ตารางสรุปความแตกต่างระหว่างหลักการและร่างประกาศ
สำหรับการแก้ไขประกาศว่าด้วยการให้ความเห็นชอบผู้สอบบัญชีในตลาดทุนในส่วนที่เกี่ยวข้องกับ
การกำหนดให้สำนักงานสอบบัญชีจัดให้มีการกำกับดูแลและการตรวจสอบด้านเทคโนโลยีสารสนเทศโดยผู้เชี่ยวชาญด้านเทคโนโลยีสารสนเทศ

หัวข้อ	หลักการ	ร่างประกาศ/ภาคผนวกแนบท้ายประกาศ	เหตุผลที่ปรับปรุง
ร่างประกาศว่าด้วยการให้ความเห็นชอบผู้สอบบัญชีในตลาดทุน			
1. วันที่มีผลบังคับใช้	สำนักงานสอบบัญชีต้องจัดให้มีการตรวจสอบด้านเทคโนโลยีสารสนเทศอย่างน้อย 1 ครั้ง สำหรับรอบการสอบทานคุณภาพสำนักงานสอบบัญชี ปี 2566 – 2568 หลังจากนั้นต้องจัดให้มีการตรวจสอบตามความถี่ที่สำนักงาน ก.ล.ต. กำหนด โดยอย่างน้อยต้องมีการตรวจสอบระบบ IT ทุก 3 ปี	สำนักงานสอบบัญชีต้องจัดให้มีการตรวจสอบด้านเทคโนโลยีสารสนเทศอย่างน้อย 1 ครั้ง สำหรับรอบการสอบทานคุณภาพสำนักงานสอบบัญชี ปี 2567 – 2569 โดยนำส่งผลการตรวจสอบและเอกสารที่เกี่ยวข้องภายในวันที่ 31 พฤษภาคม 2570 หลังจากนั้นต้องจัดให้มีการตรวจสอบและนำส่งผลการตรวจสอบตามความถี่ที่สำนักงาน ก.ล.ต. กำหนด โดยอย่างน้อยต้องมีการตรวจระบบ IT ทุก 3 ปี และนำส่งรายงานการตรวจสอบภายใน 5 เดือนนับแต่วันสิ้นสุดรอบการตรวจสอบหรือภายในระยะเวลาที่ได้รับการผ่อนผันจากสำนักงาน ทั้งนี้ หากมีการเปลี่ยนแปลงรอบการตรวจสอบให้สำนักงานสอบบัญชีแจ้งการเปลี่ยนแปลงดังกล่าวต่อสำนักงานภายใน 30 วัน	สำนักงาน ก.ล.ต. รับฟังความคิดเห็นจากสำนักงานสอบบัญชีแล้วเห็นควรขยายวันที่มีผลบังคับใช้ออกไป 1 ปี เพื่อให้สำนักงานสอบบัญชีมีเวลาเตรียมตัวอย่างเพียงพอ นอกจากนี้ เห็นควรกำหนดกรอบเวลาในการนำส่งรายงานการตรวจสอบให้ชัดเจน และยืดหยุ่นมากขึ้น โดยเปิดโอกาสให้มีการขอผ่อนผันระยะเวลาการนำส่งรายงานการตรวจสอบได้ รวมทั้งอนุญาตให้สำนักงานสอบบัญชีเปลี่ยนรอบการตรวจสอบได้โดยต้องมีการแจ้งมายังสำนักงานภายในระยะเวลาที่กำหนด

หัวข้อ	หลักการ	ร่างประกาศ/ภาคผนวกแนบท้ายประกาศ	เหตุผลที่ปรับปรุง
ภาคผนวก 1 แนบท้ายประกาศ : การกำกับดูแลและการตรวจสอบด้านเทคโนโลยีสารสนเทศ (Information Technology) สำหรับสำนักงานสอบบัญชี			
2. หมวดที่ 1 เรื่อง การกำกับดูแลและบริหารจัดการด้านเทคโนโลยีสารสนเทศ (Information Technology Governance)	2.1 ไม่ได้กำหนดแนวปฏิบัติที่ชัดเจนสำหรับข้อกำหนดในหัวข้อ “การกำหนดนโยบายที่เกี่ยวข้องกับการกำกับดูแลความเสี่ยงด้าน IT อย่างเป็นลายลักษณ์อักษร” (อ้างอิงหมวดที่ 1 ข้อ 1.1 ส่วนที่ 1 ข้อ 1.3)	2.1 ปรับปรุงภาคผนวกแนบท้ายประกาศในเรื่องดังกล่าวให้ชัดเจนขึ้น โดยมีความยืดหยุ่นเพียงพอที่สำนักงานสอบบัญชีแต่ละแห่งจะสามารถปรับใช้แนวปฏิบัติให้สอดคล้องกับสภาพแวดล้อมของสำนักงานสอบบัญชีแต่ละแห่ง ดังนี้ “<u>ข้อกำหนด</u> 1.3 การกำหนดนโยบายที่เกี่ยวข้องกับการกำกับดูแลความเสี่ยงด้าน IT อย่างเป็นลายลักษณ์อักษร โดยอย่างน้อยต้องครอบคลุมนโยบายที่กำหนดในหมวดที่ 1 ส่วนที่ 2 ข้อ 2.2.1 และ 2.2.2 <u>แนวปฏิบัติ</u> หากสำนักงานสอบบัญชีพิจารณาเรื่องการบริหารจัดการความเสี่ยงด้าน IT ตามหมวดที่ 1 ส่วนที่ 2 ข้อ 2.2.1 แล้วพบว่าสำนักงานสอบบัญชีไม่มีกิจกรรมที่อาจจะก่อให้เกิดความเสี่ยงด้าน IT ในหัวข้อเรื่องที่ระบุไว้ในหมวดที่ 1 ส่วนที่ 2 ข้อ 2.2.2 (2) เฉพาะเรื่องการบริหารจัดการบุคคลภายนอก (6) การควบคุมการเข้ารหัส (cryptographic control)	2.1 ปรับปรุงแนวปฏิบัติให้มีความชัดเจนมากยิ่งขึ้นตามข้อเสนอแนะที่ได้รับจากสำนักงานสอบบัญชี นอกจากนี้ เนื่องจากสำนักงานสอบบัญชีในตลาดทุนมีการใช้ระบบ IT ซึ่งมีความซับซ้อนและความเสี่ยงที่แตกต่างกัน สำนักงาน ก.ล.ต. จึงได้ปรับปรุงหลักเกณฑ์ในการกำกับดูแลและการตรวจสอบด้านเทคโนโลยีสารสนเทศให้มีความยืดหยุ่นมากขึ้น โดยเปิดโอกาสให้สำนักงานสอบบัญชีไม่ต้องปฏิบัติตามข้อกำหนดในบางเรื่องหากประเมินแล้วว่าไม่มีกิจกรรมที่อาจก่อให้เกิดความเสี่ยง ทั้งนี้ สำหรับแนวปฏิบัติข้ออื่นนอกเหนือจากที่ระบุไปข้างต้น สำนักงาน ก.ล.ต. พิจารณาแล้วว่าเป็นการควบคุมพื้นฐานที่ควรจะมีในทุกสำนักงานสอบบัญชีจึงไม่ได้ยกเว้นการกำหนดนโยบายการกำกับดูแลความเสี่ยงด้าน IT ในข้ออื่นนอกเหนือจากที่ระบุไว้

