แบบรายงานผลการดำเนินงาน (Organizational Performance Form)

หมวดที่ 4 การวัด การวิเคราะห์ และการจัดการความรู้

4.2 การจัดการสารสนเทศ ความรู้ และเทคโนโลยีสารสนเทศ

หัวข้อที่	ประเด็นพิจารณา
4.2 ก (1)	**คุณลักษณะ** ● รัฐวิสาหกิจดำเนินการอย่างไร เพื่อให้ข้อมูล สารสนเทศ และความรู้ของรัฐวิสาหกิจมีคุณลักษณะดังนี้ ■ แม่นยำ ■ ถูกต้องและเชื่อถือได้ ■ ทันกาล ■ ปลอดภัยและเป็นความลับ

ปัจจัยสำคัญที่เกี่ยวข้อง (จากบริบทของรัฐวิสาหกิจ)	
บริบท 1 ก (1) กลไกในการนำผลิตภัณฑ์และบริการให้แก่ลูกค้า	บริบท 1 ข (2) ส่วนตลาด กลุ่มลูกค้า ผู้มีส่วนได้ส่วนเสีย ความต้องการและความคาดหวัง

ประเด็นประเมิน	คำอธิบาย	เอกสารอ้างอิง
แนวทาง	■ **<u>แม่นยำ</u>** ของข้อมูล สารสนเทศ ใช้การควบคุมการพัฒนาระบบงาน (Implementation controls) โดยมีการตรวจสอบและการควบคุมภายในที่ดี มีแนวทาง/ขั้นตอน/มาตรฐานการพัฒนาระบบงานและการสอบทานการดำเนินงาน มีระบบงานที่สนับสนุนและควบคุมการปฏิบัติงาน รวมทั้งมีคณะกรรมการและทีมงานต่าง ๆ ที่เกี่ยวข้องในการพัฒนาระบบงาน ทำหน้าที่ควบคุม กำกับดูแล ติดตาม และให้ข้อเสนอแนะแนวทางแก้ไข เพื่อให้การพัฒนาระบบงาน มีการควบคุมภายในที่ดี ส่งผลให้ข้อมูล สารสนเทศมีความแม่นยำ ผิดพลาดน้อยที่สุด 1) คณะกรรมการและคณะอนุกรรมการต่างๆ ด้าน IT กำหนดนโยบาย และอนุมัติแผนงานพัฒนาระบบ 2) ฝ่ายพัฒนาและสนับสนุนเทคโนโลยี (ฝพท.) กำหนดแบบฟอร์มสำหรับการพัฒนาระบบงาน และนำไปใช้เป็นมาตรฐานและควบคุมการพัฒนาระบบงาน ได้แก่ แบบฟอร์มปรับปรุงเปลี่ยนแปลงระบบงาน แบบฟอร์มทดสอบ/อนุมัติติดตั้งโปรแกรม แบบรายงานการศึกษาความเป็นไปได้ของโครงการ แบบควบคุมแผนงานโครงการ/โครงสร้างทีมงานแบบคำนวณต้นทุนในการดำเนินงาน เป็นต้น พร้อมทั้งกำหนดแบบควบคุมการปฏิบัติงานพัฒนาระบบงาน (Check List)	

ประเด็นประเมิน	คำอธิบาย	เอกสารอ้างอิง
	3) ฝพท. มีการวิเคราะห์ความเป็นไปได้ของระบบงาน/โครงการ และจัดทำเอกสารประกอบขั้นตอนที่สำคัญของการพัฒนาและออกแบบระบบ เช่น System Flow chart เป็นต้น ตามแนวทางการพัฒนาระบบงานด้านเทคโนโลยีสารสนเทศ (System Development Life Cycle - SDLC) 4) ฝพท. จัดทำคู่มือปฏิบัติงานเป็นมาตรฐานในการพัฒนาระบบงานและโครงการ ทั้งในส่วนของการจัดซื้อ/จัดจ้าง และดำเนินการเอง สำหรับระบบงานต่าง ๆ และระบบจัดทำผังกระบวนงาน (ARIS Web publisher) ประกอบด้วย คู่มือการปฏิบัติงานด้านการพัฒนาระบบ คู่มือการปฏิบัติงานทั่วไป และแบบฟอร์ม Check List โดยมีขั้นตอนการทำงานที่สำคัญ โดยที่คู่มือนั้นหน่วยงานอื่นๆที่สนใจสามารถเข้ามาศึกษาผ่านระบบ ARIS ได้ 5) สำนักตรวจสอบ (สตส.) มีการตรวจสอบและการควบคุมภายในที่ดีด้านเทคโนโลยีสารสนเทศตามมาตรฐาน COBIT มาใช้ในการตรวจสอบภายในกระบวนการระหว่างดำเนินการ เพื่อให้มั่นใจว่าการดำเนินงานหรือการเปลี่ยนแปลงแก้ไขระบบงาน โดยมีการวิเคราะห์และออกแบบการพัฒนาระบบ รวมถึงการทดสอบ (Analysis –Design – Implementation –Testing) อย่างเป็นระบบตามวงจร SDLC เพื่อให้ระบบงานที่พัฒนาขึ้นตรงความต้องการของผู้ใช้งาน ข้อมูลสารสนเทศมีความแม่นยำและมีประสิทธิภาพตอบสนองต่อเป้าหมายขององค์กร ตามแนวทางการปฏิบัติที่ดี (Best Practice) ▪ **<u>ถูกต้องและเชื่อถือได้</u>** กระบวนการที่ทำให้ข้อมูลสารสนเทศขององค์กรมีความถูกต้องและเชื่อถือได้ มีกระบวนการดังนี้ 1) ฝพท. มีกระบวนการการควบคุมเฉพาะระบบงาน (Application Control) ที่เหมาะสม สร้างความมั่นใจให้แก่ผู้มีส่วนได้เสีย ว่ารายงานที่ได้รับจากระบบมีความถูกต้องเชื่อถือได้ โดยมีรายละเอียดดังนี้ - การนำเข้าข้อมูล (Input Control) มีวิธีปฏิบัติและการกำหนดสิทธิการเพิ่มเติม แก้ไขข้อมูลเฉพาะเจ้าหน้าที่ที่ได้รับมอบหมายเท่านั้น แล้วตรวจสอบความครบถ้วนถูกต้องของข้อมูลก่อนทำการ Interface ข้อมูลสู่ระบบ โดยมีกระบวนการตรวจสอบ 2 วิธีคือ 1. พนักงานผู้รับผิดชอบนำข้อมูลเข้าตรวจสอบความถูกต้องของข้อมูลที่นำเข้า 2. ตรวจสอบโดยระบบสารสนเทศที่นำข้อมูลเข้า โดยมีขั้นตอนการ Verify และ Algorithm ของ Application ในการ Validate ข้อมูลเพื่อความถูกต้องของข้อมูลที่นำเข้า	-รายงานการตรวจสอบและการควบคุมภายในด้านเทคโนโลยีสารสนเทศ

ประเด็นประเมิน	คำอธิบาย	เอกสารอ้างอิง
	- การประมวลผล (Processing Control) โปรแกรมมีการคำนวณประมวลผลแบบอัตโนมัติ และประมวลผลรายงาน หากมีข้อผิดพลาดเกิดขึ้นจากการประมวลผล ฝพท. สามารถตรวจสอบเพื่อค้นหาข้อผิดพลาด เพื่อดำเนินการแก้ไขได้จาก LogFile - การควบคุมผลลัพธ์ และการรายงานผล (Output Control) มีขั้นตอนปฏิบัติในการตรวจสอบหาความผิดปกติ โดยผู้ออกรายงานอย่างเป็นประจำ ซึ่งอาจเปรียบเทียบกับรายงานอื่น ๆ ประกอบ มีการสอบทานกับข้อมูลต่าง ๆ ที่เกี่ยวข้องและทดสอบสุ่มคำนวณอีกครั้ง เมื่อพบข้อผิดพลาดจะประสานงานกับเจ้าของข้อมูลหรือผู้ดูแลระบบงาน เพื่อดำเนินการหาสาเหตุและแก้ไขข้อผิดพลาด 2) สตส. มีการวางแผนการตรวจสอบ Computer Audit ประจำปี 2556 ได้ใช้กรอบการควบคุมด้านสารสนเทศที่ดีตามกรอบ COBI T มาช่วยในการพิจารณาประเมินความเสี่ยงด้านการบริหารจัดการด้านเทคโนโลยีและการใช้งาน Application เพื่อให้มีแผนตรวจสอบ ข้อมูลระบบสารสนเทศ (Application) ที่สนับสนุนกระบวนงานทางธุรกิจ โดยจะทำการประเมินความเสี่ยงแต่ละระบบงาน โดยพิจารณาทั้งในส่วนของกรอบ COBIT และการใช้งาน Application ตัวอย่างเช่น การตรวจสอบเรื่องการควบคุมการแปลงข้อมูลจากระบบงานเก่าขึ้นสู่ระบบงานใหม่ (Data conversion) เพื่อตรวจสอบความถูกต้องครบถ้วนของข้อมูล โดยผู้ใช้งานที่เกี่ยวข้องจะต้องพิมพ์รายงานที่เกี่ยวข้องจากระบบงานเดิมเปรียบเทียบกับรายงาน/ข้อมูลที่นำขึ้นระบบงาน ▪ **<u>ทันกาล</u>** สามารถนำสารสนเทศมาใช้ได้ทันที เมื่อต้องการใช้ข้อมูลสารสนเทศ มีกระบวนการดังนี้ 1) ฝ่ายเทคโนโลยีและสื่อสาร (ฝทส.) ใช้การควบคุมซอฟต์แวร์ (Software Control) ตรวจสอบและปรับปรุงโปรแกรมให้ทันสมัยอยู่เสมอโดยอัตโนมัติเพื่อปิดช่องโหว่ของโปรแกรมต่าง ๆ โดยใช้เครื่องมือดังนี้ - เครื่องมือรักษาความปลอดภัยคอมพิวเตอร์ทางเครือข่าย (Directory Service) ประกอบด้วย ระบบตรวจสอบสิทธิ์การเข้าใช้เครื่องคอมพิวเตอร์, ระบบป้องกันการใช้โปรแกรมที่อาจเกิดความเสียหายต่อเครื่องคอมพิวเตอร์, ระบบตรวจสอบการติดตั้งโปรแกรมให้เครื่องคอมพิวเตอร์, ระบบซ่อมแซมโปรแกรมที่ขัดข้องหรือเกิดความเสียหาย, ระบบให้ความช่วยเหลือระยะไกล, ระบบป้องกันการติดตั้งโปรแกรมหรือดาวน์โหลดโปรแกรมจากอินเตอร์เน็ต และระบบตรวจสอบและปรับปรุงโปรแกรมให้ทันสมัยอยู่เสมออัตโนมัติเพื่อปิด	

ประเด็นประเมิน	คำอธิบาย	เอกสารอ้างอิง
	ช่องโหว่ของโปรแกรมต่าง ๆ 2) ผู้รับผิดชอบหน่วยงานเจ้าของข้อมูล ต้องปรับปรุงข้อมูลสารสนเทศทันทีที่ข้อมูลสารสนเทศมีการเปลี่ยนแปลง เพื่อให้ข้อมูลมีความทันสมัย อย่างรวดเร็ว 3) ระบบเครือข่าย (Network) โดย ฝทส. ดำเนินการปรับปรุงคุณภาพความรวดเร็วของระบบเครือข่าย จาก 10/100 MB เป็น GB ทั้งองค์กร ทำให้สามารถสื่อสารข้อมูลสารสนเทศได้อย่างทันเวลา โดยเครือข่ายที่เชื่อมโยงระหว่างสำนักงานใหญ่กับสาขา มี 2 วงจร โดยวงจรแรกเป็น leased line 2 Mbps และวงจร MPLS 12 Mbps 4) ระบบสื่อสาร (Internet) แบ่งออกเป็น 2 วงจร คือวงจรแรกสำหรับผู้บริหาร และการทำธุรกรรมทางการเงิน ความเร็ว 40/10 Mbps และวงจรที่สองสำหรับพนักงานและบุคคลทั่วไป ความเร็ว 200/50 Mbps เพื่อให้เกิดความรวดเร็วในการเข้าถึงข้อมูลสารสนเทศ ▪ **<u>ปลอดภัยและเป็นความลับ</u>** กระบวนการสำคัญที่นำมาใช้งานมีดังนี้ 1) การควบคุมซอฟต์แวร์ (Software Control) ฝทส. กำหนดกฎระเบียบนโยบาย และเครื่องมือ/ระบบการรักษาความปลอดภัยคอมพิวเตอร์ เพื่อควบคุม/ตรวจสอบการเข้าใช้ซอฟต์แวร์ระบบ และซอฟต์แวร์ประเภทต่างๆ ไม่ให้มีการเปลี่ยนแปลงแก้ไขข้อมูลโดยไม่มีสิทธิ/ไม่ได้รับอนุญาต และป้องกันการติดตั้งหรือดาวน์โหลดโปรแกรม มีรายละเอียดดังนี้ - เครื่องมือรักษาความปลอดภัยคอมพิวเตอร์ทางเครือข่าย (Directory Service) ประกอบด้วย ระบบตรวจสอบสิทธิ์การเข้าใช้เครื่องคอมพิวเตอร์, ระบบป้องกันการใช้โปรแกรมที่อาจเกิดความเสียหายต่อเครื่องคอมพิวเตอร์, ระบบตรวจสอบการติดตั้งโปรแกรมให้เครื่องคอมพิวเตอร์, ระบบซ่อมแซมโปรแกรมที่ขัดข้องหรือเกิดความเสียหาย, ระบบให้ความช่วยเหลือระยะไกล, ระบบป้องกันการติดตั้งโปรแกรมหรือดาวน์โหลดโปรแกรมจากอินเตอร์เน็ต และระบบตรวจสอบและปรับปรุงโปรแกรมให้ทันสมัยอยู่เสมออัตโนมัติเพื่อปิดช่องโหว่ของโปรแกรมต่าง ๆ -ระบบตรวจจับการบุกรุก (Intrusion Prevention System : IPS) ด้วยโปรแกรม McAfee รุ่น IntruShield 2700 เป็นเครื่องมือสำหรับตรวจจับความพยายามบุกรุกเครือข่าย สกัดกั้นการโจมตีทางช่องโหว่ระบบปฏิบัติการ (IPS Signature) สิ่งผิดปกติและการโจมตีแบบ Denial of Service (DoS) โดยจะแจ้งเตือนผู้ดูแลระบบ (ส่วนรักษาความมั่นคงปลอดภัยเครือข่าย) ทราบเมื่อมีการบุกรุก -ไฟร์วอลล์ (NetScreenFirewall) ทำหน้าที่ควบคุมการ	

