แบบฟอร์มการพัฒนาปรับปรุงและบันทึกความรู้หลังการปฏิบัติงาน (AAR)

1.ชื่อองค์ความรู้	**5.3 กระบวนการตรวจสอบการบริหารจัดการความมั่งคงปลอดภัยสารสนเทศขององค์กร**
2.ประเภทสินทรัพย์ทางความรู้	ด้านการพัฒนาเทคโนโลยีดิจิทัล
3.วันที่บันทึกความรู้	10 ตุลาคม 2567
4.ผู้เข้าร่วมบันทึกความรู้	1. นายสุเมธ เพ็ชรนิล
	2. นางสาวทรายแก้ว เกษมณี
	3.

5.วัตถุประสงค์ของการบันทึกความรู้เรื่องนี้

1. เพื่อนำข้อเสนอแนะ/ปัญหาอุปสรรคที่พบจากกระบวนการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศมาพิจารณาพัฒนาปรับปรุงอย่างต่อเนื่อง และยกระดับการดำเนินงานด้านการพัฒนาเทคโนโลยีดิจิทัล
2. เพื่อสรุปองค์ความรู้ที่ได้จากการปรับปรุงกระบวนการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศซึ่งสอดคล้องกับเกณฑ์ประเมินผลด้านการพัฒนาเทคโนโลยีดิจิทัล
3. เพื่อเป็นส่วนหนึ่งขององค์ความรู้ของการเคหะแห่งชาติ และใช้เป็นศูนย์กลางความรู้ให้กับหน่วยงานอื่น นำไปประยุกต์ใช้ในการปรับปรุงกระบวนการทำงานต่อไป

6. รายละเอียดเกี่ยวกับกระบวนการ (ก่อนปรับปรุง)

ชื่อกระบวนการ	**การบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ**
วัตถุประสงค์ของกระบวนการ	1. เพื่อบริหารจัดการ การตรวจสอบการบริหารจัดการความมั่งคงปลอดภัยสารสนเทศขององค์กร อย่างเป็นระบบ มีประสิทธิภาพ และผ่านการตรวจรับรองมาตรฐานสากล 2. เพื่อปรับปรุงทบทวนขอบเขตการประเมินระบบบริหารความมั่นคงปลอดภัยสารสนเทศ 3. เพื่อทบทวนเกณฑ์การตรวจประเมิน และขอบเขตการประเมิน การพิจารณาเลือกผู้ตรวจประเมินและดำเนินการตรวจประเมินอย่างมีมาตรฐาน 4. เพื่อให้การดำเนินงานไม่พบความไม่สอดคล้อง (CAR) ตามข้อกำหนดในการตรวจประเมิน

