สำนักตรวจสอบ
รับที่ 1970 เวลา 12.49 น.
วันที่ 3 ก.ค. 66

รับอีกครั้ง 13 กค 66
เวลา 15.00 น.

บันทึกข้อความ

หน่วยงาน ฝ่ายตรวจสอบกระบวนงานหลัก โทร. 2521

ที่ ฝตล 90 /2566 **วันที่** 3 กรกฎาคม 2566

เรื่อง ขอความเห็นชอบผลการทบทวน/ปรับปรุงคู่มือปฏิบัติงานของ ฝตล. ปีงบประมาณ 2566

เรียน ชวก.(สตส)

การประปานครหลวงกำหนดให้หน่วยงานระดับฝ่ายและกองที่ไม่สังกัดฝ่ายทุกหน่วยงานจัดทำคู่มือปฏิบัติงานรวมทั้งทบทวนและปรับปรุงให้เป็นปัจจุบัน สอดคล้องกับผลการประเมินการควบคุมด้วยตนเองอย่างน้อยปีละ 1 ครั้ง และกำหนดให้หัวหน้าหน่วยงานทุกระดับสื่อสารให้บุคลากรในสังกัด ทราบ และติดตามควบคุมให้บุคลากรถือปฏิบัติในส่วนที่เกี่ยวข้องอย่างเคร่งครัด ดังรายละเอียดปรากฏในคำสั่งการประปานครหลวงที่ 1104/2565 เรื่อง แนวทางปฏิบัติเกี่ยวกับการควบคุมภายใน สั่ง ณ วันที่ 28 กันยายน 2565

ฝตล. ได้พิจารณาทบทวน/ปรับปรุงคู่มือปฏิบัติงาน ประจำปีงบประมาณ 2566 เพื่อให้สอดคล้องกับการปฏิบัติงานในปัจจุบัน พร้อมทั้งจัดทำรายงานผลการทบทวนคู่มือปฏิบัติงานแล้วเสร็จรายละเอียดตามเอกสารแนบ รวมทั้งได้แนบคู่มือฯ ฉบับทบทวน/ปรับปรุง มาพร้อมนี้

จึงเรียนมาเพื่อโปรดพิจารณาให้ความเห็นชอบผลการทบทวนคู่มือปฏิบัติงาน เพื่อใช้เป็นแนวทางในการปฏิบัติ ต่อไป

สุชาดา นาคย้อย

(นางสุชาดา นาคย้อย)
ผู้อำนวยการฝ่ายตรวจสอบกระบวนงานหลัก

(1) **- เห็นชอบ**

เรียน ผอ.ฝตล.

เพื่อทราบและจัดเก็บคู่มือปฏิบัติงาน ในระบบเอกสารอิเล็กทรอนิกส์ ตู้คู่มือปฏิบัติงาน ภายใน 10 วันทำการ โดยไม่เกินวันที่ 17 สิงหาคม 2566

(นางอำไพศรี ธารธรรมวงศ์)
ชวก.(สตส)
วันที่ 13 ก.ค. 66

(2) เรียน เลขานุการคณะกรรมการดำเนินการเกี่ยวกับการควบคุมภายใน (ผอ.ฝบส.)

เพื่อทราบผลการทบทวนคู่มือปฏิบัติงาน ทั้งนี้ได้จัดเก็บคู่มือปฏิบัติงาน ในระบบเอกสารอิเล็กทรอนิกส์ ครบถ้วนแล้ว

สุชาดา นาคย้อย

(นางสุชาดา นาคย้อย)
ผอ.ฝตล.
วันที่ 13 ก.ค. 66

รายงานผลการทบทวนคู่มือปฏิบัติงานของหน่วยงานระดับฝ่ายและกองที่ไม่สังกัดฝ่าย ปีงบประมาณ 2566

ลำดับที่	หน่วยงาน	รายการ	ประเภทของคู่มือ	ทบทวนแล้วเสร็จ วัน/เดือน/ปี	ผลการทบทวน					วันที่ให้ความเห็นชอบ	ผลการจัดเก็บคู่มือฯ ใน INFOMA Webform
					การปรับปรุงคู่มือฯ			กรณีมีการยกเลิกคู่มือฯ			
					ไม่ปรับปรุง	ปรับปรุง	หัวข้อเนื้อหาที่ปรับปรุง	ยกเลิก	ระบุสาเหตุที่ยกเลิก		วันที่จัดเก็บ
					* (ทำเครื่องหมาย ✓ ในช่อง)			* (ทำเครื่องหมาย ✓ ในช่อง)			
1	ฝ่ายตรวจสอบกระบวนงานหลัก	คู่มือขั้นตอนการปฏิบัติในการตรวจสอบระบบความมั่นคงปลอดภัยสารสนเทศ ISO 27001 (Internal Audit Procedure Manual)	3	22 พ.ค. 2566		/	1. ผู้มีส่วนได้ส่วนเสียและหน้าที่ความรับผิดชอบ (หน้า 2) 2. ขั้นตอนการบริหารจัดการการตรวจสอบระบบความมั่นคงปลอดภัยสารสนเทศ (หน้า 4) 3. คำอธิบายขั้นตอนการบริหารจัดการการตรวจสอบระบบความมั่นคงปลอดภัยสารสนเทศ (หน้า 5) 4. ผู้รับการสื่อสาร ในหัวข้อ การสื่อสาร (หน้า 17)				

ภายใน

คู่มือขั้นตอนการปฏิบัติในการตรวจสอบ ระบบความมั่นคงปลอดภัยสารสนเทศ ISO 27001

Internal Audit Procedure Manual

หมายเลขเอกสาร	IA.PCD.001
ปรับปรุงครั้งที่	08
วันที่มีผลบังคับใช้	22 พฤษภาคม 2566
ประเภทเอกสาร	ภายใน
เจ้าของเอกสาร	สำนักตรวจสอบ
ทบทวนโดย	กองตรวจสอบสารสนเทศ
มีผลบังคับใช้กับ	พนักงาน ลูกจ้าง เจ้าหน้าที่ตามสัญญาจ้าง
อนุมัติโดย	ฝ่ายตรวจสอบกระบวนงานหลัก

เอกสารฉบับนี้เป็นทรัพย์สินของการประปานครหลวง ห้ามมิให้ทำการเผยแพร่ส่วนหนึ่งส่วนใดโดยไม่ได้รับอนุญาตเป็นลายลักษณ์อักษรจาก *ผู้อำนวยการฝ่ายตรวจสอบกระบวนงานหลัก* ผู้ฝ่าฝืนจะถูกดำเนินการลงโทษขั้นสูงสุดตามระเบียบข้อบังคับของ กปน. กรณีมีข้อสงสัยต้องการคำอธิบายหรือพบความไม่สอดคล้องของเอกสารฉบับนี้ แจ้งให้ผู้บังคับบัญชาหรือหัวหน้าทราบทันที หรือติดต่อเลขานุการคณะกรรมการด้านการรักษาความปลอดภัยสารสนเทศตามมาตรฐาน ISO 27001

การอนุมัติเอกสาร

ผู้จัดทำ	
ชื่อ นางสาวณัฐนี อมตะธงไชย ตำแหน่ง ผู้ตรวจสอบ 6 กตส.ฝตล. วันที่ 22 พ.ค. 66	ลงชื่อ ณัฐนี อมตะธงไชย ((นางสาวณัฐนี อมตะธงไชย)) ผู้ตรวจสอบ ๖ กองตรวจสอบสารสนเทศ
ผู้สอบทาน	
ชื่อ นายพัทยา ปานสุวรรณ ตำแหน่ง ผอ.กตส. วันที่ 22 พ.ค. 66	ลงชื่อ ((นายพัทยา ปานสุวรรณ)) ผู้อำนวยการกองตรวจสอบสารสนเทศ
ผู้อนุมัติ	
ชื่อ นางสุชาดา นาคย้อย ตำแหน่ง ผอ.ฝตล. วันที่ 3 ก.ค. 66	ลงชื่อ สุชาดา นาคย้อย ((นางสุชาดา นาคย้อย)) ผู้อำนวยการฝ่ายตรวจสอบกระบวนงานหลัก

