานสอบบัญชีควรจัดเก็บข้อมูลบันทึกเหตุการณ์กิจกรรมสำคัญที่เกี่ยวกับกุญแจเข้ารหัส เช่น การสร้างกุญแจ การสำรองกุญแจ การเข้าถึงหรือใช้งานกุญแจ และการเพิกถอนกุญแจ เป็นต้น

ข้อกำหนด	แนวปฏิบัติ
6.3 ควรกำหนดมาตรการการควบคุมกุญแจเข้ารหัสที่ให้บริการโดยบุคคลภายนอก ซึ่งควรตรวจสอบเพื่อให้มั่นใจได้ว่ากุญแจการเข้ารหัสที่สร้างขึ้นไม่มีการนำมาใช้ร่วมกับบุคคลอื่น	1. กรณีที่สำนักงานสอบบัญชีไม่สามารถสร้างกุญแจเข้ารหัสด้วยตนเองได้ หรือมีความจำเป็นต้องใช้กุญแจเข้ารหัสที่ให้บริการโดยบุคคลภายนอก สำนักงานสอบบัญชีควรดำเนินการเพื่อให้มั่นใจได้ว่ากุญแจเข้ารหัสที่ให้บริการโดยบุคคลภายนอกไม่มีการนำมาใช้งานร่วมกับผู้ใช้บริการรายอื่นและมีความมั่นคงปลอดภัย โดยพิจารณาเงื่อนไขหรือรายละเอียดของการให้บริการ ดังนี้ (1) ประเภทของกุญแจเข้ารหัส (2) รายละเอียดของระบบ และกระบวนการบริหารจัดการกุญแจเข้ารหัส (3) ข้อแนะนำการใช้งานและการควบคุมการเข้ารหัสข้อมูล
6.4 ควรกำหนดกระบวนการรองรับกรณีเกิดการรั่วไหลของกุญแจเข้ารหัส	1. สำนักงานสอบบัญชีควรกำหนดกิจกรรมที่ควรดำเนินการเมื่อเกิดการรั่วไหลของกุญแจเข้ารหัส เช่น การติดต่อหน่วยงานและผู้ที่เกี่ยวข้องกับชุดข้อมูลที่ใช้กุญแจเข้ารหัสชุดดังกล่าว การตรวจสอบชุดข้อมูลที่มีความเสี่ยงในการรั่วไหล การเปลี่ยนหรือเพิกถอนกุญแจการเข้ารหัสข้อมูล เป็นต้น
2.7 การรักษาความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อม (physical and environmental security)	
ส่วนที่ 7 การรักษาความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อม (physical and environmental security) สำนักงานสอบบัญชีควรจัดให้มีการรักษาความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อมของทรัพย์สินด้าน IT พร้อมทั้งมีระบบการป้องกัน และกระบวนการบำรุงรักษาฮาร์ดแวร์และระบบสาธารณูปโภค (facilities) ที่เกี่ยวข้องกับ IT เพื่อให้สามารถป้องกันความเสียหายต่อทรัพย์สินด้าน IT ซึ่งรวมถึงอุปกรณ์ที่จัดเก็บอยู่ในศูนย์คอมพิวเตอร์หลัก ศูนย์คอมพิวเตอร์สำรอง หรือ ศูนย์คอมพิวเตอร์จากบุคคลภายนอก (co-location) (ถ้ามี)	1. สำนักงานสอบบัญชีควรออกแบบศูนย์คอมพิวเตอร์ และพื้นที่ที่เกี่ยวข้องกับระบบงาน IT ที่มีนัยสำคัญ โดยคำนึงถึงความเสี่ยงจากภัยธรรมชาติและภัยคุกคามจากมนุษย์ เช่น มีกำแพงหรือรั้วที่มั่นคง และมีระยะห่างของศูนย์คอมพิวเตอร์สำรองและศูนย์คอมพิวเตอร์หลักที่เพียงพอ เป็นต้น 2. สำนักงานสอบบัญชีควรมีการบริหารจัดการสิทธิการเข้าถึงศูนย์คอมพิวเตอร์ และพื้นที่ที่เกี่ยวข้องกับระบบงาน IT ที่มีนัยสำคัญ โดยควรครอบคลุมเนื้อหาอย่างน้อยในเรื่องดังต่อไปนี้ (1) ควรให้สิทธิการเข้าถึงตามหลักความจำเป็น (2) ควรอนุมัติสิทธิการเข้าถึงโดยผู้มีอำนาจ (3) ควรปรับปรุง/ยกเลิกสิทธิการเข้าถึง ทันทีที่พนักงานลาออกหรือเปลี่ยนหน้าที่ความรับผิดชอบ (4) ควรทบทวนสิทธิการเข้าถึงอย่างสม่ำเสมออย่างน้อยปีละ 1 ครั้ง 3. สำนักงานสอบบัญชีควรจัดให้มีวิธีการยืนยันตัวตนผู้เข้า-ออกศูนย์คอมพิวเตอร์ และพื้นที่ที่เกี่ยวข้องกับระบบงาน IT ที่มีนัยสำคัญ เช่น การใช้ access card door หรือ ลงชื่อในใบลงชื่อเข้า-ออก เป็นต้น ทั้งนี้ สำหรับพื้นที่ที่มีความเสี่ยงสูง สำนักงานสอบบัญชีอาจพิจารณาใช้วิธีการยันตัวตนแบบ MFA เช่น ใช้ access card door ร่วมกับรหัสผ่านส่วนตัว (PIN) เป็นต้น 4. สำนักงานสอบบัญชีควรมีมาตรการควบคุมการเข้า-ออกศูนย์คอมพิวเตอร์ และพื้นที่ที่เกี่ยวข้องกับระบบงาน IT ที่มีนัยสำคัญ สำหรับพนักงานที่ไม่ได้มีหน้าที่ปฏิบัติงานประจำหรือผู้ที่เข้าถึงแบบชั่วคราว โดยควรจัดให้มีการอนุมัติจากผู้มีอำนาจ การบันทึกเหตุการณ์เข้า-

ข้อกำหนด	แนวปฏิบัติ
	ออก และมีการติดตามและควบคุม (escort) อย่างใกล้ชิด ตลอดระยะเวลาปฏิบัติงานในพื้นที่ดังกล่าว 5. สำนักงานสอบบัญชีควรจัดให้มีระบบรักษาความมั่นคงปลอดภัยให้กับศูนย์คอมพิวเตอร์ เช่น ระบบกล้องวงจรปิด ระบบแจ้งเตือนและระงับอัคคีภัย ระบบควบคุมแรงดันและกระแสไฟฟ้า ระบบสำรองไฟฟ้า (uninterrupted power supply) และระบบควบคุมอุณหภูมิและความชื้น เป็นต้น พร้อมทั้งควรมีการบำรุงรักษาอย่างสม่ำเสมอ 6. สำนักงานสอบบัญชีควรจัดให้มีมาตรการรองรับการทำงานผิดพลาดของระบบสาธารณูปโภคของศูนย์คอมพิวเตอร์ เช่น ระบบไฟฟ้า ระบบโทรคมนาคมและระบบปรับอากาศ เป็นต้น 7. สำนักงานสอบบัญชีควรจัดเก็บอุปกรณ์คอมพิวเตอร์ที่สำคัญ เช่น เครื่องแม่ข่าย และอุปกรณ์เครือข่าย เป็นต้น ไว้ในพื้นที่ที่มีการควบคุมอย่างปลอดภัย 8. สำนักงานสอบบัญชีควรจัดให้มีมาตรการป้องกันสายเคเบิลและสายไฟของศูนย์คอมพิวเตอร์จากการขัดขวางการทำงาน หรือการทำให้เสียหาย และบำรุงรักษาอย่างสม่ำเสมอ 9. สำนักงานสอบบัญชีควรจัดให้มีการดูแลและบำรุงรักษาทรัพย์สินด้าน IT ประเภทฮาร์ดแวร์อย่างถูกวิธี เพื่อให้อยู่ในสภาพครบถ้วนสมบูรณ์และพร้อมใช้งาน 10. สำนักงานสอบบัญชีควรควบคุมมิให้มีการนำทรัพย์สินด้าน IT ประเภทฮาร์ดแวร์ออกนอกพื้นที่โดยมิได้รับอนุญาต 11. ก่อนการยกเลิกการใช้งานหรือจำหน่ายทรัพย์สินด้าน IT ประเภทฮาร์ดแวร์ เช่น hard disk, switch, firewall และ router เป็นต้น สำนักงานสอบบัญชีควรจัดเก็บทรัพย์สินในพื้นที่ปลอดภัย และตรวจสอบให้มั่นใจว่าได้มีการลบ ย้าย ทำลายข้อมูลสำคัญและข้อมูลการปรับแต่ง (configuration) หรือปรับค่าดังกล่าวกลับไปสู่ค่าตั้งต้น (factory reset) ด้วยวิธีการที่ไม่สามารถกู้คืนได้อีก
2.8 การรักษาความมั่นคงปลอดภัยในการปฏิบัติงานด้าน IT (IT operations security)	
ส่วนที่ 8 การรักษาความมั่นคงปลอดภัยในการปฏิบัติงานด้าน IT (IT operations security) สำนักงานสอบบัญชีควรมีมาตรการรักษาความมั่นคงปลอดภัยในการปฏิบัติงานด้าน IT เพื่อให้การปฏิบัติงานเกี่ยวกับการประมวลผลข้อมูลมีความถูกต้องและมั่นคงปลอดภัย โดยควรครอบคลุมเนื้อหาอย่างน้อยในเรื่องดังต่อไปนี้	

ข้อกำหนด	แนวปฏิบัติ
2.8.1 การบริหารจัดการการตั้งค่าระบบ (system configuration management)	
8.1 ควรมีการบริหารจัดการการตั้งค่าระบบ (system configuration management) โดยมีกระบวนการในการควบคุมการตั้งค่าระบบ และสอบทานการตั้งค่าระบบอย่างสม่ำเสมอ เพื่อให้การตั้งค่าระบบเป็นไปอย่างถูกต้อง และปลอดภัย	1. สำนักงานสอบบัญชีควรกำหนดมาตรฐานการตั้งค่าด้านความมั่นคงปลอดภัย (security configuration standard) หรือ security based line อย่างเป็นลายลักษณ์อักษร เพื่อใช้ในการตั้งค่าระบบปฏิบัติการ ระบบฐานข้อมูล และอุปกรณ์เครือข่าย โดยควรคำนึงถึงเรื่อง ดังนี้ (1) ควรมีการลบบัญชีผู้ใช้งานตั้งต้น (default user) หรือการเปลี่ยนแปลงรหัสผ่านตั้งต้น (default password) (2) ควรมีการใช้วิธีการยืนยันตัวตนที่มีความรัดกุมปลอดภัย (3) ควรมีการกำหนดบริการ แอปพลิเคชัน และพอร์ตการเชื่อมต่อเท่าที่จำเป็น (4) ควรมีการจัดเก็บข้อมูลบันทึกเหตุการณ์ (log) (5) ควรมีการปรับปรุงเวอร์ชันของซอฟต์แวร์หรือ firmware ให้เป็นปัจจุบัน 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)	
8.2 ควรมีการบริหารจัดการการเปลี่ยนแปลง (change management) อย่างรัดกุมเพียงพอเพื่อให้การเปลี่ยนแปลงเป็นไปตามวัตถุประสงค์ที่กำหนดไว้อย่างถูกต้องครบถ้วน และป้องกันการเปลี่ยนแปลงโดยที่ไม่ได้รับอนุญาต	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 เป็นลายลักษณ์อักษรเพื่อเป็นหลักฐานแสดงให้เห็นว่าการเปลี่ยนแปลงได้ผ่านการพิจารณาจากเจ้าของข้อมูล เจ้าของระบบ หรือผู้มีอำนาจตามสิทธิ

