EGA
e-Government Agency

สถาปัตยกรรมองค์กรของอีจีเอ
EGA Enterprise Architecture

(เอกสารเผยแพร่)
สถาปัตยกรรมองค์กรของ
สำนักงานรัฐบาลอิเล็กทรอนิกส์ (องค์การมหาชน)

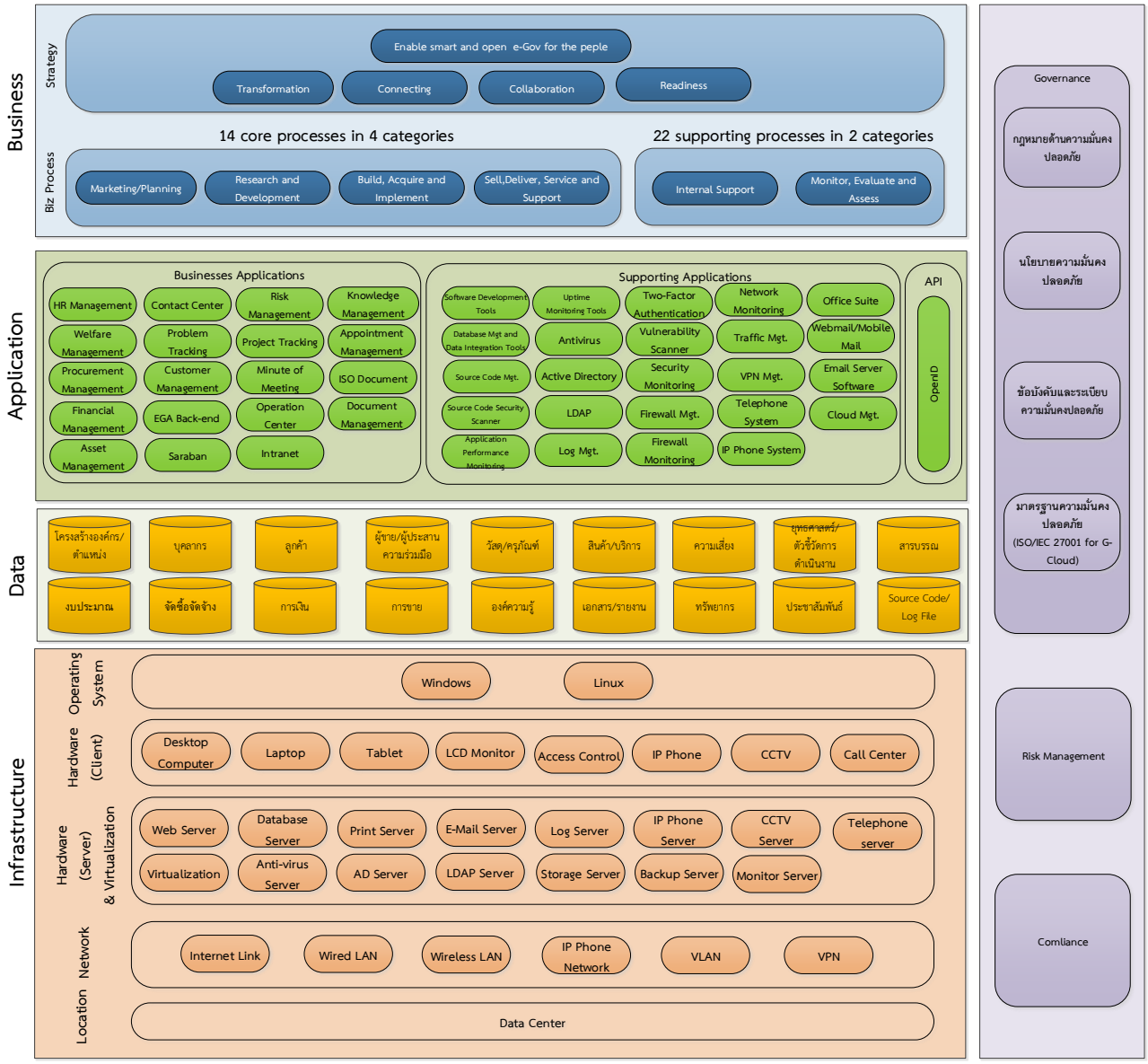
สารบัญ

สารบัญตาราง

สารบัญภาพ

บทสรุปผู้บริหาร (Executive Summary)

สถาปัตยกรรมองค์กรของสำนักงานรัฐบาลอิเล็กทรอนิกส์ (องค์การมหาชน) (สรอ.) ได้ถูกจัดทำขึ้น เพื่อใช้เป็นแนวทางการดำเนินงานที่เหมาะสมด้านการจัดการระบบสารสนเทศของสำนักงาน และสอดรับกับตัวชี้วัดการพัฒนาสถาปัตยกรรมองค์กรตามแผนกลยุทธ์ ประจำปีงบประมาณ ๒๕๕๘ ภายใต้ยุทธศาสตร์ที่ ๓ การขับเคลื่อนรัฐบาลอิเล็กทรอนิกส์อย่างมีส่วนร่วมด้วยนวัตกรรมบริการรูปแบบใหม่ ตามแผนยุทธศาสตร์ ๔ ปี สรอ. (พ.ศ. ๒๕๕๗–๒๕๖๐) และเป็นหนึ่งในตัวชี้วัดการดำเนินงานตัวชี้วัดที่ ๔.๔ ในมิติที่ ๔ มิติด้านการกำกับดูแลกิจการและการพัฒนาองค์การ ของ ก.พ.ร. ด้วย จากการดำเนินการสำรวจและวิเคราะห์สถานะสถาปัตยกรรมองค์กร พบว่าสถานะปัจจุบันของสถาปัตยกรรมองค์กร สรอ. (Current State View of EGA Enterprise Architecture) เป็นไปตามรูปที่ ๑



รูปที่ ๑ ภาพสถานะปัจจุบันของสถาปัตยกรรมองค์กร สรอ.

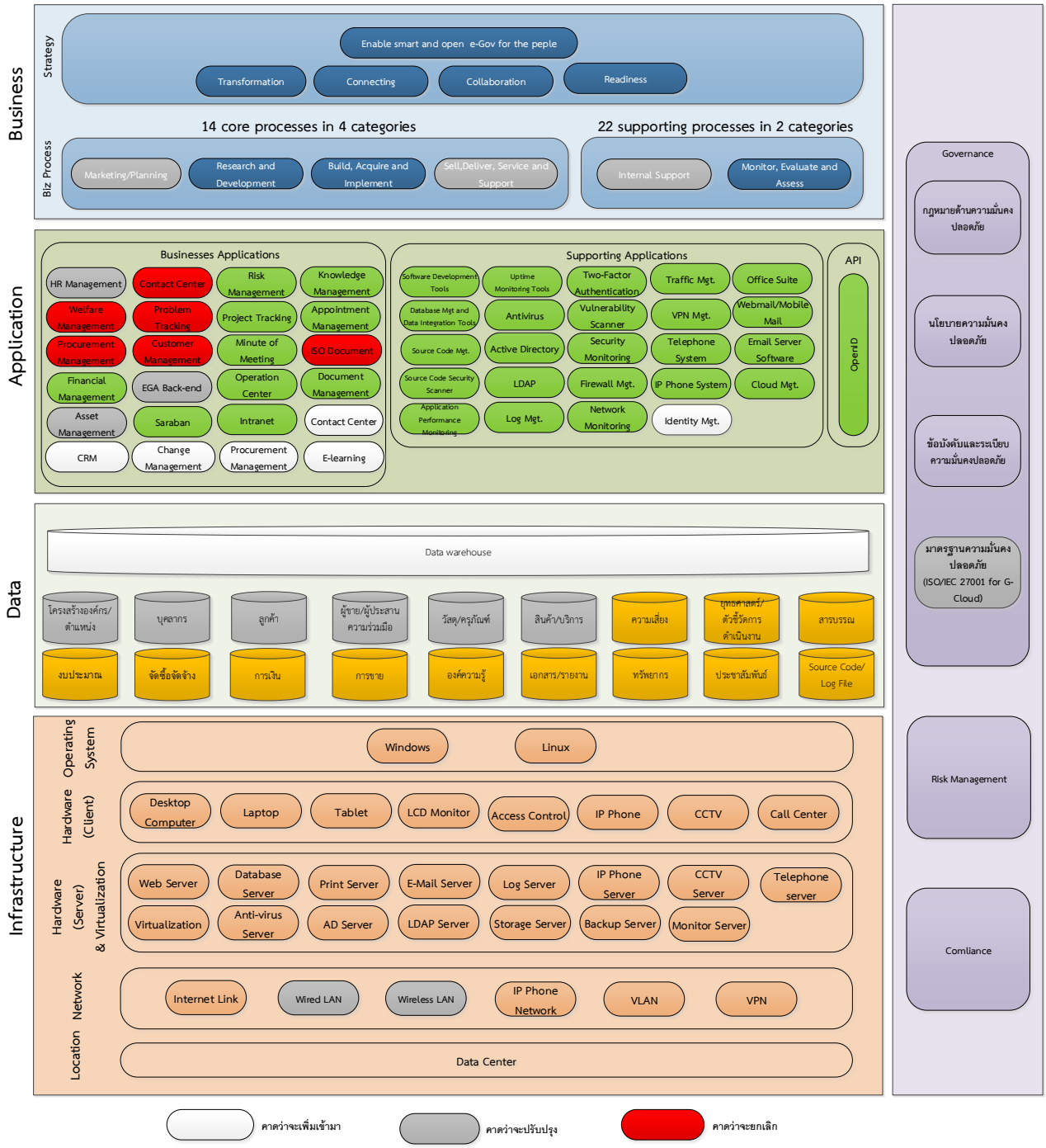
จากผลการสำรวจพบประเด็นปัญหาที่มีอยู่ในปัจจุบัน ตามรายการต่อไปนี้

๑) ขั้นตอนในการปฏิบัติงานหลายขั้นตอน
๒) การปฏิบัติงานใช้กระดาษเป็นจำนวนมาก
๓) แอปพลิเคชันยังไม่ครอบคลุมถึงกระบวนการปฏิบัติงานที่สำคัญ
๔) ข้อมูลมีการจัดเก็บซ้ำซ้อน
๕) ขาดผู้รับผิดชอบข้อมูลสำหรับข้อมูลที่ใช้งานร่วมกัน เป็นต้น

สำหรับการออกแบบสถาปัตยกรรมองค์กรในอนาคต ของ สรอ. ประกอบขึ้นจากข้อเสนอแนะจากผลการวิเคราะห์สถานะปัจจุบัน และแนวทางการพัฒนาสถาปัตยกรรมในอนาคต (Architecture Principle) ดังต่อไปนี้

๑) มุ่งเน้นไปสู่การเป็นองค์กรที่ใช้ข้อมูล เพื่อการตัดสินใจในการทำงาน (Data-driven Organization) และลดการใช้กระดาษให้มากที่สุด
๒) กำหนดกระบวนการปฏิบัติงานและการบริหารจัดการที่มีมาตรฐาน และรองรับการเปลี่ยนแปลงได้อย่างมีประสิทธิภาพ
๓) ดำเนินการบริหารจัดการข้อมูลให้อยู่ในรูปแบบ Single Source โดยมีการกำหนด Data Operation และ Data Governance ที่เหมาะสม
๔) กำหนดกรอบการพัฒนาแอปพลิเคชันที่เน้นการเชื่อมโยงระบบผ่าน API เพื่อแลกเปลี่ยนข้อมูล รวมถึงการเปิดข้อมูลให้กับ Stakeholder ผ่าน Public API
๕) สร้างความตระหนักด้านมั่นคงปลอดภัยสำหรับการพัฒนาสถาปัตยกรรมองค์ทั้งทางด้านธุรกิจ ด้านแอปพลิเคชัน ด้านข้อมูล และด้านโครงสร้างพื้นฐาน
๖) พัฒนาโครงสร้างพื้นฐานสารสนเทศโดยใช้ Cloud Computing เป็นหลัก และเน้นการใช้ทรัพยากรร่วมกัน

ซึ่งผลของการออกแบบเพื่อให้เกิดความพร้อม ตอบสนองการใช้งานและทำให้เกิดความสะดวก รวดเร็ว รองรับการให้บริการแก่ประชาชนหรือหน่วยงานภายนอกได้ สามารถแสดงออกมาเป็นสถานะอนาคตของสถาปัตยกรรมองค์กร สรอ. (Future State View of EGA Enterprise Architecture) ดังรูปที่ ๒



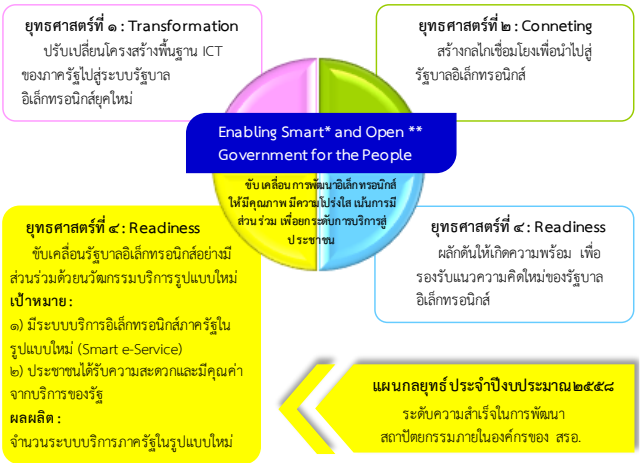
รูปที่ ๒ ภาพสถานะอนาคตของสถาปัตยกรรมองค์กร สรอ.

บทที่ ๑ บทนำ

๑.๑ ความเป็นมา

ตามกรอบแนวทางการดำเนินงานของสรอ. ที่มุ่งเน้นการพัฒนาและให้บริการระบบรัฐบาลอิเล็กทรอนิกส์ (e-Government) ของภาครัฐ ส่งเสริมการพัฒนาด้านโครงสร้างพื้นฐาน ด้านการวิจัยพัฒนาและจัดทำมาตรฐานแนวปฏิบัติที่เป็นประโยชน์ต่อการพัฒนาและขับเคลื่อนรัฐบาลอิเล็กทรอนิกส์ของประเทศและการให้คำปรึกษาและถ่ายทอดองค์ความรู้ต่างๆ ที่เกี่ยวข้องกับภารกิจและบริการ ตลอดจนเร่งผลักดันให้เกิดนโยบายสำคัญต่างๆ ที่ช่วยขับเคลื่อนการพัฒนาด้านรัฐบาลอิเล็กทรอนิกส์ให้มีความก้าวหน้าสอดคล้องกับยุทธศาสตร์การพัฒนาด้านเทคโนโลยีสารสนเทศของประเทศอย่างเป็นรูปธรรม ซึ่งมุ่งปรับเปลี่ยนประเทศไทยไปสู่การบริหารจัดการที่ทันสมัย การเพิ่มความสามารถในการแข่งขันของประเทศและการสร้างความเท่าเทียมกันในการได้รับบริการของภาครัฐ โดยใช้ ICT หรือสื่ออิเล็กทรอนิกส์เป็นเครื่องมือสำคัญ มีความมุ่งมั่นและเตรียมพร้อมในการทำงานเพื่อยกระดับการบริการด้านรัฐบาลอิเล็กทรอนิกส์ของภาครัฐในเชิงรุกด้วย นอกจากสำนักงานจะให้ความสำคัญกับการพัฒนาในด้านต่างๆของประเทศแล้ว ยังมุ่งเน้นการพัฒนา Smart e-Service ภายในองค์กรด้วยการผลักดันให้เกิดการบูรณาด้านเทคโนโลยีสารสนเทศและกระบวนดำเนินงานเพื่อสร้างความเชื่อมโยงกระบวนการทางธุรกิจ ลดความซ้ำซ้อนด้านเทคโนโลยีสารสนเทศและสนับสนุนการดำเนินงานต่างๆ ภายในองค์กร ให้เกิดความสะดวก รวดเร็ว ทันสมัย ทันเวลา รองรับการให้บริการแก่ประชาชนหรือหน่วยงานภายนอกได้

ในการนี้ คณะกรรมการบริหารสำนักงาน จึงให้ความสำคัญกับการพัฒนารัฐบาลอิเล็กทรอนิกส์ในรูปแบบการบูรณาการภายใน โดยเห็นชอบให้สำนักงานดำเนินการศึกษาและจัดทำแนวทางการพัฒนาสถาปัตยกรรมองค์กร (Enterprise Architecture) ภายในสำนักงานขึ้นในปี ๒๕๕๘ เพื่อยกระดับการดำเนินงานภายในให้มีประสิทธิภาพประสิทธิผลมากยิ่งขึ้น ซึ่งการดำเนินการนี้จะสอดคล้องกับตัวชี้วัดตามคำรับรองการปฏิบัติงานของสรอ. คณะกรรมการพัฒนาระบบราชการ (ก.พ.ร.) ที่ได้มีการกำหนดตัวชี้วัดการพัฒนาประสิทธิภาพสารสนเทศภาครัฐ ให้กับส่วนราชการระดับกรมจำนวน ๑๔๖ ส่วนราชการ เพื่อสำรวจสถานะภาพปัจจุบันของการพัฒนารัฐบาลอิเล็กทรอนิกส์และเตรียมความพร้อมในการพัฒนาไปด้วยกัน อันจะนำไปสู่การเป็น “Single Government” ต่อไป โดยสำนักงานได้กำหนดเป็นแผนกลยุทธ์ ประจำปี ๒๕๕๘ ตัวชี้วัด ระดับความสำเร็จในการพัฒนาสถาปัตยกรรมองค์กร และสอดคล้องกับยุทธศาสตร์ ๔ ปี ในยุทธศาสตร์ที่ ๓ : Collaboration ด้วยดัง รูปที่ ๓



รูปที่ ๓ ภาพความสัมพันธ์ของยุทธศาสตร์ กลยุทธ์ศาสตร์ขององค์กร กับการพัฒนา EA

๑.๒ วัตถุประสงค์

วัตถุประสงค์ของการพัฒนาสถาปัตยกรรมองค์กรของ สรอ. มีรายละเอียดดังต่อไปนี้

๑) เพื่อสร้างความเข้าใจและความสัมพันธ์ที่ชัดเจนต่อสถานะปัจจุบันสถาปัตยกรรมองค์กร (Current State of Enterprise Architecture) ทั้ง ๕ ด้าน ประกอบไปด้วย ด้านธุรกิจ (Business) ด้านแอปพลิเคชัน (Application) ด้านข้อมูล (Data) ด้านโครงสร้างพื้นฐาน (Infrastructure) และด้านความมั่นคงปลอดภัย (Security)

๒) เพื่อกำหนดกรอบของสถานะอนาคตของสถาปัตยกรรมองค์กร (Future State of Enterprise Architecture) ทั้ง ๕ ด้าน เพื่อนำมาปรับปรุงประสิทธิภาพและให้เป็นไปตามเป้าหมายของสรอ.

๓) เพื่อวิเคราะห์ถึงความแตกต่างระหว่างสถานะปัจจุบันและอนาคตของสถาปัตยกรรมองค์กร (Gap Analysis)

๔) เพื่อกำหนดแผนการดำเนินงาน (Roadmap) ที่ส่งผลต่อการบรรลุถึงสถานะอนาคตของสถาปัตยกรรมองค์กร (Future State of Enterprise Architecture)

๑.๓ ขอบเขตการดำเนินงาน

จากกรอบสถาปัตยกรรมองค์กรของ สรอ. (ตามที่แสดงในรูปที่ ๘) คือ ***"๓ มุมมอง (Viewpoints) ๔ กระบวนการพัฒนา (Development Processes) และ ๕ ด้าน (Sub Architecutres/Models)"*** ซึ่งประกอบไปด้วย ๓ มุมมอง (Viewpoints) อันได้แก่ ๑) มุมมองผู้บริหาร หมายถึง มุมมองของ คณะกรรมการบริหาร ผู้อำนวยการสำนักงาน ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง และรองผู้อำนวยการสำนักงาน ผู้อำนวยการฝ่ายและผู้จัดการส่วน ๒) มุมมองผู้ใช้งาน และ ๓) มุมมองเชิงพัฒนา หมายถึง มุมมองของเจ้าหน้าที่บริหารจัดการทางธุรกิจ และเจ้าหน้าที่ด้านเทคโนโลยีสารสนเทศ โดยมี ๔ กระบวนการพัฒนาสถาปัตยกรรมองค์กร ได้แก่ กระบวนการขั้นต้น (Initial) กระบวนการการออกแบบ (Design) กระบวนการการปรับเปลี่ยน (Transition) และกระบวนการการวัดผลประสิทธิภาพองค์กร (Measurement) และการศึกษาสถาปัตยกรรมองค์กรโดยแบ่งเป็น ๕ ด้าน ได้แก่ ด้านธุรกิจ (Business) ด้านแอปพลิเคชัน (Application) ด้านข้อมูล (Data) ด้านโครงสร้างพื้นฐาน (Infrastructure) และด้านความมั่นคงปลอดภัย (Security)

ในปี ๒๕๕๘ นี้สำนักงานได้กำหนดขอบเขตการดำเนินการพัฒนาสถาปัตยกรรมองค์กรให้ครอบคลุมมุมมองทั้ง ๓ มุมมองและสถาปัตยกรรมองค์กรทั้ง ๕ ด้าน สำหรับกระบวนการพัฒนาจะครอบคุม ๒ กระบวน ประกอบไปด้วย ขั้นต้น (Initial) และขั้นการออกแบบ (Design)

๑.๔ ขั้นตอนการดำเนินงาน

ขั้นตอนการดำเนินงานเพื่อพัฒนาสถาปัตยกรรมองค์กรของ สรอ. ในปี ๒๕๕๘ สอดคล้องกับกรอบของสถาปัตกรรมองค์กรและขอบเขตของการดำเนินงาน ดังแสดงในรูปที่ ๔ และให้รายละเอียดดังต่อไปนี้

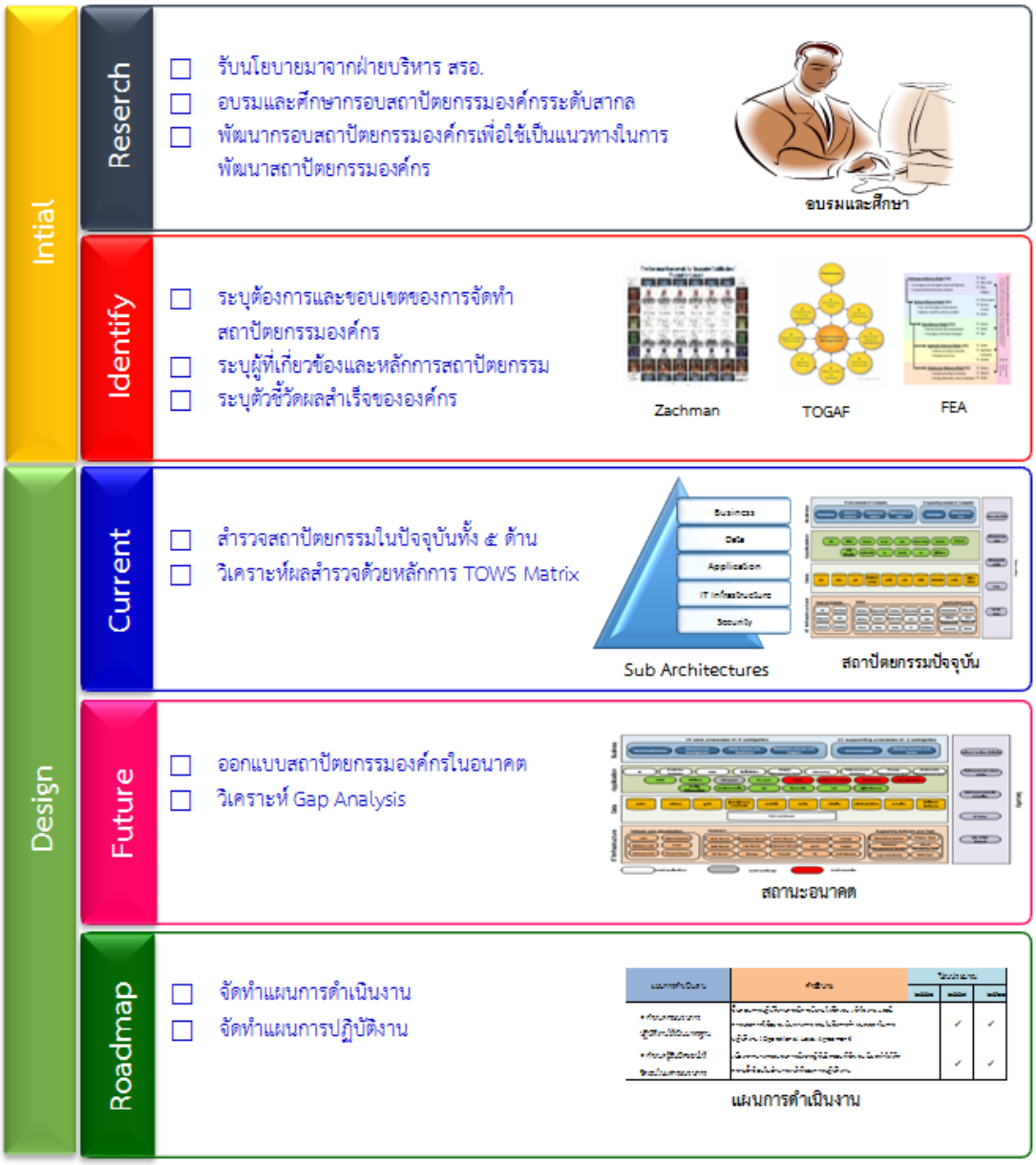
(๑) ขั้นต้น (Initial)

- การศึกษา (Research) : รับนโยบายมาจากฝ่ายบริหาร อบรมและศึกษากรอบสถาปัตยกรรมองค์กรระดับสากล ศึกษาตัวอย่างสถาปัตยกรรมองค์การจากองค์กรอื่นๆ พัฒนากรอบสถาปัตยกรรมองค์กรเพื่อใช้เป็นแนวทางในการพัฒนาสถาปัตยกรรมองค์กร

- การระบุ (Indentify) : กำหนดความต้องการและขอบเขตของการจัดทำสถาปัตยกรรมองค์กร (Requirement and Scope) ผู้ที่เกี่ยวข้อง (Stakeholders) หลักการสถาปัตยกรรม (Architecture Principle) ซึ่งจะให้โครงร่างของสถาปัตยกรรมองค์กรในอนาคต (Future State Outline) และตัวชี้วัดผลสำเร็จขององค์กร (Key Performance Indicator)

(๒) ขั้นการออกแบบ (Design)

- สถาปัตยกรรมปัจุบัน (Current Architecure) : สำรวจและวิเคราะห์สถานะปัจจุบันของสถาปัตยกรรม (Current State of Enterprise Architecture) ซึ่งครอบคุลมทั้ง ๕ ด้าน ดังนี้ ด้านธุรกิจ (Business) ด้านแอปพลิเคชัน (Application) ด้านข้อมูล (Data) ด้านโครงสร้างพื้นฐาน (Infrastructure) และด้านความมั่นคงปลอดภัย (Security) รวมทั้งสำรวจประเด็นปัญหา ให้ข้อเสนอแนะพร้อมทั้งความต้องการในอนาคต
- สถาปัตยกรรมอนาคต (Future Architecure) : ออกแบบและแสดงให้เห็นถึงสถานะอนาคตของสถาปัตยกรรมองค์กร (Future State of Enterprise Architecture) ทั้ง ๕ ด้าน และวิเคราะห์ความแตกต่างของทั้งสองสถานะ (Gap Analysis)
- แผนการดำเนินงาน (Roadmap) : กำหนดแผนการดำเนินงานเพื่อใช้สำหรับปรับเปลี่ยนสถาปัตยกรรมองค์กรจากปัจจุบันไปยังอนาคตตามที่ได้ออกแบบไว้



รูปที่ ๔ ภาพขั้นตอนการดำเนินงาน

๑.๕ องค์ประกอบของการพัฒนาสถาปัตยกรรมองค์กร

องค์ประกอบของการพัฒนาสถาปัตยกรรมองค์กร แบ่งเนื้อหาออกเป็น ๕ บท โดยมีเนื้อหาสาระสำคัญดังต่อไปนี้

บทที่ ๑ บทนำ เป็นการกล่าวถึงความเป็นมา วัตถุประสงค์ ขอบเขตการดำเนินงาน และขั้นตอนการพัฒนาสถาปัตยกรรมองค์กรของ สรอ. ซึ่งการพัฒนาสถาปัตยกรรมองค์กรนี้ต้องมีความสอดคล้องกับนโยบาย วิสัยทัศน์ ยุทธศาสตร์ พันธกิจ แผนการดำเนินงานต่างๆ ของสำนักงาน

บทที่ ๒ ที่มาและกรอบสถาปัตยกรรมองค์กรของ สรอ. เกือบ ๓๐ ปีที่ผ่านมา ในระดับสากลมีการนำเสนอกรอบแนวคิดและหลักการในการพัฒนาสถาปัตยกรรมองค์กรที่หลากหลาย ซึ่งแต่ละแนวคิดมีจุดเด่นที่แตกต่างกันไป ดังนั้นในการจัดทำกรอบและหลักการพัฒนาสถาปัตยกรรมองค์กรของ สรอ. จึงได้นำเอาจุดเด่นของแต่ละแนวคิดมาประยุกต์ใช้ให้เหมาะสมกับสำนักงาน โดยประกอบไปด้วย ๓ แนวคิดหลักๆ อันได้แก่ The Zachman Framework, The Open Group Architecture Framework (TOGAF) และ Federal Enterprise Architecture (FEA)

บทที่ ๓ การวิเคราะห์สถานะปัจจุบันของสถาปัตยกรรมองค์กร สรอ. ในบทนี้จะกล่าวถึงผลการสำรวจและศึกษาข้อมูลทั้งในด้านธุรกิจ เทคโนโลยีสารสนเทศ และความมั่นคงปลอดภัย ซึ่งครอบคลุมนโยบาย/วิสัยทัศน์ พันธกิจ แผนยุทธศาสตร์ ๔ ปี สรอ. (พ.ศ. ๒๕๕๗ – ๒๕๖๐) แผนกลยุทธ์ ประจำปีงบประมาณ ๒๕๕๘ แผนแม่บทเทคโนโลยีสารสนเทศและการสื่อสาร ระยะ ๓ ปี (พ.ศ.๒๕๕๘ – ๒๕๖๐) แผนบริหารจัดการระบบสารสนเทศ สรอ. ประจำปี พ.ศ.๒๕๕๘ โครงการจัดทำกระบวนการดำเนินงาน Business Process Improvement (BPI) และนโยบายความมั่นคงปลอดภัยสารสนเทศ จากผลการสำรวจและการศึกษาข้อมูลได้ทำการวิเคราะห์ออกเป็น ๕ ด้านอันได้แก่ ด้านธุรกิจ (Business) ด้านแอปพลิเคชัน (Application) ด้านข้อมูล (Data) ด้านโครงสร้างพื้นฐาน (Infrastructure) และด้านความมั่นคงปลอดภัย(Security) ทั้งนี้ได้รายงานถึงประเด็นปัญหาที่เกิดขึ้นและให้ข้อเสนอแนะสำหรับการออกแบบสถาปัตยกรรมองค์กรในอนาคต

บทที่ ๔ การออกแบบสถาปัตยกรรมองค์กรในอนาคตของ สรอ. ในบทนี้จะพูดถึงการออกแบบสถาปัตยกรรมองค์กรในอนาคต โดยได้นำเอาข้อเสนอแนะจากผลการวิเคราะห์สถานะปัจจุบัน และแนวทางการพัฒนาสถาปัตยกรรมในอนาคต (Architecture Principle) มาใช้สำหรับการออกแบบสถาปัตยกรรมองค์กร

บทที่ ๕ แผนการดำเนินงาน (Roadmap) เป็นการกำหนดกรอบและแนวทางการนำเอาระบบเทคโนโลยีสารสนเทศมาช่วยสนับสนุนและสร้างความเชื่อมโยงกับกระบวนการการดำเนินงานขององค์กร เพื่อช่วยลดประเด็นปัญหาและช่วยยกระดับศักยภาพของระบบเทคโนโลยีสารสนเทศองค์กรให้ตอบสนองกับกระบวนการการปฏิบัติงานภายในสำนักงาน

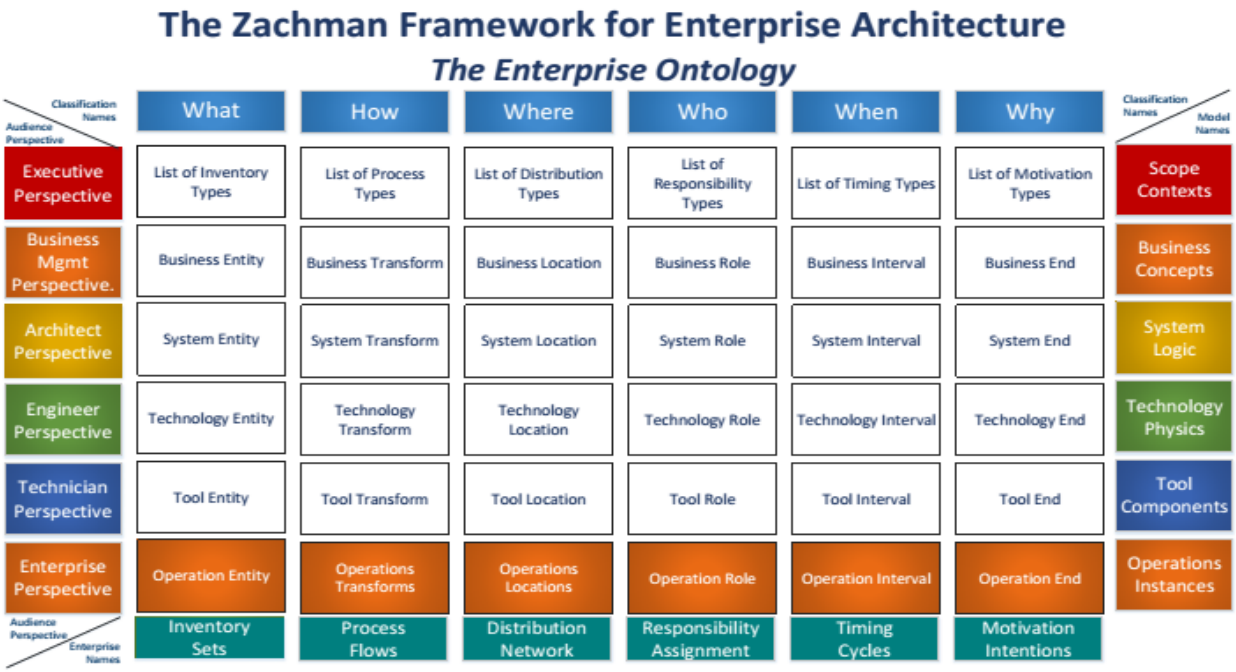
บทที่ ๒ ที่มาและกรอบสถาปัตยกรรมองค์กรของ สรอ.