หัวข้อ	หลักการ	ร่างประกาศ/ภาคผนวกแนบท้ายประกาศ	เหตุผลที่ปรับปรุง
		(8) เฉพาะเรื่องการประเมินช่องโหว่ทางเทคนิค (technical vulnerability assessment) (10) การบริหารจัดการโครงการด้าน IT และการจัดหา พัฒนา และบำรุงรักษาระบบงาน IT สำนักงานสอบบัญชีสามารถยกเว้นการกำหนดนโยบายการกำกับดูแลความเสี่ยงด้าน IT ในเรื่องนั้น ๆ ได้ ทั้งนี้ หากสำนักงานสอบบัญชีมีกิจกรรมที่อาจจะก่อให้เกิดความเสี่ยงด้าน IT แต่มีข้อจำกัดในการดำเนินการตามหลักเกณฑ์และแนวปฏิบัติฉบับนี้ สำนักงานสอบบัญชีจำเป็นต้องหาวิธีการควบคุมอื่นทดแทน เพื่อลดระดับความเสี่ยงดังกล่าวให้อยู่ในระดับที่ยอมรับได้ อย่างไรก็ดี สำนักงานสอบบัญชีควรทบทวนความเหมาะสมของนโยบายดังกล่าวทุกปีเพื่อให้สอดคล้องกับความเสี่ยงของสำนักงานสอบบัญชีในปัจจุบัน”	
	2.2 กำหนดให้สำนักงานสอบบัญชีต้องจัดให้มีโครงสร้างการกำกับดูแลและบริหารจัดการความเสี่ยงด้าน IT โดยอย่างน้อยต้องมีลักษณะดังนี้ 2.1.1 ทำให้เกิดการถ่วงดุลอย่างเป็นอิสระ 2.1.2 สอดคล้องตามหลักการแบ่งแยกหน้าที่ 3 ระดับ (3 Lines of Defense: 3 LoDs)	2.2 ได้ปรับปรุงภาคผนวกแนบท้ายประกาศสำหรับนิยามของการทำหน้าที่ด้าน IT ระดับที่ 2 (second line of defense) ดังนี้ “ระดับที่ 2 (second line of defense): การบริหารความเสี่ยงที่เกี่ยวข้องกับระบบงาน IT หมายถึง หน่วยงาน หรือ บุคลากรที่บริหารความเสี่ยงด้าน IT (IT risk function)	2.2 ปรับปรุงแนวคำนิยามให้เหมาะสมกับลักษณะของธุรกิจของสำนักงานสอบบัญชีตามข้อเสนอแนะที่ได้รับจากผู้สอบบัญชีและสำนักงานสอบบัญชี เนื่องจากสำนักงานสอบบัญชีที่มีเครือข่ายในต่างประเทศโดยส่วนใหญ่มีการจัดให้มีการตรวจสอบด้าน IT โดยหน่วยงานเครือข่ายซึ่งหน่วยงานดังกล่าวอาจมีขอบเขตงานครอบคลุมถึงการกำกับ