ประวัติการแก้ไขเอกสาร

ครั้งที่	รายละเอียดการแก้ไข	วันที่มีผลบังคับใช้
01	ปรับปรุงขั้นตอนการดำเนินงาน เนื้อหา และฟอร์มเอกสาร	3 ตุลาคม 2556
02	ปรับปรุงแนวทางการดำเนินงาน รหัสเอกสารให้สอดคล้องกับการเปลี่ยนแปลง	8 มีนาคม 2559
03	ปรับปรุงโครงสร้างหมายเลขเอกสาร	3 มีนาคม 2560
04	เพิ่มเติมหัวข้อการจัดทำรายงานผลการตรวจสอบ ในเรื่องของการจัดลำดับความสำคัญของผลการตรวจสอบ (Audit Rating) และข้อเสนอแนะ	19 พฤษภาคม 2560
05	ปรับปรุงชื่อเอกสารและเพิ่มเติมเอกสารสำหรับบันทึก	16 กรกฎาคม 2563
06	1. ปรับปรุง วัตถุประสงค์ให้สอดคล้องกับการดำเนินงาน 2. ปรับปรุง ผู้ที่เกี่ยวข้องและมีหน้าที่ความรับผิดชอบ 3. เพิ่มเติม ขั้นตอนและคำอธิบายกระบวนงานการบริหารจัดการตรวจสอบระบบความมั่นคงปลอดภัยสารสนเทศ 4. ปรับปรุง ขั้นตอนและคำอธิบายการดำเนินการตรวจสอบภายใน 5. เพิ่มเติม การวัดประสิทธิผลงานตรวจสอบ 6. เพิ่มเติม การสื่อสาร	30 มิถุนายน 2564
07	ปรับปรุง การสื่อสาร (หน้า 17) เพิ่มเติม การวิเคราะห์และประเมินการรับรู้ของผู้มีส่วนได้ส่วนเสียที่สำคัญที่เกี่ยวข้องกับกระบวนการ และการกำหนดการวัด ติดตาม วิเคราะห์ประเมิน ตัววัดผลลัพธ์ (Outcome) ของกระบวนการ (หน้า 18)	12 กรกฎาคม 2565
08	ปรับปรุง 1. ผู้มีส่วนได้ส่วนเสียและหน้าที่ความรับผิดชอบ (หน้า 2) 2. ขั้นตอนการบริหารจัดการการตรวจสอบระบบความมั่นคงปลอดภัยสารสนเทศ (หน้า 4) 3. คำอธิบายขั้นตอนการบริหารจัดการการตรวจสอบระบบความมั่นคงปลอดภัยสารสนเทศ (หน้า 5) 4. ผู้รับการสื่อสาร ในหัวข้อ การสื่อสาร (หน้า 17)	22 พฤษภาคม 2566

สรุปเปรียบเทียบคู่มือขั้นตอนการปฏิบัติในการตรวจสอบ
ระบบความมั่นคงปลอดภัยสารสนเทศ ISO 27001
ฉบับปรับปรุงปี 2565 และฉบับปรับปรุงปี 2566

สรุปเปรียบเทียบคู่มือขั้นตอนการปฏิบัติในการตรวจสอบระบบความมั่นคงปลอดภัยสารสนเทศ ISO 27001 ฉบับปรับปรุงปี 2565 และฉบับปรับปรุงปี 2566

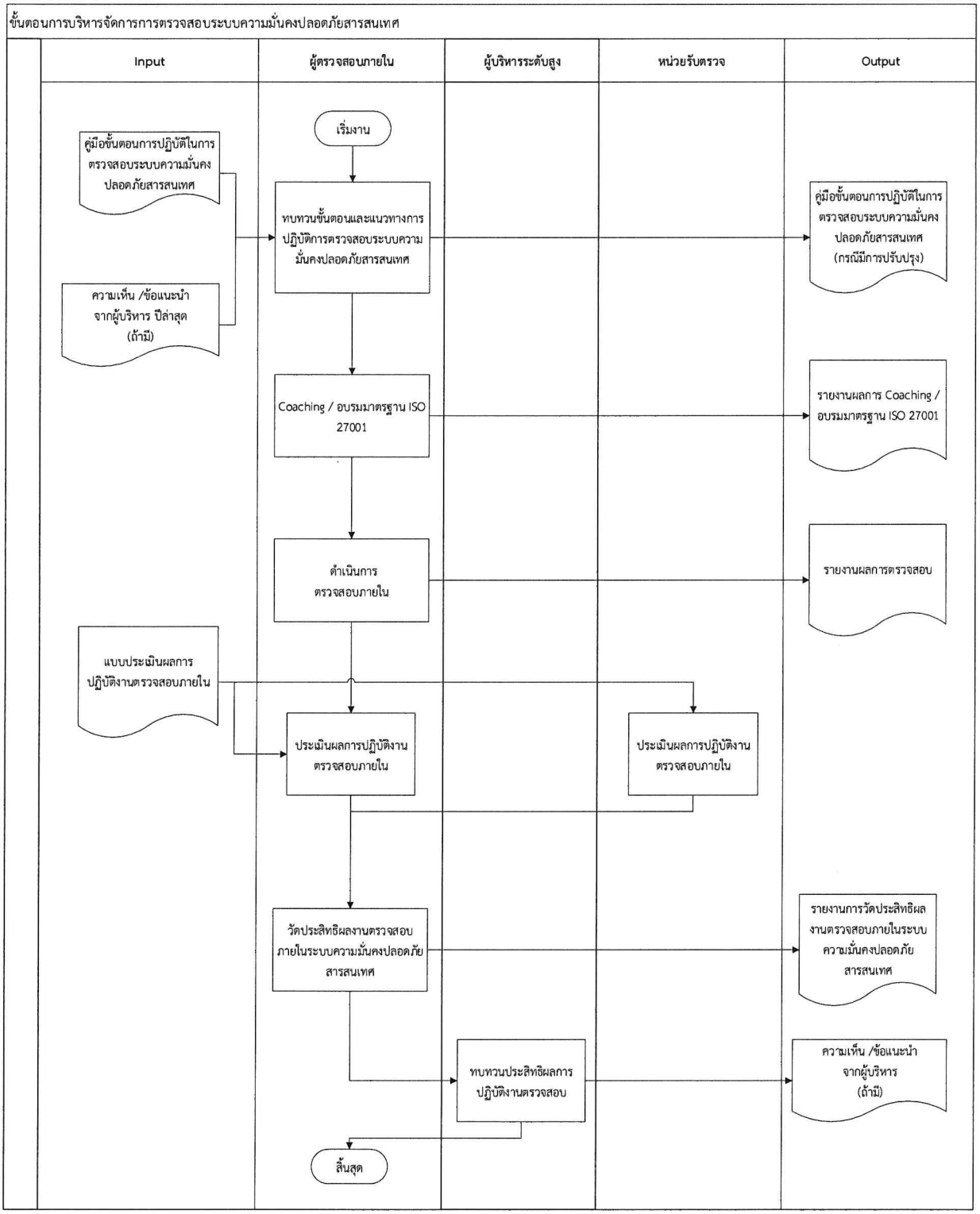
หัวข้อเนื้อหาตามคู่มือ	ฉบับปรับปรุงปี 2565	ฉบับปรับปรุงปี 2566	เหตุผล
1. วัตถุประสงค์	1. วัตถุประสงค์	เนื้อหาคงเดิม	ทบทวนแล้วให้เนื้อหาคงเดิม
2. ขอบเขต	2. ขอบเขต		
3. นิยามและคำจำกัดความ	3. นิยามและคำจำกัดความ		
4. ผู้มีส่วนได้ส่วนเสียและหน้าที่ความรับผิดชอบ	ผู้บริหารระดับสูง	คณะอนุกรรมการพัฒนาเทคโนโลยีดิจิทัลของ กปน. / IT Steering Commitee	เพื่อสื่อความหมายได้ชัดเจนยิ่งขึ้น
5. ขั้นตอนการบริหารจัดการการตรวจสอบระบบความมั่นคงปลอดภัยสารสนเทศ	ตามแนบ 1	ตามแนบ 2	เพื่อให้เป็นไปตามการปฏิบัติงานในปัจจุบัน และสอดคล้องกับเกณฑ์ประเมิน Enabler
6. คำอธิบายขั้นตอนการบริหารจัดการการตรวจสอบระบบความมั่นคงปลอดภัยสารสนเทศ	ไม่มี	เพิ่มขั้นตอน ที่ 5 และคำอธิบาย <u>วิเคราะห์การรับรู้การสื่อสาร</u> ผู้ตรวจสอบภายในวิเคราะห์การรับรู้การสื่อสารจากผู้มีส่วนได้ส่วนเสียและจัดทำเป็นรายงานเพื่อนำไปทบทวนในขั้นตอน และแนวทางการปฏิบัติการตรวจสอบในปีถัดไป	เพื่อให้เป็นไปตามการปฏิบัติงานในปัจจุบัน และสอดคล้องกับเกณฑ์ประเมิน Enabler
	ขั้นตอนที่ 5-6 เดิม	ปรับปรุงลำดับเป็นขั้นตอนที่ 6-7 เนื้อหาไม่เปลี่ยนแปลง	ปรับปรุงให้เรียงตามลำดับตัวเลข
	ไม่มี	เพิ่มขั้นตอนที่ 8 และคำอธิบาย <u>รับทราบผลการดำเนินงานและประสิทธิผลงานตรวจสอบ</u>	เพื่อให้เป็นไปตามการปฏิบัติงานในปัจจุบัน และสอดคล้องกับเกณฑ์ประเมิน Enabler

หัวข้อเนื้อหาตามคู่มือ	ฉบับปรับปรุงปี 2565	ฉบับปรับปรุงปี 2566	เหตุผล
		คณะอนุกรรมการพัฒนาเทคโนโลยีดิจิทัลของ กปน. /IT Steering Committee รับทราบผลการดำเนินงาน และประสิทธิผลงานตรวจสอบ ให้ความเห็นและข้อแนะนำ (ถ้ามี) เพื่อให้ผู้ตรวจสอบนำไปพัฒนางานตรวจสอบต่อไป	
7. ขั้นตอนการดำเนินการตรวจสอบภายในระบบความมั่นคงปลอดภัยสารสนเทศ	7. ขั้นตอนการดำเนินการตรวจสอบภายในระบบความมั่นคงปลอดภัยสารสนเทศ	เนื้อหาคงเดิม	ทบทวนแล้วให้เนื้อหาคงเดิม
8. คำอธิบายขั้นตอนการตรวจสอบภายในระบบความมั่นคงปลอดภัยสารสนเทศ	8. คำอธิบายขั้นตอนการตรวจสอบภายในระบบความมั่นคงปลอดภัยสารสนเทศ		
9. ขั้นตอนการปฏิบัติเพื่อการแก้ไข (Corrective Action)	9. ขั้นตอนการปฏิบัติเพื่อการแก้ไข (Corrective Action)		
10. คำอธิบายขั้นตอนการปฏิบัติเพื่อการแก้ไข	10. คำอธิบายขั้นตอนการปฏิบัติเพื่อการแก้ไข		
11. การวางแผนและจัดเตรียมทรัพยากร	11. การวางแผนและจัดเตรียมทรัพยากร		
12. การประชุมเปิดการตรวจสอบ	12. การประชุมเปิดการตรวจสอบ		
13. จัดทำแนวทางตรวจสอบ	13. จัดทำแนวทางตรวจสอบ		
14. การปฏิบัติงานตรวจสอบ	14. การปฏิบัติงานตรวจสอบ		

