บทที่ 1 บททั่วไป

1.1 ความเป็นมา

บริษัท อู่กรุงเทพ จำกัด เป็นรัฐวิสาหกิจ ในความควบคุมของกองทัพเรือ สังกัดกระทรวงกลาโหม จัดเป็นรัฐวิสาหกิจประเภทนโยบายพิเศษของรัฐประเภทยุทธปัจจัย ประกอบกิจการอุตสาหกรรมอู่เรือ และอุตสาหกรรมต่อเนื่องกับกิจการพาณิชยนาวี และเป็นอุตสาหกรรมพื้นฐานในการพัฒนาอุตสาหกรรมต่อเนื่องหลายประเภท ซึ่งอุตสาหกรรมอู่เรือภายในประเทศเป็นส่วนประกอบที่สำคัญของสมุทานุภาพ เป็นอุตสาหกรรมที่ก่อให้เกิดการจ้างแรงงานฝีมือจำนวนมาก เป็นอุตสาหกรรมที่สนับสนุนและส่งเสริมการขนส่งทางทะเล การค้าระหว่างประเทศส่งเสริมอุตสาหกรรมปิโตรเคมีและอุตสาหกรรมเหล็ก และประการที่สำคัญที่สุดคือ เป็นอุตสาหกรรมที่ทำให้เกิดความมั่นคงทางการทหารและเพิ่มศักย์สงครามให้แก่ประเทศ

บริษัท อู่กรุงเทพ จำกัด (สำนักงานใหญ่) ตั้งอยู่ริมแม่น้ำเจ้าพระยาฝั่งตะวันออกบนถนนเจริญกรุง ระหว่างสะพานกรุงเทพ และสะพานตากสิน มีพื้นที่ทั้งหมด 20 ไร่ 1 งาน 82 ตารางวา มีอาณาเขตติดกับวัดยานนาวา มีลักษณะเป็นอู่แห้งทั้งหมด 2 อู่ ในส่วนของสำนักงานสาขาสัตหีบ (สำนักงานธุรกิจสัตหีบ) ตั้งอยู่ในพื้นที่ราชพัสดุกรมธนารักษ์ (บริเวณอู่ราชนาวีมหิดลอดุลยเดช กรมอู่ทหารเรือ) ตำบลสัตหีบ อำเภอสัตหีบ จังหวัดชลบุรี พื้นที่ 44 ไร่ 2 งาน มีระบบเชื่อมโยงเครือข่ายผ่านระบบ VPN โดยสายสัญญาณอินเตอร์เน็ตเพื่อสามารถใช้ทรัพยากรต่างๆ ที่สำนักงานใหญ่ได้เช่น Data Center ผ่านระบบอินทราเนท หรือระบบงานต่าง ๆ

การกำหนดทิศทางการกำกับดูแลการบริหารจัดการเทคโนโลยีดิจิทัล ของสำนักงานคณะกรรมการนโยบายรัฐวิสาหกิจ (สคร.) รัฐวิสำหกิจส่วนใหญ่ มีการกำหนดกระบวนการกำกับดูแลด้านเทคโนโลยีดิจิทัล ที่ครอบคลุมถึงการบริหารจัดการทรัพยากรเทคโนโลยีดิจิทัลอย่างเหมาะสม มีประสิทธิภาพและมีความโปร่งใส และการกำกับดูแลการบริหารความเสี่ยงด้านเทคโนโลยีดิจิทัล แผนปฏิบัติการดิจิทัลระยะ 3-5 ปี รัฐวิสาหกิจบางแห่ง เริ่มมีการกำหนดรายละเอียดที่ชัดเจนในส่วนของเป้าหมายการนำเทคโนโลยีดิจิทัลมาปรับใช้กับทุกส่วนขององค์กร (Digital Transformation) ที่แสดงให้เห็นถึงการปรับเปลี่ยนทั้งส่วนของกระบวนการ (Process) บุคลากร (People) และเทคโนโลยี (Technology) มีกระบวนการจัดการคุณภาพให้มีแนวทำงปฏิบัติอย่างเป็นระบบที่สามารถทำซ้ำได้ มีการกำหนดขอบเขตและแนวทางในการสร้างระบบบริหารคุณภาพที่ชัดเจน มีการตรวจสอบด้านเทคโนโลยีดิจิทัล (Digital Audit หรือ Computer Audit)

ทั้งนี้ เพื่อให้การดำเนินการแผนปฏิบัติการดิจิทัล ประจำปี 2568 – 2572 ของบริษัท อู่กรุงเทพ จำกัด สอดคล้องสถานการณ์ปัจจุบัน และเป็นประโยชน์สูงสุดต่อการบริหารจัดการด้านการัฒนาเทคโนโลยีดิจิทัลต่อไป

1.2 วิสัยทัศน์

“เป็นอู่เรือที่มีศักยภาพในการบริหารจัดการระดับสากล เติบโต และเป็นกลไกสำคัญในอุตสาหกรรมป้องกันประเทศและพาณิชย์นาวีของไทย สามารถพึ่งพาตนเองอย่างยั่งยืน”

1.3 พันธกิจ

(1) ให้บริการต่อเรือและซ่อมเรือ ซ่อมบำรุงยุทธโธปกรณ์ และจัดส่งพัสดุให้แก่กองทัพเรือ

(2) ให้บริการต่อเรือและซ่อมเรือ หน่วยข้าราชการ รัฐวิสาหกิจ และ เอกชน

(3) ขยายกิจการโดยการสร้างอู่เรือแห่งใหม่บริเวณชายทะเล

(4) ขยายกิจการในอุตสาหกรรมป้องกันประเทศ การต่อเรือเฉพาะทาง การพัฒนาอสังหาริมทรัพย์ เพื่อความมั่นคงทางการเงินในระยะยาว

(5) บริหารจัดการเพื่อมุ่งสู่การเป็นองค์กรแห่งความเป็นเลิศ

(6) ดำเนินกิจการตามหลักการกำกับดูแลที่ดี และมีความ รับผิดชอบต่อสังคม และสิ่งแวดล้อม รวมถึง การป้องกันและปราบปรามการทุจริต และประพฤติมิชอบอย่างเคร่งครัด

1.4 ค่านิยมและวัฒนธรรมองค์กร

(1) ค่านิยม

“แสวงหาโอกาสทางธุรกิจ สั่งสมความเชี่ยวชาญทางอาชีพ สร้างสรรค์ นวัตกรรมสู่ความยั่งยืน”

(2) วัฒนธรรมองค์กร

“อุทิศตนเพื่อให้ความต้องการของลูกค้าบรรลุผลสำเร็จ และดำเนินการปรับปรุงองค์กรเพื่อ สร้างความประทับใจให้ลูกค้าอย่างต่อเนื่อง”

บทที่ 2

กระบวนการจัดทำแผนปฏิบัติการดิจิทัล

2.1 ขั้นตอนศึกษา ทบทวนเอกสารต่าง ๆ ที่เกี่ยวข้อง

2.1.1 ทบทวนแผนยุทธศาสตร์ชาติ 20 ปี พ.ศ.2561 - 2580

โดยที่รัฐธรรมนูญแห่งราชอาณาจักรไทย มาตรา ๖๕ กำหนดให้รัฐ พึงจัดให้มียุทธศาสตร์ชาติเป็นเป้าหมายการพัฒนาประเทศอย่างยั่งยืน ตามหลัก ธรรมาภิบาลเพื่อใช้เป็นกรอบในการจัดทำแผนต่าง ๆ ให้สอดคล้องและบูรณาการกันเพื่อให้เกิดเป็นพลังผลักดันร่วมกันไปสู่เป้าหมายดังกล่าว โดยให้เป็นไปตามที่ กำหนดในกฎหมายว่าด้วยการจัดทำยุทธศาสตร์ชาติ และต่อมาได้มีการตรา พระราชบัญญัติการจัดทำยุทธศาสตร์ชาติ พ.ศ. ๒๕๖๐ โดยกำหนดให้มีการแต่งตั้ง คณะกรรมการยุทธศาสตร์ชาติ เพื่อรับผิดชอบในการจัดทำร่างยุทธศาสตร์ชาติ กำหนดวิธีการการมีส่วนร่วมของประชาชนในการจัดทำร่างยุทธศาสตร์ชาติ ในการติดตาม การตรวจสอบ และการประเมินผล รวมทั้ง กำหนดมาตรการส่งเสริม และสนับสนุนให้ประชาชนทุกภาคส่วนดำเนินการให้สอดคล้องกับยุทธศาสตร์ชาติ เพื่อให้เป็นไปตามที่กำหนดในพระราชบัญญัติการจัดทำยุทธศาสตร์ชาติ พ.ศ. ๒๕๖๐ คณะกรรมการยุทธศาสตร์ชาติได้แต่งตั้งคณะกรรมการจัดทำยุทธศาสตร์ชาติด้านต่าง ๆ รวม ๖ คณะ เพื่อรับผิดชอบในการดำเนินการจัดทำ ร่างยุทธศาสตร์ชาติให้เป็นไปตามหลักเกณฑ์ วิธีการ และเงื่อนไขที่กำหนด ตลอดจนได้จัดให้มีการรับฟังความคิดเห็นของประชาชนและหน่วยงานของรัฐที่เกี่ยวข้องอย่างกว้างขวาง เพื่อประกอบการจัดทำร่างยุทธศาสตร์ชาติตามที่ กฎหมายกำหนด ยุทธศาสตร์ชาติ ๒๐ ปี (พ.ศ. ๒๕๖๑-๒๕๘๐) เป็นยุทธศาสตร์ชาติ ฉบับแรกของประเทศไทยตามรัฐธรรมนูญแห่งราชอาณาจักรไทย ซึ่งจะต้องนำไปสู่ การปฏิบัติเพื่อให้ประเทศไทยบรรลุวิสัยทัศน์ “ประเทศไทยมีความมั่นคง มั่งคั่ง ยั่งยืน เป็นประเทศพัฒนาแล้วด้วยการพัฒนาตามหลักปรัชญาของเศรษฐกิจ พอเพียง” เพื่อความสุขของคนไทยทุกคน

http://nscr.nesdc.go.th/ns/

ยุทธศาสตร์ชาติ 20 ปี เป็นแผนการพัฒนาประเทศ ที่จะกำหนดกรอบและแนวทางการพัฒนาให้หน่วยงานของรัฐทุกภาคส่วนต้องทำตาม เพื่อให้บรรลุวิสัยทัศน์ "ประเทศไทยมีความมั่นคง มั่งคั่ง ยั่งยืน เป็นประเทศที่พัฒนาแล้วด้วยการพัฒนาตามหลักปรัชญาของเศรษฐกิจพอเพียง" หรือตามคติพจน์ "มั่นคง มั่งคั่ง ยั่งยืน" โดยมีระยะเวลาบังคับนานถึง 20 ปี ตั้งแต่ปี 2560-2579 แบ่งยุทธศาสตร์ออกเป็น 6 ด้าน คือ

1. ยุทธศาสตร์ด้านความมั่นคง
2. ยุทธศาสตร์ด้านการสร้างความสามารถในการแข่งขัน
3. ยุทธศาสตร์การพัฒนาและเสริมสร้างศักยภาพคน
4. ยุทธศาสตร์ด้านการสร้างโอกาสความเสมอภาคและเท่าเทียมกันทางสังคม
5. ยุทธศาสตร์ด้านการสร้างการเติบโตบนคุณภาพชีวิตที่เป็นมิตรกับสิ่งแวดล้อม
6. ยุทธศาสตร์ด้านการปรับสมดุลและพัฒนาระบบการบริหารจัดการภาครัฐ

ยุทธศาสตร์ชาติ 20 ปี (พ.ศ. 2561-2580) มุ่งเน้นการพัฒนาประเทศไทยให้มีความมั่นคงและเป็นประชาชนมีความสุขการจัดทำแผนการพัฒนานี้เป็นกรอบและแนวทางที่หน่วยงานของรัฐต้องปฏิบัติตาม

2.1.2 แผนพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคม พ.ศ.2561 - 2580

ตามแผนพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคม ซึ่งจัดทำโดยกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร ได้รับความเห็นชอบจากคณะรัฐมนตรีเมื่อวันที่ 5 เมษายน พ.ศ. 2559 โดยแผนฉบับนี้ได้กำหนดวิสัยทัศน์ในการปฏิรูปประเทศไทยสู่ดิจิทัลไทยแลนด์ (Digital Thailand) ซึ่งหมายถึง ประเทศไทยที่สามารถสร้างสรรค์และใช้ประโยชน์จากเทคโนโลยีดิจิทัลอย่างเต็มศักยภาพในการพัฒนาโครงสร้างพื้นฐาน นวัตกรรม ข้อมูล ทุนมนุษย์ และทรัพยากรอื่นใดเพื่อขับเคลื่อนประเทศไปสู่ความมั่นคง มั่งคั่ง และยั่งยืน โดยมีเป้าหมายหลัก 4 ประการคือ

1) เพิ่มขีดความสามารถในการแข่งขันทางเศรษฐกิจของประเทศด้วยการใช้นวัตกรรมและเทคโนโลยีดิจิทัล เป็นเครื่องมือหลักในการสร้างสรรค์นวัตกรรมการผลิต การบริการ
2) สร้างโอกาสทาง สังคมอย่างเท่าเทียม ด้วยข้อมูลข่าวสารและบริการต่าง ๆ ผ่านสื่อดิจิทัลเพื่อยกระดับคุณภาพชีวิตของประชาชน
3) เตรียมความพร้อมให้บุคลากรทุกกลุ่ม มีความรู้และทักษะที่เหมาะสมต่อการดำเนินชีวิตและการประกอบอาชีพในยุคดิจิทัล
4) ปฏิรูปกระบวนทัศน์การทำงานและการให้บริการของภาครัฐ ด้วยเทคโนโลยีดิจิทัลและการใช้ประโยชน์จากข้อมูล เพื่อให้การปฏิบัติงานเกิดความโปร่งใส มีประสิทธิภาพ และประสิทธิผล

ยุทธศาสตร์แผนพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคม กำหนดภูมิทัศน์ดิจิทัล เพื่อกำหนดทิศทางการพัฒนาและเป้าหมายใน 4 ระยะ ภายในเวลา 20 ปี (2561 – 2580) และกำหนดยุทธศาสตร์ในการดำเนินงานเพื่อไปสู่เป้าหมาย 6 ยุทธศาสตร์ ประกอบด้วย

ยุทธศาสตร์ที่ 1 พัฒนาโครงสร้างพื้นฐานดิจิทัลประสิทธิภาพสูงให้ครอบคลุมทั่วประเทศ

ยุทธศาสตร์ที่ 2 ขับเคลื่อนเศรษฐกิจด้วยเทคโนโลยีดิจิทัล

ยุทธศาสตร์ที่ 3 สร้างสังคมคุณภาพที่ทั่วถึงเท่าเทียมด้วยเทคโนโลยีดิจิทัล

ยุทธศาสตร์ที่ 4 ปรับเปลี่ยนภาครัฐสู่การเป็นรัฐบาลดิจิทัล

ยุทธศาสตร์ที่ 5 พัฒนากำลังคนให้พร้อมเข้าสู่ยุคเศรษฐกิจและสังคมดิจิทัล

ยุทธศาสตร์ที่ 6 สร้างความเชื่อมั่นในการใช้เทคโนโลยีดิจิทัล

ตามแผนพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคม พ.ศ.2561 - 2580 ที่ได้รับการกำหนดจากกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมและสำนักงานคณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งชาติ (สดช.) แผนนี้มุ่งเน้นการส่งเสริมให้เทคโนโลยีดิจิทัลเข้าสู่การใช้งานทั่วไปในด้านต่างๆ เพื่อเพิ่มประสิทธิภาพในเศรษฐกิจและชีวิตสังคม

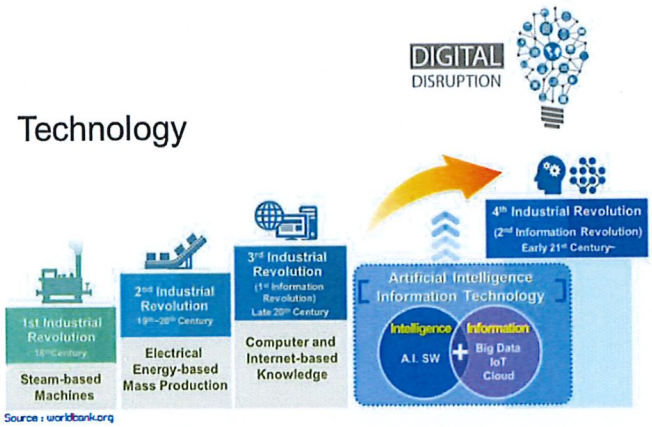
2.1.3 ทบทวนผลการประเมินและข้อเสนอแนะของสำนักงานคณะกรรมการนโยบายรัฐวิสาหกิจ (สคร.)