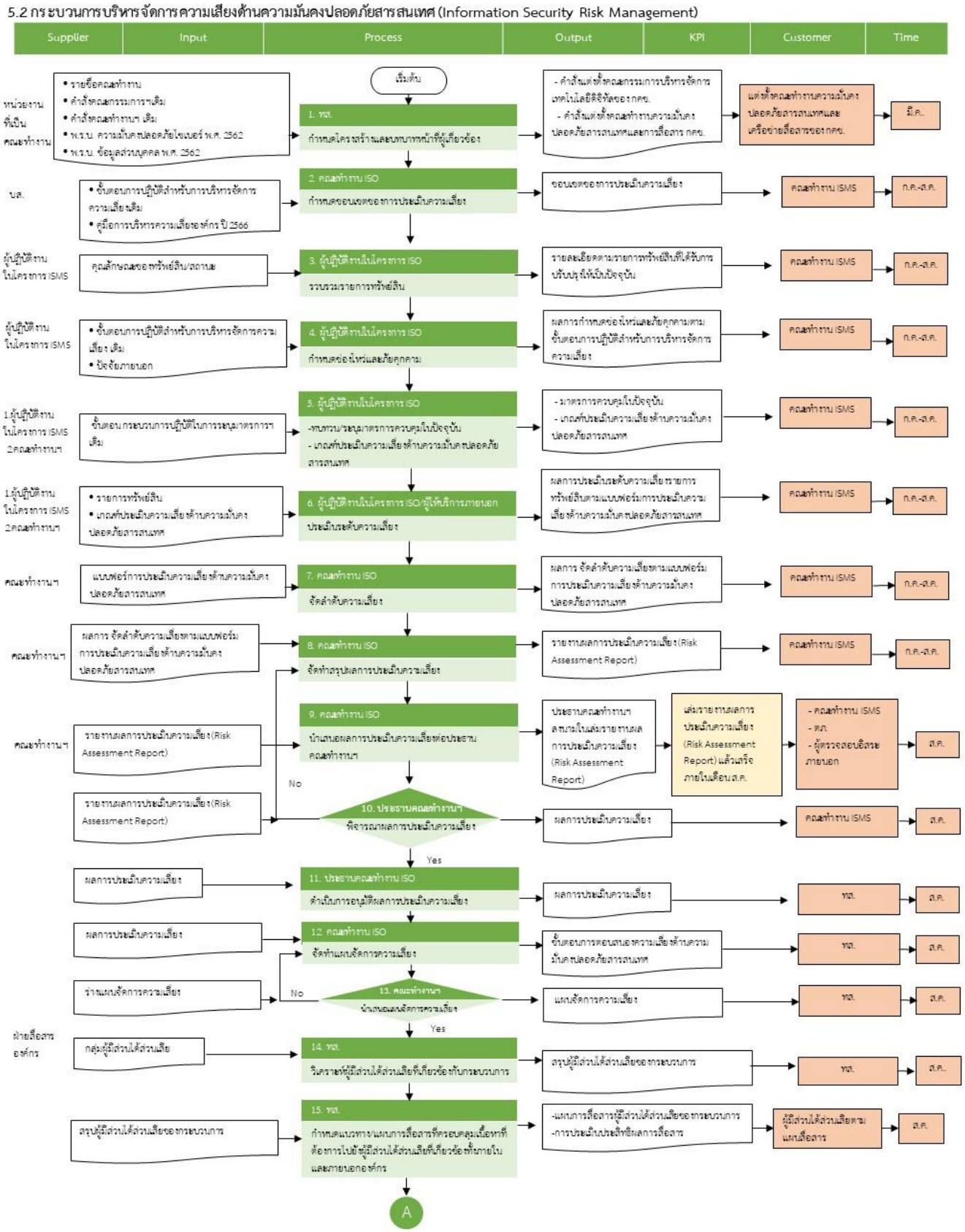
7. แนวทางการปรับปรุงกระบวนการ (ใช้ในปี 2566)

1. ปรับปรุงกระบวนการใน SIPOC เพิ่มขั้นตอนดำเนินการตามคู่มือและแนวปฏิบัติการตรวจสอบการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศขององค์กร จากเดิมจำนวน 21 กระบวนการ ปรับเป็น 22 กระบวนการ
2. ทบทวนและปรับปรุงตัวชี้วัดของกระบวนการให้มี KPI in process จำนวน 6 ตัวชี้วัด
3. จัดทำ RACI Chat ของกระบวนการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ
4. จัดทำแผนการสื่อสารผู้มีส่วนได้ส่วนเสียของกระบวนการ ตามกลุ่มผู้มีส่วนได้ส่วนเสียขององค์กร และจำแนกผู้มีส่วนได้ส่วนเสียตาม RACI Chat
6. กำหนดให้มีการติดตามและการวัดผลลัพธ์ตามตัวชี้วัดประสิทธิผลของกระบวนการ และนำผลลัพธ์รายงานต่อคณะทำงาน