ประเด็นประเมิน	คำอธิบาย	เอกสารอ้างอิง
	อนุญาตหรือไม่อนุญาตให้ผ่านเข้าใช้บริการเครือข่ายจากภายในและภายนอกตามนโยบายความปลอดภัย (Security Policy) ของระบบเครือข่าย เป็นการปิดช่องโหว่มิให้เครือข่ายถูกโจมตีได้ง่าย -ระบบป้องกันไวรัสเครื่องแม่ข่าย ด้วยโปรแกรม Trend Micro และ NOD 32 เป็นระบบป้องกันไวรัสเครื่องแม่ข่าย โดยทำหน้าที่ตรวจจับ ป้องกัน และกำจัดภัยคุกคามของ Malware (Virus, Worms, Trojans, Ad-wares) 2) การควบคุมทางกายภาพ (Physical hardware controls) คณะกรรมการ/คณะทำงานด้านความปลอดภัยสารสนเทศ ดำเนินการพัฒนาและบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ มีการจัดการด้านกายภาพ การตรวจสอบและการควบคุมการเข้า-ออก ศูนย์คอมพิวเตอร์หลักและสำรอง มีการตรวจสอบอุปกรณ์และเครื่องมือต่างๆ มีรายละเอียดดังนี้ -คณะกรรมการด้านการรักษาความปลอดภัยสารสนเทศตามมาตรฐาน ISO 27001 และคณะทำงานความมั่นคงปลอดภัยสารสนเทศตามมาตรฐาน ISO 27001 ดำเนินการพัฒนาระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (Information Security Management Systems :ISMS) ฮาร์ดแวร์ มีกระบวนการบริหารจัดการด้านความมั่นคงปลอดภัยสารสนเทศ ตามมาตรฐาน ISO/IEC 27001:2005 พัฒนาและดูแลระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศของศูนย์คอมพิวเตอร์หลักและศูนย์คอมพิวเตอร์สำรองของ กปน. ให้สามารถดำเนินการได้อย่างต่อเนื่องและมีประสิทธิภาพ -ฝทส. ควบคุมดูแลสัญญาว่าจ้างบำรุงรักษาเชิงป้องกันสำหรับเครื่องแม่ข่ายและอุปกรณ์ภายในห้องคอมพิวเตอร์แม่ข่าย (Data Center) เช่น ระบบเปิด-ปิดประตูอัตโนมัติระบบตรวจวัดอุณหภูมิ ระบบตรวจจับควันไฟ ระบบตรวจจับการรั่วซึมของน้ำ ระบบดับเพลิงด้วยสารเคมี และระบบปรับอากาศ เป็นต้น โดยบริษัทผู้รับจ้างจะบำรุงรักษาอย่างสม่ำเสมอทุก 1-2 เดือน -การเข้าออกห้องเครื่องคอมพิวเตอร์แม่ข่าย มีระบบ Access Door ซึ่งพนักงานที่มีสิทธิเข้า-ออกต้องใช้บัตรผ่าน (Access Card) เพื่อพิสูจน์ตัวตนทุกครั้ง หากเป็นบุคคลภายนอกต้องบันทึกแบบฟอร์มเมื่อได้รับอนุญาต จะมีเจ้าหน้าที่ดูแลการปฏิบัติงาน ด้านหน้าประตูทางเข้ามีกล้องวงจรปิด (CCTV) เพื่อบันทึกเหตุการณ์เคลื่อนไหวและภายในห้องแม่ข่ายมีกล้อง Web Cam เพื่อใช้สังเกตุการณ์การปฏิบัติงานภายใน 3) การควบคุมความปลอดภัยข้อมูล (Data security controls) ฝทส. มีเครื่องมือและระบบการควบคุมการเข้าถึงข้อมูลสารสนเทศ	

ประเด็นประเมิน	คำอธิบาย	เอกสารอ้างอิง
	ระบบตรวจสอบและป้องกันภัยคุกคามต่าง ๆ ที่อาจส่งผลให้ข้อมูลสารสนเทศของ กปน. ถูกตรวจจับ แก้ไขเปลี่ยนแปลง ขโมยความลับหรือทำลายให้เกิดความเสียหาย รวมทั้งมีการเข้ารหัสข้อมูล/ใช้ SSL-VPN สำหรับการส่งข้อมูลออกไปยังหน่วยงานภายนอก กปน. 4) กระบวนการตรวจสอบภายในด้าน ICT ตามมาตรฐาน COBIT โดย สตส. มีการสอบทานกระบวนการควบคุมภายในของการปฏิบัติงานและการรักษาความปลอดภัยทางด้านเทคโนโลยีสารสนเทศ รวมถึงมีผู้ให้บริการภายนอกมาตรวจสอบการจัดทำระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศตามมาตรฐาน ISO27001 เป็นประจำทุกปี 5) คณะทำงานบริหารความเสี่ยงและควบคุมภายในประจำสายงานเทคโนโลยีสารสนเทศ กำหนดแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่อง (Business Continuity Plan: BCP) มีขั้นตอนหลักประกอบด้วย การแจ้งและสื่อสารผู้ที่เกี่ยวข้อง การกอบกู้และปฏิบัติงานในขณะเกิดเหตุการณ์ฉุกเฉิน และการกลับคืนสู่ภาวะการดำเนินธุรกิจตามปกติ โดยมีการฝึกซ้อมแผนปฏิบัติการกรณีเหตุฉุกเฉินประจำทุกปี **<u>ตัวชี้วัด</u>** เพื่อให้ข้อมูล สารสนเทศ และความรู้ มีแม่นยำ ถูกต้องและเชื่อถือได้ ทันกาล และปลอดภัยและเป็นความลับ ได้แก่ 1) รายงานผลการตรวจสอบภายในด้าน ICT ตามมาตรฐาน COBIT 2) ระดับความพึงพอใจของผู้ใช้บริการต่อระบบสารสนเทศผู้ใช้บริการภายใน และผู้ใช้บริการภายนอก 3) การควบคุมการปฏิบัติงานภายใต้กรอบความมั่นคงปลอดภัยสารสนเทศตามมาตรฐานสากล ISO/IEC 27001:2005 – วัดระดับความสำเร็จในการดำเนินงาน โดยที่เครื่องแม่ข่ายสามารถให้บริการระบบ CIS และ SAP ได้รับการดูแลตามมาตรฐาน ISO/IEC 27001:2005 โดยมีระยะเวลาหยุดให้บริการ (Downtime) ไม่เกิน 3% (262 ชั่วโมง) 4) การจัดทำแผนทบทวนการบริหารความต่อเนื่องทางธุรกิจ (BCP) ด้านเทคโนโลยีสารสนเทศ ตามมาตรฐาน ISO/IEC 27001:2005	-รายงานผลการตรวจสอบ ICT ประจำปี 2556
การนำแนวทางไปปฏิบัติ	กระบวนการที่กล่าวมาข้างต้นสายงานเทคโนโลยีสารสนเทศแจ้งให้ผู้ปฏิบัติงานในทุกหน่วยงานได้รับทราบถึงวิธีการใช้งานของระบบเพื่อ นำไปปฏิบัติในทุกหน่วยงานได้อย่างทั่วถึงทั้งองค์กร ด้วยวิธีการดังนี้ 1) สายงานเทคโนโลยีสารสนเทศ ได้จัดทำคู่มือการปฏิบัติงานการพัฒนาระบบ คู่มือการปฏิบัติงานทั่วไป และแบบฟอร์ม Check List โดยมีขั้นตอนการทำงานที่สำคัญ ให้แก่ผู้ปฏิบัติงานเพื่อให้สามารถ	

ประเด็นประเมิน	คำอธิบาย	เอกสารอ้างอิง
	เข้าใจขั้นตอน/กระบวนการและมีแนวทางในการปฏิบัติงานได้อย่างถูกต้อง 2) มีการจัดทำผังการทำงาน (Flow Chart) ในโปรแกรม ARIS เพื่อให้ทุกหน่วยงานในสายงานเทคโนโลยีสารสนเทศได้ทราบถึงขั้นตอนการปฏิบัติงานของแต่ละหน่วยงานภายในสายงาน หน้าที่ความรับผิดชอบ รวมถึงความเชื่อมโยงของกระบวนงานของแต่ละหน่วยงาน โดยเผยแพร่ผังการทำงาน(Flow Chart) ทาง Intranet 3) มี Internal Audit ตรวจสอบเป็นประจำทุกปี ตามมาตรฐาน COBIT และรายงานผลการตรวจสอบ สรุปประเด็นที่ตรวจพบและข้อเสนอแนะ ให้กับหน่วยรับตรวจสอบด้วย	
การเรียนรู้	นำผลการสำรวจความพึงพอใจ มาวิเคราะห์ประเมินผล และนำไป พัฒนาปรับปรุงในกระบวนงานที่เกี่ยวข้องเป็นประจำทุกปี กระบวนการ ISMS มีการทบทวนทุกปี ตามมาตรฐาน ISO/IEC 27001:2005 (ตามรูปแบบ PDCA) และในปี 2556ขยายขอบเขตงานโดยเครื่องแม่ข่ายที่สามารถให้บริการระบบ CIS และ SAP ได้รับการดูแลตามมาตรฐาน ISO/IEC 27001:2005 เพื่อพัฒนาระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (Information Security Management Systems :ISMS) ให้เป็นไปตามมาตรฐานสากล 3 ด้าน คือ ด้านบุคลากร ด้านกระบวนการปฏิบัติงาน และด้านเทคโนโลยี	
การบูรณาการ	กระบวนการนี้สนับสนุนการพัฒนา/ปรับปรุงกระบวนงานภายในองค์กร โดยนำระบบสารสนเทศเข้าไปใช้ในการทำงาน ด้านผลิต ด้านบริการ ด้านบริหาร และงานสนับสนุนต่าง ๆ เพื่อมีข้อมูล สารสนเทศและองค์ความรู้ ที่มีคุณภาพ ถูกต้อง แม่นยำ เชื่อถือได้ทันกาล มีความปลอดภัยเป็นความลับ ตอบสนองความต้องการขององค์กร และผู้มีส่วนได้เสียขององค์กร ครอบคลุมทุกด้าน และเหมาะสมกับสถานการณ์	

แบบรายงานผลการดำเนินงาน (Organizational Performance Form)

หมวดที่ 4 การวัด การวิเคราะห์ และการจัดการความรู้

หัวข้อที่	ประเด็นพิจารณา
4.2 ก (2)	**ความพร้อมใช้งานของข้อมูลและสารสนเทศ** ● รัฐวิสาหกิจดำเนินการอย่างไร ในการทำให้ข้อมูลและสารสนเทศที่จำเป็นมีความพร้อมใช้งาน ● รัฐวิสาหกิจดำเนินการอย่างไร ในการทำให้บุคลากร ผู้ส่งมอบ คู่ค้า คู่ความร่วมมือ รวมทั้งลูกค้าและหน่วยงานอื่นที่เกี่ยวข้องภายนอกองค์กรสามารถเข้าถึงและแบ่งปันข้อมูล (พิจารณาตามความเหมาะสม)

ปัจจัยสำคัญที่เกี่ยวข้อง (จากบริบทของรัฐวิสาหกิจ)	
บริบท 1 ก (3) ลักษณะโดยรวมของบุคลากร บริบท 1 ข (2) กลุ่มลูกค้า กลุ่มผู้มีส่วนได้ส่วนเสีย และส่วนตลาด	บริบท 1 ข (3) ผู้ส่งมอบ คู่ค้า คู่ความร่วมมือ

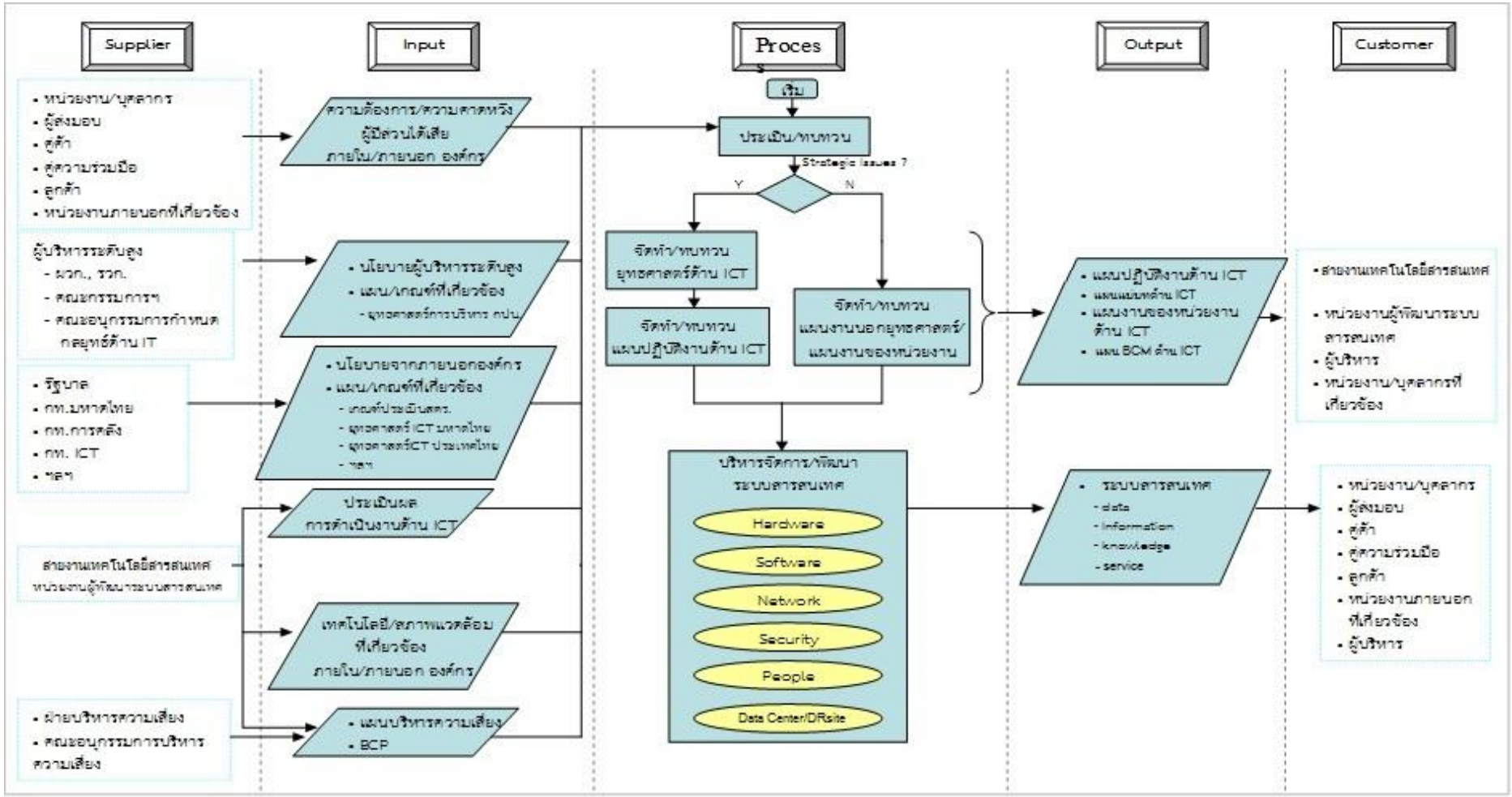
ประเด็นประเมิน	คำอธิบาย	เอกสารอ้างอิง
แนวทาง	กปน. มีการจัดทำนโยบายแนวทางการสำรองข้อมูลและระบบคอมพิวเตอร์ และการเตรียมพร้อมกรณีฉุกเฉิน (Backup and IT Continuity Plan) เพื่อให้มีข้อมูลและระบบคอมพิวเตอร์สามารถใช้งานได้อย่างต่อเนื่อง สามารถเข้าถึงและใช้งานได้ทุกเวลาที่ต้องการใช้งาน (Availability) เช่น ระเบียบ กปน. ฉบับที่ 18 ว่าด้วยการรักษาความปลอดภัยสารสนเทศ พ.ศ.2548, คู่มือการปฏิบัติงาน, แผนรองรับการดำเนินธุรกิจอย่างต่อเนื่อง (Business Continuity Plan: BCP) , และการจัดทำการสำเนาข้อมูลตามแผน DRP ,มีการกำหนดผู้รับผิดชอบ กระบวนการปฏิบัติไว้เป็นลายลักษณ์อักษร ● กปน. มีกระบวนการทำให้ข้อมูลสารสนเทศที่จำเป็นมีความพร้อมใช้งานภายใต้กระบวนการดำเนินงานด้าน ICT ดังแสดงในภาพที่ 4.2 ก(2)-1 ซึ่งมีรายละเอียดดังนี้ 1) หน่วยงานในสายงานเทคโนโลยีสารสนเทศ เป็นผู้ดูแลด้าน Infrastructure, Development, และ Strategy, IT Strategy Committee และ ICT Steering Committee ที่ดูแลให้มีการพัฒนาและสนับสนุนระบบสารสนเทศตามความต้องการขององค์กรอย่างเพียงพอ และเหมาะสม 2) ฝ่ายยุทธศาสตร์ด้านเทคโนโลยีสารสนเทศ (ฝยท.) ดำเนินการรวบรวมข้อมูลความต้องการ นโยบาย ด้าน ICT จากปัจจัยภายในและ	- ระเบียบ กปน. ฉบับที่ 18 ว่าด้วยการรักษาความปลอดภัยสารสนเทศ พ.ศ. 2548 -คู่มือการปฏิบัติงาน -แผน BCP & DRP -แผนแม่บทเทคโนโลยี