หัวข้อเนื้อหาตามคู่มือ	ฉบับปรับปรุงปี 2565	ฉบับปรับปรุงปี 2566	เหตุผล
15. การรายงานผลการตรวจสอบ	15. การรายงานผลการตรวจสอบ	เนื้อหาคงเดิม	ทบทวนแล้วให้เนื้อหาคงเดิม
16. การรับทราบและแก้ไข	16. การรับทราบและแก้ไข		
17. การจัดทำรายงานผลการตรวจสอบ	17. การจัดทำรายงานผลการตรวจสอบ		
18. เอกสารสำหรับบันทึก	18. เอกสารสำหรับบันทึก		
19. การวัดประสิทธิผลงานตรวจสอบ	19. การวัดประสิทธิผลงานตรวจสอบ		
20. การสื่อสาร	ผู้บริหารระดับสูง	คณะอนุกรรมการพัฒนาเทคโนโลยีดิจิทัลของ กปน. / IT Steering Commitee	เพื่อสื่อความหมายได้ชัดเจนยิ่งขึ้น
21. การวิเคราะห์และประเมินการรับรู้ของผู้มีส่วนได้ส่วนเสียที่สำคัญที่เกี่ยวข้องกับกระบวนการ	21. การวิเคราะห์และประเมินการรับรู้ของผู้มีส่วนได้ส่วนเสียที่สำคัญที่เกี่ยวข้องกับกระบวนการ	เนื้อหาคงเดิม	ทบทวนแล้วให้เนื้อหาคงเดิม
22. การกำหนดการวัด ติดตาม วิเคราะห์ประเมิน ตัววัดผลลัพธ์ (Outcome) ของกระบวนการ	22. การกำหนดการวัด ติดตาม วิเคราะห์ประเมิน ตัววัดผลลัพธ์ (Outcome) ของกระบวนการ		

แนบ 1

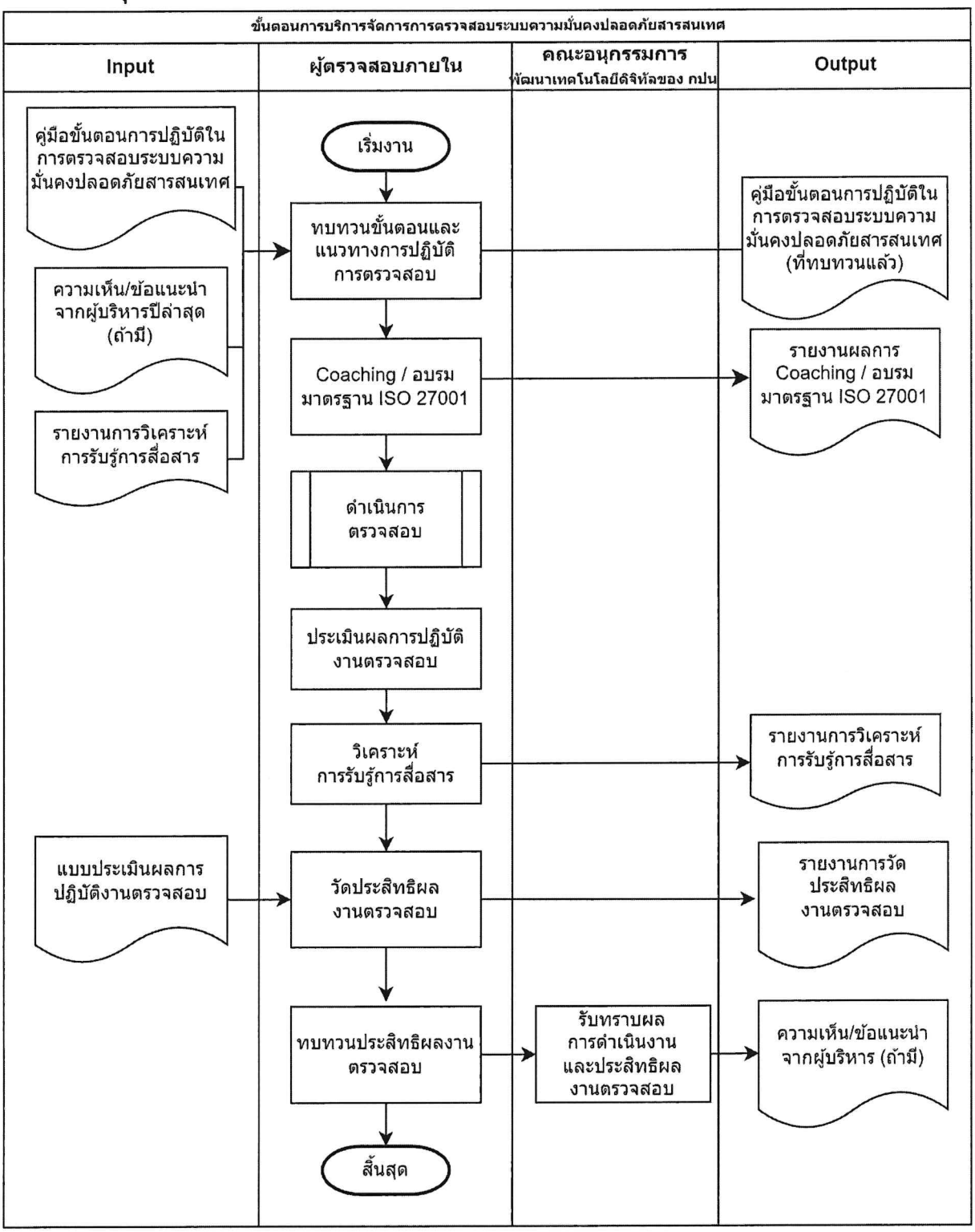
ขั้นตอนการบริหารจัดการการตรวจสอบระบบความมั่นคงปลอดภัยสารสนเทศ ฉบับปรับปรุงปี 2565



แนบ 2

ขั้นตอนการบริหารจัดการการตรวจสอบระบบความมั่นคงปลอดภัยสารสนเทศ

ฉบับปรับปรุงปี 2566



สารบัญ

หน้า

1. วัตถุประสงค์.....1
2. ขอบเขต.....1
3. นิยามและคำจำกัดความ.....1
4. ผู้มีส่วนได้ส่วนเสียและหน้าที่ความรับผิดชอบ.....2
5. ขั้นตอนการบริหารจัดการการตรวจสอบระบบความมั่นคงปลอดภัยสารสนเทศ.....4
6. คำอธิบายขั้นตอนการบริหารจัดการการตรวจสอบระบบความมั่นคงปลอดภัยสารสนเทศ.....5
7. ขั้นตอนการดำเนินการตรวจสอบภายในระบบความมั่นคงปลอดภัยสารสนเทศ.....6
8. คำอธิบายขั้นตอนการตรวจสอบภายในระบบความมั่นคงปลอดภัยสารสนเทศ.....7
9. ขั้นตอนการปฏิบัติเพื่อการแก้ไข (Corrective Action).....8
10. คำอธิบายขั้นตอนการปฏิบัติเพื่อการแก้ไข.....9
11. การวางแผนและจัดเตรียมทรัพยากร.....10
12. การประชุมเปิดการตรวจสอบ.....11
13. จัดทำแนวทางตรวจสอบ.....12
14. การปฏิบัติงานตรวจสอบ..... 12
15. การรายงานผลการตรวจสอบ.....13
16. การรับทราบและแก้ไข.....13
17. การจัดทำรายงานผลการตรวจสอบ.....13
18. เอกสารสำหรับบันทึก.....14
19. การวัดประสิทธิผลงานตรวจสอบ.....16
20. การสื่อสาร.....17
21. การวิเคราะห์และประเมินการรับรู้ของผู้มีส่วนได้ส่วนเสียที่สำคัญที่เกี่ยวข้องกับกระบวนการ.....18
22. การกำหนดการวัด ติดตาม วิเคราะห์ประเมิน ตัววัดผลลัพธ์ (Outcome) ของกระบวนการ.....18

1. วัตถุประสงค์

1) เพื่อเป็นแนวทางการปฏิบัติงานตรวจสอบของผู้ตรวจสอบภายในสารสนเทศ

2) เพื่อให้การตรวจสอบด้านความมั่นคงปลอดภัยสารสนเทศ มีประสิทธิผล ประสิทธิภาพและได้รับการควบคุมดูแลอย่างเหมาะสม

3) เพื่อให้เกิดการบริหารจัดการกระบวนการตรวจสอบระบบความมั่นคงปลอดภัยสารสนเทศมีการพัฒนาอย่างต่อเนื่อง

2. ขอบเขต

อ้างอิงจากเอกสารคู่มือบริหารจัดการระบบความมั่นคงปลอดภัยสารสนเทศ (ISMS Manual) (IS.HBK.002)