ข้อกำหนด	แนวปฏิบัติ
	ที่กำหนดไว้ โดยคำขอการเปลี่ยนแปลงมีการระบุเหตุผลความจำเป็นและผลกระทบที่อาจเกิดขึ้นจากการเปลี่ยนแปลง 5. สำนักงานสอบบัญชีควรจัดให้มีระบบหรือทะเบียนในการจัดเก็บคำขอเปลี่ยนแปลงและเอกสารรายละเอียดที่เกี่ยวข้อง เพื่อใช้ควบคุมการปฏิบัติงานตั้งแต่ต้นจนจบกระบวนการ และสามารถใช้ในการติดตามและสอบทานการปฏิบัติงาน 6. กรณีที่การเปลี่ยนแปลงมีผลกระทบต่อการปฏิบัติงาน สำนักงานสอบบัญชีควรสื่อสารให้ผู้เกี่ยวข้องรับทราบการเปลี่ยนแปลงเพื่อให้สามารถปฏิบัติงานได้อย่างถูกต้อง 7. สำนักงานสอบบัญชีควรจัดให้มีแผนการถอยกลับสู่สภาพเดิม (fallback procedure) หากเกิดข้อผิดพลาดจากการเปลี่ยนแปลง เช่น การจัดเก็บเวอร์ชันของระบบก่อนการเปลี่ยนแปลงไว้ เป็นต้น
2.8.3 การบริหารจัดการขีดความสามารถของระบบงาน IT (capacity management)	
8.3 ควรมีการบริหารจัดการขีดความสามารถของระบบงาน IT (capacity management) โดยจัดให้มีมาตรฐานและวิธีปฏิบัติเรื่องการจัดการขีดความสามารถ การติดตามประสิทธิภาพการทำงานของระบบ และการประเมินแนวโน้มการใช้ทรัพยากรด้าน IT เพื่อให้สามารถรองรับการดำเนินธุรกิจในปัจจุบัน และสามารถวางแผนการจัดสรรทรัพยากรให้รองรับการใช้งานในอนาคตได้อย่างมีประสิทธิภาพ	1. สำนักงานสอบบัญชีควรกำหนดมาตรฐานและระเบียบวิธีปฏิบัติในการบริหารจัดการขีดความสามารถของระบบ เพื่อประเมินและติดตามดูแลความเพียงพอของโครงสร้างพื้นฐานด้าน IT ซึ่งรวมถึงระบบคอมพิวเตอร์ ระบบฐานข้อมูล ระบบเครือข่ายสื่อสาร และระบบสาธารณูปโภคที่เกี่ยวข้องกับงานด้าน IT 2. สำนักงานสอบบัญชีควรจัดทำรายงานความเพียงพอของทรัพยากรด้าน IT นำเสนอต่อหัวหน้าสำนักงานสอบบัญชี หรือคณะกรรมการบริหารของสำนักงานสอบบัญชีรับทราบอย่างสม่ำเสมอ เพื่อให้มีการกำกับดูแลความพร้อมใช้และความเพียงพอของระบบในการรองรับการให้บริการทางธุรกิจได้อย่างต่อเนื่อง และสามารถพิจารณาแนวทางลดความเสี่ยงได้อย่างทันการณ์
2.8.4 การรักษาความมั่นคงปลอดภัยของเครื่องแม่ข่าย (server) และอุปกรณ์ที่ใช้ปฏิบัติงาน (endpoint)	
8.4 ควรมีการรักษาความมั่นคงปลอดภัยของเครื่องแม่ข่าย (server) และอุปกรณ์ที่ใช้ปฏิบัติงาน (endpoint) เพื่อไม่ให้ถูกใช้เป็นช่องทางที่ทำให้ข้อมูลสำคัญรั่วไหล หรือมีการเข้าใช้งานระบบงาน IT โดยไม่ได้รับอนุญาต	1. สำนักงานสอบบัญชีควรกำหนดมาตรการรักษาความปลอดภัยของเครื่องแม่ข่าย และอุปกรณ์ที่ใช้ในการปฏิบัติงาน เพื่อให้สามารถป้องกันและตรวจจับโปรแกรมไม่ประสงค์ดี (malware) และภัยคุกคามทางไซเบอร์ โดยควรครอบคลุมเนื้อหาอย่างน้อยในเรื่องดังต่อไปนี้ (1) ควรมีกระบวนการหรือเครื่องมือในการควบคุมและติดตามไม่ให้มีการติดตั้งซอฟต์แวร์ที่ไม่ได้รับอนุญาต (2) ควรติดตั้งเครื่องมือในการป้องกันและตรวจจับโปรแกรมไม่ประสงค์ดี เช่น anti-virus, anti-malware และ intrusion prevention system เป็นต้น โดยปรับปรุง (update) เครื่องมือที่ใช้งานให้เป็นปัจจุบันอย่างสม่ำเสมอ เพื่อให้เท่าทันในการป้องกันภัยคุกคามใหม่ ๆ (3) ควรควบคุมการใช้งานหรือการเชื่อมต่อสื่อบันทึกข้อมูลพกพา (removable media) เช่น กำหนดแนวทางการควบคุมการใช้งาน universal serial bus (USB) หรือ external hard disk เป็นต้น

ข้อกำหนด	แนวปฏิบัติ
	2. สำนักงานสอบบัญชีควรจัดให้มีการควบคุมป้องกันทรัพย์สินด้าน IT ประเภทฮาร์ดแวร์ระหว่างที่ไม่มีผู้ใช้งาน (unattended user equipment) ให้มีความปลอดภัย โดยควรครอบคลุมเนื้อหาอย่างน้อยในเรื่องดังต่อไปนี้ (1) ควรควบคุมเอกสาร อุปกรณ์ที่ใช้ปฏิบัติงาน หรือสื่อบันทึกข้อมูลต่าง ๆ ที่มีการจัดเก็บข้อมูลสำคัญหรือข้อมูลลับ ไม่ให้วางทิ้งไว้บนโต๊ะทำงานหรือสถานที่ไม่ปลอดภัยในขณะที่ไม่ได้ใช้งาน (clear desk) (2) ควรควบคุมหน้าจอคอมพิวเตอร์ไม่ให้มีข้อมูลสำคัญปรากฏในขณะที่ไม่ได้ใช้งาน (clear screen) เช่น การตัดออกจากระบบ (session time out) หรือการล็อคหน้าจอ (lock screen) อัตโนมัติ เมื่อไม่มีการใช้งานถึงระยะเวลาที่กำหนด เป็นต้น
2.8.5 การรักษาความปลอดภัยสำหรับการปฏิบัติงานจากเครือข่ายภายนอก (teleworking) การใช้งานอุปกรณ์เคลื่อนที่ (mobile device) และการใช้งานอุปกรณ์ส่วนตัว (bring your own device : BYOD)	
8.5 ควรมีการกำหนดนโยบายและมาตรการรักษาความปลอดภัยสำหรับการปฏิบัติงานจากเครือข่ายภายนอก (teleworking) การใช้งานอุปกรณ์เคลื่อนที่ (mobile device) และรวมถึงการใช้งานอุปกรณ์ส่วนตัว (bring your own device : BYOD) โดยพิจารณาความเสี่ยงที่เกี่ยวข้อง และจัดให้มีมาตรการควบคุมอย่างเหมาะสม	1. ในกรณีที่มีการปฏิบัติงานจากเครือข่ายภายนอก (teleworking) เพื่อเข้าถึงระบบงาน IT ที่มีนัยสำคัญ สำนักงานสอบบัญชีควรจัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่รัดกุมเพียงพอเหมาะสมกับระบบงาน IT และข้อมูลที่ถูกเข้าถึง โดยควรครอบคลุมเนื้อหาอย่างน้อยในเรื่องดังต่อไปนี้ (1) ควรมีมาตรการรักษาความมั่นคงปลอดภัยด้านกายภาพที่เหมาะสม รัดกุมเพียงพอกับขอบเขตการปฏิบัติงาน สำหรับพื้นที่ปฏิบัติงานนอกองค์กร (2) ควรมีการอนุมัติการปฏิบัติงานจากเครือข่ายภายนอกโดยผู้มีอำนาจหรือผู้บริหารที่เกี่ยวข้อง (3) ควรมีการกำหนดสิทธิการเข้าถึงข้อมูลและระบบงาน IT จากเครือข่ายภายนอกเท่าที่จำเป็น พร้อมทั้งมีการทบทวนสิทธิอย่างสม่ำเสมอ (4) ควรมีการยืนยันตัวตน (authentication) ของพนักงานที่ปฏิบัติงานจากเครือข่ายภายนอกด้วยวิธีการที่รัดกุมปลอดภัย เช่น การใช้วิธียืนยันตัวตนแบบหลายปัจจัย (multi-factor authentication) และการเข้าใช้งานผ่านอุปกรณ์ที่อนุญาตเท่านั้น เป็นต้น (5) ควรมีมาตรการป้องกันความเสี่ยงจากการใช้อุปกรณ์ที่ใช้ในการปฏิบัติงานจากเครือข่ายภายนอกเป็นช่องทางในการแพร่กระจายของโปรแกรมไม่ประสงค์ดี (malware) และการรั่วไหลของข้อมูลสำคัญ (6) ควรมีมาตรการป้องกันข้อมูลที่เป็นความลับหรือมีความสำคัญ (sensitive data) เช่น การยืนยันตัวตนก่อนใช้งานอุปกรณ์ (lock screen) การเข้ารหัสข้อมูลบนอุปกรณ์ที่ใช้ในการปฏิบัติงาน หรือการลบข้อมูลจากระยะไกล (remote wipe-out) เป็นต้น 2. ในการปฏิบัติงานที่มีการใช้อุปกรณ์เคลื่อนที่ (mobile device) เพื่อเข้าถึงระบบงาน IT ที่มีนัยสำคัญ สำนักงานสอบบัญชีควรจัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่รัดกุมเพียงพอ เหมาะสมกับระบบงาน IT และข้อมูลที่ถูกเข้าถึง เช่น