๒.๑ ที่มากรอบสถาปัตยกรรมองค์กร

สถาปัตยกรรมองค์กร (Enterprise Architecture) คือ กระบวนในการนำเอาเทคโนสารสนเทศ (Information Technology: IT) มาสนับสนุนการดำเนินงานธุรกิจ (Business) ให้เกิดประสิทธิภาพและประสิทธิผลสูงสุดต่อองค์กร แม้ว่าสถาปัตยกรรมองค์กรจะเน้นในเรื่องความสอดคล้องกันของการดำเนินงานด้านธุรกิจและเทคโนโลยีสารสนเทศ อย่างไรก็ตามด้านความมั่นคงปลอดภัยก็ถือเป็นอีกหนึ่งองค์ประกอบที่ขาดไม่ได้ ซึ่งจะช่วยให้ทั้งการดำเนินงานธุรกิจและการบริหารจัดการเทคโนโลยีสารสนเทศเป็นไปด้วยความถูกต้อง ครอบถ้วน โปร่งใส และตรวจสอบได้ เป็นเวลาเกือบ ๓๐ ปีที่ผ่านมาที่นักวิจัยและนักปฏิบัติเริ่มมีการศึกษาถึงการพัฒนาสถาปัตยกรรมองค์กร จากอดีตจนถึงปัจจุบันกรอบแนวความคิดและหลักการในการพัฒนาสถาปัตยกรรมองค์กรถูกนำเสนอขึ้นมามากมาย โดย The Zachman Framework for Enterprise Architecture ถือเป็นกรอบของสถาปัตยกรรมองค์กรแรกที่ถูกนำเสนอ ในปี พ.ศ. ๒๕๓๐ และเป็นกรอบแนวคิดที่ถูกนำมาประยุกต์ใช้เป็นจำนวนมาก นอกจากนี้ยังมีกรอบแนวคิดอื่นที่ได้ถูกนำมาปรับใช้ เช่น The Open Group Architecture Framework (TOGAF) และ Federal Enterprise Architecture (FEA) ซึ่งแต่ละแนวคิดมีใจความสำคัญดังต่อไปนี้

๒.๑.๑ The Zachman Framework

The Zachman Framework ดังแสดงตามรูปที่ ๕ เป็นแนวคิดที่พิจารณาอยู่ ๒ องค์ประกอบ โดยองค์ประกอบแรกคือ 5W1H (ตามแนวนอนของรูป) เป็นองค์ประกอบเกี่ยวกับการสื่อสารโดยการสอบถามด้วย ๖ คำถามต่อไปนี้ ใคร (Who) ทำอะไร (What) ที่ไหน (Where) เมื่อไร (When) ทำไม (Why) และอย่างไร (How) คำถามเหล่านี้จะช่วยรวบรวมและวิเคราะห์เรื่องราวหรือสิ่งต่างๆและการหาความสัมพันธ์ในเชิงเหตุผลของสิ่งเหล่านั้น องค์ประกอบที่สองคือ มุมมองผู้รับฟัง (ตามแนวตั้งของรูป) เป็นองค์ประกอบที่กล่าวถึงมุมมองของผู้ที่เกี่ยวข้องกับสถาปัตยกรรมองค์กรในมุมมองต่างๆโดยประกอบไปด้วย ๖ มุมมองดังต่อไปนี้ มุมมองผู้บริหาร (Executive) มุมมองผู้จัดการธุรกิจ (Business Mgnt.) มุมมองสถาปนิก (Architect) มุมมองวิศวกร (Engineer) มุมมองช่างเทคนิค (Technician) และมุมมองระดับองค์กร (Enterprise) มุมมองเหล่านี้จะมองสิ่งที่ได้มาจาก 5W1H จากนามธรรมสู่รูปธรรมมากขึ้นตามลำดับ



รูปที่ ๕ The Zachman Framework for Enterprise Architecture [๑]

๒.๑.๒ TOGAF Framework

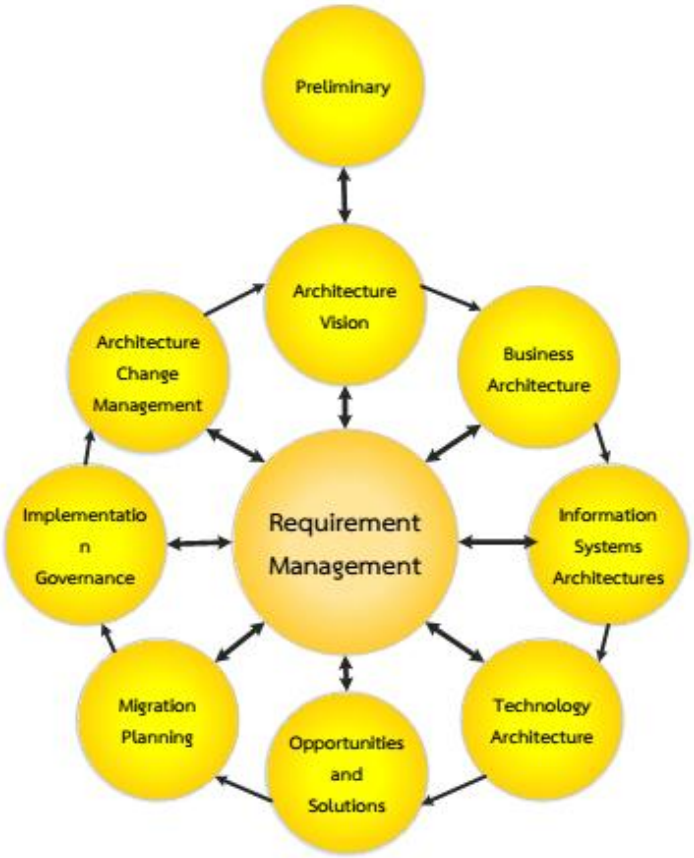
TOGAF ให้แนวทางในการจัดทำและการนำเอาสถาปัตกรรมองค์กรไปใช้งาน TOGAF แบ่งสถาปัตยกรรมองค์กรออกเป็น ๔ องค์ประกอบนั่นคือ

1) สถาปัตยกรรมด้านธุรกิจ (Business Architecture) : กล่าวถึงยุทธศาสตร์และกลยุทธ์องค์กร (Business Strategy and Tactic) กระบวนการธุรกิจ (Business Processes) รวมไปถึงการกำกับดูแลกิจการ (Governance)
2) สถาปัตยกรรมด้านข้อมูล (Data Architecture) : อธิบายถึงโครงสร้างของข้อมูลทั้งในระดับ Logical และระดับ Physical และครื่องมือ/กระบวนการในการบริหารจัดการข้อมูล
3) สถาปัตยกรรมด้านแอปพลิเคชัน (Application Architecture) : แสดงความสัมพันธ์ระหว่างแอปพลิเคชันกับกระบวนการธุรกิจ และความเชื่อมโยงกันระหว่างแอปพลิเคชันกับแอปพลิเคชัน
4) สถาปัตยกรรมด้านเทคโนโลยี (Technology Architecture) : อธิบายถึงการนำเอาซอฟต์แวร์ (Software) และฮาร์ดแวร์ (Hardware) มาสนับสนุนการบริหารจัดการกับข้อมูล แอปพลิเคชัน และธุรกิจ ในส่วนนี้จะกล่าวรวมไปถึงโครงสร้างพื้นฐานทางด้านเทคโนโลยีสารสนเทศ (IT Infrastructure) เช่นเครือข่าย (Network) กระบวนการ (Process) และ มาตรฐาน (Standard)

TOGAF Framework มีจุดเด่นที่สำคัญคือการให้แนวทางและรายละเอียดของการพัฒนาสถาปัตยกรรมองค์กร (Enterprise Architecture Development) ดังแสดงตาม รูปที่ ๖ โดยประกอบไปด้วยขั้นตอนต่อไปนี้

1) ขั้นต้น (Preliminary) : อธิบายถึงการปรับปรุงเปลี่ยนแปลง TOGAF เพื่อให้สอดคล้องกับรูปแบบการดำเนินงานขององค์กร และระบุหลักการสถาปัตยกรรม (Architecture Principle) ซึ่งจะใช้เป็นโครงร่างในการออกแบบสถาปัตยกรรมองค์กร

2) วิสัยทัศน์สถาปัตยกรรม (Architecture Vision) : อธิบายถึงกิจกรรมในขั้นต้นของการพัฒนาสถาปัตยกรรม ซึ่งประกอบไปด้วย การกำหนดขอบเขตของการพัฒนา (Scope) ระบุผู้ที่มีส่วนได้ส่วนเสียต่อการพัฒนา (Stakeholders) การปรับปรุงหลักการสถาปัตยกรรมที่ได้รับมาจากขั้นต้น การจัดทำวิสัยทัศน์สถาปัตยกรรม (Architecture Vision) ซึ่งเป็นการอธิบายพอสังเขปของสถาปัตยกรรมองค์กรในอนาคตและบอกถึงประโยชน์ที่จะได้รับจากความสำเร็จของการพัฒนาสถาปัตยกรรม
3) สถาปัตยกรรมธุรกิจ (Business Architecture) : อธิบายการพัฒนาสถาปัตยกรรมด้านธุรกิจเพื่อสนับสนุนวิสัยทัศน์สถาปัตยกรรมตามที่ได้ระบุไว้ในขั้นตอนก่อนหน้า
4) สถาปัตยกรรมระบบสารสนเทศ (Information System Architecture) : อธิบายการพัฒนาสถาปัตยกรรมด้านระบบสารสนเทศเพื่อสนับสนุนวิสัยทัศน์สถาปัตยกรรม
5) สถาปัตยกรรมด้านเทคโนโลยี (Technology Architecture) : อธิบายการพัฒนาสถาปัตยกรรมด้านเทคโนโลยีเพื่อสนับสนุนวิสัยทัศน์สถาปัตยกรรม
6) โอกาสและแนวทางการแก้ปัญหา (Opportunities and Solution) : วางแผนในการดำเนินการพัฒนาสถาปัตยกรรมในด้านต่างๆตามที่ระบุไว้ พร้อมทั้งกำหนดรอบหรือระยะเวลาการส่งมอบงานตามแผนงาน
7) การวางแผนการเปลี่ยนแปลง (Migration Planning) : ให้รายละเอียดในการพัฒนาสถาปัตยกรรมเพื่อเปลี่ยนจากสถาปัตยกรรมปัจจุบัน (Baseline/Current Architecture) ไปสู่สถาปัตยกรรมเป้าหมาย (Target/Future Architecture)
8) การกำกับดูแลการดำเนินการ (Implementation Governance) : เป็นการกำกับดูแลการพัฒนาโครงการหรือกิจกรรมต่างๆให้สอดคล้องกับสถาปัตยกรรมที่ได้ออกแบบไว้ โดยมีขั้นตอนดังนี้ ระบุทรัพยากร (Resources) และทักษะ (Skill) ที่จำเป็นต่อการพัฒนาโครงการ ให้แนวทางในการนำเอาวิธีการแก้ไขปัญหาไปใช้ (Guide for applying solution) ทบทวนความสอดคล้องระหว่างสิ่งที่กำลังพัฒนากับสถาปัตยกรรมที่ออกแบบไว้ (Compliance Review)
9) การจัดการการเปลี่ยนแปลงสถาปัตยกรรม (Architecture Change Management) : เป็นการบริหารจัดการเมื่อเกิดการเปลี่ยนแปลงต่อสถาปัตยกรรมองค์กร



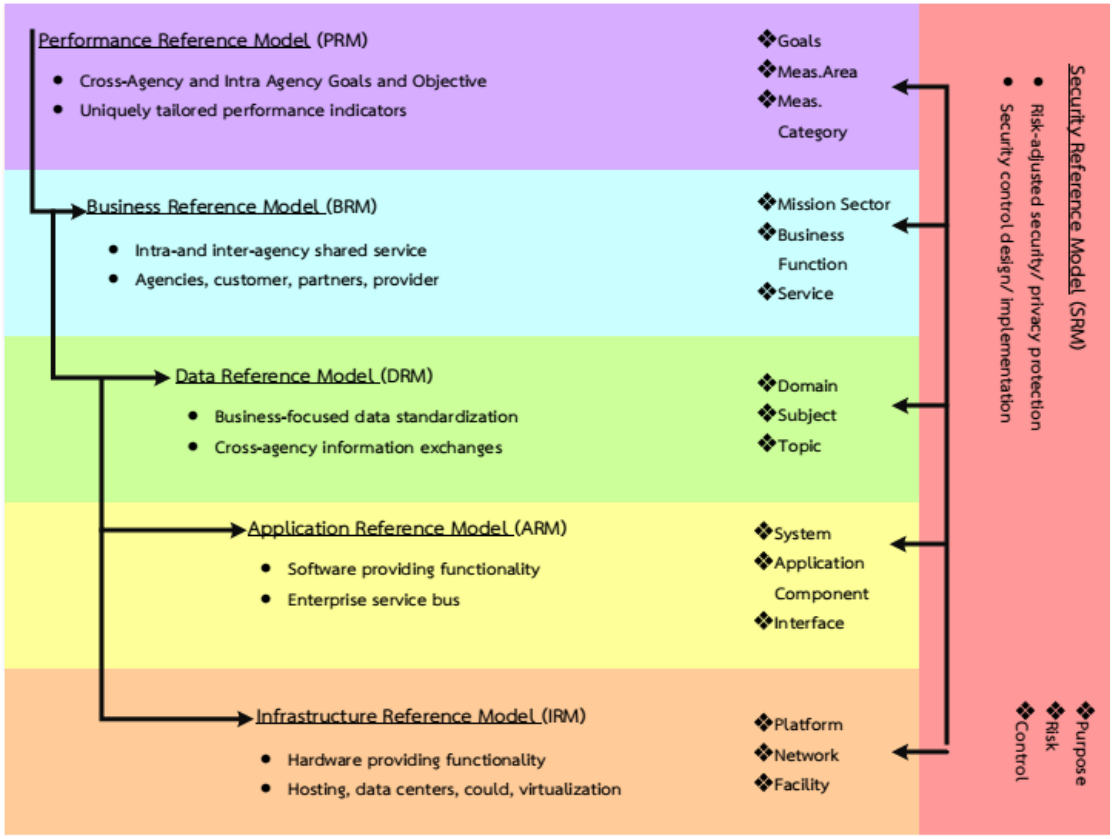
รูปที่ ๖ TOGAF Architecture Development Method [๒]

๒.๑.๓ Federal Enterprise Architecture (FEA)

FEA ได้ให้แนวทางในการจัดทำและการนำเอาสถาปัตกรรมองค์กรไปใช้งาน ซึ่งแบ่งแบบจำลองการอ้างอิง (Consolidated Reference Models) ดังแสดงตาม รูปที่ ๗ ออกเป็น ๕ แบบจำลองประกอบไปด้วย

1) แบบจำลองอ้างอิงประสิทธิภาพองค์กร (Performance Reference Model) : กล่าวถึงวัตถุประสงค์และเป้าหมายขององค์กร และความสัมพันธ์ระหว่างเป้าหมายองค์กรกับองค์กรอื่น นอกจากนี้ยังรวมไปถึงการติดตามและวัดประสิทธิภาพขององค์กร
2) แบบจำลองอ้างอิงธุรกิจ (Business Reference Model) : อธิบายถึงบริการต่างๆ (Business Services) ที่มีการใช้ร่วมกันภายในองค์กรและระหว่างองค์กร และกระบวนการธุรกิจ
3) แบบจำลองอ้างอิงข้อมูล (Data Reference Model) : อธิบายถึงการบริหารจัดการข้อมูลให้เป็นมาตรฐานและการแลกเปลี่ยนข้อมูลตลอดทั้งองค์กร
4) แบบจำลองอ้างอิงแอปพลิเคชัน (Application Reference Model) : ระบุถึงการนำเอาแอปพลิคชันมาใช้งานให้สอดคล้องกับกระบวนการธุรกิจ
5) แบบจำลองอ้างอิงโครงสร้างพื้นฐาน (Infrastructure Reference Model) : อธิบายถึงโครงสร้างพื้นฐานต่างๆที่ถูกนำมาใช้เพื่ออำนวยความสะดวกต่อการบริหารจัดการกับธุรกิจ แอปพลิเคชัน ข้อมูล และความมั่นคงปลอดภัย

6) แบบจำลองอ้างอิงความมั่นคงปลอดภัย (Security Reference Model) : กล่าวถึงการออกแบบและนำเอามาตรการควบคุม (Controls) ความมั่นคงปลอดภัยไปใช้เพื่อให้การดำเนินการด้านธุรกิจและเทคโนโลยีสารสนเทศเป็นไปด้วยการรักษาความลับ (Confidentiality) ความถูกต้อง (Integrity) ความพร้อมใช้ (Availability) ความโปร่งใส (Transparency) และตรวจสอบได้ (Accountability) รวมไปถึงการบริหารจัดการความเสี่ยง (Risk Management)



รูปที่ ๗ Federal Enterprise Architecture Framework : FEA [๓]

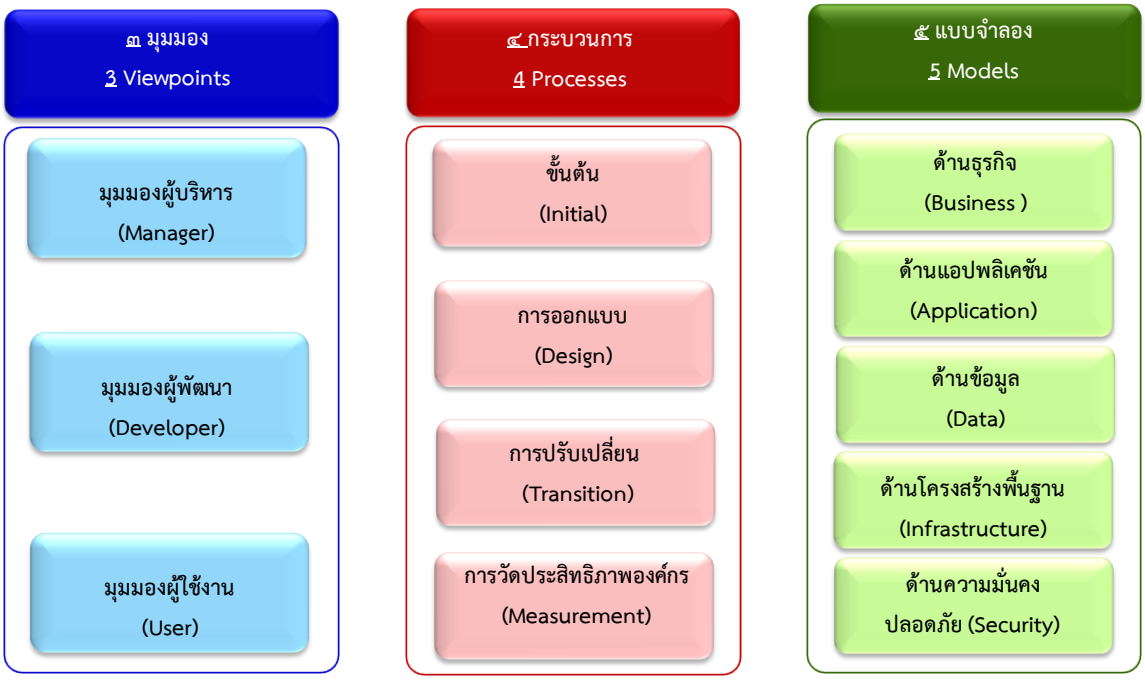
FEA ได้ให้แนวทางการพัฒนาสถาปัตยกรรมองค์กร (Enterprise Architecture Development) เช่นเดียวกับ TOGAF แต่มีขั้นตอนและรายละเอียดที่แตกต่างกันดังรายการต่อไปนี้

1) การระบุและทวนสอบ (Identify and Validate) : ผู้ที่เกี่ยวข้องร่วมกันระบุความต้องการ (Requirement) และขอบเขต (Scope) ในการพัฒนาสถาปัตยกรรมองค์กร พร้อมทั้งทวนสอบเพื่อให้มั่นใจได้ว่ามีความเข้าใจต่อความต้องการตรงกัน ระบุตัวชี้วัดประสิทธิภาพองค์กร และระบุบุคคลที่มีหน้าที่รับผิดชอบต่อการอนุมัติ (Approve) ความต้องการในการเปลี่ยนแปลงสถาปัตยกรรม
2) การวิจัยและการสืบค้น (Research and Leverage) : สำรวจสิ่งที่องค์กรมีหรือองค์กรอื่นมี เพื่อระบุถึงโอกาสที่จะนำเอาสิ่งที่มีอยู่แล้วมาปรับใช้ให้ตรงกับความต้องการที่ได้ระบุไว้ในข้อแรก
3) การนิยามและการวางแผน (Define and Plan) : วิเคราะห์และออกแบบสถาปัตยกรรมองค์กรในด้านต่างๆ เช่น ยุทธศาสตร์ (Strategy) ธุรกิจ (Business) ข้อมูล (Data) แอปพลิเคชัน (Application) โครงสร้างพื้นฐาน (Infrastructure) และความมั่นคงปลอดภัย (Security) จัดทำแนวทาง (Roadmap) และแผน (Plan) การดำเนินงาน

4) การลงทุนและการดำเนินการ (Invest and Execute) : ทำการตัดสินว่าจะลงทุนหรือดำเนินการตามแผนที่ได้ระบุไว้หรือไม่ ย้อนกลับไปปรับปรุงแผนใหม่ในกรณีตัดสินใจไม่ดำเนินการ การตัดสินใจว่าไม่ลงทุนอาจเกิดจากการเปลี่ยนแปลงในด้านต่างๆ เช่น นโยบาย เทคโนโลยี กระบวนการ หรือทรัพยากร
5) การวัดผล (Perform and Masure) : วัดผลลัพธ์ที่เกิดขึ้นจากการดำเนินงานในขั้นที่ ๔ ด้วยมาตรวัดที่ได้กำหนดขึ้นในขั้นตอนที่ ๑ ผลจากการวัดสามารถนำไปปรับปรุงแผนการพัฒนาในรอบต่อไป

๒.๒ กรอบสถาปัตยกรรมองค์กร

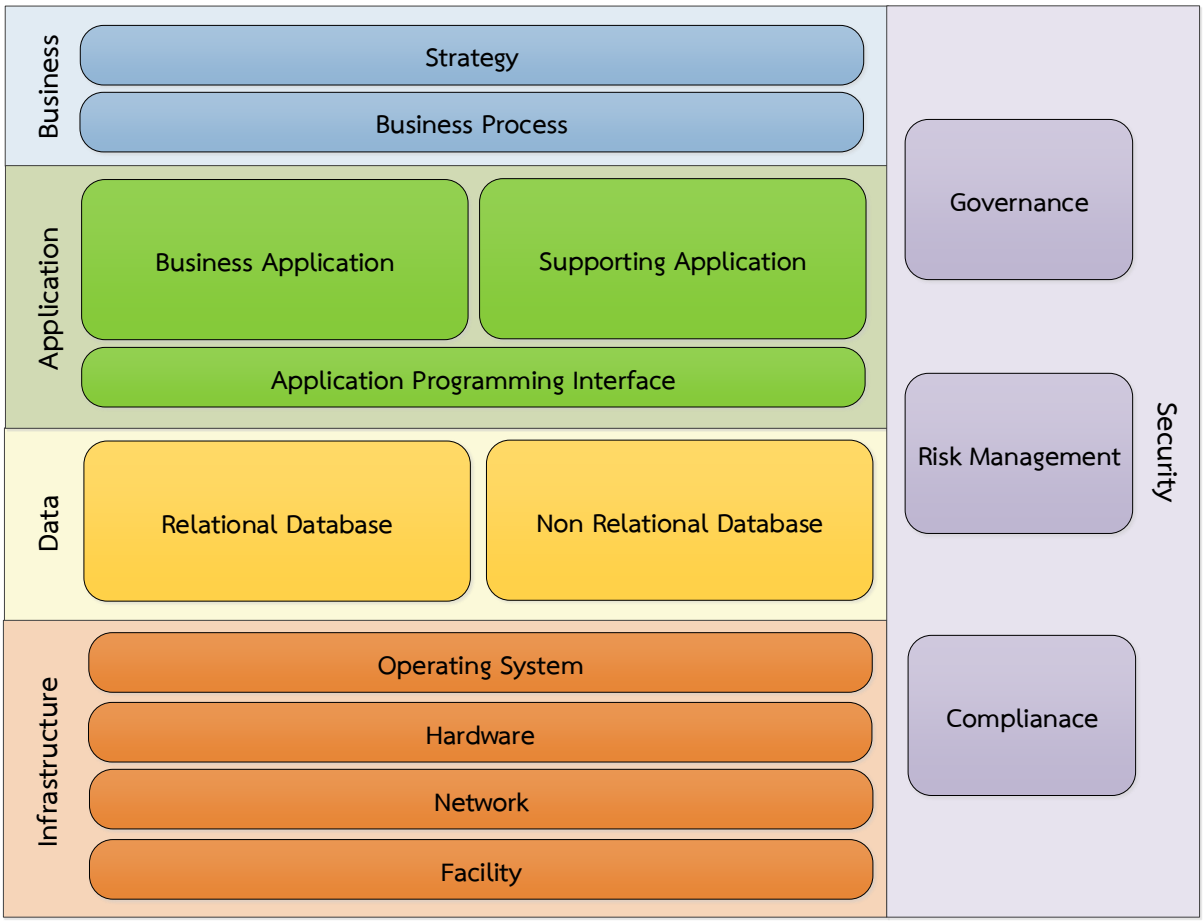
ในการดำเนินการพัฒนาสถาปัตยกรรมองค์กรของ สรอ. ได้นำเอาข้อดีของกรอบแนวคิดของทั้ง Zachman TOGAF และ FEA มาปรับปรุงให้กระชับและเข้าใจง่ายสอดคล้องกับรูปแบบการดำเนินงานขององค์กร โดยสามารถนำมาจัดทำเป็นกรอบสถาปัตยกรรมองค์กรของ สรอ. (EGA Enterprise Architecture Framework) ได้เป็น ***"๓ มุมมอง (Viewpoints) ๔ กระบวนการ (Processes) และ ๕ สถาปัตยกรรมย่อย/แบบจำลอง (Sub Architectures/Models)"*** ตามแสดงในรูปที่ ๘



รูปที่ ๘ ภาพแสดงกรอบสถาปัตยกรรมองค์กรของ สรอ.

มุมมองของสถาปัตยกรรมองค์กรของ สรอ. (EGA Enterprise Architecture ViewPoints) สามารถแบ่งมุมมองออกเป็น ๓ มุมมองหลัก อันได้แก่ ๑) มุมมองผู้บริหาร ประกอบไปด้วย คณะกรรมการบริหาร อนุคณะกรรมการบริหาร ผู้อำนวยการสำนักงาน (Chief Executive Officer : CEO) ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (Chief Information Officer : CIO) รองผู้อำนวยการสำนักงาน ผู้อำนวยการฝ่าย รองผู้อำนวยการฝ่าย และและผู้จัดการส่วน ๒) มุมมองเชิงพัฒนา ประกอบไปด้วย เจ้าหน้าที่พัฒนาธุรกิจ เจ้าหน้าที่ด้านเทคโนโลยีสารสนเทศ ๓) มุมมองผู้ใช้อ้างถึงผู้ที่เกี่ยวข้องทั้งด้านธุรกิจและด้านเทคโนโลยีสารสนเทศ

สถาปัตยกรรมย่อยและแบบจำลองอ้างองค์กรของ สรอ. (EGA Enterprise Reference Models) ประกอบไปด้วย ๕ ด้าน ได้แก่ ด้านธุรกิจ (Business) ด้านแอปพลิเคชัน (Application) ด้านข้อมูล (Data) ด้านโครงสร้างพื้นฐาน (Infrastructure) และด้านความมั่นคงปลอดภัย (Security) ตามที่แสดงในรูปที่ ๙



รูปที่ ๙ EGA Enterprise Reference Model

จากรูปที่ ๙ ด้านธุรกิจแบ่งออกเป็นสองหมวดประกอบไปด้วย ยุทธศาสตร์ (Strategy) และกระบวนการธุรกิจ (Business Process) ด้านแอปพลิเคชันแบ่งออกเป็นสามหมวดประกอบไปด้วย แอปพิเคชันธุรกิจ (Business Application) แอปพลิเคชันสนับสนุน (Supporting Application) และส่วนต่อประสานโปรแกรมประยุกต์ (Application Programming Interface) ด้านข้อมูลแบ่งออกเป็นสองหมวดประกอบไปด้วย ข้อมูลที่ถูกจัดเก็บในแบบฐานข้อมูล (Relational Database) และข้อมูลที่ไม่ได้จัดเก็บในรูปแบบฐานข้อมูล (Non Relational Database) ด้านโครงสร้างพื้นฐานแบ่งออกเป็นสี่หมวดประกอบไปด้วย ระบบปฏิบัติการ (Operating System) ฮาร์ดแวร์ (Hardware) เครือข่าย (Network) และระบบอำนวยการ (Facility) ด้านความมั่นคงปลอดภัยประกอบไปด้วย ธรรมาภิบาล (Governance) การบริหารจัดการความเสี่ยง (Risk Management) และความสอดคล้องกับกฎระเบียบ (Compliance) โดยแต่ละมุมมองของสถาปัตยกรรมองค์กรนั้นจะมีมุมมองต่อแบบจำลอง (Enterprise Reference Models) ที่แตกต่างกันตามที่แสดงในรูปที่ ๑๐

Viewpoint/ Model	Business	Application	Data	Infrastructure	Security
Manager	Work Products	Work Products	Work Products	Work Products	Work Products
Developer	Work Products	Work Products	Work Products	Work Products	Work Products
User	Work Products	Work Products	Work Products	Work Products	Work Products

รูปที่ ๑๐ Work Products ของมุมมอง (Viewpoint) ในแต่ละแบบจำลอง (Reference Model)

กระบวนกาพัฒนาสถาปัตยกรรมองค์กรของ สรอ. (EGA Enterprise Architecture Development Processes) ตามที่แสดงในรูปที่ ๑๑

Development Processes		
1	Initial	Scope, Stakeholders, Architecture Principle, and Key Performance indicator
2	Design	Current and Future States of EA, Gap Analysis, Prioritization, and Roadmap
3	Transition	Transition plan and Implementation Governance
4	Measurement	Performance Measurement and Continual Improvement

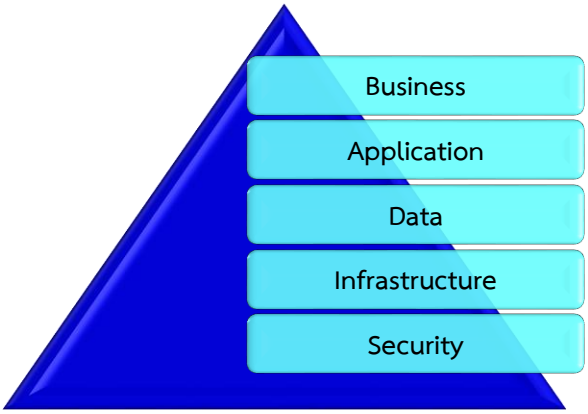
รูปที่ ๑๑ EGA Enterprise Architecture Development Process

กระบวนกาพัฒนาสถาปัตยกรรมองค์กรถูกกำหนดขึ้นมาเพื่อใช้เป็นแนวทางในการพัฒนาสถาปัตยกรรมองค์กรเพื่อให้ได้ผลลัพธ์ (Work Product) ของแบบจำลองในมุมมองต่างๆ โดยสามารถแบ่งกระบวนการการพัฒนาสถาปัตยกรรมออกเป็น ๔ กระบวนการหลัก อันได้แก่ กระบวนการขั้นต้น (Initial) กระบวนการการออกแบบ (Design) กระบวนการการปรับเปลี่ยน (Transition) และกระบวนการการวัดประสิทธิภาพองค์กร (Measurement) ซึ่งกระบวนการขั้นต้นจะกล่าวถึง ขอบเขตของการจัดทำสถาปัตยกรรมองค์กร (Scope) ผู้ที่เกี่ยวข้อง (Stakeholders) หลักการสถาปัตยกรรม (Architecture Principle) ซึ่งจะให้โครงร่างของสถาปัตยกรรมองค์กรในอนาคต (Future State Outline) และตัวชี้วัดผลสำเร็จขององค์กร (Key

Performance Indicator) กระบวนการการออกแบบจะกล่าวถึง สถานะปัจจุบันและอนาคตของสถาปัตยกรรมองค์กร (Current and Future States of Enterprise Architecture) การวิเคราะห์ความแตกต่างของทั้งสองสถานะ (Gap Analysis) การจัดเรียงลำดับและเลือกโครงการที่ต้องการจะปรับเปลี่ยน (Prioritization) และแผนการดำเนินงาน (Roadmap) ส่วนกระบวนการการปรับเปลี่ยนจะกล่าวถึง แผนการปรับเปลี่ยน (Transition Plan) และการกำกับดูแลการพัฒนาโครงการ (Implementation Governance) และสุดท้ายคือกระบวนการการวัดผลประสิทธิภาพองค์กรจะกล่าวถึง การวัดประสิทธิภาพองค์กร (Performance Measurement) ซึ่งสอดคล้องกับตัวชี้วัดผลสำเร็จขององค์กรตามที่ระบุไว้ในกระบวนการขั้นต้น และการปรับปรุงสถาปัตยกรรมองค์กรอย่างต่อเนื่อง (Continual Improvement)