3. นิยามและคำจำกัดความ

ภายใต้เอกสารขั้นตอนการปฏิบัติในการตรวจสอบระบบความมั่นคงปลอดภัยสารสนเทศ ISO 27001 ฉบับนี้ ได้กำหนดนิยามและคำจำกัดความดังนี้

1. **ผู้ตรวจสอบภายใน (Internal Auditor)** หมายถึง หน่วยงานผู้รับผิดชอบหลัก ฝ่าย กอง หรือผู้มีอำนาจและหน้าที่ในการตรวจสอบระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศภายในซึ่งได้รับการแต่งตั้งถูกต้องเป็นทางการ

2. **การตรวจสอบภายใน (Internal Audit)** หมายถึง การให้ความเชื่อมั่นและการให้คำปรึกษาอย่างเที่ยงธรรมและเป็นอิสระ เพื่อเพิ่มคุณค่าและปรับปรุงการดำเนินงานขององค์กร การตรวจสอบภายในช่วยให้องค์กรบรรลุเป้าหมายด้วยการประเมินและปรับปรุงประสิทธิผลของกระบวนการบริหารความเสี่ยง การควบคุม และการกำกับดูแลอย่างเป็นระบบและเป็นระเบียบ

3. **คณะกรรมการตรวจสอบ (Audit Committee)** หมายถึงคณะกรรมการตรวจสอบการประปานครหลวง ซึ่งมีอำนาจหน้าที่ กำกับดูแล การปฏิบัติงานภายในให้มีประสิทธิภาพ ประสิทธิผลเป็นที่น่าเชื่อถือ และการตรวจสอบภายในให้มีมาตรฐานรัดกุมเพียงพอ

4. **คณะกรรมการด้านการรักษาความปลอดภัยสารสนเทศ** หมายถึง คณะกรรมการด้านการรักษาความปลอดภัยสารสนเทศตามมาตรฐาน ISO 27001

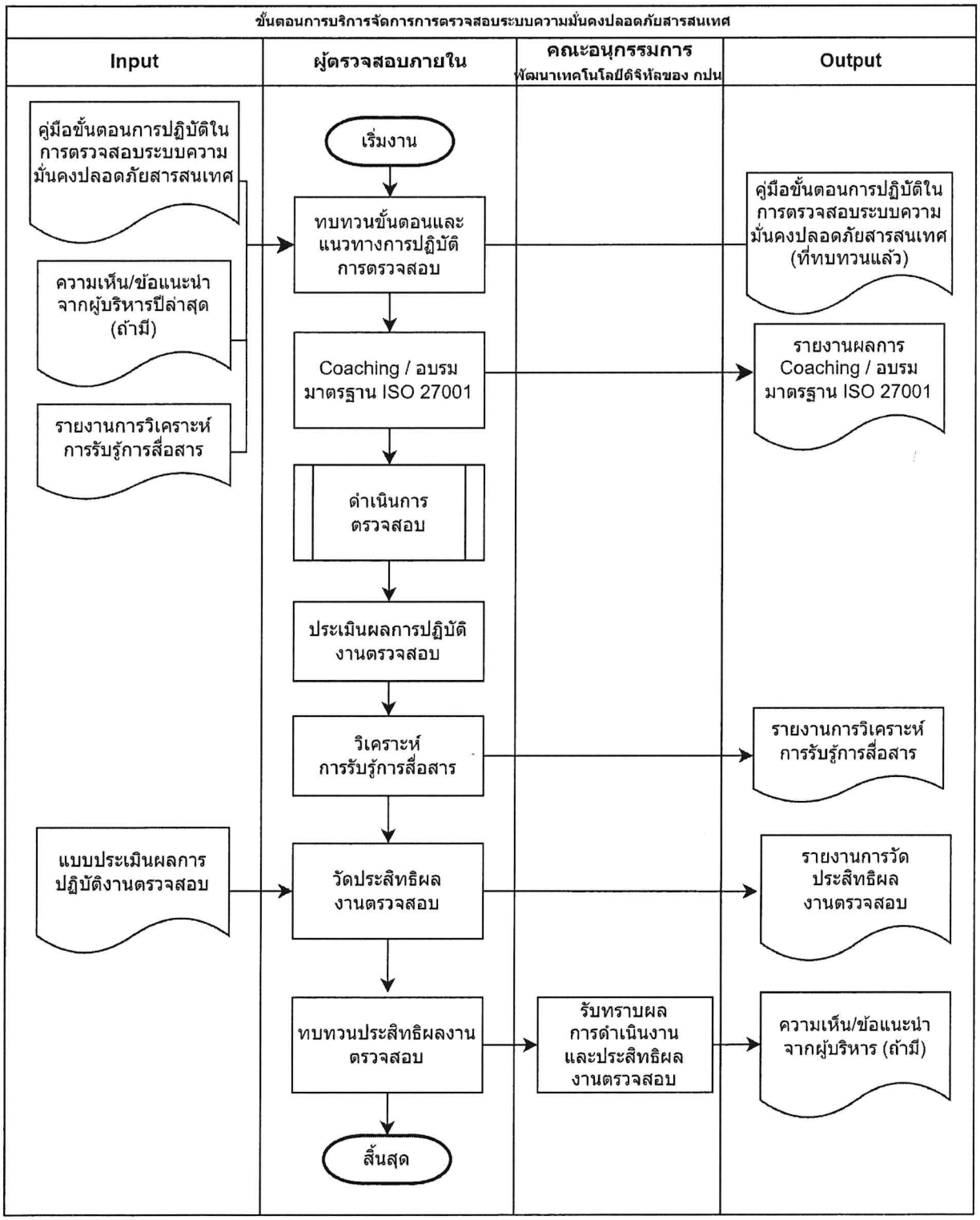
5. **หน่วยรับตรวจ (Auditee) หมายถึง** หน่วยงานผู้รับผิดชอบหลัก ฝ่าย กอง หรือผู้มีหน้าที่เกี่ยวข้องในการดำเนินการตามระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ

6. **สิ่งที่ไม่เป็นไปตามข้อกำหนดหรือข้อบกพร่อง (Non-conformity)** หมายถึง การปฏิบัติที่ไม่สอดคล้องกับข้อกำหนดที่ได้กำหนดไว้

7. **ความไม่สอดคล้องหลัก (Major Non-conformity)** หมายถึง ไม่ปรากฏว่าได้มีการดำเนินการตามข้อกำหนดของระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศโดยสิ้นเชิง หรือพบว่ามี Minor ในข้อกำหนดเดียวกันหรือเรื่องเดียวกันจำนวนมาก อนุมานได้ว่า ข้อกำหนดดังกล่าวไม่ได้ดำเนินการอย่างสิ้นเชิง

ลำดับที่	ตำแหน่ง	หน้าที่ความรับผิดชอบ
		▪ สรุปผลการดำเนินงาน และรายงานต่อผู้ตรวจสอบภายใน / สายงานเทคโนโลยีสารสนเทศ
4	คณะกรรมการด้านการรักษาความปลอดภัยสารสนเทศ	▪ รับทราบผล และลงนามอนุมัติผลการดำเนินงาน
5	คณะกรรมการตรวจสอบ	▪ รับทราบผลการดำเนินงาน
6	คณะอนุกรรมการพัฒนาเทคโนโลยีดิจิทัลของ กปน. / IT Steering Commitee	▪ รับทราบผลการดำเนินงาน และประสิทธิผลงานตรวจสอบ

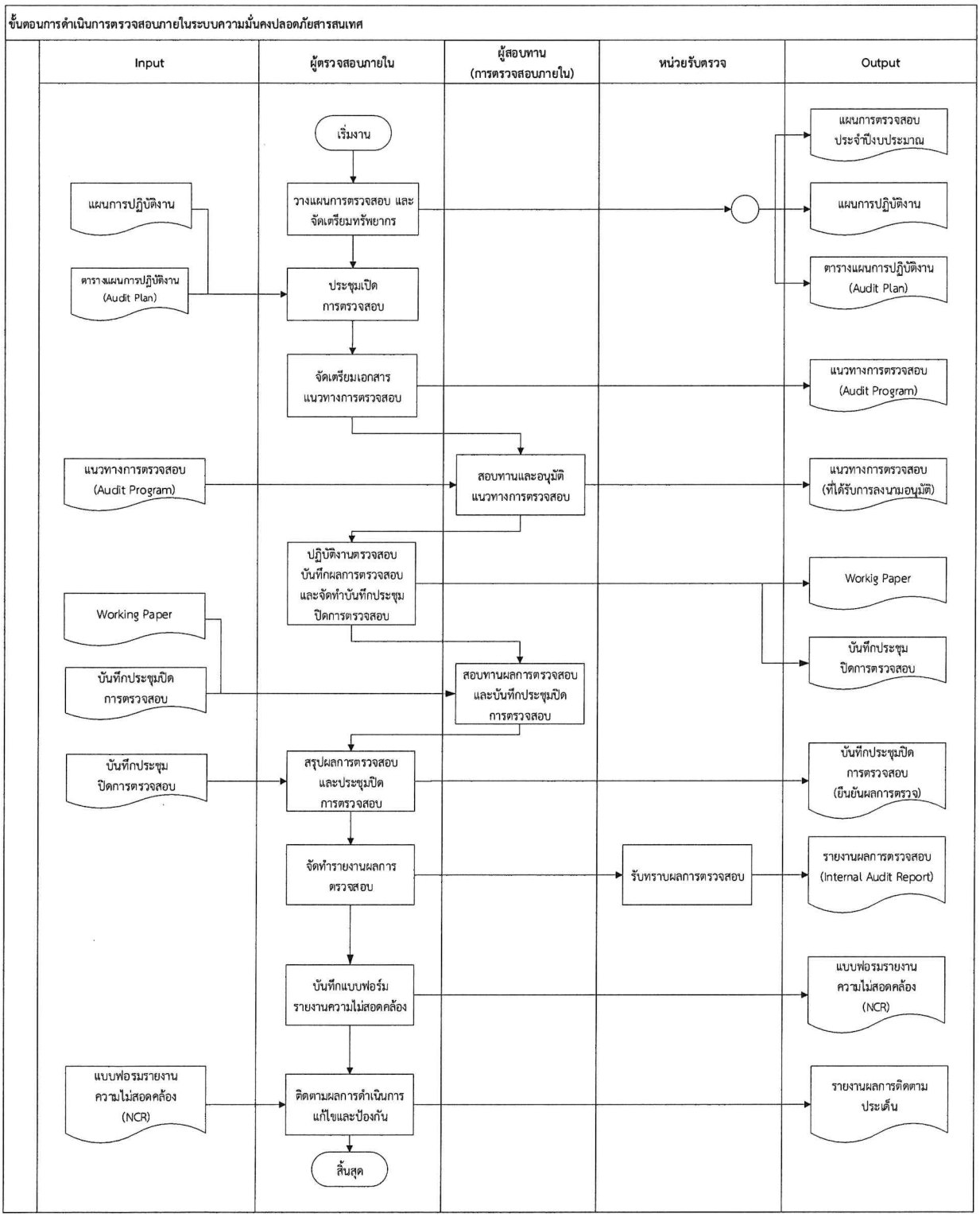
5. ขั้นตอนการบริหารจัดการการตรวจสอบระบบความมั่นคงปลอดภัยสารสนเทศ