ข้อกำหนด	แนวปฏิบัติ
	(1) ควรมีการลงทะเบียนอุปกรณ์เคลื่อนที่ก่อนการใช้งาน และมีการอนุมัติโดยผู้มีอำนาจที่เกี่ยวข้อง โดยควรมีการทบทวนทะเบียนดังกล่าวอย่างน้อยปีละ 1 ครั้ง และเมื่อมีการเปลี่ยนอุปกรณ์ พร้อมทั้งยกเลิกสิทธิการใช้งานของอุปกรณ์เดิม เพื่อให้มั่นใจได้ว่าอุปกรณ์เคลื่อนที่ดังกล่าวมีความความมั่นคงปลอดภัยเพียงพอ ทั้งนี้ สำนักงานสอบบัญชีอาจใช้ระบบหรือเทคโนโลยีการลงทะเบียนอื่นทดแทนได้ หากพิจารณาแล้วเห็นว่าเหมาะสม (2) ควรมีมาตรการป้องกันข้อมูลที่เป็นความลับหรือมีความสำคัญ (sensitive data) เช่น การยืนยันตัวตนก่อนใช้งานอุปกรณ์ (lock screen) การเข้ารหัสข้อมูลบนอุปกรณ์ที่ใช้ปฏิบัติงาน หรือการลบข้อมูลจากระยะไกล (remote wipe-out) เป็นต้น 3. กรณีที่อนุญาตให้พนักงานสามารถใช้อุปกรณ์ส่วนตัวของพนักงาน (bring your own device : BYOD) สำนักงานสอบบัญชีควรพิจารณาความเสี่ยงที่เกี่ยวข้อง และจัดให้มีมาตรการควบคุมความเสี่ยงอย่างเหมาะสม โดยควรครอบคลุมเนื้อหาอย่างน้อยในเรื่องดังต่อไปนี้ (1) ควรมีการกำหนดหลักเกณฑ์การอนุญาตให้ใช้งาน BYOD (2) ควรมีการควบคุมการใช้ BYOD ให้สามารถเข้าถึงเครือข่ายสื่อสาร ข้อมูล และระบบงาน IT เท่าที่จำเป็น (3) ควรมีการยืนยันตัวตนเพื่อปลดล็อคในการเข้าถึง BYOD เช่น การใช้รหัสผ่าน และการสแกนลายนิ้วมือ เป็นต้น (4) ในกรณีเครื่องคอมพิวเตอร์ส่วนตัวของพนักงาน (personal computer, notebook) สามารถเชื่อมต่อเข้าสู่ระบบเครือข่ายภายในหรือข้อมูลสำคัญ ควรจัดให้มีการติดตั้งซอฟต์แวร์ป้องกันโปรแกรมไม่ประสงค์ดี (anti-virus/ anti-malware) และปรับปรุงให้ทันสมัย (update) อยู่เสมอ (5) ควรห้ามการใช้อุปกรณ์เคลื่อนที่ (tablet, smartphone) ที่ถูกปรับแต่ง (rooted หรือ jailbroken) เข้าถึงระบบงาน IT
2.8.6 การสำรองข้อมูล (data backup)	
8.6 ควรมีการสำรองข้อมูล (data backup) ที่สำคัญด้วยวิธีการและความถี่ที่เหมาะสม เพื่อให้ข้อมูลสำรองมีสภาพพร้อมใช้งาน สอดคล้องกับเป้าหมายการกู้คืนระบบงาน IT ในกรณีที่ระบบงาน IT และข้อมูลหลักเกิดเหตุขัดข้องหรือได้รับความเสียหาย โดยควรมีการทดสอบข้อมูลสำรองและกระบวนการกู้คืนข้อมูลอย่างน้อยปีละ 1 ครั้ง	1. สำนักงานสอบบัญชีควรกำหนดมาตรฐานหรือวิธีปฏิบัติในการสำรองข้อมูลที่สอดคล้องกับระยะเวลาเป้าหมายในการกู้คืนระบบงาน IT (Recovery Time Objective : RTO) และระยะเวลาเป้าหมายสูงสุดที่ยอมให้ข้อมูลเสียหาย (Recovery Point Objective : RPO) โดยควรครอบคลุมเนื้อหาอย่างน้อยในเรื่องดังต่อไปนี้ (1) ข้อมูลที่ควรสำรอง (2) ความถี่หรือรอบเวลาในการสำรองข้อมูล (3) ขั้นตอนและวิธีการสำรองข้อมูล (4) ขั้นตอนและวิธีการกู้คืนข้อมูล

ข้อกำหนด	แนวปฏิบัติ
	(5) สถานที่และวิธีการเก็บรักษาสื่อบันทึกข้อมูล 2. สำนักงานสอบบัญชีควรจัดเก็บสื่อบันทึกข้อมูลสำรอง พร้อมทั้งสำเนาขั้นตอนหรือวิธีปฏิบัติงานต่าง ๆ ไว้นอกศูนย์คอมพิวเตอร์หลัก หรือนอกสถานที่ปฏิบัติงานหลัก โดยสถานที่ดังกล่าวควรจัดให้มีมาตรการรักษาความปลอดภัยอย่างเหมาะสมตามนโยบายของสำนักงานสอบบัญชี หรือ เทียบเคียงกับศูนย์คอมพิวเตอร์หลักหรือสถานที่ปฏิบัติงานหลัก 3. สำนักงานสอบบัญชีควรจัดให้มีการสอบทานการสำรองข้อมูล และทดสอบข้อมูลสำรองอย่างน้อยปีละ 1 ครั้ง เพื่อให้มั่นใจว่ามีการสำรองข้อมูลมีความครบถ้วนถูกต้อง พร้อมใช้งาน และปลอดภัย 4. ในกรณีที่จำเป็นต้องจัดเก็บข้อมูลเป็นระยะเวลานาน สำนักงานสอบบัญชีควรคำนึงถึงวิธีการนำข้อมูลกลับมาใช้งานในอนาคตด้วย หากมีความจำเป็น เช่น เมื่อมีการจัดเก็บข้อมูลลงในสื่อบันทึกข้อมูลใด ควรมีการจัดเก็บอุปกรณ์และโปรแกรมที่ใช้อ่านสื่อบันทึกข้อมูลนั้นด้วย เป็นต้น
2.8.7 การจัดเก็บข้อมูลบันทึกเหตุการณ์การใช้งานเกี่ยวกับระบบงาน IT (log)	
8.7 ควรมีการจัดเก็บข้อมูลบันทึกเหตุการณ์การใช้งานเกี่ยวกับระบบงาน IT (log) อย่างครบถ้วนและเพียงพอ เพื่อให้สามารถใช้เป็นหลักฐานการทำธุรกรรมทางอิเล็กทรอนิกส์ และสามารถติดตามและตรวจสอบการเข้าถึงและใช้งานข้อมูลและระบบงาน IT ย้อนหลังได้ตามที่กฎหมายกำหนด	1. สำนักงานสอบบัญชีควรจัดเก็บข้อมูลบันทึกเหตุการณ์ (log) ด้วยวิธีการที่ปลอดภัย โดยมีรายละเอียดครบถ้วนเพียงพอที่จะใช้เป็นหลักฐานในการตรวจสอบที่สามารถระบุตัวบุคคลผู้กระทำได้ และควรจัดเก็บเป็นระยะเวลาอย่างน้อย 90 วัน หรือจัดเก็บตามกฎหมายที่เกี่ยวข้องกำหนด โดยควรประกอบด้วยรายการหลักฐานอย่างน้อย ดังนี้ (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 โดยควรครอบคลุมเนื้อหาอย่างน้อยในเรื่องดังต่อไปนี้ (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 โดยสอดคล้องกับกฎหมายและหลักเกณฑ์

ข้อกำหนด	แนวปฏิบัติ
	ที่เกี่ยวข้อง เช่น กฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ และกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล เป็นต้น 3. สำนักงานสอบบัญชีควรจัดเก็บ log ของอุปกรณ์สำคัญไว้ที่เครื่องแม่ข่ายที่ใช้จัดเก็บ log (logging server) ที่แยกเฉพาะ หรือใช้วิธีการที่เทียบเคียงซึ่งสามารถป้องกันการเปลี่ยนแปลง แก้ไข หรือทำลาย log ได้ โดยควรมีมาตรการรักษาความปลอดภัยอย่างน้อย ดังนี้ (1) กำหนดหน้าที่และความรับผิดชอบผู้ที่สามารถเข้าถึง log ตามความจำเป็น (2) มีกระบวนการยืนยันตัวตนและตรวจสอบสิทธิในการเข้าถึง log (3) ติดตั้งเครื่องแม่ข่าย หรืออุปกรณ์ที่ใช้จัดเก็บ log ให้อยู่ในโซนเครือข่ายที่มีความมั่นคงปลอดภัย
2.8.8 การติดตามดูแลระบบและเฝ้าระวังภัยคุกคามทางไซเบอร์ (security monitoring)	
8.8 ควรมีการติดตามดูแลระบบและเฝ้าระวังภัยคุกคามทางไซเบอร์ (security monitoring) โดยมีกระบวนการหรือเครื่องมือป้องกันและตรวจจับเหตุการณ์ผิดปกติด้าน IT โปรแกรมไม่ประสงค์ดี (malware) หรือภัยคุกคามทางไซเบอร์ที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยต่อระบบงาน IT ที่มีนัยสำคัญ	1. สำนักงานสอบบัญชีควรจัดให้มีกระบวนการหรือเครื่องมือในการตรวจจับเหตุการณ์ผิดปกติที่อาจส่งผลกระทบต่อความปลอดภัยของระบบ IT ที่มีนัยสำคัญอย่างทันท่วงที เช่น กระบวนการหรือเครื่องมือในการสอบทาน log เป็นต้น เพื่อให้รับทราบความผิดปกติหรือภัยคุกคาม และสามารถดำเนินการป้องกันหรือรับมือได้อย่างเหมาะสม 2. สำนักงานสอบบัญชีควรจัดให้มีกระบวนการหรือเครื่องมือในการรับข้อมูลข่าวสารเกี่ยวกับภัยคุกคาม (cyber threat intelligence) เพื่อให้สามารถติดตามและวิเคราะห์ภัยคุกคามทางไซเบอร์ที่อาจเกิดขึ้น และสามารถดำเนินการป้องกันหรือรับมือได้อย่างเหมาะสม
2.8.9 การประเมินช่องโหว่ทางเทคนิค (technical vulnerability assessment)	
8.9 ควรมีการประเมินช่องโหว่ทางเทคนิค (technical vulnerability assessment) ของระบบงาน IT ที่เหมาะสมกับระดับความเสี่ยงเพื่อให้ทราบถึงช่องโหว่และสามารถดำเนินการแก้ไขและป้องกันภัยคุกคามทางไซเบอร์ที่อาจเกิดขึ้นได้อย่างทันท่วงที โดยการประเมินช่องโหว่ทางเทคนิคควรครอบคลุมถึงระบบงาน IT ที่มีนัยสำคัญ และระบบงาน IT ที่เชื่อมต่อกับเครือข่ายสาธารณะ (internet facing) ทุกระบบ และทุกครั้งที่มีการเปลี่ยนแปลงอย่างมีนัยสำคัญของระบบดังกล่าว เช่น การเปลี่ยนแปลงโครงสร้างพื้นฐานของระบบงาน IT หรือการเพิ่มเติมฟังก์ชันสำคัญของระบบงาน IT เป็นต้น	1. สำนักงานสอบบัญชีควรกำหนดขอบเขตและความถี่ของการประเมินช่องโหว่ทางเทคนิคให้ครอบคลุมทุกระบบงานตามระดับความเสี่ยง ทั้งนี้ สำหรับระบบงาน IT ที่มีนัยสำคัญและระบบงาน IT ที่เชื่อมต่อกับเครือข่ายสาธารณะทุกระบบควรได้รับการประเมินช่องโหว่ทุกครั้งที่มีการเปลี่ยนแปลงระบบดังกล่าวอย่างมีนัยสำคัญ 2. สำนักงานสอบบัญชีควรประเมินความเสี่ยงของช่องโหว่ที่ตรวจพบและกำหนดระยะเวลาแก้ไขที่เหมาะสมกับความเสี่ยง 3. สำนักงานสอบบัญชีควรรายงานผลการประเมินช่องโหว่ไปยังผู้รับผิดชอบ รวมถึงควรติดตามให้มีการแก้ไขช่องโหว่ภายในระยะเวลาที่กำหนดไว้ โดยนำเสนอความคืบหน้าของการดำเนินการต่อหัวหน้าสำนักงานสอบบัญชี หรือคณะกรรมการบริหารของสำนักงานสอบบัญชีที่ได้รับมอบหมาย