หัวข้อ	หลักการ	ร่างประกาศ/ภาคผนวกแนบท้ายประกาศ	เหตุผลที่ปรับปรุง
	โดยมีการแบ่งแยกหน้าที่อย่างชัดเจนระหว่างการทำหน้าที่ด้าน IT ดังนี้ ระดับที่ 1 (first line of defense): การปฏิบัติงาน ระดับที่ 2 (second line of defense): การบริหารความเสี่ยงและการกำกับดูแลการปฏิบัติตามกฎหมายและหลักเกณฑ์ที่เกี่ยวข้อง ระดับที่ 3 (third line of defense): การตรวจสอบ โดยกำหนดนิยาม ระดับที่ 2 (second line of defense): การบริหารความเสี่ยงและการกำกับดูแลการปฏิบัติตามกฎหมายและหลักเกณฑ์ที่เกี่ยวข้องว่า หมายถึง <u>หน่วยงานหรือบุคลากรที่บริหารความเสี่ยงด้าน IT และหน่วยงานหรือบุคลากรที่กำกับดูแลการปฏิบัติตามกฎหมายและหลักเกณฑ์ด้าน IT</u> (อ้างอิงหมวดที่ 1 ข้อ 1.2 ส่วนที่ 2 ข้อ 2.1)	มีหน้าที่กำหนดกรอบนโยบาย และกระบวนการบริหารความเสี่ยงด้าน IT สนับสนุนให้มีการประเมินความเสี่ยงเป็นไปตามกรอบการบริหารความเสี่ยงที่กำหนด พร้อมทั้งให้คำปรึกษา ติดตามความเสี่ยง และทบทวนการควบคุมความเสี่ยงด้าน IT ให้อยู่ในระดับความเสี่ยงที่ยอมรับได้ โดยมีการรวบรวมและเชื่อมโยงความเสี่ยงด้าน IT กับ ความเสี่ยงด้านอื่น และนำเสนอผลการบริหารความเสี่ยงต่อหัวหน้าสำนักงานสอบบัญชี หรือคณะกรรมการบริหารของสำนักงานสอบบัญชีที่ได้รับมอบหมาย”	ดูแลการปฏิบัติตามกฎหมายหรือหลักเกณฑ์ที่เกี่ยวข้องด้วย ดังนั้น หากไม่มีการแก้ไขนิยามของระดับที่ 2 (รอบหลักการ) โดยตัดเรื่องการดูแลการปฏิบัติตามกฎหมายหรือหลักเกณฑ์ที่เกี่ยวข้องออก อาจส่งผลให้สำนักงานสอบบัญชีซึ่งมีการตรวจสอบด้าน IT โดยหน่วยงานเครือข่ายอยู่แล้วต้องจ้างบุคคลอื่นมาตรวจสอบด้าน IT เพิ่มเติม ทั้งที่การตรวจสอบด้าน IT ของสำนักงานเครือข่ายดังกล่าวดังกล่าวอาจเป็นไปตามหลักการการแบ่งแยกหน้าที่ที่ทำให้เกิดการถ่วงดุลอย่างเป็นอิสระอยู่แล้ว
3. หมวดที่ 2 เรื่อง การรักษาความมั่นคงปลอดภัยด้านเทคโนโลยี	3.1 ไม่ได้ระบุอย่างชัดเจนในข้อกำหนดว่าบุคลากรภายนอกที่ต้องบริหารจัดการรวมถึง	3.1 ได้ปรับปรุงภาคผนวกแนบท้ายประกาศในเรื่องดังกล่าวให้ชัดเจนขึ้น ดังนี้	3.1 ปรับปรุงเพื่อให้มีความชัดเจนมากยิ่งขึ้นและสอดคล้องกับคำนิยามบุคคลภายนอกตาม TSQM 1 ย่อหน้า 32 (ค) “กลุ่มบุคคล

หัวข้อ	หลักการ	ร่างประกาศ/ภาคผนวกแนบท้ายประกาศ	เหตุผลที่ปรับปรุง
สารสนเทศ (Information Technology Security)	พนักงานของสำนักงานเครือข่ายหรือบริษัทในเครือของสำนักงานสอบบัญชีด้วยหรือไม่ (อ้างอิงหมวดที่ 2 ข้อ 2.2.2 ข้อ 2.2 บุคลากรที่ต้องบริหารจัดการ)	“2.2 บุคคลภายนอก ให้รวมถึงพนักงานของสำนักงานเครือข่ายหรือบริษัทในเครือของสำนักงานสอบบัญชีในกรณีที่สำนักงานสอบบัญชีมีการดำเนินการอย่างใดอย่างหนึ่งดังนี้ • ใช้บริการงานด้าน IT จากบุคคลภายนอก • เชื่อมต่อระบบงาน IT กับบุคคลภายนอก • อนุญาตให้บุคคลภายนอกสามารถเข้าถึงข้อมูลสำคัญหรือข้อมูลของลูกค้าของสำนักงานสอบบัญชีได้”	ที่มาจากแหล่งภายนอก (เช่น เครือข่ายสำนักงานเครือข่ายอื่น หรือผู้ให้บริการ) เมื่อสำนักงานไม่มีบุคลากรเพียงพอหรือเหมาะสมเพื่อสนับสนุนการดำเนินงานของระบบการบริหารคุณภาพของสำนักงานหรือการปฏิบัติงาน”
	3.2 ไม่ได้กำหนดแนวปฏิบัติที่ชัดเจนเกี่ยวกับการโอนย้ายหรือการเข้าถึงข้อมูล ในกรณีที่สำนักงานสอบบัญชีมีการยุติสัญญาหรือข้อตกลงการใช้บริการ cloud service provider (อ้างอิงหมวดที่ 2 ข้อ 2.2.2 ข้อ 2.2 การบริหารจัดการ (6))	3.2 กำหนดแนวปฏิบัติเพิ่มเติมในหัวข้อ “การบริหารจัดการบุคคลภายนอก (third-party management” ที่เกี่ยวข้องกับการโอนย้ายหรือการเข้าถึงข้อมูล ในกรณีที่สำนักงานสอบบัญชีมีการยุติสัญญาหรือข้อตกลงการใช้บริการ cloud service provider ให้ชัดเจน ดังนี้ “หากสำนักงานสอบบัญชีมีการใช้บริการจาก cloud service provider สำนักงานสอบบัญชีต้องกำหนดนโยบายและวิธีปฏิบัติ	3.2 ปรับปรุงแนวปฏิบัติตามข้อเสนอแนะที่ได้รับจากการเปิดรับฟังความคิดเห็น เนื่องจากสำนักงานสอบบัญชีในตลาดทุนหลายแห่งมีการใช้บริการจาก cloud service provider สำนักงาน ก.ล.ต. จึงได้ปรับปรุงแนวปฏิบัติเพื่อให้มั่นใจว่าสำนักงานสอบบัญชีจะสามารถได้รับการโอนย้ายข้อมูลหรือเข้าถึงข้อมูลได้อย่างครบถ้วน ถูกต้องและทันเวลาเมื่อยุติสัญญาหรือข้อตกลงการให้บริการ cloud service provider แล้ว