6. ขั้นตอนการบริหารจัดการการตรวจสอบระบบความมั่นคงปลอดภัยสารสนเทศ

ลำดับที่	ขั้นตอน	คำอธิบาย
1	ทบทวนขั้นตอนและแนวทางการปฏิบัติการตรวจสอบ	ผู้ตรวจสอบภายในทบทวนขั้นตอน และแนวทางการปฏิบัติ การตรวจสอบ เพื่อให้สอดคล้องกับการปฏิบัติงานในปัจจุบัน ปรับปรุงงานตรวจสอบตามการวัดประสิทธิผล และเป็นไปตามคู่มือการตรวจสอบภายในของสำนักตรวจสอบ หากมีการปรับปรุงเปลี่ยนแปลงให้ปรับปรุงคู่มือขั้นตอนการปฏิบัติในการตรวจสอบระบบความมั่นคงปลอดภัยสารสนเทศ ISO 27001 (Internal Audit Procedure Manual)
2	Coaching / อบรมมาตรฐาน ISO 27001	ผู้ตรวจสอบภายในฝึกสอนหรืออบรมมาตรฐาน ISO 27001 เพื่อทบทวนก่อนเริ่มดำเนินการตรวจสอบ
3	ดำเนินการตรวจสอบ	ผู้ตรวจสอบภายในดำเนินการตามขั้นตอนใน ข้อ 7. ขั้นตอนการดำเนินการตรวจสอบภายในระบบความมั่นคงปลอดภัยสารสนเทศ (หน้า 6)
4	ประเมินผลการปฏิบัติงานตรวจสอบ	เมื่อผู้ตรวจสอบภายในปฏิบัติงานตรวจสอบเสร็จเรียบร้อยแล้ว ให้ทำการประเมินผลการปฏิบัติงานตรวจสอบ โดยผู้ตรวจสอบภายใน และหน่วยรับตรวจ เพื่อนำไปวัดประสิทธิผล
5	วิเคราะห์การรับรู้การสื่อสาร	ผู้ตรวจสอบภายในวิเคราะห์การรับรู้การสื่อสารจากผู้มีส่วนได้ส่วนเสียและจัดทำเป็นรายงานเพื่อนำไปทบทวนในขั้นตอนและแนวทางการปฏิบัติการตรวจสอบในปีถัดไป
6	วัดประสิทธิผลงานตรวจสอบ	ผู้ตรวจสอบภายในวัดประสิทธิผลงานตรวจสอบ ตามหลักเกณฑ์ที่กำหนด เพื่อนำผลมาปรับปรุงการบริหารจัดการงานตรวจสอบให้มีประสิทธิภาพยิ่งขึ้น
7	ทบทวนประสิทธิผลงานตรวจสอบ	ผู้ตรวจสอบภายในรายงานผลการตรวจสอบและรายงานประสิทธิผลการปฏิบัติงานตรวจสอบ ให้ผู้บริหารระดับสูงรับทราบและพิจารณากรณีที่ควรมีการปรับปรุง
8	รับทราบผลการดำเนินงานและประสิทธิผลงานตรวจสอบ	คณะอนุกรรมการพัฒนาเทคโนโลยีดิจิทัลของ กปน. /IT Steering Committee รับทราบผลการดำเนินงานและประสิทธิผลงานตรวจสอบ ให้ความเห็นและข้อแนะนำ (ถ้ามี) เพื่อให้ผู้ตรวจสอบนำไปพัฒนางานตรวจสอบต่อไป