ข้อกำหนด	แนวปฏิบัติ
2.8.10 การบริหารจัดการโปรแกรมแก้ไขช่องโหว่ (patch management)	
8.10 ควรมีการบริหารจัดการโปรแกรมแก้ไขช่องโหว่ (patch management) โดยจัดให้มีกระบวนการควบคุมการติดตั้งโปรแกรมแก้ไขช่องโหว่บนระบบและอุปกรณ์เพื่อลดความเสี่ยงที่จะถูกโจมตีในอนาคต	1. สำนักงานสอบบัญชีควรมีการกำหนดมาตรฐานและระเบียบวิธีปฏิบัติในการบริหารจัดการโปรแกรมแก้ไขช่องโหว่ (patch) โดยควรครอบคลุมเนื้อหาอย่างน้อยในเรื่องดังต่อไปนี้ (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 หรือควรจัดให้มีมาตรการควบคุมทดแทน เพื่อลดความเสี่ยงจากการถูกโจมตีผ่านช่องโหว่นั้น ๆ 4. สำนักงานสอบบัญชีควรมอบหมายผู้รับผิดชอบ หรือควรจัดให้มีเครื่องมือที่ใช้ติดตาม patch ด้านการรักษาความปลอดภัย (patch monitoring tool) ที่ยังไม่มีการติดตั้งบนระบบปฏิบัติการ (operation system) และระบบฐานข้อมูล (database system) ที่สำคัญของสำนักงานสอบบัญชี
2.9 การรักษาความมั่นคงปลอดภัยเกี่ยวกับระบบเครือข่ายสื่อสาร (communication system security)	
ส่วนที่ 9 การรักษาความมั่นคงปลอดภัยเกี่ยวกับระบบเครือข่ายสื่อสาร (communication system security) สำนักงานสอบบัญชีควรมีการรักษาความมั่นคงปลอดภัยเกี่ยวกับระบบเครือข่ายสื่อสารอย่างเหมาะสม เพื่อให้ระบบเครือข่ายสื่อสารและข้อมูลที่รับส่งผ่านระบบเครือข่ายสื่อสารมีความมั่นคงปลอดภัย สามารถป้องกันการบุกรุกหรือภัยคุกคามทางไซเบอร์ที่อาจเกิดขึ้น	1. สำนักงานสอบบัญชีควรจัดให้มีการรักษาความมั่นคงปลอดภัยของระบบเครือข่ายสื่อสาร โดยควรมีการดำเนินการอย่างน้อย ดังนี้ (1) ควรออกแบบเครือข่ายสื่อสารที่มีการแบ่งแยกเครือข่ายอย่างเหมาะสม โดยคำนึงถึงระดับความสำคัญของระบบงาน (application system) ระดับความสำคัญของข้อมูล รวมถึงความจำเป็นในการเชื่อมต่อจากระบบงานอื่น ๆ หรือจากภายนอกองค์กร (2) ควรจัดให้มีการควบคุมการเชื่อมต่อของระบบงาน (application system) ที่สำคัญ (3) ควรมีการแบ่งแยกเครือข่ายให้มีความรัดกุมปลอดภัย เช่น (3.1) แบ่งแยกเครือข่ายภายใน (private network) และเครือข่ายภายนอก (public network) ออกจากกัน (3.2) แบ่งแยกเครือข่ายของระบบงาน IT ที่มีนัยสำคัญ เครือข่ายสำหรับการปฏิบัติงานของพนักงาน และเครือข่ายสำหรับ

ข้อกำหนด	แนวปฏิบัติ
รวมทั้งพร้อมใช้งานได้อย่างต่อเนื่อง	การใช้งานทั่วไป/เครือข่ายสำหรับบุคคลภายนอก (guest network) ออกจากกัน (3.3) จุดที่มีการแบ่งแยกเครือข่ายที่มีความสำคัญและมีความเสี่ยง ควรติดตั้งอุปกรณ์รักษาความปลอดภัยเครือข่ายที่มีความสามารถในการควบคุมและคัดกรองข้อมูล (traffic) ที่รับส่งผ่านเครือข่าย เพื่อป้องกันและตรวจจับการบุกรุกของไวรัสหรือมัลแวร์ต่าง ๆ (4) ควรควบคุม และจำกัดให้เฉพาะอุปกรณ์ที่ได้รับอนุญาตเท่านั้นที่สามารถเชื่อมต่อกับระบบเครือข่ายภายในได้ (5) ควรกำหนดกระบวนการเปิดใช้งานช่องทางเชื่อมต่อ (port) ตามความจำเป็น รวมทั้งการขออนุมัติจากผู้มีอำนาจ และควรจัดให้มีการควบคุมอย่างเหมาะสม (6) ควรติดตามสถานะความพร้อมใช้งานของระบบเครือข่ายให้อยู่ในระดับ service level agreement (SLA) ที่กำหนด (7) ควรจัดให้มีระบบหรือมาตรการป้องกันการโจมตีผ่านเครือข่ายสาธารณะที่เหมาะสมตามความเสี่ยง เช่น การใช้อุปกรณ์การรักษาความปลอดภัย intrusion prevention system (IPS) และการป้องกันการโจมตีแบบ Distributed Denial of Service (DDoS protection) เป็นต้น 2. สำนักงานสอบบัญชีควรจัดให้มีการรักษาความมั่นคงปลอดภัยของข้อมูลสารสนเทศที่รับส่งผ่านระบบเครือข่ายสื่อสาร (information transfer) เช่น (1) ควรกำหนดแนวปฏิบัติที่ดีในการรับส่งข้อมูลสารสนเทศผ่านช่องทางการสื่อสารอิเล็กทรอนิกส์ประเภทต่าง ๆ (2) ควรนำเทคนิคการเข้ารหัสข้อมูลมาใช้ในการรับส่งข้อมูลสารสนเทศที่เป็นความลับและมีความสำคัญ (3) ควรมีมาตรการป้องกันข้อมูลที่เป็นความลับหรือมีความสำคัญที่รับส่งในรูปแบบของไฟล์แนบ (attachment files) และการส่งต่ออีเมลแบบอัตโนมัติออกสู่ภายนอกองค์กร 3. สำนักงานสอบบัญชีควรจัดให้มีการรักษาความมั่นคงปลอดภัยสำหรับการใช้งานระบบรับส่งข้อมูลสารสนเทศผ่านระบบเครือข่ายสื่อสาร (ระบบ electronic messaging) โดยมีการดำเนินการอย่างน้อย ดังนี้ (1) กรณีที่มีการใช้งานระบบ electronic messaging ที่ให้บริการโดยบุคคลภายนอก เช่น โปรแกรมสนทนาผ่านระบบอิเล็กทรอนิกส์ (instant messaging) ระบบเครือข่ายสังคมออนไลน์ (social networking) หรือโปรแกรมเรียกใช้แฟ้มข้อมูลร่วมกัน (file sharing) เป็นต้น สำนักงานสอบบัญชีควรจัดให้มีการควบคุมดูแลอย่างเหมาะสมเพียงพอ และคำนึงถึงการปฏิบัติตามกฎหมายและหลักเกณฑ์ที่เกี่ยวข้องอย่างเคร่งครัด (2) ควรจัดให้มีมาตรการคัดกรอง (filter) อีเมลที่มีความเสี่ยงต่อการเกิดภัยคุกคามทางไซเบอร์ เช่น อีเมลที่มีไฟล์แนบชนิด .exe เป็นต้น

ข้อกำหนด	แนวปฏิบัติ
2.10 การบริหารจัดการโครงการด้าน IT (IT project management) และการจัดหา พัฒนา และบำรุงรักษาระบบงาน IT (system acquisition, development and maintenance)	
ส่วนที่ 10 การบริหารจัดการโครงการด้าน IT (IT project management) และการจัดหา พัฒนา และบำรุงรักษาระบบงาน IT (system acquisition, development and maintenance) ในการบริหารจัดการโครงการด้าน IT (IT project management) และการจัดหา พัฒนา และบำรุงรักษาระบบงาน IT ในปัจจุบัน หรือวางแผนว่าจะมีในอนาคต สำนักงานสอบบัญชีควรจัดทำนโยบายและแนวปฏิบัติสำหรับการบริหารจัดการ โครงการด้าน IT การจัดหา พัฒนา รวมถึงบำรุงรักษาระบบงาน IT เป็นลายลักษณ์อักษร เพื่อให้มั่นใจได้ว่า เมื่อใดก็ตามที่มีการดำเนินโครงการด้าน IT สำนักงานสอบบัญชีจะมีกรอบและแนวทางที่จะช่วยรักษาความมั่นคงปลอดภัยตลอดวงจรชีวิตของระบบงาน IT (entire life cycle) โดยควรครอบคลุมเนื้อหาอย่างน้อยในเรื่องดังต่อไปนี้	
2.10.1 การบริหารจัดการโครงการด้าน IT (IT project management)	
<u>10.1 บริหารจัดการโครงการด้าน IT (IT project management)</u> ควรกำหนดกรอบการบริหารจัดการโครงการ (project management framework) เพื่อให้การบริหารจัดการโครงการด้าน IT ที่มีนัยสำคัญเป็นไปอย่างมีประสิทธิภาพ สามารถส่งมอบโครงการได้อย่างถูกต้อง ครบถ้วน ตามแผนงานและบรรลุวัตถุประสงค์ตามเป้าหมายที่กำหนดไว้ ไม่ว่างานโครงการนั้นจะดำเนินการโดย	1. สำนักงานสอบบัญชีควรกำหนดกรอบการบริหารจัดการโครงการ (project management framework) เป็นลายลักษณ์อักษร โดยควรครอบคลุมเนื้อหาอย่างน้อยในเรื่องดังต่อไปนี้ (1) โครงสร้างการควบคุมและกำกับดูแลโครงการ (project governance) ที่ชัดเจน เพื่อให้มีการควบคุมดูแลโครงการให้สำเร็จเป็นไปตามแผนงานที่กำหนด โดยควรพิจารณาการจัดให้มีผู้รับผิดชอบในบทบาทหน้าที่ตามความจำเป็นและความเหมาะสม เช่น (1.1) คณะกรรมการกำกับดูแลโครงการ (project steering committee) ควรมีบทบาทหน้าที่และความรับผิดชอบในการกำกับดูแลและติดตามความคืบหน้าของโครงการ รวมทั้งให้คำแนะนำ และพิจารณาตัดสินใจการดำเนินงานในโครงการที่สำคัญ เพื่อให้โครงการสามารถดำเนินการได้ตามแผนที่กำหนดไว้ โดยควรประกอบด้วยผู้บริหารจากหน่วยงานที่เกี่ยวข้อง และเจ้าของโครงการหรือผู้สนับสนุนโครงการ (project owner/project sponsor)

ข้อกำหนด	แนวปฏิบัติ
สำนักงานสอบบัญชีเอง หรือบุคคลภายนอก	(1.2) ผู้จัดการโครงการ (project manager) ควรมีบทบาทหน้าที่และความรับผิดชอบในการบริหารจัดการโครงการให้เป็นไปตามระเบียบขั้นตอนการบริหารจัดการโครงการ เพื่อให้โครงการสามารถส่งมอบได้อย่างถูกต้องครบถ้วนสำเร็จตามแผนงานที่กำหนด (2) แนวทางการบริหารจัดการโครงการ โดยควรครอบคลุมเนื้อหาอย่างน้อยในเรื่องดังต่อไปนี้ (2.1) ระเบียบขั้นตอนการบริหารจัดการโครงการ ซึ่งควรครอบคลุมตั้งแต่ก่อนเริ่มโครงการ การดำเนินการและควบคุมโครงการ การปิดโครงการ และการสอบทานโครงการ (2.2) ปัจจัยและเกณฑ์ในการประเมินหรือจัดระดับความสำคัญของโครงการที่ชัดเจน รวมถึงขอบเขตอำนาจหน้าที่ในการอนุมัติและกำกับดูแลโครงการตามระดับความสำคัญของโครงการ (2.3) เอกสารหรือสิ่งส่งมอบในแต่ละขั้นตอนที่ชัดเจน เช่น แผนการดำเนินโครงการ รายงานความคืบหน้า รายงานการปิดโครงการ เป็นต้น 2. การเริ่มโครงการ สำนักงานสอบบัญชีควรดำเนินการอย่างน้อย ดังนี้ (1) ควรประเมินความจำเป็นและประโยชน์ที่คาดว่าจะได้รับ รวมถึงความเสี่ยงและผลกระทบที่อาจเกิดขึ้นต่อระบบและหน่วยงานที่เกี่ยวข้อง (2) ควรจัดทำแผนการดำเนินโครงการที่มีรายละเอียดครบถ้วนเพียงพอต่อการบริหารจัดการโครงการ โดยควรครอบคลุมเนื้อหาอย่างน้อยในเรื่องดังต่อไปนี้ (2.1) เป้าหมายโครงการ (2.2) ทรัพยากร และเทคโนโลยีที่ใช้ (2.3) บทบาทหน้าที่และความรับผิดชอบของทีมงานในการดำเนินโครงการ (2.4) ขอบเขตและระยะเวลาของการดำเนินโครงการในแต่ละขั้นตอน (2.5) ผลงานที่จะส่งมอบในแต่ละขั้นตอน (2.6) ข้อกำหนดเงื่อนไขที่เกี่ยวข้องกับโครงการ (ถ้ามี) เช่น ข้อกำหนดของผู้ว่าจ้าง ภาระผูกพัน ข้อจำกัด เป็นต้น (3) ควรมีการนำเสนอแผนการดำเนินโครงการ เพื่อขออนุมัติโครงการต่อหัวหน้าสำนักงานสอบบัญชี หรือคณะกรรมการบริหารของสำนักงานสอบบัญชีตามขอบเขตในการอนุมัติที่กำหนดไว้ 3. การดำเนินงานและควบคุมโครงการ สำนักงานสอบบัญชีควรดำเนินการอย่างน้อย ดังนี้ (1) ควรติดตามและประเมินการดำเนินโครงการอย่างต่อเนื่องและครอบคลุมขอบเขต ระยะเวลา และทรัพยากรที่วางแผนไว้