บทที่ ๓ การวิเคราะห์สถานะปัจจุบันของสถาปัตยกรรมองค์กร

การพัฒนาสถาปัตยกรรมองค์กรจัดทำขึ้นเพื่อให้สำนักงาน สามารถยกระดับสถานะปัจจุบันไปสู่เป้าหมายที่ต้องการได้นั้น จำเป็นต้องมีการวิเคราะห์ปัจจัยต่างๆที่มีผลต่อการพัฒนาสถาปัตยกรรมองค์กรทั้งในด้านธุรกิจ เทคโนโลยีสารสนเทศ และความมั่นคงปลอดภัย โดยเริ่มสำรวจและรวบรวมข้อมูลโครงสร้างองค์กร (**ภาคผนวก ก**) นโยบาย/วิสัยทัศน์ พันธกิจ แผนยุทธศาสตร์ ๔ ปี สรอ. (พ.ศ. ๒๕๕๗ – ๒๕๖๐) แผนกลยุทธ์ ประจำปีงบประมาณ ๒๕๕๘ แผนแม่บทเทคโนโลยีสารสนเทศและการสื่อสาร ระยะ ๓ ปี (พ.ศ.๒๕๕๘ – ๒๕๖๐) แผนบริหารจัดการระบบสารสนเทศ สรอ. ประจำปี พ.ศ.๒๕๕๘ โครงการจัดทำกระบวนการดำเนินงาน Business Process Improvement (BPI) และนโยบายความมั่นคงปลอดภัยสารสนเทศ จากผลการสำรวจและการศึกษาข้อมูลได้ทำการวิเคราะห์ออกเป็น ๕ ด้านอันได้แก่ ด้านธุรกิจ (Business) ด้านแอปพลิเคชัน (Application) ด้านข้อมูล (Data) ด้านโครงสร้างพื้นฐาน (Infrastructure) และด้านความมั่นคงปลอดภัย(Security) ดังแสดงในรูปที่ ๑๒



รูปที่ ๑๒ ภาพแสดงรายการสถาปัตยกรรมองค์กรในด้านต่างๆที่มีการสำรวจ

ผลจากการสำรวจข้อมูลสถานะปัจจุบันของสถาปัตยกรรมองค์กร สรอ. พบว่ามีการประยุกต์ใช้ระเบียบ หลักการ ข้อบังคับ หรือกฎหมายที่เกี่ยวข้องด้านความปลอดภัยเทคโนโลยีสารสนเทศ มาเป็นหลักเกณฑ์ในการควบคุมบริการ กระบวนการทางธุรกิจ แอปพลิเคชัน ข้อมูล โครงสร้างพื้นฐาน ของสำนักงาน ให้เกิดความถูกต้อง ครบถ้วน และมีความพร้อมในการให้บริการด้วย ซึ่งสามารถแสดงสถานะปัจจุบันของสถาปัตยกรรมภายองค์กรดังแสดงตามรูปที่ ๑ ความเชื่อมโยงสถาปัตยกรรมองค์กรด้านต่างๆดังแสดงตาม **ภาคผนวก ข**

นอกจากนี้ TOWS Matrix ถูกใช้เพื่อวิเคราะห์และประเมินหาจุดแข็ง จุดอ่อน โอกาสและอุปสรรค และกำหนดเป็นกลยุทธ์สำหรับการพัฒนาสถาปัตยกรรมภายในองค์กรของ สรอ. โดยการลดหรือกำจัดจุดอ่อนที่เป็นอยู่ การรับมือกับปัจจัยที่เป็นอุปสรรคต่างๆ การสร้างความได้เปรียบและเสริมจุดแข็งและโอกาสที่มี อันจะนำไปสู่การปรับปรุงประสิทธิภาพและสนับสนุนการดำเนินงานภายในสำนักงาน ให้สามารถนำไปขับเคลื่อนภารกิจ ยุทธศาสตร์และโครงการหลักของสำนักงาน ลดความซ้ำซ้อน สร้างมูลค่าและเกิดประโยชน์สูงสุดจากการลงทุนด้านเทคโนโลยีสารสนเทศต่อไป

๓.๑ ด้านธุรกิจ (Businesses)

การสำรวจและวิเคราะห์สถานะปัจจุบันของสถาปัตยกรรมองค์กรด้านธุรกิจนั้น ประกอบไปด้วยสองส่วนหลักดังต่อไปนี้ (๑ ยุทธศาสตร์ และ (๒) กระบวนการดำเนินงานภายในสำนักงาน

ยุทธศาสตร์ (Strategy)

สำนักงานได้มีการกำหนด วิสัยทัศน์ ภารกิจ ยุทธศาสตร์ กลยุทธ์ พร้อมทั้งการกำหนดตัวชี้วัดผลการดำเนินงานขึ้นมีเพื่อวัดประสิทธิภาพขององค์กร

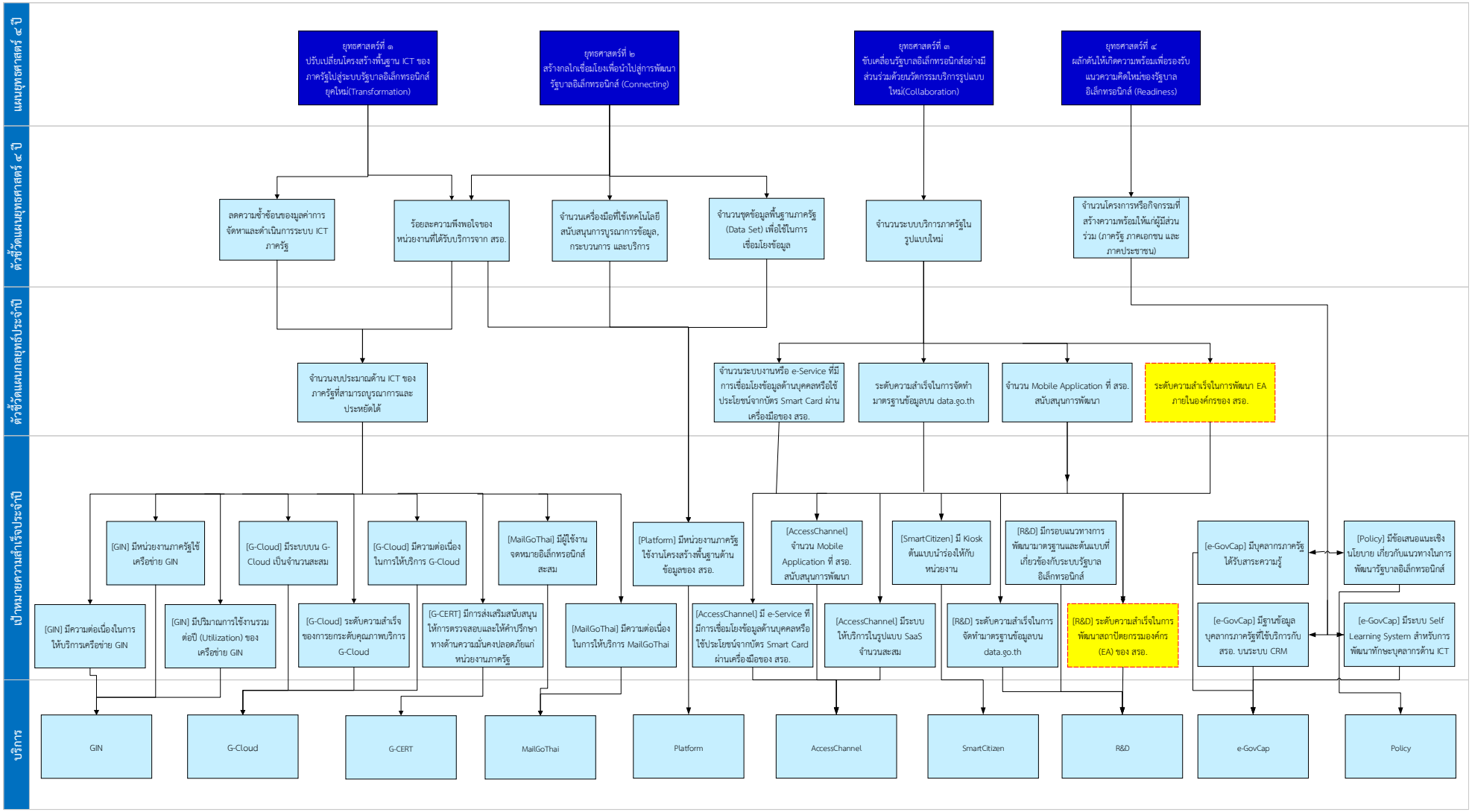
เป้าหมาย/วิสัยทัศน์ เป็นหน่วยงานกลางของประเทศด้านการผลักดันและขับเคลื่อนการพัฒนารัฐบาลอิเล็กทรอนิกส์ให้มีความสมบูรณ์และมั่นคงปลอดภัย

ภารกิจ ประกอบไปด้วย

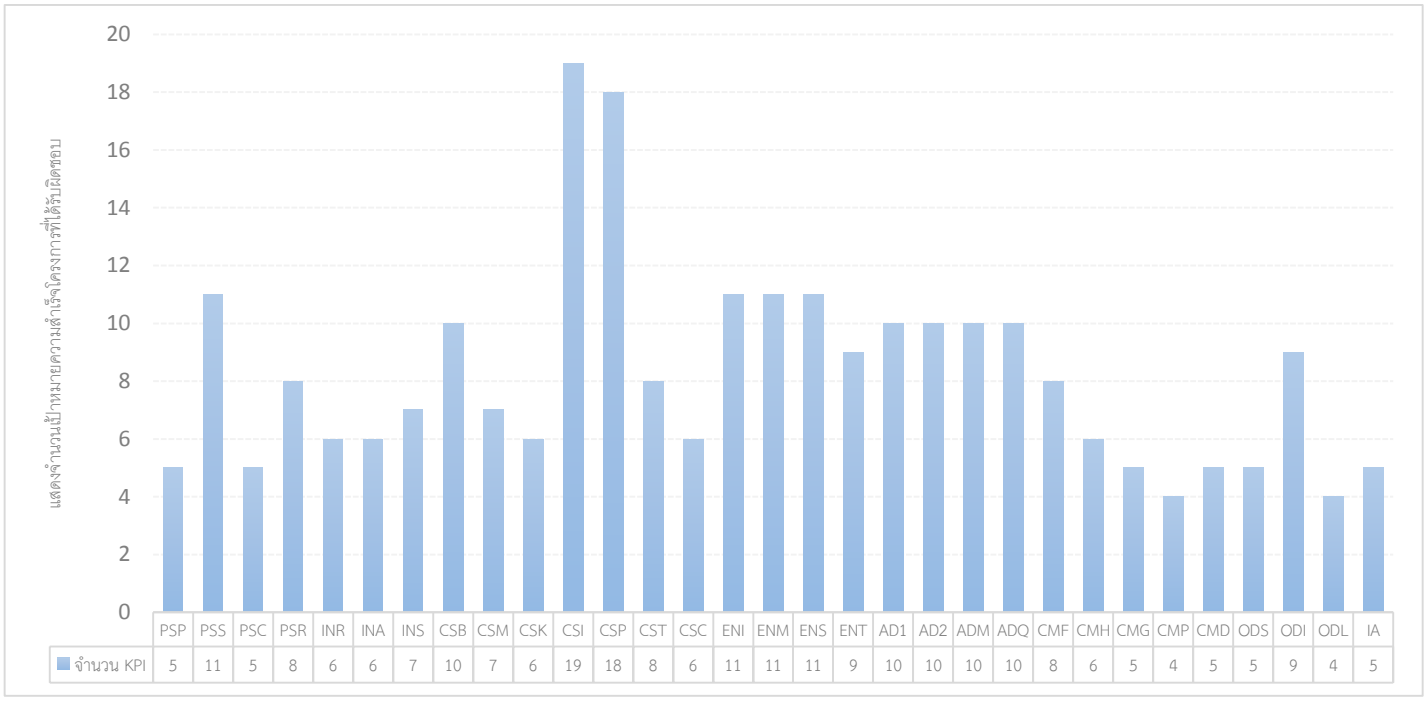
๑) พัฒนา บริหารจัดการ และให้บริการโครงสร้างพื้นฐานสารสนเทศในส่วนที่เกี่ยวกับรัฐบาลอิเล็กทรอนิกส์
๒) ศึกษา วิจัย พัฒนา และเสนอแนะแนวทาง มาตรการ และมาตรฐานด้านรัฐบาลอิเล็กทรอนิกส์
๓) ให้คำปรึกษา บริการด้านวิชาการ และบริหารจัดการโครงการด้านเทคโนโลยีสารสนเทศและการสื่อสารในส่วนที่เกี่ยวข้องกับรัฐบาลอิเล็กทรอนิกส์
๔) ส่งเสริม สนับสนุน และจัดอบรมเพื่อยกระดับทักษะความรู้ความสามารถด้านรัฐบาลอิเล็กทรอนิกส์ตลอดจนเผยแพร่ข้อมูลข่าวสาร

ยุทธศาสตร์ กลยุทธ์ และตัวชี้วัดผลการดำเนินงาน เพื่อบรรลุภารกิจและวิสัยทัศน์ขององกรค์สำนักงานมีการกำหนดยุทธศาสตร์องค์กรในระยะ ๔ ปี และกลยุทธ์รายปี นอกจากนี้ยังมีการกำหนดตัวชี้วัดเพื่อวัดประสิทธิภาพองค์กรทั้งในระยะ ๔ ปี และรายปีเช่นเดียวกัน รูปที่ ๑๓ แสดงความสัมพันธ์ระหว่างแผนยุทธศาสตร์ ๔ ปี (พ.ศ.๒๕๕๗ – ๒๕๖๐) ตัวชี้วัดแผนยุทธศาสตร์ ๔ ปี ตัวชี้วัดแผนกลยุทธ์และเป้าหมายความสำเร็จโครงการประจำปี พ.ศ.๒๕๕๘ ขณะที่ รูปที่ ๑๓แสดงความสัมพันธ์ระหว่างเป้าหมายความสำเร็จโครงการกับส่วนงานที่รับผิดชอบ

จากรูปที่ ๑๓ แสดงให้เห็นว่าแผนยุทธศาสตร์ ๔ ปี ประกอบด้วยยุทธศาสตร์ ๔ ด้านดังนี้ ยุทธศาสตร์ที่ ๑ ปรับเปลี่ยนโครงสร้างพื้นฐาน ICT ของภาครัฐไปสู่ระบบรัฐบาลอิเล็กทรอนิกส์ยุคใหม่ (Transformation) ยุทธศาสตร์ที่ ๒ สร้างกลไกเชื่อมโยงเพื่อนำไปสู่การพัฒนารัฐบาลอิเล็กทรอนิกส์ (Connecting) ยุทธศาสตร์ที่ ๓ ขับเคลื่อนรัฐบาลอิเล็กทรอนิกส์อย่างมีส่วนร่วมด้วยนวัตกรรมบริการรูปแบบใหม่ (Collaboration) และยุทธศาสตร์ที่ ๔ ผลักดันให้เกิดความพร้อมเพื่อรองรับแนวความคิดใหม่ของรัฐบาลอิเล็กทรอนิกส์ (Readiness) ตัวชี้วัดของแผนยุทธศาสตร์ ๔ มีอยู่ด้วยกัน ๖ ตัวชี้วัด ตัวชี้วัดแผนกลยุทธ์ประจำปี ๒๕๕๘ มีอยู่ด้วยกัน ๕ ตัวชี้วัด และเป้าหมายความสำเร็จโครงการประจำปี ๒๕๕๘ มีอยู่ด้วยกัน ๒๑ ข้อ ซึ่งเป้าหมายความสำเร็จนี้จะครอบคลุมบริการโครงการของสำนักงานดังต่อไปนี้



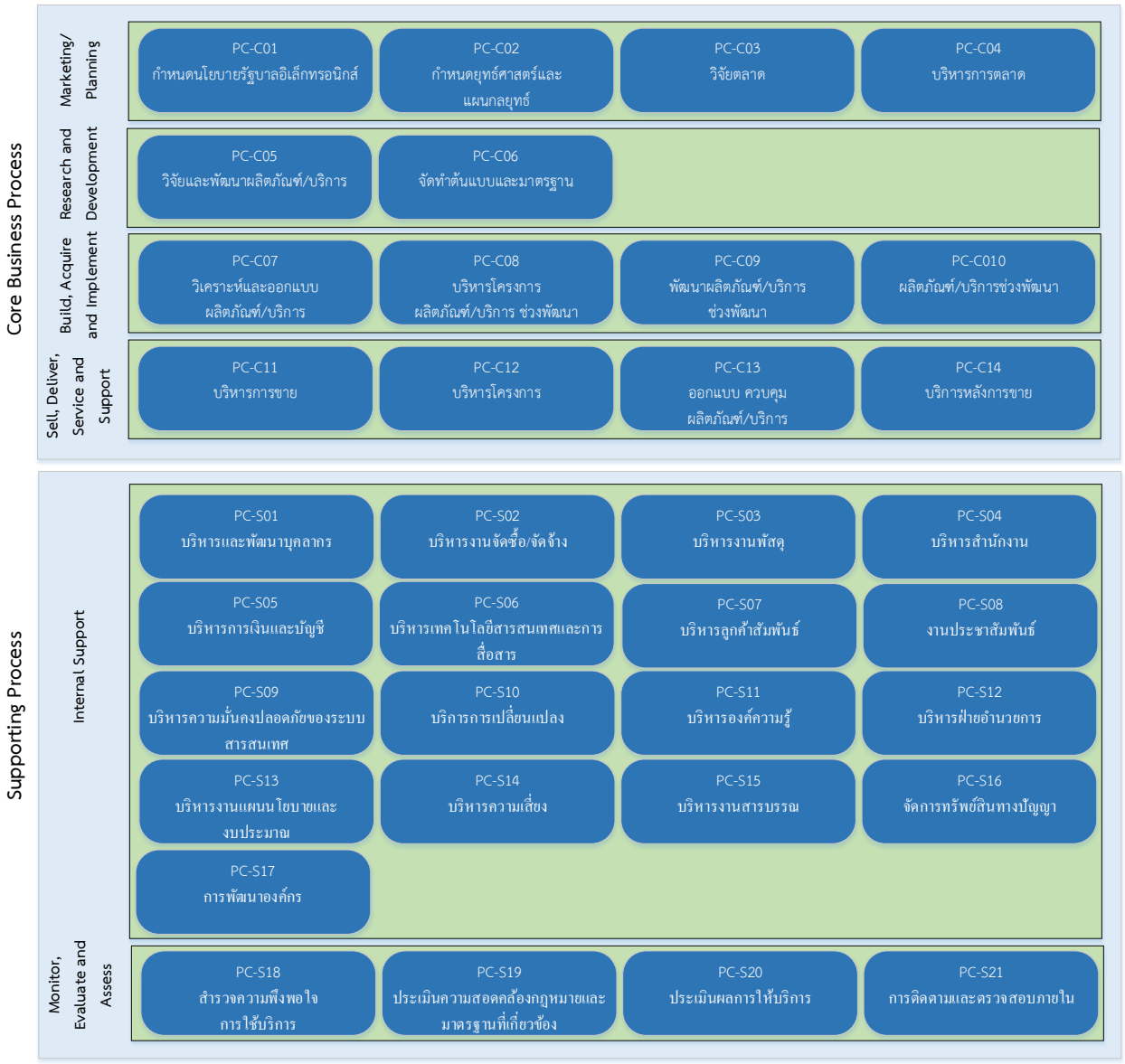
รูปที่ ๑๓ ไดอะแกรมความเชื่อมโยงของยุทธศาสตร์ ตัวชี้วัดองค์กรและบริการ



รูปที่ ๑๔ ภาพแสดงจำนวนเป้าหมายความสำเร็จโครงการที่ได้รับผิดชอบโดยส่วนงานต่างๆ

กระบวนการธุรกิจ (Business Process)

ในส่วนที่สองพิจารณาถึงกระบวนการปฏิบัติงาน โดยแบ่งออกเป็น ๒ หมวดตามรูปที่ ๑๕ ประกอบด้วย หมวดกระบวนการหลัก (Core Business Process) และหมวดกระบวนการสนับสนุน (Supporting Processes) หมวดกระบวนการหลักจำนวน ๑๔ กระบวนการปฏิบัติงานซึ่งกระจายอยู่ภายใน ๔ หมวดย่อยประกอบด้วย การตลาดและการวางแผน (Marketing and Planning) การวิจัยและพัฒนาต้นแบบ (Research and Development) การพัฒนา (Build, Acquire, and Implement) และการขาย (Sell, Deliver, Service, and Support) หมวดกระบวนการสนับสนุนจำนวน ๒๒ กระบวนการปฏิบัติงาน ซึ่งกระจายอยู่ภายใน ๒ หมวดย่อยประกอบด้วย การสนับสนุนภายใน (Internal Support) และการติดตาม (Monitor, Evaluate, and Assess)

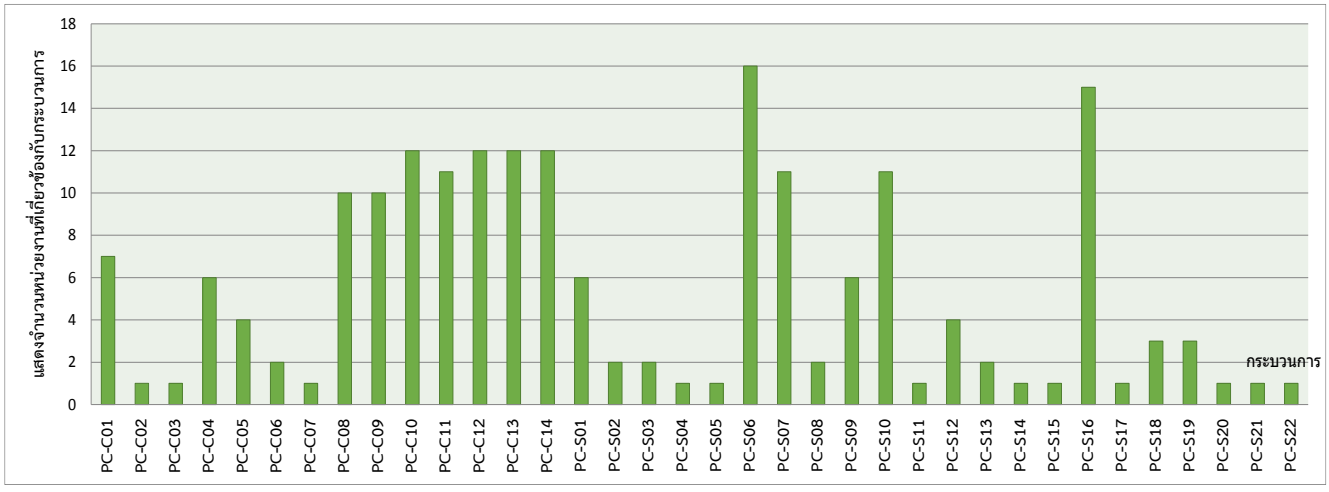


รูปที่ ๑๕ ภาพรวมของกระบวนการธุรกิจ [๘]

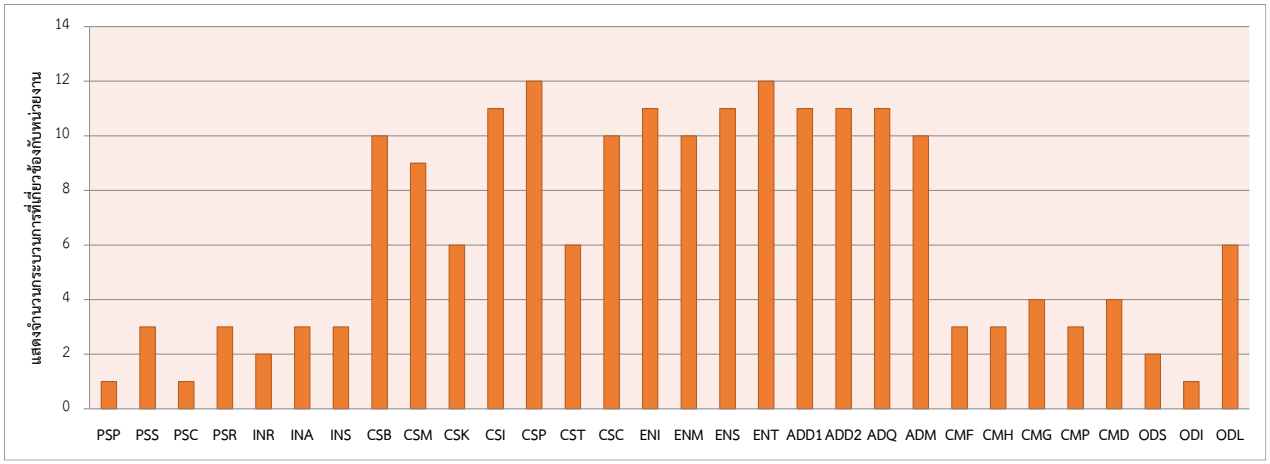
ตารางที่ ๑ แสดงความสัมพันธ์ระหว่างกระบวนการปฏิบัติงานและส่วนงานเพื่อแสดงให้เห็นว่าแต่ละส่วนงานมีส่วนเกี่ยวข้องกับกระบวนการปฏิบัติงานใดบ้าง รูปที่ ๑๖ แสดงจำนวนส่วนงานที่เกี่ยวข้องกับกระบวนการปฏิบัติงานซึ่งชี้ให้เห็นว่าแต่ละกระบวนการจะมีหลายส่วนงานเกี่ยวข้องโดยเฉพาะกระบวนการบริหารเทคโนโลยีและการสื่อสาร (PC-S06) มีส่วนงานที่เกี่ยวข้องทั้งหมดจำนวน ๓ ฝ่าย ๑๖ ส่วนงาน คิดเป็นร้อยละ ๕๓.๓๓ ของส่วนงานทั้งหมด ขณะที่รูปที่ ๑๗ แสดงจำนวนกระบวนการปฏิบัติงานที่เกี่ยวข้องกับส่วนงานซึ่งชี้ให้เห็นว่า ส่วนงานสนับสนุนและบริการด้านเทคนิค (ENT) มีส่วนเกี่ยวข้องกับกระบวนการปฏิบัติงานมากที่สุดคือ ๑๒ กระบวนการซึ่งคิดเป็นร้อยละ ๓๓ ของกระบวนการทั้งหมด

รหัส	กระบวนการธุรกิจ/ส่วนงาน	ฝ่ายนโยบายและ				ฝ่ายนวัตกรรม			ฝ่ายบริการให้คำปรึกษา							ฝ่ายวิศวกรรมและ				ฝ่ายพัฒนาและจัดการ				ฝ่ายบริหารประสิทธิภาพ					ฝ่ายอำนวยการ		
		ส่วนนโยบายรัฐบาลอิเล็กทรอนิกส์	ส่วนยุทธศาสตร์	ส่วนประสานความร่วมมือ	ส่วนบริหารความเสี่ยง	ส่วนวิจัยและพัฒนา	ส่วนปัจจัยและมาตรฐาน	ส่วนมาตรฐาน	ส่วนลูกค้า	ส่วนจัดการความรู้และสารสนเทศ	ส่วนที่ปรึกษาเทคโนโลยีสารสนเทศ	ส่วนบริหารโครงการ	ส่วนถ่ายทอดเทคโนโลยี	ส่วนศูนย์บริการลูกค้า	ส่วนโครงสร้างพื้นฐานสารสนเทศ	ส่วนระบบสารสนเทศ	ส่วนความมั่นคงปลอดภัยสารสนเทศ	ส่วนสนับสนุนและบริการด้านเทคนิค	ส่วนพัฒนาเทคโนโลยีระดับ 1	ส่วนพัฒนาเทคโนโลยีระดับ 2	ส่วนจัดการเทคโนโลยี	ส่วนจัดการพัฒนาองค์กร	ส่วนการเงินและบัญชี	ส่วนบริหารทรัพยากรบุคคล	บริการงานทั่วไปและอาคารสถานที่	ส่วนจัดซื้อจัดจ้างและพัสดุ	ส่วนพัฒนาองค์กร	ส่วนกฎหมาย	ส่วนรับเรื่องร้องเรียนและตรวจสอบ	ส่วนโฆษก
		PSP	PSS	PSC	PSR	INR	INA	INS	CSB	CSM	CSK	CSI	CSP	CST	CSC	ENI	ENM	ENS	ENT	ADD1	ADD2	ADQ	ADM	CMF	CMH	CMG	CMP	CMD	ODS	ODI	ODL
PC-C01	กำหนดนโยบายรัฐบาลอิเล็กทรอนิกส์	■		■						■	■	■		■																	■
PC-C02	กำหนดยุทธศาสตร์และแผนกลยุทธ์		■																												
PC-C03	วิจัยตลาด									■																					
PC-C04	บริหารการตลาด								■	■		■	■		■																
PC-C05	วิจัยและพัฒนาผลิตภัณฑ์/บริการ					■	■	■	■																						
PC-C06	จัดทำต้นแบบและมาตรฐาน						■	■																							
PC-C07	วิเคราะห์และออกแบบบริการ/ผลิตภัณฑ์								■																						
PC-C08	บริหารโครงการผลิตภัณฑ์/บริการ ช่วงพัฒนา											■	■			■	■	■	■	■	■	■	■								
PC-C09	พัฒนาผลิตภัณฑ์/บริการช่วงพัฒนา								■				■			■	■	■	■	■	■	■	■								
PC-C10	ผลิตภัณฑ์/บริการช่วงพัฒนา								■	■	■			■		■	■	■	■	■	■	■	■								
PC-C11	บริการการขาย											■	■		■	■	■	■	■	■	■	■	■								
PC-C12	บริหารโครงการ											■	■	■	■	■	■	■	■	■	■	■	■								
PC-C13	ออกแบบ ควบคุมผลิตภัณฑ์/บริการ				■							■	■		■	■	■	■	■	■	■	■	■								
PC-C14	บริหารหลังการขาย								■			■	■		■	■	■	■	■	■	■	■	■								
PC-S01	บริหารและพัฒนาบุคลากร																		■					■	■	■	■				■
PC-S02	บริหารงานจัดซื้อจัดจ้าง																										■				■
PC-S03	บริหารงานพัสดุ																									■	■				
PC-S04	บริหารสำนักงาน																									■					
PC-S05	กระบวนการบริการเงินและบัญชี																							■							
PC-S06	บริหารเทคโนโลยีสารสนเทศและการสื่อสาร								■	■	■	■	■	■	■	■	■	■	■	■	■	■	■		■						
PC-S07	บริหารลูกค้าสัมพันธ์									■		■			■	■	■	■	■	■	■	■	■								
PC-S08	งานประชาสัมพันธ์									■	■																				
PC-S09	บริหารความมั่นคง ปลอดภัยระบบสารสนเทศ												■		■	■		■	■							■					
PC-S10	กระบวนการบริหารการเปลี่ยนแปลง								■			■	■		■	■	■	■	■	■	■	■	■								
PC-S11	บริหารองค์ความรู้										■																				
PC-S12	กระบวนการบริหารฝ่ายอำนวยการ																								■					■	■	■
PC-S13	บริหารงานแผนนโยบายและงบประมาณ		■																					■							
PC-S14	บริหารความเสี่ยง				■																										
PC-S15	กระบวนการบริหารงานสารบรรณ																												■		
PC-S16	จัดการทรัพย์สินทางปัญญา					■	■	■	■	■	■	■	■	■	■					■	■	■	■								■
PC-S17	การพัฒนาองค์กร																											■			
PC-S18	สำรวจความพึงพอใจการใช้บริการ								■	■			■																		
PC-S19	ประเมินความสอดคล้องกฎหมายและมาตรฐานที่เกี่ยวข้อง				■																							■			■
PC-S20	ประเมินผลการให้บริการ		■																												
PC-S21	การติดตามและตรวจสอบภายใน																											■			
PC-S22	การจัดการระบบมาตรฐาน																											■			

ตารางที่ ๑ ตารางความสัมพันธ์ระหว่างกระบวนการปฏิบัติงานและส่วนงาน



รูปที่ ๑๖ ภาพแสดงจำนวนส่วนงานที่เกี่ยวข้องกับกระบวนการ



รูปที่ ๑๗ ภาพแสดงจำนวนกระบวนการที่เกี่ยวข้องกับส่วนงาน

ผลการสำรวจพบประเด็นปัญหาหลักๆในด้านธุรกิจ (Business) สามารถสรุปรายละเอียดได้ดังนี้

๑) กระบวนการปฏิบัติงานภายในสำนักงาน ใช้เวลาในการติดต่อประสานงานระหว่างกระบวนการหรือระหว่างส่วนงานค่อนข้างมาก ซึ่งปัจจัยที่ส่งผลให้ใช้เวลามาก คือ