ประเด็นประเมิน	คำอธิบาย	เอกสารอ้างอิง
	ภายนอกองค์กร รวมถึงข้อมูลด้านความเสี่ยงขององค์กร จัดทำแผนแม่บทเทคโนโลยีสารสนเทศและการสื่อสาร พ.ศ. 2556-2559 เป็นฉบับปัจจุบัน และแผนงาน/โครงการด้าน ICT 3) ฝ่ายพัฒนาและสนับสนุนเทคโนโลยี (ฝพท.) ทำหน้าที่บริหารจัดการ พัฒนาระบบสารสนเทศ โดยมีบุคลากรที่มีความรู้ความชำนาญในการออกแบบ วิเคราะห์และ พัฒนาระบบสารสนเทศที่จำเป็นตลอดจนการนำ Software ที่เหมาะสมมาใช้ในองค์กร เพื่อให้มีข้อมูลสารสนเทศที่ตรงตามความต้องการของผู้ใช้ 4) ฝ่ายเทคโนโลยีและสื่อสาร (ฝยส.) ทำหน้าที่บริหารจัดการในด้านต่าง ๆ คือ Hardware, Network, Security, People และ Data Center/DR Site มีการจัดทำนโยบายแนวทางการสำรองข้อมูลและระบบคอมพิวเตอร์ และการเตรียมพร้อมกรณีฉุกเฉิน (Backup and IT Continuity Plan) เพื่อให้มีข้อมูลและระบบคอมพิวเตอร์สามารถใช้งานได้อย่างต่อเนื่อง 5) คณะทำงานบริหารความเสี่ยงและควบคุมภายในประจำสายงานเทคโนโลยีสารสนเทศ กำหนดแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่อง (Business Continuity Plan: BCP) มีขั้นตอนหลักประกอบด้วย การแจ้งและสื่อสารผู้ที่เกี่ยวข้อง การกอบกู้และปฏิบัติงานในขณะเกิดเหตุการณ์ฉุกเฉิน และการกลับคืนสู่ภาวะการดำเนินธุรกิจตามปกติ โดยมีการฝึกซ้อมแผนปฏิบัติการกรณีเหตุฉุกเฉินประจำทุกปี สำหรับระบบงานที่สำคัญ ได้แก่ ระบบงาน SAP ระบบข้อมูลผู้ใช้น้ำ (CIS) ระบบสารบรรณอิเล็กทรอนิกส์ เป็นต้น 6) ฝยส. จัดทำการสำเนาข้อมูลตามแผน DRP หรือ BCP เพื่อให้ระบบสารสนเทศอยู่ในสภาพที่พร้อมใช้งานอยู่เสมอ 7) การจัดทำข้อตกลงระดับการให้บริการประจำปี (SlA) ระหว่างหน่วยงานผู้ให้บริการ(ฝพท. และ ฝยส.) กับหน่วยงานผู้รับบริการ(ทุกหน่วยงานที่ใช้บริการ เช่น ฝพท. กำหนด SLA ในเรื่องการบริการจัดทำข้อมูล การบริการให้คำปรึกษาหรือแก้ไขปัญหา การบำรุงรักษาระบบงานให้แก่ผู้ใช้ระบบงานหลัก การบำรุงรักษาระบบงานให้แก่ผู้ใช้ระบบงานรอง และการพัฒนาระบบงาน และ ฝยส. กำหนด SLA ในเรื่องการซ่อมบำรุง/แก้ไข เครื่องคอมพิวเตอร์ลูกข่าย การใช้งานในระบบเครือข่าย การบริการรับ-ส่งและประมวลผลข้อมูล และการใช้งานในระบบเครื่องแม่ข่าย เป็นต้น ● บุคลากร ผู้ส่งมอบ คู่ค้า คู่ความร่วมมือ รวมทั้งลูกค้าและหน่วยงานอื่นที่เกี่ยวข้องภายนอกองค์กรสามารถเข้าถึงและแบ่งปัน	สารสนเทศและการสื่อสาร พ.ศ. 2556-2559

ประเด็นประเมิน	คำอธิบาย	เอกสารอ้างอิง
	ข้อมูล สารสนเทศและความรู้ ตามตารางที่ 4.2 ก(2)-1 ผ่านกระบวนการดังต่อไปนี้ **1.** ฝยส. ควบคุมดูแลระบบเครือข่ายหลักให้มีประสิทธิภาพ มีการทำ Zoning รองรับการเข้าถึงและแบ่งปันข้อมูลของผู้ใช้งานกลุ่มต่าง ๆ ทั้งกลุ่มผู้ใช้ภายในและกลุ่มผู้ใช้ภายนอก ดังนี้ 1) กลุ่มผู้ใช้ภายใน เช่น บุคลากร เข้าถึงข้อมูลจากระบบเครือข่ายภายใน หากจะเข้าถึงข้อมูลจากเครือข่ายภายนอก ผ่านทาง Internet ด้วยเทคโนโลยี แบบ SSL-VPN คือ 1.1) กลุ่ม Admin – แบบ Two factor authentication โดยผู้ใช้ต้องระบุ User/Password และ Hardware Token 1.2) กลุ่ม User – แบบ Extranet 2) กลุ่มผู้ใช้ภายนอก เช่น ผู้ส่งมอบ คู่ค้า คู่ความร่วมมือ รวมทั้งลูกค้าและหน่วยงานอื่นที่เกี่ยวข้องภายนอกองค์กร สามารถเข้าถึงโปรแกรมและข้อมูลได้ทาง Internet ที่จัดแยก zone การให้ข้อมูลอย่างชัดเจน 2.1) DMZ Zone เข้าถึงข้อมูลทั่วไป www.mwa.co.th 2.2) Application Zone เช่น การรับชำระค่าน้ำผ่านWeb 2.3) Database Zone จะมี Security เพราะสามารถ Access เข้ามาได้จากเครื่องที่ได้รับอนุญาตเท่านั้น 2.4) Remote Zone สำหรับ Admin และ Security เช่น หน่วยงานตัวแทนรับชำระค่าน้ำ โดยมี Firewall กั้น หรือการแลกเปลี่ยนข้อมูลค่าน้ำหักบัญชีกับธนาคาร ใช้ File Transfer Protocol ทางหน้า Web 2. ฝยส. กำกับดูแลให้มีการปฏิบัติตามมาตรการรักษาความปลอดภัยอย่างเคร่งครัด กำหนดระบบรักษาความปลอดภัย (Security) ของการเข้าถึงข้อมูลหรือระบบให้เฉพาะผู้ที่มีสิทธิ์เท่านั้น ด้วยการใช้รหัสประจำตัวผู้ใช้ (User Identification) และรหัสผ่าน (Password) เข้าใช้ระบบตามสิทธิ์ของผู้ใช้ระบบ 3. รวก.(ท) มอบหมายให้หน่วยงานที่รับผิดชอบ เช่น ฝยส., ฝพท. เป็นผู้กำหนดข้อตกลงและมาตรฐานในการแลกเปลี่ยนข้อมูล (Protocal) กับหน่วยงานภายนอกในช่องทางเฉพาะระหว่างการประปานครหลวงกับหน่วยงานภายนอกนั้น ๆ เช่นกระทรวงมหาดไทย กระทรวงเทคโนโลยีสารสนเทศฯ ธนาคาร กรมชลประทาน กรมควบคุมมลพิษ เป็นต้น โดยไม่ใช้ช่องทางสาธารณะในการส่งมอบเอกสาร หรือข้อมูลที่สำคัญ 4. ฝยส. กำหนดการประมวลผลในการรับ – ส่งข้อมูลให้กับหน่วยงานภายนอกองค์กรตามกำหนดเวลาที่ควบคุมของแต่ละ	

ประเด็นประเมิน	คำอธิบาย	เอกสารอ้างอิง
	ระบบงาน และมีการตรวจสอบข้อมูลให้ถูกต้อง โดยเจ้าหน้าที่ผู้มีหน้าที่เฉพาะงานนั้น ๆ ซึ่งไม่ใช่ผู้ดูแลระบบงาน **<u>ตัวชี้วัด</u>** 1) การจัดทำและดำเนินการตามแผนแม่บทด้าน ICT, แผนปฏิบัติด้านงาน ICT และ แผน BCM ด้าน ICT เพื่อให้ระบบสารสนเทศที่มีความจำเป็นและมีประสิทธิภาพ ตอบสนองต่อความต้องการของบุคลากร ลูกค้า และผู้มีส่วนได้ส่วนเสีย 2) ระดับความพึงพอใจของผู้ใช้บริการต่อระบบสารสนเทศ ผู้ใช้บริการภายใน และผู้ใช้บริการภายนอก	
การนำแนวทางไปปฏิบัติ	กระบวนการที่กล่าวมาข้างต้น นำแนวทางไปปฏิบัติเป็นประจำทุกปี ดังนี้ ● แผนแม่บทเทคโนโลยีสารสนเทศและการสื่อสาร พ.ศ. 2555-2559 ฝยท. ประชาสัมพันธ์เผยแพร่ ในรูปแบบเล่มเอกสาร และเอกสารอิเล็คทรอนิคส์ ฉบับสมบูรณ์ให้ทุกหน่วยงานภายใน กปน. และหน่วยงานภายนอก กปน. ที่เกี่ยวข้อง เพื่อให้รับทราบ และแจ้งให้หน่วยงานผู้รับผิดชอบแผนงาน/โครงการ ดำเนินการตามแผน และมีระบบติดตามและประเมินผลโครงการ เพื่อวัดผลการดำเนินงานตามตัวชี้วัด เพื่อบรรลุเป้าหมายที่กำหนดไว้ ● ฝยท. เผยแพร่ประชาสัมพันธ์ให้กับบุคลากร ผู้ส่งมอบ คู่ค้า คู่ความร่วมมือ รวมทั้งลูกค้า และหน่วยงานอื่นที่เกี่ยวข้องภายนอกองค์กร โดยผ่านทางสื่อสิ่งพิมพ์, จดหมายอิเล็กทรอนิกส์, ทางหน้าเว็ปไซด์อินเตอร์เน็ต ของ กปน. และทาง Social Network ให้รับทราบและปฏิบัติตามแนวทางการเข้าถึงข้อมูลของแต่ละงาน และหากเกิดข้อขัดข้องในการเข้าถึงสามารถแจ้งขอความช่วยเหลือได้จากผู้ปฏิบัติงานของ กปน. ที่ดูแลงานนั้น ๆ หรือ Call Center ได้ตลอด 24 ชั่วโมง ● ฝยท. ดำเนินการสำรวจความพึงพอใจของผู้ใช้บริการทั้งภายในและภายนอกองค์กรครอบคลุมผู้มีส่วนได้ส่วนเสียทุกกลุ่ม ต่อระบบสารสนเทศ ซึ่งจัดทำเป็นประจำทุกปี อย่างน้อยปีละ 1 ครั้ง เพื่อนำไปจัดทำแนวทางปรับปรุงระบบให้ตรงต่อความต้องการของผู้มีส่วนได้ส่วนเสีย ● สายงานเทคโนโลยีสารสนเทศ มีแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่อง (Business Continuity Plan: BCP) มีการฝึกซ้อมแผนปฏิบัติการกรณีเหตุฉุกเฉินประจำทุกปี โดยการแจ้งและสื่อสารกับผู้ที่เกี่ยวข้อง สำหรับระบบงานที่สำคัญ ได้แก่ ระบบงาน SAP ระบบข้อมูลผู้ใช้น้ำ (CIS) เป็นต้น โดยจะระบุรายละเอียดขั้นตอนการปฏิบัติงานการสำรองข้อมูล วิธีการกู้ระบบงาน และกำหนด	

ประเด็นประเมิน	คำอธิบาย	เอกสารอ้างอิง
	ผู้รับผิดชอบอย่างชัดเจนครบถ้วน	
การเรียนรู้	- ฝยท. สรุปผลการสำรวจความพึงพอใจ วิเคราะห์ประเมินผลและนำส่งแบบสรุปผลฯ ให้แก่หน่วยงานผู้รับผิดชอบระบบงาน เพื่อนำไปพัฒนาปรับปรุงในกระบวนงานที่เกี่ยวข้องเป็นประจำทุกปี เช่น ฝพท. นำสรุปผลมาจัดทำแนวทางปรับปรุงระบบงานโดยปรับเปลี่ยน Version ระบบ SAP ที่ กปน. ใช้อยู่ ให้เป็น Version ECC 6.0 Version ล่าสุด เพื่อลดความเสี่ยงจากการใช้ระบบที่ล้าสมัย ปรับปรุงระบบให้รองรับมาตรฐานการรายงานทางการเงินระหว่างประเทศ (IFRS : International Financial Reporting Standards) รองรับเทคโนโลยีซึ่งมีการพัฒนาอย่างต่อเนื่อง มีการเพิ่มระบบงานหรือฟังก์ชั่นงานใหม่เพื่อให้ กปน. มีระบบงาน ERP ที่มีการควบคุมภายในที่ดี เป็นมาตรฐานสากล สนับสนุนการปฏิบัติงาน และตอบสนองการใช้งานได้ดียิ่งขึ้น และมีข้อมูลเพื่อการตัดสินใจของผู้บริหาร ได้อย่างมีประสิทธิภาพ ฝยท. นำผลจากการทบทวน/ปรับปรุงแผนแม่บทเทคโนโลยีสารสนเทศและการสื่อสารไปใช้ปรับปรุงแผนการปฏิบัติงานเป็นประจำทุกปี ตัวอย่างการพัฒนาระบบสำหรับกลุ่มผู้มีส่วนได้ส่วนเสีย ปี 2556 เช่น มีการจัดทำระบบ Management Cockpit เพื่อสนับสนุนการตัดสินใจของผู้บริหารระดับสูง และการบูรณาการระบบเทคโนโลยีสารสนเทศ โดยพัฒนาตามหลักการของ SOA เป็นต้น	
การบูรณาการ	กปน. มีข้อมูลและสารสนเทศมีความพร้อมใช้งาน เพื่อใช้ในการติดตาม ประเมินผลและปรับปรุงการดำเนินงาน และนำข้อมูลสารสนเทศไปใช้ในการบริหารจัดการและตัดสินใจต่าง ๆ เป็นไปอย่างมีประสิทธิภาพ โดยบุคลากร ผู้ส่งมอบ คู่ค้า คู่ความร่วมมือ ลูกค้า และหน่วยงานอื่นที่เกี่ยวข้องภายนอกองค์กร สามารถเข้าถึงและแบ่งปันข้อมูลในส่วนที่เกี่ยวข้องได้สอดคล้องกับการดำเนินงานขององค์กร รวมทั้งทิศทางการดำเนินงานด้าน ICT (ตามแผนแม่บทเทคโนโลยีสารสนเทศและการสื่อสาร พ.ศ. 2556-2559) สอดคล้องและสนับสนุนยุทธศาสตร์องค์กร การดำเนินการเพื่อสร้างความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ พร้อมใช้งาน และใช้งานต่อเนื่องในการให้บริการลูกค้า ผู้มีส่วนได้เสีย ประชาชน และพนักงานสามารถปฏิบัติงานทุกกระบวนงานขององค์กร ได้อย่างมั่นใจ ถูกต้อง ถูกกฎหมาย และมีประสิทธิภาพ เพื่อให้บรรลุผลลัพธ์ตามยุทธศาสตร์การบริหาร กปน. ที่ได้กำหนดไว้	



ภาพที่ 4.2 ก (2)-1 : กระบวนการดำเนินงานด้าน ICT ของ กปน.