หลักเกณฑ์ระบบประเมินผลการดำเนินงานรัฐวิสาหกิจ โดยเปลี่ยนแนวคิดในการกำกับรัฐวิสาหกิจจากการควบคุมขั้นตอนในการทำงานมาเป็นการควบคุมผลการดำเนินงานแทน และให้อำนาจแก่คณะกรรมการรัฐวิสาหกิจในการบริหารจัดการภายในองค์กรได้เอง โดยให้เริ่มนำระบบประเมินผลฯ มาใช้วัดประสิทธิภาพการ

ดำเนินงานของรัฐวิสาหกิจใหม่ โดยคณะกรรมการประเมินผลงานรัฐวิสาหกิจได้พิจารณาปรับปรุงระบบประเมินผลฯ เพื่อให้มีความเหมาะสมกับการดำเนินงานของรัฐวิสาหกิจเป็นระยะในปี 2547 คณะกรรมการประเมินผลฯ ได้กำหนดเกณฑ์การประเมินผลในหัวข้อการบริหารจัดการองค์กร (ข้อ 3.) ขึ้น เพื่อผลักดันให้รัฐวิสาหกิจพัฒนาระบบการบริหารจัดการองค์กรในด้านต่างๆ ให้ทัดเทียมกับมาตรฐานสากล โดยการคัดเลือกกระบวนงานหลัก 6 ด้าน ซึ่งมีความสำคัญและเป็นพื้นฐานของการบริหารจัดการที่ดีมาเป็นหัวข้อการประเมินหลัก ได้แก่ บทบาทคณะกรรมการรัฐวิสาหกิจ การบริหารความเสี่ยง การควบคุมภายใน การตรวจสอบภายใน การบริหารจัดการสารสนเทศ และการบริหารทรัพยากรบุคคล

พระราชบัญญัติการพัฒนาการกำกับดูแลและบริหารรัฐวิสาหกิจ (พ.ร.บ. พัฒนารัฐวิสาหกิจฯ) เมื่อวันที่ 19 พฤษภาคม 2562 ซึ่งถือเป็นหัวใจสำคัญของการปฏิรูปรัฐวิสาหกิจไทย โดย พ.ร.บ. พัฒนารัฐวิสาหกิจฯ ดังกล่าวได้กำหนดวัตถุประสงค์สำคัญในการพัฒนาการกำกับดูแลและบริหารรัฐวิสาหกิจไว้ 4 ประเด็นซึ่งรวมถึงการส่งเสริมให้รัฐวิสาหกิจดำเนินการอย่างมีประสิทธิภาพ โปร่งใส สอดคล้องกับหลักการกำกับดูแลกิจการที่ดีและมีการประเมินผลการดำเนินการอย่างต่อเนื่อง สคร.เห็นถึงความจำเป็นของการพัฒนาระบบประเมินผลเพื่อพัฒนาต่อยอดจากโครงการระบบประเมินผลเดิมที่สามารถใช้เป็นเครื่องมือในการกำกับ ติดตาม ประเมินผลการดำเนินงานรัฐวิสาหกิจที่มีความเหมาะสมเป็นรูปธรรม และสามารถสะท้อนถึงความมีประสิทธิภาพในการดำเนินงานได้อย่างแท้จริง โดยได้พิจารณานำข้อดี/จุดแข็งของระบบปัจจุบันที่มีมาใช้ ปรับปรุงข้อด้อยของระบบปัจจุบัน รวมทั้งปรับปรุง เพิ่มเติมประเด็นของการจัดการสมัยใหม่และ Update ให้เป็นปัจจุบัน และจะนำมาใช้ในการประเมินผลรัฐวิสาหกิจในปี 2563 โดยมีรายละเอียดดังนี้คือ

เหตุผลและความจำเป็นในการพัฒนาระบบประเมินผลฯ ใหม่

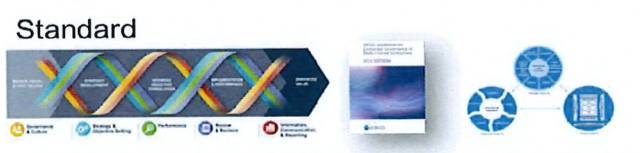


วัตถุประสงค์

เพื่อส่งเสริมให้ รส. ตอบสนองกับสภาพแวดล้อมในการดำเนินภารกิจ/ธุรกิจ การแข่งขัน ความต้องการของผู้ใช้บริการ และ บริบทที่เปลี่ยนแปลงไป เช่น การเปลี่ยนแปลงของเทคโนโลยีดิจิทัล เป็นต้น รวมถึงนโยบายสำคัญไทยแลนด์ 4.0 ที่ต้องการขับเคลื่อนประเทศด้วยความคิดสร้างสรรค์และนวัตกรรม ทั้งหมดนี้ด้วยการดำเนินงานที่มีประสิทธิภาพ โปร่งใส ตรวจสอบได้

หลักการ

1. รักษาข้อดี/จุดแข็ง ของระบบปัจจุบัน
2. ปรับปรุงข้อด้อย ของระบบปัจจุบัน
3. ปรับปรุง เพิ่มเติม ประเด็นของการจัดการสมัยใหม่/Update ให้เป็นปัจจุบัน พร้อมข้อสังเกต/ข้อเสนอแนะที่ได้รับ



10

1 เหตุผลและความจำเป็นในการพัฒนาระบบประเมินผลฯ ใหม่

1 ระบบประเมินผลในปัจจุบันมี 2 ระบบ 2

ระบบ SEPA

1. กระบวนการ/ระบบ (Process)

หมวด 1 การนำองค์กร
หมวด 2 การวางแผนเชิงยุทธศาสตร์
หมวด 3 การมุ่งเน้นลูกค้าและตลาด
หมวด 4 การวัด วิเคราะห์ และการจัดการความรู้
หมวด 5 การมุ่งเน้นบุคลากร
หมวด 6 การจัดการกระบวนการ

2. ภารกิจตามยุทธศาสตร์

3. ผลลัพธ์ (Result)

ระบบบริหารจัดการองค์กร (ข้อ 3)

1. การดำเนินการตามนโยบาย

2. ผลการดำเนินงานของรัฐวิสาหกิจ

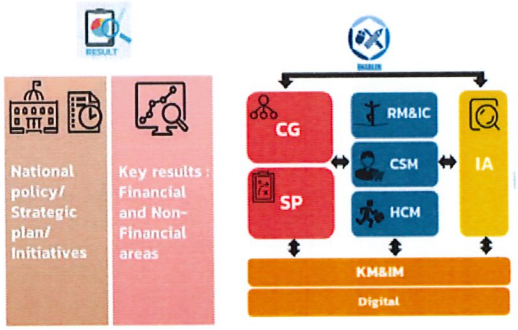
3. การบริหารจัดการองค์กร

3.1 บทบาทของคณะกรรมการรัฐวิสาหกิจ
3.2 การบริหารความเสี่ยง
3.3 การควบคุมภายใน
3.4 การตรวจสอบภายใน
3.5 การบริหารจัดการสารสนเทศและดิจิทัล
3.6 การบริหารทรัพยากรบุคคล

2 ภาพรวมหลักเกณฑ์และแนวทางระบบการประเมินผลใหม่ของรัฐวิสาหกิจ

Key Performance Areas (60 ± 15%)

1. การดำเนินงานตามยุทธศาสตร์ (National Policy, Strategic Plan, Initiatives)
2. ผลการดำเนินงานที่สำคัญ (Key Results)



Enablers (40 ± 15%)

1. การกำกับดูแลที่ดีและการนำองค์กร (Corporate Governance & Leadership : CG)
2. การวางแผนเชิงกลยุทธ์ (Strategic Planning : SP)
3. การบริหารความเสี่ยง และการควบคุมภายใน (Risk Management & Internal Control : RM & IC)
4. การมุ่งเน้นผู้มีส่วนได้ส่วนเสีย และลูกค้า (Stakeholder & Customer : CSM)
5. การพัฒนาเทคโนโลยีดิจิทัล (Digital Technology : Digital)
6. การบริหารทุนมนุษย์ (Human Capital Management : HCM)
7. การจัดการความรู้และนวัตกรรม (Knowledge Management & Innovation Management: KM & IM)
8. การตรวจสอบภายใน (Internal Audit : IA)

กรอบหลักการและแนวคิดเพื่อการประเมินการพัฒนาเทคโนโลยีดิจิทัล ปี 2567 ที่ผ่านมา

หลักเกณฑ์ประเมินการพัฒนาเทคโนโลยีดิจิทัลของรัฐวิสาหกิจ เกิดจากการประยุกต์หลักการ มาตรฐานและแนว

ปฏิบัติที่ดีด้านการพัฒนาเทคโนโลยีดิจิทัลของภาครัฐและภาคเอกชน ที่เป็นที่ยอมรับทั้งในและต่างประเทศ ตลอดจนสอดคล้องกับทิศทาง นโยบาย กรอบการดำเนินงานของประเทศ เช่น นโยบายไทยแลนด์ 4.0 แผนดิจิทัลเพื่อเศรษฐกิจและสังคม

ผลการดำเนินงาน ประจำปีบัญชี 2567
ด้าน Core Business Enablers

(outcome) ของกระบวนการประเมินประสิทธิผลของกระบวนการที่สอดคล้องตามเกณฑ์ โดยแสดงให้เห็นว่าผลลัพธ์ (outcome) ของกระบวนการครบถ้วนตามเกณฑ์ รวมถึงควรมีการนำผลลัพธ์ที่สำคัญของกระบวนการ เข้าสู่กระบวนการทบทวน ปรับปรุงและพัฒนากระบวนการอย่างต่อเนื่อง

กราฟสรุปผลการประเมิน	หัวข้อ "การพัฒนาเทคโนโลยีดิจิทัล"	อยู่ที่ระดับคะแนน 1.1529

ผลการดำเนินงาน ประจำปีบัญชี 2567
ด้าน Core Business Enablers

สรุปข้อเสนอแนะด้านการพัฒนาเทคโนโลยีดิจิทัล

1. รัฐวิสาหกิจต้องนำเทคโนโลยีดิจิทัลมาปรับใช้กับทุกส่วนขององค์กรโดยสามารถกำหนดเป้าหมายที่สะท้อนถึงการเปลี่ยนแปลง People Process Technology ออกมาได้อย่างชัดเจนเป็นรูปธรรม ตลอดจนสามารถประเมินและติดตามผลได้ รวมถึงมีการวัดผลลัพธ์ (Outcome) ในเชิงปริมาณที่สะท้อนให้เห็นผลดำเนินงานที่สำคัญของรัฐวิสาหกิจที่ดียิ่งขึ้น เช่น การให้บริการประชาชน การอำนวยความสะดวกให้กับผู้มีส่วนได้ส่วนเสีย เป็นต้น เพื่อยกระดับการดำเนินงานขององค์กร เช่น ทอท. กปน. กปภ. กทพ. กตช. อภ. บวท. กนอ. รฟม. กทพ. ทชท. รฟท. ขสมก. บขส. เป็นต้น
2. รัฐวิสาหกิจต้องดำเนินการป้องกันความเสี่ยงด้านเทคโนโลยีดิจิทัล ที่ปัจจุบันมีภัยคุกคามจากหลากหลายรูปแบบ เช่น Cyber Security Hacking the home Beware of the 'wares' Application-Based or Web-based Threats อาชญากรรมจากคอลเซ็นเตอร์ เป็นต้น โดยต้องมีการกำหนดเป็นแผนการรองรับที่ชัดเจน มีการนำเครื่องมือป้องกันหรือเทคโนโลยีที่เหมาะสมเข้ามาใช้ รวมถึงมีการติดตามผลการดำเนินงานอย่างต่อเนื่อง เช่น อภ. กปน. กปภ. ทชท. ทอท. กนอ. รฟม. กทพ. กทท. กกท กตช. รฟท. สบพ. ขสมก. บขส. เป็นต้น
3. รัฐวิสาหกิจต้องนำเทคโนโลยีดิจิทัลที่ทันสมัยมาประยุกต์ใช้กับการดำเนินงานให้มีประสิทธิภาพ เช่น การใช้ Cloud Computing Services เพื่อลดการลงทุน Data Center การใช้ Big Data, Data Analytics และ AI เพื่อให้เกิดการใช้ประโยชน์ข้อมูลอย่างมีประสิทธิภาพ การบริหารจัดการ Digital Outsource เพื่อลดปัญหาการขาดแคลนทรัพยากรและบุคลากรด้านเทคโนโลยีดิจิทัล เป็นต้น โดยต้องคำนึงถึงความคุ้มค่าการลงทุน ความมั่นคงปลอดภัย และเทคโนโลยีที่เหมาะสม
4. รัฐวิสาหกิจต้องดำเนินการให้มีการประกอบธุรกิจ หรือการปฏิบัติที่มีความสอดคล้องกับกฎหมาย ระเบียบ ข้อบังคับ และมาตรฐานต่างๆ ที่เกี่ยวข้องกับการพัฒนาเทคโนโลยีดิจิทัล เช่น พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล 2562 และ พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 เป็นต้น โดยแสดงให้เห็นถึงแผนงาน/โครงการที่ชัดเจนเป็นรูปธรรม เพื่อลดช่องว่าง (GAP) การปฏิบัติที่ยังไม่มีความสอดคล้อง โดยเฉพาะรัฐวิสาหกิจที่จัดเป็นหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Critical Information Infrastructure: CII) ที่ สกมช. มีการใช้ NIST2.0 เป็นแนวทางในการประเมินผลกับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Critical Information Infrastructure: CII) ซึ่งแบ่งลักษณะการให้บริการ ได้ดังต่อไปนี้
   หมวด 2 ด้านบริการภาครัฐที่สำคัญ ได้แก่ อจน. อสมท.
   หมวด 3 ด้านการเงินการธนาคาร ได้แก่ ธกส. ธสน. ธพว. ออมสิน ธอส. ธอท. บสย.
   หมวด 4 ด้านเทคโนโลยีสารสนเทศและดิจิทัล ได้แก่ ปณท. เอ็นที
   หมวด 5 ด้านขนส่งและโลจิสติกส์ ได้แก่ กทพ. บขส. ขสมก. รฟท. รฟม. กทท. ทอท. บวท.
   หมวด 6 ด้านพลังงานและสาธารณูปโภค ได้แก่ กฟน. กฟผ. กฟภ. ปตท. กปน. กปภ.
   หมวด 7 ด้านสาธารณสุข ได้แก่ อภ.
   รวมถึงควรมีการกำหนดบทบาทความร่วมมือกับหน่วยงานกำกับดูแลต่างๆ อย่างใกล้ชิด