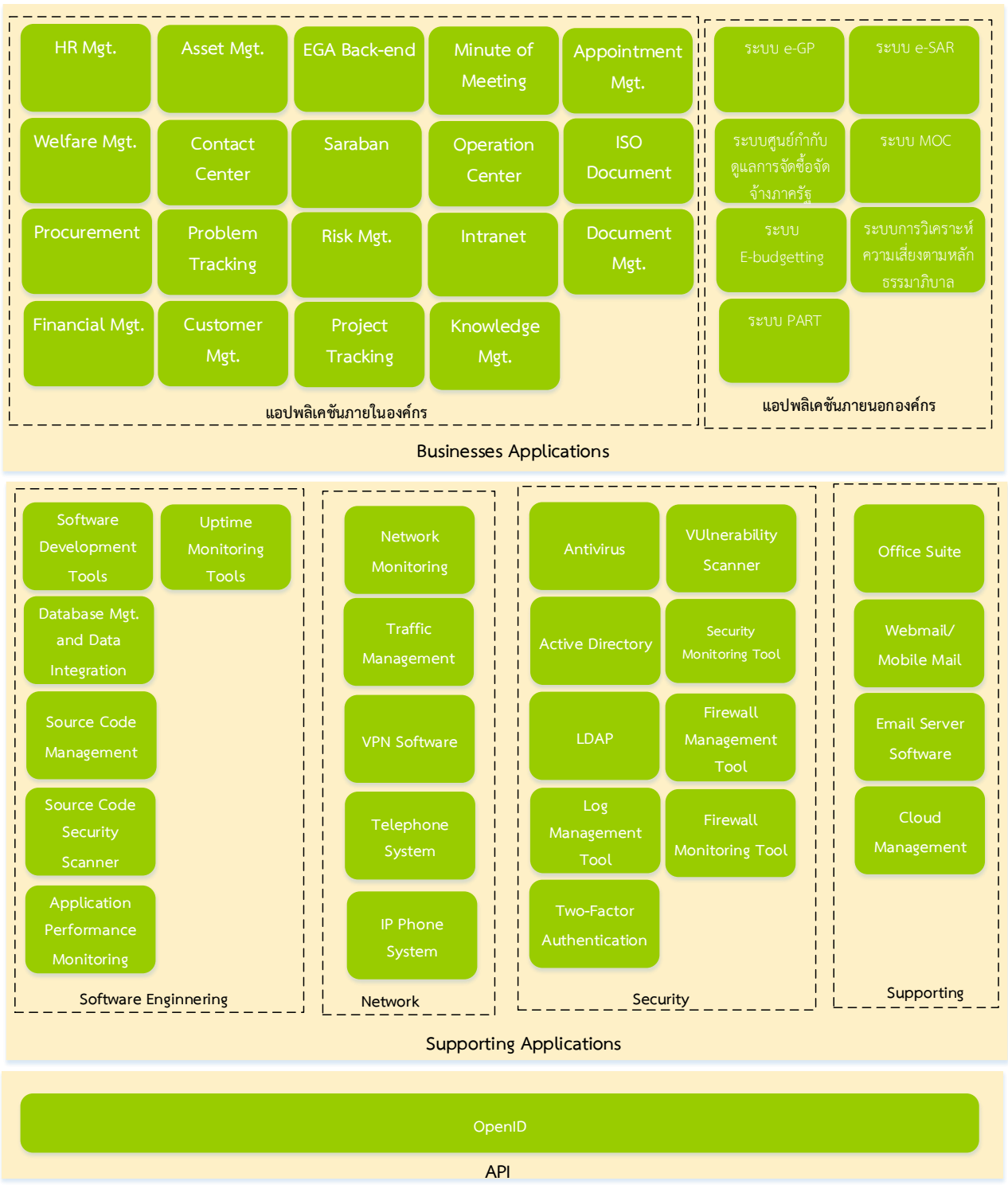
- กระบวนการปฏิบัติงานที่ต้องประสานงานกันระหว่างกระบวนการหรือระหว่างส่วนงานยังใช้ช่องทางผ่านการประชุม หรือผ่านทางเอกสาร (กระดาษ) หรือผ่านทางจดหมายอิเล็กทรอนิกส์ (e-mail) เป็นส่วนใหญ่ นอกเหนือจากที่ใช้ระยะเวลาประสานงานที่ค่อนข้างมากแล้ว ยังอาจเกิดการสูญหายของข้อมูลหรือข้อมูลไม่ครบถ้วนตามที่กำหนดไว้ด้วย เช่น กระบวนการบริหารงานแผนนโยบายและงบประมาณ (PC-S13) ขั้นตอนการโอนงบประมาณยังส่งข้อมูลผ่านทางกระดาษแจ้งให้กับผู้ที่เกี่ยวข้องได้รับทราบ (ข้อมูลจากผู้ที่ดำเนินการส่งให้ส่วนงานยุทธศาสตร์ และส่วนงานการเงินและบัญชี) หรือกระบวนการบริหารงานพัสดุ (PC-S03) ขั้นตอนการตรวจนับครุภัณฑ์ประจำปียังคงใช้กระดาษในการจดบันทึกครุภัณฑ์ที่ตรวจสอบและจะนำข้อมูลที่จดบันทึกบนกระดาษมาบันทึกข้อมูลลงในระบบต่อไป ซึ่งข้อมูลที่ได้มานั้นอาจบันทึกไม่ครบถ้วนหรือบันทึกผิดส่งผลให้ต้องกลับไปตรวจสอบใหม่อีกครั้ง เป็นต้น
- กระบวนการการปฏิบัติงานมีหลายขั้นตอน เช่น การขออนุมัติหลายขั้นตอน และการใช้กระดาษเพื่อเสนอพิจารณา ตัวอย่าง กระบวนการบริหารและพัฒนาบุคลากร (PC-S01) หรือกระบวนการบริหารงานจัดซื้อและจัดจ้าง (PC-S02) เป็นต้น

๒) ขาดความเชื่อมโยงของกระบวนการ ในกรณีส่งต่อข้อมูลไปยังกระบวนการหรือส่วนงานถัดไปหากต้องการจะทราบข้อมูลต้องติดตามกับส่วนงานที่รับเรื่อง ส่งผลให้ไม่สามารถทราบสถานะการดำเนินงาน หรือข้อมูลต่างๆได้ ยกตัวอย่างเช่น กระบวนการบริหารงานแผนนโยบายและงบประมาณ (PC-S13) การขอตรวจสอบงบประมาณคงเหลือระหว่างปี หากส่วนงานใดต้องการทราบสถานะการเบิกจ่ายงบประมาณต้องประสานติดต่อกับส่วนงานการเงินและบัญชี เป็นต้น

๓.๒ ด้านแอปพลิเคชัน (Application)

จากผลการสำรวจด้านแอปพลิเคชันพบว่า สำนักงานได้นำเอาแอปพลิเคชันมาใช้เพื่อดำเนินการภายในองค์กร โดยแบ่งออกเป็น ๓ หมวดหมู่ดังต่อไปนี้ (๑) แอปพลิเคชันธุรกิจ (Business Applications) (๒) แอปพลิเคชันสนับสนุน (Supporting Applications) และ (๓) ส่วนต่อประสานโปรแกรมประยุกต์ (Application Programming Interface - API) รูปที่ ๑๘ แสดงภาพรวมของแอปพลิเคชันที่ใช้ดำเนินงาน โดยแยกแอปพลิเคชันตามหมวดหมู่

ตารางที่ ๒ แสดงรายการของแปพลิเคชันธุรกิจ ซึ่งอ้างอิงแอปพลิเคชันที่ถูกนำมาใช้เพื่อตอบสนองทางด้านธุรกิจ เช่น งานบริหารทรัพยากรมนุษย์ งานจัดซื้อจัดจ้าง และงานการเงินและบัญชี เป็นต้น โดยแบ่งออกเป็น (๑) แอปพลิเคชันภายในองค์กร เป็นแอปพลิเคชันที่สำนักงานใช้เพื่อดำเนินกิจการภายในองค์กร และ (๒) แอปพลิเคชันภายนอกองค์กร เป็นแอปพลิเคชันที่สำนักงานใช้เพื่อรายงานผลการดำเนินงานและงบประมาณต่อภาครัฐ ตารางที่ ๓ แสดงรายการของแอปพลิเคชันสนับสนุน ซึ่งอ้างถึงแอปพลิเคชันที่ใช้เพื่องานสนับสนุน ถูกแบ่งออกเป็น ๔ ประเภทประกอบไปด้วย (๑) Software Enginnering-ซอร์ฟแวร์ที่เกี่ยวข้องกับการพัฒนาแอปบพิลเคชันรวมไปถึงฐานข้อมูล (๒) Network (๓) Security และ (๔) Supporting ตารางที่ ๔ แสดงรายการของ API ซึ่งอ้างถึง Software Component หรือ Web Service ที่ใช้เป็นตัวกลางในการเชื่อมโยงข้อมูลระหว่างแอปพลิเคชัน



รูปที่ ๑๘ ภาพรวมของแอปพลิชันที่ใช้สำหรับการดำเนินงาน

ประเภท	ชื่อแอปพลิเคชัน	รายละเอียด
๑๙ Business Applications ภายในองค์กร	Human Resource Management System	แอปพลิเคชันที่บริหารจัดการงานทรัพยากรบุคคล ครอบคลุมงานในด้านข้อมูลของเจ้าหน้าที่ เงินเดือน และการอบรม
	Welfare Management System	แอปพลิเคชันที่บริหารทรัพยากรบุคคล ครอบคลุมงานในด้านสวัสดิการต่างๆ ของเจ้าหน้าที่
	Procurement Management System	แอปพลิเคชันที่บริหารจัดการงานจัดซื้อจัดจ้าง
	Financial Management System	แอปพลิเคชันที่บริหารจัดการงานการเงินและบัญชี
	Asset Management System	แอปพลิเคชันที่บริหารจัดการงานพัสดุ ครุภัณฑ์
	Contact Center System	แอปพลิเคชันที่บริหารจัดการงานศูนย์บริการลูกค้า
	Problem Tracking System	แอปพลิเคชันที่บริหารจัดการงานศูนย์บริการลูกค้า
	Customer Management System	แอปพลิเคชันที่บริหารจัดการงานฝ่ายบริการให้คำปรึกษา
	EGA Back-end System	แอปพลิเคชันที่บริหารจัดการเว็บไซต์ของสำนักงาน
	Saraban System	แอปพลิเคชันที่ใช้สำหรับบริหารจัดการ การรับส่งเอกสารและการสั่งการ
	Risk Management System	แอปพลิเคชันที่บริหารจัดการการประเมินความเสี่ยงด้วยตนเองและการควบคุมภายในองค์กร
	Project Tracking System	แอปพลิเคชันที่ใช้ติดตามงานที่ใช้พัฒนาแอปพลิเคชัน
	Minute of Meeting System	แอปพลิเคชันที่บริหารจัดการเก็บข้อมูลรายงานการประชุมต่างๆ เช่น รายงานการประชุมฝ่ายบริหาร หรือคณะกรรมการบริหารสำนักงาน
	Operation Center System	แอปพลิเคชันที่บริหารจัดการติดตามผลการดำเนินงานตามยุทธศาสตร์ขององค์กร
	Intranet System	แอปพลิเคชันที่บริหารจัดการระบบงานภายในสำนักงาน
	Knowledge Management System	แอปพลิเคชันที่บริหารจัดการองค์ความรู้ภายในสำนักงาน
	Appointment Management System	แอปพลิเคชันที่บริหารจัดการปฏิทินการนัดหมายภายในสำนักงาน
	ISO Document System	แอปพลิเคชันที่บริหารจัดการการเอกสารตามมาตรฐาน ISO
	Document Management System	แอปพลิเคชันที่บริหารจัดการเอกสารที่นำเสนอต่อคณะกรรมการบริหารสำนักงาน
๗ Business Applications ภายภายนอกองค์กร	ระบบการจัดซื้อจัดจ้างภาครัฐ (e-GP)	ใช้สำหรับรายงานข้อมูลคณะกรรมการ ผู้ขาย ผู้สั่งซื้อ รายละเอียดการส่งมอบงาน ต่อกรมบัญชีกลาง
	ระบบศูนย์กำกับดูแลการจัดซื้อจัดจ้างภาครัฐ	ใช้สำหรับรายงานข้อมูลสัญญาการจัดซื้อจัดจ้างภาครัฐ ต่อสำนักงานคณะกรรมการป้องกันและปราบปรามการทุจริตแห่งชาติ
	ระบบการจัดการงบประมาณอิเล็กทรอนิกส์ (e-budgetting)	ใช้สำหรับรายงานงบประมาณที่ขอ ต่อสำนักงบประมาณ
	ะบบสารสนเทศเพื่อการติดตามและประเมินผล (PART)	ใช้สำหรับรายงานงบประมาณที่ใช้ไป ต่อสำนักงบประมาณ
	ระบบรายงานผลการปฏิบัติราชการตามคำรับรองการปฏิบัติราชการทางอิเล็กทรอนิกส์ (e-SAR)	ใช้สำหรับรายงานผลการดำเนินงานขององค์กร ต่อสำนักงานคณะกรรมการพัฒนาระบบราชการ (ก.พ.ร.)
	ระบบศูนย์ปฏิบัติการกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร (MOC)	ใช้สำหรับรายงานผลการดำเนินงานขององค์กร ต่อกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร
	ระบบการวิเคราะห์ความเสี่ยงตามหลักธรรมาภิบาล	ใช้สำหรับรายงานข้อมูลแผนงาน/โครงการ และวงเงินงบประมาณเพื่อใช้วิเคราะห์ความเสี่ยงตามหลักธรรมาภิบาล ต่อสำนักงบประมาณ

ตารางที่ ๒ รายการของแอปพลิเคชันธุรกิจ

ประเภท	ชื่อแอปพลิเคชัน	รายละเอียด
Software Engineering	Software Development Tools	ใช้เป็นเครื่องมือในการพัฒนาแอปพลิเคชัน
	Database Management and Data Integration Tools	ใช้สำหรับบริหารจัดการฐานข้อมูลและใช้สหรับการถ่ายโอนถ่ายข้อมูล
	Source Code Management	ใช้สำหรับจัดเก็บ Source Code
	Source Code Security Scanner	ใช้สำหรับวิเคราะห์ Source Code เพื่อค้นหาช่องโหว่ของแอปพลิเคชัน
	Application Performance Monitoring	ใช้สำหรับตรวจสอบประสิทธิภาพการทำงานของแอปพลิเคชัน
	Uptime Monitoring Tools	ใช้สำหรับตรวจสอบความต่อเนื่องของการให้บริการของแอปพลิเคชัน
Network	Network Monitoring Tool	ใช้สำหรับตรวจสอบและติดตามการใช้งาน Network
	Traffic Management Tool	ใช้สำหรับการควบคุมปริมาณการใช้งาน Network
	Virtual Private Network (VPN) Software	ใช้สำหรับบริหารจัดการ VPN
	Telephone System	ใช้สำหรับบริหารจัดการ Telephone ซึ่งใช้ติดต่อระหว่างลูกค้ากับศูนย์บริการลูกค้า
	IP Phone System	ใช้สำหรับบริหารจัดการ IP Phone ซึ่งใช้ภายในสำนักงาน
Security	Antivus	ใช้สำหรับ ป้องกัน ตรวจจับ และกำจัดโปรแกรมคุกคามทางคอมพิวเตอร์
	Active Directory (AD)	ใช้สำหรับการควบคุมสิทธิ์การเข้าถึงเครื่อง Desktop Computer สิทธิ์การใช้งาน File Sharing และสิทธิ์การใช้งาน Internet
	Lightweight Directory Access Protocol (LDAP) สำหรับอีเมล	ใช้สำหรับการควบคุมสิทธิ์การเข้าถึงและใช้งานอีมล
	Lightweight Directory Access Protocol (LDAP) สำหรับ OpenID	ใช้สำหรับการควบคุมสิทธิ์การใช้งานแอปพลิเคชัน เช่นระบบ Intranet
	Log management Tool	ใช้สำหรับบริหารจัดการ Log จาก Servers, Firewall และ Network Devices
	Two-Factor Authentication Software	ใช้สำหรับตรวจสอบสิทธิ์การใช้งานอินเทอร์เน็ต
	Vulnerability Scanner	ใช้สำหรับตรวจหาช่องโหว่ของแอปพลิเคชัน
	Security Monitoring Tool	ใช้สำหรับตรวจหาช่องโหว่ของ Network Devices
	Firewall Management Tool	ใช้สำหรับบริหารจัดการ Firewall
	Firewall Monitoring Tool (Capacity)	ใช้สำหรับตรวจสอบปริมาณการใช้งาน CPU และ Memory ของ Firewall
	Firewall Monitoring Tool (Availability)	ใช้สำหรับตรวจสอบความพร้อมใช้ของ Firewall
Supporting	Office Suite	เป็นชุดซอฟต์แวร์สำหรับงานทั่วไป ประกอบไปด้วยงานเอกสาร งานนำเสนอ งานคำนวณ งานฐานข้อมูล และงานไดอะแกรม
	Webmail	ใช้สำหรับอ่านหรือส่งอีเมลผ่าน Webbroswer
	Mobile Email	ใช้สำหรับอ่านหรือส่งอีเมลผ่าน Smart Phone
	Email Server Software	ใช้สำหรับให้บริการในการรับส่งอีเมล
	Cloud Management	ใช้สำหรับบริหารจัดการผลิตภัณฑ์หรือบริการ

ตารางที่ ๓ รายการของแอปพลิชันสนับสนุน

ชื่อ API	รายละเอียด
OpenID	เป็นระบบ Single Sign On สำหรับการกำหนดสิทธิ์การเข้าถึงหลายแอปพลิเคชันด้วย ชื่อผู้ใช้งาน (User Name) เดียว

ตารางที่ ๔ รายการของ API

ตารางที่ ๕ แสดงความสัมพันธ์ระหว่างแอปพลิเคชันกับเทคโนโลยี ซึ่งเทคโนโลยีแบ่งออกเป็นเทคโนโลยีภาษาในการพัฒนาแอปพลิเคชัน เทคโนโลยี Single-Sign-On เทคโนโลยี Cloud Computing c]t เทคโนโลยีการพัฒนาแอปพลิเคชันประกอบ (Web Application Desktop Application และ Mobile Application)

ความสัมพันธ์ระหว่างแอปพลิเคชันกับเทคโนโลยี		เทคโนโลยี การพัฒนาแอปพลิเคชัน																	
		Web Application												Desktop Application					
		EGA Contact Center	Problem Tracking	Customer Mgt.	EGA Back-end	Saraban	Risk Mgt.	Operation Center	Intranet*	Knowledge Mgt.	Appointment Mgt.	ISO Document	Document Mgt.	Project Tracking	Human Resource Mgt.	Welfare Mgt.	Financial Mgt.	Procurement Mgt.	Asset Mgt.	Minute of Meeting
เทคโนโลยี ภาษาในการพัฒนาแอปพลิเคชัน	ASP.NET	X	X	X	X	X		X	X	X					X					
	ASP								X			X								
	PHP						X				X									
	VBA																			X
	JAVA												X							
	Ruby													X						
	Java Android								X											
	Objective C								X											
	ซอฟต์แวร์สำเร็จรูป															X	X	X	X	
Single Sign-On (OpenID)		X	X		X	X	X	X	X	X	X	X		X						
Private Cloud		X	X	X	X	X	X	X	X	X	X	X	X	X						

ตารางที่ ๕ ตารางความสัมพันธ์ระหว่างแอปพลิเคชันกับเทคโนโลยี

ตารางที่ ๖ แสดงความสัมพันธ์ระหว่างแอปพลิเคชันธุรกิจภายในองคกรและส่วนงานของสำนักงาน จากตารางจะเห็นว่ายังมีหลายส่วนงานที่ไม่ได้มีการนำเอาแอปพลิเคชันมาใช้เพื่อดำเนินงาน เช่น ส่วนนโยบายรัฐบาลอิเล็กทรอนิกส์ ส่วนประสานความร่วมมือ และ ฝ่ายนวัตกรรม เป็นต้น ตารางที่ ๗ แสดงความสัมพันธ์ระหว่างแอปพลิเคชันสนับสนุนและส่วนงานของสำนักงาน ตารางที่ ๘ แสดงความสัมพันธ์ระหว่างแอปพลิเคชันภายในองค์กรกับกระบวนการปฏิบัติงานของสำนักงานจากตารางจะเห็นว่ายังมีหลายหมวดกระบวนที่ไม่ได้มีการนำเอาแอปพลิเคชันมาใช้เพื่อดำเนินงาน เช่น หมวดวิจัยตลาด หมวดวิจัยและพัฒนาผลิตภัณฑ์/บริการ และ กระบวนการบริหารการเปลี่ยนแปลง เป็นต้น ตารางที่ ๙ แสดงความสัมพันธ์ระหว่างแอปพลิเคชันภายนอกและแอปพลิเคชันภายในสำนักงาน จากตารางพบว่ามี ๒ แอปพลิเคชันภายในองค์การที่มีความสัมพันธ์กับแอปพลิเคชันภายนอก อย่างไรก็ตามแอปพลิเคชันของสำนักงาน เหล่านี้ยังไม่รองรับการเชื่อมโยงกับแอปพลิเคชันภายนอก

แอปพลิเคชัน/ส่วนงาน	PSP	PSS	PSC	PSR	INR	INA	INS	CSB	CSM	CSK	CSI	CSP	CST	CSC	ENI	ENM	ENS	ENT	AD	ADD1	ADD2	ADQ	ADM	CMF	CMH	CMG	CMP	CMD	ODS	ODI	ODL	Vendor
	ฝ่ายนโยบายและยุทธศาสตร์														ฝ่ายวิศวกรรมและปฏิบัติการ				ฝ่ายพัฒนาและจัดการแอปพลิเคชัน					ฝ่ายบริหารประสิทธิภาพองค์กร					ฝ่ายอำนวยการ			
	ส่วนนโยบายรัฐบาลอิเล็กทรอนิกส์	ส่วนยุทธศาสตร์	ส่วนประสานความร่วมมือ	ส่วนบริหารความเสี่ยง	ส่วนวิจัยและพัฒนา	ส่วนสถาปัตยกรรมและต้นแบบ	ส่วนมาตรฐาน	ส่วนพัฒนาธุรกิจ	ส่วนการตลาดและการสื่อสาร	ส่วนจัดการความรู้และสารสนเทศ	ส่วนที่ปรึกษาเทคโนโลยีสารสนเทศ	ส่วนบริหารโครงการ	ส่วนถ่ายทอดเทคโนโลยี	ส่วนศูนย์บริการลูกค้า	ส่วนโครงสร้างพื้นฐานสารสนเทศ	ส่วนระบบสารสนเทศ	ส่วนความมั่นคงปลอดภัยสารสนเทศ	ส่วนสนับสนุนและบริการด้านเทคนิค	ฝ่ายพัฒนาและจัดการแอปพลิเคชัน	ส่วนพัฒนาแอปพลิเคชัน 1	ส่วนพัฒนาแอปพลิเคชัน 2	ส่วนจัดการแอปพลิเคชัน	ส่วนจัดการคุณภาพ	ส่วนการเงินและบัญชี	สวนบริหารทรัพยากรบุคคล	บริหารงานทั่วไปและอานวยการ	ส่วนจัดซื้อและพัสดุ	ส่วนพัฒนาองค์กร	ส่วนสนับสนุนการผู้บริหาร	ส่วนวิเคราะห์และจัดเตรียมข้อมูล	ส่วนกฎหมาย	
Human Resource Mgt.																									■								■
Welfare Mgt.																									■								■
Procurement Mgt.																												■					■
Financial Mgt.																								■									■
Asset Mgt.																												■					■
Contact Center														■																			■
Problem Tracking														■				■	■														
Customer Mgt.								■	■	■	■	■	■	■																			
EGA Back-end										■			■						■						■		■						
Saraban																			■											■			
Risk Mgt.				■																													■
Project Tracking																			■	■	■	■	■										
Minute of Meeting																															■		
Operation Center		■																	■														
Intranet																			■														
- การลา																									■								
- ลงเวลา																									■								
- ขอหนังสือรับรอง																									■								
- สมัครกองทุนสำรองเลี้ยงชีพ																									■								
- เบิกวัสดุ																										■							
- จองรถตู้																										■							
- จองห้องประชุม																										■							
- แจ้งซ่อม																										■							
- ขอทำนามบัตร																										■							
Knowledge Mgt.										■									■														
Appointment Mgt.																			■											■			
ISO Document																			■									■					
Document Mgt.																			■												■		

■ หมายถึง ส่วนงานที่ใช้แอปพลิเคชันเพื่อดำเนินงานตามกระบวนการที่รับผิดชอบ
■ หมายถึง ส่วนงานที่พัฒนาและดูแลแอปพลิเคชัน
■ หมายถึง ส่วนงานที่ใช้ดำเนินการ พัฒนาและดูแลแอปพลิเคชัน

ตารางที่ ๖ ตารางความสัมพันธ์ระหว่างแอปพลิเคชันธุรกิจและส่วนงาน

ตารางที่ ๗ ตารางความสัมพันธ์ระหว่างแอปพลิเคชันสนับสนุนและส่วนงาน

รหัส	หมวดกระบวนการ/ แอปพลิเคชัน	Human Resource Mgt.	Welfare Mgt.	Procurement Mgt.	Financial Mgt.	Asset Mgt.	Contact Center	Problem Tracking	Customer Mgt.	EGA Back-end	Saraban	Risk Mgt.	Project Tracking	Minute of Meeting	Operation Center	Intranet	Knowledge Mgt.	Appointment Mgt.	ISO Document	Document Mgt.
	Marketing/Planning																			
PC-C01	กำหนดนโยบายรัฐบาลอิเล็กทรอนิกส์									■										
PC-C02	กำหนดยุทธศาสตร์และแผนกลยุทธ์														■					
PC-C03	วิจัยตลาด																			
PC-C04	บริหารการตลาด								■											
	Research and Development																			
PC-C05	วิจัยและพัฒนาผลิตภัณฑ์/บริการ																			
PC-C06	จัดทำต้นแบบและมาตรฐาน																			
	Build, Acquire and Implement																			
PC-C07	วิเคราะห์และออกแบบบริการ/ผลิตภัณฑ์								■											
PC-C08	บริหารโครงการผลิตภัณฑ์/บริการ ช่วงพัฒนา								■				■							
PC-C09	พัฒนาผลิตภัณฑ์/บริการช่วงพัฒนา								■											
PC-C10	ผลิตภัณฑ์/บริการช่วงพัฒนา								■											
	Sell,Deliver, Service and Support																			
PC-C11	บริการการขาย			■	■	■	■		■	■									■	
PC-C12	บริหารโครงการ								■				■							
PC-C13	ออกแบบ ควบคุมผลิตภัณฑ์/บริการ								■											
PC-C14	บริหารหลังการขาย						■	■	■											
	Internal Support																			
PC-S01	บริหารและพัฒนาบุคลากร	■	■													■				
PC-S02	บริหารงานจัดซื้อจัดจ้าง			■		■														
PC-S03	บริหารงานพัสดุ					■										■				
PC-S04	บริหารสำนักงาน															■				
PC-S05	กระบวนการบริการเงินและบัญชี				■															
PC-S06	บริหารเทคโนโลยีสารสนเทศและการสื่อสาร						■	■												
PC-S07	บริหารลูกค้าสัมพันธ์								■											
PC-S08	งานประชาสัมพันธ์																			
PC-S09	บริหารความมั่นคง ปลอดภัยระบบสารสนเทศ						■	■												
PC-S10	กระบวนการบริหารการเปลี่ยนแปลง																			
PC-S11	บริหารองค์ความรู้																■			
PC-S12	กระบวนการบริหารฝ่ายอำนวยการ													■				■	■	■
PC-S13	บริหารงานแผนนโยบายและงบประมาณ														■					
PC-S14	บริหารความเสี่ยง											■								
PC-S15	กระบวนการบริหารงานสารบรรณ										■									
PC-S16	จัดการทรัพย์สินทางปัญญา																			
PC-S17	การพัฒนาองค์กร															■				
PC-S22	การจัดการระบบมาตรฐาน																		■	
	Monitor, Evaluate and Assess																			
PC-S18	สำรวจความพึงพอใจการใช้บริการ																			
PC-S19	ประเมินความสอดคล้องกฎหมายและมาตรฐานที่เกี่ยวข้อง											■								
PC-S20	ประเมินผลการให้บริการ																			
PC-S21	การติดตามและตรวจสอบภายใน											■								

ตารางที่ ๘ ตารางความสัมพันธ์ระหว่างแอปพลิเคชันและกระบวนการปฏิบัติงาน

แอปพลิเคชันภายนอกสำนักงาน	แอปพลิเคชันภายในสำนักงาน		ส่วนงานที่รับผิดชอบ	
	แอปพลิเคชัน Procurement Mgt. (จัดซื้อจัดจ้าง)	แอปพลิเคชัน Operation Center (ศูนย์ปฏิบัติการ)	ส่วนงานภายภายนอก	ส่วนงานภายใน สรอ.
ระบบการจัดซื้อจัดจ้างภาครัฐ (e-GP)	ข้อมูลคณะกรรมการ ผู้ขาย ผู้สั่งซื้อ รายละเอียดการส่งมอบงาน		กรมบัญชีกลาง	งานจัดซื้อและพัสดุ
ระบบศูนย์กำกับดูแลการจัดซื้อจัดจ้างภาครัฐ	ข้อมูลสัญญา		สำนักงานคณะกรรมการป้องกันและปราบปรามการทุจริตแห่งชาติ	งานจัดซื้อและพัสดุ
ระบบการจัดการงบประมาณอิเล็กทรอนิกส์ (e-budgetting)		งบประมาณที่ขอ	สำนักงบประมาณ	งานยุทธศาสตร์
ระบบสารสนเทศเพื่อการติดตามและประเมินผล (PART)		งบประมาณที่ใช้ไป	สำนักงบประมาณ	งานยุทธศาสตร์
ระบบรายงานผลการปฏิบัติราชการตามคำรับรองการปฏิบัติราชการทางอิเล็กทรอนิกส์ (e-SAR)		ผลการดำเนินงาน	สำนักงานคณะกรรมการพัฒนาระบบราชการ (ก.พ.ร.)	งานยุทธศาสตร์
ระบบศูนย์ปฏิบัติการกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร (MOC)		ผลการดำเนินงาน	กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร	งานยุทธศาสตร์
ระบบการวิเคราะห์ความเสี่ยงตามหลักธรรมาภิบาล		แผนงาน/โครงการ และวงเงินงบประมาณเพื่อ	สำนักงบประมาณ	งานยุทธศาสตร์

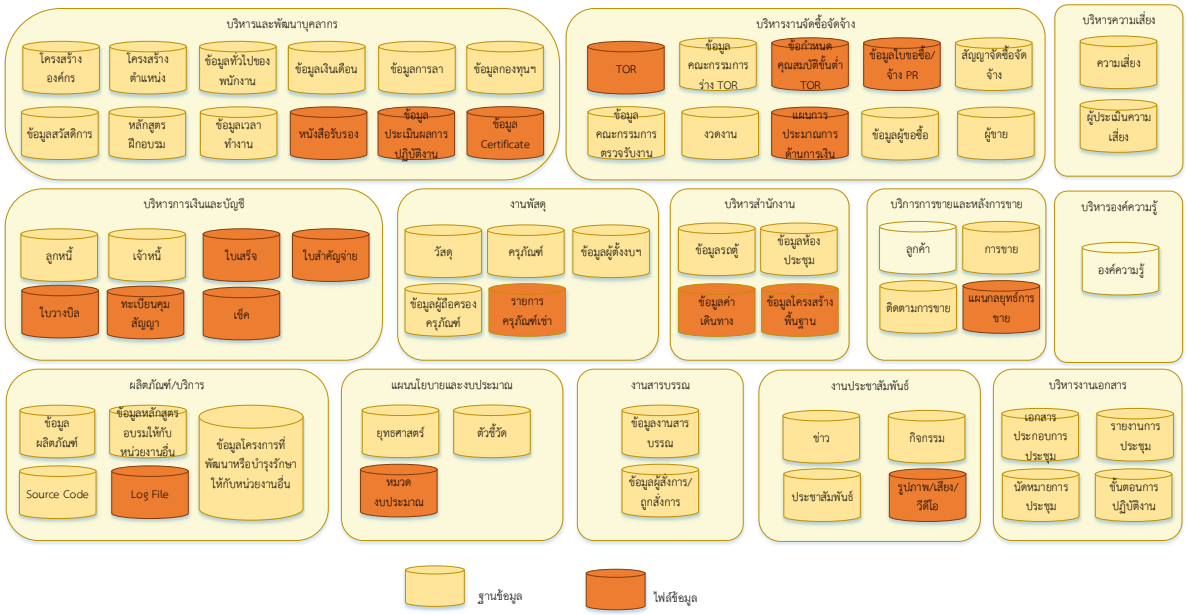
ตารางที่ ๙ ตารางความสัมพันธ์ระหว่างแอปพลิเคชันภายนอกและแอปพลิเคชันภายในสำนักงาน

สรุปประเด็นปัญหาหลักๆ ของด้านแอปพลิเคชัน ตามรายละเอียดดังนี้

1) แอปพลิเคชันที่ใช้ในปัจจุบัน ไม่ได้ครอบคลุมถึงกระบวนการปฏิบัติงานที่สำคัญ เช่น กระบวนการบริหารงานแผนนโยบายและงบประมาณ ขั้นตอนการโอนงบประมาณ เป็นต้น
2) การตอบสนองตามความต้องการสำหรับการใช้งานแอปพลิเคชันในปัจจุบัน บาง แอปพลิเคชันไม่สามารถออกรายงานได้ตามความต้องการและก็ไม่สามารถพัฒนาเพิ่มเติมได้ เช่น ระบบจัดซื้อ/ระบบการเงินและบัญชี (Procurement Management / Financial Management System) ของงานจัดซื้อและพัสดุและส่วนงานการเงินและบัญชี เป็นต้น

๓.๓ ด้านข้อมูล (Data)

จากการสำรวจในด้านข้อมูลสามารถจัดแบ่งประเภทข้อมูลออกเป็น ๑๓ หมวด และแต่ละหมวดแบ่งออกเป็น ๒ หมวดย่อย คือ (๑) ข้อมูลที่จัดเก็บอยู่ในรูปแบบฐานข้อมูลที่มีโครงสร้างหรือมีความสัมพันธ์ชัดเจน (Rational Database) และ (๒) ข้อมูลที่จัดเก็บในแบบไฟล์ เช่น ภาพ เสียง และวีดีโอ เป็นต้น รูปที่ ๑๙ และตารางที่ ๑๐ แสดงภาพรวมของข้อมูลภายในองค์กร และให้รายละเอียดของข้อมูลตามลำดับ ตารางที่ ๑๑ แสดงให้เห็นว่าแต่ละแอปพลิเคชันมีความสัมพันธ์กับข้อมูลใดบ้าง ตารางที่ ๑๒ แสดงความสัมพันธ์ระหว่างข้อมูล ฐานข้อมูล และเครื่องที่เก็บฐานข้อมูล และรูปที่ ๒๙ แสดงให้เห็นถึงภาพรวามความเชื่อมโยงข้อมูลกับ โครงสร้างพื้นฐาน แอปพลิชัน และธุรกิจ