7. ขั้นตอนการดำเนินการตรวจสอบภายในระบบความมั่นคงปลอดภัยสารสนเทศ

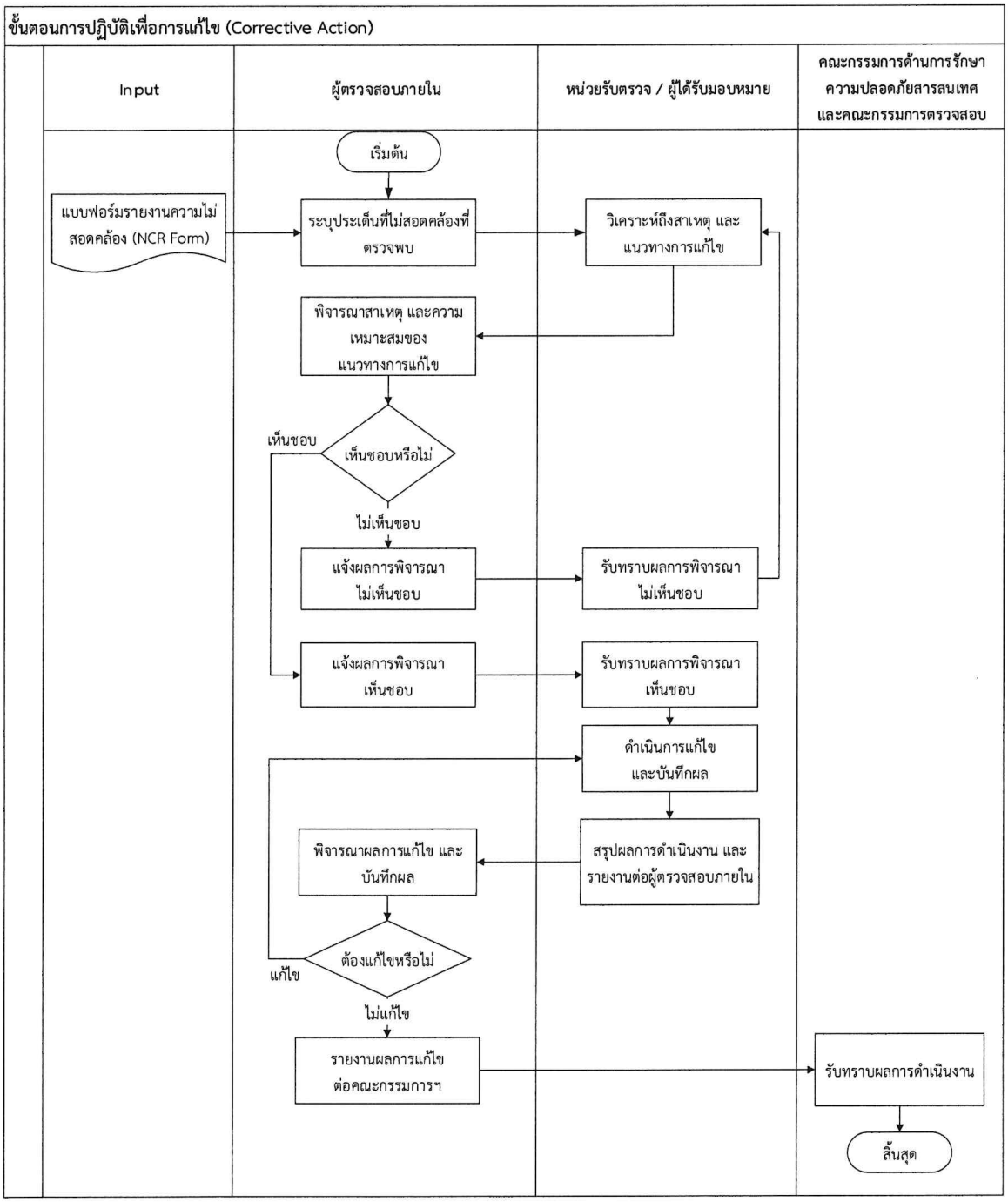


8. คำอธิบายขั้นตอนการตรวจสอบภายในระบบความมั่นคงปลอดภัยสารสนเทศ

ลำดับที่	ขั้นตอน	คำอธิบาย
1	วางแผนการตรวจสอบ และจัดเตรียมทรัพยากร	ผู้ตรวจสอบภายในวางแผนการตรวจสอบ และจัดเตรียมทรัพยากรโดยจัดทำแผนการตรวจสอบประจำปีงบประมาณ แผนการปฏิบัติงาน และตารางแผนการปฏิบัติงาน
2	ประชุมเปิดการตรวจสอบ	ผู้ตรวจสอบภายในประชุมเปิดการตรวจสอบกับหน่วยรับตรวจตามแผนการปฏิบัติงานและตารางแผนการปฏิบัติงาน (Audit Plan)
3	จัดเตรียมเอกสารแนวทางการตรวจสอบ	ผู้ตรวจสอบภายในจัดทำแนวทางการตรวจสอบภายในระบบความมั่นคงปลอดภัยสารสนเทศให้สอดคล้องตามมาตรฐาน ISO 27001โดยจัดทำเป็นเอกสารแนวทางการตรวจสอบ (Audit Program)
4	สอบทานและอนุมัติแนวทางการตรวจสอบ	ผู้สอบทาน (การตรวจสอบภายใน) สอบทานและอนุมัติแนวทางการตรวจสอบ
5	ปฏิบัติงานตรวจสอบ บันทึกผลการตรวจสอบ และจัดทำบันทึกประชุมปิดการตรวจสอบ	ผู้ตรวจสอบภายในปฏิบัติงานตรวจสอบ โดยการตรวจสอบจะต้องบันทึกสิ่งที่ตรวจพบทั้งที่เป็นความสอดคล้องและไม่สอดคล้อง
6	สอบทานผลการตรวจสอบและบันทึกประชุมปิดการตรวจสอบ	ผู้สอบทาน (การตรวจสอบภายใน) สอบทานผลการตรวจสอบและบันทึกประชุมปิดการตรวจสอบ
7	สรุปผลการตรวจสอบและประชุมปิดการตรวจสอบ	ผู้ตรวจสอบภายในสรุปผลการตรวจสอบและประชุมปิดการตรวจสอบ
8	จัดทำรายงานผลการตรวจสอบ	ผู้ตรวจสอบภายในจัดทำรายงานผลการตรวจสอบ (Internal Audit Report)
9	รับทราบผลการตรวจสอบ	หน่วยรับตรวจรับทราบผลการตรวจสอบตามแบบฟอร์มรายงานความไม่สอดคล้อง (NCR)
10	บันทึกแบบฟอร์มรายงานความไม่สอดคล้อง	ผู้ตรวจสอบภายในบันทึกแบบฟอร์มรายงานความไม่สอดคล้อง
11	ติดตามผลการดำเนินการแก้ไขและป้องกัน	ผู้ตรวจสอบภายในติดตามผลการดำเนินการแก้ไขและป้องกัน

9. ขั้นตอนการปฏิบัติเพื่อการแก้ไข (Corrective Action)

ขั้นตอนในการดำเนินการแก้ไขมีผู้เกี่ยวข้องคือ ฝ่ายผู้ตรวจสอบภายใน ฝ่ายหน่วยรับตรวจหรือผู้ได้รับมอบหมายฝ่ายคณะกรรมการด้านการรักษาความปลอดภัยสารสนเทศ และคณะกรรมการตรวจสอบ ซึ่งได้กำหนดขั้นตอนในการดำเนินการไว้ดังแผนภาพต่อไปนี้



10. คำอธิบายขั้นตอนการปฏิบัติเพื่อการแก้ไข

ลำดับที่	ขั้นตอน	คำอธิบาย
1	ระบุประเด็นที่ไม่สอดคล้องที่ตรวจพบ	ผู้ตรวจสอบภายใน ระบุประเด็นที่ไม่สอดคล้องตามข้อกำหนดที่ตรวจพบ โดยบันทึกลงในแบบฟอร์ม Non-conformity Report (NCR) (IA.FRM.001)ในส่วนที่ 1 โดยเลือกประเภท NCR - ความไม่สอดคล้องหลัก (Major Non-conformity) - ความไม่สอดคล้องย่อย (Minor Non-conformity) - ข้อสังเกต (Observation) - โอกาสในการปรับปรุง (Opportunity for Improvement) จากนั้นระบุรายละเอียดสิ่งที่ตรวจพบ ข้อกำหนดที่ไม่สอดคล้องกับ ISO/IEC 27001 ระบุความเสี่ยงและผลกระทบ และข้อเสนอแนะ แล้วลงชื่อ ผู้จัดทำ
2	วิเคราะห์ถึงสาเหตุและแนวทางการแก้ไข	หน่วยรับตรวจ / ผู้ได้รับมอบหมาย วิเคราะห์ถึงสาเหตุที่ทำให้ไม่เป็นไปตามข้อกำหนดและหาแนวทางการแก้ไข โดยบันทึกลงในแบบฟอร์ม Non-conformity Report (NCR)(IA.FRM.001) ในส่วนที่ 2 จากนั้น กรอกวันที่คาดดำเนินการแล้วเสร็จแล้ว จึงลงชื่อ ผู้รับผิดชอบ
3	พิจารณาสาเหตุ และความเหมาะสมของแนวทางการแก้ไข	ผู้ตรวจสอบภายใน พิจารณาสาเหตุที่ทำให้ไม่เป็นไปตามข้อกำหนดและความเหมาะสมของแนวทางการแก้ไข
4	พิจารณาเห็นชอบหรือไม่	ผู้ตรวจสอบภายใน พิจารณาเห็นชอบสาเหตุและความเหมาะสมของแนวทางการแก้ไข ▪ หากเห็นชอบสาเหตุและความเหมาะสมของแนวทางการแก้ไข /ป้องกันให้ดำเนินการตามข้อ5 ▪ หากไม่เห็นชอบสาเหตุและความเหมาะสมของแนวทางการแก้ไข/ป้องกันให้ดำเนินการตามข้อ13 โดยบันทึกลงในแบบฟอร์ม Non-conformity Report (NCR) (IA.FRM.001) ในส่วนที่ 3 โดยระบุความเห็นว่าเห็นชอบตามเสนอหรือไม่เห็นชอบ พร้อมทั้งระบุรายละเอียด แล้วลงชื่อ ผู้สอบทาน และวันที่
5	แจ้งผลการพิจารณาเห็นชอบ	ผู้ตรวจสอบภายใน แจ้งผลการพิจารณาเห็นชอบสาเหตุและความเหมาะสมของแนวทางการแก้ไข

ลำดับที่	ขั้นตอน	คำอธิบาย
6	รับทราบผลการพิจารณาเห็นชอบ	หน่วยรับตรวจ / ผู้ได้รับมอบหมาย รับทราบผลการพิจารณาเห็นชอบสาเหตุและความเหมาะสมของแนวทางการแก้ไข
7	ดำเนินการแก้ไขและบันทึกผล	หน่วยรับตรวจ / ผู้ได้รับมอบหมาย ดำเนินการแก้ไขและบันทึกผล
8	สรุปผลการดำเนินงาน และรายงานต่อผู้ตรวจสอบภายใน	หน่วยรับตรวจ / ผู้ได้รับมอบหมาย สรุปผลการดำเนินงาน และรายงานผลต่อผู้ตรวจสอบภายใน
9	พิจารณาผลการแก้ไขและบันทึกผล	ผู้ตรวจสอบภายใน พิจารณาผลการแก้ไขว่าต้องแก้ไขอีกหรือไม่ และบันทึกผล โดยบันทึกลงในแบบฟอร์ม Non-conformity Report (NCR) (IA.FRM.001)ในส่วนที่ 4 บันทึกผลการติดตาม โดยระบุสถานะดำเนินการเรียบร้อยหรือดำเนินการยังไม่แล้วเสร็จพร้อมทั้งรายละเอียด แล้วลงชื่อ ผู้ติดตามผลและวันที่
10	พิจารณาต้องแก้ไขหรือไม่	ผู้ตรวจสอบภายใน พิจารณาต้องแก้ไขหรือไม่ ▪ หากต้องแก้ไขผลการแก้ไขให้ดำเนินการตามข้อ7 ▪ หากไม่ต้องแก้ไขผลการแก้ไขให้ดำเนินการตามข้อ11
11	รายงานผลการแก้ไขต่อคณะกรรมการด้านการรักษาความมั่นคงปลอดภัยและคณะกรรมการตรวจสอบ	ผู้ตรวจสอบภายใน รายงานผลการแก้ไขต่อคณะกรรมการด้านการรักษาความปลอดภัยสารสนเทศและคณะกรรมการตรวจสอบ
12	รับทราบผล และลงนามอนุมัติผลการดำเนินงาน	คณะกรรมการด้านการรักษาความปลอดภัยสารสนเทศรับทราบผลและลงนามอนุมัติผลการดำเนินงาน
13	แจ้งผลการพิจารณาไม่เห็นชอบ	ผู้ตรวจสอบภายใน แจ้งผลการพิจารณาไม่เห็นชอบสาเหตุและความเหมาะสมของแนวทางการแก้ไข
14	รับทราบผลการพิจารณาไม่เห็นชอบ	หน่วยรับตรวจ / ผู้ได้รับมอบหมาย รับทราบผลการพิจารณาไม่เห็นชอบสาเหตุและความเหมาะสมของแนวทางการแก้ไข