ตารางที่ 4.2 ก (2) –1 การเข้าถึงข้อมูลสารสนเทศของผู้ใช้งาน

ข้อมูลและสารสนเทศ	การเข้าถึงข้อมูล	กลุ่มผู้ใช้ภายใน			กลุ่มผู้ใช้ภายนอก				
		ผู้บริหาร	พนักงานระดับ 1-5	ลูกจ้าง/ตัวแทน	ผู้ส่งมอบ	คู่ค้า	คู่ความร่วมมือ	ลูกค้า	หน่วยงานเชิงนโยบาย/ผู้ถือหุ้น
การตัดสินใจของผู้บริหารระดับองค์กร และวางแผนยุทธศาสตร์/แผนปฏิบัติงาน	Online ผ่านระบบ BI,MIS,EIS ,Management Cockpit	✓							
การติดตามผลการดำเนินงานตามแผนปฏิบัติงาน และแผนบริหารความเสี่ยง	Online ผ่านระบบติดตามและประเมินผลโครงการ	✓							
การบริหารผลการปฏิบัติงานของบุคลากร	Online ผ่านระบบประเมินผลบุคคล COACH	✓							
การบริหารจัดการความเสี่ยงและควบคุมภายใน และการตรวจสอบภายใน	Online ผ่านระบบ RMIC ,IAIS	✓							
การบริหารจัดการงานหลักองค์กร	Online ผ่านระบบ SAP	✓	✓						
การบริหารจัดการข้อมูล และการให้บริการผู้ใช้น้ำ	Online ผ่านระบบ CIS	✓	✓						
การบริหารจัดการคุณภาพน้ำดิบ	Online ผ่านระบบเฝ้าระวังคุณภาพน้ำดิบทางไกลอัตโนมัติ	✓	✓						
การบริหารจัดน้ำลดน้ำสูญเสีย	Online ผ่านระบบ DMA ,WLMA	✓	✓						
การบริหารจัดการแรงดันน้ำ	Online ผ่านระบบ SCADA	✓	✓						
การบริหารจัดการงานวิศวกรรมและงานโครงการ	Online ผ่านระบบบริหารวิศวกรรมและโครงการ ,GIS	✓	✓						
การบริหารจัดการด้านบัญชี การเงิน	Online ผ่านระบบ CMS ,การจัดทำงบลงทุน	✓	✓						
ข้อมูลสารสนเทศส่วนบุคคลพนักงาน	Online ผ่านระบบ e-HR, Pay Slip และระบบการลาฯ	✓	✓						
การบริหารจัดการองค์ความรู้	Online ผ่านระบบ KM/LO ,e-Learning ,ระบบคลังความรู้	✓	✓	✓					
การบริหารจัดการงานสำรวจ ความพึงพอใจ ความคิดเห็นด้านต่างๆ	Online ผ่านระบบสำรวจออนไลน์	✓	✓	✓					
ข่าวประชาสัมพันธ์ภายในองค์กร	Online ผ่านระบบ Intranet / e-mail	✓	✓	✓					
งานเอกสาร และสารบรรณอิเล็กทรอนิกส์	Online ผ่านระบบ INFORMA WEBFORM		✓	✓					
สารสนเทศ ใบแจ้งหนี้ค่าน้ำประปา	ระบบอ่านมาตรออกใบแจ้งหนี้ ด้วยอุปกรณ์ Handheld		✓	✓					
ข้อมูลแจ้งข่าวสารและประชาสัมพันธ์ก่อนหยุดจ่ายน้ำ	SMS Alert, Internet,e-mail, Social Network (Facebook,Twitter)	✓	✓	✓	✓	✓	✓	✓	✓
การรับฟังเสียง และเรื่องร้องเรียนของลูกค้า (ผู้มีส่วนได้ส่วนเสียภายนอก)	e-mail, Web Board ,Social Network (Facebook,Twitter), MWA Call Center 1125				✓	✓	✓	✓	✓

ข้อมูลและสารสนเทศ	การเข้าถึงข้อมูล	กลุ่มผู้ใช้ภายใน			กลุ่มผู้ใช้ภายนอก				
		ผู้บริหาร	พนักงานระดับ 1-5	ลูกจ้าง/ตัวแทน	ผู้ส่งมอบ	คู่ค้า	คู่ความร่วมมือ	ลูกค้า	หน่วยงานเชิงนโยบาย/ผู้ถือหุ้น
การบริการงานติดตั้งประปา ธุรกรรมให้กับลูกค้า	e-Service ผ่านระบบ Internet							✓	
ข้อมูลบริหารการเงินการคลังภาครัฐ	GFMIS ผ่านระบบวงจรเช่า (Leased Line)								✓
การบริหารจัดการการเบิกจ่ายเงินของผู้ขาย/ผู้รับจ้าง	e-Tracking ผ่านระบบ Internet				✓	✓			
การบริหารจัดการสารเคมี	Online ผ่านระบบโลจิสติกส์ในการจัดซื้อสารเคมีของโรงงานผลิตน้ำ	✓	✓			✓			
ข้อมูลแผนที่หัวดับเพลิง	ระบบแผนที่หัวดับเพลิง ผ่านระบบ Internet	✓	✓	✓	✓	✓	✓	✓	✓
การจัดหาพัสดุ	ประกาศ ทางหน้า เว็บไซต์ กปน. www.mwa.co.th	✓	✓	✓	✓	✓	✓	✓	✓
ข้อมูลองค์กร ผลิตภัณฑ์และบริการ ความรู้เกี่ยวกับกิจการประปา ข่าวประชาสัมพันธ์ และสถิติและการดำเนินงาน รวมถึงงานวิจัย พัฒนาและนวัตกรรม	ประกาศ ทางหน้า เว็บไซต์ กปน. www.mwa.co.th	✓	✓	✓	✓	✓	✓	✓	✓
ข้อมูลคุณภาพน้ำประปา	ประกาศ ทางหน้า เว็บไซต์ กปน. www.mwa.co.th	✓	✓	✓	✓	✓	✓	✓	✓

แบบรายงานผลการดำเนินงาน (Organizational Performance Form)

หมวดที่ 4 การวัด การวิเคราะห์ และการจัดการความรู้

หัวข้อที่	ประเด็นพิจารณา
4.2 ก (3)	**การจัดการความรู้** ● รัฐวิสาหกิจดำเนินการอย่างไร ในการจัดการความรู้ขององค์กร เพื่อให้บรรลุผลในเรื่องต่อไปนี้ ■ การรวบรวมและถ่ายทอดความรู้ของบุคลากร ■ การใช้ผลการทบทวนผลการดำเนินการเพื่อแลกเปลี่ยนเรียนรู้บทเรียนและวิธีปฏิบัติที่เป็นเลิศข้ามหน่วยงานและกระบวนการทำงาน ■ การถ่ายทอดความรู้ที่เกี่ยวข้องกับองค์กร ระหว่างองค์กรกับลูกค้า ผู้ส่งมอบ คู่ค้า และคู่ความร่วมมือ ■ การค้นหาและระบุ การแบ่งปัน และการนำวิธีปฏิบัติที่เป็นเลิศไปปฏิบัติอย่างรวดเร็ว ■ การรวบรวมความรู้และถ่ายทอดความรู้ที่เกี่ยวข้องไปใช้ในการสร้างนวัตกรรมและกระบวนการวางแผนเชิงยุทธศาสตร์

ปัจจัยสำคัญที่เกี่ยวข้อง (จากบริบทของรัฐวิสาหกิจ)	
บริบท 1 ก (2) วิสัยทัศน์ ค่านิยม ภารกิจ บริบท 1 ก (3) ลักษณะโดยรวมของบุคลากร บริบท 1 ข (2) กลุ่มลูกค้า กลุ่มผู้มีส่วนได้ส่วนเสีย และส่วนตลาด	บริบท 1 ข (3) ผู้ส่งมอบ คู่ค้า คู่ความร่วมมือ บริบท 2 ค การปรับปรุงผลการดำเนินการ

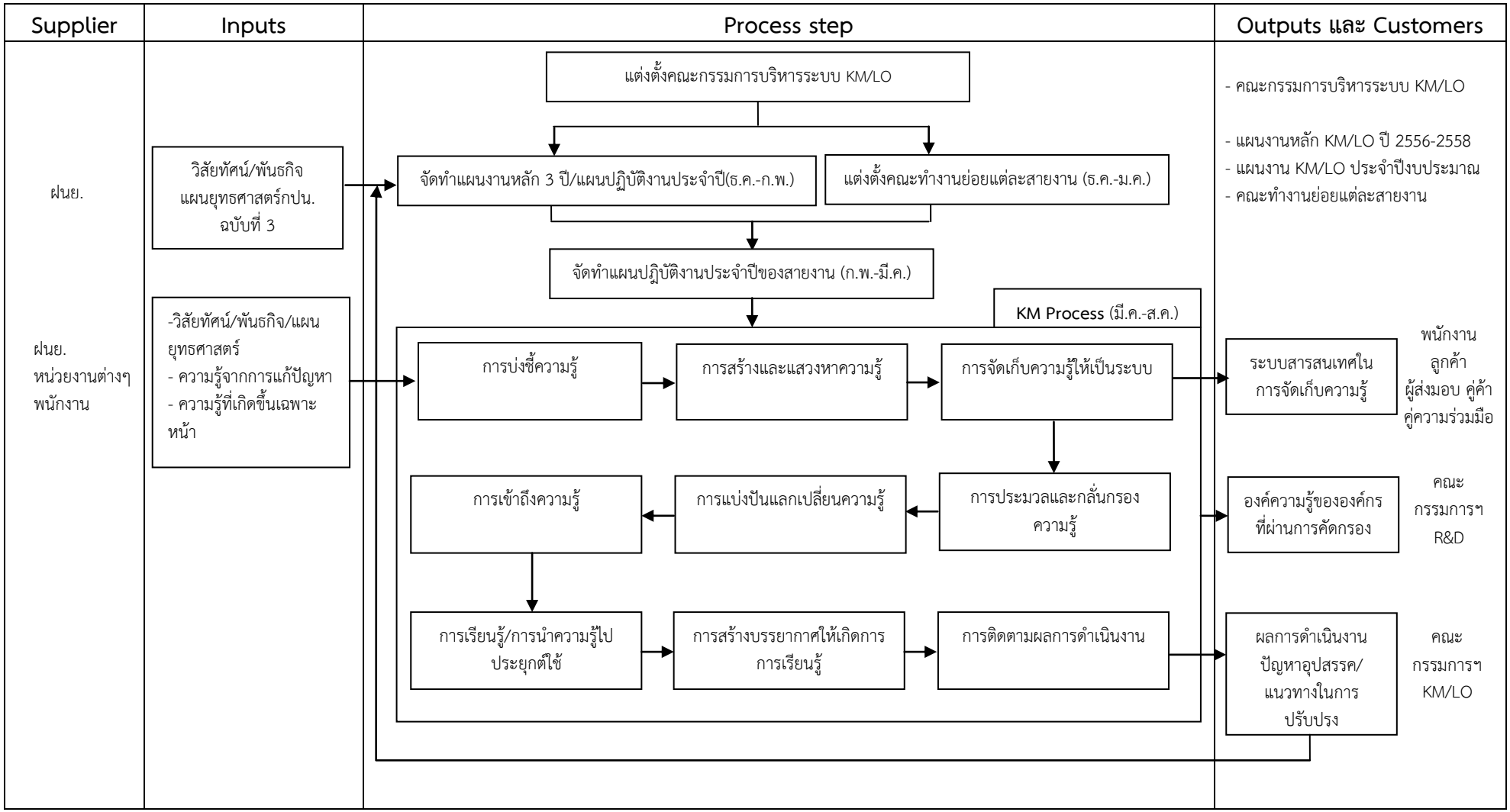
ประเด็นประเมิน	คำอธิบาย	เอกสารอ้างอิง
แนวทาง	● **การรวบรวมและถ่ายทอดความรู้ของบุคลากร** ผู้ว่าการแต่งตั้งคณะกรรมการบริหารระบบการบริหารองค์ความรู้และการสร้างองค์การแห่งการเรียนรู้ เพื่อดำเนินการบริหารกระบวนการ KM/LO ให้สอดคล้องกับวิสัยทัศน์ ภารกิจ แนวนโยบายและแผนยุทธศาสตร์ขององค์กร และแต่งตั้งคณะทำงานย่อยแต่ละสายงานจำนวน 8 คณะในการดำเนินการให้บรรลุตามวัตถุประสงค์ ของแผนงานหลัก KM/LO ปีงบประมาณ 2556-2558 และแผนปฏิบัติงานประจำปีที่กำหนดไว้ โดยมีขั้นตอนการดำเนินกิจกรรมการจัดการความรู้ของ กปน. ตามภาพที่ 4.2 ข(2)–1 ซึ่งประกอบด้วยขั้นตอนสำคัญ (KM Process) 9 ขั้นตอน ได้แก่ การบ่งชี้ความรู้ การสร้างและแสวงหาความรู้ การจัดเก็บความรู้ให้เป็นระบบ การประมวลผลและกลั่นกรองความรู้ การแบ่งปันแลกเปลี่ยนความรู้ การเข้าถึงความรู้ การเรียนรู้/การนำความรู้ไปประยุกต์ใช้ การสร้างบรรยากาศให้เกิดการเรียนรู้ และการติดตามผลการดำเนินงาน โดยแต่ละขั้นตอนจะมี	- แผนงานหลัก KM/LO ปีงบประมาณ 2556-2558 -แผนงาน KM/LO ประจำปีงบประมาณ 2556 -คำสั่งแต่งตั้งคณะกรรมการบริหารระบบการบริหารองค์ความรู้และการสร้าง

ประเด็นประเมิน	คำอธิบาย	เอกสารอ้างอิง
	ผู้รับผิดชอบและตัวชี้วัดผลการดำเนินงานตามตารางที่ 4.2 ข(3)–1 คณะกรรมการ KM/LO กำหนดขอบเขตความรู้ (KM Focus Areas) เป็น 3 แนวทาง ได้แก่ 1) ความรู้ที่สำคัญและจำเป็นต่อการสนับสนุน ประเด็นยุทธศาสตร์ วิสัยทัศน์ พันธกิจขององค์กร 2) ความรู้ที่ใช้ในการแก้ไขปัญหาการปฏิบัติงานด้านต่าง ๆ ของหน่วยงานหรือสายงาน หรือองค์กร 3) ความรู้ที่เกิดขึ้นเฉพาะหน้า ไม่มีการเตรียมการมาก่อน โดยคณะทำงานย่อยฯ (KM Team) และกลุ่มนักปฏิบัติ (CoPs) ใช้เป็นกรอบในการสร้างและแสวงหาความรู้ และดำเนินการจัดความรู้ตามแผนงาน ซึ่งสามารถแบ่งความรู้ออกเป็น 3 ประเภท ได้แก่ Explicit และ Tacit Knowledge และความรู้ประเภท Innovation และนำมาจัดเก็บในระบบสารสนเทศ KM/LO ของสายงาน (เว็บบล็อก กระดานข่าว ระบบฐานข้อมูล และการค้นหา) และกองวิจัย พัฒนาและนวัตกรรม สถาบันพัฒนาวิชาการประปา (กวพ.สพป.) ร่วมกับฝ่ายยุทธศาสตร์ด้านเทคโนโลยี (ฝยท.) ดำเนินการเชื่อมโยงระบบสารสนเทศ KM/LO ระดับองค์กร โดยมีการพัฒนาเว็ปไซต์ KM/LO ให้ทันสมัยและน่าสนใจอยู่เสมอ และแยกประเภทความรู้อย่างเป็นหมวดหมู่ชัดเจนเพื่อสะดวกในการสืบค้น คณะกรรมการฯ คัดกรององค์ความรู้ที่จัดเก็บเป็นองค์ความรู้ของระบบสารสนเทศขององค์กร โดยพิจารณาจากองค์ความรู้ที่มีความสำคัญ เป็นประโยชน์ และสอดคล้องกับประเด็นยุทธศาสตร์ สามารถนำความรู้ไปปฏิบัติได้จริง เกิดผลลัพธ์ที่เป็นรูปธรรม และมีโอกาสในการสร้างมูลค่าเพิ่ม จัดเก็บในระบบ KM/LO และถ่ายทอดให้กับพนักงานได้ใช้ในการศึกษา และนำไปประยุกต์ใช้ให้เกิดประโยชน์ต่อการปฏิบัติงาน และสามารถสร้างคุณประโยชน์ให้กับ กปน. ได้อย่างเป็นรูปธรรม ▪ การใช้ผลการทบทวนผลการดำเนินการเพื่อแลกเปลี่ยนเรียนรู้บทเรียนและวิธีปฏิบัติที่เป็นเลิศข้ามหน่วยงานและกระบวนการทำงาน คณะทำงานย่อยฯ (KM Team) กลุ่มนักปฏิบัติ (CoPs) ทั้งในสายงานและข้ามสายงานมีการพิจารณาความรู้ที่ใช้ในการแก้ไขปัญหาการปฏิบัติงานด้านต่าง ๆ ของหน่วยงาน หรือสายงาน หรือองค์กร และความรู้ที่เกิดขึ้นเฉพาะหน้า ไม่มีการเตรียมการมาก่อน ซึ่งได้มาจากการทบทวนผลการดำเนินงานเทียบกับตัวชี้วัดผลการดำเนินงานระดับหน่วยงาน และระดับบุคคล มาใช้ในเป็นหัวข้อการจัดการความรู้และแลกเปลี่ยนเรียนรู้ตามที่กล่าวไว้ข้างต้น ● **การถ่ายทอดความรู้ระหว่างรัฐวิสาหกิจกับลูกค้า ผู้ส่งมอบ คู่ค้าและคู่ความร่วมมือ**	องค์การแห่งการเรียนรู้ -คำสั่งแต่งตั้งคณะทำงานย่อยแต่ละสายงาน - คู่มือการจัดการความรู้