2.1.4 แผนพัฒนารัฐบาลดิจิทัลของประเทศไทย พ.ศ. 2566-2570

แผนพัฒนารัฐบาลดิจิทัลบับนี้มุ่งยกระดับภาครัฐไทยสู่เป้าหมายการให้บริการตอบสนองประชาชน และลดความเหลื่อมล้ำการเพิ่มความสามารถและศักยภาพในการแข่งขันของภาคธุรกิจ การสร้างความโปร่งใส ที่เน้นการเปิดเผยข้อมูลแก่ประชาชนโดยไม่ต้องร้องขอและการสนับสนุนการมีส่วนร่วมของประชาชน และการเป็นภาครัฐที่

ปรับตัวทันการณ์ อันจะเป็นพื้นฐานสำคัญในการขับเคลื่อนเศรษฐกิจและสังคมของประเทศต่อไป แผนพัฒนารัฐบาลดิจิทัลของประเทศไทย พ.ศ. 2566 – 2570 กำหนดยุทธศาสตร์การพัฒนาเพื่อให้สอดรับ กับวิสัยทัศน์ข้างต้นไว้ 4 ยุทธศาสตร์ประกอบด้วย

ยุทธศาสตร์ที่ 1 : ยกระดับการเปลี่ยนผ่านดิจิทัลภาครัฐ เพื่อการบริหารงานที่ยืดหยุ่น คล่องตัวและขยายสู่หน่วยงานภาครัฐระดับท้องถิ่น

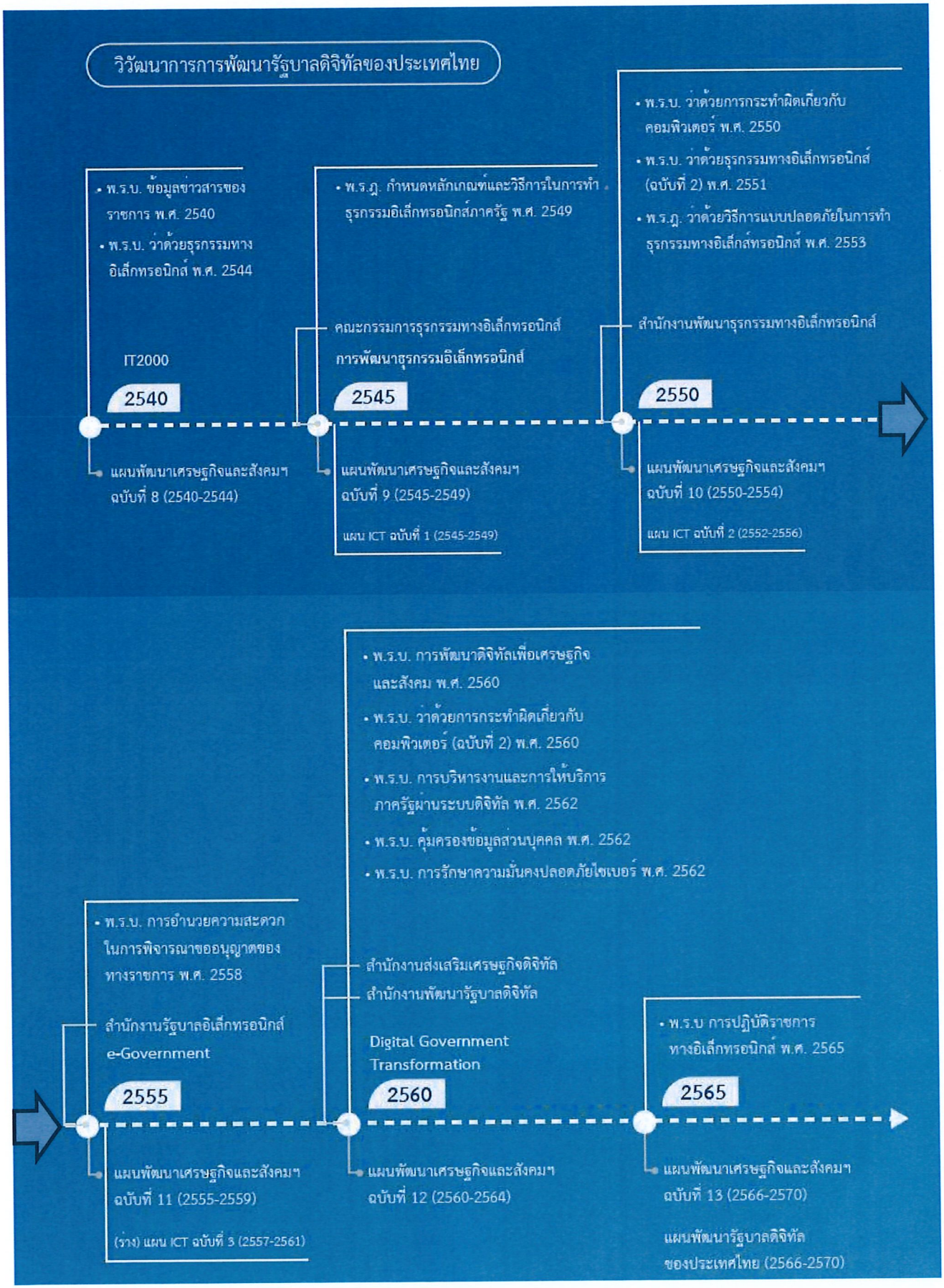
ยุทธศาสตร์ที่ 2 : พัฒนาบริการที่สะดวกและเข้าถึงง่าย

ยุทธศาสตร์ที่ 3 : สร้างมูลค่าเพิ่มและอำนวยความสะดวกแก่ภาคธุรกิจ

ยุทธศาสตร์ที่ 4 : ส่งเสริมการมีส่วนร่วมของประชาชน และเปิดเผยข้อมูลเปิดภาครัฐ

นอกจากนี้ เพื่อให้การดำเนินการขับเลื่อนรัฐบาลดิจิทัลทิศทางที่ชัดเจนและเกิดขึ้นได้จริงในเชิงปฏิบัติ จึงได้กำหนดแนวทางการพัฒนาในด้านที่มุ่งเน้นสำคัญ ไว้ทั้งหมด 10 ด้าน ได้แก่ การศึกษา สุขภาพและการแพทย์ ความเหลื่อมล้ำทางสิทธิสวัสดิการประชาชน สิ่งแวดล้อม การเกษตร การท่องเที่ยว การส่งเสริมวิสาหกิจขนาดกลางและขนาดย่อม (SME:) แรงงาน การยุติธรรมและการมีส่วนร่วม โปร่งใส และตรวจสอบได้ของประชาชน อีกทั้ง มุ่งส่งเสริมให้หน่วยงานภาครัฐ นำเทคโนโลยีและนวัตกรรมมาประยุกต์ใช้ในการเพิ่ม ประสิทธิภาพและมูลค่าของสินค้าและบริการ พร้อมยกระดับ ขีดความสามารถในการแข่งขันบนเวทีโลกด้วยการนำความหลากหลายทางชีวภาพและวัฒนธรรมของประเทศไทย มาพัฒนาเศรษฐกิจที่เป็นมิตรกับสิ่งแวดล้อมและการพัฒนาที่ยั่งยืนตามแนวคิดเศรษฐกิจชีวภาพ เศรษฐกิจหมุนเวียน และเศรษฐกิจสีเขียว (Bic-Circular-Green Economy: BCG Economyโดยเฉพาะด้านการเกษตร สุขภาพและการแพทย์ และการท่องเที่ยวและบริการ เพื่อนำพาประเทศสู่การพัฒนาทางสังคม เศรษฐกิจและสิ่งแวดล้อมอย่างยั่งยืน (sustainable Development) ที่สามารถตอบสนองความต้องการของสังคมในปัจจุบันพร้อมส่งต่อทรัพยากร ที่สามารถตอบสนองความต้องการของคนรุ่นต่อไป โดยไม่ทิ้งใครไว้ข้างหลัง ทั้งนี้ แผนพัฒนารัฐบาลดิจิทัลมีความเกี่ยวข้องและจำเป็นต้องอาศัยการบูรณาการจากทุกหน่วยงานภาครัฐ ที่จำเป็นต้องเร่งพัฒนาและยกระดับหน่วยงานให้สอดล้องกับทิศทางการขับเคลื่อนของประเทศ จึงไม่ใช่เป็นเพียงการพัฒนาหน่วยงานใดหน่วยงานหนึ่ง หากแต่จำเป็นต้องอาศัยความร่วมมือจากทุกหน่วยงานภาครัฐในการพัฒนาและขับเคลื่อนไปสู่การเป็นรัฐบาลดิทัลในทิศทางเดียวกันอย่างเป็นรูปรรม ให้ตอบสนองต่อความต้องการของประชาชน และมีมาตรฐานทัดเทียมกับนานาประเทศ

แผนปฏิบัติการดิจิทัล ประจำปี 2569 – 2573



แผนแม่บทภายใต้ยุทธศาสตร์ชาติ ประเด็นการบริการประชาชนและประสิทธิภาพภาครัฐ(พ.ศ. 2561 - 2580) ระบุเป้าหมาย ปี 2566 - 2570 ประเทศไทยต้องอยู่ในกลุ่มประเทศที่มีการพัฒนาด้านรัฐบาลดิจิทัลสูงสุด 50 อันดับแรกในการจัดลำดับดัชนีรัฐบาลอิเล็กทรอนิกส์ขององค์การสหประชาชาติ(E-Government Development Index: EGDI) โดยจากการศึกษาผลการสำรวจในปี 2565 พบว่าประเทศไทยมีคะแนนและอันดับสูงขึ้นเมื่อเทียบกับผลการสำรวจ ในปี 2563 โดยได้รับการปรับอันดับขึ้นจากอันดับที่ 57 เป็นอันดับที่ 55 จาก 193 ประเทศ ซึ่งเป็นการยกระดับขึ้นจากประเทศในกลุ่มที่มีการพัฒนารัฐบาลดิจิทัลในระดับสูง มาอยู่ในกลุ่มที่มีการพัฒนาในระดับสูงมากร่วมกับอีก 60 ประเทศ และยังถือได้ว่าเป็นอันดับที่ 3 ของอาเซียน รองจากสิงคโปร์ ซึ่งอยู่ในอันดับที่ 12 ของโลก และมาเลเซีย อันดับที่ 53 และเมื่อพิจารณาคะแนนในแต่ละด้าน พบว่า ด้านที่มีคะแนนเพิ่มขึ้น จากปีก่อน ได้แก่ โครงสร้างพื้นฐานโทรคมนาคม (Telecommunication Infrastructure Index: TII) และทุนมนุษย์ (Human Capital Index: HII) การให้บริการออนไลน์ (Online Service Index: OSI) มีคะแนนปรับลดเพียงเล็กน้อย แสดงให้เห็นว่า การเปลี่ยนแปลงดังกล่าวเป็นผลมาจากการพัฒนาด้านโครงสร้างพื้นฐานเทคโนโลยีสารสนเทศที่รองรับเข้าถึงข้อมูลและบริการภาครัฐผ่านช่องทางออนไลน์ของประชาชน5 และการพัฒนาทุนมนุษย์ด้านดิจิทัลที่จำเป็นต่อการใช้ประโยชน์จากเทคโนโลยี และความสามารถในการใช้บริการภาครัฐผ่านระบบดิจิทัล

ตามมาตรา 10 (3) แห่งพระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ. 2562 ให้สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) หรือ บอท. สำรวจ เก็บรวบรวมข้อมูล วิเคราะห์ และวิจัย เพื่อจัดทำตัวชี้วัด ดัชนีสนับสนุนการพัฒนารัฐบาลดิจิทัลเสนอต่อคณะกรรมการพัฒนารัฐบาลดิจิทัล ซึ่งสอดคล้องกับโครงการสำรวจระดับความพร้อมการพัฒนารัฐบาลดิจิทัลหน่วยงานภาครัฐ ที่ทำการสำรวจมาอย่างต่อเนื่องตั้งแต่ปี พ.ศ. 2558 จนถึงปัจจุบัน โดยในปี พ.ศ. 2567 บอท. ได้กำหนดกลุ่มเป้าหมายในการสำรวจ จำนวนรวมทั้งสิ้น 378 หน่วยงาน ประกอบด้วย หน่วยงานภาครัฐระดับกรมหรือเทียบเท่า จำนวน 302 หน่วยงาน ซึ่งในจำนวนนี้ รวมถึงหน่วยงานระดับกรมที่มีหน่วยงานใต้สังกัดตั้งอยู่ในจังหวัด รวมทั้งราชการส่วนภูมิภาค 21 หน่วยงาน และคณะกรรมการผู้บริหารเทคโนโลยีสารสนเทศระดับสูงระดับจังหวัด (Provincial Chief Information Officer Committee: PCIO) จำนวน 76 จังหวัด จำนวน 7 ตัวชี้วัด ประกอบด้วย

ตัวชี้วัดที่ 1 แนวนโยบายและหลักปฏิบัติ (Policies & Practices)

ตัวชี้วัดที่ 2 กระบวนการพัฒนาด้วยข้อมูล (Data-driven Practices)

ตัวชี้วัดที่ 3 ศักยภาพเจ้าหน้าที่ภาครัฐด้านดิจิทัล (Digital Capabilities)

ตัวชี้วัดที่ 4 บริการภาครัฐ (Public Services)

ตัวชี้วัดที่ 5 การบริหารจัดการรูปแบบดิจิทัล (Smart Back Office)

ตัวชี้วัดที่ 6 โครงสร้างพื้นฐานความมั่นคง ปลอดภัยและมีประสิทธิภาพ (Secure and Efficient Infrastructure)

ตัวชี้วัดที่ 7 เทคโนโลยีดิจิทัลและการนำไปใช้ (Digital Technological Practices)