หัวข้อ	หลักการ	ร่างประกาศ/ภาคผนวกแนบท้ายประกาศ	เหตุผลที่ปรับปรุง
		เพิ่มเติมในเรื่องการโอนย้ายหรือการเข้าถึงข้อมูล เมื่อเกิดการยุติสัญญาหรือข้อตกลงการให้บริการ ทั้งนี้ สำนักงานสอบบัญชีควรกำหนดเงื่อนไขเกี่ยวกับสิทธิในการขอโอนย้ายหรือเข้าถึงข้อมูลดังกล่าวในสัญญาหรือข้อตกลงการให้บริการอย่างเป็นลายลักษณ์อักษร เพื่อให้มั่นใจว่าสำนักงานสอบบัญชีจะสามารถได้รับการโอนย้ายข้อมูลหรือเข้าถึงข้อมูลได้อย่างครบถ้วน ถูกต้องและทันเวลา”	
	3.3 แนวปฏิบัติเกี่ยวกับการรักษาความปลอดภัยสำหรับการปฏิบัติงานจากเครือข่ายภายนอก (teleworking) การใช้งานอุปกรณ์เคลื่อนที่ (mobile device) และการใช้งานอุปกรณ์ส่วนตัว (bring your own device: BYOD) ยังไม่ชัดเจน (อ้างอิงหมวด 2 หัวข้อ 2.8.5 ข้อ 8.5 แนวปฏิบัติข้อ 2 (1))	3.3 เพิ่มคำอธิบายแนวปฏิบัติกรณีใช้งานอุปกรณ์ส่วนตัวให้มีความชัดเจนขึ้น โดยกำหนดเพิ่มเติมเกี่ยวกับการลงทะเบียนอุปกรณ์ที่ต้องมีการอนุมัติโดยผู้มีอำนาจที่เกี่ยวข้องและต้องมีกระบวนการยกเลิกสิทธิ์การใช้งานอุปกรณ์เดิมเมื่อเลิกใช้ โดยกำหนดแนวปฏิบัติไว้ดังนี้ “2. ในการปฏิบัติงานที่มีการใช้อุปกรณ์เคลื่อนที่ (mobile device) เพื่อเข้าถึงระบบงาน IT ที่มีนัยสำคัญ สำนักงานสอบบัญชีควรจัดให้มีมาตรการรักษาความมั่นคงปลอดภัยที่รัดกุมเพียงพอ เหมาะสมกับระบบงาน IT และข้อมูลที่ถูกเข้าถึง เช่น	3.3 ปรับปรุงแนวปฏิบัติตามข้อเสนอแนะที่ได้รับจากการเปิดรับฟังความคิดเห็น

หัวข้อ	หลักการ	ร่างประกาศ/ภาคผนวกแนบท้ายประกาศ	เหตุผลที่ปรับปรุง
		(1) การลงทะเบียนอุปกรณ์เคลื่อนที่ก่อนการใช้งานโดยมีการอนุมัติโดยผู้มีอำนาจที่เกี่ยวข้อง และมีการทบทวนทะเบียนดังกล่าวอย่างน้อยปีละ 1 ครั้ง และเมื่อมีการเปลี่ยนอุปกรณ์ พร้อมทั้งมีการยกเลิกสิทธิการใช้งานของอุปกรณ์เดิม เพื่อให้มั่นใจได้ว่าอุปกรณ์เคลื่อนที่ดังกล่าวมีความความมั่นคงปลอดภัยเพียงพอ ทั้งนี้ สำนักงานสอบบัญชีอาจใช้ระบบหรือเทคโนโลยีการลงทะเบียนอื่นทดแทนได้ หากพิจารณาแล้วเห็นว่าเหมาะสม”	
4. หมวดที่ 3 เรื่อง การตรวจสอบด้านเทคโนโลยีสารสนเทศ (Information Technology Audit)	4.1 กำหนดคุณสมบัติของผู้ตรวจสอบตามประกาศที่ต้องผ่านการรับรองและมีวุฒิบัตรและมีวุฒิบัตรซึ่งยังไม่สิ้นผล อย่างไรก็ดี ยังไม่ได้ระบุอย่างชัดเจนว่าผู้ตรวจสอบต้องเป็นผู้ตรวจสอบจากภายในหรือภายนอกสำนักงานสอบบัญชี (อ้างอิงหมวด 3 หัวข้อ 1 ข้อ 1.1 และ 1.2)	4.1 ปรับปรุงภาคผนวกแนบท้ายประกาศให้มีความชัดเจนมากขึ้น โดยระบุว่าผู้ตรวจสอบอาจเป็นได้ทั้งผู้ตรวจสอบภายนอกหรือผู้ตรวจสอบภายในสำนักงานสอบบัญชีก็ได้ หากมีคุณสมบัติตามที่สำนักงาน ก.ล.ต. กำหนด และหัวหน้าทีมผู้ตรวจสอบที่เป็นผู้รับผิดชอบต่อผลการตรวจสอบด้านเทคโนโลยีสารสนเทศต้องผ่านการรับรองและมีวุฒิบัตรตามประกาศ	4.1 ปรับปรุงข้อกำหนดเกี่ยวกับคุณสมบัติของผู้ตรวจสอบให้มีความชัดเจนและยืดหยุ่นมากขึ้น เพื่อให้สำนักงานสอบบัญชีสามารถปฏิบัติตามประกาศได้อย่างมีประสิทธิภาพและประสิทธิผล