11. การวางแผนและจัดเตรียมทรัพยากร

สำนักตรวจสอบมีการกำหนดกิจกรรมการตรวจสอบระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศภายในไว้ในแผนการตรวจสอบภายในประจำปีงบประมาณ โดยการตรวจสอบระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศภายในจะดำเนินการปีละ 1 ครั้ง หรือเมื่อมีความต้องการ โดยมีการจัดทำแผนการปฏิบัติงานและตารางแผนการปฏิบัติงาน เพื่อแจ้งให้หน่วยรับตรวจทราบเป็นการล่วงหน้า

สำนักตรวจสอบจะต้องเตรียมแผนการปฏิบัติงานและตารางแผนการปฏิบัติงานดังนี้

- วัตถุประสงค์และขอบเขตของการตรวจสอบ
- หน่วยงานและผู้รับผิดชอบ

- รายชื่อสมาชิกทีมตรวจสอบ
- ประเภทและวิธีการตรวจสอบ
- กิจกรรมที่ทำการตรวจสอบ
- วันที่ สถานที่ เวลา ในการตรวจสอบและวันที่ในการเสนอรายงานการตรวจสอบ
- ผู้เสนอแผน ผู้เห็นชอบแผน ผู้รับผิดชอบหลัก และผู้รับทราบ

ผู้ตรวจสอบภายในจัดทำเอกสาร ดังนี้

1) แผนการตรวจสอบประจำปีงบประมาณ
2) ใบมอบหมายให้ทำการตรวจสอบ (แบบ ตส.1_01)
3) ผังแสดงทางเดินของการควบคุม (Control Flow) (แบบ ตส.1_03)
4) แบบประเมิน COSO และ ข้อบ่งชี้ทุจริต (แบบ ตส.1_04)
5) แผนการตรวจสอบในรายละเอียด (แบบ ตส.1_05)
6) แบบรับรองความขัดแย้งทางผลประโยชน์ – ผู้ตรวจสอบ (แบบ ตส.1_06)
7) บันทึกแจ้งเปิดการตรวจสอบ (แบบ ตส.1_07)
8) รายการตรวจสอบ (Audit Matrix) (IA.LST.001)
9) ตารางแผนการปฏิบัติงาน (Audit plan) (IA.PLN.002)
10) แนวทางการตรวจสอบ (Audit Program) (แบบ ตส.1_08)
11) กระดาษทำการ (แบบ ตส.1_09)
12) บันทึกแจ้งปิดการตรวจสอบ (แบบ ตส.1_11)
13) บันทึกปิดการตรวจสอบ (แบบ ตส.1_12)
14) แบบประเมินผลด้านการให้ความเชื่อมั่น : โดยหน่วยงานผู้รับตรวจ (แบบ ตส.1_14)
15) บันทึกรายงานผลการตรวจสอบ (แบบ ตส.1_15)
16) บทสรุปสำหรับผู้บริหาร (แบบ ตส.1_16)
17) รายงานผลการตรวจสอบ (แบบ ตส.1_16.1)
18) แบบรายงานการควบคุมภายใน (แบบ ตส.1_17)
19) แบบฟอร์มรายงานความไม่สอดคล้อง (Non-conformity Report Form : NCR) (IA.FRM.001)
20) แบบประเมินความร่วมมือของหน่วยรับตรวจ : โดยผู้ตรวจสอบภายใน (แบบ ตส.1_20)

12. การประชุมเปิดการตรวจสอบ

การประชุมเปิดการตรวจสอบจะต้องจัดขึ้นระหว่างหัวหน้าผู้ตรวจสอบภายใน ตัวแทนคณะกรรมการฯ และหน่วยรับตรวจ โดยมีวัตถุประสงค์ ดังนี้

- เพื่อชี้แจงวัตถุประสงค์ ขอบเขต และแผนการตรวจสอบ
- การสรุปวิธีการตรวจสอบและกิจกรรมที่จะทำการตรวจสอบ
- การกำหนดผู้รับผิดชอบหรือช่องทางการสื่อสาร

- การชี้แจงรูปแบบการรายงานและการปิดตรวจสอบ

การประชุมเปิดการตรวจสอบ เพื่อพิจารณาดังนี้

- จุดประสงค์และขอบเขตของการตรวจสอบ
- การยืนยันแผนการตรวจสอบ

13. จัดทำแนวทางตรวจสอบ

ผู้ตรวจสอบภายในจะต้องจัดทำแนวทางการตรวจสอบ โดยการสรุปข้อกำหนดของระบบความมั่นคงปลอดภัยสารสนเทศ ISO 27001 หรือเกณฑ์การตรวจสอบเป็นแนวทางการตรวจสอบ เช่น การสัมภาษณ์ การสอบทาน โดยมีหัวข้ออย่างน้อยดังนี้

- ข้อกำหนด/เกณฑ์การตรวจสอบ
- แนวทางการตรวจสอบ
- ผลการตรวจสอบ

14. การปฏิบัติงานตรวจสอบ

การดำเนินการตรวจสอบระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศภายในได้มาจากการสัมภาษณ์ การตรวจสอบเอกสาร การสังเกต การใช้การวิเคราะห์ การทดสอบ กิจกรรมควบคุม และเงื่อนไขในขอบเขตที่ตรวจสอบ โดยจะพิจารณาถึงความสอดคล้องกับความปลอดภัยเป็นหลักผู้ตรวจสอบภายในจะตรวจสอบตามตารางแผนการปฏิบัติงานและแนวทางการตรวจสอบดังนี้

- การระบุและรวบรวมข้อมูลที่ใช้ในการตรวจสอบ
- การวิเคราะห์และประเมินผล
- การบันทึกข้อมูลที่เกี่ยวข้อง

ผู้ตรวจสอบภายในจะพิจารณาประเด็นที่ตรวจพบ ดังนี้

1. การปฏิบัตินั้นสอดคล้องกับมาตรการควบคุมในข้อกำหนดแล้ว
2. การปฏิบัติไม่สอดคล้องกับมาตรการควบคุมในข้อกำหนด หรือมีข้อเสนอแนะเพื่อปรับปรุงการทำงานให้มีประสิทธิผลมากยิ่งขึ้น ผู้ตรวจสอบภายในจะเขียนรายงานไว้ในแบบฟอร์มรายงานความไม่สอดคล้อง (Non-conformity Report Form: NCR)

ทั้งนี้ ผู้ตรวจสอบภายในและหน่วยรับตรวจจะเป็นผู้พิจารณาถึงระบบหรือสิ่งที่ได้ดำเนินการว่าสิ่งนั้นเป็นไปตามข้อกำหนดหรือไม่ โดยผู้ตรวจสอบภายในจะจำแนกหมวดหมู่ผลการตรวจสอบที่พบเหล่านั้น ซึ่งหลักการพิจารณาหมวดหมู่จะอยู่ในขั้นตอนการปฏิบัติในการแก้ไข (Corrective Action)

15. การรายงานผลการตรวจสอบ

ผู้ตรวจสอบภายในจะดำเนินการประชุมปิดการตรวจสอบหลังจากดำเนินการตรวจสอบเสร็จเรียบร้อย โดยวัตถุประสงค์เพื่อ

- การทบทวนและวิเคราะห์ผลที่พบ
- การรวบรวมผลที่พบทั้งหมดโดยรวมถึงการรวมกลุ่มและการจัดระเบียบ
- การจำแนกหมวดหมู่ผลที่พบ
- การเตรียมข้อเสนอแนะและรายงานการตรวจสอบ

อนึ่ง เพื่อให้การดำเนินการแก้ไขสามารถติดตามผลได้ ผู้ตรวจสอบภายในหน่วยรับตรวจและคณะกรรมการฯ จะดำเนินการประชุมเพื่อแจ้งผลการตรวจสอบ ซึ่งจะกล่าวในหัวข้อต่อไป

16. การรับทราบและแก้ไข

ผู้ตรวจสอบภายในหน่วยรับตรวจและคณะกรรมการฯ จะประชุมร่วมกันเพื่อรับทราบผลการตรวจสอบระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศภายในโดยหัวหน้าผู้ตรวจสอบภายในรายงานผลที่พบ การสังเกต และข้อเสนอแนะ และใช้แบบฟอร์มรายงานความไม่สอดคล้อง (Non-conformity Report Form: NCR) เพื่อให้หน่วยรับตรวจสามารถบันทึกรายละเอียดสาเหตุที่เกิดความไม่สอดคล้องและแผนการแก้ไขพร้อมระบุวันที่สามารถดำเนินการแก้ไขได้เสร็จสิ้น

การดำเนินการแก้ไขเป็นขั้นตอนที่คณะกรรมการฯ และหน่วยรับตรวจจะดำเนินการร่วมกันเพื่อหาวิธีการแก้ไขความไม่สอดคล้อง หลังจากนั้นจึงดำเนินการสั่งการให้ผู้ดูแลหรือผู้รับผิดชอบดำเนินการแก้ไข การแก้ไขควรดำเนินการให้เสร็จสิ้นตามระดับความสำคัญของข้อเสนอแนะเมื่อดำเนินการแก้ไขเสร็จสิ้นจะรายงานผลแก่หัวหน้าผู้ตรวจสอบภายใน เพื่อการติดตามผลต่อไป

17. การจัดทำรายงานผลการตรวจสอบ

ภายหลังการดำเนินการประชุมปิดการตรวจสอบเสร็จสิ้นแล้ว ผู้ตรวจสอบภายในจะสรุปรายงานผลการตรวจสอบ ซึ่งประกอบด้วยหัวข้ออย่างน้อย ดังนี้