ซึ่งผลการสำรวจดังกล่าวจะสามารถใช้เป็นข้อมูลประกอบการจัดทำนโยบายและแผนการขับเคลื่อนภาครัฐไปสู่การเป็นรัฐบาลดิจิทัล (Digital Government) ให้มีประสิทธิภาพและเป็นเอกภาพมากยิ่งขึ้น นอกจากนี้ เพื่อเป็นการให้เกียรติและเชิดชูหน่วยงานที่มีความมุ่งมั่นที่จะพัฒนาองค์กรไปสู่การเป็นรัฐบาลดิจิทัล บอท. จะนำผลการสำรวจดังกล่าว มาพิจารณามอบรางวัลรัฐบาลดิจิทัล ประจำปี 2567 (Digital Government Awards 2024) ให้แก่หน่วยงานภาครัฐที่มีการปรับเปลี่ยนองค์กรสู่การเป็นรัฐบาลดิจิทัลในระดับสูง เพื่อเป็นแบบอย่างที่ดีให้กับส่วนราชการและหน่วยงานของรัฐต่อไป

ตัวชี้วัดที่ 1 แนวนโยบายและหลักปฏิบัติ (Policies & Practices)

ตัวชี้วัด	วัตถุประสงค์
1.1 Digital Policy	สำรวจความสอดคล้องของการจัดทำแผนปฏิบัติการหรือแผนงานของหน่วยงานที่สอดคล้องกับแผนพัฒนารัฐบาลดิจิทัลของประเทศไทย ปี พ.ศ. 2566 - 2570
1.2 Cyber Security Policy	สำรวจการดำเนินการที่สอดคล้องกับพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 และกฎหมายลำดับรองที่เกี่ยวข้อง
1.3 Legal & Regulatory Mechanism	สำรวจการดำเนินการตามกฎหมายที่เกี่ยวข้อง และการปฏิบัติตามพระราชบัญญัติการปฏิบัติราชการทางอิเล็กทรอนิกส์ พ.ศ. 2565
1.4 Data Policy	สำรวจการจัดทำแผนปฏิบัติการหรือแผนงานสำหรับ ธรรมาภิบาลข้อมูลภาครัฐ (Data Governance) การเปิดเผยข้อมูล (Open Data) และ การคุ้มครองข้อมูลส่วนบุคคล (PDPA)

ตัวชี้วัดที่ 2 กระบวนการพัฒนาด้วยข้อมูล (Data-driven Practices)

ตัวชี้วัด	วัตถุประสงค์
2.1 Data Governance	สำรวจการดำเนินการและปฏิบัติการด้านธรรมาภิบาลข้อมูลภาครัฐ
2.2 Open Data & Sharable Data	สำรวจการดำเนินการและปฏิบัติการด้านข้อมูลเปิดภาครัฐ และด้านการแลกเปลี่ยนข้อมูล
2.3 Data Privacy	สำรวจการดำเนินการและปฏิบัติการด้านการคุ้มครองข้อมูลส่วนบุคคล

ตัวชี้วัดที่ 3 ศักยภาพเจ้าหน้าที่ภาครัฐด้านดิจิทัล (Digital Capability)

ตัวชี้วัด	วัตถุประสงค์

3.1 Digital Leadership	สำรวจบทบาทความเป็นผู้นำในการริเริ่มปรับเปลี่ยนหน่วยงานสู่การเป็นรัฐบาลดิจิทัลของ DCIO
3.2 Training and Development	สำรวจการส่งเสริมให้ความรู้ การอบรมและพัฒนาบุคลากรและการวัดผลด้านทักษะดิจิทัล
3.3 Digital Competency	สำรวจผลการประเมินระดับทักษะ ความสามารถ และความเข้าใจเทคโนโลยีดิจิทัลของบุคลากรในหน่วยงาน

ตัวชี้วัดที่ 4 บริการภาครัฐ (Public Services)

ตัวชี้วัด	วัตถุประสงค์
4.1 Service Provision	
4.1.1 Digital Service Facilitation	สำรวจการอำนวยความสะดวกของการให้บริการภาครัฐในรูปแบบดิจิทัล
4.1.2 Paperless Service	สำรวจการให้บริการภาครัฐโดยไม่จำเป็นต้องเรียกสำเนาเอกสาร
4.1.3 Digital Service for the Vulnerable	สำรวจการให้บริการภาครัฐในรูปแบบดิจิทัลแก่ผู้รับบริการกลุ่มเปราะบาง
4.2 Promotion for Digital Service Usage	สำรวจการส่งเสริมให้ใช้บริการของหน่วยงานภาครัฐผ่านช่องทางดิจิทัล
4.3 Customer Experience (Usability)	สำรวจประสบการณ์ของผู้เข้าใช้งานเว็บไซต์ของหน่วยงาน
4.4 Public Participation	สำรวจการสร้างการมีส่วนร่วมของผู้รับบริการโดยนำเทคโนโลยีดิจิทัลมาใช้ในการให้ข้อมูลข่าวสาร การปรึกษาหารือ รับฟังความคิดเห็น การเสนอทางเลือกและร่วมตัดสินใจเกี่ยวกับนโยบายและการบริการจากภาครัฐ
4.4.1 e-Information	สำรวจการเปิดโอกาสให้ผู้รับบริการรับข้อมูลข่าวสารและมีช่องทางการเข้าถึงข้อมูลข่าวสารผ่านช่องทางอิเล็กทรอนิกส์
4.4.2 e-Consultation	สำรวจการเปิดโอกาสให้ผู้รับบริการเข้ามามีส่วนร่วมโดยนำเทคโนโลยีดิจิทัลมาใช้ เพื่อให้สามารถแสดงความคิดเห็นเกี่ยวกับนโยบายหรือการบริการจากภาครัฐ
4.4.3 e-Decision Making	สำรวจการเปิดโอกาสให้ผู้รับบริการเข้ามามีส่วนร่วม โดยนำ

	เทคโนโลยีดิจิทัลมาใช้เพื่อให้ประชาชนสามารถเสนอทางเลือกและร่วมตัดสินใจเกี่ยวกับนโยบายหรือการบริการจากภาครัฐ

ตัวชี้วัดที่ 5 การบริหารจัดการรูปแบบดิจิทัล (Smart Back Office)

ตัวชี้วัด	วัตถุประสงค์
5.1 Integrated Enterprise	สำรวจประสิทธิภาพในการนำเอาระบบดิจิทัลมาบริหารงานในหน่วยงาน และการเชื่อมโยงกับระบบอื่น
5.2 Process Optimization	สำรวจประสิทธิภาพของกระบวนการทำงานด้วยการนำเทคโนโลยีดิจิทัลและแพลตฟอร์มมาประยุกต์ใช้
5.2.1 Administration	สำรวจการนำเทคโนโลยีดิจิทัลมาเพิ่มประสิทธิภาพในการบริหารจัดการภายในองค์กร
5.2.2 Platform for Communication and Collaboration	สำรวจกระบวนการติดต่อสื่อสาร การทำงานระหว่างหน่วยงานภายในองค์กรและ ข้ามองค์กร

ตัวชี้วัดที่ 6 โครงสร้างพื้นฐานความมั่นคงปลอดภัยและมีประสิทธิภาพ (Secure and Efficient Infrastructure)

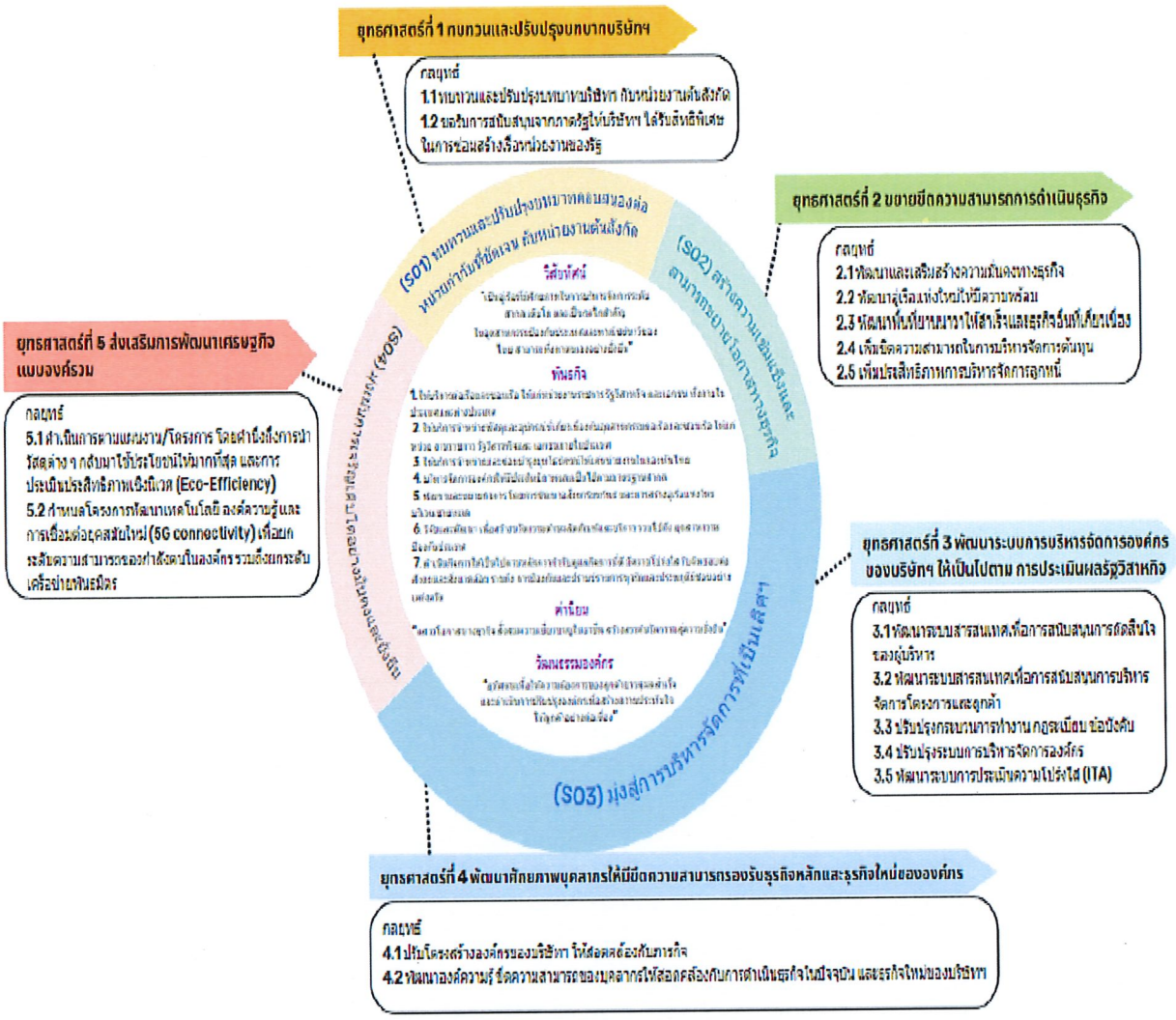
ตัวชี้วัด	วัตถุประสงค์
6.1 Reliable Infrastructure	สำรวจการนำโครงสร้างพื้นฐานกลางภาครัฐที่มีเสถียรภาพและมีประสิทธิภาพมาปรับใช้ในหน่วยงาน
6.2 Cybersecurity (Cybersecurity Standard and Procedure)	สำรวจการมีมาตรฐานและแนวทางในการดำเนินการด้านความมั่นคงปลอดภัยทางไซเบอร์

ตัวชี้วัดที่ 7 เทคโนโลยีดิจิทัลและการนำไปใช้ (Digital Technology Practices)

ตัวชี้วัด	วัตถุประสงค์
7.1 Digital Technological Practices	สำรวจการใช้ประโยชน์จากเทคโนโลยีที่เกิดขึ้นใหม่

2.1.5 **ทบทวนยุทธศาสตร์ตามแผนวิสาหกิจ บริษัท อู่กรุงเทพ จำกัด**

แผนวิสาหกิจ ปีงบประมาณ พ.ศ.2568 – 2572 ของ บริษัท อู่กรุงเทพ จำกัด จัดทำขึ้นเพื่อใช้เป็นแผนหลักและปรับปรุงให้สอดคล้องตามสถานการณ์ในปัจจุบัน และตอบสนองต่อวัตถุประสงค์ ภารกิจหลักขององค์กร และคำนึงถึงบริบทการเปลี่ยนแปลงที่คาดว่าจะเกิดขึ้นในอนาคต ซึ่งแสดงให้เห็นถึงทิศทาง และแนวทางที่กำหนดไว้ ในระยะเวลา 5 ปีข้างหน้ารวมถึงเป็นไปตามข้อเสนอแนะของสำนักงานคณะกรรมการนโยบายรัฐวิสาหกิจ รวมถึงเป็นไปตามกระบวนการวางแผนยุทธศาสตร์ตามแนวทางระบบการประเมินผลการดำเนินงานของรัฐวิสาหกิจ State Enterprise Assessment Model : SE-AM และสอดคล้องกับแผนพัฒนารัฐวิสาหกิจ พ.ศ.2566 – 2570 และสอดคล้องกับยุทธศาสตร์ชาติ 20 ปี แผนแม่บทภายใต้ยุทธศาสตร์ชาติ 20 ปี แผนพัฒนาเศรษฐกิจและสังคมแห่งชาติ ฉบับที่ 13 แผนยุทธศาสตร์รัฐวิสาหกิจรายสาขา แผนยุทธศาสตร์รัฐวิสาหกิจ แผนยุทธศาสตร์บริษัทฯ รวมทั้งการดำเนินงานที่ควรให้ความสำคัญอย่างต่อเนื่องที่มีนัยสำคัญต่อการดำเนินงานของบริษัทฯ



ภาพที่ 1 ความสอดคล้องระหว่างยุทธศาสตร์ แผนวิสาหกิจ และแผนปฏิบัติการ ของ บริษัท อู่กรุงเทพ จำกัด ปีงบประมาณ พ.ศ.2568 – 2572

ยุทธศาสตร์ของบริษัท อู่กรุงเทพ จำกัด ตามแผนวิสาหกิจ ปีงบประมาณ พ.ศ.2569 - พ.ศ.2573 เกี่ยวกับการพัฒนาเทคโนโลยีดิจิทัล มีรายละเอียดดังนี้