ข้อกำหนด	แนวปฏิบัติ
	(2) ในกรณีที่มีการเปลี่ยนแปลงขอบเขต ระยะเวลาหรือทรัพยากร หรือยกเลิกโครงการ ควรมีการนำเสนอผู้มีอำนาจเพื่อขออนุมัติการเปลี่ยนแปลงหรือยกเลิกโครงการ (3) รายงานความคืบหน้า ปัญหา อุปสรรคและข้อจำกัดในการดำเนินโครงการ ต่อคณะกรรมการกำกับดูแลโครงการหรือผู้บริหารระดับสูงที่ได้รับมอบหมายอย่างสม่ำเสมอ โดยโครงการที่ส่งผลกระทบต่อธุรกิจของสำนักงานสอบบัญชีอย่างมีนัยสำคัญควรมีการนำเสนอแก่หัวหน้าสำนักงานสอบบัญชี หรือคณะกรรมการบริหารของสำนักงานสอบบัญชีด้วย 4. การปิดโครงการ สำนักงานสอบบัญชีควรดำเนินการอย่างน้อย ดังนี้ (1) ควรสรุปประโยชน์ที่ได้รับจากโครงการเปรียบเทียบกับเป้าหมายที่กำหนด (2) ควรรวบรวมปัญหา อุปสรรคจากการบริหารจัดการโครงการ เพื่อนำมาเป็นสิ่งที่ได้เรียนรู้ (lesson learned) ใช้สำหรับวิเคราะห์ปรับปรุง และพัฒนากระบวนการหรือเครื่องมือในการบริหารจัดการโครงการต่อไปให้มีประสิทธิภาพมากขึ้น 5. สำนักงานสอบบัญชีควรสอบทานโครงการที่มีนัยสำคัญ เพื่อให้มั่นใจได้ว่าโครงการสอดคล้องกับเป้าหมายของโครงการ นโยบาย มาตรฐาน ระเบียบและวิธีปฏิบัติของสำนักงานสอบบัญชี รวมทั้งกฎหมายและหลักเกณฑ์ที่เกี่ยวข้อง
2.10.2 การจัดหาระบบงาน IT (system acquisition)	
<u>10.2 จัดหาระบบงาน IT (system acquisition)</u> ควรจัดให้มีหลักเกณฑ์ในการจัดหาระบบงาน IT และผู้ให้บริการ เพื่อให้มั่นใจว่าระบบที่จัดหาสามารถตอบสนองความต้องการทางธุรกิจและความต้องการด้านความมั่นคงปลอดภัย IT โดยคำนึงถึงความยืดหยุ่นในการเปลี่ยนแปลงผู้ให้บริการ การเปลี่ยนแปลงเทคโนโลยี รวมถึงการเปลี่ยนแปลงต่าง ๆ ที่เกี่ยวข้องกับการดำเนินธุรกิจอย่างมีนัยสำคัญ	1. สำนักงานสอบบัญชีควรจัดให้มีหลักเกณฑ์การคัดเลือกระบบงาน IT และผู้ให้บริการ เพื่อให้มั่นใจว่าระบบที่จัดหาสามารถตอบสนองความต้องการทางธุรกิจและความต้องการด้านความมั่นคงปลอดภัยสารสนเทศ โดยควรครอบคลุมเนื้อหาอย่างน้อยในเรื่องดังต่อไปนี้ (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

ข้อกำหนด	แนวปฏิบัติ
2.10.3 การพัฒนาระบบงาน IT (system development))	
10.3 พัฒนาระบบงาน IT (system development) ควรจัดให้มีมาตรการควบคุมเกี่ยวกับการพัฒนาระบบงาน IT ในการออกแบบ พัฒนา ทดสอบระบบ และนำระบบขึ้นใช้งานจริง เพื่อให้มั่นใจว่าระบบมีความถูกต้อง มั่นคงปลอดภัย เชื่อถือได้ พร้อมใช้งาน และมีความยืดหยุ่นเพียงพอจะรองรับการใช้งานได้สอดคล้องกับแผนการดำเนินธุรกิจ โดยควรดำเนินการอย่างน้อย ดังนี้	[ไม่มีการกำหนดแนวปฏิบัติไว้เป็นการเฉพาะ]
(1) ควรมีการกำหนดรายละเอียดความต้องการของระบบ (requirement) และคุณสมบัติทางเทคนิค (technical specification) ของระบบที่พัฒนา ดังนี้ (1.1) ความมั่นคงปลอดภัย (security) (1.2) สภาพพร้อมใช้งาน (availability) (1.3) ขีดความสามารถที่รองรับ (capacity)	การออกแบบระบบ 1. สำนักงานสอบบัญชีควรกำหนดให้หน่วยงานอื่นที่เกี่ยวข้องมีส่วนร่วมในการกำหนดรายละเอียดความต้องการของระบบ 2. สำนักงานสอบบัญชีควรจัดทำเอกสารระบุรายละเอียดความต้องการของระบบ (functional requirement และ non-functional requirement) และคุณสมบัติทางเทคนิค (technical specification) โดยควรครอบคลุมเนื้อหาอย่างน้อยในเรื่องดังต่อไปนี้ (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) ขีดความสามารถที่รองรับ (capacity) ตามอัตรากำลังคนของสำนักงานสอบบัญชีที่วางแผนไว้ในปัจจุบัน ทั้งนี้ เอกสารข้างต้นควรผ่านการสอบทานความถูกต้องครบถ้วนและได้รับอนุมัติจากผู้เกี่ยวข้องก่อนเริ่มพัฒนาระบบ
(2) ควรมีการแบ่งแยกบทบาทหน้าที่และความรับผิดชอบของผู้ที่เกี่ยวข้องในการพัฒนาระบบ เพื่อให้มีการสอบทานก่อนนำระบบขึ้นไปให้บริการจริง ทั้งนี้ หากระบบถูกพัฒนาโดยบุคคลภายนอก และมีข้อจำกัดในการแบ่งแยกหน้าที่ สำนักงานสอบบัญชีควรมี	การพัฒนาระบบ 1. สำนักงานสอบบัญชีควรแบ่งแยกบทบาทหน้าที่และความรับผิดชอบของผู้ที่เกี่ยวข้องในการพัฒนาระบบ (segregation of duty) เพื่อให้มีการสอบทานก่อนนำระบบขึ้นไปให้บริการจริง เช่น แยกผู้พัฒนาระบบ ออกจากผู้นำระบบขึ้นใช้งานจริง เป็นต้น

ข้อกำหนด	แนวปฏิบัติ
การจัดหาการควบคุมอื่นทดแทนเพื่อตอบสนองต่อความเสี่ยงจากการแบ่งแยกหน้าที่ไม่เหมาะสม	
(3) ควรมีการแบ่งแยกสภาพแวดล้อมของระบบงานที่ใช้สำหรับการพัฒนา (development) และการทดสอบ (testing) ออกจากระบบงานที่ให้บริการจริง (production) เช่น	1. สำนักงานสอบบัญชีควรแบ่งแยกสภาพแวดล้อมของระบบงานที่ใช้สำหรับการพัฒนา (development) และการทดสอบ (testing) ออกจากระบบงานที่ให้บริการจริง (production) เพื่อควบคุมการทดสอบและลดผลกระทบที่อาจเกิดขึ้นต่อระบบงานที่ให้บริการจริง 2. สำนักงานสอบบัญชีควรจัดให้มีการรักษาความมั่นคงปลอดภัยของเครื่องที่ไม่ได้อยู่บนระบบที่ให้บริการจริง (non-production) ให้เพียงพอกับระดับความเสี่ยงของการเข้าถึงระบบและข้อมูลโดยไม่ได้รับอนุญาต และการรั่วไหลของข้อมูลที่ใช้ทดสอบ 3. สำนักงานสอบบัญชีควรจัดให้มีการควบคุมไม่ให้มีการติดตั้งเครื่องมือการพัฒนาระบบ (development tools) และเครื่องมือแปลโปรแกรม (compilers) ไว้บนระบบที่ให้บริการจริง เพื่อป้องกันความเสี่ยงที่อาจถูกปรับเปลี่ยนหรือติดตั้งโปรแกรมโดยไม่ได้รับอนุญาต
(4) ควรมีกระบวนการหรือเครื่องมือควบคุมการพัฒนาชุดคำสั่งคอมพิวเตอร์ให้มีความปลอดภัย เช่น	1. สำนักงานสอบบัญชีควรกำหนดมาตรฐานและระเบียบวิธีปฏิบัติในการออกแบบและพัฒนาระบบอย่างปลอดภัย (secure coding) สอดคล้องกับมาตรฐานสากล รวมทั้งควบคุมให้ผู้พัฒนาระบบปฏิบัติตามมาตรฐานและระเบียบวิธีปฏิบัติดังกล่าว 2. สำนักงานสอบบัญชีควรมีกระบวนการหรือเครื่องมือควบคุมเวอร์ชันของชุดคำสั่งคอมพิวเตอร์ (source code version control) 3. สำนักงานสอบบัญชีควรสอบทานคำสั่งในการเขียนโปรแกรม (source code review) โดยใช้ระบบอัตโนมัติ (automated review) หรือแบบ manual review ซึ่งดำเนินการโดยบุคคลที่ไม่ใช่ผู้พัฒนาโปรแกรม เมื่อมีการพัฒนาหรือแก้ไขเปลี่ยนแปลงระบบงาน IT ที่มีนัยสำคัญ และมีความเสี่ยงด้านความมั่นคงปลอดภัย เพื่อให้สามารถระบุข้อบกพร่องด้านความมั่นคงปลอดภัย และแก้ไขก่อนนำระบบไปใช้งานจริง