รูปที่ ๑๙ ภาพรวมของข้อมูลภายในองค์กร

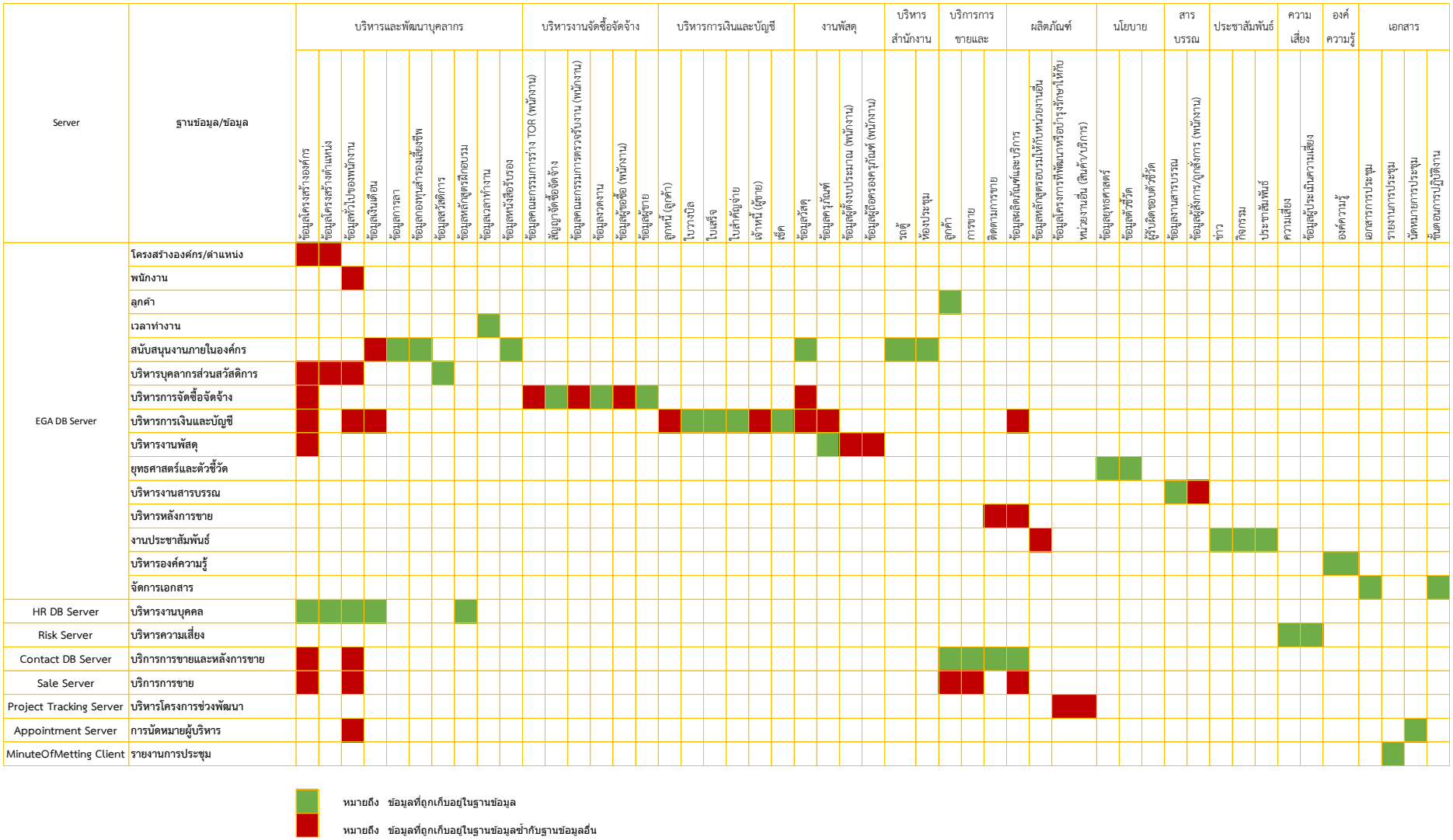
ข้อมูล	ข้อมูลย่อย	รายละเอียด	ฐานข้อมูล
บริหารและพัฒนาบุคลากร	ข้อมูลโครงสร้างองค์กร	ชื่อส่วนงาน ชื่อส่วนงานระดับเหนือกว่า	✓
	ข้อมูลโครงสร้างตำแหน่ง	ชื่อตำแหน่ง ชื่อตำแหน่งระดับเหนือกว่า	✓
	ข้อมูลทั่วไปของพนักงาน	ชื่อ นามสกุล ที่อยู่ เบอร์โทรศัพท์ อีเมล ความสามารถ	✓
	ข้อมูลเงินเดือน	เงินเดือน เกณฑ์การจ่ายเงินเดือน	✓
	ข้อมูลการลา	วันที่ลา เวลาที่ลา ประเภทการลา	✓
	ข้อมูลกองทุนสำรองเลี้ยงชีพ	ประเภทกองทุน อัตราสะสมของลูกจ้าง อัตราสะสมของนายจ้าง	✓
	ข้อมูลสวัสดิการ	ชื่อสวัสดิการ เกณฑ์การได้รับสิทธิ์	✓
	ข้อมูลหลักสูตรฝึกอบรม	ชื่อหลักสูตรฝึกอบรม รายละเอียด ค่าใช้จ่าย	✓
	ข้อมูลเวลาทำงาน	เวลาเข้างาน เวลาออกจากงาน	✓
	ข้อมูลหนังสือรับรอง	เลขที่ เรื่อง วันที่ รายละเอียด	✓
	ข้อมูลประเมินผลการปฏิบัติงาน	ปีงบฯที่ประเมิน ชื่อผู้ประเมิน งานที่ดำเนินการ	✗
	ข้อมูล Certificate	ชื่อใบ Certificate กลุ่ม Certificate	✗
บริหารงานจัดซื้อจัดจ้าง	ข้อมูล TOR	เรื่อง ความเป็นมา วัตุประสงค์ ขอบเขต วงเงิน	✗
	ข้อมูลคณะกรรมการร่าง TOR	ชื่อ นามสกุล ที่อยู่ เบอร์โทรศัพท์	✓
	ข้อมูลข้อกำหนดคุณสมบัติขั้นต่ำ	ชื่อโครงการ ขอบเขตงาน งวดงาน กำหนดการส่งมอบ รายละเอียด	✗
	ข้อมูลใบขอซื้อ/จ้าง PR	ชื่อ นามสกุล ที่อยู่ เบอร์โทรศัพท์ เรื่องการขอจัดซื้อจัดจ้าง รหัสงบประมาณ	✗
	สัญญาจัดซื้อจัดจ้าง	ชื่อบริษัท/หน่วยงาน ที่อยู่ เบอร์โทรศัพท์ อีเมล ชื่อผู้รับจ้าง กำหนดการส่ง	✓
	ข้อมูลคณะกรรมการตรวจรับงาน	ชื่อ นามสกุล ที่อยู่ เบอร์โทรศัพท์	✓
	ข้อมูลงวดงาน	เลขที่ PR เลขที่สัญญา กรรมการตรวจรับ รายละเอียดส่งมอบงาน ผู้ชาย ผู้	✓
	แผนการประมาณด้านการเงินราย	งวดงาน มูลค่า กำหนดการส่งมอบ ค่าใช้จ่าย	✗
	ข้อมูลผู้ขอซื้อ	ชื่อ นามสกุล ที่อยู่ เบอร์โทรศัพท์	✓
	ข้อมูลผู้ขาย	ชื่อบริษัท/หน่วยงาน ที่อยู่ เบอร์โทรศัพท์ อีเมล ชื่อผู้ติดต่อ	✓
บริหารการเงินและ	ลูกหนี้	ชื่อบริษัท/หน่วยงาน ที่อยู่ เบอร์โทรศัพท์ อีเมล ชื่อบริการ	✓
	ใบวางบิล	ชื่อบริษัท/หน่วยงาน ที่อยู่ เบอร์โทรศัพท์ อีเมล ชื่อบริการ ค่าบริการ	✓
	ใบเสร็จ	ชื่อบริษัท/หน่วยงาน ที่อยู่ เบอร์โทรศัพท์ อีเมล ชื่อบริการ ค่าบริการ	✓

	ใบสำคัญจ่าย	ชื่อบริษัท/หน่วยงาน ที่อยู่ เบอร์โทรศัพท์ อีเมล ชื่อธนาคาร เลขที่เช็ค	✓
	เจ้าหนี้	ชื่อบริษัท/หน่วยงาน ที่อยู่ เบอร์โทรศัพท์ อีเมล ชื่อบริการ	✓
	เช็ค	ชื่อบริษัท/หน่วยงาน ที่อยู่ เบอร์โทรศัพท์ อีเมล ชื่อธนาคาร เลขที่เช็ค	✓
	ทะเบียนคุมสัญญา	ชื่อสัญญา งวดงาน ชื่อบริษัท/หน่วยงาน	✗
งานพัสดุ	ข้อมูลวัสดุ	ชื่อวัสดุ ราคา	✓
	ข้อมูลครุภัณฑ์	ชื่อครุภัณฑ์ ราคา	✓
	ข้อมูลผู้ตั้งงบประมาณ	ชื่อ นามสกุล ที่อยู่ เบอร์โทรศัพท์ อีเมล	✓
	ข้อมูลผู้ถือครองครุภัณฑ์	ชื่อ นามสกุล ที่อยู่ เบอร์โทรศัพท์ อีเมล	✓
	ข้อมูลครุภัณฑ์ที่เช่า	ชื่อครุภัณฑ์ ราคา ช่วงเวลาที่เช่า ราคา	✗
บริหารสำนักงาน	รถตู้	ชื่อคนขับรถตู้ ทะเบียนรถ พ.ร.บ.คุ้มครองผู้ประสบภัยจากรถ	✓
	ห้องประชุม	ชื่อห้องประชุม หมายเลขโทรศัพท์	✓
	โครงสร้างพื้นฐาน	ชื่อโครงสร้างพื้นฐาน รายละเอียด	✗
	ค่าเดินทาง	ระยะทาง ค่าเดินทาง	✗
การขายและหลังการขาย	ลูกค้า	ชื่อบริษัท/หน่วยงาน ที่อยู่ เบอร์โทรศัพท์ อีเมล ชื่อผู้ติดต่อ	✓
	การขาย	เลขโครงการ ชื่อบริการ ข้อมูลที่ลูกค้าขอใช้บริการ	✓
	ติดตามการขาย	เลขโครงการ ชื่อบริการ สถานะการขาย	✓
	แผนกลยุทธ์การขาย	รายละเอียดแผนกลยุทธ์การขาย	✗
ผลิตภัณฑ์และบริการ	ข้อมูลผลิตภัณฑ์และบริการ	ชื่อบริการ (เช่น G-CERT MailGoTh GIN และ Cloud) รายละเอียด	✓
	ข้อมูลหลักสูตรอบรมให้กับ	ชื่อหลักสูตรฝึกอบรม รายละเอียด ค่าใช้จ่าย	✓
	ข้อมูลโครงการที่พัฒนาหรือ	ชื่อโครงการ ระยะเวลาพัฒนา ราคา	✓
	Source Code	Source Code จากการพัฒนาแอปพลิเคชัน	✓
	Log File	Log File จาก CCTV Web Server Mail Server อื่นๆ	✗
แผนนโยบายและงบประมาณ	ข้อมูลยุทธศาสตร์	ยุทธศาสตร์ ๔ ปี กลยุทธ์ประจำปี	✓
	ข้อมูลตัวชี้วัด	ตัวชี้วัดยุทธศาสตร์ ๔ ปี ตัวชี้วัดกลยุทธ์ประจำปี เกณฑ์การให้คะแนน ระดับ	✓
	ข้อมูลผู้รับผิดชอบตัวชี้วัด	ชื่อ นามสกุล ที่อยู่ เบอร์โทรศัพท์ อีเมล	✓
	ข้อมูลงบประมาณ	หมวดงบประมาณ งบประมาณที่ได้รับ	✗
สารบรรณ	ข้อมูลงานสารบรรณ	เลขที่ เรื่อง วันที่ รายละเอียด	✓
	ข้อมูลผู้สั่งการ/ถูกสั่งการ	ชื่อ นามสกุล ที่อยู่ เบอร์โทรศัพท์ อีเมล	✓
งานประชาสัมพันธ์	ข่าว	หัวข้อข่าว วัน เวลาประกาศ รายละเอียด	✓
	กิจกรรม	ชื่อกิจกรรม วัน เวลา รายละเอียด	✓
	ประชาสัมพันธ์	เรื่องประชาสัมพันธ์ วัน เวลา รายละเอียด	✓
	รูปภาพ/เสียง/วีดีโอ	ไฟล์ รูปภาพ/เสียง/วีดีโอ	✗
ความเสี่ยง	ความเสี่ยง	ข้อมูลทรัพย์สิน ผู้รับผิดชอบ ระดับความเสี่ยง แนวทางแก้ไข	✓
	ข้อมูลผู้ประเมินความเสี่ยง	ชื่อ นามสกุล ที่อยู่ เบอร์โทรศัพท์ อีเมล	✓
องค์ความรู้	องค์ความรู้	เรื่อง วัน เวลาประกาศ ชื่อผู้ประกาศ รายละเอียด	✓
บริหารงานเอกสาร	เอกสารการประชุม	เลขที่ หัวเรื่อง วัน เวลา รายละเอียด เช่นเอกสารประกอบการประชุม	✓
	รายงานการประชุม	เลขที่ หัวเรื่อง วัน เวลา รายละเอียด เช่นรายงานการประชุม	✓
	นัดหมายการประชุม	หัวเรื่อง รายละเอียด ผู้เข้าร่วมประชุม ผู้นัดหมายการประชุม	✓
	ขั้นตอนการปฏิบัติงาน	เลขที่ ชื่อขั้นตอน รายละเอียด	✓

ตารางที่ ๑๐ รายการข้อมูล

ฐานข้อมูล/ข้อมูล	บริหารและพัฒนาบุคลากร										บริหารงานจัดซื้อจัดจ้าง						บริหารการเงินและบัญชี						งานพัสดุ				บริหารสำนักงาน		บริการการขายและ			ผลิตภัณฑ์			นโยบาย			สารบรรณ		ประชาสัมพันธ์			ความเสี่ยง		องค์ความรู้	เอกสาร			
	ข้อมูลโครงสร้างองค์กร	ข้อมูลโครงสร้างตำแหน่ง	ข้อมูลตัวโปรของพนักงาน	ข้อมูลเงินเดือน	ข้อมูลการลา	ข้อมูลกองทุนสำรองเลี้ยงชีพ	ข้อมูลสวัสดิการ	ข้อมูลหลักสูตรฝึกอบรม	ข้อมูลเวลาทำงาน	ข้อมูลหนังสือรับรอง	ข้อมูลคณะกรรมการร่าง TOR (พนักงาน)	สัญญาจ้างซื้อจัดจ้าง	ข้อมูลคณะกรรมการตรวจรับงาน (พนักงาน)	ข้อมูลงวดงาน	ข้อมูลผู้ขาย (พนักงาน)	ข้อมูลผู้ขาย	ลูกหนี้ (ลูกค้า)	ใบวางบิล	ใบเสร็จ	ใบสำคัญจ่าย	เจ้าหนี้ (ผู้ขาย)	เช็ค	ข้อมูลวัสดุ	ข้อมูลครุภัณฑ์	ข้อมูลผู้ดูแลงบประมาณ (พนักงาน)	ข้อมูลผู้ถือครองครุภัณฑ์ (พนักงาน)	รถตู้	ห้องประชุม	ลูกค้า	การขาย	ติดตามการขาย	ข้อมูลผลิตภัณฑ์และบริการ	ข้อมูลหลักสูตรอบรมให้กับหน่วยงานอื่น	ข้อมูลโครงการพัฒนาหรือปรับรุงรักษาให้กับหน่วยงานอื่น (สินค้า/บริการ)	ข้อมูลนโยบายคุณธรรม	ข้อมูลตัวชี้วัด	ผู้รับผิดชอบตัวชี้วัด	ข้อมูลงานสารบรรณ	ข้อมูลผู้ส่งการ/ผู้ปฏิสั่งการ (พนักงาน)	ข่าว	กิจกรรม	ประชาสัมพันธ์	ความเสี่ยง	ข้อมูลประเมินความเสี่ยง	องค์ความรู้	เอกสารประชุม	รายงานการประชุม	นัดหมายการประชุม	ข้อตกลงการปฏิบัติงาน
Human Resource Mgt.	■	■	■	■				■																																							
Welfare Mgt.	■	■	■				■																																								
Procurement Mgt.	■										■	■	■	■	■	■							■																							
Financial Mgt.	■		■	■													■	■	■	■	■	■	■	■								■														
Asset Mgt.	■																							■	■	■																				
EGA Contact Center	■		■																										■	■	■	■														
Problem Tracking	■		■																												■	■														
Customer Mgt.	■		■																										■	■		■														
EGA Back-end	■		■																														■					■	■	■						
Saraban	■																																					■	■							
Risk Mgt.	■																																		■	■						■	■			
Operation Center	■		■							■																							■			■	■									
Intranet	■		■	■	■	■				■													■				■	■																	
Knowledge Mgt.	■		■																																								■			
Appointment Mgt.			■																																									■		
ISO Document	■		■																																										■	■
Document Mgt.	■		■																																									■		■
Minute of Meeting																																												■		
Project Tracking			■																														■	■												

ตารางที่ ๑๑ ตารางความสัมพันธ์ระหว่างข้อมูลและแอปพลิเคชัน



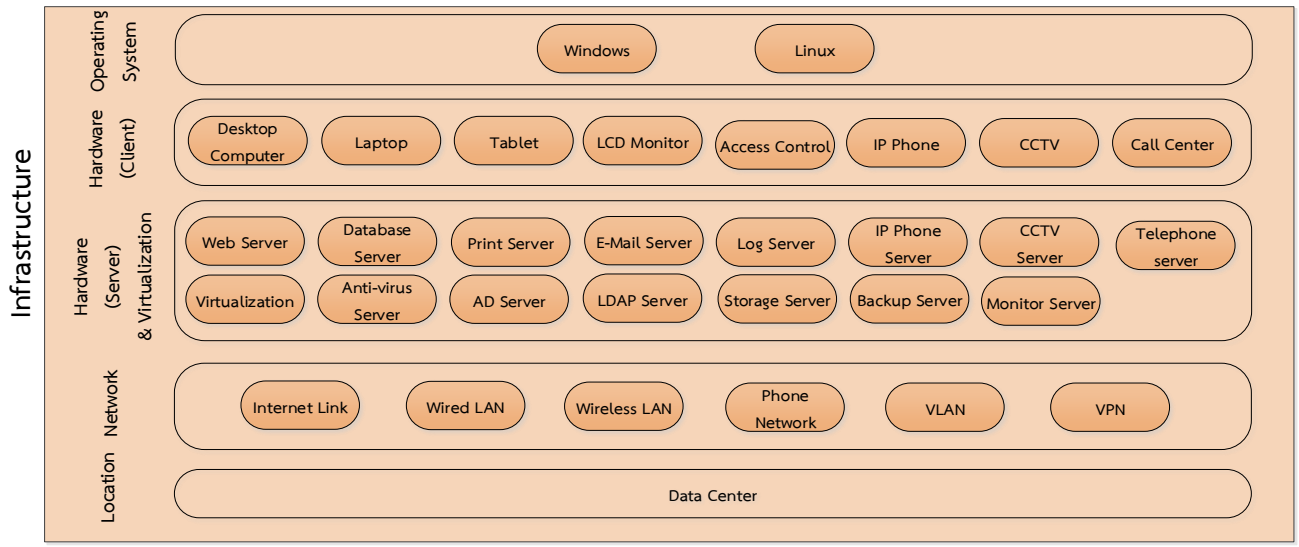
ตารางที่ ๑๒ ตารางความสัมพันธ์ระหว่างข้อมูล ฐานข้อมูล และเครื่องที่เก็บฐานข้อมูล

จากผลการสำรวจด้านข้อมูลดังกล่าว พบว่ายังไม่มีการจัดเก็บข้อมูลที่เป็นมาตรฐานเดียวกัน ขาดความเชื่อมโยงด้านข้อมูลภายใน มีการจัดเก็บข้อมูลที่ซ้ำซ้อน และข้อมูลที่จัดเก็บอาจไม่เป็นปัจจุบัน เนื่องจากการจัดเก็บข้อมูลภายในสรอ.จะจัดเก็บด้วยเครื่องคอมพิวเตอร์และไดรฟ์ส่วนบุคคลเป็นส่วนใหญ่ หรือหากมีการใช้งานข้อมูลร่วมกันภายในส่วนงานจะจัดข้อมูลนั้นไว้ที่ไดรฟ์กลางหรือบนแอปพลิเคชันของส่วนงานนั้นๆ การเชื่อมโยงด้านข้อมูลภายในจะเกิดขึ้นกับบางแอปพลิเคชันที่พัฒนาโดยทีมพัฒนาภายในสรอ. โดยสรุปประเด็นปัญหาหลักๆ และข้อเสนอแนะได้ดังนี้

1) การจัดเก็บข้อมูลภายในสรอ. ที่ซ้ำซ้อนกันอาจเกิดจาก ไม่มีการจัดเก็บข้อมูลกลางที่เป็นมาตรฐานเดียวกัน ส่งผลให้ขาดความเชื่อมโยงด้านข้อมูล การใช้งานข้อมูลประเภทเดียวกันต้องบันทึกข้อมูลซ้ำซ้อน เช่น งานบริหารทรัพยากรบุคคล มีหลายแอปพลิเคชันที่ช่วยในการปฏิบัติงานภายในส่วนงาน แต่ข้อมูลไม่มีความเชื่อมโยงกันส่งผลให้หากมีการเปลี่ยนแปลงหรือแก้ไขข้อมูล ต้องบันทึกข้อมูลใหม่ในแต่ละแอปพลิเคชันที่ใช้งานอยู่ เป็นต้น
2) ขาดผู้รับผิดชอบข้อมูลที่ใช้งานร่วมกัน ส่งผลให้ข้อมูลไม่ได้รับการทบทวน เปลี่ยนแปลงหรือแก้ไขให้เป็นปัจจุบัน เช่น ข้อมูลลูกค้ามีการจัดเก็บทั้งในแอปพลิเคชันของศูนย์บริการลูกค้า และในระบบ Customer Management ของงานบริการให้คำปรึกษา เป็นต้น
3) ข้อมูลถูกจัดเก็บในหลายประเภท ทั้งกระดาษและสื่ออิเล็กทรอนิกส

๓.๔ ด้านโครงสร้างพื้นฐาน (Infrastructure)

โครงสร้างพื้นฐาน (Infrastructure) ถูกนำไปใช้เพื่อสนับสนุนการดำเนินงานในด้านต่างๆ ทั้งด้าน ธุรกิจ แอพลิเคชัน ข้อมูล และความมั่นคงปลอดภัย โครงสร้างพื้นฐานถูกแบ่งออกเป็นหมวดหมู่ดังต่อไปนี้ (๑) Operating System (๒) Hardware ซึ่งแบ่งออกเป็น Client และ Server & Vertualization (๓) Network และ (๔) Facility รูปที่ ๒๐ และ ตารางที่ ๑๓ แสดงภาพรวมและรายการโครงสร้างพื้นฐานตามลำดับ



รูปที่ ๒๐ ภาพรวมของโครงสร้างพื้นฐาน

ประเภท	รายการ	รายละเอียด
Operating System	Windows	เป็นระบบปฏิบัติการของบริษัท Microsoft ซึ่งมีใช้งานในสำนักงานแบ่งออกเป็น ๒ ประเภทคือ ๑) เพื่อติดตั้งลงบนเครื่อง Desktop Computer สำหรับทำงานทั่วไป เช่นงานเอกสาร งานตัดต่อวีดีโอ หรือใช้สำหรับเป็น Thin Client เพื่อทำงานร่วมกับ Server Computer ๒) เพื่อติดตั้งลงบนเครื่อง Server Computer สำหรับงานบริการ เช่น เว็บและอีเมล
	Linux	เป็นระบบปฏิบัติการ Open Source ซึ่งมีใช้งานในสำนักงานแบ่งออกเป็น ๒ ประเภทคือ ๑) เพื่อติดตั้งลงบนเครื่อง Desktop Computer เป็น Thin Client เพื่อ Config อุปกรณ์ Network ๒) เพื่อติดตั้งลงบนเครื่อง Server Computer สำหรับงานบริการ เช่น LDAP
Hardware (Client)	Desktop Computer	คอมพิวเตอร์ตั้งโต๊ะ(Desktop computer) เป็นเครื่องคอมพิวเตอร์สำหรับทำงานทั่วไป เช่นงานเอกสาร งานตัดต่อวีดีโอ หรือใช้สำหรับเป็น Thin Client
	Laptop	เครื่องโน้ตบุ๊กคอมพิวเตอร์ (Notebook computer) เป็นเครื่องคอมพิวเตอร์ ที่ถูกออกแบบมาให้มีขนาดเล็กสามารถขนย้ายได้สะดวก ถูกนำมาใช้สำหรับทำงานทั่วไป เช่น งานเอกสาร หรือใช้สำหรับเป็น Thin Client
	Tablet	แท็บเล็ต (Tablet) เป็นคอมพิวเตอร์ส่วนบุคคลชนิดหนึ่งที่มีขนาดเล็กกว่าคอมพิวเตอร์โน้ตบุ๊ค พกพาง่าย น้ำหนักเบา มีคีย์บอร์ด (keyboard) ในตัว หน้าจอเป็นระบบสัมผัส (Touch-screen) เป็นอุปกรณ์สนับสนุนให้สำหรับเจ้าหน้าที่ในระดับ ผช.ผจก. ขึ้นไปเพื่อใช้ในการดำเนินงานตามหน้าที่ความรับผิดชอบ
	LCD Monitor	จอภาพ เป็นอุปกรณ์ที่รับสัญญาณจากการ์ดแสดงผล มาแสดงเป็นภาพบน จอภาพ โดยมีการใช้งานในส่วนอาคารสถานที่(ห้องประชุม) ใช้ในการเฝ้าระวังด้านเครือข่าย เฝ้าระวังด้านความมั่นคงปลอดภัยสารสนเทศ และใช้สนับสนุนการดำเนินงานของเจ้าหน้าที่ภายใน เป็นต้น
	Access Control	ระบบป้องกันการเข้าถึงซึ่งช่วยควบคุมคัดกรองจำกัดบุคคลที่ไม่ได้รับอนุญาติให้เข้าพื้นที่ หรือต้องการให้ เข้า-ออกในพื้นที่ ที่กำหนด ประกอบด้วย - ชั้น ๑๙ จำนวน ๓ ประตู - ชั้น ๑๘ จำนวน ๕ ประตู - ชั้น ๑๗ จำนวน ๑ ประตู - ชั้น ๑๖ จำนวน ๑ ประตู
	IP Phone	โทรศัพท์ภายในสำนักงานที่ให้สำหรับเจ้าหน้าที่ โดยใช้เทคโนโลยี VoIP สามารถใช้งานผ่านระบบ LAN โดยไม่ต้องเดินสายโทรศัพท์ และเลขหมายประจำตัวของผู้ใช้งานของเจ้าหน้าที่แต่ละท่านสามารถใช้งานระบบโทรศัพท์ได้จากทุกแห่งที่มีการติดตั้งเครื่อง IP Phone
	CCTV	CCTV เป็นการส่งสัญญาณภาพ จากกล้องวงจรปิด ที่ได้ติดตั้งตามพื้นที่ต่างๆ มายังส่วนรับภาพ/ดูภาพ ซึ่งเรียกว่า จอภาพ (Monitor) โดยปัจจุบันมีการติดตั้งกล้องวงจรปิดครอบคลุม บริเวณพื้นที่สำนักงาน ดังนี้ - ชั้น ๑๙ จำนวน ๑๑ ตัว - ชั้น ๑๘ จำนวน ๕ ตัว - ชั้น ๑๗ จำนวน ๔ ตัว - ชั้น ๑๖ จำนวน ๔ ตัว
	Call Center	เครื่องให้บริการศูนย์บริการลูกค้า (CSC) ในการรับเรื่องร้องเรียน รับการร้องขอ รับแจ้งปัญหาสิ่งบกพร่อง หรือ รับแจ้งปัญหาที่เกิดจากความมั่นคงปลอดภัยของลูกค้าและเจ้าหน้าที่ภายใน ผ่านช่องทาง โทรศัพท์หรือผ่านทาง E-mail ในการตอบคำถามข้อสงสัยรวมถึงการติดตามสถานะการดำเนินงาน

ประเภท	รายการ	รายละเอียด
Hardware (Server) & Virtualization	Web Server	เครื่องคอมพิวเตอร์ซึ่งให้บริการเว็บไซต์ ผู้ใช้เรียกชมหน้าเว็บไซต์ได้โดยใช้โพรโทคอล HTTP และ HTTPS ผ่านทางเว็บเบราว์เซอร์
	Database Server	เครื่องบริการด้านข้อมูล เพื่อใช้ในการจัดเก็บข้อมูล เช่น MySQL Server และ Microsoft SQL Server เป็นต้น
	Print Server	เครื่องที่ให้บริการเกี่ยวกับการพิมพ์ โดยทุกเครื่องในเครือข่ายของสำนักงานสามารถส่งงานของเจ้าหน้าที่ไปพิมพ์ที่เครื่องทำหน้าที่เป็น Print Server ได้
	Log Server	ระบบที่ใช้ในการจัดเก็บ Log File คือ การจัดเก็บข้อมูลทั้งหมดที่เกี่ยวข้องกับการใช้งาน Internet ของเจ้าหน้าที่ภายในสำนักงานตามพรบ. คอมพิวเตอร์ ปี ๒๕๕๐ มาตรา ๒๖ เนื่องด้วย พรบ. คอมพิวเตอร์ ปี ๒๕๕๐ มาตรา ๒๖ ที่กล่าวถึง ผู้ให้บริการต้องเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ไว้ไม่น้อยกว่า ๙๐ วันนับแต่วันที่ข้อมูลนั้นเข้าสู่ระบบคอมพิวเตอร์ โดยสิ่งที่สรอ.จัดเก็บประกอบไปด้วย - เครื่องแม่ข่ายของสรอ. - อุปกรณ์เครือข่ายของสรอ. - อุปกรณ์ Firewall ของพนักงานสรอ.
	IP Phone Server	เครื่องคอมพิวเตอร์ที่ใช้ในการสื่อสารกับโปรแกรมบนเครื่อง (Software Client) ผ่านระบบอินเตอร์เน็ต ในการบริหารจัดการการใช้งานโทรศัพท์ IP Phone ภายในองค์กร
	E-mail Server	เครื่องบริการรับ-ส่งจดหมายอิเล็กทรอนิกส์ ซึ่งสามารถรองรับการรับ-ส่งจดหมายทั้งแบบที่เป็นข้อความและรูปภาพ และมีที่เก็บข้อมูลผู้ติดต่อผู้ใช้งานที่เรียกว่า Address book โดยสามารถใช้งานผ่าน Web browser และ Mail client
	Anti-Virus Server	ให้บริการ ในการกระจาย Signature ให้เครื่องพนักงานภายในของสรอ. รวมถึงออกรายงานการใช้งาน Anti virus
	AD Server	Active Directory เป็นเครื่องมือ ที่มีมากับ Windows Server Operating System โดยทำหน้าที่ช่วยจัดการทรัพยากรในระบบ จากจุดศูนย์กลางโดยเครื่องมือของ Server Domain Controller โดยสำนักงาน นำ Active Directory มาใช้งานในการควบคุมการเข้าถึง เครื่องใช้งานพนักงานของสรอ. ควบคุมการออก Internet โดย Wireless lan การเข้าใช้งาน VPN
	LDAP Server	ระบบพิสูจน์สิทธิ์(Authentication) โดยทำการกำหนดสิทธิ์ (Authorization) และการบันทึกการใช้งาน (Accounting)
	Storage Server	ระบบการจัดเก็บข้อมูล ซึ่งถูกใช้ในการจัดเก็บข้อมูลของเครื่องแม่ข่ายหรือเครื่องให้บริการภายในสรอ. อาทิเช่น - งานจัดเก็บฐานข้อมูล Database - ข้อมูลเสมือน Virtualization / Cloud ภายใน - งานจัดเก็บข้อมูลกล้องวงจรปิด CCTV Camera - Log ภายใน
	Backup Server	ระบบสำรองข้อมูล เครื่องให้บริการภายในสรอ.
	Monitor Server	ระบบเฝ้าระวัง ที่ครอบคลุมด้าน Availability และด้าน Capacity ของเครื่องให้บริการภายในสรอ.
Network	Telephone Server	ระบบโทรศัพท์ ที่ให้บริการเจ้าหน้าที่ศูนย์บริการข้อมูล (CSC) ในการใช้งานในการตอบคำถามเจ้าหน้าที่ภายในสรอ.
	Internet Link	เครือข่ายการเชื่อมต่อออกอินเตอร์เน็ต ของสรอ. รวมการออกอินเทอร์เน็ต ทั้ง Domestic International
	Wired LAN	การเชื่อมต่อแบบมีสาย ในการเชื่อมโยงเครือข่ายคอมพิวเตอร์ถึงกันภายในสำนักงาน

ประเภท	รายการ	รายละเอียด
	Wireles LAN	ระบบ LAN ที่ไม่ใช้สาย และใช้คลื่นความถี่วิทยุในการรับ-ส่งข้อมูลแทนการใช้สายเคเบิ้ลนำสัญญาณ จำเป็นต้องมี Access Point (AP) ที่ต่อกับระบบ LAN ด้วยสายเคเบิ้ล โดย AP จะทำหน้าที่เป็นตัวกลางในการเชื่อมต่ออุปกรณ์ Wireless ชนิดต่าง ๆ เข้ากับระบบเน็ตเวิร์ค โดยครอบคลุมการให้บริการพื้นที่ภายในสำนักงาน ดังนี้ - ชั้น ๑๙ จำนวน ๓ Access points - ชั้น ๑๘ จำนวน ๕ Access points - ชั้น ๑๗ จำนวน ๓ Access points - ชั้น ๑๖ จำนวน ๒ Access points
	Phone Network	ระบบโทรศัพท์ที่ใช้งานผ่านระบบอินเตอร์เน็ต โดยสำนักงาน มีเครื่องโทรศัพท์ IP Phone พร้อมสำหรับเจ้าหน้าที่ทุกท่าน เชื่อมต่อกับเครือข่ายทุกเครื่อง
	VLAN	การแบ่งแยกเครือข่ายภายในสรอ. ในการใช้บริการภายในเพื่อความปลอดภัยในการใช้บริการ
	VPN	การเข้าใช้งานจากระยะไกล ภายนอกสรอ. ในการใช้งานระบบภายในสรอ. เช่น Intranet เป็นต้น

ตารางที่ ๑๓ รายการของโครงสร้างพื้นฐาน

โดยมีการแสดงความเชื่อมโยงของโครงสร้างพื้นฐานดังต่อไปนี้ (๑) ความสัมพันธ์ระหว่างโครงสร้างพื้นฐาน (ฮาร์ดแวร์) และแอปพลิเคชันธุรกิจตามตารางที่ ๑๔ และ (๒) ความสัมพันธ์ระหว่างโครงสร้างพื้นฐาน (ระบบปฏิบัติการและฮาร์ดแวร์) และแอปพลิเคชันสนับสนุนตารางที่ ๑๕

ความสัมพันธ์ระหว่างโครงสร้างพื้นฐาน (ฮาร์ดแวร์) และแอปพลิเคชันธุรกิจ			แอปพลิเคชันธุรกิจ																	
			Web Application												Desktop Application					
			EGA Contact	Problem Tracking	Customer Mgt.	EGA Back-end	Saraban	Risk Mgt.	Operation Center	Intranet	Knowledge Mgt.	Appointment Mgt.	ISO Document	Document Mgt.	Project Tracking	Human Resource	Welfare Mgt.	Financial Mgt.	Procurement Mgt.	Asset Mgt.	Minute of Meeting
Virtualization (Private-Cloud)	Web Server	Intranet Web Server		■			■			■	■		■	■							
		EGA-Website Web Server				■															
		EGA Contact Web Server	■																		
		OC Web Server							■												
	DB Server	EGA DB Server		■		■	■		■	■	■		■	■			■	■	■	■	
		HR DB Server														■					
		EGA Contact DB Server	■																		
	Web&DB Server	Risk Server						■													
		Appointment Server										■									
		Customer Server			■																
		Project Tracking Server													■						
Client		HR Client														■					
		Welfare Client															■				
		Financial Client																■	■		
		Asset Client																		■	
		Minute of Meeting Client																			■