ประเด็นประเมิน	คำอธิบาย	เอกสารอ้างอิง
	กปน. มีการถ่ายทอดความรู้ระหว่างรัฐวิสาหกิจ ที่เกี่ยวข้องกับลูกค้า ผู้ส่งมอบ คู่ค้า และคู่ความร่วมมือ โดย ฝยท. และหน่วยงานที่เกี่ยวข้องร่วมกันพิจารณาคัดกรองความรู้และจัดทำระบบสารสนเทศเพื่อให้ลูกค้า ผู้ส่งมอบ คู่ค้า และคู่ความร่วมมือ ให้สามารถเข้าถึงความรู้ผ่านทางระบบสารสนเทศในรูปแบบ Online ซึ่งตอบสนองตามความต้องการของทุกกลุ่มผู้ใช้บริการ ตามตารางที่ 4.2 ก (3)-1 อาทิเช่น - เว็บไซต์งานจัดซื้อจัดจ้างสำหรับ ผู้ส่งมอบ คู่ค้า เพื่อการติดตามข่าว ประกาศ จัดซื้อ/จัดจ้าง ระเบียบ กฎหมายที่เกี่ยวข้อง การขึ้นทะเบียนผู้ขาย การอบรม และการติดตามการเบิกจ่ายเงินของผู้ขาย - เว็บไซต์เผยแพร่ข้อมูลให้กับคู่ความร่วมมือ เพื่อการเผยแพร่ผลงานวิจัย และนวัตกรรมของ กปน. เป็นต้น ● **การค้นหาและระบุ การแบ่งปัน และนำวิธีการปฏิบัติที่เป็นเลิศไปปฏิบัติอย่างรวดเร็ว** คณะทำงานย่อยฯ (KM Team) กลุ่มนักปฏิบัติ (CoPs) ทั้งในสายงานและข้ามสายงาน ดำเนินการค้นหาและระบุ การแบ่งปัน และนำวิธีการปฏิบัติที่เป็นเลิศไปปฏิบัติตามขั้นตอนการจัดการความรู้ตามภาพที่ 4.2 ก(3)–1 โดยผ่านกระบวนการแบ่งปันและแลกเปลี่ยนเรียนรู้ที่สำคัญ ได้แก่ การสอนงาน (Coaching) การจัดให้มีพี่เลี้ยง (Mentoring) การถ่ายทอดความรู้จากรุ่นสู่รุ่น (Knowledge Transfer) การจัดเวทีแลกเปลี่ยน ถ่ายทอดความรู้ระหว่างพนักงานหรือจากบุคคลภายนอก การประชุมแลกเปลี่ยนกันในกลุ่มนักปฏิบัติ (CoPs) ตลอดจนการเผยเพร่ความรู้ผ่านช่องทางต่างๆ เพื่อสื่อสารประชาสัมพันธ์ เชิญชวนบุคลากรให้เข้ามาศึกษาความรู้ และนำไปประยุกต์ใช้ให้เกิดประโยชน์ต่อการปฏิบัติงาน และสามารถสร้างคุณประโยชน์ให้กับ กปน. นอกจากนั้น คณะทำงานคัดเลือกฯ ของแต่ละสายงาน คัดเลือกหัวข้อ KM และการพัฒนากระบวนงานที่ผ่านการประกวดจากปีที่ผ่านมา รวมทั้งแนวความคิดด้านนวัตกรรมจากหน่วยงาน/พนักงานที่ได้จากการศึกษาดูงานวิธีปฏิบัติที่เป็นเลิศในด้านกิจการประปาทั้งหน่วยงานภายในและต่างประเทศ นำเสนอคณะกรรมการวิจัยและพัฒนาการบริหารจัดการองค์ความรู้ให้ความเห็นชอบพิจารณาข้อเสนอโครงการวิจัยจากหน่วยงานภายในและภายนอก เพื่อสนับสนุนให้เกิดงานวิจัย พัฒนาต่อยอด และนำไปประยุกต์ใช้ให้เกิดประโยชน์ ตลอดจนก่อให้เกิดเป็นนวัตกรรมขององค์กร โดยมี กวพ.สพป. รวบรวมจัดเก็บ และเผยแพร่ ประชาสัมพันธ์ผลงานวิจัยและองค์ความรู้ในเว็ปไซต์ R&D ตลอดจนการจัดการประชุมวิชาการ	รายงานผลตามแผนงาน โครงการเพิ่มประสิทธิภาพการบริหารสินทรัพย์เพื่อสร้างมูลค่าเพิ่มให้แก่องค์กร

ประเด็นประเมิน	คำอธิบาย	เอกสารอ้างอิง
	ด้านวิจัย พัฒนา และนวัตกรรม ตามภาพที่ 4.2 ก(3) – 2 ตัวอย่างผลงานวิจัยที่นำมาสร้างมูลค่าเพิ่มโดยนำมาต่อยอดในเชิงพาณิชย์ ได้แก่ โครงการการศึกษาคุณสมบัติและองค์ประกอบของดินตะกอนประปา เพื่อนำมาผลิตเป็นดินเพาะปลูกและอิฐบล๊อกประสาร และโครงการการศึกษาวิจัยศักยภาพและคุณสมบัติทางกายภาพของส่วนผสมดินตะกอนประปากับซีเมนต์เพื่อใช้ลดความซึมผ่านของรอยแตกในมวลหิน ● การรวบรวมความรู้และถ่ายทอดความรู้ที่เกี่ยวข้องไปใช้ในการสร้างนวัตกรรมและกระบวนการวางแผนเชิงยุทธศาสตร์ - คณะกรรมการฯ KM/LO กำหนดขอบเขตความรู้โดยมีการพิจารณาความรู้ที่สำคัญและจำเป็นต่อการสนับสนุน ประเด็นยุทธศาสตร์ วิสัยทัศน์ พันธกิจขององค์กร และมีการกำหนดประเภทของความรู้ประเภท Innovation ขึ้นเพื่อให้คณะทำงานย่อยฯ (KM Team) และกลุ่มนักปฏิบัติ (CoPs) ใช้ในการสร้างและแสวงหาความรู้ตามขอบเขตที่กำหนดและดำเนินการจัดการความรู้ตามภาพที่ 4.2 ก (3)–1 ทั้งนี้เพื่อนำความรู้ที่ได้ไปใช้สนับสนุนการดำเนินงานตามแผนยุทธศาสตร์ให้บรรลุผลตามเป้าหมายที่กำหนดไว้ และคัดกรองความรู้ที่สามารถวิจัย พัฒนาต่อยอดให้เกิดนวัตกรรมในกระบวนการ R&D ต่อไป - คณะกรรมการฯ R&D และคณะทำงานคัดเลือกฯของแต่ละสายงาน คัดเลือกองค์ความรู้ และการพัฒนากระบวนงานที่ผ่านการคัดกรองจากปีที่ผ่านมา และแนวคิดด้านนวัตกรรม นำมาพิจารณาต่อยอด สนับสนุนให้เกิดงานวิจัย พัฒนาและนวัตกรรมตามภาพที่ 4.2 ก (3) – 2 - ผู้บริหารระดับสูง และ ฝนย. นำผลการดำเนินงานด้าน KM/LO และ R&D ประกอบการทบทวนแผนยุทธศาสตร์และแผนปฏิบัติงานประจำปี และการจัดทำแผนยุทธศาสตร์	
การนำแนวทางไปปฏิบัติ	คณะกรรมการฯ KM/LO และ สพป. ถ่ายทอดและประชาสัมพันธ์แนวทางการจัดการความรู้ให้กับคณะทำงานย่อย ฯของแต่ละสายงาน กลุ่มนักปฏิบัติ และพนักงานทุกคน ผ่านทางคู่มือการจัดการความรู้ เว็ปไซต์ KM/LO และสื่อประชาสัมพันธ์ เป็นประจำทุกปี	-คู่มือการจัดการความรู้
การปรับปรุง	ผู้บริหารระดับสูงทบทวนการแต่งตั้งคณะกรรมการฯ KM/LO คณะกรรมการฯ R&D คณะทำงานย่อย แผนการดำเนินงานและตัวชี้วัดเป็นประจำทุกปี ให้สอดคล้องกับแผนยุทธศาสตร์และถ่ายทอดแผนปฏิบัติงานให้กับหน่วยงานที่เกี่ยวข้อง และมีการติดตามความก้าวหน้าตามแผนการปฏิบัติงานอย่างสม่ำเสมอ	

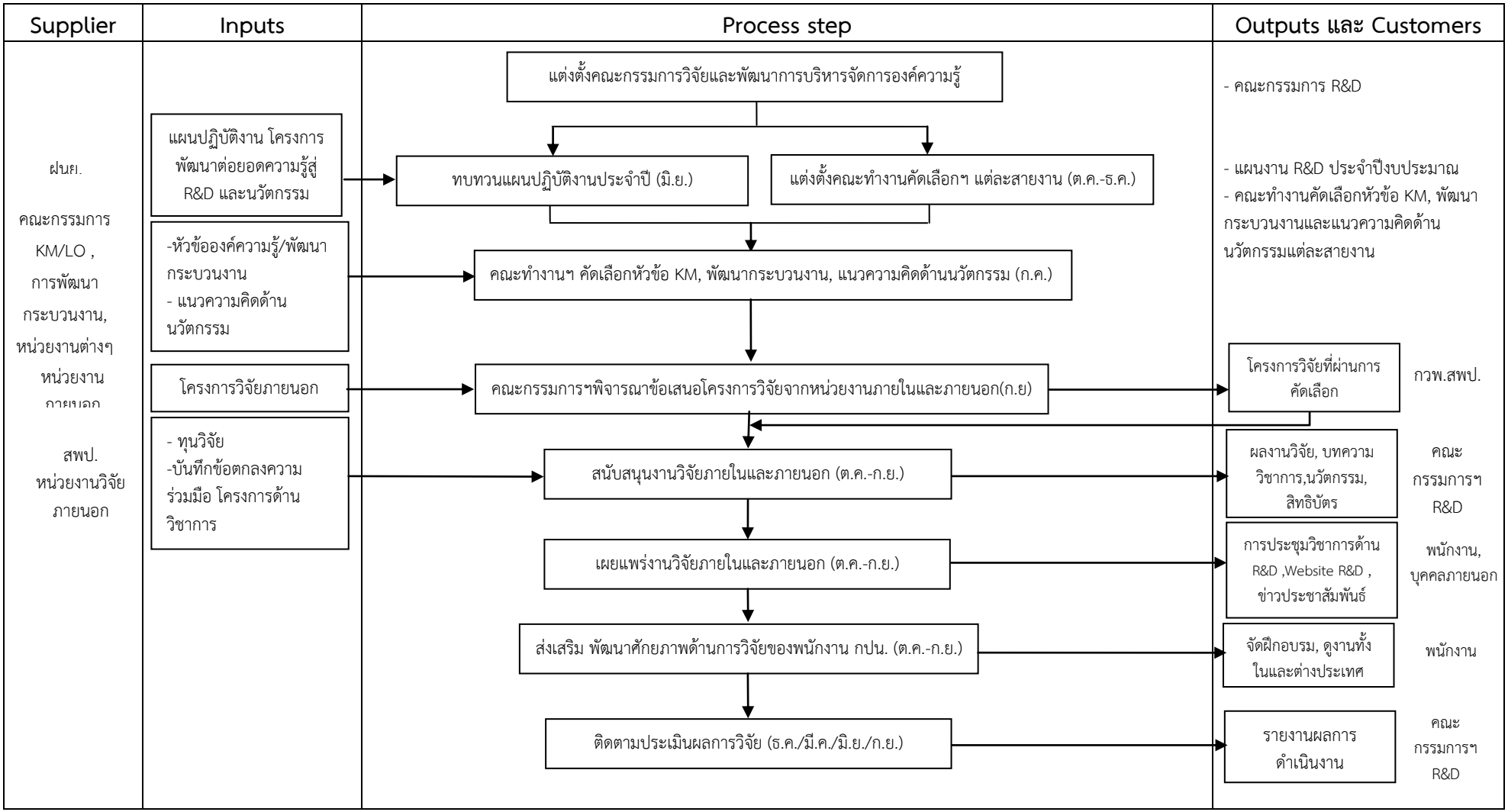
ประเด็นประเมิน	คำอธิบาย	เอกสารอ้างอิง
	ผวก. และคณะกรรมการฯ KM/LO ประชุมทบทวนกระบวนการจัดการรู้ของ กปน. โดยมีการปรับปรุงที่สำคัญดังนี้ 1. เปลี่ยนหน้าที่ความรับผิดชอบหลักในการบริหารจัดการจากฝ่ายบริหารทรัพยากรบุคคล (ฝบบ.) ไปเป็น กวพ.สพป. ทั้งนี้เพื่อความคล่องตัวในการปฏิบัติงาน และความเชื่อมโยงกับกระบวนการวิจัย พัฒนา และนวัตกรรมของ กปน. 2. จัดทำแผนงานหลัก KM/LO 3 ปี (ปีงบประมาณ 2556 – 2558) เพื่อกำหนดแนวทางในการดำเนินงานจัดการความรู้ของ กปน. ให้เป็นส่วนหนึ่งของวัฒนธรรมองค์กร และพัฒนาไปสู่การเป็นองค์กรแห่งการเรียนรู้ 3. ทบทวนตัวชี้วัดผลการดำเนินงานให้มีประสิทธิผลทั้งตัวชี้วัดในแต่ละขั้นตอนและภาพรวมของการจัดการความรู้ เพื่อนำ ผลมาใช้ปรับปรุง และพัฒนาการจัดการความรู้ต่อไป สำหรับกระบวนการด้านวิจัย พัฒนา และนวัตกรรม ปีงบประมาณ 2556 คณะกรรมการฯ R&D และ สพป. ประชุมทบทวนกระบวนการ อยู่ระหว่างการจัดทำแผนแม่บทงานวิจัย พัฒนา และนวัตกรรมของ กปน.ปี 2557 - 2561 เพื่อให้มีกรอบแนวทางและเป้าหมายโดยรวมของการดำเนินงานด้านวิจัย พัฒนา และนวัตกรรมของ กปน. แบบบูรณาการและสอดคล้องกับนโยบายการดำเนินงานของ กปน. รวมถึงยุทธศาสตร์การบริหาร กปน. และยุทธศาสตร์การวิจัยของชาติ	
การบูรณาการ	กปน. มีการจัดการความรู้จากความรู้ที่สำคัญและจำเป็นต่อการสนับสนุน ประเด็นยุทธศาสตร์ วิสัยทัศน์ พันธกิจขององค์กร (บริบท 1 ก (2)) และความรู้ที่ใช้ในการแก้ไขปัญหาการปฏิบัติงานด้านต่าง ๆ ของหน่วยงาน หรือสายงาน หรือองค์กร ตลอดจนความรู้ที่เกิดขึ้นเฉพาะหน้า ไม่มีการเตรียมการมาก่อน โดยถ่ายทอดให้บุคลากรทุกกลุ่ม และกลุ่มผู้มีส่วนได้ส่วนเสีย (บริบท 1 ก (3) และบริบท 1 ข (2) –(3)) นำไปปฏิบัติ ผ่านกระบวนการแบ่งปันและแลกเปลี่ยนเรียนรู้ที่สำคัญ เช่น การสอนงาน การจัดให้มีพี่เลี้ยง การถ่ายทอดความรู้จากรุ่นสู่รุ่น (Knowledge Transfer) การจัดเวทีแลกเปลี่ยนถ่ายทอดความรู้ระหว่างพนักงาน หรือจากบุคคลภายนอก (หมวด 5) รวมถึงนำความรู้ไปต่อยอด สนับสนุนให้เกิดงานวิจัย และพัฒนาให้เกิดนวัตกรรม และประกอบการทบทวนแผนยุทธศาสตร์และแผนปฏิบัติงานประจำปี และการจัดทำแผนยุทธศาสตร์ขององค์กร (หมวด 2)	



ภาพที่ 4.2 ก (3) – 1 : กระบวนการจัดการความรู้ของ กปน.