ยุทธศาสตร์	วัตถุประสงค์เชิงยุทธศาสตร์	กลยุทธ์การดำเนินการ	ตัวชี้วัด/แผนงาน	เป้าหมาย				
				2569	2570	2571	2572	2573
ยุทธศาสตร์ที่ 3 พัฒนาระบบการบริหารจัดการองค์กรของบริษัทฯ ให้เป็นไปตามการประเมินผลรัฐวิสาหกิจ	3.1 พัฒนาระบบสารสนเทศเพื่อสนับสนุนการตัดสินใจของผู้บริหารและการบริหารจัดการโครงการ	3.1 พัฒนาระบบสารสนเทศเพื่อการสนับสนุนการตัดสินใจของผู้บริหาร	3.1.1 ความสำเร็จในการดำเนินการตามโครงการ (1) แผนงานพัฒนาระบบสารสนเทศเพื่อการสนับสนุนการตัดสินใจของผู้บริหาร - ระบบวิเคราะห์เชิงลึก (BI) ตัดสินใจแบบ Real-Time	>1 โครงการ	>1 โครงการ	>1 โครงการ	>1 โครงการ	>1 โครงการ
		3.2 พัฒนาระบบสารสนเทศเพื่อการสนับสนุนการบริหารจัดการโครงการและลูกค้า	3.2.1 ความสำเร็จในการดำเนินการตามโครงการ (1) แผนงานพัฒนาระบบสารสนเทศเพื่อการสนับสนุนการบริหารจัดการโครงการและผู้มีส่วนได้เสียทั้งภายในและภายนอก - จัดทำแพลตฟอร์มจอง/ติดตามงานซ่อมแบบออนไลน์	>1 โครงการ	>1 โครงการ	>1 โครงการ	>1 โครงการ	>1 โครงการ
	3.2 ปรับปรุงกระบวนการทำงาน กฎระเบียบ และข้อบังคับให้สอดคล้องกับการดำเนินธุรกิจในปัจจุบัน	3.3 ปรับปรุงกระบวนการทำงาน กฎระเบียบข้อบังคับให้สอดคล้อง เหมาะสมกับการดำเนินธุรกิจของบริษัทฯ ในปัจจุบันที่ต้องแข่งขันกับภาคเอกชน	3.3.1 จำนวนกระบวนการทำงาน/ระเบียบ/ข้อบังคับบริษัทฯ ที่ได้รับการทบทวนปรับปรุงแก้ไข /การอนุมัติยกเว้นการปฏิบัติตามระเบียบกระทรวงการคลังว่าด้วยการจัดซื้อจัดจ้างและการบริหารพัสดุ ภาครัฐ พ.ศ. 2560 ให้สอดคล้องกับการดำเนินธุรกิจในปัจจุบันที่ต้องแข่งขันกับภาคเอกชน (1) แผนงานปรับปรุงเพิ่มเติมกฎระเบียบข้อบังคับให้หน่วยงานมีมาตรฐานสากลมีความคล่องตัวโปร่งใสและสามารถตรวจสอบได้	>2	>2	>2	>2	>2
	3.3 เสริมสร้างความโปร่งใสและธรรมาภิบาลในการดำเนินงานของบริษัทฯ	3.4 ปรับปรุงระบบการบริหารจัดการองค์กรให้เป็นไปตามมาตรฐานที่ สคร. กำหนด	3.4.1 คะแนนผลประเมินด้านการบริหารจัดการองค์กร (1) การกำกับดูแลที่ดีและการนำองค์กร (2) การวางแผนเชิงกลยุทธ์ (3) การบริหารความเสี่ยงและการควบคุม	>1.70	>1.80	>1.90	>2.20	>2.50

ยุทธศาสตร์	วัตถุประสงค์เชิงยุทธศาสตร์	กลยุทธ์การดำเนินการ	ตัวชี้วัด/แผนงาน	เป้าหมาย				
				2569	2570	2571	2572	2573
			ภายใน (4) การมุ่งเน้นผู้มีส่วนได้ส่วนเสีย และลูกค้า (5) การพัฒนาเทคโนโลยีดิจิทัล (6) การบริหารทุนมนุษย์ (7) การจัดการความรู้และนวัตกรรม (8) การตรวจสอบภายใน					
		3.5 พัฒนาระบบการประเมินความโปร่งใสในการดำเนินงานของบริษัทฯ (ITA) และเลิกทำผิดกฎระเบียบ	3.5.1 ผลประเมินความโปร่งใสในการดำเนินงานของบริษัทฯ (1) โครงการพัฒนาระบบการประเมินความโปร่งใสในการดำเนินงานฯ	>94.00	>94.15	>94.30	>94.45	>94.60
ยุทธศาสตร์ที่ 5 ส่งเสริมการพัฒนาเศรษฐกิจแบบองค์รวม	5.1 ดำเนินการตามแผนงาน/โครงการโดยคำนึงถึงการใช้ทรัพยากรอย่างมีประสิทธิภาพและลดผลกระทบต่อสิ่งแวดล้อม	5.1 ดำเนินการตามแผนงาน/โครงการ โดยคำนึงถึงการนำวัสดุต่าง ๆ กลับมาใช้ประโยชน์ให้มากที่สุด เพื่อลดปัญหาขยะที่ส่งผลเสียต่อสิ่งแวดล้อม และการประเมินประสิทธิภาพเชิงนิเวศเศรษฐกิจ	5.1.1 ร้อยละความสำเร็จในการดำเนินโครงการลดผลเสียต่อสิ่งแวดล้อม (1) การประเมินประสิทธิภาพเชิงนิเวศเศรษฐกิจ (Eco-Efficiency)	>20	>40	>60	>80	100
	5.2 พัฒนาเทคโนโลยีและองค์ความรู้เพื่อยกระดับความสามารถของกำลังคนและเครือข่ายพันธมิตร	5.2 พัฒนาเทคโนโลยี องค์ความรู้ และการเชื่อมต่อยุคสมัยใหม่ (5G connectivity) เพื่อยกระดับความสามารถของกำลังคนในองค์กร รวมถึงยกระดับเครือข่ายพันธมิตร	5.2.1 ความสำเร็จในการดำเนินการตามโครงการพัฒนาเทคโนโลยี องค์ความรู้ และการเชื่อมต่อยุคสมัยใหม่ (1) แผนงานพัฒนาโครงสร้างพื้นฐานทางด้านเทคโนโลยีสารสนเทศ (2) แผนงานนำเทคโนโลยีและนวัตกรรมเข้ามาใช้	>1 โครงการ	>1 โครงการ	>1 โครงการ	>1 โครงการ	>1 โครงการครงการ

2.1.6 ทบทวนกฎหมาย ระเบียบข้อบังคับที่เกี่ยวข้อง

2.1.6.1 แนวทางปฏิบัติด้านการพัฒนาดิจิทัลรองรับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล 2562

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562
Personal Data Protection Act (PDPA), B.E 2562 (2019)

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (Personal Data Protection Act, B.E. 2562 - PDPA) ของประเทศไทยกำหนดแนวทางและข้อบังคับเพื่อปกป้องข้อมูลส่วนบุคคลของประชาชนจากการถูกใช้งานโดยไม่ได้รับความยินยอม และเพื่อให้มั่นใจว่ามีการจัดการข้อมูลส่วนบุคคลอย่างปลอดภัยและถูกต้องตามกฎหมายแนวทางปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล 2562

1. **การเก็บรวบรวมข้อมูลส่วนบุคคล:**
    - ต้องได้รับความยินยอมจากเจ้าของข้อมูลก่อนการเก็บรวบรวม ยกเว้นในกรณีที่กฎหมายอนุญาต
    - ต้องมีการแจ้งวัตถุประสงค์ในการเก็บรวบรวมข้อมูล และใช้ข้อมูลเฉพาะวัตถุประสงค์ที่ได้รับการยินยอมเท่านั้น
2. **การใช้ข้อมูลส่วนบุคคล:**
    - ใช้ข้อมูลตามวัตถุประสงค์ที่ได้แจ้งไว้และได้รับความยินยอมจากเจ้าของข้อมูล
    - หากต้องการใช้ข้อมูลนอกเหนือจากวัตถุประสงค์ที่ได้รับการยินยอม ต้องได้รับความยินยอมใหม่จากเจ้าของข้อมูล
3. **การเปิดเผยข้อมูลส่วนบุคคล:**
    - ต้องได้รับความยินยอมจากเจ้าของข้อมูลก่อนการเปิดเผย ยกเว้นในกรณีที่กฎหมายอนุญาต
    - ต้องมีการป้องกันและรักษาความลับของข้อมูลในกรณีที่มีการเปิดเผย

4. **การรักษาความปลอดภัยของข้อมูลส่วนบุคคล:**
    - ต้องมีมาตรการรักษาความปลอดภัยที่เหมาะสมเพื่อป้องกันการสูญหาย การเข้าถึง การใช้ การเปลี่ยนแปลง หรือการเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต
    - ต้องทำการทบทวนและปรับปรุงมาตรการรักษาความปลอดภัยอย่างสม่ำเสมอ
5. **สิทธิของเจ้าของข้อมูลส่วนบุคคล:**
    - เจ้าของข้อมูลมีสิทธิในการเข้าถึงข้อมูลส่วนบุคคลของตนเอง
    - มีสิทธิในการขอแก้ไขหรือปรับปรุงข้อมูลส่วนบุคคลที่ไม่ถูกต้องหรือไม่เป็นปัจจุบัน
    - มีสิทธิในการขอให้ลบหรือทำลายข้อมูลส่วนบุคคลเมื่อไม่ต้องการให้เก็บข้อมูลต่อไป
6. **การจัดตั้งผู้ควบคุมข้อมูลและผู้ประมวลผลข้อมูล:**
    - องค์กรต้องจัดตั้งบุคคลหรือหน่วยงานที่มีหน้าที่ในการควบคุมและประมวลผลข้อมูลส่วนบุคคล
    - ต้องมีการอบรมและสร้างความตระหนักรู้ให้กับบุคลากรในองค์กรเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล
7. **การแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล:**
    - หากเกิดเหตุการละเมิดข้อมูลส่วนบุคคล ต้องแจ้งเหตุการละเมิดไปยังสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลภายใน 72 ชั่วโมง
    - ต้องแจ้งเจ้าของข้อมูลถึงเหตุการละเมิดหากมีความเสี่ยงที่จะกระทบสิทธิและเสรีภาพของเจ้าของข้อมูล

การปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลอย่างเคร่งครัดจะช่วยให้การจัดการข้อมูลส่วนบุคคลเป็นไปอย่างมีประสิทธิภาพและถูกต้องตามกฎหมาย รวมถึงปกป้องสิทธิและความเป็นส่วนตัวของเจ้าของข้อมูลส่วนบุคคลจากที่กฎหมาย PDPA เริ่มบังคับใช้ตั้งแต่วันที่ 1 มิถุนายน 2565 นับจนถึงปัจจุบัน คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (PDPC) ได้ออกประกาศกฎหมายลำดับรองของกฎหมาย PDPA เพิ่มเติมอีกหลายฉบับตามมา เพื่อยกระดับมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลให้มีประสิทธิภาพยิ่งขึ้น เรามาดูกันว่ามีอะไรเปลี่ยนแปลง แล้วองค์กรควรต้องปรับตัวอย่างไรบ้างเนื้อหาตามประกาศหลัก ๆ ที่สำคัญมีดังนี้

- Security Measures of Data Controller: มาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล2.) Record of Processing Activities (ROPA): บันทึกรายการของกิจกรรมการประมวลผลข้อมูลส่วนบุคคล (ROPA) กำหนดวิธีการจัดทำและเก็บรักษาบันทึกรายละเอียดเกี่ยวกับกิจกรรมการประมวลผลข้อมูลส่วน
- Data Breach Notification: การแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล กำหนดแนวทางการประเมินความเสี่ยงและความร้ายแรงของ

- Data Protection Officer: เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) กำหนดลักษณะขององค์กรที่ต้องจัดให้มีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO
- Security Measures for Historical Research for Public Task: มาตรการปกป้องข้อมูลส่วนบุคคลสำหรับการจัดทำเอกสารประวัติศาสตร์หรือจดหมายเหตุเพื่อประโยชน์
- Security Measures for Scientific Research and Statistical Purposes: มาตรการที่เหมาะสมสำหรับการเก็บรวบรวมข้อมูลส่วนบุคคลเพื่อให้บรรลุวัตถุประสงค์ที่เกี่ยวกับการศึกษาวิจัยหรือสถิติกำหนดมาตรการปกป้องที่เหมาะสมเพื่อคุ้มครองสิทธิและเสรีภาพของเจ้าของข้อมูลส่วน
- Cross-Border Transfer: หลักเกณฑ์การให้ความคุ้มครองข้อมูลส่วนบุคคลที่ส่งหรือโอนไปยังต่างประเทศ
- Security Measures for Criminal Record: มาตรการคุ้มครองข้อมูลส่วนบุคคลเกี่ยวกับประวัติอาชญากรรม

2.1.6.2 พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562

พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 (Cybersecurity Act, B.E. 2562) ของประเทศไทยมีข้อกำหนดหลายประการในการรักษาความมั่นคงปลอดภัยทางไซเบอร์ของประเทศ ทั้งนี้เพื่อป้องกันและลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ และเพื่อรักษาความมั่นคงของระบบสารสนเทศในภาคส่วนต่างๆ

ตามพระราชบัญญัตินี้เน้นการปฏิบัติตามและมาตรการที่ต้องดำเนินการโดยองค์กรต่างๆ เพื่อให้มั่นใจว่ามีการรักษาความมั่นคงปลอดภัยทางไซเบอร์ตามมาตรฐานที่กำหนดสิ่งที่สำคัญในมาตรา 2.5 ประกอบด้วย:

1. **การประเมินและจัดการความเสี่ยง**: องค์กรต่างๆ ต้องดำเนินการประเมินความเสี่ยงที่อาจเกิดขึ้นจากภัยคุกคามทางไซเบอร์ และจัดการความเสี่ยงนั้นอย่างมีประสิทธิภาพ
2. **การพัฒนานโยบายและแผนการรักษาความมั่นคงปลอดภัยไซเบอร์**: องค์กรต้องมีนโยบายและแผนการที่ชัดเจนในการรักษาความมั่นคงปลอดภัยไซเบอร์ รวมถึงการปรับปรุงและทบทวนนโยบายและแผนการดังกล่าวอย่างสม่ำเสมอ
3. **การป้องกันและตรวจจับภัยคุกคามทางไซเบอร์**: องค์กรต้องมีมาตรการที่เหมาะสมในการป้องกันและตรวจจับภัยคุกคามทางไซเบอร์ รวมถึงการใช้เทคโนโลยีที่ทันสมัยในการตรวจจับและตอบโต้ภัยคุกคาม
4. **การบริหารจัดการเหตุการณ์**: องค์กรต้องมีแผนการบริหารจัดการเหตุการณ์ที่เกี่ยวข้องกับภัยคุกคามทางไซเบอร์อย่างมีประสิทธิภาพ รวมถึงการรายงานและการตอบสนองต่อเหตุการณ์อย่างรวดเร็ว