ข้อกำหนด	แนวปฏิบัติ
(5) ควรมีการทดสอบระบบงาน IT ที่ได้รับการพัฒนาหรือแก้ไขเปลี่ยนแปลง เพื่อให้มั่นใจได้ว่าระบบดังกล่าวสามารถประมวลผลได้อย่างถูกต้องครบถ้วน และเป็นไปตามความต้องการของผู้ใช้งาน	<u>การทดสอบระบบ</u> 1. สำนักงานสอบบัญชีควรจัดให้มีการทดสอบระบบก่อนนำไปใช้งานหรือให้บริการจริง เพื่อให้มั่นใจได้ว่าระบบดังกล่าวสามารถทำงานได้อย่างถูกต้อง ปลอดภัย มีประสิทธิภาพ และเป็นไปตามความต้องการของผู้ใช้งาน โดยควรครอบคลุมเนื้อหาอย่างน้อยในเรื่องดังต่อไปนี้ (1) การทดสอบการทำงานของแต่ละหน่วย (unit test) (2) การทดสอบการทำงานของระบบและการเชื่อมต่อ (system and integration test) (3) การทดสอบความต้องการของผู้ใช้งาน (user acceptance test) (4) การทดสอบการรักษาความปลอดภัย (security test) ได้แก่ การประเมินช่องโหว่ (vulnerabilities assessment) และการทดสอบการเจาะระบบ (penetration test) ตามความจำเป็น สำหรับระบบใหม่ใด ๆ ที่มีการเชื่อมต่อกับระบบงาน IT ที่มีนัยสำคัญ เพื่อให้สามารถตรวจพบช่องโหว่และดำเนินการปรับปรุงแก้ไขอย่างเหมาะสมก่อนเริ่มให้บริการจริง 2. สำนักงานสอบบัญชีควรกำหนดสถานการณ์ที่ใช้ทดสอบ (test scenario) หรือกรณีที่ใช้ทดสอบ (test case) แบบ end-to-end และมีกระบวนการสอบทาน test scenario หรือ test case เพื่อให้มั่นใจว่ามีความครอบคลุมเพียงพอและตรงกับความต้องการของสำนักงานสอบบัญชี 3. สำนักงานสอบบัญชีควรทดสอบระบบบนสภาพแวดล้อม (test environment) ที่ใกล้เคียงระบบที่ให้บริการจริง เพื่อลดความเสี่ยงที่อาจเกิดขึ้นจากการเปลี่ยนแปลงบนระบบงานที่ให้บริการจริง 4. สำนักงานสอบบัญชีควรมีการจัดการข้อบกพร่อง (defect) ของระบบที่พบในการทดสอบ โดยพิจารณาแนวทางปรับปรุง หรือลดความเสี่ยงและผลกระทบของข้อบกพร่องดังกล่าว 5. สำนักงานสอบบัญชีควรมีการขออนุมัติผลการทดสอบจากฝ่ายงานที่เกี่ยวข้อง ก่อนนำระบบขึ้นใช้งานจริง
(6) ควรมีมาตรการควบคุมความถูกต้องครบถ้วนของการแปลงข้อมูล (data conversion)	1. มาตรการควบคุมความถูกต้องครบถ้วนของการแปลงข้อมูล (data conversion) ควรครอบคลุมกรณีที่มีการโอนย้ายข้อมูลจากระบบเดิมไปยังระบบใหม่ (data migration) เช่น การทำ storage migration, cloud migration หรือ application migration เป็นต้น
(7) ควรมีมาตรการรักษาความมั่นคงปลอดภัย และความลับของข้อมูลสำคัญที่นำไปใช้ในการทดสอบ	1. กรณีที่มีการนำข้อมูลสำคัญจากระบบจริงมาใช้เพื่อทดสอบระบบ สำนักงานสอบบัญชีควรจัดให้มีแนวทางการรักษาความปลอดภัยและความลับของข้อมูลดังกล่าว เช่น การทำ data masking เป็นต้น เพื่อป้องกันความเสี่ยงในการรั่วไหลของข้อมูล
(8) ในกรณีที่มีการมอบให้มอบหมายให้บุคคลภายนอกเป็นผู้พัฒนาหรือแก้ไขเปลี่ยนแปลงระบบงาน IT สำนักงานสอบบัญชีควรจัดให้มีการติดตาม และควบคุม	[ไม่มีการกำหนดแนวปฏิบัติไว้เป็นการเฉพาะ]

ข้อกำหนด	แนวปฏิบัติ
การดำเนินการให้ไปตามข้อตกลงในการมอบหมายงาน	
(9) ควรมีกระบวนการขออนุมัติหัวหน้าสำนักงานสอบบัญชี หรือคณะกรรมการบริหารของสำนักงานสอบบัญชีก่อนนำระบบขึ้นใช้งานจริง	<u>การนำระบบขึ้นใช้งานจริง</u> 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) และแนวปฏิบัติเรื่องการพัฒนาระบบ
(1) ควรมีการประเมินผลกระทบ และจัดลำดับความสำคัญของการเปลี่ยนแปลง	[ไม่มีการกำหนดแนวปฏิบัติไว้เป็นการเฉพาะ]
(2) ควรมีกระบวนการขออนุมัติการเปลี่ยนแปลง (change request) โดยได้รับการอนุมัติจากหน่วยงานเจ้าของระบบ (system owner) เป็นลายลักษณ์อักษร เพื่อให้มั่นใจได้ว่าการเปลี่ยนแปลงได้รับการพิจารณาความจำเป็นอย่างเหมาะสมแล้ว	[ไม่มีการกำหนดแนวปฏิบัติไว้เป็นการเฉพาะ]
(3) ควรมีการทดสอบระบบก่อนนำไปตั้งค่า หรือนำไปติดตั้งบนระบบที่ให้บริการจริง เพื่อลดความเสี่ยงและผลกระทบที่อาจเกิดขึ้น	[ไม่มีการกำหนดแนวปฏิบัติไว้เป็นการเฉพาะ]
(4) ควรมีกระบวนการขออนุมัติจากหัวหน้าสำนักงานสอบบัญชี หรือคณะกรรมการบริหารของสำนักงานสอบบัญชีก่อนนำระบบขึ้นใช้งานจริง	[ไม่มีการกำหนดแนวปฏิบัติไว้เป็นการเฉพาะ]

ข้อกำหนด	แนวปฏิบัติ
(5) ควรมีกระบวนการหรือเครื่องมือควบคุมการเปลี่ยนแปลงรุ่น (version) ของชุดคำสั่งคอมพิวเตอร์ (source code version control) และรองรับการถอยกลับสู่สภาพเดิม (fallback)	[ไม่มีการกำหนดแนวปฏิบัติไว้เป็นการเฉพาะ]
(6) ควรปรับปรุงรายละเอียดประกอบระบบงานที่ได้มีการแก้ไขเปลี่ยนแปลงให้เป็นปัจจุบัน	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) สำนักงานสอบบัญชีควรมีการบริหารจัดการเหตุการณ์ผิดปกติด้าน IT อย่างเหมาะสมและทันท่วงที ดังนี้	
11.1 ควรจัดให้มีช่องทางรับแจ้งเหตุการณ์ผิดปกติด้าน IT จากบุคลากร ผู้ใช้บริการ และผู้ที่เกี่ยวข้อง	1. สำนักงานสอบบัญชีควรจัดให้มีหน่วยงานหรือบุคลากรที่มีหน้าที่รับแจ้งเหตุการณ์ (point of contact) โดยทำหน้าที่ในการบันทึกข้อมูลแก้ไขในเบื้องต้น หรือส่งต่อเหตุการณ์ผิดปกติไปยังหน่วยงานด้าน IT ที่เกี่ยวข้อง
11.2 ควรกำหนดแผน หรือขั้นตอนการบริหารจัดการเหตุการณ์ผิดปกติด้าน IT	1. สำนักงานสอบบัญชีควรจัดให้มีแผนการบริหารจัดการ หรือแผนการรับมือกับเหตุการณ์ผิดปกติ (incident response plan) ตามความสำคัญของเหตุการณ์ เพื่อให้สามารถรับมือและตอบสนองต่อเหตุการณ์ได้อย่างรวดเร็วและทันการณ์ โดยควรครอบคลุมเนื้อหาอย่างน้อยในเรื่องดังต่อไปนี้ (1) การตรวจสอบความถูกต้องของข้อมูลที่ได้รับแจ้ง (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) และรายงานความคืบหน้าของเหตุการณ์ต่อหัวหน้าสำนักงานสอบบัญชี และคณะกรรมการของสำนักงานสอบบัญชีให้รับทราบ ตามระดับความรุนแรงของเหตุการณ์ (5) การแจ้งหรือสื่อสารลูกค้า โดยกำหนดผู้รับผิดชอบในการสื่อสารไปยังลูกค้า และช่องทางการสื่อสาร เพื่อให้ลูกค้ารับทราบ

ข้อกำหนด	แนวปฏิบัติ
	ผลกระทบ และความคืบหน้าการแก้ไขเหตุการณ์ผิดปกติ (6) การตรวจพิสูจน์พยานหลักฐานทางดิจิทัล (digital forensic) ในกรณีภัยคุกคามทางไซเบอร์ซึ่งส่งผลกระทบอย่างมีนัยสำคัญต่อทรัพย์สินและข้อมูลของลูกค้า โดยผู้ที่มีความเชี่ยวชาญเพื่อให้ทราบสาเหตุหรือช่องโหว่ของระบบ และสามารถดำเนินการปิดช่องโหว่ได้อย่างปลอดภัย
11.3 ควรรายงานเหตุการณ์ผิดปกติด้าน IT เหตุการณ์การละเมิดต่อข้อมูลส่วนบุคคล และเหตุการณ์ที่ส่งผลให้ทรัพย์สินของผู้ใช้งานเสียหายอันเกิดจากเหตุการณ์ด้านความมั่นคงปลอดภัยของระบบงาน IT ต่อผู้มีหน้าที่รับผิดชอบเหตุการณ์ และหน่วยงานที่เกี่ยวข้องโดยไม่ชักช้า ตามที่กฎหมายกำหนด เช่น สำนักงาน ก.ล.ต. และ สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เป็นต้น	1. สำนักงานสอบบัญชีควรรายงานเหตุการณ์ที่มีการละเมิดกฎหมาย กฎ และระเบียบที่เกี่ยวข้องกับสำนักงานสอบบัญชี ต่อหน่วยงานที่เกี่ยวข้องโดยไม่ชักช้า ตามที่กฎหมายกำหนด เช่น มาตรา 37 (4) แห่ง พรบ. คุ้มครองข้อมูลส่วนบุคคลฯ แจ้งให้รายงานเหตุการณ์ละเมิดข้อมูลส่วนบุคคลแก่สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลภายใน 72 ชั่วโมงนับแต่ทราบเหตุเท่าที่สามารถกระทำได้ ทั้งนี้ การแจ้งดังกล่าวและข้อยกเว้นให้เป็นไปตามหลักเกณฑ์และวิธีการที่คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลประกาศกำหนด เป็นต้น รวมทั้ง สำนักงานสอบบัญชีควรรายงานเหตุการณ์ดังกล่าวแก่สำนักงาน ก.ล.ต. ภายใน 72 ชั่วโมงนับแต่ทราบเหตุเท่าที่สามารถกระทำได้ด้วยเช่นกัน 2. สำนักงานสอบบัญชีควรรายงานสำนักงาน ก.ล.ต. ในกรณีที่มีเหตุการณ์ด้าน IT ซึ่งอาจส่งผลกระทบต่อการดำเนินงาน ธุรกิจ ชื่อเสียง ฐานะ ผลการดำเนินงานของสำนักงานสอบบัญชี หรือลูกค้าในวงกว้าง โดยควรครอบคลุมเหตุการณ์อย่างน้อยในเรื่องดังต่อไปนี้ (1) การละเมิดต่อข้อมูลส่วนบุคคลที่เกิดจากเหตุการณ์ผิดปกติด้าน IT (2) ทรัพย์สินของผู้ใช้งานสูญหาย หรือเสียหาย (3) การบุกรุก เข้าถึง หรือใช้งานระบบโดยไม่ได้รับอนุญาต (system compromised) (4) เหตุการณ์ที่ส่งผลกระทบต่อชื่อเสียงของสำนักงานสอบบัญชี (harm to reputation) เช่น ถูกปลอมแปลงหน้าเว็บไซต์ของบริษัท (website defacement) เป็นต้น 3. สำนักงานสอบบัญชีควรรายงานเหตุการณ์ต่อสำนักงาน ก.ล.ต. ภายในกรอบระยะเวลา ดังนี้ (1) ควรรายงานโดยไม่ชักช้า ภายใน 72 ชั่วโมงนับแต่ทราบเหตุเท่าที่สามารถกระทำได้ โดยมีเนื้อหาครอบคลุมถึงวันเวลา ประเภทเหตุการณ์ เหตุการณ์ และผลกระทบที่คาดว่าจะเกิดขึ้น ทั้งนี้ สามารถแจ้งโดยวาจาหรือรายงานผ่านช่องทางอิเล็กทรอนิกส์ตามที่สำนักงาน ก.ล.ต. กำหนดตามความเหมาะสม (2) ควรรายงานความคืบหน้าเป็นลายลักษณ์อักษรทุก ๆ 14 วัน หรือ ตามความเหมาะสมจนกว่าระบบงาน IT จะกลับสู่การให้บริการได้อย่างเป็นปกติ โดยมีเนื้อหาครอบคลุมถึงวันเวลา ประเภทเหตุการณ์ เหตุการณ์ ผลกระทบที่เกิดขึ้น และความคืบหน้าในการแก้ไขปัญหา ทั้งนี้ ให้รายงานผ่านช่องทางอิเล็กทรอนิกส์ที่สำนักงาน ก.ล.ต. กำหนด (auditoversight@sec.or.th)