ขั้นตอน	ผู้รับผิดชอบ						ตัวชี้วัดการดำเนินการ
	คณะกรรมการฯ KM/LO	คณะทำงานย่อยแต่ละสายงาน	กลุ่มนักปฏิบัติ	บุคลากรทั้งองค์กร	กวพ.สพป.	ฝยท.	
การบ่งชี้ความรู้	✓	✓					-จำนวนประเด็นความรู้ที่สอดคล้องกับยุทธศาสตร์
การสร้างและแสวงหาความรู้		✓	✓				-มีการจัดทำแผนการสอนงานและดำเนินการสอนงาน -ทุกหน่วยงานที่มีพนักงานใหม่จัดให้มีพี่เลี้ยง
การจัดเก็บความรู้ให้เป็นระบบ		✓	✓		✓	✓	-มีบัญชีความรู้ที่จัดทำในปีบัญชี จัดเก็บและเผยแพร่ในระบบ KM/LO ครบถ้วน
การประมวลผลและกลั่นกรองความรู้	✓	✓			✓	✓	-มีความรู้ที่ได้รับการคัดกรองจากคณะกรรมการฯ เพื่อนำไปจัดเก็บในคลังความรู้ของ กปน.
การแบ่งปันแลกเปลี่ยนความรู้	✓	✓	✓		✓	✓	-จำนวนหัวข้อความรู้ที่ได้รับจากผู้บริหาร และพนักงาน ผู้เชี่ยวชาญซึ่งจะเกษียณอายุ จัดเก็บในระบบ KM/LO -จำนวนครั้งในการจัดเวทีถ่ายทอดความรู้จากรุ่นสู่รุ่น -จำนวนคนในทำเนียบผู้เชี่ยวชาญ กปน. -จำนวนครั้งในการจัดเวทีแลกเปลี่ยน ถ่ายทอดความรู้ -จำนวนกระทู้ที่เข้ามา Sharing ใน Web board -จำนวนกลุ่มนักปฏิบัติ
การเข้าถึงความรู้	✓	✓	✓				-ทุกสายงานมีบอร์ดเผยแพร่องค์ความรู้ของสายงาน -จำนวนเรื่องในการเผยแพร่ข่าวประชาสัมพันธ์
การเรียนรู้/การนำความรู้ไปประยุกต์ใช้	✓	✓	✓	✓			-จำนวนเรื่องที่มีการนำความรู้ไปประยุกต์ใช้ -จำนวนเรื่องที่มีการนำองค์ความรู้ไปต่อยอด ให้เกิดเป็นนวัตกรรม
การสร้างบรรยากาศให้เกิดการเรียนรู้	✓	✓	✓				-มีการกำหนดหลักเกณฑ์และแนวทางการพิจารณารางวัลผลงานการจัดการความรู้ดีเด่น -จำนวนสายงานที่มีกิจกรรมการนำเสนอผลงาน -มีกิจกรรมงานวันแห่งการจัดการความรู้ (KM Day)
การติดตามผลการดำเนินงาน	✓	✓	✓		✓		-มีรายงานผลการดำเนินงานเสนอผู้ว่าการ -มีรายงานผลการดำเนินงานตามแผนงาน KM/LO ประจำปี -มีแบบสอบถามขอรับความคิดเห็นของพนักงาน

ตารางที่ 4.2 ก (3) – 1 : ผู้รับผิดชอบและตัวชี้วัดในแต่ละขั้นตอนของกระบวนการจัดการความรู้ของ กปน.



ภาพที่ 4.2 ก (3) – 2 : กระบวนการวิจัย พัฒนา และนวัตกรรมของ กปน.

แบบรายงานผลการดำเนินงาน (Organizational Performance Form)

หมวดที่ 4 การวัด การวิเคราะห์ และการจัดการความรู้

หัวข้อที่	ประเด็นพิจารณา
4.2 ข (1)	**คุณลักษณะของฮาร์ดแวร์และซอฟต์แวร์** ● รัฐวิสาหกิจดำเนินการอย่างไร เพื่อให้ฮาร์ดแวร์และซอฟต์แวร์มีความเชื่อถือได้ ปลอดภัย และใช้งานง่าย

ปัจจัยสำคัญที่เกี่ยวข้อง (จากบริบทของรัฐวิสาหกิจ)	
บริบท 1 ก (5) รัฐวิสาหกิจดำเนินการภายใต้สภาพแวดล้อมด้านกฎ ระเบียบข้อบังคับ บริบท 1 ข (2) กลุ่มลูกค้า กลุ่มผู้มีส่วนได้ส่วนเสีย และส่วนตลาด	บริบท 1 ข (3) ผู้ส่งมอบ คู่ค้า คู่ความร่วมมือ บริบท 2 ค การปรับปรุงผลการดำเนินการ

ประเด็นประเมิน	คำอธิบาย	เอกสารอ้างอิง
แนวทาง	■ **<u>ความเชื่อถือได้</u>** กระบวนการที่ทำให้ฮาร์ดแวร์และซอฟต์แวร์มีความเชื่อถือได้ มีรายละเอียดดังนี้ คณะกรรมการ ICT (ICT Steering Committee) มีเกณฑ์การพิจารณาจัดหาอุปกรณ์ฮาร์ดแวร์ และซอฟต์แวร์ที่เหมาะสม โดยพิจารณาจากผลิตภัณฑ์ต้องได้รับรองตามมาตรฐานสากล เช่น ISO9000 FC UL เป็นต้น การได้รับความนิยม Gartner magic quadrant และมีการบำรุงรักษาอย่างต่อเนื่อง นอกจากนั้นซอฟต์แวร์ที่ได้รับความเชื่อถือ จะต้องมีการใช้งานกันอย่างแพร่หลายในหน่วยงานทั้งภาครัฐและเอกชน มีการพัฒนาอย่างต่อเนื่อง อีกทั้งเป็นมาตรฐานในการแลกเปลี่ยนข้อมูลระหว่างหน่วยงาน เช่น ซอฟต์แวร์ SAP, MS Office, Oracle Database เป็นต้น ■ **<u>ความปลอดภัย</u>** กระบวนการที่ทำให้ฮาร์ดแวร์และซอฟต์แวร์มีความปลอดภัย มีรายละเอียดดังนี้ 1) คณะกรรมการด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ ได้กำหนดนโยบายการบริหารจัดการระบบความมั่นคงปลอดภัยสารสนเทศและคู่มือการปฏิบัติงานภายใต้ “ระเบียบการประปานครหลวง ฉบับที่ 18 ว่าด้วยการรักษาความปลอดภัยระบบสารสนเทศ (พ.ศ. 2548)” โดยพนักงาน กปน. ทุกคนต้องถือปฏิบัติ และมีส่วนบริหารความมั่นคงปลอดภัยสารสนเทศเป็น	-คู่มือประกอบ “ระเบียบการประปานครหลวง ฉบับที่ 18 ว่าด้วยการรักษาความปลอดภัยระบบ

ประเด็นประเมิน	คำอธิบาย	เอกสารอ้างอิง
	ผู้รักษาระเบียบนี้ โดยนำเครื่องมือสารสนเทศ เช่น ระบบ Active Directory (AD), ระบบตรวจจับการบุกรุก (Intrusion Prevention System : IPS), ระบบ Firewall และ ระบบป้องกันไวรัส พร้อมทั้งกำหนดขั้นตอนในการปรับปรุงแก้ไข Config หรือโปรแกรมโดยได้รับการอนุมัติจากผู้บริหารระดับสูง 2) ฝ่ายเทคโนโลยีสารสนเทศและสื่อสาร (ฝยส.) ได้จัดให้มีระบบจัดเก็บ Log 90 วันตามข้อกำหนดตามพระราชบัญญัติว่าด้วยการกระทำความผิดทางคอมพิวเตอร์ พ.ศ. 2550 เพื่อบันทึกความเคลื่อนไหวข้อมูลภายในองค์กรที่มีการเชื่อมต่ออินเตอร์เน็ตสู่ภายนอก ทำให้สามารถทราบถึงภัยคุกคามที่อาจเกิดขึ้น และเป็นแนวทางในการทำการแก้ไขปรับปรุงการใช้งานข้อมูลคอมพิวเตอร์ ทั้งยังเป็นแหล่งข้อมูลในการทำ Computer Audit ของหน่วยงานภาครัฐภายนอก 3) คณะกรรมการด้านการรักษาความมั่นคงปลอดภัยสารสนเทศตามมาตรฐาน ISO 27001 กำหนด นโยบาย มาตรการ และกระบวนการรักษาความมั่นคงปลอดภัยสารสนเทศ ของ กปน. เพื่อให้มั่นใจว่าสารสนเทศได้มีการบริหารจัดการความมั่นคงปลอดภัยอย่างเป็นระบบ มีการประเมินผล ทบทวน และนำมาพัฒนาปรับปรุงอย่างสม่ำเสมอ และเป็นไปตามบทบัญญัติกฎหมาย โดยคณะกรรมการฯ มีการทบทวนนโยบาย เป็นประจำทุกปีและสอดคล้องกับการรับการตรวจสอบ Certificate ISO/IEC27001:2005 ของ External Auditor 4) ฝยส. มีหน้าที่ดูแล และกำหนดการเข้าถึงระบบสารสนเทศให้มีความพร้อมใช้และปลอดภัย โดยมีเกณฑ์จัดแบ่ง Zone ของการจัดวางอุปกรณ์ เช่น Zone ผู้ดูแลระบบ, Zone ผู้ใช้งานระบบงาน, Zone ผู้ใช้งานทั่วไป(ผู้มีส่วนได้ส่วนเสียภายในและภายนอก)และ Zone ผู้ใช้งานระดับสูง 5) ผวก. มีคำสั่งแต่งตั้งคณะทำงานกำหนดนโยบายและแนวปฏิบัติด้านเทคโนโลยีสารสนเทศและการสื่อสารในสถานการณ์อุทกภัยกำหนดให้มีแผนรองรับสถานการณ์ในภาวะฉุกเฉิน เช่น ไฟไหม้ ภัยธรรมชาติ โดยในปี 2555 ได้มีการจัดทำแผนฉุกเฉินเพื่อรองรับเหตุอุทกภัย และมีการประกาศแผนให้พนักงานได้รับทราบเพื่อปฏิบัติตามนโยบายและแผนปฏิบัติในสถานการณ์อุทกภัย ■ **<u>ใช้งานง่าย</u>** กระบวนการที่ทำให้ฮาร์ดแวร์และซอฟต์แวร์ใช้งานง่าย มีรายละเอียดดังนี้ 1) การจัดหาฮาร์ดแวร์ ซอฟต์แวร์โดยผ่านคณะกรรมการบริหารงานด้านสารสนเทศ (IT Streering Committee) ซึ่งมา	สารสนเทศ (พ.ศ. 2548)”

ประเด็นประเมิน	คำอธิบาย	เอกสารอ้างอิง
	จากสายงานที่ต้องการนำไปใช้งาน จะมีขั้นตอนการตรวจสอบ Prove Of Concept (POC) เพื่อคัดเลือกผลิตภัณฑ์ที่ใช้งานง่ายและตรงความต้องการ โดย Weight Score แต่ละผลิตภัณฑ์ โดยใช้เกณฑ์ในการจัดหาอุปกรณ์ ฮาร์ดแวร์และซอฟต์แวร์ ให้เป็นไปตามมาตรฐานกระทรวงเทคโนโลยีสารสนเทศ และกระทรวงมหาดไทย จากนั้นจึงจัดหาให้กับหน่วยงานต่าง ๆ เช่น 1.1 นำระบบ GIS มาใช้สนับสนุนงานบริการลูกค้าให้สื่อสารได้ง่าย และ ง่ายต่อการปฏิบัติงานของพนักงานในสำนักงาน และการปฏิบัติงานในภาคสนาม 1.2 การเข้าถึงข้อมูลสารสนเทศด้วย Web Application เช่น ใช้งานด้วย Web Browser ผ่านทาง PC, Notebook หรือ Mobile device 2) ฝพท. ใช้กระบวนการพัฒนาซอฟต์แวร์ตามหลัก SDLC เพื่อให้ตรงตามความต้องการของผู้ใช้งาน โดยให้ผู้ใช้งานมีส่วนร่วมในขั้นตอนการพัฒนา มีขั้นตอนการพัฒนา ตามที่ ฝพท. กำหนด 3) สายงานเทคโนโลยีสารสนเทศ ร่วมกับ ฝ่ายพัฒนาทรัพยากรบุคคล (ฝพบ.) อบรมเผยแพร่ความรู้ด้านการใช้งานระบบงานหรือซอฟต์แวร์ และความปลอดภัยให้กับบุคลากรด้าน ICT อย่างต่อเนื่อง เช่นการอบรมการใช้งานในผลิตภัณฑ์ใหม่ หรืออบรมเมื่อมีการแก้ไข ปรับปรุงพัฒนาซอฟต์แวร์เป็นต้น **<u>ตัวชี้วัด</u>** 1) ระดับความพึงพอใจต่อระบบสารสนเทศ ของผู้ใช้บริการภายในและภายนอกองค์กร 2) การควบคุมการปฏิบัติงานภายใต้กรอบความมั่นคงปลอดภัยสารสนเทศตามมาตรฐานสากล ISO/IEC 27001:2005 – วัดระดับความสำเร็จในการดำเนินงาน โดยที่เครื่องแม่ข่ายสามารถให้บริการระบบ CIS และ SAP ได้รับการดูแลตามมาตรฐาน ISO/IEC 27001:2005 โดยมีระยะเวลาหยุดให้บริการ (Downtime) ไม่เกิน 3% (262 ชั่วโมง)	
การนำแนวทางไปปฏิบัติ	1) ฝยส. ใช้กระบวนการบริหารจัดการด้านความมั่นคงปลอดภัยระบบ ICT ตามมาตรฐาน ISO/IEC 27001:2005 กำหนดขอบเขตดำเนินการที่ศูนย์คอมพิวเตอร์หลักและศูนย์คอมพิวเตอร์สำรอง โดยดำเนินการเกี่ยวกับ Physical and System Environment Control Systems Security Infrastucture Systems และ Server Infrastructure รวมทั้งตรวจสอบช่องโหว่ของระบบปฏิบัติการ (Vulnerability Assessment) และวิเคราะห์ผลการตรวจสอบตามมาตรฐาน CWE/SANS TOP 25 / OWASP	