■ หมายถึง เครื่องที่จัดเก็บแอปพลิเคชัน
■ หมายถึง เครื่องที่จัดเก็บข้อมูล
■ หมายถึง เครื่องที่เก็บทั้งแอปพลิเคชันและข้อมูล

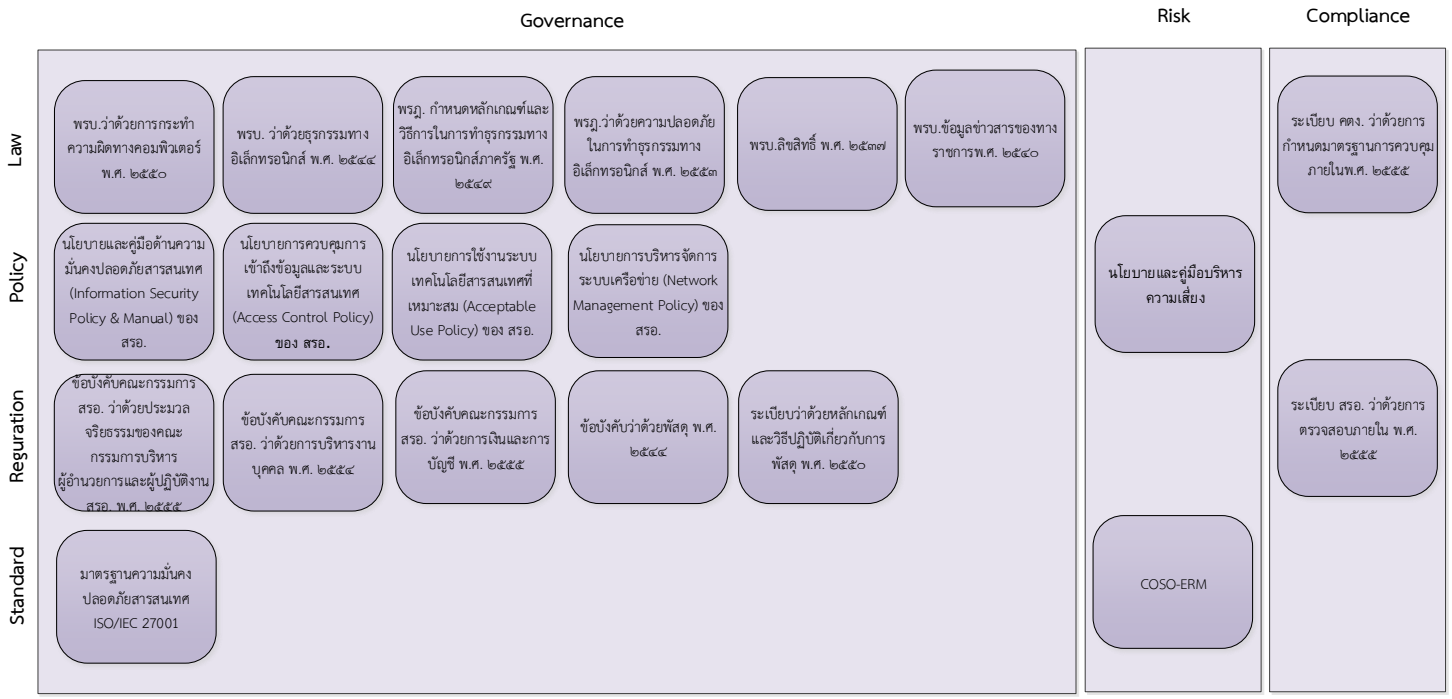
ตารางที่ ๑๔ ตารางความสัมพันธ์ระหว่างโครงสร้างพื้นฐาน (ฮาร์ดแวร์) และแอปพลิเคชันธุรกิจ

ความสัมพันธ์ระหว่างแอปพลิเคชันสนับสนุน ระบบปฏิบัติการ และฮาร์ดแวร์			โครงสร้างพื้นฐาน																	
			Hardware (Client)						Hardware (Server) & Virtualization											
			Client						Web Server				DB Server			Web&DB Server				
			HR Client	Welfare Client	Financial Client	Procurement Client	Asset Client	Minute of Meeting Client	Intranet Web Server	EGA-Website Web Server	EGA Contact Web Server	OC Web Server	EGA DB Server	HR DB Server	EGA Contact DB Server	Risk Server	Appointment Server	Customer Server	Project Tracking Server
แอปพลิเคชันสนับสนุน	Database Management	MS SQL Server 2008											X	X		X		X	
		MySQL Server													X		X		X
		PostgreSQL 8.4															X		
		MS Access						X											
	Web Server	IIS							X	X	X	X						X	
		Apache httpd 2.2														X	X		
		Thin																	X
โครงสร้างพื้นฐาน	Operating System	Windows Server 2008							X	X	X	X	X	X	X	X	X	X	X
		Windwos XP		X															
		Windwos 7	X		X	X	X	X											

ตารางที่ ๑๕ ตารางความสัมพันธ์ระหว่างโครงสร้างพื้นฐาน (ระบบปฏิบัติการและฮาร์ดแวร์) และแอปพลิเคชันสนับสนุน

๓.๕ ด้านความมั่นคงปลอดภัย (Security)

ความมั่นคงปลอดภัย (Security) เข้ามามีส่วนเกี่ยวข้องกับด้านอื่นๆของสถาปัตยกรรมองค์กร ทั้งด้านธุรกิจ แอปพลิเคชัน ข้อมูล และโครงสร้างพื้นฐาน โดยที่ความมั่นคงปลอดภัยจะพิจารณาถึงหลักการ GRC ซึ่งเน้นในเรื่อง ธรรมาภิบาล (Governance) การบริหารจัดการความเสี่ยง (Risk Management) และความสอดคล้องกับกฎระเบียบ (Compliance) แต่ละส่วนถูกแบ่งออกเป็น ๔ ระดับนั่นคือ (๑) กฎหมาย (Law) (๒) นโยบาย (Polycy) (๓) ข้อบังคับและระเบียบ (Regulation) และ (๔) มาตฐาน (Standard) รูปที่ ๒๑ แสดงรายการมาตรการควบคุมที่ทางสำนักงานนำมาหรือกำหนดขึ้นมาใช้สำหรับการดำเนินงานด้านความมั่นคงปลอดภัยตามที่แสดงในรูปที่ ๒๑



รูปที่ ๒๑ ภาพรวมของมาตรการควบคุมความมั่นคงปลอดภัย

ขณะที่ในตารางที่ ๑๖ แสดงรายการมาตรการควบคุมความมั่นคงปลอดภัยที่ทางสำนักงานนำมาหรือกำหนดขึ้นมาใช้สำหรับการดำเนินงานด้านความมั่นคงปลอดภัย

มาตรการควบคุม	คำอธิบาย	ขอบเขตการบังคับใช้	แหล่งที่มา
กฎหมาย			
พรบ.ว่าด้วยการกระทำความผิดทางคอมพิวเตอร์ พ.ศ. ๒๕๕๐	กฎหมายว่าด้วยการกระทำความผิดทางคอมพิวเตอร์	ทั้งองค์กร	ราชกิจจานุเบกษา
พรบ. ว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๔๔	กฎหมายว่าด้วยการกระทำธุรกรรมทางอิเล็กทรอนิกส์	ทั้งองค์กร	ราชกิจจานุเบกษา
พรฎ. กำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙	กฎหมายว่าด้วยการกำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ	ทั้งองค์กร	ราชกิจจานุเบกษา
พรฎ.ว่าด้วยความปลอดภัยในการทำธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๕๓	กฎหมายว่าด้วยความปลอดภัยในการทำธุรกรรมทางอิเล็กทรอนิกส์	ทั้งองค์กร	ราชกิจจานุเบกษา
พรบ.ลิขสิทธิ์ พ.ศ. ๒๕๓๗	กฎหมายว่าด้วยการคุ้มครองด้านลิขสิทธิ์	ทั้งองค์กร	ราชกิจจานุเบกษา
พรบ.ข้อมูลข่าวสารของทางราชการพ.ศ. ๒๕๔๐	กฎหมายว่าด้วยข้อมูลข่าวสารของทางราชการ	ทั้งองค์กร	ราชกิจจานุเบกษา
นโยบาย			
นโยบายด้านความมั่นคงปลอดภัยสารสนเทศของ (Information Security Policy) ของสำนักงาน	นโยบายด้านความมั่นคงปลอดภัยสารสนเทศของสำนักงานถูกกำหนดให้เป็นไปตามข้อกำหนดของ ISO/IEC 27001	ทั้งองค์กร	สรอ.

นโยบายการควบคุมการเข้าถึงข้อมูลและระบบเทคโนโลยีสารสนเทศ (Access Control Policy) ของสำนักงาน	นโยบายการควบคุมการเข้าถึงข้อมูลและระบบเทคโนโลยีสารสนเทศของสำนักงาน	ทั้งองค์กร	สรอ.
นโยบายการใช้งานระบบเทคโนโลยีสารสนเทศ (Acceptable Use Policy) ของสำนักงาน	นโยบายในการใช้งานระบบเทคโนโลยีสารสนเทศที่เหมาะสมของสำนักงาน	ทั้งองค์กร	สรอ.
นโยบายการบริหารจัดการระบบเครือข่าย (Network Management Policy) ของสำนักงาน	นโยบายในการบริหารจัดการระบบเครือข่ายของสำนักงาน	ทั้งองค์กร	สรอ.
นโยบายและคู่มือบริหารความเสี่ยง	นโยบายและคู่มือบริหารความเสี่ยง	ทั้งองค์กร	สรอ.
ข้อบังคับและระเบียบ			
ข้อบังคับคณะกรรมการ สรอ. ว่าด้วยประมวลจริยธรรมของคณะกรรมการบริหาร ผู้อำนวยการและผู้ปฏิบัติงาน สรอ. พ.ศ. ๒๕๕๕	ข้อบังคับการกำหนดมาตรฐานทางจริยธรรมของผู้ดำรงตำแหน่งทางการเมือง ข้าราชการ หรือเจ้าหน้าที่ของรัฐเป็นไปตามประมวลจริยธรรมที่กำหนดขึ้น	ทั้งองค์กร	สรอ.
ข้อบังคับคณะกรรมการ สรอ. ว่าด้วยการบริหารงานบุคคล พ.ศ. ๒๕๕๔	ข้อบังคับการบริหารงานบุคคล	ทั้งองค์กร	สรอ.
ข้อบังคับคณะกรรมการ สรอ. ว่าด้วยการเงินและการบัญชี พ.ศ. ๒๕๕๕	ข้อบังคับการบริการการเงินและบัญชี	ทั้งองค์กร	สรอ.
ข้อบังคับว่าด้วยพัสดุ พ.ศ. ๒๕๔๔	ข้อบังคับว่าด้วยพัสดุ	ทั้งองค์กร	สวทช.
ระเบียบว่าด้วยหลักเกณฑ์และวิธีปฏิบัติเกี่ยวกับการพัสดุ พ.ศ. ๒๕๕๐	หลักเกณฑ์และวิธีปฏิบัติเกี่ยวกับการพัสดุ	ทั้งองค์กร	สวทช.
ระเบียบ คตง. ว่าด้วยการกำหนดมาตรฐานการควบคุมภายในพ.ศ. ๒๕๕๕	ระเบียบ คตง. ว่าด้วยการกำหนดมาตรฐานการควบคุมภายใน	ทั้งองค์กร	ราชกิจจานุเบกษา
มาตรฐาน			
ISO/IEC 27001	มาตรฐานด้านความมั่นคงปลอดภัยสารสนเทศ	ส่วนงานที่เกี่ยวข้องกับบริการ G-Cloud	British Standards Institution (BSI)
COSO-ERM	Framework สำหรับการบริหารจัดการความเสี่ยง	ทั้งองค์กร	The Committee of Sponsoring Organizations (COSO)

ตารางที่ ๑๖ รายการมาตรการควบคุมความมั่นคงปลอดภัย

จากตารางที่ ๑๖ พบว่ามีการนำมาตรฐาน ISO/IEC27001:2013 มาใช้ในการรักษาความมั่นคงปลอดภัยสารสนเทศ โดยเริ่มจากส่วนงานที่เกี่ยวข้องกับบริการ G-Cloud ของสำนักงาน และมีการดำเนินงานตาม นโยบาย ข้อบังคับ ระเบียบ และกฎหมายที่เกี่ยวข้อง ตารางที่ ๑๗ แสดงความสัมพันธ์ระหว่างมาตรการควบคุมความมั่นคงปลอดภัยกับส่วนงาน **ภาคผนวก ค** จะแสดงให้เห็นความเชื่อมโยงการประยุกต์ใช้ระหว่างข้อกำหนดและมาตรการควบคุมด้านความมั่นคงปลอดภัยสารสนเทศ ตามมาตรฐาน ISO/IEC27001:2013 กับ นโยบาย ข้อบังคับ ระเบียบ และกฎหมายที่เกี่ยวข้องกับการดำเนินงาน

มาตรการควบคุมความปลอดภัย/ส่วนงาน	PSP	PSS	PSC	PSR	INR	INA	INS	CSB	CSM	CSK	CSI	CSP	CST	CSC	ENI	ENM	ENS	ENT	ADD1	ADD2	ADQ	ADM	CMF	CMH	CMG	CMP	CMD	ODS	ODI	ODL	AI	VT
	ฝ่ายนโยบายและ				ฝ่ายนวัตกรรม			ฝ่ายบริการให้คำปรึกษา							ฝ่ายวิศวกรรมและ				ฝ่ายพัฒนาและจัดการ				ฝ่ายบริหารประสิทธิภาพ					ฝ่ายอำนวยการ				
กฎหมาย																																
พรบ.ว่าด้วยการกระทำความผิดทางคอมพิวเตอร์ พ.ศ. ๒๕๕๐																																
พรบ. ว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๔๔																																
พรฎ. กำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙																																
พรฎ.ว่าด้วยความปลอดภัยในการทำธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๕๓																																
พรบ.ลิขสิทธิ์ พ.ศ. ๒๕๓๗																																
พรบ.ข้อมูลข่าวสารของทางราชการพ.ศ. ๒๕๔๐																																
นโยบาย																																
นโยบายด้านความมั่นคงปลอดภัยสารสนเทศของ (Information Security Policy) ของสำนักงาน																																
นโยบายการควบคุมการเข้าถึงข้อมูลและระบบเทคโนโลยีสารสนเทศ (Access Control Policy) ของสำนักงาน																																
นโยบายการใช้งานระบบเทคโนโลยีสารสนเทศ (Acceptable Use Policy) ของสำนักงาน																																
นโยบายการบริหารจัดการระบบเครือข่าย (Network Management Policy) ของสำนักงาน																																
นโยบายและคู่มือบริหารความเสี่ยง																																
ข้อบังคับและระเบียบ																																
ข้อบังคับคณะกรรมการ สรอ. ว่าด้วยประมวลจริยธรรม ฯ สรอ. พ.ศ. ๒๕๕๕																																
ข้อบังคับคณะกรรมการ สรอ. ว่าด้วยการบริหารงานบุคคล พ.ศ. ๒๕๕๔																																
ข้อบังคับคณะกรรมการ สรอ. ว่าด้วยการเงินและการบัญชี พ.ศ. ๒๕๕๕																																
ข้อบังคับว่าด้วยพัสดุ พ.ศ. ๒๕๔๔																																
ระเบียบว่าด้วยหลักเกณฑ์และวิธีปฏิบัติเกี่ยวกับการพัสดุ พ.ศ. ๒๕๕๐																																
ระเบียบ คตง. ว่าด้วยการกำหนดมาตรฐานการควบคุมภายในพ.ศ. ๒๕๕๕																																
มาตรฐาน																																
ISO/IEC 27001																																
COSO-ERM																																

VT หมายถึง ทีมที่ถูกกำหนดขึ้นมาเพื่อดำเนินการควบคุม (Virtual Team)

หมายถึง หน่วยงานที่ต้องปฏิบัติตามมาตรการควบคุมความมั่นคงความปลอดภัย

หมายถึง หน่วยงานที่ดำเนินการควบคุมให้เป็นไปตามมาตรการความมั่นคงปลอดภัย

หมายถึง หน่วยงานที่ต้องปฏิบัติตามและควบคุมให้เป็นไปตามมาตรการควบคุมความมั่นคงความปลอดภัย

ตารางที่ ๑๗ ตารางความสัมพันธ์ระหว่างมาตรการควบคุมความมั่นคงปลอดภัยกับส่วนงาน

๓.๖ การวิเคราะห์ศักยภาพของสถานะปัจจุบันของสถาปัตยกรรมองค์กร สรอ. ตามหลักการ TOWS Matrix

จากการสำรวจและรวบรวมข้อมูลตั้งแต่นโยบาย วิสัยทัศน์ ยุทธศาสตร์ พันธกิจ แผนการดำเนินงานต่างๆ ที่เกี่ยวข้อง อันได้แก่ ด้านธุรกิจ (Business) ด้านแอปพลิเคชัน (Application) ด้านข้อมูล (Data) ด้านโครงสร้างพื้นฐาน (Infrastructure) และด้านความมั่นคงปลอดภัย (Security) ถูกนำมาวิเคราะห์ด้วยหลักการ TOWS Matrix เพื่อกำหนดเป็นกลยุทธ์สำหรับการพัฒนาสถาปัตยกรรมภายในองค์กรของ สรอ. ดังนี้

๑) **กลยุทธ์ SO** :

เป็นการจับคู่ระหว่างจุดแข็ง (Strenght) กับโอกาส (Opportunity) โดยทั้งคู่เป็นปัจจัยเชิงบวก

สรุป องค์กรควรจะใช้จุดแข็งและโอกาสร่วมกัน เพื่อสร้างความได้เปรียบในการแข่งขัน

๒) **กลยุทธ์ ST** :

เป็นการจับคู่ระหว่างจุดแข็งกับอุปสรรค โดยจุดแข็ง (Strength) เป็นปัจจัยเชิงบวกและมีอุปสรรค (Threat) เป็นปัจจัยเชิงลบ

สรุป องค์กรต้องการนำปัจจัยเชิงบวกไปจัดการกับปัจจัยเชิงลบ คือ นำจุดแข็งมาใช้เพื่อป้องกันหรือหลีกเลี่ยงอุปสรรค

๓) **กลยุทธ์ WO** :

เป็นการจับคู่ระหว่างจุดอ่อนกับโอกาส โดยจุดอ่อน (Weakness) เป็นปัจจัยเชิงลบแต่มีโอกาส (Opportunity) เป็นปัจจัยเชิงบวก

สรุป องค์กรต้องนำปัจจัยเชิงบวกไปจัดการกับปัจจัยเชิงลบ คือ นำโอกาสมากำจัดจุดอ่อนหรือ นำโอกาสมาใช้ให้เกิดประโยชน์ต่อองค์กร

๔) **กลยุทธ์ WT** :

เป็นการจับคู่ระหว่างจุดอ่อน (Weakness) กับอุปสรรค (Threat) โดยทั้งคู่เป็นปัจจัยเชิงลบ

สรุป องค์กรต้องคิดกลยุทธ์หรือแนวทางที่กระทำแล้วสามารถกำจัดจุดอ่อนได้และสามารถป้องกันอุปสรรคได้ด้วยในคราวเดียวกัน

ปัจจัยแวดล้อมภายใน / ปัจจัยแวดล้อมภายนอก	**S : จุดแข็ง** S1 : มีการกำหนดขั้นตอนของกระบวนการการปฏิบัติงาน (BPI) S2 : มีการนำเอาแอปพลิเคชันมาช่วยในการดำเนินงาน S3 : ข้อมูลถูกจัดเก็บอย่างเป็นระบบในรูปแบบของ RDBMS S4 : มีเครือข่ายภายในที่หลากหลาย เช่น Wire LAN, Wireless LAN, และ Voice Network S5 : มีการนำเอาเทคโนโลยีใหม่ๆมาปรับใช้ในองค์กร เช่น Cloud computing	**W : จุดอ่อน** W1 : มีขั้นตอนในการดำเนินงานหลายขั้นตอน W2 : มีแอปพลิเคชันไม่ครอบคลุมทุกกระบวนการปฏิบัติงานที่สำคัญ W3 : ข้อมูลมีการจัดเก็บซ้ำซ้อน W4 : ขาดผู้รับผิดชอบข้อมูลสำหรับข้อมูลที่ใช้งานร่วมกัน
O : โอกาส O1 : ข้อตกลงร่วมระหว่างการปฏิบัติของแต่ละกระบวนการ (OLA : Operational Level Agreement) O2 : องค์กรมีบุคลากรมีความเชี่ยวชาญด้านเทคโนโลยีสารสนเทศ ทั้งด้าน แอปพลิเคชัน ข้อมูล เครือข่าย และความปลอดภัยสารสนเทศ O3 : การเปลี่ยนแปลงด้านเทคโนโลยีมีการเปลี่ยนแปลงที่รวดเร็ว O4 : ภาครัฐมีกฎหมายรองรับพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๔๔	**สร้างความได้เปรียบ** S1,O1, : กำหนด OLA ของแต่ละกระบวนการปฏิบัติงานภายในองค์กร S2,S3,S4,S5,O2,O3 : ปรับปรุงเทคโนโลยีสารสนเทศอย่างต่อเนื่องเพื่อให้สอดรับกับการดำเนินงานทางธุรกิจมากยิ่งขึ้น S2,O4 : ปรับปรุงแอปพลิเคชันให้รองรับกับพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๔๔	**กำจัดจุดอ่อน** W1,W2,O4 : นำเอาแอปพลิเคชันที่รองรับกฎหมายเกี่ยวข้องกับธุรกรรมทางอิเล็กทรอนิกส์มาใช้งาน W1,W2,W3,W4,O2,O3 : ออกแบบสถาปัตยกรรมระบบและข้อมูลเพื่อลดการจัดเก็บข้อมูลที่ซ้ำซ้อนพร้อมทั้งกำหนดผู้รับผิดชอบที่ชัดเจน
T : อุปสรรค T1 : เนื่องจากกระบวนการทางธุรกิจมีการเปลี่ยนแปลง ส่งผลให้แอปพลิเคชั่นที่ใช้อยู่อาจจะไม่ตอบสนองความต้องการในปัจจุบัน T2 : การเปลี่ยนแปลงด้านเทคโนโลยีมีการเปลี่ยนแปลงที่รวดเร็ว	**หลีกเลี่ยงอุปสรรค** S2,T1,T2 : ออกแบบการพัฒนาแอปพลิเคชันให้มีความยืดหยุ่นเพื่อรองรับการเปลี่ยนแปลงกระบวนการทางธุรกิจ	**หลีกเลี่ยงอุปสรรคและกำจัดจุดอ่อน** W1,W2,W3,W4,T1,T2 : ดำเนินการพัฒนาสถาปัตยกรรมภายในองค์กรของ สรอ. อย่างต่อเนื่อง

ตารางที่ ๑๘ แสดงการวิเคราะห์ TOWS Matrix ของสถาปัตยกรรมปัจจุบันของ สรอ.

บทที่ ๔ การออกแบบสถาปัตยกรรมองค์กรในอนาคต

จากการสำรวจสถานะปัจจุบันของสถาปัตยกรรม สรอ. โดยสะท้อนผ่านทางมุมมองของสถาปัตยกรรมองค์กร ทั้ง ๓ มุมมอง (EGA Enterprise Architecture Viewpoints) ๔ กระบวนการ การพัฒนาสถาสถาปัตยกรรมองค์กร (Enterprise Architecture Development Processes) และ ๕ แบบจำลองอ้างอิงองค์กร (Enterprise Reference Models) แสดงให้เห็นถึงประเด็นปัญหาในปัจจุบัน นอกเหนือจากปัจจัยภายในด้านต่างๆเหล่านี้ที่ส่งผลต่อการพัฒนาสถาปัตยกรรมองค์กรของ สรอ. แล้ว ยังพบปัจจัยภายนอกที่มีผลต่อการพัฒนาด้วย ยกตัวอย่างเช่น การเปลี่ยนแปลงเทคโนโลยีรวดเร็ว ความต้องการทางธุรกิจที่มีความหลากหลายหรือมีการขยายตัวเพิ่มมากขึ้น รวมทั้งการเปลี่ยนแปลงด้านนโยบายทางการเมือง เป็นต้น

โดยการออกแบบสถาปัตยกรรมองค์กรในอนาคต จะนำเอาทั้งปัจจัยภายใน (นั้นคือประเด็นปัญหาจากการวิเคราะห์สถานะปัจจุบันและความต้องการจากหลักการสถาปัตยกรรม) และปัจจัยภายนอกมาใช้เพื่อบูรณาการสถาปัตยกรรมองค์กร ทั้งด้านธุรกิจ เทคโนโลยีสารสนเทศและความมั่นคงปลอดภัยดังแสดงใน รูปที่ ๒๒

รูปที่ ๒๒ ภาพแสดงปัจจัยภายนอกและภายใน

๔.๑ ด้านธุรกิจ (Businesses)

จากผลการสำรวจและการวิเคราะห์สถานะปัจจุบันของสถาปัตยกรรมองค์กรด้านธุรกิจ สามารถสรุปประเด็นปัญหาและหลักการด้านธุรกิจ ได้ดังนี้

ประเด็นปัญหา (Issue)

๑) บางกระบวนการปฏิบัติงานมีขั้นตอนการปฏิบัติงาน (กิจกรรม การตัดสินใจและการอนุมัติ) จำนวนมาก

๒) การติดต่อประสานงานระหว่างกระบวนการหรือระหว่างส่วนงานใช้เวลาค่อนข้างมาก เนื่องจากการประสานงานยังใช้ช่องทางผ่านการประชุมหรือผ่านทางเอกสาร (กระดาษ) เป็นส่วนใหญ่ รวมทั้งผ่านทางจดหมายอิเล็กทรอนิกส์

๓) บางกระบวนการยังขาดผู้รับผิดชอบที่ชัดเจนหรือมีความซ้ำซ้อนในอำนาจหน้าที่ของการปฏิบัติงาน

๔) ขาดความเชื่อมโยงระหว่างกระบวนการ ส่งผลให้ไม่สามารถติดตามสถานะของการปฏิบัติงานได้

๕) มีการสูญหายของข้อมูล (เอกสาร) ระหว่างกระบวนการ

หลักการด้านธุรกิจ (Business Principle)

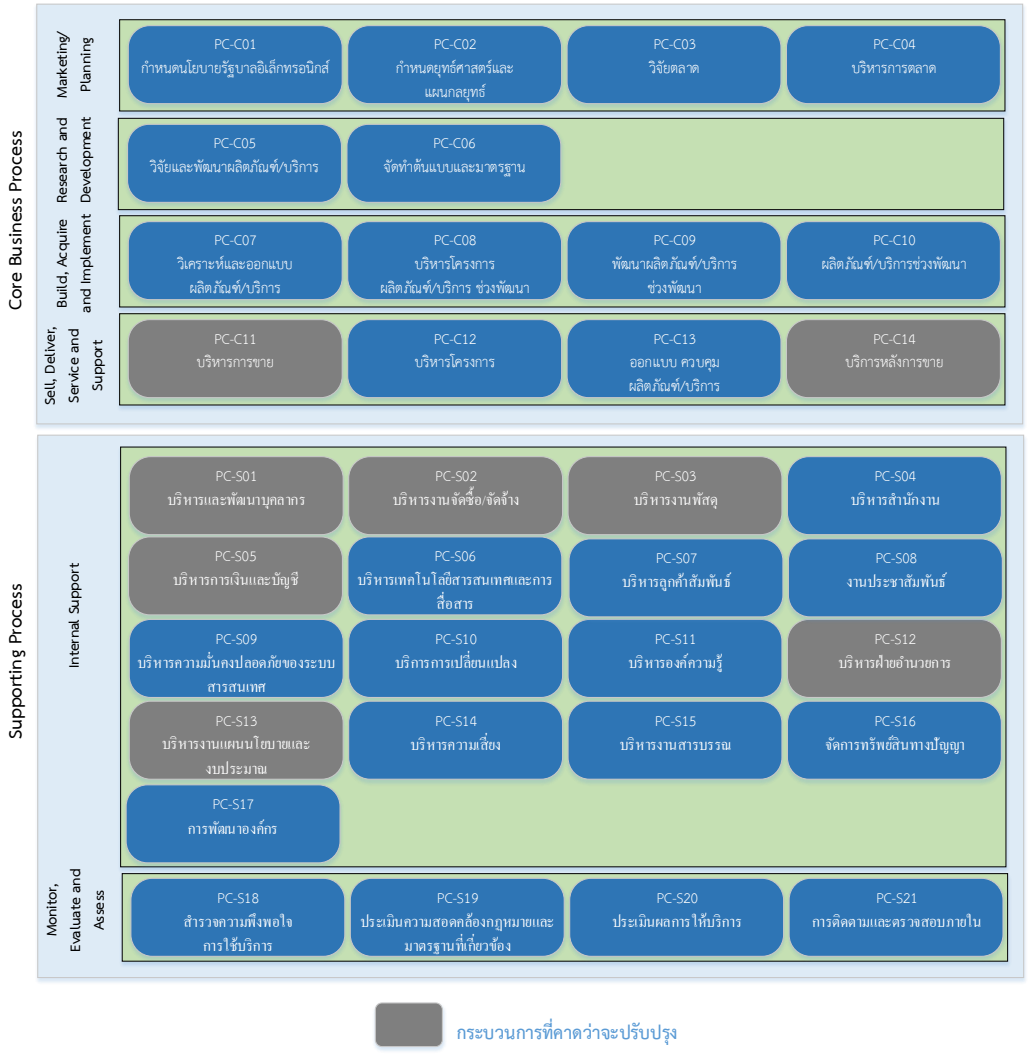
๑) มีกระบวนการและขั้นตอนการปฏิบัติงานที่เป็นมาตรฐาน ควรมีการนิยามให้ชัดเจน เข้าใจง่าย และมีการประกาศใช้อย่างเป็นทางการ รวมไปถึงการกำหนดเวลาในการปฏิบัติงาน (Operational Level Agreement)

๒) มีขั้นตอนการปฏิบัติงานที่ กระชับและไม่ซ้ำซ้อน เพื่อลดเวลาและเพิ่มความถูกต้องในการปฏิบัติงาน

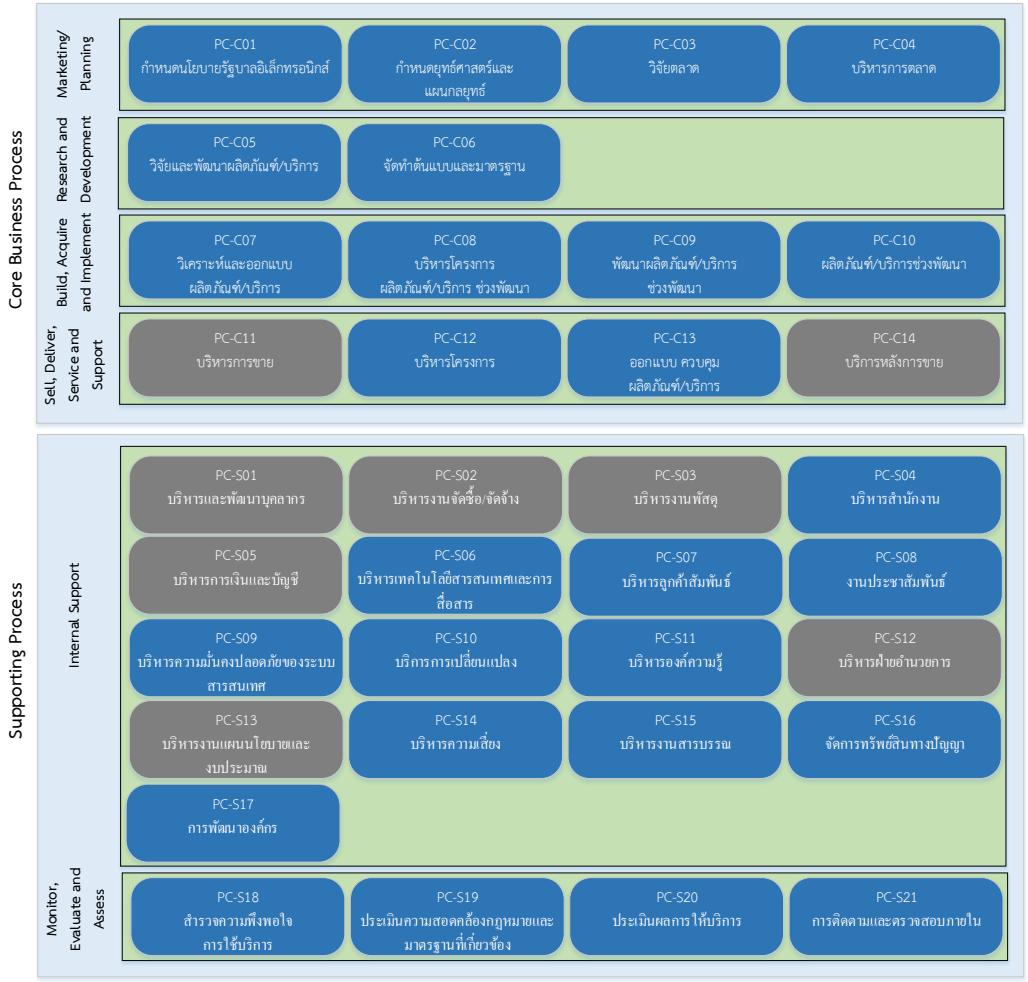
๓) มีการกำหนดขอบเขต บทบาท หน้าที่ และความรับผิดชอบต่อกระบวนการปฏิบัติงานที่ชัดเจน เพื่อช่วยลดการทำงานที่ซ้ำซ้อน

๔) มุ่งเน้นการลดการใช้กระดาษให้มากที่สุด

ประเด็นปัญหาที่พบจากการวิเคราะห์และหลักการด้านธุรกิจถูกนำมาใช้เพื่อการดำเนินการออกแบบสถาปัตยกรรมองค์กรในอนาคตตามที่แสดงใน



รูปที่ ๒๓ จากรูปจะเห็นได้ว่ามี ๘ หมวดกระบวนการ ที่คาดว่าจะปรับปรุง โดยแบ่งเป็น ๒ หมวดกระบวนการหลักและ ๖ หมวดกระบวนการสนับสนุน ตารางที่ ๑๙ แสดงผลการวิเคราะห์ความแตกต่าง (Gap Analysis) ระหว่างสถานะปัจจุบันและอนาคตของสถาปัตยกรรมองค์กรด้านธุรกิจ