ข้อกำหนด	แนวปฏิบัติ
	(3) ควรรายงานเมื่อเหตุการณ์ยุติหรือแก้ไขปัญหาแล้วเสร็จ โดยมีเนื้อหาครอบคลุมถึงวันเวลา ประเภทเหตุการณ์ เหตุการณ์ ผลกระทบที่เกิดขึ้น การดำเนินการแก้ไขปัญหา ผลการแก้ไขปัญหา ระยะเวลาในการแก้ไข สาเหตุที่เกิดปัญหา และแนวทางป้องกันในอนาคต ทั้งนี้ ให้รายงานผ่านช่องทางอิเล็กทรอนิกส์ที่สำนักงาน ก.ล.ต. กำหนด (auditoversight@sec.or.th)
11.4 ควรวิเคราะห์สาเหตุที่แท้จริง (root cause) ของเหตุการณ์ผิดปกติด้าน IT เพื่อกำหนดแนวทางการแก้ไขและป้องกันไม่ให้เกิดเหตุการณ์ซ้ำในอนาคต	1. สำนักงานสอบบัญชีควรวิเคราะห์สาเหตุที่แท้จริงของเหตุการณ์ และนำบทเรียน (lesson learned) จากเหตุการณ์ไปป้องกันไม่ให้เกิดเหตุการณ์นี้อีกในอนาคต หรือปรับปรุงกระบวนการรับมือเหตุการณ์ผิดปกติให้มีประสิทธิภาพดีขึ้น
11.5 ควรบันทึกข้อมูลที่เกี่ยวข้องกับการบริหารจัดการเหตุการณ์ผิดปกติด้าน IT และจัดเก็บข้อมูลดังกล่าวเป็นระยะเวลาไม่น้อยกว่า 5 ปีนับแต่วันที่เกิดเหตุการณ์นั้น โดยควรจัดเก็บไว้ในลักษณะที่พร้อมให้สำนักงาน ก.ล.ต. สามารถเรียกดูและตรวจสอบได้โดยไม่ชักช้า	1. สำนักงานสอบบัญชีควรจัดเก็บบันทึกข้อมูลเหตุการณ์ที่เกิดขึ้นในรูปแบบที่เป็นมาตรฐาน และมีเนื้อหาขั้นต่ำประกอบด้วย วันเวลาที่เกิดเหตุการณ์ รายละเอียดเหตุการณ์ ผลกระทบ วิธีการแก้ไข วันเวลาที่สิ้นสุดเหตุการณ์ สาเหตุที่เกิดปัญหา และแนวทางการป้องกันในอนาคต โดยจัดเก็บข้อมูลดังกล่าวเป็นระยะเวลาไม่น้อยกว่า 5 ปีนับแต่วันที่เกิดเหตุการณ์นั้น โดยควรจัดเก็บไว้ในลักษณะที่พร้อมให้สำนักงาน ก.ล.ต. สามารถเรียกดูและตรวจสอบได้โดยไม่ชักช้า
11.6 ควรทดสอบและทบทวนขั้นตอนปฏิบัติหรือแผนการบริหารจัดการเหตุการณ์ผิดปกติด้าน IT อย่างน้อยปีละ 1 ครั้ง โดยควรครอบคลุมถึงการทดสอบการบริหารจัดการเหตุการณ์ด้านภัยคุกคามทางไซเบอร์ (cyber security drill) และควรจัดให้มีการรายงานผลการทดสอบและทบทวนต่อหัวหน้าสำนักงานสอบบัญชี หรือคณะกรรมการบริหารของสำนักงานสอบบัญชี	1. สำนักงานสอบบัญชีควรทดสอบและทบทวนขั้นตอนปฏิบัติหรือแผนการบริหารจัดการเหตุการณ์ผิดปกติ อย่างน้อยปีละ 1 ครั้ง เพื่อให้สามารถจัดการแก้ไขเหตุการณ์ให้กลับสู่สภาพปกติได้อย่างรวดเร็วและจำกัดความเสียหายที่ส่งผลกระทบต่อธุรกิจ โดยควรดำเนินการดังนี้ (1) ควรจัดให้มีการจำลองสถานการณ์เสี่ยง (risk scenario) ด้านเหตุการณ์ภัยคุกคามทางไซเบอร์ที่มีความเป็นไปได้ที่จะเกิดขึ้น สอดคล้องกับลักษณะ ขอบเขต และความซับซ้อนในการประกอบธุรกิจ และสอดคล้องกับแนวโน้มภัยคุกคามไซเบอร์ที่อาจเกิดขึ้นกับสำนักงานสอบบัญชีโดยสถานการณ์ดังกล่าวควรเป็นสถานการณ์ที่เกิดขึ้นแล้วส่งผลกระทบต่อระบบงาน IT อย่างมีนัยสำคัญ (2) ควรจัดเก็บเอกสารที่เกี่ยวข้องกับการทดสอบให้ครบถ้วนและเป็นปัจจุบัน ดังนี้ (2.1) สถานการณ์ความเสี่ยง (risk scenario) รูปแบบการทดสอบ วัน เวลา สถานที่ในการทดสอบ บทบาทหน้าที่ของผู้ที่เกี่ยวข้องที่ใช้ในการทดสอบ (2.2) สรุปผลการทดสอบ และผลการทบทวนขั้นตอนการบริหารจัดการเหตุการณ์ (3) ควรจัดให้มีการรายงานผลการทดสอบและทบทวนต่อหัวหน้าสำนักงานสอบบัญชี หรือคณะกรรมการบริหารของสำนักงานสอบบัญชี

ข้อกำหนด	แนวปฏิบัติ
2.12 แผนฉุกเฉินด้าน IT (IT contingency plan)	
ส่วนที่ 12 แผนฉุกเฉินด้าน IT (IT contingency plan) สำนักงานสอบบัญชีควรจัดให้มีแผนฉุกเฉินด้าน IT เพื่อรองรับเหตุการณ์ผิดปกติด้าน IT ซึ่งส่งผลกระทบให้ไม่สามารถใช้งานได้ตามปกติ หรือไม่สามารถดำเนินธุรกิจอย่างต่อเนื่อง โดยควรกู้คืนระบบให้กลับคืนสู่สภาพปกติภายในระยะเวลาที่เหมาะสมได้ ดังนี้	
12.1 ควรจัดให้มีคณะทำงานหรือหน่วยงานที่รับผิดชอบในการจัดทำแผนฉุกเฉินด้าน IT	1. สำนักงานสอบบัญชีควรจัดให้มีคณะทำงานหรือหน่วยงานที่รับผิดชอบในการจัดทำแผนฉุกเฉินด้าน IT ไว้อย่างเป็นลายลักษณ์อักษร โดยมีผู้บริหารและบุคลากรของหน่วยงานด้านต่าง ๆ ที่เกี่ยวข้องเข้าร่วมด้วย เช่น ด้าน IT ด้านธุรกิจ และด้านสื่อสารองค์กร เป็นต้น
12.2 กระบวนการจัดทำแผนฉุกเฉินด้าน IT โดยควรครอบคลุมเนื้อหาอย่างน้อยในเรื่องดังต่อไปนี้ 12.2.1 ควรประเมินความเสี่ยง (risk analysis) เพื่อให้สามารถระบุเหตุการณ์ความเสี่ยงที่อาจทำให้กระบวนการและระบบงาน IT หยุดชะงัก ไม่สามารถให้บริการได้ตามปกติ หรือไม่สามารถดำเนินธุรกิจอย่างต่อเนื่อง	1. สำนักงานสอบบัญชีควรประเมินความเสี่ยง (risk analysis) เพื่อให้สามารถระบุเหตุการณ์ความเสี่ยงซึ่งส่งผลกระทบต่อการหยุดชะงักของกระบวนการและระบบงาน IT โดยมีแนวทางดำเนินการ ดังนี้ (1) ควรระบุเหตุการณ์ความเสี่ยง (risk scenarios) ที่อาจทำให้กระบวนการและระบบงาน IT หยุดชะงัก ทั้งจากภายในและภายนอก เช่น การโจมตีด้านไซเบอร์ ไฟไหม้ เป็นต้น (2) ควรประเมินความเสี่ยงโดยพิจารณาผลกระทบและโอกาสที่จะเกิดขึ้น รวมถึงการควบคุมที่มีอยู่ (3) ควรจัดให้มีกระบวนการและทรัพยากรที่จำเป็นในการควบคุมความเสี่ยงให้อยู่ในระดับที่ยอมรับได้
12.2.2 ควรวิเคราะห์ผลกระทบทางธุรกิจ (business impact analysis) จากเหตุการณ์ความเสี่ยงตาม 12.2.1 เพื่อกำหนดระยะเวลาเป้าหมายในการกู้คืนระบบงาน IT (Recovery Time Objective : RTO) ระยะเวลาเป้าหมายสูงสุดที่ยอมให้ข้อมูลเสียหาย (Recovery Point Objective : RPO) และระยะเวลาสูงสุดที่ยอมให้กระบวนการทางธุรกิจหยุดชะงัก (Maximum Tolerable Downtime : MTD) อย่างเหมาะสม	1. สำนักงานสอบบัญชีควรวิเคราะห์ผลกระทบทางธุรกิจ (business impact analysis) เพื่อให้ทราบถึงความสำคัญของระบบงาน IT ที่มีผลต่อการดำเนินธุรกิจ โดยมีแนวทางการดำเนินการ ดังนี้ (1) ควรระบุรายการกระบวนการทางธุรกิจ (business process) และระบบงาน IT ที่กระบวนการทางธุรกิจพึ่งพา (2) ควรวิเคราะห์ผลกระทบที่เกิดจากการหยุดชะงักของระบบงาน IT เพื่อกำหนดระยะเวลา RTO, RPO และ MTD ตามความเหมาะสม (3) ควรระบุระบบงาน IT และทรัพยากรที่จำเป็นต่อกระบวนทางธุรกิจที่สำคัญ (ฮาร์ดแวร์ ซอฟต์แวร์ ข้อมูล และทรัพยากรอื่น ๆ) พร้อมทั้งรายละเอียดคุณสมบัติ (specification) ขั้นต่ำของระบบงาน IT และทรัพยากรดังกล่าว (4) ควรจัดลำดับความสำคัญของระบบงาน IT เพื่อให้ระบบงาน IT ที่สนับสนุนกระบวนการทางธุรกิจที่สำคัญสูงได้รับการกู้คืนเป็นลำดับแรก