- บทสรุปผู้บริหาร
- วัตถุประสงค์การตรวจสอบ
- ขอบเขตการตรวจสอบ
- สิ่งที่ตรวจพบ
- ความเสี่ยง / การควบคุมภายใน
- ประเด็นที่ตรวจพบ / ข้อเท็จจริงและสาเหตุ / ความเห็นของผู้ตรวจสอบ / ข้อเสนอแนะ
- ความเห็นของหน่วยรับตรวจ / แนวทางแก้ไข
- การจัดลำดับความสำคัญของผลการตรวจสอบ (Audit Rating) และข้อเสนอแนะ

โดยมีตารางแสดงการเปรียบเทียบระดับความไม่สอดคล้องกับการจัดลำดับความสำคัญของผลการตรวจสอบ ของสำนักตรวจสอบ ดังนี้

ระดับความไม่สอดคล้อง	การจัดระดับความสำคัญของผลการตรวจสอบ
ความไม่สอดคล้องหลัก (Major Non-conformity)	สูง (High)
ความไม่สอดคล้องย่อย (Minor Non-conformity)	ปานกลาง (Medium)
ข้อสังเกต (Observation)	ต่ำ (Low)
โอกาสในการปรับปรุง (Opportunity for Improvement)	-

รายละเอียดเหล่านี้จะถูกบรรจุในรายงานเพื่อแสดงถึงประสิทธิภาพ และประสิทธิผลของการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ

18. เอกสารสำหรับบันทึก

1. แผนการตรวจสอบประจำปีงบประมาณ*
2. ใบมอบหมายให้ทำการตรวจสอบ (แบบ ตส.1_01)*
3. ผังแสดงทางเดินของการควบคุม (Control Flow) (แบบ ตส.1_03)*
4. แบบประเมิน COSO และ ข้อบ่งชี้ทุจริต (แบบ ตส.1_04)*
5. แผนการตรวจสอบในรายละเอียด (แบบ ตส.1_05)*
6. แบบรับรองความขัดแย้งทางผลประโยชน์ – ผู้ตรวจสอบ (แบบ ตส.1_06)*
7. บันทึกแจ้งเปิดการตรวจสอบ (แบบ ตส.1_07)*
8. รายการตรวจสอบ (Audit Matrix) (IA.LST.001)
9. ตารางแผนการปฏิบัติงาน (Audit plan) (IA.PLN.002)
10. แนวทางการตรวจสอบ (Audit Program) (แบบ ตส.1_08)*
11. กระดาษทำการ (แบบ ตส.1_09)*
12. บันทึกแจ้งปิดการตรวจสอบ (แบบ ตส.1_11)*
13. บันทึกปิดการตรวจสอบ (แบบ ตส.1_12)*
14. แบบประเมินผลด้านการให้ความเชื่อมั่น : โดยหน่วยงานผู้รับตรวจ (แบบ ตส.1_14)*
15. บันทึกรายงานผลการตรวจสอบ (แบบ ตส.1_15)*
16. บทสรุปสำหรับผู้บริหาร (แบบ ตส.1_16)*

17. รายงานผลการตรวจสอบ (แบบ ตส.1_16.1)*
18. แบบรายงานการควบคุมภายใน (แบบ ตส.1_17)*
19. แบบฟอร์มรายงานความไม่สอดคล้อง (Non-conformity Report Form : NCR) (IA.FRM.001)
20. แบบประเมินความร่วมมือของหน่วยรับตรวจ : โดยผู้ตรวจสอบภายใน (แบบ ตส.1_20)*

หมายเหตุ : *อ้างอิงรหัสเอกสารตามคู่มือการปฏิบัติงานตรวจสอบภายใน สำนักตรวจสอบ

19. การวัดประสิทธิผลงานตรวจสอบ

19.1 งานตรวจสอบมีการปรับปรุงคุณภาพงานอย่างต่อเนื่อง

ตัวชี้วัด	% ที่หน่วยรับตรวจที่ยอมรับประเด็น/ข้อตรวจพบที่สำคัญ/วิกฤต/ความเสี่ยงสูง พร้อมจัดทำแผนปรับปรุง
ข้อกำหนด	Clause 10.1 ความไม่สอดคล้องและการดำเนินการแก้ไข
ผู้ติดตามและวัดผล	นักคอมพิวเตอร์ 7 /ผู้ตรวจสอบ 7 กตส.ฝตล. และ ผอ.กตส.
ผู้วิเคราะห์และรายงานผล	หัวหน้าทีมตรวจสอบ
ข้อมูลประกอบการชี้วัด	รายงานความไม่สอดคล้อง (Non-conformity Report Form :NCR)
วิธีการคำนวณตัวชี้วัด	ร้อยละของจำนวน NCR ที่ได้รับการแก้ไขแล้วเสร็จตามแผนปรับปรุงที่กำหนดไว้จากทั้งหมด (คำนวณเฉพาะระดับ Major และ Minor)
ความถี่ในการติดตาม	ปีละ 1 ครั้ง
เป้าหมาย	มีการแก้ไขตามที่ในกำหนดแผนปรับปรุง ร้อยละ 100
หมายเหตุ	กระบวนการตรวจสอบต้องได้รับการ ทบทวน/ปรับปรุง โดยมีการควบคุม/ดูแล โดย Information Security หรือ คณะกรรมการที่เกี่ยวข้อง เพื่อให้ความมั่นใจว่า ประเด็น/ข้อตรวจพบที่สำคัญ/วิกฤต/ความเสี่ยงสูง ได้มีการระบุประเด็นและมีการจัดทำแผนปรับปรุง

20. การสื่อสาร

ลำดับที่	รายการ	ความถี่	ผู้รับผิดชอบในการสื่อสาร	ผู้รับการสื่อสาร	ช่องทางในการสื่อสาร			
					จัดประชุม/หารือ/บันทึกข้อความ/รายงาน	Intranet	ฝึกอบรม	แบบสอบถาม
1	คู่มือขั้นตอนการปฏิบัติในการตรวจสอบระบบความมั่นคงปลอดภัยสารสนเทศ ISO 27001	ปีละ 1 ครั้ง	- ผู้ตรวจสอบภายใน - ผู้สอบทาน (การตรวจสอบภายใน)	- ผู้ตรวจสอบภายใน - ผู้สอบทาน (การตรวจสอบภายใน) - หน่วยรับตรวจ/ผู้ได้รับมอบหมาย	✓	✓		
2	อบรม ISO 27001 และสร้างความตระหนักด้านความมั่นคงปลอดภัยสารสนเทศ	ปีละ 1 ครั้ง	- ผู้ตรวจสอบภายใน - ผู้สอบทาน (การตรวจสอบภายใน)	- ผู้ตรวจสอบภายใน - ผู้สอบทาน (การตรวจสอบภายใน)			✓	
3	เอกสารในการปฏิบัติงานตรวจสอบ - ชุดเปิดตรวจสอบ - Audit Plan - NCR (ถ้ามี) - ใบปิดตรวจสอบ	ปีละ 1 ครั้ง	- ผู้ตรวจสอบภายใน - ผู้สอบทาน (การตรวจสอบภายใน)	- คณะกรรมการด้านการรักษาความปลอดภัยสารสนเทศ	✓			
	- รายงานผลการตรวจสอบ	ปีละ 1 ครั้ง	- ผู้ตรวจสอบภายใน - ผู้สอบทาน (การตรวจสอบภายใน)	- คณะกรรมการด้านการรักษาความปลอดภัยสารสนเทศ - คณะกรรมการตรวจสอบ - คณะอนุกรรมการพัฒนาเทคโนโลยีดิจิทัลของ กปน. /IT Steering Committee	✓			
4	แบบประเมินทีมตรวจสอบภายใน: โดยหน่วยงานผู้รับตรวจ (แบบ ตส.1_14)	ปีละ 1 ครั้ง	ผู้ตรวจสอบภายใน	หน่วยรับตรวจ/ผู้ได้รับมอบหมาย				✓

ลำดับที่	รายการ	ความถี่	ผู้รับผิดชอบในการสื่อสาร	ผู้รับการสื่อสาร	ช่องทางในการสื่อสาร			
					จัดประชุม/หารือ/บันทึกข้อความ/รายงาน	Intranet	ฝึกอบรม	แบบสอบถาม
5	แบบประเมิน : ความร่วมมือของหน่วยรับตรวจ (แบบ ตส.1_20)	ปีละ 1 ครั้ง	ผู้ตรวจสอบภายใน	หน่วยรับตรวจ/ผู้ได้รับมอบหมาย				✓

หมายเหตุ : ผู้รับผิดชอบในการสื่อสารสามารถเลือกช่องทางในการสื่อสารได้ตามความเหมาะสม

21. การวิเคราะห์และประเมินการรับรู้ของผู้มีส่วนได้ส่วนเสียที่สำคัญที่เกี่ยวข้องกับกระบวนการ

ถ่ายทอดกระบวนการตรวจสอบการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศแก่ผู้มีส่วนได้ส่วนเสียอย่างครบถ้วน โดยมีการแสดงการวิเคราะห์ที่ชัดเจนและมีการประเมินการรับรู้ของผู้มีส่วนได้ส่วนเสีย

22. การกำหนดการวัด ติดตาม วิเคราะห์ประเมิน ตัววัดผลลัพธ์ (Outcome) ของกระบวนการ

กำหนดการวัด ติดตาม วิเคราะห์ประเมิน ตัววัดผลลัพธ์ (Outcome) ของกระบวนการตรวจสอบการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