หัวข้อ	หลักการ	ร่างประกาศ/ภาคผนวกแนบท้ายประกาศ	เหตุผลที่ปรับปรุง
	4.2 ข้อกำหนดในการวางแผนและกำหนดขอบเขตการตรวจสอบและการนำส่งรายงานผลการตรวจสอบที่กำหนดไว้เดิมยังไม่ชัดเจนเพียงพอ ดังนี้ “2. การวางแผนและกำหนดขอบเขตการตรวจสอบ: ทบทวนแผนงานและขอบเขตการตรวจสอบให้สอดคล้องกับความเสี่ยงของสำนักงานสอบบัญชี ตามเกณฑ์การประเมินระดับความเสี่ยงด้านเทคโนโลยีสารสนเทศของสำนักงานสอบบัญชี (IT Risk assessment : ITRA)” (อ้างอิงหมวด 3 หัวข้อ 2)	4.2 ข้อกำหนดในการวางแผนและกำหนดขอบเขตการตรวจสอบและการนำส่งรายงานผลการตรวจสอบ กำหนดไว้ ดังนี้ “2. การวางแผนและกำหนดขอบเขตการตรวจสอบ 2.1 ทบทวนแผนงานและขอบเขตการตรวจสอบให้สอดคล้องกับความเสี่ยงของสำนักงานสอบบัญชี ตามผลการประเมินความเสี่ยง (risk assessment) ของสำนักงานสอบบัญชีอย่างน้อยปีละ 1 ครั้ง และเมื่อมีการเปลี่ยนแปลงระบบงาน IT อย่างมีนัยสำคัญ 2.2 สำนักงานสอบบัญชีควรกำหนดรอบการตรวจสอบให้ครอบคลุมระยะเวลาอย่างน้อย 12 เดือน และรอบการตรวจถัดไปควรมีวันที่เริ่มต้นและสิ้นสุดสอดคล้องกับรอบการตรวจครั้งก่อนหน้าที่เคยนำส่งรายงานผลการตรวจสอบระบบงาน IT ให้สำนักงาน ก.ล.ต. ทั้งนี้ กรณีสำนักงานสอบบัญชีมีความประสงค์จะเปลี่ยนแปลงรอบการตรวจในปัจจุบัน สำนักงานสอบบัญชีต้องแจ้งการเปลี่ยนแปลงรอบการตรวจใหม่ภายใน	4.2 ปรับปรุงข้อกำหนดเกี่ยวกับการวางแผนและขอบเขตการตรวจสอบให้ชัดเจนมากยิ่งขึ้น รวมถึงมีการระบุระยะเวลาในการนำส่งรายงานเพื่อเป็นกรอบที่ชัดเจนเพื่อให้สำนักงานสอบบัญชีนำไปปฏิบัติให้เป็นไปในแนวทางเดียวกัน โดยเปิดโอกาสให้สำนักงานสอบบัญชีมีความยืดหยุ่นในการกำหนดกรอบระยะเวลาในการนำส่งรายงานต่อหัวหน้าสำนักงานสอบบัญชีก่อนที่จะนำส่งรายงานดังกล่าวต่อสำนักงาน ก.ล.ต. และเพื่อให้มั่นใจได้ว่าผลการตรวจสอบทางด้าน IT root cause analysis และ remediation plan ที่ได้รับจากสำนักงานสอบบัญชี จะถูกจัดทำด้วยรอบระยะเวลาการตรวจสอบที่เพียงพอที่จะใช้วัดคุณภาพการบริหารทรัพยากรทางเทคโนโลยีของสำนักงานสอบบัญชีอย่างเหมาะสม รวมถึงระบุรายละเอียดของแนวปฏิบัติให้ครอบคลุมกรณีสำนักงานสอบบัญชีมีการเปลี่ยนแปลงรอบการตรวจสอบให้ชัดเจนยิ่งขึ้น

หัวข้อ	หลักการ	ร่างประกาศ/ภาคผนวกแนบท้ายประกาศ	เหตุผลที่ปรับปรุง
		30 วันนับแต่มีการเปลี่ยนแปลง อย่างไรก็ดี หากสำนักงานสอบบัญชีมีการเปลี่ยนแปลงรอบการตรวจสอบใหม่ สำนักงานสอบบัญชีต้องจัดให้มีกระบวนการตรวจสอบเพื่อให้มาซึ่งหลักฐานที่สามารถให้ความเชื่อมั่นว่าระบบทรัพยากรทางเทคโนโลยีตามมาตรฐานการบริหารคุณภาพและการควบคุมที่เกี่ยวข้องระหว่างรอบการตรวจสอบเดิมและรอบการตรวจสอบใหม่ยังคงมีอยู่ และมีประสิทธิภาพ”	
	4.3 ข้อกำหนดในการเสนอรายงานผลการตรวจสอบกำหนดไว้ ดังนี้ “5. การเสนอรายงานผลการตรวจสอบ 5.1 เสนอรายงานผลการตรวจสอบ รวมทั้ง root cause analysis และ remediation plan ต่อหัวหน้าสำนักงานสอบบัญชี หรือคณะกรรมการบริหารของสำนักงานสอบบัญชี ภายใน 30 วัน หลังวันสุดท้ายที่สิ้นสุดการตรวจสอบ 5.2 นำส่งรายงานผลการตรวจสอบ รวมถึง root cause analysis และ remediation	4.3 ปรับปรุงข้อกำหนดในการเสนอรายงานผลการตรวจสอบ ดังนี้ “5. การนำส่งรายงานผลการตรวจสอบและเอกสารที่เกี่ยวข้อง 5.1 เสนอรายงานผลการตรวจสอบระบบงาน IT ที่จัดทำโดยผู้เชี่ยวชาญ รวมทั้ง root cause analysis และ remediation plan กรณีพบข้อสังเกตหรือข้อบกพร่อง รวมถึงผล ITRA ที่ประเมินใหม่ในปีนั้น เพื่อหารอบระยะเวลาถัดไปที่จะตรวจแบบเต็มรูปแบบอีกครั้ง ต่อหัวหน้าสำนักงานสอบบัญชี แล้วนำส่งสำนักงาน ก.ล.ต. ตามรูปแบบและ	4.3 ปรับปรุงข้อกำหนดและแนวปฏิบัติในการนำส่งและการจัดเก็บรายงานผลการตรวจสอบและเอกสารที่เกี่ยวข้องให้ชัดเจนและเหมาะสมมากยิ่งขึ้น