ประเด็นประเมิน	คำอธิบาย	เอกสารอ้างอิง
	TOP 10 โดยมีการตรวจสอบภายใน การทบทวนผลการดำเนินงานเพื่อกำหนด/ปรับปรุงนโยบายและการดำเนินงาน ISMS เป็นประจำทุกปี 2) คณะกรรมการบริหารงานด้านสารสนเทศ (IT Streering Committee) กำหนดให้ กปน. ใช้เกณฑ์ในการจัดหาอุปกรณ์ฮาร์ดแวร์และซอฟต์แวร์ ให้เป็นไปตามมาตรฐานกระทรวงเทคโนโลยีสารสนเทศ และกระทรวงมหาดไทย หากรายการใดไม่เป็นไปตามมาตรฐานดังกล่าว กปน. จะใช้หลักเกณฑ์ความนิยมของผู้ใช้งานทั่วไป โดยอ้างอิงจาก Gartner magic quadrant ซึ่งนำไปใช้เป็นเงื่อนไขในการจัดหาเป็นประจำทุกปี 3) การสอบทานด้าน ICT เป็นประจำทุกปี โดยผู้ตรวจสอบจากภายในและภายนอก เพื่อตรวจสอบความถูกต้อง และความเสี่ยงในด้านต่างๆ 4) การควบคุมด้าน ICT เป็นประจำทุกปี โดยสายงานเทคโนโลยีสารสนเทศ ร่วมกับ หน่วยงานเจ้าของข้อมูล (Data Owner) เช่น การควบคุมสิทธิ์ในการเข้าถึงข้อมูลสารสนเทศ การบริหารจัดการกลุ่มผู้ใช้งานระบบงาน 5) สายงานเทคโนโลยีสารสนเทศ ร่วมกับ หน่วยงานผู้ใช้ระบบงาน การฝึกซ้อมแผนรองรับสถานการณ์ในภาวะฉุกเฉินเป็นประจำทุกปี	
การปรับปรุง	ฝยท. นำผลการสำรวจความพึงพอใจมาวิเคราะห์โดยพิจารณาในผลลัพธ์ที่มีความพึงพอใจมาก ถึงมากที่สุด และในส่วนผลลัพธ์ที่พึงพอใจน้อย หรือไม่พอใจเลย เพื่อหาแนวทางปรับปรุงในกระบวนงานที่เกี่ยวข้องเป็นประจำทุกปี ตัวอย่างเช่น การขยายขอบเขตการควบคุมฯ ISO27001 ออกไปครอบคลุมถึง เครื่องแม่ข่ายของระบบงานหลัก (Infrastructure Server) เพื่อให้ได้รับการดูแลอย่างต่อเนื่อง ให้มีความพร้อมใช้และปลอดภัย	
การบูรณาการ	กระบวนการเพื่อให้ฮาร์ดแวร์และซอฟต์แวร์มีความเชื่อถือได้ ปลอดภัย และใช้งานง่ายเป็นการบริหารจัดการเพื่อให้เกิดมาตรฐานด้านฮาร์ดแวร์ ซอฟต์แวร์ที่ใช้อยู่ใน กปน. นับตั้งแต่กระบวนการในการจัดซื้อจัดหา จัดจ้างออกแบบและพัฒนาซอฟต์แวร์ เพื่อสนับสนุนการใช้เทคโนโลยีสารสนเทศใน ด้านผลิต ด้านบริการ ด้านบริหาร และงานสนับสนุนต่าง ๆ โดยที่ฮาร์ดแวร์ ซอฟต์แวร์ นั้นจะต้องใช้งานง่าย มีความปลอดภัย และเชื่อถือได้ ตอบสนองความต้องการขององค์กร และผู้มีส่วนได้เสียขององค์กร ครอบคลุมทุกด้าน และเหมาะสมกับสถานการณ์	

แบบรายงานผลการดำเนินงาน (Organizational Performance Form)

หมวดที่ 4 การวัด การวิเคราะห์ และการจัดการความรู้

หัวข้อที่	ประเด็นพิจารณา
4.2 ข (2)	**ระบบเตือนภัย** ● รัฐวิสาหกิจดำเนินการอย่างไร ในการจัดทำระบบสารสนเทศสนับสนุนรายงาน การวิเคราะห์ระดับผลกระทบความเสี่ยง และการเตือนภัย/แจ้งให้รู้ล่วงหน้า (Early Warning System) ถึงเหตุการณ์หรือความเสี่ยงที่จะเกิดขึ้น ซึ่งมีผลกระทบรุนแรงต่อองค์กร

ปัจจัยสำคัญที่เกี่ยวข้อง (จากบริบทของรัฐวิสาหกิจ)	
บริบท 2 ค ระบบปรับปรุงผลการดำเนินงาน	

ประเด็นประเมิน	คำอธิบาย	เอกสารอ้างอิง
แนวทาง	กปน. มีกระบวนการบริหารความเสี่ยงตามมาตรฐาน COSO ตั้งแต่การกำหนดนโยบายโดยคณะอนุกรรมการบริหารความเสี่ยง โดยมีฝ่ายบริหารความเสี่ยง (ฝบส.) ประสานงานและอำนวยความสะดวกแก่หน่วยงานเจ้าของความเสี่ยง ประกอบด้วย การกำหนดวัตถุประสงค์ การระบุเหตุการณ์ การประเมินความเสี่ยง การตอบสนองความเสี่ยง กิจกรรมการควบคุม การติดตามและประเมินผล สารสนเทศและการสื่อสาร สายงานเทคโนโลยีสารสนเทศ, ฝบส. และสำนักตรวจสอบ (สตส.) ร่วมกำหนดแนวทางการบูรณาการระบบสารสนเทศสนับสนุน การควบคุมภายใน การบริหารความเสี่ยง และการตรวจสอบภายใน พร้อมทั้งให้แสดงรายงานระดับผลกระทบความเสี่ยงและการเตือนภัย/แจ้งให้รู้ล่วงหน้า (Early Warning System) ระดับองค์กร ระบบสารสนเทศที่สนับสนุนรายงาน การวิเคราะห์ระดับผลกระทบความเสี่ยงและการเตือนภัย/แจ้งให้รู้ล่วงหน้า (Early Warning System)นั้นจะเป็นเครื่องมือที่สนับสนุนการตัดสินใจในกระบวนการตอบสนองความเสี่ยงและกิจกรรมการควบคุม ได้ทันท่วงที ดังนี้ 1. ระบบบริหารความเสี่ยงและควบคุมภายใน (Risk Management & Internal Control : RMIC) และระบบติดตามและประเมินผลโครงการ 2. ระบบ Early Warning System (ระดับเตือนภัย/แจ้งให้ทราบถึงเหตุการณ์หรือความเสี่ยงที่จะเกิดขึ้น ซึ่งมีผลกระทบรุนแรง	

ประเด็นประเมิน	คำอธิบาย	เอกสารอ้างอิง
	ต่อองค์กร) ประกอบด้วย 1) ระบบ (Business Intelligent) ด้านการบริหารความเสี่ยง ได้แก่ การเฝ้าระวังความเสี่ยงตามค่าดัชนีชี้วัดความเสี่ยง Key Risk Indicator : KRI และเหตุการณ์ที่มีผลกระทบต่อองค์กร (Incidents) ได้แก่ระบบน้ำดิบ, ระบบผลิต–สูบส่ง, ระบบสารสนเทศและระบบการเงิน 2) ระบบ Management Information System Express 3) ระบบ Executive Information System Express 4) ระบบงานการติดตามบริหารสัญญา (Contract Monitoring System : CMS) เพื่อสนับสนุนการติดตามการเบิกจ่ายงบลงทุน ให้สามารถติดตามและเร่งรัดการดำเนินการเบิกจ่ายงบลงทุนให้เป็นไปตามแผน ซึ่งระบบพัฒนาขึ้นในรูปแบบของ web Application ที่สามารถเข้าใช้งานได้ง่าย มีรายงานผลการดำเนินงาน รูปแบบแถบสีแจ้งสถานะ ทั้งนี้ถ้ารายการสัญญาใดมีการดำเนินงานที่ช้ากว่าแผนระบบจะบังคับให้หน่วยงานรายงานปัญหาและแนวทางการแก้ไข 5) ระบบสารสนเทศอื่นๆเพื่อ Early Warning System ด้านผลิตและส่งน้ำ ได้แก่ ระบบเครื่องวัดคุณภาพน้ำดิบทางไกลอัตโนมัติ , ระบบการเฝ้าระวังคุณภาพน้ำดิบทางไกลอัตโนมัติจากสถานีสูบน้ำดิบสำแลและบางเลนด้วยตู้ปลาไวพิษ (Real Time Fish Bio-monitoring) , ระบบเฝ้าระวังคุณภาพน้ำดิบทางไกลอัตโนมัติ, ระบบการรายงานคุณภาพน้ำประปา Real Time ผ่าน Internet นอกจากนั้น การวัดความเสี่ยงในระดับองค์กรกรณีตัวชี้วัดมีค่าเกิน Threshold ที่กำหนดไว้จะมีการ Early Warning โดยส่งข้อความแจ้งแก่ผู้บริหารผ่านทางโทรศัพท์มือถือ **<u>ตัวชี้วัด</u>** 1) ระดับความพึงพอใจต่อระบบสารสนเทศ ที่เกี่ยวข้องกับความเสี่ยงขององค์กรที่มี Early Warning เช่น ระดับความพึงพอใจระบบเฝ้าระวังคุณภาพน้ำดิบทางไกลและ ระบบบริหารความเสี่ยงและควบคุมภายใน (RMIC) เป็นต้น 2) การบูรณาการระบบเทคโนโลยีสารสนเทศ - ออกแบบการเชื่อมโยงข้อมูลสารสนเทศ ระบบงานผลิตและงานบริการ ได้ภายในเวลาที่กำหนด และ วัดจำนวน Service ของการบูรณาการระบบงาน ระบบงานผลิตและงานบริการ ได้ตามเกณฑ์ที่กำหนดภายใน 30 ก.ย.56	
การนำแนวทาง	1) ฝบส. กำหนดให้ทุกหน่วยงาน รายงานความเสี่ยงพร้อมทั้ง	

ประเด็นประเมิน	คำอธิบาย	เอกสารอ้างอิง
ไปปฏิบัติ	แผนปรับปรุงความเสี่ยงของแต่ละหน่วยงาน นำเสนอตามลำดับชั้นผ่านระบบบริหารความเสี่ยงและควบคุมภายใน (RMIC) และระบบติดตาม /ประเมินผลโครงการ เป็นประจำปีละ 2 ครั้ง 2) ฝยท. ดำเนินการจัดทำผลสำรวจความพึงพอใจของผู้ใช้บริการระบบสารสนเทศ และสรุปผล วิเคราะห์ (Gap Analysis) ร่วมกับ ฝบส. และสตส. เพื่อนำมาพัฒนาปรับปรุงระบบงานเป็นประจำทุกปี	
การปรับปรุง	1) คณะทำงานพัฒนาระบบงานบริหารความเสี่ยงและควบคุมภายใน มีการทบทวนและปรับปรุงระบบสารสนเทศที่สนับสนุนการบริหารความเสี่ยงและควบคุมภายใน โดยมีการบูรณาการระหว่างระบบ RMIC และระบบติดตามและประเมินผลโครงการตามแนวทาง Service Oriented Architecture (SOA) เพื่อให้สามารถติดตามแผนงานด้านความเสี่ยงได้จากระบบ RMIC แบบครบวงจร เพื่อเชื่อมโยงความเสี่ยงของแต่ละระบบอย่างเหมาะสม และเพิ่มประสิทธิภาพการใช้ระบบเทคโนโลยีสารสนเทศได้อย่างเต็มที่ รวมทั้งส่งผลต่อคุณภาพและความรวดเร็วของข้อมูลที่นำมาใช้ประกอบการตัดสินใจของผู้บริหาร 2) ฝยท. ส่งสรุปผลให้ ฝบส. และ สตส. นำผลสำรวจความพึงพอใจของผู้ใช้บริการ ระบบงานที่เกี่ยวข้อง มาพิจารณา ทบทวนและปรับปรุงให้ระบบสามารถสนับสนุนการทำงานได้ทันต่อความต้องการ ซึ่งอาจมีการทบทวนปรับปรุงกระบวนงานได้ทุกปี	
การบูรณาการ	กปน. มีการจัดทำระบบสารสนเทศสนับสนุนการบริหารความเสี่ยง และการเตือนภัย/แจ้งให้รู้ล่วงหน้า (Early Warning System) สอดคล้องกระบวนการบริหารความเสี่ยงตามมาตรฐาน COSO ขององค์กร และจากข้อกำหนดและกิจกรรมควบคุมของกระบวนการทำงานหลักของหน่วยงานที่ต้องมีการติดตามเฝ้าระวังอย่างใกล้ชิด เพื่อจะได้ปรับเปลี่ยนการปฏิบัติงานได้อย่างเหมาะสมและทันต่อเหตุการณ์ ตลอดจนการบูรณาการระบบสารสนเทศด้านการบริหารความเสี่ยงและควบคุมภายในแบบครบวงจร เพื่อเชื่อมโยงความเสี่ยงของแต่ละระบบอย่างเหมาะสม และเพิ่มประสิทธิภาพการใช้ระบบเทคโนโลยีสารสนเทศ และความพร้อมใช้งานของข้อมูลที่นำมาใช้ประกอบการตัดสินใจของผู้บริหาร	

แบบรายงานผลการดำเนินงาน (Organizational Performance Form)

หมวดที่ 4 การวัด การวิเคราะห์ และการจัดการความรู้

หัวข้อที่	ประเด็นพิจารณา
4.2 ข (3)	**ความพร้อมใช้งานในภาวะฉุกเฉิน** ● รัฐวิสาหกิจดำเนินการอย่างไรเพื่อให้ ในกรณีฉุกเฉิน ระบบฮาร์ดแวร์และซอฟแวร์ รวมทั้งข้อมูลและสารสนเทศมีความพร้อมใช้งานอย่างต่อเนื่อง เพื่อตอบสนองลูกค้าและความต้องการทางธุรกิจอย่างมีประสิทธิผล

ปัจจัยสำคัญที่เกี่ยวข้อง (จากบริบทของรัฐวิสาหกิจ)	
บริบท 1 ก (5) รัฐวิสาหกิจดำเนินการภายใต้สภาพแวดล้อมด้านกฎ ระเบียบข้อบังคับ บริบท 1 ข (2) กลุ่มลูกค้า กลุ่มผู้มีส่วนได้ส่วนเสียและส่วนตลาด	บริบท 1 ข (3) ผู้ส่งมอบ คู่ค้า คู่ความร่วมมือ บริบท 2 ค การปรับปรุงผลการดำเนินการ