5. **การฝึกอบรมและสร้างความตระหนักรู้**: องค์กรต้องจัดการฝึกอบรมและสร้างความตระหนักรู้ให้กับบุคลากรในองค์กรเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์การปฏิบัติตามข้อกำหนดเหล่านี้จะช่วยให้องค์กรสามารถป้องกันและตอบโต้ภัยคุกคามทางไซเบอร์ได้อย่างมีประสิทธิภาพ และรักษาความมั่นคงของระบบสารสนเทศในองค์กรได้อย่างยั่งยืนความตระหนักถึงบทบาทหน้าที่ตามกฎหมายในเรื่องของการรักษาความมั่นคงปลอดภัย มีความรู้ความเข้าใจในการจัดการเกี่ยวกับภัยคุกคามด้านความมั่นคงปลอดภัยและความเสี่ยงทางด้านเทคโนโลยีดิจิทัล ที่กำลังเป็นปัญหาในการทำงานในยุคดิจิทัลได้อย่างมีประสิทธิภาพตามแนวทางของ NIST Cybersecurity Framework โดยแบ่งออกเป็น 5 ขั้นตอนสำคัญ คือ Identity, Protect, Detect, Response และ Recovery สำหรับช่วยให้องค์กรสามารถวางแผนป้องกัน ตรวจจับ และตอบสนองต่อภัยคุกคามได้อย่างรวดเร็วและเป็นระบบ และเข้าใจในกระบวนการในการวางแผนรับมือกับภัยคุกคามและความเสี่ยงทางด้านเทคโนโลยีดิจิทัล การเข้าใจในกระบวนการจะทำให้เกิดการวางแผนที่ดีและยั่งยืนในการรับมือกับความเสี่ยงรูปแบบต่าง ๆ ที่เกิดขึ้นทั้งในปัจจุบันและอนาคตที่มีการเปลี่ยนแปลงทางด้านเทคโนโลยีอย่างรวดเร็วเพื่อช้ในการวางแผนการรับมือกับภัยคุกคามและความเสี่ยงทางด้านดิจิทัลในองค์กรได้อย่างมีประสิทธิภาพ

   5.1 ภาพรวมความมั่นคงปลอดภัยไซเบอร์ (Security Overview) เป็นการเรียนรู้ Security Awareness การรู้เท่าทันการโจมตีและความมั่นคงปลอดภัยทางไซเบอร์ สถานการณ์ต่าง ๆ ที่เกิดขึ้นในการองค์กรทั้งภาครัฐและเอกชนกรณีศึกษาต่าง ๆ ที่เกิดขึ้นทั้งในประเทศและต่างประเทศ การเรียนรู้ถึงความเสียหายที่เกิดขึ้นจากภัยคุกคามไซเบอร์ Security Trend แนวโน้มของภัยคุกคามต่าง ๆ แนวโน้มของความมั่นคงปลอดภัย ไซเบอร์ Information security Concept: CIA แนวคิดพื้นฐานของความมั่นคงปลอดภัยไซเบอร์ Confidentiality คือ การรักษาความลับของ ไซเบอร์ Integrity คือความถูกต้องของข้อมูลไซเบอร์ Availability คือความพร้อมใช้งานของ เทคโนโลยีไซเบอร์

   5.2 กฎหมายที่เกี่ยวข้องกับความมั่นคงปลอดภัย ไซเบอร์ (Laws and Regulation) พ.ร.บ. ว่าด้วยการกระทาความผิดเกี่ยวกับคอมพิวเตอร์ 2560 พ.ร.บ.การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.2562 พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 กรณีศึกษาที่เกี่วข้องกับกฎหมายที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์

   5.3 การระบุความเสี่ยงด้านความมั่นคงปลอดภัย ไซเบอร์ (Identify) การศึกษาทำความเข้าใจบริบท ทรัพยากรและกิจกรรมงานสาคัญเพื่อบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ที่มีต่อระบบทรัพย์สิน ข้อมูล และขีดความสามารถ Identity: Assessment and Auditing แนวทางและกรอบในการการประเมินองค์กรด้านความมั่นคงปลอดภัยไซเบอร์ และความเสี่ยง เพื่อ

วิเคราะห์ช่องว่าง (Gap Analysis) หรือจุดอ่อนของกระบวนการในการรักษาความมั่นคงปลอดภัยทางไซเบอร์ขององค์กร ตัวอย่าง ของ Framework ในการประเมินขององค์กรต่าง ๆ

5.4 การป้องกันด้านความมั่นคงปลอดภัยไซเบอร์ (Protection) การศึกษาแนวทางการจัดทำและดำเนินการตามมาตรการป้องกันที่เหมาะสม เพื่อการจำกัดระดับผลกระทบของเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ และการสร้ างความตระหนักมาตรการควบคุมการเข้าถึงและมาตรการด้านความมั่นคงปลอดภัยต่าง ๆ ทั้งกระบวนการและวิธีปฏิบัติการศึกษากรอบงานความมั่นคงปลอดภัยทาง ไซเบอร์ (Cybersecurity framework) Protection: Security Design Principles ความรู้พื้นฐานและแนวทางการออกแบบระบบให้มีความมั่นคงปลอดภัย แนวทางการเลือกใช้วิธีการ ระบบหรือเทคโนโลยีเพื่อการรักษาความมั่นคงปลอดภัยในองค์กร เช่น ไฟร์วอล (Firewall) การป้องกันเครื่องอุปกรณ์ปลายทาง (Endpoint Security) การสำรองข้อมูล (Data backup) เพื่อให้เหมาะสมกับการใช้งานในองค์กรเทคโนโลยีในการรักษาความมั่นคงปลอดภัย ไซเบอร์

5.5 การเฝ้าระวังด้านความมั่นคงปลอดภัยไซเบอร์ (Detection) เรียนรู้การจัดทำและดำเนินกิจกรรมเพื่อตรวจหาเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ที่อาจเกิดขึ้น Detection: Security Monitoring การเรียนรู้แนวทางการวิเคราะห์ เฝ้าระวังและแจ้งเตือนภัยคุกคามทางคอมพิวเตอร์ (Security Monitoring Service) การวิเคราะห์ความเกี่ยวโยงของเหตุการณ์และภัยคุกคามด้านความปลอดภัยไซเบอร์ (Security Monitoring) จากข้อมูลจราจรทางคอมพิวเตอร์ (Log) ของเครื่องแม่ข่ายอุปกรณ์เครือข่ายและระบบงานต่าง ๆ เรียนรู้แนวทางการจัดตั้งศูนย์ปฏิบัติการเฝ้าระวังความมั่นคงปลอดภัยระบบ

5.6 การรับมือด้านความมั่นคงปลอดภัยไซเบอร์ (Response) เรียนรู้การจัดทาและดาเนินกิจกรรมเพื่อตอบสนองต่อเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ที่ตรวจพบ ครอบคลุมถึงการวางแผนรับมือ การสื่อสาร การวิเคราะห์ การลดความเสี่ยง และการปรับปรุงเรียนรู้เกี่ยวกับกระบวนการ “Incident Response” การตอบสนองต่อสถานการณ์ไม่พึงประสงค์และไม่คาดคิดเพื่อให้องค์กรสามารถควบคุมสถานการณ์และมูลค่าความเสียหายที่เกิดขึ้นให้รวดเร็วทันการณ์และลดความเสียหาย กรณีศึกษาของการจัดทำแผนการตอบสนองภัยคุกคาม (Incident Response Plan) ในองค์กรทั้งในและต่างประเทศกระบวนการและขั้นตอนในการจัดทำแผนการตอบสนองภัยคุกคาม (Incident Response Plan)

5.7 การกู้คืนด้านความมั่นคงปลอดภัยไซเบอร์ (Recovery) เรียนรู้การกู้คืนระบบในกรณีเกิดการโจมตี การกู้คืนข้อมูล เรียนรู้ ในวิธีการและแนวทางในการกู้คืนระบบให้กลับสู่สภาวะปกติและแก้ไข

สาเหตุที่ทำให้เกิดปัญหากรณี ศึกษาและตัวอย่างของการกู้คืนระบบ (Recovery) ที่เกิดขึ้นจากการโจมตีทางไซเบอร์

2.2 การสำรวจข้อมูลผู้มีส่วนได้ส่วนเสียกับกระบวนการจัดทำแผนพัฒนาดิจิทัล

การระบุผู้มีส่วนได้ส่วนเสียในแต่ละกระบวนการธุรกิจ มีวัตถุประสงค์เพื่อตอบสนองความ ต้องการขององค์กรที่มีต่อผู้มีส่วนได้ส่วนเสียใน 2 ลักษณะ คือ องค์กรต้องการปรับกระบวนการทางธุรกิจเพื่อ สร้างผลกระทบเชิงบวกและลดผลกระทบเชิงลบที่มีต่อผู้มีส่วนได้ส่วนเสีย และหากองค์กรพิจารณาแล้วว่า กระบวนการทางธุรกิจดีอยู่แล้ว แต่ผู้มีส่วนได้ส่วนเสียยังมีความวิตกกังวลอยู่ องค์กรจำเป็นต้องสร้างความ เข้าใจเพื่อเปลี่ยนแปลงทัศนคติของผู้มีส่วนได้ส่วนเสีย โดยองค์กรต้องมีแผนพัฒนาให้เห็นภาพรวมทั้งหมดของ การปรับปรุงกระบวนการและการสื่อสารเชื่อมโยงผู้มีส่วนได้ส่วนเสียอย่างชัดเจน นอกจากนี้ องค์กรต้องจัดทำ Stakeholder Profile ที่ระบุถึงรายชื่อ/สถานะ รูปแบบการทำงานผู้มีอิทธิพลในหน่วยงาน รายชื่อผู้ ประสานงาน บริบทอื่น ๆ ที่เกี่ยวกับผู้มีส่วนได้ส่วนเสีย ประเภทของผู้มีส่วนได้ส่วนสีย (เช่น รัฐบาล สังคม ลูกค้า เป็นต้น) จุดประสงค์ในการสร้างสัมพันธ์กับผู้มีส่วนได้ส่วนเสีย ประเด็นที่สำคัญของผู้มีส่วนได้ส่วนเสีย ระดับความสัมพันธ์ระหว่างองค์กรกับผู้มีส่วนได้ส่วนเสียในปัจจุบัน ระดับความสัมพันธ์ที่องค์กรคาดหวังจาก ผู้มีส่วนได้ส่วนเสีย ความสามารถ/ข้อจำกัดของผู้มีส่วนได้ส่วนเสีย (เช่น ภาษา วัฒนธรรมความสามารถในการสื่อสาร เป็นต้น) เพื่อสื่อสารให้หน่วยงานต่างๆ เข้าใจเกี่ยวกับผู้มีส่วนได้ส่วนเสียแต่ละกลุ่มและสามารถ วางแผนสร้างความสัมพันธ์กับผู้มีส่วนได้ส่วนเสียกลุ่มต่างๆ ได้สอดรับกับความต้องการและความคาดหวังของ ผู้มีส่วนได้ส่วนเสียที่มีต่อองค์กรทั้งในระยะสั้นและระยะยาวอย่างเหมาะสม

การระบุผู้มีส่วนได้เสียขององค์กร

ที่มา : www.setsustainablity.com

ตารางจำแนกประเภทข้อมูลผู้มีส่วนได้เสีย (Stakeholder Profile)

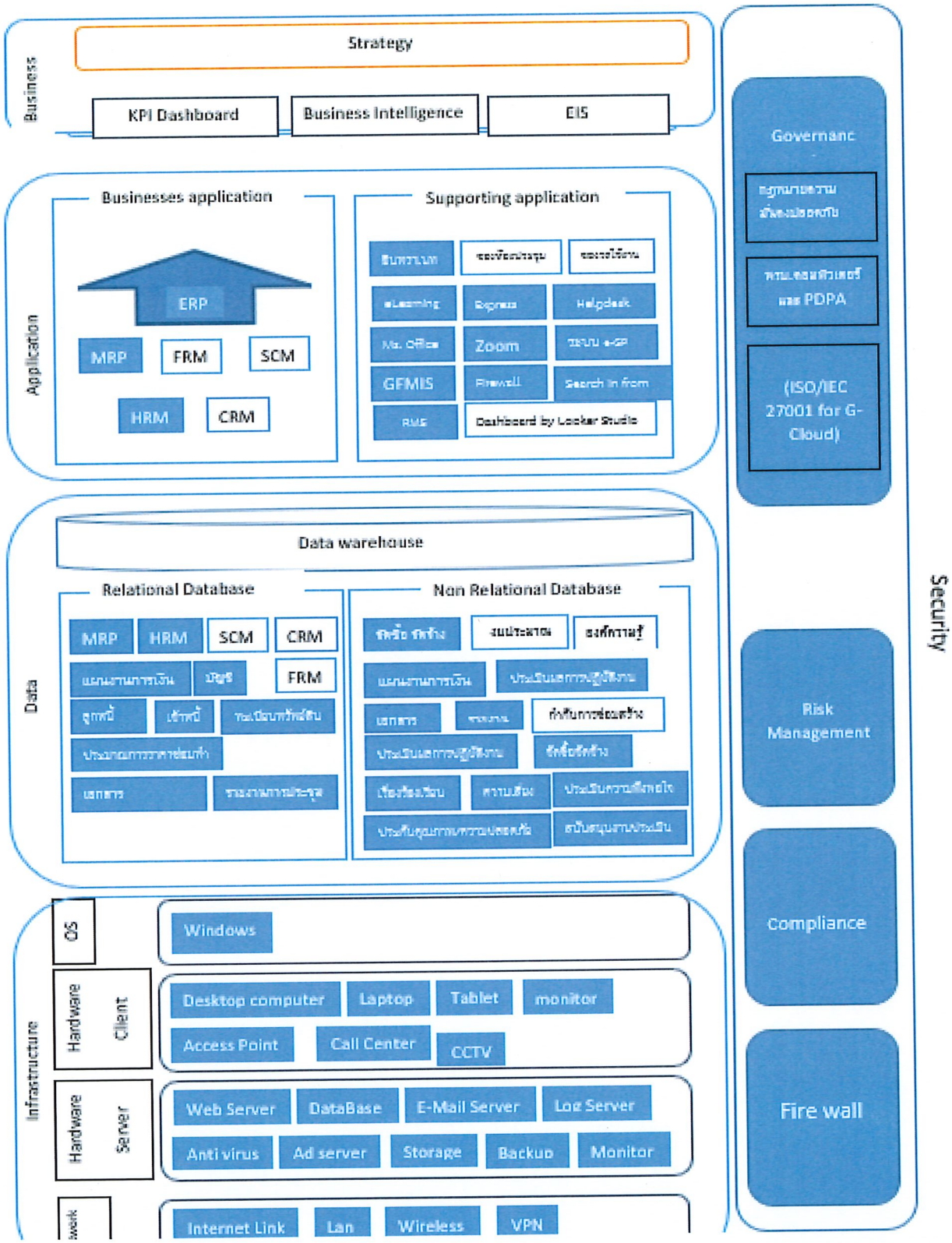
ประเภท	ความเกี่ยวข้องผู้มีส่วนได้เสียกับองค์กร		
	ภายใน	ภายนอก	ความคาดหวัง/ข้อเสนอแนะ
1.กลุ่มคณะกรรมการบริษัท	1.1 คณะกรรมการบริษัทฯ		สนับสนุนการปฏิบัติงานในด้านการพัฒนาเทคโนโลยีดิจิทัล ให้เป็นไปตามแผนงานและมีการติดตามประเมินผลการดำเนินงานให้เป็นไปอย่างมีประสิทธิภาพ
	1.2 คณะอนุกรรมการชุดต่าง ๆ		สนับสนุนการปฏิบัติงานของคณะกรรมการบริษัทฯ ในด้านการพัฒนาเทคโนโลยีดิจิทัล ให้เป็นไปตามแผนงานและมีการติดตามประเมินผลการดำเนินงานให้เป็นไปอย่างมีประสิทธิภาพ
2.กลุ่มผู้บริหารและพนักงาน	2.1 ผู้บริหาร ได้แก่ กรรมการผู้จัดการ รอง.กก.ผจก. ผู้อำนวยการ รอง.ผอ. หัวหน้าแผนก หัวหน้าส่วนงานต่าง ๆ		การสนับสนุนในด้านเทคโนโลยีดิจิทัล เกี่ยวกับข้อมูลสำหรับการตัดสินใจในด้านต่าง ๆ รวมถึงการบริหารโครงการของบริษัทฯ ให้เป็นไปอย่างมีประสิทธิภาพ