หัวข้อ	หลักการ	ร่างประกาศ/ภาคผนวกแนบท้ายประกาศ	เหตุผลที่ปรับปรุง
	plan ที่ผ่านการพิจารณาจากหัวหน้าสำนักงานสอบบัญชี หรือคณะกรรมการบริหารของสำนักงานสอบบัญชีตาม 5.1 รวมถึง ITRA ที่ประเมินใหม่ในปีนั้น ต่อสำนักงาน ก.ล.ต. ตามรูปแบบและวิธีการที่กำหนดไว้บนเว็บไซต์ของสำนักงาน ก.ล.ต. ภายใน 90 วัน หลังจากวันที่เสนอรายงานและแผนดังกล่าวต่อหัวหน้าสำนักงานสอบบัญชี หรือคณะกรรมการบริหารของสำนักงานสอบบัญชี 5.3 จัดเก็บรายงานผลการตรวจสอบ รวมถึง root cause analysis และ remediation plan เป็นระยะเวลาไม่น้อยกว่า 5 ปี นับแต่วันที่จัดทำรายงานและแผนดังกล่าว โดยต้องจัดเก็บไว้ในลักษณะที่พร้อมให้สำนักงาน ก.ล.ต. สามารถเรียกดูและตรวจสอบได้โดยไม่ชักช้า” (อ้างอิงหมวด 3 หัวข้อ 5)	วิธีการที่กำหนดไว้บนเว็บไซต์ของสำนักงาน ก.ล.ต. ภายใน 5 เดือนนับแต่วันสิ้นสุดรอบการตรวจสอบ 5.2 จัดเก็บเอกสารตาม 5.1 เป็นระยะเวลาไม่น้อยกว่า 5 ปีนับแต่วันที่จัดทำรายงานและแผนดังกล่าว โดยต้องจัดเก็บไว้ในลักษณะที่พร้อมให้สำนักงาน ก.ล.ต. สามารถเรียกดูและตรวจสอบได้โดยไม่ชักช้า”	
	4.4 การขอผ่อนผัน แนวปฏิบัติ : ไม่มีการกำหนดแนวปฏิบัติไว้เป็นการเฉพาะ	4.4 การขอผ่อนผัน “6. การขอผ่อนผัน กรณีมีเหตุผลจำเป็นและสมควรที่ทำให้สำนักงานสอบบัญชีไม่สามารถดำเนินการตรวจสอบระบบงาน IT ได้ภายในรอบ	4.4 เพิ่มแนวปฏิบัติเกี่ยวกับการขอผ่อนผันเพื่อให้เกิดความยืดหยุ่นแก่สำนักงานสอบบัญชีในการปฏิบัติตามประกาศมากยิ่งขึ้น

หัวข้อ	หลักการ	ร่างประกาศ/ภาคผนวกแนบท้ายประกาศ	เหตุผลที่ปรับปรุง
		ระยะเวลาตามที่ผล ITRA ล่าสุดกำหนดไว้ หรือสำนักงานสอบบัญชีไม่สามารถนำส่งเอกสารประกอบการตรวจสอบระบบงาน IT ได้ภายในระยะเวลาตามที่หัวข้อที่ “5. การนำส่งรายงานผลการตรวจสอบและเอกสารที่เกี่ยวข้อง” กำหนด สำนักงานสอบบัญชีต้องยื่นหนังสือขอผ่อนผันการดำเนินการตรวจสอบระบบงาน IT ต่อสำนักงาน ก.ล.ต. ก่อนสิ้นสุดระยะเวลาที่กำหนดให้สำนักงานสอบบัญชีต้องจัดทำและส่งรายงานผลการตรวจสอบและเอกสารที่เกี่ยวข้องให้แก่สำนักงาน ก.ล.ต. อ้างอิงรอบการตรวจปัจจุบัน พร้อมทั้งชี้แจงเหตุผลและความจำเป็นในการขอผ่อนผันและแจ้งกำหนดระยะเวลาใหม่ที่จะดำเนินการตรวจสอบด้าน IT หรือจัดส่งเอกสารนั้น ซึ่งสำนักงาน ก.ล.ต. จะพิจารณาผ่อนผันเป็นรายกรณีตามความจำเป็นและสมควร” (อ้างอิงหมวด 3 หัวข้อ 6)	
	4.5 วิธีปฏิบัติสำหรับสำนักงานสอบบัญชีที่มีการรวมศูนย์เทคโนโลยีสารสนเทศไว้ที่ต่างประเทศ หรือมีสำนักงานเครือข่ายในต่างประเทศหรือได้รับการตรวจคุณภาพตามมาตรฐานสากล	4.5 มีการกำหนดวิธีปฏิบัติสำหรับสำนักงานสอบบัญชีที่มีการรวมศูนย์เทคโนโลยีสารสนเทศไว้ที่ต่างประเทศ หรือมีสำนักงานเครือข่ายในต่างประเทศหรือได้รับการตรวจ	4.5 ปรับปรุงข้อกำหนดตามข้อเสนอแนะที่ได้รับจากการเปิดรับฟังความคิดเห็นให้ชัดเจนและครอบคลุมสำนักงานสอบบัญชีที่มีเครือข่ายต่างประเทศ หรือได้รับ

หัวข้อ	หลักการ	ร่างประกาศ/ภาคผนวกแนบท้ายประกาศ	เหตุผลที่ปรับปรุง
	แนวปฏิบัติ : ไม่มีการกำหนดแนวปฏิบัติไว้เป็นการเฉพาะ	คุณภาพตามมาตรฐานสากล ให้ชัดเจนขึ้น ดังนี้ "9. <u>วิธีปฏิบัติสำหรับสำนักงานสอบบัญชีที่มีการรวมศูนย์เทคโนโลยีสารสนเทศไว้ที่ต่างประเทศ หรือมีสำนักงานเครือข่ายในต่างประเทศหรือได้รับการตรวจคุณภาพตามมาตรฐานสากล เช่น ISO27001</u> หากสำนักงานสอบบัญชีมีการรวมศูนย์เทคโนโลยีสารสนเทศไว้ที่ต่างประเทศและถูกตรวจสอบโดยสำนักงานเครือข่ายในต่างประเทศ หรือได้รับการตรวจคุณภาพตามมาตรฐานสากลแล้ว สำนักงานสอบบัญชีสามารถนำข้อมูลจากรายงานผลการตรวจสอบดังกล่าวมากรอกในแบบรายงานผลการตรวจสอบระบบงานทางด้านเทคโนโลยีสารสนเทศด้าน IT แบบ full-scope ตามที่สำนักงาน ก.ล.ต. กำหนด เพื่อนำส่งสำนักงาน ก.ล.ต. ได้ หากพิจารณาแล้วพบว่าการตรวจสอบดังกล่าวมีลักษณะดังนี้ 9.1 ขอบเขตการตรวจสอบครอบคลุมระบบงาน IT ที่เกี่ยวข้องทั้งหมดตามที่มาตรฐานการบริหารคุณภาพ (TSQM1)	การตรวจคุณภาพตามมาตรฐานสากล เพื่อลดภาระในการตรวจสอบด้าน IT