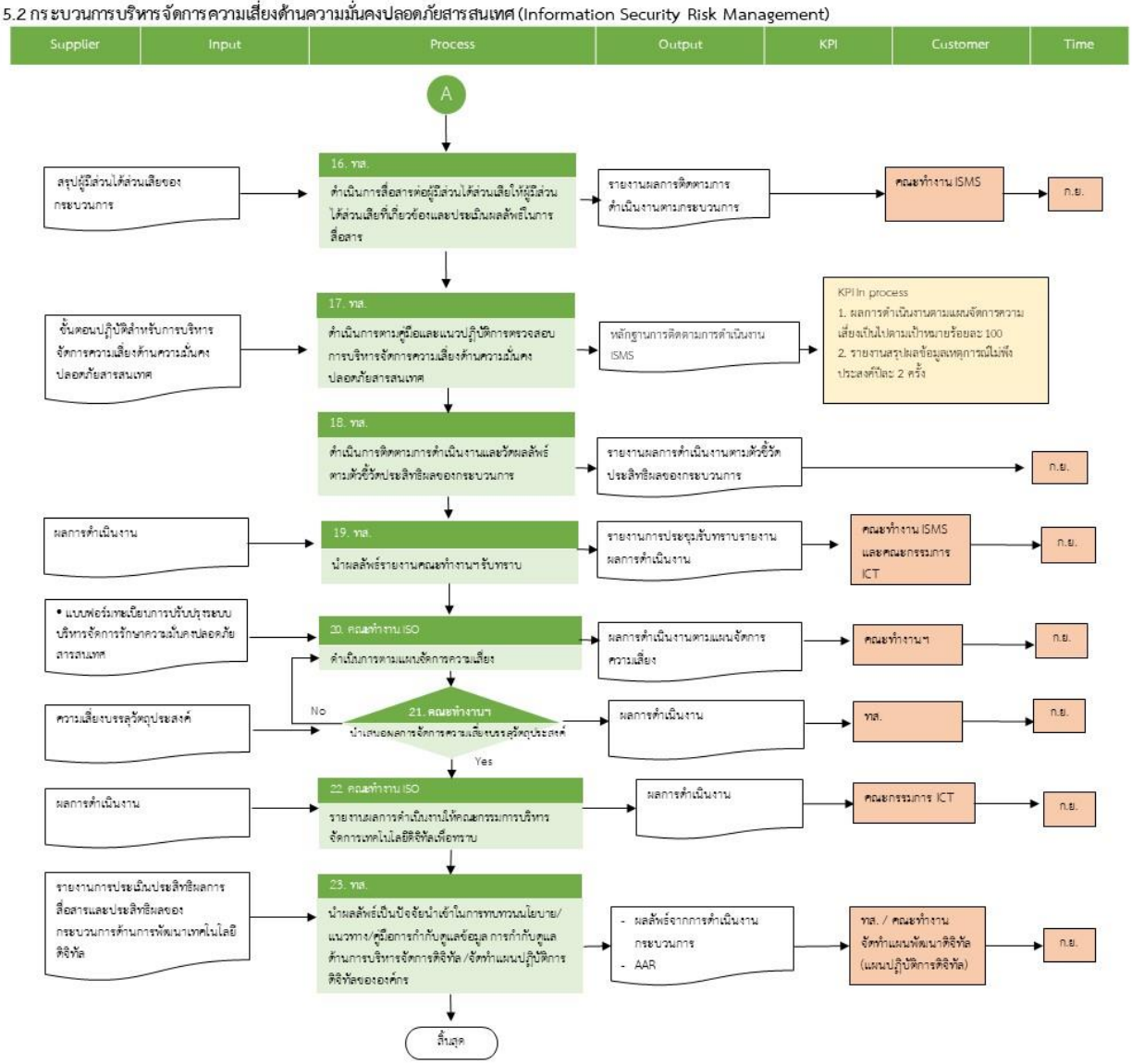
8. รายละเอียดเกี่ยวกับกระบวนการ (หลังปรับปรุง)

ตัวชี้วัดของกระบวนการ ประจำปี 2567	**เป้าหมายตัวชี้วัดของกระบวนการ ประจำปี 2567**	**ผลการดำเนินงาน ประจำปี 2567**
1. รายงานสรุปผลข้อมูลเหตุการณ์ไม่พึงประสงค์	ปีละ 2 ครั้ง	รายงานผลต่อคณะทำงาน 2 ครั้ง เมื่อวันที่ 26 สิงหาคม 2567 และ 26 กันยายน 2567 ไม่เกิดเหตุการณ์ไม่พึงประสงค์
2. ความสำเร็จของการจัดทำแผนตรวจสอบความมั่นคงปลอดภัยสารสนเทศ	ปีละ 1 ครั้ง	เผยแพร่แผนการตรวจสอบเมื่อวันที่ 16 กันยายน 2567 และ 26 กันยายน 2567