	2.2 พนักงาน ได้แก่ เจ้าหน้าที่ทุกระดับชั้น และลูกจ้าง		การสนับสนุนในด้าน เทคโนโลยีดิจิทัล เกี่ยวกับ คอมพิวเตอร์และอุปกรณ์ ต่อพ่วง รวมถึงระบบงาน ต่าง ๆ เป็นไปอย่างมี ประสิทธิภาพ
3.กลุ่มลูกค้า		3.1 ลูกค้าผู้เช่า อาคาร สถานที่	การสนับสนุนข้อมูล เกี่ยวกับอาคารสถานที่ สำหรับการขอใช้บริการ ผ่านทาง Social Network ต่าง ๆ เช่น Website หรือ Line เป็นต้น
		3.2 ลูกค้าผู้เช่า ท่าเทียบ เรือ อู่เรือ หรือซ่อมสร้าง เรือ	การสนับสนุนข้อมูล เกี่ยวกับท่าเทียบเรือ อู่เรือ สำหรับการขอใช้บริการ ผ่านทาง Social Network ต่าง ๆ เช่น Website หรือ Line เป็นต้น
		3.3 ผู้ใช้บริการ (ประชาชน)	การสนับสนุนข้อมูล เกี่ยวกับเรื่องทั่ว ๆ ไป สำหรับการขอใช้บริการ ผ่านทาง Social Network ต่าง ๆ เช่น Website หรือ Line เป็นต้น
4.กลุ่มหน่วยงานกำกับ		4.1 กองทัพเรือ กระทรวงกลาโหม	สนับสนุนการปฏิบัติงาน ของบริษัทฯ ในด้านการ พัฒนาเทคโนโลยีดิจิทัล ให้ เป็นไปตามแผนงานและมี การติดตามประเมินผลการ ดำเนินงานให้เป็นไปอย่าง มีประสิทธิภาพ
		4.2 กระทรวงการคลัง	
		4.3 ผู้ถือหุ้น	

5.กลุ่มหน่วยงานประเมิน		5.1 สำนักงานคณะกรรมการนโยบายรัฐวิสาหกิจ (สคร.)	สนับสนุนการปฏิบัติงานของบริษัทฯ ในด้านการพัฒนาเทคโนโลยีดิจิทัล ให้เป็นไปตามแผนงานและมีการติดตามประเมินผลการดำเนินงานให้เป็นไปอย่างมีประสิทธิภาพ
		5.2 บริษัท ทริส คอร์ปอเรชั่น จำกัด	
		5.3 สำนักงานคณะกรรมการป้องกัน และปราบปรามการทุจริตแห่งชาติ	
6.กลุ่มประสานงาน		สำนักงานเขต/ที่ว่าการอำเภอ สรรพากร สถาบันการเงิน กรมป้องกันและบรรเทาสาธารณภัย เป็นต้น	การสนับสนุนข้อมูลเกี่ยวกับเรื่องทั่ว ๆ ไป สำหรับการได้รับข้อมูลข่าวสารผ่านทาง Social Network ต่าง ๆ เช่น Website หรือ Line เป็นต้น
7.กลุ่มอื่น ๆ		ชุมชน เจ้าหนี้การค้า คู่ค้า สื่อมวลชน	การสนับสนุนข้อมูลเกี่ยวกับเรื่องทั่ว ๆ ไป สำหรับการขอใช้บริการผ่านทาง Social Network ต่าง ๆ เช่น Website หรือ Line เป็นต้น

2.3 วิเคราะห์ข้อมูลที่เกี่ยวข้องกับการพัฒนาเทคโนโลยีดิจิทัล

2.3.1 สถาปัตยกรรมองค์กร ของ บอท. (Enterprise Architecture)



2.3.1.1 สถาปัตยกรรมด้านธุรกิจ (Business Architecture) ประกอบไปด้วย ยุทธศาสตร์ (Strategy) และกระบวนการธุรกิจ (Business Process) การวิเคราะห์สถาปัตยกรรมด้านธุรกิจเป็นกระบวนการที่สำคัญในการกำหนด

โครงสร้างและกระบวนการทำงานของธุรกิจในระดับองค์กร มันรวมถึงการวิเคราะห์และออกแบบกระบวนการธุรกิจที่ชัดเจน เพื่อให้ตรงกับเป้าหมายและยุทธศาสตร์ขององค์กร

2.3.1.2 สถาปัตยกรรมด้านข้อมูล (Data Architecture) ประกอบไปด้วย แอปพิเคชันธุรกิจ (Business Application) แอปพลิเคชันสนับสนุน (Supporting Application) การวิเคราะห์สถาปัตยกรรมด้านข้อมูลเป็นกระบวนการที่ใช้เพื่อออกแบบโครงสร้างข้อมูลภายในองค์กร เพื่อให้มีความสอดคล้องกับภารกิจและกระบวนการทำงานต่าง ๆ โดยมุ่งเน้นไปที่การวิเคราะห์และออกแบบเชิงกลยุทธ์ในการจัดเก็บข้อมูล การประมวลผลข้อมูล และการนำข้อมูลไปใช้ประโยชน์ สถาปัตยกรรมด้านข้อมูลมีเป้าหมายในการเพิ่มประสิทธิภาพในการจัดการข้อมูล ลดความซ้ำซ้อน และเพิ่มความยืดหยุ่นในการใช้งานข้อมูลต่าง ๆ

2.3.1.3 สถาปัตยกรรมด้านระบบงาน (Application Architecture) ประกอบไปด้วย ข้อมูลที่ถูกจัดเก็บในแบบฐานข้อมูล (Relational Database) และข้อมูลที่ไม่ได้จัดเก็บในรูปแบบฐานข้อมูล (Non-Relational Database) การวิเคราะห์และออกแบบโครงสร้างและการทำงานของระบบงานภายในองค์กร เพื่อให้มีความเหมาะสมและเชื่อมโยงกับความต้องการและวัตถุประสงค์ทางธุรกิจขององค์กรได้อย่างมีประสิทธิภาพ การวิเคราะห์สถาปัตยกรรมด้านระบบงานรวมถึงการศึกษาและกำหนดโครงสร้างของระบบงานหลักและระบบงานสนับสนุนที่จำเป็นสำหรับการดำเนินงานขององค์กร

2.3.1.4 สถาปัตยกรรมด้านโครงสร้างพื้นฐาน (Infrastructure Architecture) ประกอบไปด้วยประบบปฏิบัติการ (Operating System) ฮาร์ดแวร์ (Hardware) เครือข่าย (Network) และระบบอำนวยการ (Facility) เป็นกระบวนการที่ศึกษาและวางแผนโครงสร้างพื้นฐานที่จำเป็นสำหรับการสร้างและบริหารจัดการระบบไอทีในองค์กร การวิเคราะห์นี้ช่วยให้องค์กรสามารถวางแผนและจัดการทรัพยากรทางเทคโนโลยีให้เหมาะสมกับความต้องการของธุรกิจ ประสิทธิภาพในการดำเนินงาน และความมั่นคงปลอดภัยของระบบ

2.3.1.5 สถาปัตยกรรมด้านการรักษาความปลอดภัย (Security Architecture) ประกอบไปด้วย ธรรมาภิบาล (Governance) การบริหารจัดการความเสี่ยง (Risk Management) และความสอดคล้องกับกฎระเบียบ (Compliance) การวิเคราะห์สถาปัตยกรรมด้านการรักษาความปลอดภัยมุ่งเน้นที่การออกแบบระบบและโครงสร้างที่ช่วยให้ข้อมูลและระบบเครือข่ายปลอดภัยจากการบุกรุกและภัยคุกคามได้ดีขึ้น เพื่อเสถียรภาพที่มีประสิทธิภาพสูงสุด การสร้าง Enterprise Security Architecture มุ่งเน้นการควบคุมเชิงป้องกันที่แข็งแกร่งเพื่อป้องกันการบุกรุกภายใน

2.3.2 การวิเคราะห์จุดแข็ง จุดอ่อน โอกาส การพัฒนาเทคโนโลยีสารสนเทศของ บอท.

2.3.2.1 การวิเคราะห์สภาพแวดล้อม (SWOT Analysis)

จุดแข็ง / Strength

1. การพัฒนาเทคโนโลยีสารสนเทศของ บอท.เป็นการพัฒนาเพื่อใช้งานเองเป็นหลัก
2. บอท. อยู่ในความควบคุมของกองทัพเรือ เป็นรัฐวิสาหกิจมีประสบการณ์ในการบริหารโครงการต่อเรือและซ่อมบำรุงเรือซึ่งเป็นยุทโธปกรณ์ที่สำคัญของกองทัพเรือมาอย่างต่อเนื่อง ทำให้มีองค์ความรู้ทางด้านซ่อมสร้างเรือในองค์กร
3. บอท.มีความสามารถปรับปรุงแบบเรือและสามารถใช้สิทธิ์แบบเรือตรวจการณ์ไกลฝั่ง ในการขยายธุรกิจการสร้างเรือตรวจการณ์ไกลฝั่ง ให้กับกองทัพเรือไทย และมิตรประเทศ
4. บอท.เป็นรัฐวิสาหกิจ ที่ได้รับการสนับสนุนการดำเนินงานด้านการบริหารจัดการการใช้ทรัพยากรอย่างเหมาะสม จากการสนับสนุนจากนโยบายภาครัฐ เช่น ระบบ Email หรือ MS.365 จาก สพร. รวมถึงระบบคราวน์ภาครัฐช่วยในเรื่องระบบการบริหารความมั่นคงปลอดภัยสารสนเทศ (Information Security Management) เป็นต้น

จุดอ่อน / Weak

1. บุคลากรมีน้อยและขาดความชำนาญเฉพาะงานวิศวกรรมคอมพิวเตอร์ งานด้านพัฒนาระบบเทคโนโลยีดิจิทัล และการจัดการด้านคุณภาพ (Quality Management)
2. บุคลากรขาดความทุ่มเทในการปฏิบัติงานและความมีส่วนร่วมของพนักงานในองค์กรในการบริหารโครงการและการดำเนินงานด้านเทคโนโลยีดิจิทัลอย่างมีประสิทธิภาพ (Project Management) บุคลากรไม่ได้รับการพัฒนาอย่างเป็นระบบและต่อเนื่อง รวมทั้งองค์กรขาดกลยุทธ์เชิงรุกในการดึงดูดคนเก่งจากองค์กรภายนอกเข้ามาร่วมงาน อาจส่งผลต่อประสิทธิภาพการทำงานของบุคลากรองค์กรในอนาคต
3. การจัดสรรงบประมาณด้าน IT ยังไม่ชัดเจนในทุก ๆ ด้าน บอท. มีข้อจำกัดด้านการเงิน รายได้ไม่เพียงพอกับรายจ่าย มีงานน้อยต่อเนื่อง รายจ่ายเพิ่มขึ้น และการปรับปรุงค่าใช้จ่ายขายและบริหารยังไม่สอดคล้องกับต้นทุนขายและบริหาร บอท. ขาดการสนับสนุนเงินงบประมาณจากภาครัฐ และต้นสังกัด พึ่งพาตนเองเป็นหลัก แต่ยังคงนำส่งเงินรายได้ให้ภาครัฐอย่างต่อเนื่อง
4. การบูรณาการเชื่อมโยงข้อมูลและการดำเนินงานร่วมกันระหว่างหน่วยงาน (Government Integration) ไม่มีประสิทธิภาพ และการนำระบบ IT มาสนับสนุนการทำงานในด้านต่าง ๆ ไม่มากเท่าที่ควร

โอกาส / Opportunities

1. บอท. อยู่ในความควบคุมของกองทัพเรือ มีโอกาสในการขอรับการสนับสนุน ด้านองค์บุคคล องค์วัตถุ และองค์ความรู้สมัยใหม่ด้านการซ่อมและสร้างเรือ

2. ภาครัฐมีนโยบายเพิ่มความแข็งแกร่งรัฐวิสาหกิจด้วยการปรับโครงสร้างการบริหารจัดการ พัฒนาประสิทธิภาพการดำเนินงานให้ได้มาตรฐานสากล ส่งเสริมความร่วมมือระหว่างภาครัฐและภาคเอกชน ทั้งในด้านการลงทุนและการบริหารจัดการเพื่อสร้างมูลค่าเพิ่มในทรัพย์สินของรัฐ
3. การพัฒนาพื้นที่ยานนาวาเชิงพาณิชย์ จะส่งผลให้ บอท. มีสถานะทางการเงินที่ดีขึ้น ทั้งการจัดการค่าใช้จ่ายประจำ (Fixed cost) งบประมาณในการลงทุนเพื่อเสริมขีดความสามารถในทางธุรกิจ
4. การพัฒนาอู่เรือแห่งใหม่ เป็นโอกาสที่บริษัทฯ ได้มีโอกาสในการลงทุนเพื่อเสริมขีดความสามารถทั้งในด้าน เครื่องมือ อุปกรณ์ สิ่งอำนวย ความสะดวก และการลงทุนในบุคลากรที่มีศักยภาพที่สอดคล้องกับ Core Business ของบริษัทฯ รวมถึงการขยายธุรกิจในด้านอื่นๆ เพิ่มเติม
5. นโยบาย Thailand 4.0 และรัฐบาลดิจิทัลส่งผลให้เกิดการพัฒนางานด้าน IT ให้ทันและรองรับความเปลี่ยนแปลงได้มากขึ้น ระบบเทคโนโลยีสมัยใหม่เอื้อต่อการเรียนรู้ และพัฒนาด้วยตัวเอง และความก้าวหน้าทางเทคโนโลยีการสื่อสารที่รวดเร็วและทั่วถึงทำให้สามารถส่งข่าวสารกับลูกค้าได้ง่ายและสะดวกขึ้นเป็นโอกาสในการให้บริการลูกค้าและเข้าถึงลูกค้าได้โดยตรง รวมทั้งสังคมดิจิทัล ส่งผลให้สามารถลดค่าใช้จ่ายที่เป็นต้นทุนค่าบริการรับเงินลงได้

อุปสรรค / Threat

1. บุคลากรไม่มีทักษะและความสามารถโดยตรง ขาดความทุ่มเทในการปฏิบัติงานอย่างเต็มที่ ขาดประสิทธิภาพในการทำงาน หรือมีประสิทธิภาพไม่เพียงพอต่อการพัฒนา
2. บุคลากรขาดความรู้ความเข้าใจการใช้เทคโนโลยีสารสนเทศ ในการพัฒนาคุณภาพการทำงานและการใช้ข้อมูลเพื่อการตัดสินใจ
3. ผลประกอบการเป็นตามสภาพเศรษฐกิจส่งผลต่อการลงทุน มีข้อจำกัดด้านการเงิน รายได้ไม่เพียงพอกับรายจ่าย
4. นโยบายภาครัฐและกฎระเบียบข้อบังคับต่างๆ ส่งผลต่อการแข่งขัน
5. บริหารจัดการขาดการบูรณาการเชื่อมโยงการทำงานร่วมกัน ไม่สามารถการนำเทคโนโลยีดิจิทัลมาปรับใช้กับทุกส่วนขององค์กร (Digital Transformation) รองรับการการกำกับดูแลข้อมูลและการบริหารจัดการข้อมูลขนาดใหญ่ขององค์กร (Data Governance and Big Data Management) การกำกับดูแลข้อมูลและการบริหารจัดการข้อมูลขนาดใหญ่ขององค์กร (Data Governance and Big Data Management)

2.3.3 การวิเคราะห์และจัดทำกลยุทธ์ TOWS Matrix

ตารางแสดงการวิเคราะห์ TOWS Matrix ของสถาปัตยกรรมปัจจุบันของ บอท.