รูปที่ ๒๓ ภาพรวมของกระบวนการธุรกิจในอนาคต

หมวดกระบวนการ	รายละเอียด
PC-C11: บริหารการขาย	มีจำนวนกิจกรรมมากเป็นอันดับ ๓ (๑๑๖ กิจกรรม) และมีจำนวนการตัดสินใจมากเป็นอันดับ ๓ (๒๖ ครั้ง)
PC-C14: บริการหลังการขาย	มีจำนวนการตัดสินใจมากเป็นอันดับ ๒ (๔๒ ครั้ง)
PC-S01: บริหารและพัฒนาบุคลากร	มีจำนวนกิจกรรมมากเป็นอันดับ ๑ (๓๐๓ กิจกรรม) มีจำนวนการตัดสินใจมากเป็นอันดับ ๑ (๔๔ ครั้ง) และมีการขออนุมัติหลายขั้นตอน
PC-S02: บริหารงานจัดซื้อ/จัดจ้าง	มีการขออนุมัติหลายขั้นตอน
PC-S03: บริหารงานพัสดุ	การตรวจนับครุภัณฑ์ประจำปียังคงใช้กระดาษในการจดบันทึกครุภัณฑ์ที่ตรวจสอบและจะนำข้อมูลที่จดบันทึกบนกระดาษมาบันทึกข้อมูลลงในระบบต่อไป ซึ่งข้อมูลที่ได้มานั้นอาจบันทึกไม่ครบถ้วนหรือบันทึกผิดส่งผลให้ต้องกลับไปตรวจสอบใหม่อีกครั้ง
PC-S05: บริหารการเงินและบัญชี	ขาดความเชื่อมโยงระหว่างกระบวนการ
PC-S12: บริหารฝ่ายอำนวยการ	มีจำนวนกิจกรรมมากเป็นอันดับ ๒ (๑๑๘ กิจกรรม) และมีจำนวนการตัดสินใจมากเป็นอันดับ ๓ (๒๖ ครั้ง)

PC-S13: บริหารงานแผนนโยบายและงบประมาณ	มีการแจ้งข้อมูลการโอนงบประมาณผ่านทางกระดาษ ทำให้ใช้เวลาประสานงานที่ค่อนข้างมากและอาจเกิดการสูญหายของข้อมูล

ตารางที่ ๑๙ แสดง Gap Analysis ของสถาปัตยกรรมด้านธุรกิจ

๔.๒ ด้านแอปพลิเคชัน (Applications)

จากผลการสำรวจและการวิเคราะห์สถานะปัจจุบันของสถาปัตยกรรมองค์กร ด้านแอปพลิเคชัน สามารถสรุปประเด็นปัญหาหลักและหลักการด้านแอปพลิเคชัน ได้ดังนี้

ประเด็นปัญหา (Issue)

๑) แอปพลิเคชันที่ใช้งานในปัจจุบัน ไม่ได้ครอบคลุมถึงกระบวนการปฏิบัติงานที่สำคัญ

๒) บางแอปพลิเคชันที่ใช้งานในปัจจุบันไม่สามารถตอบสนองความต้องการการใช้งาน เช่น การออกรายงานได้ตามความต้องการเนื่องจากบางแอปพลิเคชันก็ไม่สามารถพัฒนาเพิ่มเติมต่อยอดได้

ตารางที่ ๒๐ แสดงหมวดกระบวนการที่ยังไม่มีแอปพลิเคชันรองรับการดำเนินงาน ซึ่งพบว่ามีทั้งหมด ๘ หมวดกระบวนการที่ยังไม่มีแอปพลิเคชันรองรับ คิดเป็น 22% จากทั้งหมด ๓๖ หมวด

รหัส	หมวดกระบวนการ
PC-C01	กำหนดนโยบายรัฐบาลอิเล็กทรอนิกส์
PC-C03	วิจัยตลาด
PC-C05	วิจัยและพัฒนาผลิตภัณฑ์/บริการ
PC-C06	จัดทำต้นแบบและมาตรฐาน
PC-S10	กระบวนการบริหารการเปลี่ยนแปลง
PC-S16	จัดการทรัพย์สินทางปัญญา
PC-S18	สำรวจความพึงพอใจการใช้บริการ
PC-S20	ประเมินผลการให้บริการ

ตารางที่ ๒๐ แสดงหมวดกระบวนการที่ยังไม่มีแอปพลิเคชันรองรับการดำเนินงาน

ตารางที่ ๒๑ แสดงรายการแอปพลิเคชันที่ไม่สามารถเพิ่มเติมหรือปรับปรุงได้ เนื่องจากแอปพลิเคชันเหล่านี้เป็น ซอฟต์แวร์สำเร็จรูป ซึ่งพบว่ามีทั้งหมด ๔ แอปพลิเคชัน คิดเป็น 21% จากทั้งหมด ๑๙ แอปพลิเคชัน

รายการแอปพลิเคชัน
Welfare Management
Procurement Management
Financial Management
Asset Management

ตารางที่ ๒๑ แสดงแอปพลิเคชันที่ไม่สามารถเพิ่มเติมหรือปรับปรุงได้

หลักการด้านแอปพลิเคชัน (Application Principle)

๑) แอปพลิเคชันควรจะเชื่อมโยงกันผ่านทาง API: API จะช่วยให้แอปพลิเคชันที่มีสถาปัตยกรรมที่แตกต่างกันสามารถเชื่อมโยงข้อมูลกันได้สะดวก
๒) แอปพลิเคชันควรมีความพร้อมใช้อยู่เสมอ

ประเด็นปัญหาที่พบจากการวิเคราะห์และหลักการด้านแอปพลิเคชันถูกนำมาใช้เพื่อการดำเนินการออกแบบสถาปัตยกรรมองค์กรในอนาคตตามที่แสดงในรูปที่ ๒๔ จากรูปในส่วนของ Business Applications จะเห็นได้ว่ามี ๓ แอปพลิเคชันที่คาดว่าจะปรับปรุง ๖ แอปพลิเคชันที่คาดว่าจะยกเลิก และ ๔ แอปพลิเคชันที่คาดว่าจะนำเข้ามาใช้งาน ในส่วนของ Supporting Applications จะพบว่ามีเพียง Identiy Management (IDM) เท่านั้นที่จะถูกนำเข้ามาใช้เพื่อบริหารจัดการ User Accounts ในส่วนของ API คาดว่าจะมีการใช้เพื่อบริหารจัดการ Master Data ซึ่งจะดำเนินการนำร่องกับ ๖ ข้อมูล ตารางที่ ๒๒ แสดงผลการวิเคราะห์ความแตกต่าง (Gap Analysis) ระหว่างสถานะปัจจุบันและอนาคตของสถาปัตยกรรมองค์กรด้านแอปพลิเคชัน

รูปที่ ๒๔ ภาพรวมของแอปพลิเคชันในอนาคต

ชื่อแอปพลิเคชัน	รายละเอียด
Customer Relationship Management (CRM)	เป็นแอปพลิเคชันที่พัฒนาขึ้นมาแทน **Customer Management** เนื่องจากแอปพลิเคชันเดิมไม่ตอบสนองการใช้งานในปัจจุบัน ซึ่งมีสาเหตุมาจากบางบริการมีความซับซ้อนสูง
Contact Center	เป็นแอปพลิเคชันที่พัฒนาขึ้นมาให้ครอบคุมฟังก์ชันการทำงานของ **Contact Center** เดิม และ **Problem Tracking** เพื่อลดความซ้ำซ้อนของข้อมูล และจะเพิ่มฟังก์ชันการทำงานใหม่เข้าไปเพื่อตอบสนองกับกระบวนการดำเนินงานในปัจจุบัน
E-learning	เป็นแอปพลิเคชันที่ให้ลูกค้าเข้ามาเรียนรู้เกี่ยวกับเนื้อหาการอบรม เช่นการอบรม CIO การอบรม e-CMS และ IPV6 เป็นต้น ซึ่ง **E-learning** จะตอบสนองกระบวนการ **PC-C10** ผลิตภัณฑ์/บริการช่วงพัฒนา
Procurement Management	เป็นแอปพลิเคชันที่พัฒนาขึ้นมาแทน **Procurement Management** เดิมเนื่องจากแอปพลิเคชันเดิมไม่ครอบคลุมกระบวนการ **PC-S02** บริหารงานจัดซื้อจัดจ้างทั้งหมด และแอปพลิเคชันเดิมเป็นแอปพลิเคชันสำเร็จรูปซึ่งไม่สามารถปรับปรุงได้
Change Management	เป็นแอปพลิเคชันที่ใช้สำหรับบริหารจัดการการเปลี่ยนแปลง ซึ่งจะสอดคล้องกับกระบวนการ **PC-S10** บริหารการเปลี่ยนแปลง
Identity Management (IDM)	**IDM** จะทำหน้าที่เป็นตัวกลางในการปรับปรุง User Account ณ จุดเดียว เนื่องจาก User Account ถูกจัดกับไว้ในหลาย Servers เช่น OpenID (LDAP), Mail Service (LDAP) และ Policy Control (AD) ซึ่ง **IDM** จะตอบสนองกระบวนการ **PC-S09** บริหารความมั่นคงปลอดภัยระบบสารสนเทศ
Prodcut, Organization Structure, Employee, Customer, Supplier, and Asset Services	เป็น **API** สินค้าและผลิตภัณฑ์ โครงสร้างองค์กร พนักงาน ลูกค้า ผู้ขายและผู้ประสานความร่วมมือ และครุภัณฑ์ ซึ่ง **API** จะเป็นตัวบริหารจัดการ Master Data เพื่อลดความซ้ำซ้อนของข้อมูล ซึ่ง **API** จะตอบสนองกระบวนการ **PC-C09** พัฒนาผลิตภัณฑ์/บริการช่วงพัฒนา

ตารางที่ ๒๒ แสดง Gap Analysis ของสถาปัตยกรรมด้านแอปพลิเคชัน

๔.๓ ด้านข้อมูล (Data)

จากผลการสำรวจและการวิเคราะห์สถานะปัจจุบันของสถาปัตยกรรมองค์กรด้านข้อมูล สามารถสรุปประเด็นปัญหาและหลักการด้านข้อมูล ได้ดังนี้

ประเด็นปัญหา (Issue)

๑) มีการจัดเก็บข้อมูลที่ซ้ำซ้อนและยังขาดการบริหารจัดการ Master Data ที่ดี

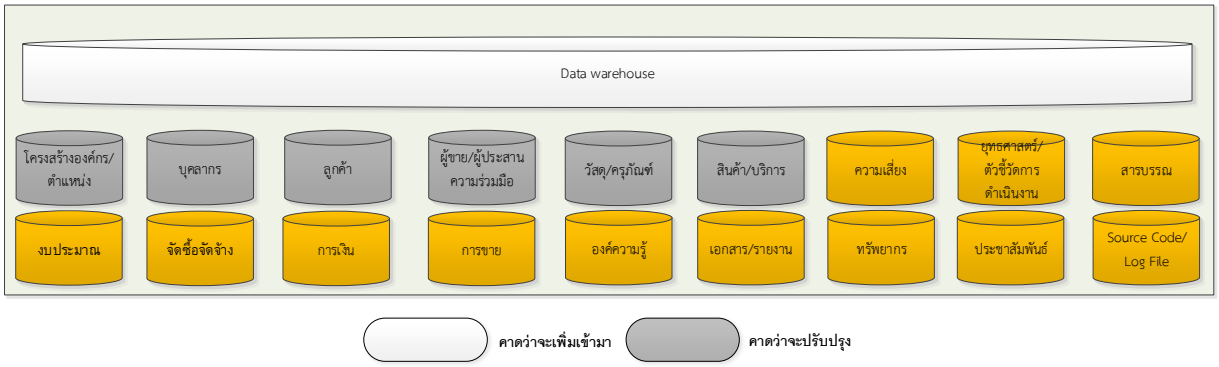
๒) ยังขาดผู้รับผิดชอบข้อมูลที่ชัดเจนสำหรับข้อมูลที่ใช้งานร่วมกัน ส่งผลให้ข้อมูลไม่ได้รับการทบทวนเปลี่ยนแปลงหรือแก้ไขให้เป็นปัจจุบัน

หลักการด้านข้อมูล (Data Principle)

๑) ควรมีการบริหารจัดการข้อมูลให้อยู่ในรูปแบบ Single Source โดยมีการกำหนด Data Operation และ Data Governance ที่เหมาะสม

๒) มุ่งเน้นไปสู่การเป็นองค์กรที่ใช้ข้อมูล เพื่อการตัดสินใจในการทำงาน (Data-driven Organization)

ประเด็นปัญหาที่พบจากการวิเคราะห์และหลักการด้านข้อมูลถูกนำมาใช้เพื่อการดำเนินการออกแบบสถาปัตยกรรมองค์กรในอนาคตตามที่แสดงในรูปที่ ๒๕ การวิเคราะห์ความแตกต่าง (Gap Analysis) เป็นไปตามที่แสดงในตารางที่ ๒๓



รูปที่ ๒๕ ภาพรวมข้อมูลในอนาคต

ชื่อข้อมูล	รายละเอียด
โครงสร้างองค์กร/ตำแหน่ง บุคลากร ลูกค้า ผู้ขาย/ผู้ประสานความร่วมมือ วัสดุ/ครุภัณฑ์ สินค้า/บริการ	ข้อมูล Master data เหล่านี้เป็นข้อมูลหลักขององค์กรที่ถูกนำมาใช้ตลาดทั้งองค์กรจึงควรที่จะถูกบริหารจัดการอยู่ที่จุดเดียว แล้วทำการแชร์ข้อมูลไปยังส่วนต่างๆ
Data warehouse	เป็นศูนย์รวมข้อมูลของทั้งองค์กรเพื่อมุ่งเน้นการนำเอาข้อมูลมาช่วยในการตัดสินใจของผู้บริหาร

ตารางที่ ๒๓ แสดง Gap Analysis ของสถาปัตยกรรมด้านข้อมูล

๔.๔ ด้านโครงสร้างพื้นฐาน (Infrastructure)

จากผลการสำรวจและการวิเคราะห์สถานะปัจจุบันของสถาปัตยกรรมองค์กรด้านข้อมูล สามารถสรุปประเด็นปัญหาและหลักการด้านโครงสร้างพื้นฐาน ได้ดังนี้

ประเด็นปัญหา (Issue)

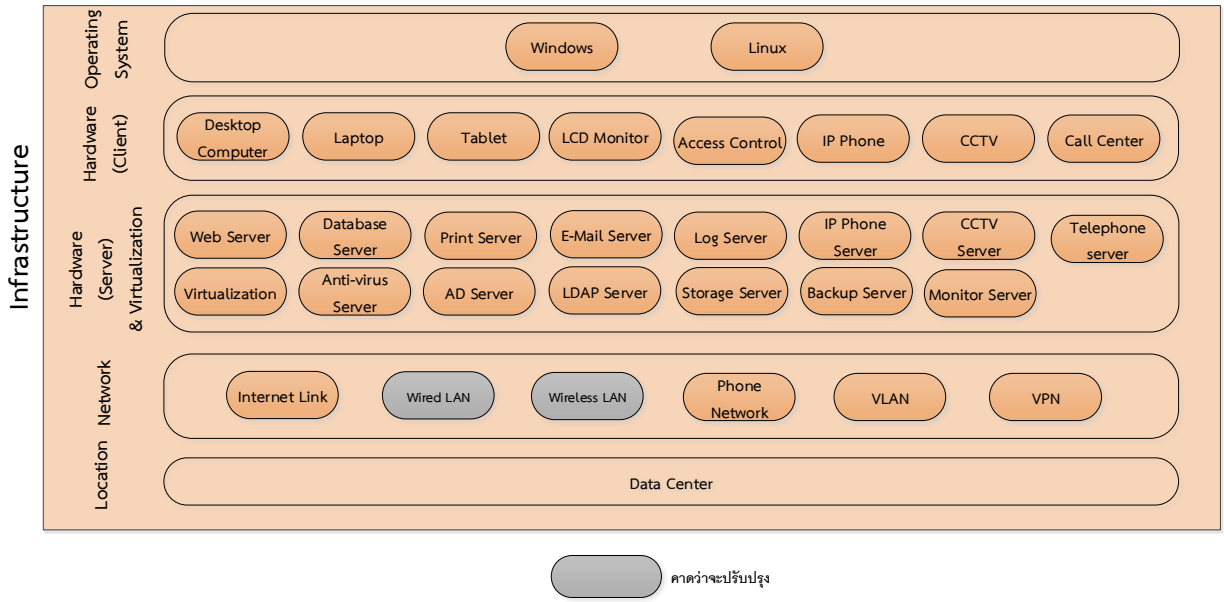
๑) เครือข่าย Wired LAN มีออกแบบที่ยากต่อการขยายตัว

๒) เครือข่าย Wireless LAN ขาดความต่อเนื่องในการให้บริการ

หลักการด้านโครงสร้างพื้นฐาน (Infrastructure Principle)

๑) พัฒนาโครงสร้างพื้นฐานสารสนเทศโดยใช้ Cloud Computing เป็นหลัก และเน้นการใช้ทรัพยากรร่วมกัน: มุ่งเน้นการใช้ Cloud Computing ทั้งในระดับ Infrastructure as a service (IaaS) Platform as a service (PaaS) และ Software as a service (SaaS)

ประเด็นปัญหาที่พบจากการวิเคราะห์และหลักการด้านโครงสร้างพื้นฐานถูกนำมาใช้เพื่อการดำเนินการออกแบบสถาปัตยกรรมองค์กรในอนาคตตามที่แสดงในรูปที่ ๒๖ การวิเคราะห์ความแตกต่าง (Gap Analysis) เป็นไปตามที่แสดงในตารางที่ ๒๔



รูปที่ ๒๖ ภาพรวมของโครงสร้างพื้นฐานในอนาคต

โครงสร้างพื้นฐาน	รายละเอียด
Wired LAN	เครือข่าย Wired LAN มีออกแบบที่ยากต่อการขยายตัว
Wireless LAN	เครือข่าย Wireless LAN ขาดความต่อเนื่องในการให้บริการ

ตารางที่ ๒๔ แสดง Gap Analysis ของสถาปัตยกรรมด้านโครงสร้างพื้นฐาน

๔.๕ ด้านความมั่นคงปลอดภัย (Security)

จากผลการสำรวจและการวิเคราะห์สถานะปัจจุบันของสถาปัตยกรรมองค์กรด้านความมั่นคงปลอดภัย สามารถสรุปประเด็นปัญหาและหลักการด้านความมั่นคงปลอดภัย ได้ดังนี้

ประเด็นปัญหา (Issue)

๑) มาตรฐานความมั่นคงปลอดภัย (ISO/IEC 27001) ถูกนำมาบังคับใช้เฉพาะส่วนงานที่เกี่ยวข้องการบริการ G-Cloud ระดับ Infrastructure as a service (IaaS)

๒) มีการระบุประเด็นปัญหาความเสี่ยง (Risk) แต่มีบางประเด็นยังไม่มีมาตรการควบคุมความเสี่ยง (Controls)

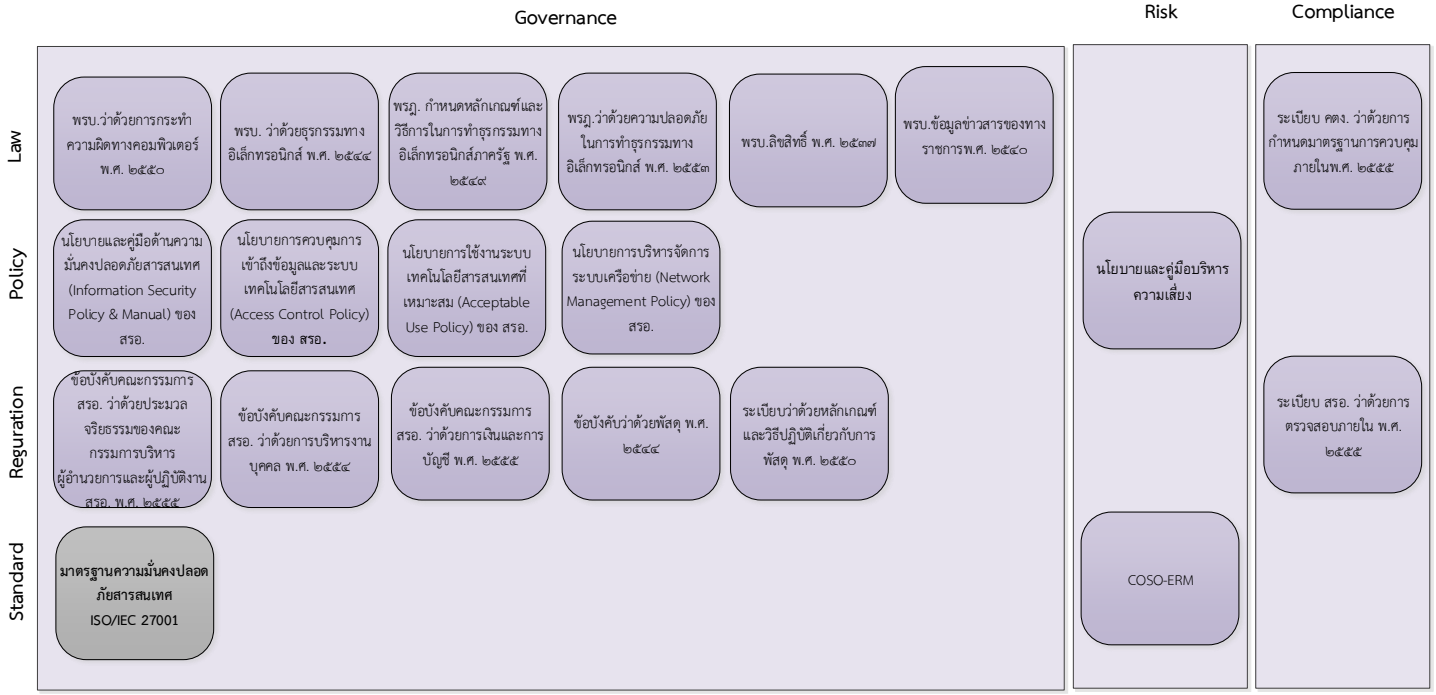
๓) บุคลากรยังไม่ได้ตระหนักเกี่ยวกับความมั่นคงปลอดภัยเท่าที่ควร (Awareness)

หลักการด้านความมั่นคงปลอดภัย (Security Principle)

๑) การปฏิบัติงานควรดำเนินงานได้อย่างต่อเนื่อง นั่นคือ ควรมีการจัดทำแผนความต่อเนื่องทางธุรกิจ (Business Continuity Plan) และการวางแผนกู้คืนกรณีเกิดภัยพิบัติ (Disaster Revery Plan)

๒) ตระหนักในด้านมั่นคงปลอดภัยสำหรับการพัฒนาสถาปัตยกรรมองค์ทั้งทางด้านธุรกิจ ด้านแอปพลิเคชัน ด้านข้อมูล และด้านโครงสร้างพื้นฐาน: ความมั่นคงปลอดภัยเข้ามามีส่วนเกี่ยวข้องกับด้านอื่นๆของสถาปัตยกรรมองค์กร

ประเด็นปัญหาที่พบจากการวิเคราะห์และหลักการด้านความมั่นคงปลอดภัยถูกนำมาใช้เพื่อการดำเนินการออกแบบสถาปัตยกรรมองค์กรในอนาคตเป็นไปตามที่แสดงในรูปที่ ๒๗ ขณะที่การวิเคราะห์ความแตกต่าง (Gap Analysis) เป็นไปตามที่แสดงในตารางที่ ๒๕



รูปที่ ๒๗ ภาพรวมของมาตรการควบคุมความมั่นคงปลอดภัยในอนาคต

ความมั่นคงปลอดภัย	รายละเอียด
ขยายขอบเขตการตรวจประเมิน ISO/IEC 27001	ขยายขอบเขตการตรวจประเมินระบบความมั่นคงปลอดภัยสารสนเทศตามมาตรฐาน ISO/IEC 27001 จากบริการ G-Cloud ในระดับ IaaS สู่บริการอื่นๆ
กำหนดมาตรการด้านความมั่นคงปลอดภัยให้เหมาะสมต่อความเสี่ยงที่จะเกิดขึ้น	ภัยคุกคาม (Threat) ที่เกิดขึ้นและความเสี่ยง (Risk) ทีอาจจะเกิดขึ้นจะต้องมีการกำหนดมาตรการด้านความมั่นคงปลอดภัยให้เหมาะสม
ผลักดันการปฏิบัติตามมาตรการการควบคุมความมั่นคงปลอดภัย (Compliance)	สนับสนุนให้บุคลากรตระหนักถึงความมั่นคงปลอดภัย พร้อมทั้งผลักดันการปฏิบัติตามมาตรการการควบคุมความมั่นคงปลอดภัย

ตารางที่ ๒๕ แสดง Gap Analysis ของสถาปัตยกรรมด้านความมั่นคงปลอดภัย

บทที่ ๕ แผนการดำเนินงาน (Roadmap)

การออกแบบสถาปัตยกรรมองค์กรในอนาคต ถูกกำหนดขึ้นมาจากการสำรวจความต้องการ ประเด็นปัญหาที่พบ และปัจจัยภายนอกอื่นๆ ดังนั้นแผนการดำเนินการจึงถูกจัดทำขึ้นเพื่อใช้เป็นแนวทางในการก้าวเข้าไปถึงสถาปัตยกรรมองค์กรในอนาตตามที่ได้ทำการออกแบบไว้ ดังรายละเอียดที่แสดงในตารางที่ ๒๖

สถาปัตยกรรมองค์กร	แผนการดำเนินงาน	คำอธิบาย	๒๕๕๘	๒๕๕๙	๒๕๖๐
ด้านธุรกิจ	■ กำหนดกระบวนการปฏิบัติงานให้เป็นมาตรฐาน	ขั้นตอนการปฏิบัติงานควรมีการนิยามให้ชัดเจน เข้าใจง่าย และมีการประกาศใช้อย่างเป็นทางการ รวมไปถึงการกำหนดเวลาในการปฏิบัติงาน (Operational Level Agreement)		✓	✓
	■ กำหนดผู้รับผิดชอบให้ชัดเจนในแต่กระบวนการ	เนื่องจากบางกระบวนการยังขาดผู้รับผิดชอบที่ชัดเจน มีผลทำให้เกิดความซ้ำซ้อนในอำนาจหน้าที่ของการปฏิบัติงาน		✓	✓
	■ พัฒนา/ปรับปรุงกระบวนการภายในให้มีความกระชับ สะดวก รวดเร็ว	เนื่องจากยังมีบางกระบวนการปฏิบัติงานมีขั้นตอนการปฏิบัติงานจำนวนมาก ส่งผลให้เกิดความล่าช้าในการดำเนินงาน		✓	✓
	■ ลดความซ้ำซ้อนของกระบวนการ	เพื่อความถูกต้องและลดเวลาในการปฏิบัติงาน		✓	✓
	■ สร้างความเชื่อมโยงในการปฏิบัติงาน	เพื่อเพิ่มความสามารถในการปฏิบัติงาน		✓	✓
	■ ลดการใช้กระดาษในการปฏิบัติงาน	เพื่อลดค่าใช้จ่ายขององค์กร		✓	✓
ด้านแอปพลิเคชัน	■ กำหนดกรอบการพัฒนา API สำหรับการเชื่อมโยงแอปพลิเคชัน	เพื่อเป็นมาตรฐานในการแลกเปลี่ยนข้อมูล		✓	
	■ พัฒนาแอปพลิเคชันให้ครอบคลุมกับกระบวนการที่สำคัญ	ดำเนินการพัฒนาแอปพลิเคชันให้แล้วเสร็จ ดังนี้ - CRM - e-Learning - Procurement - Contact Center - Change management	✓ ✓ ✓	✓ ✓ ✓ ✓	✓
	■ ปรับปรุงแอปพลิเคชันให้ครอบคลุมกับกระบวนการที่สำคัญและสอดคล้องกับความต้องการใช้งานมากขึ้น	ดำเนินการปรับปรุงแอปพลิเคชันให้แล้วเสร็จ ดังนี้ - Human Resource Mgt. - Asset Mgt. - EGA Back-end		✓ ✓ ✓	

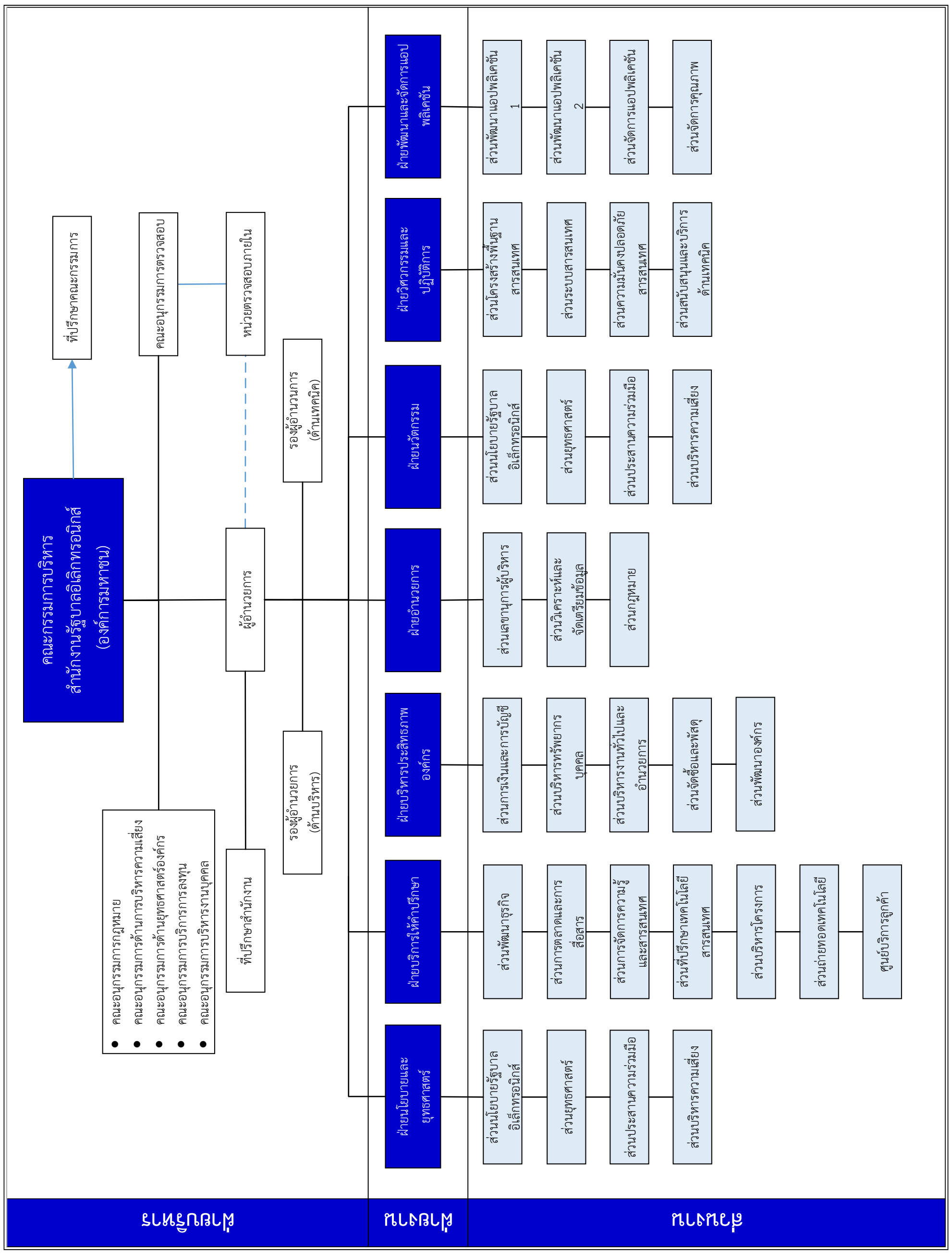
ด้านข้อมูล	■ บริหารจัดการ Master Data (Master Data Management)	นิยาม Data Integration Architecture Integrate Master Data และ Replicate Master Data	✓	✓	
	■ บริหารจัดการ Data Operation (Data Operation Management)	ควบคุม Archive, Retrieve and Purge Data วางแผนและควบคุม Data Backup และ Data Recovery ตรวจสอบประสิทธิภาพและปรับแต่ง Database	✓	✓	✓
	■ ธรรมมาภิบาลข้อมูล (Data Governance)	กำหนด Data Steward พัฒนา Data Architecture ติดตามเพื่อให้มั่นใจว่าการบริหารจัดการข้อมูลเป็นไปตาม นโยบายข้อมูล (Data Policy)	✓	✓	✓
	■ มุ่งเน้นการใช้ข้อมูลในการตัดสินใจ	Data Warehouse Business Intelligent และ Predictive Analytics		✓	✓
ด้านโครงสร้างพื้นฐาน	■ ปรับปรุงเครือข่าย Wired LAN	เครือข่ายมีการออกแบบที่ยากต่อการขยายตัวของอุปกรณ์เชื่อมต่อ		✓	
	■ ปรับปรุงเครือข่าย Wireless LAN	จากผลสำรวจการให้บริการพบว่าความต่อเนื่องของเครือข่ายยังไม่เป็นที่พอใจของพนักงาน		✓	
ด้านความมั่นคงปลอดภัย	■ ประยุกต์ใช้มาตรการความมั่นคงปลอดภัยและธรรมาภิบาลในการให้บริการหรือปฏิบัติงาน	- ขยายขอบเขตการตรวจประเมินตามมาตรฐาน ISO/IEC 27001 จาก G-Cloud ในระดับ IaaS สู่บริการอื่นๆ		✓	✓
	■ มีความต่อเนื่องในการปฏิบัติงาน	จัดทำแผนความต่อเนื่องทางธุรกิจ (Business Continuity Plan) และการวางแผนกู้คืนกรณีเกิดภัยพิบัติ (Disaster Revery Plan) เพื่อให้แน่ใจได้ว่าหากมีเหตุการณ์ผิดปกติเกิดขึ้น (Incident) การดำเนินงานธุรกิจยังสามารถดำเนินต่อไปได้ - Business Continuity Plan - Disaster Revery Plan	✓ ✓	✓	✓
	■ บริหารจัดการความเสี่ยง (Risk Management)	กำหนดมาตรการด้านความมั่นคงปลอดภัยสารสนเทศที่อิงผลการประเมินความเสี่ยง		✓	
	■ การปฏิบัติตามข้อกำหนด (Compliance)	ตรวจสอบความสอดคล้องกันระหว่างนโยบาย/มาตรฐานด้านความมั่นคงปลอดภัยกับกฎหมาย		✓	

ตารางที่ ๒๖ แสดงแผนดำเนินงาน (Roadmap)