หัวข้อ	หลักการ	ร่างประกาศ/ภาคผนวกแนบท้ายประกาศ	เหตุผลที่ปรับปรุง
		กำหนด และเทียบเท่าได้กับการกำกับดูแลและการตรวจสอบด้านเทคโนโลยีสารสนเทศ (Information Technology) สำหรับสำนักงานสอบบัญชีฉบับนี้ 9.2 ผู้ตรวจสอบมีคุณสมบัติตามที่ประกาศหรือการกำกับดูแลและการตรวจสอบด้านเทคโนโลยีสารสนเทศ (Information Technology) สำหรับสำนักงานสอบบัญชีฉบับนี้กำหนด 9.3 รอบการตรวจสอบของรายงานดังกล่าวตรงกับรอบการตรวจตามเกณฑ์การประเมินระดับความเสี่ยงด้านเทคโนโลยีสารสนเทศของสำนักงานสอบบัญชี (IT Risk Assessment: ITRA) ตามที่สำนักงาน ก.ล.ต. กำหนด .... ทั้งนี้ หากสำนักงานสอบบัญชีพบว่ารายงานผลการตรวจสอบที่ได้มาจากสำนักงานเครือข่ายในต่างประเทศ หรือจากผู้เชี่ยวชาญที่ตรวจสอบคุณภาพตามมาตรฐานสากล ไม่ครอบคลุมตามหลักเกณฑ์ในการกำกับดูแล IT ฉบับนี้ อนุโลมให้สำนักงานสอบบัญชีดำเนินการตรวจสอบเพิ่มเติมเฉพาะส่วนที่ยังไม่ครบถ้วนตามข้อกำหนดในการกำกับดูแลและการตรวจสอบด้านเทคโนโลยีสารสนเทศ (Information	

หัวข้อ	หลักการ	ร่างประกาศ/ภาคผนวกแนบท้ายประกาศ	เหตุผลที่ปรับปรุง
		Technology) สำหรับสำนักงานสอบบัญชี ฉบับนี้กำหนด” (อ้างอิงหมวด 3 หัวข้อ 9)	
	4.6 ไม่ได้ระบุคำจำกัดความ “ระบบงานเทคโนโลยีสารสนเทศ หรือ ระบบงาน IT”	4.6 เพิ่มคำจำกัดความของ “ระบบงานเทคโนโลยีสารสนเทศ หรือ ระบบงาน IT” ในเอกสาร “การกำกับดูแลและการตรวจสอบด้านเทคโนโลยีสารสนเทศ (Information Technology) สำหรับสำนักงานสอบบัญชี” เพื่อให้ครอบคลุมถึงนิยามของทรัพยากรทางเทคโนโลยีตามมาตรฐานการบริหารคุณภาพ	4.6 ปรับปรุงตามข้อเสนอแนะที่ได้รับจากการเปิดรับฟังความคิดเห็นเพื่อให้สำนักงานสอบบัญชีสามารถดำเนินการตามวัตถุประสงค์ของประกาศได้อย่างเหมาะสม
	4.7 ไม่ได้ระบุคำจำกัดความ “การตรวจสอบด้าน IT แบบเต็มรูปแบบ (“full-scope”)”	4.7 เพิ่มคำจำกัดความของ “การตรวจสอบด้าน IT แบบเต็มรูปแบบ (“full-scope”)” ในเอกสาร “การกำกับดูแลและการตรวจสอบด้านเทคโนโลยีสารสนเทศ (Information Technology) สำหรับสำนักงานสอบบัญชี” ดังนี้ “การตรวจสอบด้าน IT แบบเต็มรูปแบบ (“full-scope”) หมายถึง การตรวจสอบระบบงานเทคโนโลยีสารสนเทศ หรือระบบงาน IT โดยผู้เชี่ยวชาญ โดยสำนักงานสอบบัญชีต้องจัดให้มีการตรวจระบบงาน	4.7 เพิ่มคำจำกัดความของการตรวจสอบด้าน IT แบบเต็มรูปแบบ (“full-scope”) เพื่อให้สำนักงานสอบบัญชีสามารถดำเนินการตามวัตถุประสงค์ของประกาศได้อย่างเหมาะสม