ข้อกำหนด	แนวปฏิบัติ
12.2.3 ควรจัดทำแผนฉุกเฉินด้าน IT อย่างเป็นลายลักษณ์อักษร ซึ่งได้รับความเห็นชอบจากหัวหน้าสำนักงานสอบบัญชี หรือคณะกรรมการบริหารของสำนักงานสอบบัญชี	1. สำนักงานสอบบัญชีควรจัดให้มีแผนฉุกเฉินด้าน IT ที่ได้รับความเห็นชอบจากหัวหน้าสำนักงานสอบบัญชี หรือคณะกรรมการบริหารของสำนักงานสอบบัญชีซึ่งมีรายละเอียดของกระบวนการหรือขั้นตอนการปฏิบัติงานที่ชัดเจน เพื่อให้สามารถดำเนินการได้อย่างรวดเร็วและง่ายต่อการปฏิบัติ โดยควรครอบคลุมเนื้อหาอย่างน้อยในเรื่องดังต่อไปนี้ (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
12.3 ควรจัดให้มีระบบงาน IT สำรอง และทรัพยากรที่จำเป็น เพื่อให้สามารถกู้คืนระบบได้ตามระยะเวลาเป้าหมายที่กำหนดไว้	1. สำนักงานสอบบัญชีควรจัดให้มีระบบงาน IT สำรอง และทรัพยากรที่จำเป็นเพื่อให้สามารถกู้คืนระบบงาน IT ได้ตามระยะเวลาเป้าหมายที่กำหนดไว้ โดยกรณีที่สำนักงานสอบบัญชีมีศูนย์คอมพิวเตอร์สำรอง ควรระบุรายละเอียดเกี่ยวกับศูนย์คอมพิวเตอร์สำรองให้ชัดเจน เช่น ทรัพยากรที่มี สถานที่ตั้งและแผนที่ เป็นต้น
12.4 ควรสื่อสารให้บุคลากรที่เกี่ยวข้องมีความเข้าใจและสามารถปฏิบัติตามแผนฉุกเฉินด้าน IT อย่างเหมาะสม	1. สำนักงานสอบบัญชีควรสื่อสารแผนฉุกเฉินด้าน IT ให้พนักงานทุกคนที่มีส่วนเกี่ยวข้องกับการปฏิบัติตามแผนฉุกเฉินด้าน IT มีความเข้าใจ และสามารถปฏิบัติตามแผนได้อย่างถูกต้อง
12.5 ควรทบทวนและทดสอบการปฏิบัติตามแผนฉุกเฉินด้าน IT อย่างน้อยปีละ 1 ครั้ง และเมื่อมีเหตุจำเป็นที่ควรได้รับการทบทวนและทดสอบดังกล่าว โดยรายงานผลการทบทวนและทดสอบต่อหัวหน้า	1. สำนักงานสอบบัญชีควรทบทวน (review) และทดสอบ (test) การปฏิบัติตามแผนฉุกเฉินด้าน IT อย่างน้อยปีละ 1 ครั้ง และเมื่อมีเหตุจำเป็นที่ควรได้รับการทดสอบและทบทวนดังกล่าว เช่น มีการเปลี่ยนแปลงกลยุทธ์ทางธุรกิจ นโยบายการบริหารความเสี่ยงโดยรวม สภาพแวดล้อมของการให้บริการหรือดำเนินธุรกิจ ทรัพยากร หรือโครงสร้างระบบงาน IT เป็นต้น 2. สำนักงานสอบบัญชีควรกำหนดเหตุการณ์ที่ใช้ในการทดสอบประจำปี (test scenario) โดยเป็นเหตุการณ์ที่มีโอกาสที่จะเกิดขึ้นและ

ข้อกำหนด	แนวปฏิบัติ
สำนักงานสอบบัญชี หรือคณะกรรมการบริหารของสำนักงานสอบบัญชี	อาจส่งผลกระทบให้กระบวนการทางธุรกิจที่สำคัญหยุดชะงัก เช่น การหยุดชะงักของระบบงาน IT ที่สนับสนุนกระบวนการทางธุรกิจที่สำคัญ การหยุดชะงักของผู้ให้บริการภายนอกที่สำคัญ (รวมถึงผู้ให้บริการคลาวด์) และการโจมตีทางไซเบอร์ เป็นต้น 3. สำนักงานสอบบัญชีควรรายงานผลการทดสอบแผนฉุกเฉินด้าน IT ต่อหัวหน้าสำนักงานสอบบัญชี หรือคณะกรรมการบริหารของสำนักงานสอบบัญชีโดยควรมีรายละเอียดอย่างน้อยครอบคลุมวัตถุประสงค์ ขอบเขตการทดสอบสถานการณ์จำลอง ผลการทดสอบ ข้อผิดพลาดและปัญหาหรืออุปสรรคที่พบ พร้อมทั้งแนวทางปรับปรุงแก้ไข
12.6 ควรจัดให้มีรายละเอียดในการติดต่อดังนี้ เพื่อให้สามารถประสานงานในการรายงานเหตุการณ์ผิดปกติด้าน IT หรือขอความช่วยเหลือจากหน่วยงานภายนอกที่เกี่ยวข้องได้อย่างมีประสิทธิภาพ โดยควรปรับปรุงข้อมูลดังกล่าวให้เป็นปัจจุบันอยู่เสมอ 12.6.1 รายชื่อหน่วยงานกำกับดูแลและบุคคลภายนอกที่ให้บริการหรือที่มีการเชื่อมต่อกับระบบงาน IT ของสำนักงานสอบบัญชี 12.6.2 ช่องทางในการติดต่อ และรายชื่อผู้ที่เกี่ยวข้องของหน่วยงานกำกับดูแลหรือบุคคลภายนอกตาม 12.6.1	[ไม่มีการกำหนดแนวปฏิบัติไว้เป็นการเฉพาะ]

หมวดที่ 3 การตรวจสอบด้านเทคโนโลยีสารสนเทศ (Information Technology Audit)

ให้สำนักงานสอบบัญชีดำเนินการตามที่กำหนดในภาคผนวกนี้

ข้อกำหนด	แนวปฏิบัติ
1. <u>การจัดให้มีผู้ตรวจสอบ</u> ผู้ตรวจสอบอาจเป็นได้ทั้งผู้ตรวจสอบภายในที่สังกัดสำนักงานสอบบัญชี หรือผู้ตรวจสอบจากภายนอก ซึ่งมีคุณสมบัติ ดังนี้ 1.1 มีความเป็นอิสระจากผู้ทำหน้าที่ด้าน IT ในระดับ ดังนี้ 1.1.1 ระดับที่ 1 (first line of defense) : การปฏิบัติงาน 1.1.2 ระดับที่ 2 (second line of defense) : การบริหารความเสี่ยงในการปฏิบัติงานทางด้าน IT 1.2 หัวหน้าทีมผู้ตรวจสอบที่เป็นผู้รับผิดชอบต่อผลการตรวจสอบด้านเทคโนโลยีสารสนเทศ (“ผลการตรวจสอบด้าน IT”) ควรเป็นผู้มีความรู้ความสามารถ เช่น ผ่านการรับรองและมีวุฒิบัตรอย่างหนึ่งอย่างใด ซึ่งยังไม่สิ้นผล ดังนี้ 1.2.1 Certified Information Systems Auditor (CISA) 1.2.2 Certified Information Security Manager (CISM) 1.2.3 Certified Information Systems Security Professional (CISSP) 1.2.4 ISO/IEC 27001 Lead Auditor	[ไม่มีการกำหนดแนวปฏิบัติไว้เป็นการเฉพาะ]
2. <u>การตรวจสอบด้าน IT ตามแผนงานและขอบเขตที่กำหนด</u> 2.1 ควรจัดให้มีการตรวจสอบด้าน IT อย่างสม่ำเสมอให้เหมาะสมตามความเสี่ยงด้านเทคโนโลยีสารสนเทศที่สำนักงานสอบบัญชีประเมินได้ โดยควรมีการตรวจสอบอย่างน้อยหนึ่งครั้งในรอบระยะเวลา 3 ปี สำหรับสำนักงานสอบบัญชีที่มีความเสี่ยงด้านเทคโนโลยีสารสนเทศสูงอาจจำเป็นต้องพิจารณาเพิ่มความถี่ในการตรวจสอบด้าน IT ตามความเหมาะสม 2.2 ควรจัดเก็บรายงานผลการตรวจสอบเพื่อแสดงต่อสำนักงาน ก.ล.ต. เป็นระยะเวลาไม่น้อยกว่า 5 ปี	[ไม่มีการกำหนดแนวปฏิบัติไว้เป็นการเฉพาะ]
3. <u>กรณีผลการตรวจสอบดังกล่าวมีข้อสังเกตหรือข้อบกพร่อง</u> สำนักงานสอบบัญชีควรจัดให้มีการวิเคราะห์เชิงลึกถึงสาเหตุของข้อบกพร่อง (“root cause analysis”) และการจัดทำแผนการแก้ไข (“remediation plan”) ข้อบกพร่องหรือข้อสังเกตจากรายงานผลการตรวจสอบด้าน IT และติดตามความคืบหน้าในการดำเนินการตามแผนดังกล่าว	[ไม่มีการกำหนดแนวปฏิบัติไว้เป็นการเฉพาะ]
4. <u>วิธีปฏิบัติสำหรับสำนักงานสอบบัญชีที่มีการรวมศูนย์เทคโนโลยีสารสนเทศไว้ที่ต่างประเทศ หรือมีสำนักงานเครือข่ายในต่างประเทศหรือได้รับการตรวจคุณภาพตามมาตรฐานสากล เช่น ISO/IEC 27001</u> หากสำนักงานสอบบัญชีมีการรวมศูนย์เทคโนโลยีสารสนเทศไว้ที่ต่างประเทศและถูกตรวจสอบโดยสำนักงานเครือข่ายในต่างประเทศ หรือได้รับ	[ไม่มีการกำหนดแนวปฏิบัติไว้เป็นการเฉพาะ]

ข้อกำหนด	แนวปฏิบัติ
การตรวจคุณภาพตามมาตรฐานสากลแล้ว สำนักงานสอบบัญชีสามารถนำข้อมูลจากรายงานผลการตรวจสอบดังกล่าวมาเป็นส่วนประกอบของการตรวจสอบทางด้านเทคโนโลยีสารสนเทศของสำนักงานสอบบัญชีได้ ถ้าการตรวจสอบดังกล่าวมีลักษณะดังนี้ 4.1 ขอบเขตการตรวจสอบครอบคลุมระบบงาน IT ที่เกี่ยวข้องตามมาตรฐานการบริหารคุณภาพ (TSQM1) และไม่น้อยกว่าแนวปฏิบัติในการกำกับดูแลและการตรวจสอบด้านเทคโนโลยีสารสนเทศ (Information Technology) สำหรับสำนักงานสอบบัญชีฉบับนี้ 4.2 ผู้ตรวจสอบมีคุณสมบัติเทียบเคียงได้กับที่ระบุไว้ในแนวปฏิบัติในการกำกับดูแลและการตรวจสอบด้านเทคโนโลยีสารสนเทศ (Information Technology) สำหรับสำนักงานสอบบัญชีฉบับนี้	

คำจำกัดความ

เพื่อวัตถุประสงค์ของแนวปฏิบัติในการกำกับดูแลและการตรวจสอบด้านเทคโนโลยีสารสนเทศ (Information Technology) สำหรับสำนักงานสอบบัญชีฉบับนี้

1. ระบบงานเทคโนโลยีสารสนเทศ หรือ ระบบงาน IT	หมายถึง ทรัพยากรทางเทคโนโลยีของสำนักงานสอบบัญชีที่มีวัตถุประสงค์เกี่ยวข้องกับระบบการบริหารคุณภาพของสำนักงานสอบบัญชี โดยอ้างอิงตามมาตรฐานการบริหารคุณภาพ (TSQM 1) ย่อหน้า 32(ฉ) ก99 ดังนี้ (1) ทรัพยากรทางเทคโนโลยี ซึ่งใช้ในการออกแบบ การนำไปปฏิบัติ หรือการดำเนินการในระบบการบริหารคุณภาพของสำนักงานสอบบัญชีโดยตรง เช่น ระบบ timesheet และ ระบบการประเมินการรับงานสอบบัญชี เป็นต้น (2) ทรัพยากรทางเทคโนโลยี ซึ่งกลุ่มผู้ปฏิบัติงานใช้ในการปฏิบัติงานโดยตรง เช่น Microsoft programs โปรแกรมคำนวณขนาดตัวอย่างในการตรวจสอบ โปรแกรมที่ใช้ในการวิเคราะห์ความสัมพันธ์ของข้อมูล (Data analytics) และระบบที่ใช้ในกระบวนการตรวจสอบและจัดเก็บกระดาษทำการ (Smart Audit Platform) เป็นต้น (3) ทรัพยากรทางเทคโนโลยี ซึ่งจำเป็นในการช่วยทำให้การดำเนินการข้างต้นมีประสิทธิภาพ เช่น เกี่ยวกับระบบงานเทคโนโลยีสารสนเทศ โครงสร้างทางเทคโนโลยีสารสนเทศ และกระบวนการทางเทคโนโลยีสารสนเทศที่ช่วยสนับสนุนระบบงานเทคโนโลยีสารสนเทศ เช่น ระบบปฏิบัติการคอมพิวเตอร์ (Operating system) และ ระบบฐานข้อมูล (Database) เป็นต้น