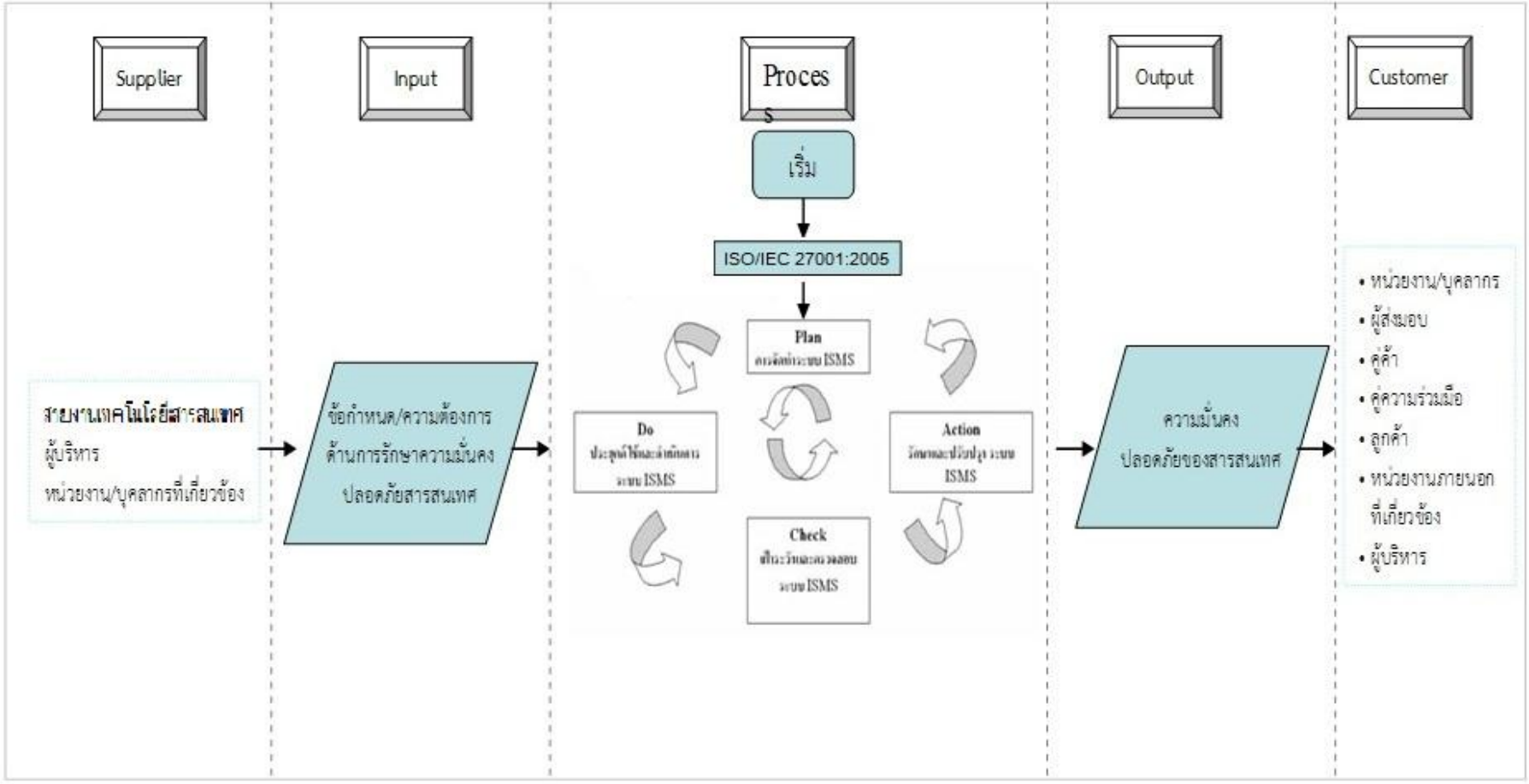
ประเด็นประเมิน	คำอธิบาย	เอกสารอ้างอิง
แนวทาง	**การบริหารความต่อเนื่องในการดำเนินงานขององค์กร (Business continuity management)** กปน. มีการบริหารความต่อเนื่องในการดำเนินงานขององค์กร เพื่อป้องกันการติดขัดหรือการหยุดชะงักของกิจกรรมต่างๆ ทางธุรกิจเพื่อป้องกันกระบวนการทางธุรกิจที่สำคัญอันเป็นผลมาจากการล้มเหลวหรือหายนะที่มีต่อระบบสารสนเทศ และเพื่อให้สามารถกู้ระบบกลับคืนมาได้ภายในระยะเวลาที่เหมาะสม ตามมาตรฐาน ISO/IEC 27001:2005 ภาพที่ 4.2 ข (3) – 1 กระบวนการสร้างความต่อเนื่องในการดำเนินธุรกิจ โดยให้บริการระบบฮาร์ดแวร์ และซอฟแวร์ ดังนี้ 1) การจัดทำแผนงานเพื่อกู้ระบบสารสนเทศ 1.1) ทุกหน่วยงานในองค์กรทำการประเมินความเสี่ยง วิเคราะห์และติดตามความเสี่ยงใหม่ ๆ ที่อาจจะเกิดขึ้น ที่ส่งผลกระทบให้ธุรกิจหยุดชะงักเป็นระยะเวลานาน ซึ่ง กปน. กำหนดระดับผลกระทบความเสี่ยงด้านเทคโนโลยีสารสนเทศ ดังตารางที่ 4.2 ข (3)–1 เพื่อนำไปประเมินร่วมกับโอกาสเกิดของเหตุการณ์ต่าง ๆ และจัดทำแผนบริหารความเสี่ยงต่อไป 1.2) คณะกรรมการด้านการรักษาความมั่นคงปลอดภัย	ภาพที่ 4.2 ข (3) – 1

ประเด็นประเมิน	คำอธิบาย	เอกสารอ้างอิง
	กำหนดกลยุทธ์ในการกู้ระบบสารสนเทศ กำหนดให้ทุกฐานข้อมูลที่สำคัญให้ทำการสำรองข้อมูลไว้นอกสถานที่ และจัดทำระบบสำรองข้อมูลระบบงานหลักจากสำนักงานใหญ่ไปยังศูนย์คอมพิวเตอร์สำรอง เป็นการสำรองข้อมูล และโปรแกรมแบบ Hardware Synchronize ซึ่งมีความต่างของข้อมูลไม่เกิน 1 นาที และโปรแกรม Synchronize มีความต่างของข้อมูลไม่เกิน 10 นาที และสำรองข้อมูล และโปรแกรมจัดเก็บนอกศูนย์คอมพิวเตอร์หลัก – สำรอง ศูนย์คอมพิวเตอร์อื่นๆ เช่น ศูนย์ 1125 สำรองข้อมูลไว้ที่ศูนย์คอมพิวเตอร์หลักทุกวัน โดยมีกระบวนการปฏิบัติงานและการจัดลำดับความสำคัญ ดังนี้ ตารางกระบวนการปฏิบัติงาน กระบวนการปฏิบัติงานทั้งหมดของฝ่ายงาน / กระบวนการหลัก (Yes/ No) ระบบข้อมูลลูกค้า (CIS) / Yes ระบบ SAP / Yes ระบบสารบรรณอิเล็กทรอนิกส์ / Yes ตารางแสดงเวลาที่คาดหมายในการกอบกู้และลำดับความสำคัญในการกอบกู้ ดังต่อไปนี้ ลำดับ / ธุรกรรมที่สำคัญของฝ่ายงาน (Critical Business Functions) / RPO / RTO / ลำดับความสำคัญในการกอบกู้ 1 / ระบบข้อมูลลูกค้า (CIS) / 4 Hrs / 4 Hrs / 1 2 / ระบบ SAP / 4 Hrs / 4 Hrs / 2 3 / ระบบสารบรรณอิเล็กทรอนิกส์ / 4 Hrs / 4 Hrs / 3 หมายเหตุ: ธุรกรรมที่สำคัญ (Critical Business Functions) หมายถึง ธุรกรรมซึ่งหากมีการหยุดชะงัก อาจส่งผลกระทบต่อการดำเนินงาน ธุรกิจ ชื่อเสียง ฐานะ และผลการดำเนินงานของการประปานครหลวง อย่างมีนัยสำคัญ 1.3) ฝยส. จัดเตรียมศูนย์คอมพิวเตอร์สำรอง ตั้งศูนย์คอมพิวเตอร์สำรองแบบ Hot Site ที่ได้รับการดูแลตามมาตรฐาน ISO 27001 เป็นอาคารแยกต่างหาก ติดตั้งอุปกรณ์ด้านคอมพิวเตอร์เพื่อรองรับการให้บริการในภาวะฉุกเฉิน และคู่มือการปฏิบัติงานในภาวะวิกฤติ ทั้งนี้ได้ใช้กรอบมาตรฐาน ISO 27001 เป็นแนวทางปฏิบัติ และมีการบำรุงรักษาอุปกรณ์ Hardware ทั้งแบบ Preventive และ Collective Maintenance 2) คณะทำงานบริหารความเสี่ยงและควบคุมภายในประจำสายงานเทคโนโลยีสารสนเทศ จัดทำแผน Business Continuity Process (BCP) โดยกำหนดรายชื่อผู้ที่มีหน้าที่รับผิดชอบ ขอบเขตงานของแต่	-คู่มือการปฏิบัติงานในภาวะวิกฤติ

ประเด็นประเมิน	คำอธิบาย	เอกสารอ้างอิง
	ละหน่วยงานในโครงสร้าง และกำหนดขั้นตอนการดำเนินงาน เทคนิควิธีการที่นำมาใช้ และการประสานงานกับเจ้าหน้าที่ทั้งภายในองค์กรและผู้ค้าที่จะให้คำปรึกษาในการกอบกู้คืนระบบสารสนเทศได้รวดเร็วที่สุด 2.1) การฝึกอบรมและทดสอบแผนการกู้ระบบอย่างสม่ำเสมอ โดยซักซ้อมการกู้ระบบที่สำคัญ SAP และ CIS ทุกปี และระบบอื่นตามระดับความเสี่ยง เช่น ระบบสารบรรณอิเล็กทรอนิกส์ เอกสารอิเล็กทรอนิกส์ ระบบCall Center และ CRM เป็นต้น ซึ่งรวมถึงการทดสอบระบบเครือข่ายสื่อสาร ระบบ server และบุคลากรที่เกี่ยวข้องทั้งหมด ให้สามารถกู้ระบบงานได้ภายในระยะเวลาที่องค์กรยอมรับ (4 ชั่วโมง) 2.2) คณะทำงานบริหารความเสี่ยงและควบคุมภายในประจำสายงานเทคโนโลยีสารสนเทศ ติดตามประเมินผลการดำเนินงานและมีข้อเสนอแนะ ให้หน่วยงานที่เกี่ยวข้องจัดทำแผนการปรับปรุงการปฏิบัติงานให้ทันสมัยและสอดคล้องกับระบบคอมพิวเตอร์ **ระบบ Offline/Manual** กปน. มีระบบรองรับในกรณีฉุกเฉินนอกเหนือจากการใช้ระบบงานที่ ศูนย์คอมพิวเตอร์สำรอง ได้แก่ ระบบการทำงานแบบ Offline หรือการทำงานแบบ Manual เช่น ระบบข้อมูลผู้ใช้น้ำ ซึ่งมีการซ้อมการทำงานเป็นประจำทุกปี **<u>ตัวชี้วัด</u>** 1) ความปลอดภัยและความพร้อมใช้งาน ของข้อมูลสารสนเทศ ปีงบประมาณ 2556 จัดทำรายงานแนวทางการออกแบบศูนย์คอมพิวเตอร์ทางเลือก 2) การควบคุมการปฏิบัติงานภายใต้กรอบความมั่นคงปลอดภัยสารสนเทศตามมาตรฐานสากล ISO/IEC 27001:2005 กำหนดให้เครื่องแม่ข่ายสามารถให้บริการระบบ CIS และ SAP ได้รับการดูแลตามมาตรฐาน ISO/IEC 27001:2005 โดยมีระยะเวลาหยุดให้บริการ (Downtime) ไม่เกิน 3% (262 ชั่วโมง) 3) แผนทบทวนการบริหารความต่อเนื่องทางธุรกิจ (BCP) ด้าน IT ปีงบประมาณ 2556 จัดทำแผน BCP ด้านเทคโนโลยีสารสนเทศ ตามมาตรฐาน ISO/IEC 27001:2005 ที่ผ่านการทบทวน และมีการซักซ้อมแผนตามกำหนด	
การนำแนวทางไปปฏิบัติ	กปน. มีการการฝึกซ้อมแผนบริหารความต่อเนื่องทางธุรกิจ (BCP) ด้าน IT 2 ครั้งต่อปี (กลางปีและปลายปี) โดยสายงานเทคโนโลยีสารสนเทศและฝ่ายบริหารความเสี่ยง ร่วมกับหน่วยงานที่	

ประเด็นประเมิน	คำอธิบาย	เอกสารอ้างอิง
	เกี่ยวข้อง เช่นฝ่ายสื่อสารองค์กร กองอาคารและสถานที่ ฝ่ายตรวจสอบภายในและหน่วยงานที่ร่วมทดสอบในการปฏิบัติการ โดยจะมีการแจ้งและประชาสัมพันธ์ให้ทุกหน่วยงานระดับฝ่ายขึ้นไป ได้ทราบการฝึกซ้อมแผนบริหารความต่อเนื่องทางธุรกิจ (BCP) เพื่อทราบแนวทางการฝึกซ้อมและร่วมให้ความคิดเห็นหลังจากการทดสอบเสร็จสิ้นแล้ว คณะกรรมการความมั่นคงปลอดภัยสารสนเทศ พิจารณาทบทวนแผนการบริหารความต่อเนื่องทางธุรกิจ (BCP) ด้าน IT ให้ครอบคลุมกับอุปกรณ์และระบบงานที่เพิ่มขึ้นเป็นประจำทุกปี	
การปรับปรุง	ฝยส. และ ฝพท. นำผลที่ได้จากการฝึกซ้อมแผนบริหารความต่อเนื่องทางธุรกิจ (BCP) ด้าน IT จัดทำรายงานเพื่อแจกแจงวิเคราะห์ผลลัพธ์ที่ได้และจุดบกพร่องต่าง ๆ เพื่อเป็นแนวทางในการพัฒนา ปรับปรุง ทบทวน แผนบริหารความต่อเนื่องทางธุรกิจ (BCP) ด้าน IT ในครั้งต่อไปอย่างต่อเนื่อง ในปี 2556 จัดทำแผน BCP ของระบบสารบรรณอิเล็กทรอนิกส์ และแนวทางปรับปรุง	
การบูรณาการ	สายงานเทคโนโลยีสารสนเทศตระหนักถึงการทำให้ข้อมูลและสารสนเทศมีความพร้อมใช้งานอย่างต่อเนื่องในกรณีเกิดเหตุฉุกเฉิน มีแนวทางการดำเนินงานที่สอดคล้องกันทั้งองค์กร ตามแผนดำเนินงานที่ได้มีการจัดเตรียมไว้แล้ว โดยที่แผนนั้นมีการทบทวนและมีการซักซ้อมแผนเป็นประจำอย่างต่อเนื่อง ดังนั้นการดำเนินการเพื่อสร้างความมั่นคงของระบบสารสนเทศ ให้สามารถใช้งานต่อเนื่องในการให้บริการลูกค้า ผู้มีส่วนได้เสีย ประชาชน และพนักงานสามารถปฏิบัติงานทุกกระบวนงานขององค์กร ได้อย่างมั่นใจ ถูกต้อง และมีประสิทธิภาพ เพื่อให้ได้ผลลัพธ์ตามยุทธศาสตร์การบริหาร กปน. ที่ได้ระบุไว้	

ภาพที่ 4.2 ข (3) – 1 มาตรฐาน ISO/IEC 27001:2005



ผลกระทบ	ระดับ 1 ต่ำมาก	ระดับ 2 ต่ำ	ระดับ 3 ปานกลาง	ระดับ 4 สูง	ระดับ 5 สูงมาก
ระยะเวลาที่ระบบงาน IT หยุดชะงัก	ระบบงาน IT มีปัญหาที่ไม่สำคัญ มีการหยุดชะงักน้อยกว่าครึ่ง ชม. โดยไม่ต้องพึ่งระบบสำรอง	ระบบงาน IT มีปัญหาเล็กน้อย ทำให้การหยุดชะงัก ครึ่ง ชม. ถึง 4 ชม. โดยสามารถใช้ระบบสำรองได้	ระบบงาน IT มีปัญหา/เสียหาย ทำให้ต้องหยุดชะงักมากกว่า 4 ถึง 8 ชม. โดยสามารถใช้ระบบสำรองได้ เริ่มหาวิธีการจัดการในการติดต่อกับผู้ให้บริการ	ระบบงาน IT มีปัญหา/เสียหายมาก ทำให้ต้องหยุดชะงักมากกว่า 8 ชม. โดยต้องไปใช้ศูนย์คอมพิวเตอร์สำรอง	ระบบงาน IT มีปัญหา/เสียหายอย่างรุนแรง โดยไม่สามารถใช้ศูนย์คอมพิวเตอร์สำรองได้

ตารางที่ 4.2 ข(3)-1 ระดับผลกระทบความเสี่ยงด้านเทคโนโลยีสารสนเทศ