หัวข้อ	หลักการ	ร่างประกาศ/ภาคผนวกแนบท้ายประกาศ	เหตุผลที่ปรับปรุง
		เทคโนโลยีสารสนเทศ หรือระบบงาน IT ตามผลการประเมินความเสี่ยงของสำนักงานสอบบัญชี โดยการตรวจสอบต้องครอบคลุมตามข้อกำหนดที่ระบุไว้ในเอกสาร “การกำกับดูแลและการตรวจสอบด้านเทคโนโลยีสารสนเทศ (Information Technology) สำหรับสำนักงานสอบบัญชี”	
ภาคผนวก 2 แนบท้ายประกาศ : การประเมินระดับความเสี่ยงด้านเทคโนโลยีสารสนเทศของสำนักงานสอบบัญชี (IT Risk Assessment: ITRA)			
5. การประเมินระดับความเสี่ยงด้านเทคโนโลยีสารสนเทศของสำนักงานสอบบัญชี (IT Risk Assessment: ITRA)	สำนักงานสอบบัญชีต้องจัดให้มีการประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศโดยพิจารณาจากความซับซ้อนของระบบงาน IT ของสำนักงานสอบบัญชีและผลกระทบต่อตลาดทุนโดยคำนวณจากมูลค่าหลักทรัพย์ตามราคาตลาดของลูกค้าสอบบัญชีที่เป็นบริษัทจดทะเบียน และตรวจสอบตามแนวปฏิบัติเกี่ยวกับการตรวจสอบด้าน IT	เพิ่มเติมคำอธิบาย ตัวอย่าง รวมทั้งปรับปรุงเกณฑ์การประเมินที่ใช้ในการพิจารณาความซับซ้อนของระบบงาน IT ให้เหมาะสมและชัดเจนมากยิ่งขึ้น เพื่อให้สำนักงานสอบบัญชีสามารถประเมินผลและปฏิบัติไปในแนวทางที่สอดคล้องกัน ตัวอย่างของคำอธิบาย/ตัวอย่าง และการปรับปรุงหลักเกณฑ์ที่เพิ่มเติม เช่น - <u>โปรแกรมหรือระบบงาน IT ที่ใช้สนับสนุนการบริหารงาน การปฏิบัติงานสอบบัญชี</u> เพิ่มคำอธิบายว่าให้สำนักงานสอบบัญชีพิจารณาเฉพาะโปรแกรมหรือระบบงานที่เกี่ยวข้องกับทรัพยากรทางเทคโนโลยีของสำนักงานสอบบัญชีที่มีวัตถุประสงค์ที่เกี่ยวข้องกับระบบการบริหารคุณภาพของสำนักงานสอบบัญชี	ปรับปรุงตามข้อเสนอแนะที่ได้รับจากการเปิดรับฟังความคิดเห็น ซึ่งต้องการให้เพิ่มคำอธิบายและตัวอย่างให้ละเอียดมากยิ่งขึ้น เพื่อให้สำนักงานสอบบัญชีสามารถประเมินผลและปฏิบัติตามประกาศไปในแนวทางที่สอดคล้องกัน

หัวข้อ	หลักการ	ร่างประกาศ/ภาคผนวกแนบท้ายประกาศ	เหตุผลที่ปรับปรุง
		โดยอ้างอิงตามมาตรฐานการบริหารคุณภาพ (TSQM1) ย่อหน้า 32 (ฉ) ก99 และเพิ่มคำอธิบายกรณีของความเสี่ยงระดับสูงให้ชัดเจนขึ้น - การจัดเก็บและเรียกใช้ข้อมูล ปรับปรุงเกณฑ์ในการประเมินความซับซ้อน/ความเสี่ยงของระบบ IT โดยเพิ่มเติมวิธีการจัดเก็บข้อมูลในรูปแบบกระดาษและการใช้บริการของผู้ให้บริการ เพื่อให้ครอบคลุมสภาพแวดล้อมในการทำงานของสำนักงานสอบบัญชีในทุกกรณี - การนับจำนวน laptop PC tablet, mobile devices, removeable storage หรืออุปกรณ์อื่น ๆ ซึ่งเป็นอุปกรณ์ส่วนตัวของพนักงาน (Bring Your Own Device) ที่สามารถเชื่อมต่อเครือข่ายภายในของสำนักงานสอบบัญชี หรือเข้าถึงข้อมูลหรือฐานข้อมูลภายในของสำนักงานสอบบัญชีได้ เพิ่มคำอธิบายว่า ให้รวมถึงการเข้าถึง e-mail ของสำนักงานสอบบัญชีด้วย และหากสำนักงานสอบบัญชีไม่สามารถทราบข้อมูลได้อย่างแน่ชัดให้ใช้การประมาณการที่ดีที่สุด ณ ขณะนั้น	

หัวข้อ	หลักการ	ร่างประกาศ/ภาคผนวกแนบท้ายประกาศ	เหตุผลที่ปรับปรุง
		- การนำเทคโนโลยีอุบัติใหม่ (“emerging technologies”) มาใช้งานในสำนักงานสอบบัญชีจริงในปีที่ผ่านมา เพิ่มคำอธิบายว่าให้พิจารณาเฉพาะงานที่เกี่ยวข้องกับทรัพยากรทางเทคโนโลยีของสำนักงานสอบบัญชีที่มีวัตถุประสงค์ที่เกี่ยวข้องกับระบบการบริหารคุณภาพของสำนักงานสอบบัญชี โดยอ้างอิงตามมาตรฐานการบริหารคุณภาพ (TSQM1) ย่อหน้า 32 (ฉ) ก99 และยกตัวอย่าง emerging technologies ให้ชัดเจนขึ้น - การถูกคุมคามทางไซเบอร์ เพิ่มคำอธิบายและปรับปรุงเกณฑ์ในการประเมินความซับซ้อนของระบบ IT/ความเสี่ยงให้เหมาะสมกับสภาพแวดล้อมกับสำนักงานสอบบัญชีในทางปฏิบัติมากขึ้น เช่น การเพิ่มตัวอย่างของการถูกโจมตี (เช่น virus/malware phishing email phishing phone ransomware) และเพิ่มคำอธิบายว่า “รวมทั้งกรณีที่มีผลเสียหายและไม่มีผลเสียหาย” รวมทั้งปรับปรุงเกณฑ์ในการประเมินระดับต่ำ ปานกลาง สูง ให้สอดคล้องกับสภาพแวดล้อมของสำนักงานสอบบัญชีในปัจจุบันมากยิ่งขึ้น	

หัวข้อ	หลักการ	ร่างประกาศ/ภาคผนวกแนบท้ายประกาศ	เหตุผลที่ปรับปรุง
		- เพิ่มเติมหลักเกณฑ์และคำอธิบายเกี่ยวกับการกำหนดรอบการตรวจสอบและกรณีมีการเปลี่ยนรอบตรวจสอบ การนำส่งรายงานผลการตรวจสอบและเอกสารที่เกี่ยวข้อง รวมถึงการขอผ่อนผัน วิธีปฏิบัติในช่วงเปลี่ยนแปลง (transitional period) วิธีปฏิบัติสำหรับสำนักงานสอบบัญชีใหม่ที่จะเข้ามาปฏิบัติงานในตลาดทุนเป็นครั้งแรก แนวปฏิบัติสำหรับปีที่สำนักงานสอบบัญชีไม่ได้ถูกกำหนดให้ดำเนินการตรวจแบบ full – scope เป็นต้น	