9. Flowchart กระบวนการ ปี 2567



5.2 กระบวนการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ (Information Security Risk Management)



10. สิ่งที่พบจากการดำเนินงานปี 2567	
ประเด็น	**รายละเอียดประเด็นที่มีการพัฒนาปรับปรุง**
	1. ปรับปรุงกระบวนการใน SIPOC เพิ่มขั้นตอนดำเนินการตามคู่มือและแนวปฏิบัติการตรวจสอบการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศขององค์กร จากเดิมจำนวน 21 กระบวนการ ปรับเป็น 22 กระบวนการ 2. ทบทวนเกณฑ์ การคัดเลือกผู้ตรวจประเมิน โดยกำหนดให้ผู้รับจ้างเสนอเกณฑ์ให้พิจารณาและคัดเลือกผู้ตรวจประเมินภายนอกตามหลักเกณฑ์ที่กำหนดขึ้นไว้ ซึ่งไม่มีการปรับปรุง รายละเอียด ดังนี้ 1) สัดส่วนการตลาด(Market Share) มีการตรวจรับรองจำนวนมาก (ตามเงื่อนไขใน องค์กรผู้ตรวจประเมินที่มีชื่อเสียง) 2) มีการตรวจประเมินของหน่วยงานภาครัฐ และรัฐวิสาหกิจ 3) มีผู้ตรวจสอบเป็นคนไทย (เรื่องการสื่อสาร) 4) เป็นบริษัทที่มีชื่อเสียง และก่อตั้งมายาวนาน (ตามเงื่อนไขใน องค์กรผู้ตรวจประเมินที่มีชื่อเสียง น่าเชื่อถือ) 5) การตรวจประเมินต่อเนื่อง ทราบบริบทของ กคช.เป็นอย่างดี 3. ดำเนินการวิเคราะห์ผู้มีส่วนได้ส่วนเสียของกระบวนการตามกลุ่มผู้มีส่วนได้ส่วนเสียขององค์กร และจำแนกผู้มีส่วนได้ส่วนเสียตาม RACI Chat เพื่อนำไปจัดทำแผนการสื่อสารตามกลุ่มของผู้มีส่วนได้ส่วนเสีย 4. จัดทำแผนการสื่อสารของกระบวนการโดยแบ่งเป็นกลุ่มผู้มีส่วนได้ส่วนเสีย สิ่งที่ต้องการจะสื่อสาร ช่องทางการสื่อสาร จำนวนครั้งในการสื่อสาร ตัวชี้วัดของการสื่อสาร และการประเมินผลลัพธ์ของการสื่อสารตามตัวชี้วัด เพื่อรวบรวมข้อมูลเพื่อพัฒนาและปรับปรุงกระบวนการในปีถัดไป 5. จัดทำแบบประเมินผลกระบวนการทำงานและบันทึกความรู้ (After Action Review : AAR) ตาม SIPOC ย่อย สำหรับกระบวนการตรวจสอบการบริหารจัดการความมั่งคงปลอดภัยสารสนเทศขององค์กร เพื่อเป็นฐานองค์ความรู้ด้าน CG และในระดับองค์กร (KM) พร้อมนำไปจัดเก็บในระบบการจัดการความรู้ของสำนักงานฯ เพื่อใช้แลกเปลี่ยนเรียนรู้และ นำไปใช้ประโยชน์ในการปรับปรุงกระบวนการปฏิบัติงานอื่น ๆ ต่อไป
ปัญหา/อุปสรรค	- ขาดผู้เชี่ยวชาญด้านกฎหมายดิจิทัล/พ.ร.บ.การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.2562 และอื่น ๆ
สาเหตุของปัญหา/อุปสรรค	1. นโยบายผู้บริหาร ให้เพิ่มการดำเนินการด้านกฎหมายที่เกี่ยวข้องให้สอดคล้องกับการดำเนินการในกระบวนการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ ทำให้เพิ่มขั้นตอนการจัดหาผู้เชี่ยวชาญด้านกฎหมายฯ ซึ่งใช้เวลาในการดำเนินการเพิ่มขึ้น 2. กระบวนการจัดหา/จัดจ้างที่ปรึกษา พ.ร.บ.จัดซื้อจัดจ้างและประกาศต่าง ๆ ทำให้กระบวนจัดหาที่ปรึกษาต้องใช้เวลามากขึ้นทำให้โครงการล่าช้ากว่าแผน