ภาคผนวก

ภาคผนวก ก

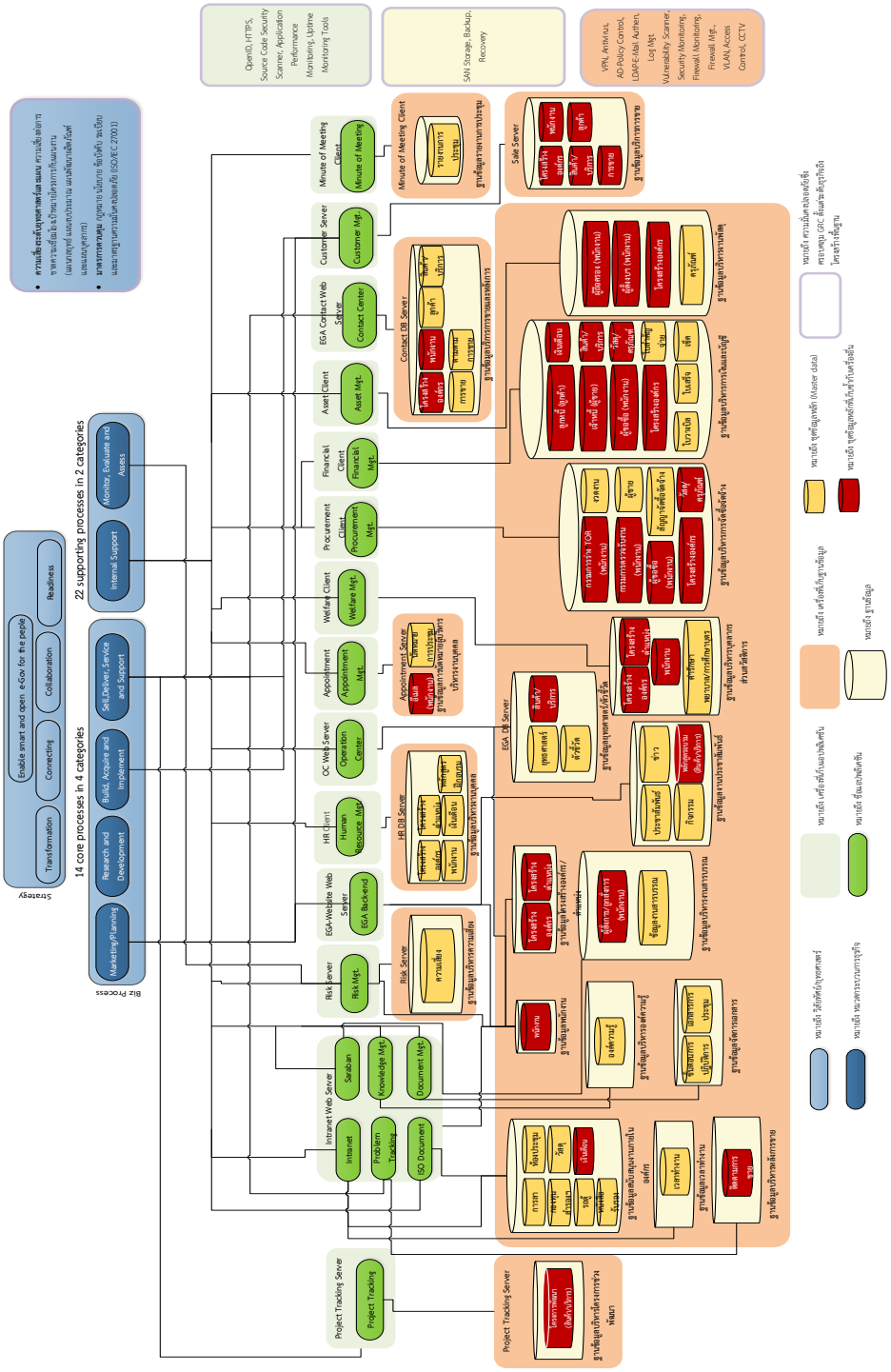
ในส่วนนี้แสดงโครงสร้างองค์กร ตามประกาศสำนักงาน ที่ ๑/๒๕๕๗ เรื่อง โครงสร้างองค์กร : สำนักงานรัฐบาลอิเล็กทรอนิกส์ (องค์การมหาชน) ณ วันที่ ๒๑ กุมภาพันธ์ ๒๕๕๗ โดยแบ่งข้อมูลเป็น ๓ ระดับ ประกอบไปด้วย ฝ่ายบริหาร ฝ่ายงาน และส่วนงาน



รูปที่ ๒๘ ไดอะแกรมโครงสร้างองค์กร

ภาคผนวก ข

ในส่วนนี้จะแสดงไดอะแกรมความซื่อมโยงภาพรวมสถาปัตยกรรมองค์กร ประกอบไปด้วย ด้านธุรกิจ ด้านข้อมูล ด้านแอปพลิเคชัน ด้านโครงสร้างพื้นฐาน และด้านความมั่นคงปลอดภัย ตามที่แสดงในรูปที่ ๒๙



รูปที่ ๒๙ ไดอะแกรมความเชื่อมโยงสถาปัตยกรรมองค์กร

ภาคผนวก ค

ตารางแสดงความสัมพันธ์ระหว่างข้อกำหนดของมาตรฐาน ISO/IEC27001:2013 กับแบบจำลองทั้ง ๔ ด้านประกอบไปด้วย ธุรกิจ (BRM) แอปพลิเคชัน (ARM) ข้อมูล (DRM) และโครงสร้างพื้นฐาน (IRM) และความสัมพันธ์ระหว่างข้อกำหนดของมาตรฐาน กับ กฎหมาย นโยบาย ข้อบังคับ และระเบียบที่เกี่ยวข้อง

Clause/ Control ID	Clause, Control Name or Requirement Text	Class	BRM	BRM	BRM	IRM	ARM	DRM		มาตรการการควบคุมความมั่นคงปลอดภัย																		
			Establish Policy and procedure	Planning and training	Monitoring, Response and reporting	Security Infrastructure and networks (incl physical security)	Securing platform& application	Securing Data		พรบ.ว่าด้วยการกระทำความผิดทางคอมพิวเตอร์ พ.ศ. ๒๕๕๐	พรบ. ว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๔๔	พรฎ.ว่าด้วยความปลอดภัยในการทำธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ.	พรบ.ลิขสิทธิ์ พ.ศ. ๒๕๓๗	พรบ.ข้อมูลข่าวสารของทางราชการพ.ศ. ๒๕๔๐	ระเบียบว่าด้วยความลับของทางราชการ พ.ศ. ๒๕๔๔	ระเบียบ คตง. ว่าด้วยการกำหนดมาตรฐานการควบคุมภายในพ.ศ.	นโยบายความมั่นคงปลอดภัยสารสนเทศ	คู่มือความมั่นคงปลอดภัยสารสนเทศ	นโยบายการควบคุมการเข้าถึงข้อมูลและระบบเทคโนโลยีสารสนเทศ	นโยบายการใช้งานระบบเทคโนโลยีสารสนเทศ	นโยบายการบริหารจัดการระบบเครือข่าย	นโยบายและคู่มือบริหารความเสี่ยง	ข้อบังคับพัสดุ	ระเบียบพัสดุ	ระเบียบ สรอ. ว่าด้วยการตรวจสอบภายใน พ.ศ. ๒๕๕๕
Cl. 4	Context of the organization																											
Cl.4.1	Understanding the organization and its context	Management	×															×										
Cl.4.2	Understanding the needs and expectations of interested	Management	×															×										
Cl.4.3	Determining the scope of the information security	Management	×															×										
Cl.4.4	Information security management system	Management	×															×										
Cl.5	Leadership																											
Cl.5.1	Leadership and commitment	Management	×															×										
Cl.5.2	Policy	Management	×	×						×		×	×	×	×		×	×	×	×	×	×	×	×				
Cl.5.3	Organizational roles, resposubilities and authorities	Management	×															×										
Cl.6	Planning																											
Cl.6.1	Actions to address risk and opputunities																											
Cl.6.1.1	General	Management		×														×										
Cl.6.1.2	information security risk assessment	Management	×		×													×						×				
Cl.6.1.3	Information security risk treatment	Management	×	×	×													×						×				
Cl.6.2	Information security objectives and planning to achieve	Management	×	×	×													×										
Cl.7	Support																											
Cl.7.1	Resources	Management	×															×										
Cl.7.2	Competence	Management	×	×														×										
Cl.7.3	Awareness	Management		×														×										
Cl.7.4	Communication	Management	×															×										
Cl.7.5	Documented information	Management	×															×										
Cl.7.5.1	General	Management	×															×										
Cl.7.5.2	Creating and updating	Management	×															×										
Cl.7.5.3	Control of documented information	Management	×															×										
Cl.8	Operation																											
Cl.8.1	Operational planning and control	Management	×	×														×										
Cl.8.2	Information security risk assessment	Management	×	×	×													×						×				
Cl.8.3	Information security risk treatment	Management	×	×	×													×						×				
Cl.9	Performance evaluation																											
Cl.9.1	Monitoring, measurement, analysis and evaluation	Management	×		×													×										
Cl.9.2	Internal audit	Management	×	×	×													×										
Cl.9.3	Management review	Management	×	×	×													×										
Cl.10	Improvement																											
Cl.10.1	Nonconformity and corrective action	Management	×		×													×										
Cl.10.2	Continual improvement	Management	×															×										

Clause/ Control ID	Clause, Control Name or Requirement Text	Class	BRM	BRM	BRM	IRM	ARM	DRM		มาตรการการควบคุมความมั่นคงปลอดภัย																		
			Establish Policy and procedure	Planning and training	Monitoring, Response and reporting	Security infrastructure and networks (incl physical security)	Securing platform& application	Securing Data		พรบ.ว่าด้วยการกระทำความผิดทางคอมพิวเตอร์ พ.ศ. ๒๕๕๐	พรบ. ว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๔๔	พรฎ.ว่าด้วยความปลอดภัยในการทำธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ.	พรบ.ลิขสิทธิ์ พ.ศ. ๒๕๓๗	พรบ.ข้อมูลข่าวสารของทางราชการพ.ศ. ๒๕๔๐	ระเบียบว่าด้วยความลับของทางราชการ พ.ศ. ๒๕๔๔	ระเบียบ คตง. ว่าด้วยการกำหนดมาตรฐานการควบคุมภายในพ.ศ.	นโยบายความมั่นคงปลอดภัยสารสนเทศ	คู่มือความมั่นคงปลอดภัยสารสนเทศ	นโยบายการควบคุมการเข้าถึงข้อมูลและระบบเทคโนโลยีสารสนเทศ	นโยบายการใช้งานระบบเทคโนโลยีสารสนเทศ	นโยบายการบริหารจัดการระบบเครือข่าย	นโยบายและคู่มือบริหารความเสี่ยง	ข้อบังคับไฟสัตู	ระเบียบไฟสัตู	ระเบียบ สรอ. ว่าด้วยการตรวจสอบภายใน พ.ศ. ๒๕๕๕
Annex A.																												
A.5	Information Security Policy																											
A.5.1	Information Security Policy																											
A.5.1.1	Policies for information security	Management	×									×					×											
A.5.1.2	Review of the policies for information security	Management	×									×					×											
A.6	Internal Organization																											
A.6.1	Internal Organization																											
A.6.1.1	Information security roles and responsibilities	Management	×									×					×											
A.6.1.2	Segregation of duties	Management	×									×					×											
A.6.1.3	Contact with authorities	Management	×									×					×											
A.6.1.4	Contact with special interest group	Management	×									×					×											
A.6.1.5	Information security in project management	Management	×		×			×				×					×											
A.6.2	Mobile devices and teleworking																											
A.6.2.1	Moblie device policy	Management	×									×					×			×								
A.6.2.2	Teleworking	Management	×									×					×											
A.7	Human Resource Security																											
A.7.1	Prior to employment																											
A.7.1.1	Screening	Management	×									×					×											
A.7.1.2	Term and conditions of employment	Management	×									×					×											
A.7.2	During employment																											
A.7.2.1	Management responsibilities	Management	×									×					×											
A.7.2.2	Information security, awareness, education and training	Management	×	×								×					×											
A.7.2.3	Disciplinary	Management	×									×					×											
A.7.3	Termination and change of employment																											
A.7.3.1	Termination or change of employment responsibilities	Management	×									×					×											
A.8	Asset Management																											
A.8.1	Responsibility for assets																											
A.8.1.1	Inventory of assets	Management	×		×							×					×									×	×	
A.8.1.2	Ownership of assets	Management	×									×					×									×	×	
A.8.1.3	Acceptable use of assets	Management	×									×					×									×	×	
A.8.1.4	Return of assets	Management	×									×					×									×	×	
A.8.2	Information Classification																											
A.8.2.1	Classification of information	Management	×					×		×		×		×			×			×								
A.8.2.2	Labeling of information	Management	×					×		×		×			×		×			×								
A.8.2.3	Handling	Management	×					×		×		×			×		×			×								
A.8.3	Media Handling																											
A.8.3.1	Management of removable media	Management	×					×				×					×			×								
A.8.3.2	Disposal of media	Management	×					×				×			×		×			×								
A.8.3.3	Physical media transfer	Management	×					×				×			×		×			×								
A.9	Access Control																											
A.9.1	Business requirements of access control																											
A.9.1.1	Access control policy	Management	×					×		×		×					×		×									
A.9.1.2	Access to networks and network services	Technical				×						×					×		×	×								

Clause/ Control ID	Clause, Control Name or Requirement Text	Class	BRM	BRM	BRM	IRM	ARM	DRM		มาตรการการควบคุมความมั่นคงปลอดภัย																		
			Establish Policy and procedure	Planning and training	Monitoring, Response and reporting	Security infrastructure and networks (incl physical security)	Securing platform& application	Securing Data		พรบ.ว่าด้วยการกระทำความผิดทางคอมพิวเตอร์ พ.ศ. ๒๕๕๐	พรบ. ว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๔๔	พรฎ.ว่าด้วยความปลอดภัยในการทำธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ.	พรบ.ลิขสิทธิ์ พ.ศ. ๒๕๓๗	พรบ.ข้อมูลข่าวสารของทางราชการพ.ศ. ๒๕๔๐	ระเบียบว่าด้วยความลับของทางราชการ พ.ศ. ๒๕๔๔	ระเบียบ คตง. ว่าด้วยการกำหนดมาตรฐานการควบคุมภายในพ.ศ.	นโยบายความมั่นคงปลอดภัยสารสนเทศ	คู่มือความมั่นคงปลอดภัยสารสนเทศ	นโยบายการควบคุมการเข้าถึงข้อมูลและระบบเทคโนโลยีสารสนเทศ	นโยบายการใช้งานระบบเทคโนโลยีสารสนเทศ	นโยบายการบริหารจัดการระบบเครือข่าย	นโยบายและคู่มือบริหารความเสี่ยง	ข้อบังคับพัสดุ	ระเบียบพัสดุ	ระเบียบ สรอ. ว่าด้วยการตรวจสอบภายใน พ.ศ. ๒๕๕๕
A.9.2	User Access management																											
A.9.2.1	User registration and deregistration	Technical					×	×				×					×		×									
A.9.2.2	User access provisioning	Technical					×	×				×					×		×									
A.9.2.3	Management of privileged access right	Technical					×	×				×					×		×									
A.9.2.4	Management of secret authentication information of	Technical						×				×					×		×									
A.9.2.5	Review of user access right	Technical					×	×				×					×		×									
A.9.2.6	Removal or adjustment of access right	Technical					×	×				×					×		×									
A.9.3	User responsibilities																											
A.9.3.1	Use of secret authentication information	Technical						×				×					×		×									
A.9.4	System and application access control																											
A.9.4.1	Information access retriction	Technical	×				×	×				×					×		×									
A.9.4.2	Secure log-on procedures	Technical	×				×	×				×					×		×									
A.9.4.3	Password management system	Management						×				×					×		×	×								
A.9.4.4	Use of priveilleged utility programs	Technical					×	×				×					×		×									
A.9.4.5	Access control to program source code	Technical					×	×				×					×		×									
A.10	Crytography																											
A.10.1	Operational Procedures and Responsibilities																											
A.10.1.1	Policy on the use of crytographic controls	Management	×					×									×											
A.10.1.2	Key management	Management	×					×									×											
A.11	Physical and environmental security																											
A.11.1	Secure areas																											
A.11.1.1	Physical secuirty perimeter	Management				×						×					×											
A.11.1.2	Physical entry controls	Management				×						×					×											
A.11.1.3	Securing office, room and facilities	Management				×						×					×											
A.11.1.4	Protecting against external and environmental threats	Management				×						×					×											
A.11.1.5	Working in secure areas	Management	×			×						×					×											
A.11.1.6	Delivery and loading areas	Management				×						×					×											
A.11.2	Equipment																											
A.11.2.1	Equipment sitting and protection	Management				×						×					×											
A.11.2.2	Supporting Utilities	Management				×						×					×											
A.11.2.3	Cabling security	Technical				×						×					×											
A.11.2.4	Equipment maintenance	Management				×						×					×											
A.11.2.5	Removal of assets	Management				×		×				×					×											
A.11.2.6	Security of equipment and assets off- premises	Management				×		×				×					×											
A.11.2.7	Secure disposal or re-use of equipment	Management				×		×				×					×											
A.11.2.8	Unattended user equipment	Management				×						×					×											
A.11.2.9	Clear desk clear screen policy	Management	×			×		×				×			×		×			×								
A.12	Operation Security																											
A.12.1	Operational Procedures and Responsibilities																											
A.12.1.1	Documented operating procedures	Management	×									×					×											
A.12.1.2	Change Management	Management	×									×					×											
A.12.1.3	Capacity Management	Management			×							×					×											
A.12.1.4	Separation of development, testing and operational	Management				×						×					×											

Clause/ Control ID	Clause, Control Name or Requirement Text	Class	BRM	BRM	BRM	IRM	ARM	DRM	มาตรการการควบคุมความมั่นคงปลอดภัย																		
			Establish Policy and procedure	Planning and training	Monitoring, Response and reporting	Security infrastructure and networks (incl physical security)	Securing platform& application	Securing Data	พรบ.ว่าด้วยการกระทำความผิดทางคอมพิวเตอร์ พ.ศ. ๒๕๕๐	พรบ. ว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๔๔	พรฎ.ว่าด้วยความปลอดภัยในการทำธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ.	พรบ.ลิขสิทธิ์ พ.ศ. ๒๕๓๗	พรบ.ข้อมูลข่าวสารของทางราชการพ.ศ. ๒๕๔๐	ระเบียบว่าด้วยความลับของทางราชการ พ.ศ. ๒๕๔๔	ระเบียบ คตง. ว่าด้วยการกำหนดมาตรฐานการควบคุมภายในพ.ศ.	นโยบายความมั่นคงปลอดภัยสารสนเทศ	คู่มือความมั่นคงปลอดภัยสารสนเทศ	นโยบายการควบคุมการเข้าถึงข้อมูลและระบบเทคโนโลยีสารสนเทศ	นโยบายการใช้งานระบบเทคโนโลยีสารสนเทศ	นโยบายการบริหารจัดการระบบเครือข่าย	นโยบายและคู่มือปฏิบัติการความเสี่ยง	ข้อบังคับฯสุด	ระเบียบฯสุด	ระเบียบ สรอ. ว่าด้วยการตรวจสอบภายในฯ พ.ศ. ๒๕๕๕
A.12.2	Protection from malware																										
A.12.2.1	Controls against malware	Technical				×					×						×										
A.12.3	Backup																										
A.12.3.1	Information backup	Management	×					×			×			×		×											
A.12.4	Logging and monitoring																										
A.12.4.1	Event logging	Technical			×				×		×						×										
A.12.4.2	Protection of log information	Technical			×	×		×	×		×						×										
A.12.4.3	Administrator and operator logs	Technical			×				×		×						×										
A.12.4.4	Clock synchronization	Technical			×						×						×										
A.12.5	Control of oprational software																										
A.12.5.1	Installalation of software on oprational systems	Management	×			×					×	×					×										
A.12.6	Technical Vulnerability Management																										
A.12.6.1	Management of technical vulnerabilities	Management			×	×		×			×						×										
A.12.6.2	Restriction on software installation	Technical			×	×		×			×	×					×										
A.12.7	Information System audit considerations																										
A.12.7.1	Information systems audit controls	Technical		×							×					×	×										
A.13	Communications security																										
A.13.1	Network security management																										
A.13.1.1	Network controls	Management	×		×	×	×				×						×				×						
A.13.1.2	Security of network services	Technical				×					×						×				×						
A.13.1.3	Segregation in networks	Technical				×					×						×				×						
A.13.2	Information Transfer																										
A.13.2.1	Information Transfer policies and procedures	Management	×					×		×	×			×			×										
A.13.2.2	Agreements on information transfer	Management						×		×				×			×				×						
A.13.2.3	Electronic messaging	Management						×		×	×			×			×				×						
A.13.2.4	Confidentiality or non-disclosure agreements	Management	×					×		×				×			×				×						
A.14	Information systems acquisition, development and																										
A.14.1	Security requirements of information systems																										
A.14.1.1	Information security requirements analysis and	Management			×						×																
A.14.1.2	Securing Application services on public networks	Technical				×	×				×						×										
A.14.1.3	Protecting application service transactions	Technical			×		×				×						×										
A.14.2	Security in developmant and support processes																×										
A.14.2.1	Secure development policy	Management	×				×				×						×										
A.14.2.2	System change control procedures	Management	×				×				×						×										
A.14.2.3	Technical review of applications after operating platform	Technical					×				×						×										
A.14.2.4	Restriction on changes to software packages	Technical					×				×	×					×										
A.14.2.5	Secure system engineering principles	Technical	×				×				×						×										
A.14.2.6	Secure development environment	Technical					×				×						×										
A.14.2.7	Outsourced development	Technical			×			×			×						×										
A.14.2.8	System security testing	Technical					×				×						×										
A.14.2.9	System acceptance testing	Technical					×				×						×										

Clause/ Control ID	Clause, Control Name or Requirement Text	Class	BRM	BRM	BRM	IRM	ARM	DRM		มาตรการการควบคุมความมั่นคงปลอดภัย																		
			Establish Policy and procedure	Planning and training	Monitoring, Response and reporting	Security infrastructure and networks (incl physical security)	Securing platform& application	Securing Data		พรบ.ว่าด้วยการกระทำความผิดทางคอมพิวเตอร์ พ.ศ. ๒๕๕๐	พรบ. ว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๔๔	พรฎ.ว่าด้วยความปลอดภัยในการทำธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ.	พรบ.ลิขสิทธิ์ พ.ศ. ๒๕๓๗	พรบ.ข้อมูลข่าวสารของทางราชการพ.ศ. ๒๕๔๐	ระเบียบว่าด้วยความลับของทางราชการ พ.ศ. ๒๕๔๔	ระเบียบ คตง. ว่าด้วยการกำหนดมาตรฐานการควบคุมภายในพ.ศ.	นโยบายความมั่นคงปลอดภัยสารสนเทศ	คู่มือความมั่นคงปลอดภัยสารสนเทศ	นโยบายการควบคุมการเข้าถึงข้อมูลและระบบเทคโนโลยีสารสนเทศ	นโยบายการใช้งานระบบเทคโนโลยีสารสนเทศ	นโยบายการบริหารจัดการระบบเครือข่าย	นโยบายและคู่มือบริหารความเสี่ยง	ข้อบังคับพัสดุ	ระเบียบพัสดุ	ระเบียบ สรอ. ว่าด้วยการตรวจสอบภายใน พ.ศ. ๒๕๕๕
A.14.3	Test data																											
A.14.3.1	Protection of test data	Technical						×				×						×										
A.15	Supplier relationships																											
A.15.1	Information security in supplier relationship																											
A.15.1.1	Information security policy for supplier relationships	Management	×					×						×	×			×										
A.15.1.2	Addressing security within supplier agreements	Management				×								×	×			×										
A.15.1.3	Information and communication technology supply	Management						×						×	×			×										
A.15.2	Supplier service delivery management																											
A.15.2.1	Monitoring and review of supplier services	Management			×							×						×										
A.15.2.2	Managing change to supplier services	Management	×									×																
A.16	Information security incident management																											
A.16.1	Management of information security incidents and																											
A.16.1.1	Responsibilities and procedures	Management	×		×							×						×			×							
A.16.1.2	Reporting information security events	Management			×							×						×			×							
A.16.1.3	Reporting information security weaknesses	Management			×							×						×										
A.16.1.4	Assessment of and decision on information security	Management			×							×						×										
A.16.1.5	Response to information security incidents	Management	×		×							×						×										
A.16.1.6	Learning from information security incidents	Management			×							×						×										
A.16.1.7	Collection of evidence	Management	×									×		×	×			×										
A.17	Information security aspects of business continuity																											
A.17.1	Information security continuity																											
A.17.1.1	Planning information security continuity	Management		×								×						×										
A.17.1.2	Implementing information security continuity	Management	×									×						×										
A.17.1.3	Verify, review and evaluate information security	Management			×							×						×										
A.17.2	Redundancies	Management				×	×	×				×						×										
A.17.2.1	Avalibility of information processing facilities	Management						×				×						×										
A.18	Compliance																											
A.18.1	Compliance with legal and contractual requirements																											
A.18.1.1	Identification of applicable legislation and contractual	Management	×							×	×	×	×	×	×			×	×									
A.18.1.2	Intellectual property rights	Management	×					×				×	×					×										
A.18.1.3	Protection of records	Management						×				×		×	×			×										
A.18.1.4	Privacy and protection of personal identifiable	Management						×				×		×	×			×			×							
A.18.1.5	Regulation of crytographip controls	Technical						×			×	×			×			×										
A.18.2	Information security reviews																											
A.18.2.1	Independent review of information security	Management	×	×								×				×	×	×										×
A.18.2.2	Compliance with security policies and standards	Management	×							×	×	×	×	×	×	×	×	×			×				×	×	×	
A.18.2.3	Technical compliance review	Technical	×									×						×										

ตารางที่ ๒๗ ตารางความสัมพันธ์ระหว่างข้อกำหนดมาตรฐาน ISO/IEC27001:2013 กับแบบจำลองสถาปัตยกรรมองค์กรทั้ง ๕ ด้าน รวมถึง นโยบาย ข้อบังคับ ระเบียบ และกฎหมายที่เกี่ยวข้อง

ภาคผนวก ง

ตารางแสดงความเชื่อมโยงรายการ Work Products กับมุมมองต่างๆ ทั้งมุมมอง Manager มุมมอง Developer และมุมมอง User ที่แต่ละมุมมองแบ่งตามแบบจำลองประกอบไปด้วย ธุรกิจ (BRM) แอปพลิเคชัน (ARM) ข้อมูล (DRM) โครงสร้างพื้นฐาน (IRM) และ ความมั่นคงปลอดภัย (SRM)

รายการ	Work Product	Manager					Developer					User				
		BRM	ARM	DRM	IRM	SRM	BRM	ARM	DRM	IRM	SRM	BRM	ARM	DRM	IRM	SRM
1	ไดอะแกรมความเชื่อมโยงยุทธศาสตร์ ตัวชี้วัดองค์กร และบริการ	■														
2	ไดอะแกรมโครงสร้างองค์กร	■														
3	ไดอะแกรมความเชื่อมโยงสถาปัตยกรรมองค์กร	■	■	■	■											
4	ไดอะแกรมเครือข่าย				■											
5	ภาพสถานะปัจจุบันของสถาปัตยกรรมองค์กร	■	■	■	■	■										
6	ภาพสถานะในอนาคตของสถาปัตยกรรมองค์กรค์กร	■	■	■	■	■										
7	ภาพรวมของกระบวนการธุรกิจ						■									
8	ภาพรวมของแอปพลิเคชัน							■								
9	ภาพรวมของข้อมูล								■							
10	ภาพรวมของโครงสร้างพื้นฐาน									■						
11	ภาพรวมของมาตรการควบคุมความมั่นคงปลอดภัยในอนาคต										■					
12	รายการของกระบวนการปฏิบัติงาน						■									
13	รายการของแอปพลิเคชัน							■								
14	รายการของข้อมูล								■							
15	รายการของโครงสร้างพื้นฐาน									■						
16	รายการของมาตรการควบคุมความมั่นคงปลอดภัย										■					
17	ตารางความสัมพันธ์ระหว่างกระบวนการปฏิบัติงานและส่วนงาน											■				
18	ตารางความสัมพันธ์ระหว่างแอปพลิเคชันกับเทคโนโลยี															
19	ตารางความสัมพันธ์ระหว่างแอปพลิเคชันธุรกิจและส่วนงาน												■			
20	ตารางความสัมพันธ์ระหว่างแอปพลิเคชันสนับสนุนและส่วนงาน												■			
21	ตารางความสัมพันธ์ระหว่างแอปพลิเคชันภายนอกและแอปพลิเคชันภายในสำนักงาน								■							
22	ตารางความสัมพันธ์ระหว่างข้อมูลและแอปพลิเคชัน							■	■							
23	ตารางความสัมพันธ์ระหว่างโครงสร้างพื้นฐานและแอปพลิเคชันธุรกิจ							■		■						
24	ตารางความสัมพันธ์ระหว่างโครงสร้างพื้นฐานและแอปพลิเคชันสนับสนุน							■		■						
25	ตารางความสัมพันธ์ระหว่างมาตรการควบคุมความมั่นคงปลอดภัยกับส่วนงาน															■
26	ตารางความสัมพันธ์ระหว่างข้อกำหนดมาตรฐานกับสถาปัตยกรรมด้านต่างๆรวมถึงมาตรการควบคุมความปลอดภัย										■					

ตารางที่ ๒๘ ตารางความเชื่อมโยงรายการ Work Products กับมุมมองด้านต่างๆ

อภิธานศัพท์

คำศัพท์	คำอธิบาย
สถาปัตยกรรมองค์กร (Enterprise Architecture)	กระบวนในการนำเอาเทคโนสารสนเทศ (Information Technology) มาสนับสนุนการดำเนินงานธุรกิจ (Business) ให้เกิดประสิทธิภาพ (Efficiency) และประสิทธิผล (Effectiveness) สูงสุดต่อองค์กร
Enterprise Architecture Framework (กรอบสถาปัตยกรรมองค์กร)	แนวทางในการจัดทำและการนำเอาสถาปัตกรรมองค์กรไปใช้งาน
Enterprise Architecture Development Process (กระบวนการพัฒนาสถาปัตยกรรมองค์กร)	การกำหนดลำดับขั้นตอนการพัฒนาสถาปัตกรรมองค์กรอย่างเป็นระบบเพื่อให้ได้ผลของมุมมองและสถาปัตยกรรมองค์กรในด้านต่างๆ (Work Product) ซึ่งอาจจะอยู่ในรูปแบบของรายการ (Catalog) ตารางการเชื่อมโยง (Matrix) และไดอะแกรม (Diagram)
Enterprise Architecture Viewpoint (มุมมองสถาปัตยกรรมองค์กร)	มุมมองของบุคคลที่เกี่ยวของกับสถาปัตยกรรมองค์กรในซึ่งสามารถแบ่งออกเป็นหลายมุมมอง เช่น มุมมองผู้บริหาร มุมมองนักพัฒนา และมุมมองผู้ใช้
Continual Improvement of Enterprise Architecture (การปรับปรุงสถาปัตยกรรมองค์กรอย่างต่อเนื่อง)	การปรับปรุงสถาปัตยกรรมองค์กรให้สามารถบรรลุผลการดำเนินงานธุรกิจตามที่ได้กำหนดไว้ในเป้าหมายการดำเนินงานขององค์กร
Enterprise Reference Model (แบบจำลองสถาปัตยกรรมองค์กร)	การอธิบายสถาปัตยกรรมองค์กรในด้านต่างๆขององค์กร เช่น ด้านธุรกิจ แอปพลิเคชัน ข้อมูล โครงสร้างพื้นฐาน และความมั่นคงปลอดภัย
Work Product	สิ่งที่ได้จากมุมมองสถาปัตยกรรมองค์กร (Enterprise Architecture Viewpoint) ในแต่ละแบบจำลองสถาปัตยกรรมองค์กร (Enterprise Reference Model)

บรรณานุกรม

[๑] Zachman, A. J..The Zachman Framework for Enterprise Architecture Version 3.0. Retrived from http://www.zachman.com/about-the-zachman-framework

[๒] The Open Group (2011). The Open Group Architecture Framework (TOGAF) Version 9.1.

[๓] U.S. Office of Management and Budget (2013, January 29). Federal Enterprise Architecture Framework Version 2.

[๔] สำนักงานรัฐบาลอิเล็กทรอนิกส์ (องค์การมหาชน). แผนแม่บทเทคโนโลยีสารสนเทศและการสื่อสาร สรอ. ๓ ปี (พ.ศ. ๒๕๕๘ – ๒๕๖๐)

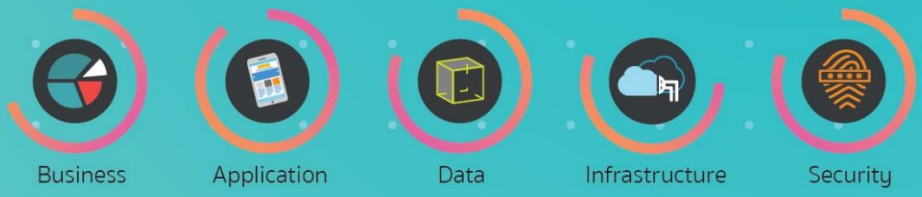
[๕] สำนักงานรัฐบาลอิเล็กทรอนิกส์ (องค์การมหาชน). แผนกลยุทธ์ สรอ. ประจำปี ๒๕๕๘

[๖] สำนักงานรัฐบาลอิเล็กทรอนิกส์ (องค์การมหาชน). แผนบริหารจัดการระบบสารสนเทศ สรอ. ประจำปี พ.ศ. ๒๕๕๘

[๗] สำนักงานรัฐบาลอิเล็กทรอนิกส์ (องค์การมหาชน). แผนยุทธศาสตร์ สรอ. ๔ ปี (พ.ศ.๒๕๕๗ – ๒๕๖๐)

[๘] สำนักงานรัฐบาลอิเล็กทรอนิกส์ (องค์การมหาชน). โครงการจัดทำกระบวนการดำเนินงาน Business Process Improvement (BPI) ของสำนักงานรัฐบาลรัฐบาลอิเล็กทรอนิกส์ (องค์การมหาชน)

[๙] The International Organization for Standardization. ISO/IEC 27001:2013 - Information security management



EGA
e-Government Agency
เอกสารเผยแพร่ **สถาปัตยกรรมองค์กร (EGA Enterprise Architecture)**
โดย สำนักงานรัฐบาลอิเล็กทรอนิกส์ (องค์การมหาชน) หรือ อีจีเอ I Electronic Government Agency (Public Organization) (EGA)
Contact Center : 026126060 I www.ega.or.th I www.facebook.com/EGATHAILAND