ทำ11. สาเหตุหรือที่มาในการพัฒนาปรับปรุงกระบวนการทำงานในปัจจุบัน (As-Is Process)

☒ ข้อเสนอแนะของผู้ประเมิน IRDP

☒ หลักเกณฑ์ Enablers หรือมาตรฐานหรือกรอบแนวทางที่เป็นที่ยอมรับ (เช่น มาตรฐาน ISO OECD COSO-ERM เป็นต้น)

☐ ผลลัพธ์ไม่เป็นไปตามเป้าหมายที่กำหนด

☒ เพิ่มประสิทธิภาพกระบวนการทำงาน เช่น เพิ่มกระบวนการสื่อสาร การติดตาผล การวัดดผล

☒ การเปลี่ยนแปลงของสภาพแวดล้อมที่เกี่ยวข้องกับกระบวนการ เช่น กฎหมาย ข้อบังคับ ระเบียบ คำสั่ง ประกาศ เป็นต้น

☒ นโยบายรัฐบาล กฎเกณฑ์และข้อเสนอแนะของหน่วยงานกำกับดูแล

☒ แนวทางปฏิบัติที่ดีของหน่วยงานชั้นนำหรือหน่วยงานคู่เทียบ

☐ อื่นๆ (โปรดระบุ) เช่น ข้อเสนอแนะจากการถามตอบในกลุ่ม LINE ของ SE-EM ของ สคร. หรือคำถาม-คำตอบในวัน Feedback Day

☐ ไม่เปลี่ยนแปลง

แบบฟอร์มการพัฒนาปรับปรุงและบันทึกความรู้หลังการปฏิบัติงาน (AAR)

12. แนวทางการเรียนรู้/การจัดการความรู้ เพื่อนำไปสู่การปรับปรุงกระบวนการในปีต่อไป (ปี 2568)

1. ส่งเสริมให้มีการปรับปรุงกระบวนการในแต่ละ SIPOC และจัดทำ AAR ให้เป็นองค์ความรู้ขององค์กรต่อไป
2. ปรับปรุงตามตัวอย่างการปฏิบัติที่ดีขององค์กรชั้นนำ
3. ปรับปรุงให้สอดคล้องมาตรฐานสากล กฎหมาย ระเบียบ ข้อบังคับ
4. เพิ่มการสื่อสารเชิงรุกเพื่อทำความเข้าใจให้กับหน่วยงานที่เกี่ยวข้อง เพื่อให้การตรวจสอบมีประสิทธิภาพและประสิทธิผล ความเสี่ยงลดลง ความปลอดภัยสูงสุด
5. ส่งเสริมให้บุคลากร/คณะทำงาน มีความรู้ความเข้าใจเกี่ยวกับการจัดทำ แนวทาง/กระบวนการ (SIPOC)/คู่มือปฏิบัติงาน เพราะเป็นจุดเริ่มต้นที่สำคัญที่จะทำให้ทราบขั้นตอนการปฏิบัติงานที่ชัดเจนและเป็นระบบ ซึ่งจะช่วยให้ผู้มีส่วนเกี่ยวกับแนวทาง/กระบวนการ (SIPOC) นั้น ๆ เข้าใจการปฏิบัติงานเป็นไปในทิศทางเดียวกัน

.....

นางสาวทรายแก้ว เกษมณี (ผู้จัดทำ)
พ.ระบบงาน 6 ผน.ทส.
วันที่ 10 ตุลาคม 2567

.....

นายสุเมธ เพ็ชรนิล (ผู้สอบทาน)
ผอก.ผน.ทส.
วันที่ 10 ตุลาคม 2567

.....

นางสาวอภิสมา ฉัตรกิตติ์พิภัทร์
ผู้อำนวยการฝ่ายเทคโนโลยีสารสนเทศ (ทส.)
ผู้ประเมินและปรับปรุงกระบวนการเพื่อบันทึกทำความรู้