ปัจจัยแวดล้อมภายนอก	S : จุดแข็ง	W : จุดอ่อน
	S1.ความสามารถในการการพัฒนาเทคโนโลยีดิจิทัลแบบพึ่งตนเอง S2.มีประสบการณ์งานต่อเรือในระดับประเทศ S3.มีความสามารถในการปรับปรุงแบบเรือสำหรับดำเนินการ S4.ได้รับการสนับสนุนภาครัฐด้านเทคโนโลยีสารสนเทศ	W1. บุคลากรมีน้อยและขาดความชำนาญ W2.บุคลากรขาดความทุ่มเท การมีส่วนร่วม และการพัฒนาความรู้ทักษะอย่างต่อเนื่อง W3. การจัดสรรงบประมาณด้าน IT ยังไม่ชัดเจนในทุก ๆ ด้าน บอท. มีข้อจำกัดด้านการเงิน W4. การบูรณาการเชื่อมโยงข้อมูลและการดำเนินงานร่วมกันระหว่างหน่วยงาน (Government Integration) ไม่มีประสิทธิภาพ
O : โอกาส	**กลยุทธ์เชิงรุก**	**กลยุทธ์เชิงแก้ไข**
O1.บอท. อยู่ในความควบคุมของกองทัพเรือ มีโอกาสในการขอรับการสนับสนุน ด้านองค์บุคคล องค์วัตถุ และองค์ความรู้สมัยใหม่ด้านการซ่อมและสร้างเรือ O2.ภาครัฐมีนโยบายเพิ่มความแข็งแกร่งรัฐวิสาหกิจด้วยการปรับโครงสร้างการบริหารจัดการ พัฒนาประสิทธิภาพการดำเนินงานให้ได้มาตรฐานสากล ส่งเสริมความร่วมมือระหว่างภาครัฐ O3.การพัฒนาพื้นที่ยานนาวาเชิงพาณิชย์ จะส่งผลให้ บอท. มีสถานะทางการเงินที่ดีขึ้น ทั้งการจัดการค่าใช้จ่ายประจำ (Fixed cost)	S1,O1,O2 : ปรับปรุงเทคโนโลยีสารสนเทศขอสนับสนุนการอบรมความรู้ทักษะจากโครงการส่งเสริมบริหารจัดการภาครัฐ และปรับปรุงแอปพลิเคชันให้รองรับนโยบาย Thailand 4.0 S2,S3,S4,O3,O4 : จัดทำระบบการจัดการความรู้และนำมาพัฒนานวตกรรมเพื่อการทำงานอย่างมีประสิทธิภาพ	W1,W2,W4,O1,O2 : ขอรับการสนับสนุนด้านบุคลากรหรือระบบการบริหารจัดการจากหน่วยงานกำกับดูแล W3,O3,O4 : เร่งรัดโครงการพัฒนาที่ดินยานนาวาเพื่อเพิ่มรายได้และส่งเสริมโครงการการลงทุน

งบประมาณในการลงทุนเพื่อเสริมขีดความสามารถในทางธุรกิจ O4.การพัฒนาอู่เรือแห่งใหม่ เป็นโอกาสที่บริษัทฯ ได้มีโอกาสในการลงทุนเพื่อเสริมขีด ของบริษัทฯ รวมถึงการขยายธุรกิจในด้านอื่นๆ เพิ่มเติม		
T : อุปสรรค	**กลยุทธ์เชิงป้องกัน**	**กลยุทธ์เชิงรับ**
1. บุคลากรไม่มีทักษะและความสามารถโดยตรง ขาดความทุ่มเทในการปฏิบัติงานอย่างเต็มที่ ขาดประสิทธิภาพในการทำงาน หรือมีประสิทธิภาพไม่เพียงพอต่อการพัฒนา 2. บุคลากรในองค์กรขาดความรู้ความเข้าใจการใช้เทคโนโลยีสารสนเทศ ในการพัฒนาคุณภาพการทำงาน และการใช้ข้อมูลเพื่อการตัดสินใจ 3. ผลประกอบการเป็นตามสภาพเศรษฐกิจส่งผลต่อการลงทุน มีข้อจำกัดด้านการเงิน รายได้ไม่เพียงพอกับรายจ่าย 4. นโยบายภาครัฐและกฎระเบียบข้อบังคับต่างๆ ส่งผลต่อการแข่งขัน 5. การบริหารจัดการขาดการบูรณาการเชื่อมโยงการทำงานร่วมกัน ไม่สามารถการนำเทคโนโลยีดิจิทัลมาปรับใช้กับทุกส่วนขององค์กร	S1,T1 : พัฒนาทักษะความรู้ในด้านการพัฒนาแอปพลิเคชัน สนับสนุนการดำเนินงาน โดยพึ่งพาตนเองและให้เป็นไปตามกฎระเบียบข้อบังคับต่างๆ ตามมาตรฐานการทำงาน S1,T2 : พัฒนาทักษะความรู้ความสามารถในด้านเทคโนโลยีสารสนเทศให้แก่พนักงานทั้งองค์กร	W1,W2,T1,T2 : กำหนดให้มีการจัดอบรมความรู้ด้านเทคโนโลยีสารสนเทศอย่างต่อเนื่อง W3,T3 : บริหารจัดการลดต้นทุนในด้านต่าง ๆ โดยรวม เช่น ต้นทุนซ่อมสร้าง หรือการจัดซื้อจัดจ้างที่ไม่จำเป็น W4,T4,T5 : สื่อสารสถาปัตยกรรมองค์กร เพื่อการทำงานร่วมกันอย่างเป็นระบบ

2.3.4 การบริหารจัดการความเสี่ยง (risk management) ด้านการพัฒนาเทคโนโลยีสารสนเทศ

ความเสี่ยงด้านเทคโนโลยีสารสนเทศ (Information Technology Risk) คือ ความเป็นไปได้ที่จะเกิดเหตุการณ์ที่คาดหวังหรือไม่คาดหวัง อันเนื่องมาจากการนำเทคโนโลยีสารสนเทศมาใช้ หรือมีการเปลี่ยนแปลงเทคโนโลยีหรือนวัตกรรมต่าง ๆ อย่างเฉียบพลัน (Disruptive Technology / Disruptive Innovation) เช่น Internet of Things (IoT), Blockchain, Big Data เป็นต้น ซึ่งมีผลกระทบถึงระบบงานและการปฏิบัติงาน ทั้งนี้ ความเสี่ยงด้านเทคโนโลยีสารสนเทศ จะมีองค์ประกอบที่สำคัญ ๓ ประการ ได้แก่ แผนงานการใช้เทคโนโลยี สารสนเทศ การตัดสินใจในการนำเทคโนโลยีสารสนเทศมาใช้ และการวัดผลและติดตามความเสี่ยงที่อาจเกิดขึ้น โดยอาจเกี่ยวข้องกับกระบวนการปฏิบัติงานภายใน ระบบงาน เหตุการณ์ภายนอก หรือคน (เจ้าหน้าที่ บุคคลภายนอก หรือลูกค้า) ซึ่งส่งผลกระทบต่อการดำเนินงานของ บอท.

2.3.4.1 ประเภทของความเสี่ยงด้านเทคโนโลยีสารสนเทศ (Type of Risk)

ค่าระดับความเสี่ยง	ระดับความเสี่ยง	ความหมาย
1	ต่ำ	ระดับความเสี่ยงที่องค์กรสามารถยอมรับได้โดยมีมาตรการควบคุมอยู่แล้วหรือไม่ก็ได้
2	ปานกลาง	ระดับความเสี่ยงที่องค์กรสามารถยอมรับได้โดยต้องมีมาตรการควบคุมหรือมีแผนการลดความ เสี่ยง เพื่อลดความเสี่ยงให้ไปอยู่ในระดับต่ าและป้องกันไม่ให้ความเสี่ยงเพิ่มขึ้น
3	สูง	ระดับความเสี่ยงที่องค์กรไม่สามารถยอมรับได้ และต้องจัดการลดความเสี่ยงให้ไปอยู่ใน ระดับต่ าลงโดยเร็ว โดยต้องจัดให้มีแผนการลดความเสี่ยงและป้องกันไม่ให้ความเสี่ยง กลับเพิ่มสูงขึ้นด้วย
4	สูงมาก	ระดับความเสี่ยงที่องค์กรไม่สามารถยอมรับได้ และต้องจัดการลดความเสี่ยงให้ไปอยู่ใน ระดับต่ าลงในทันที หรืออาจมีการถ่ายโอนความเสี่ยง โดยต้องจัดให้มีแผนการลดความ เสี่ยงและป้องกันไม่ให้ความเสี่ยงกลับเพิ่มสูงขึ้นด้วย

โอกาสในการเกิด	ระดับความเสี่ยง	โอกาสที่จะเกิด
1	ต่ำ	แทบจะไม่เกิดหรืออย่างมากปีละ 1 ครั้ง
2	ต่ำ	โอกาสเกิดน้อยหรืออย่างมากไม่เกินปีละ 2 ครั้ง
3	ปานกลาง	ปานกลาง ปีละ 3-5 ครั้ง
4	สูง	ค่อนข้างบ่อย ปีละ 6-10 ครั้ง
5	สูงมาก	เกิดเป็นประจ า อย่างน้อยเดือนละ 1 ครั้ง

ตารางประเมินความเสี่ยง

ด้านการพัฒนาดิจิทัล

ประเภทความเสี่ยง	ภัยคุกคาม	ช่องโหว่	โอกาสในการเกิดความเสี่ยง	ระดับความเสี่ยง
1.ความเสี่ยงด้านข้อมูล (Information Risk)	เมื่อเกิดเหตุกับ Server ขององค์กรซึ่งเป็นพื้นที่จัดเก็บข้อมูลทั้งหมด	องค์กรไม่มีแหล่งจัดเก็บภายนอก	1	ปานกลาง
2.ความเสี่ยงด้านอุปกรณ์เทคโนโลยีสารสนเทศ (Hardware Risk)	เมื่อเกิดการชำรุดเสียหายของอุปกรณ์จาก อายุการใช้งานหรือลักษณะการใช้งานที่ไม่ถูกต้องหรือภัยจากภายนอก	องค์กรขาดแนวทางในการบริหารจัดการทรัพย์สินที่ดี	5	ต่ำ
3.ความเสี่ยงด้านโปรแกรมคอมพิวเตอร์ (Software Risk)	ผู้ใช้สามารถลงโปรแกรมใช้งานเองได้ ทำให้เกิดปัญหาผิด พรบ.คอมพิวเตอร์	องค์กรขาดระบบป้องกัน	2	ต่ำ
4.ความเสี่ยงด้านบุคลากร (People Risk)	ผู้ใช้ขาดความรู้ ทักษะในการใช้ระบบสารสนเทศในองค์กร	องค์กรขาดการอบรมการใช้ระบบสารสนเทศในองค์กร	5	สูง
5.ความเสี่ยงด้านกายภาพและสิ่งแวดล้อม (Physical and Environment Risk)	เหตุการณ์หรือสถานการณ์ที่เป็นภัยพิบัติต่าง ๆ เช่น ไฟไหม น้ำท่วม เป็นต้น	องค์กรไม่มีบริหารจัดการ BCP อย่างเป็นระบบ	1	ต่ำ

6.ความเสี่ยงด้านเครือข่ายสื่อสาร (Network Communication Risk)	ผู้ใช้ไม่สามารถเข้าถึงอินเตอร์เนทหรือระบบ Data Center ภายใน	ผู้ให้บริการไม่สามารถดำเนินการแก้ไขได้ทันท่วงที	3	ปานกลาง
7.ความเสี่ยงจากการว่าจ้างหรือจัดจ้างผู้ให้บริการภายนอก	องค์กรไม่สามารถพัฒนาระบบงานได้เอง	ผู้ให้บริการไม่สามารถดำเนินการแก้ไขได้ทันท่วงที	1	สูง
8.ความเสี่ยงด้านกระบวนการทำงาน (Business Process Risk)	ขาดความรู้ความเข้าใจในการทำงาน	องค์กรขาดการอบรมการใช้ระบบสารสนเทศในองค์กร	3	สูง

2.3.4.2 การตอบสนองความเสี่ยง (Risk Response)

ในการควบคุมและบรรเทาความเสี่ยง จะขึ้นอยู่กับค่าระดับความเสี่ยงที่ประเมินและได้ค่ามานั้น ทางเลือก ในการควบคุมหรือบรรเทาความเสี่ยงจะมีด้วยกัน ๔ ทางเลือก ดังนี้

2.3.4.2.1 การยอมรับความเสี่ยง (Acceptance) กรณีที่ค่าระดับความเสี่ยงอยู่ในบริเวณสีเขียว ผู้ประเมินความเสี่ยงสามารถยอมรับความเสี่ยงได้ กรณีการยอมรับความเสี่ยงยังหมายรวมถึง กรณีที่ค่าความเสี่ยงตกอยู่ในบริเวณโซนสีเหลือง สีส้ม หรือ สีแดง ก็ตาม แต่หน่วยงานหรือ สำนักงานยังไม่สามารถระบุมาตรการที่เหมาะสมได้ จึงอาจต้องยอมรับความเสี่ยงไว้ก่อน ใน ภายหลังเมื่อได้มาตรการที่เหมาะสมแล้ว จึงเสนอมาตรการเพื่อหาทางลดความเสี่ยงให้ลดลง มาอยู่ในระดับสีเขียว เป็นต้น - กรณีที่ค่าความเสี่ยงตกอยู ่ในบริเวณโซนสีเหลือง สีส้ม หรือ สีแดง แต่หน่วยงานหรือสำนักงาน พบว่าการจะจัดการกับความเสี่ยงนี้จะมีค่าใช้จ่ายที่ค่อนข้างสูงและไม่คุ้มค่าที่จะลงทุน จึงเห็นสมควรให้ยอมรับความเสี่ยงและไม่ดำเนินการใด ๆ ในทั้งสองกรณีนี้หน่วยงานหรือสำนักงานจ าเป็นจะต้องรายงานให้คณะกรรมการ บอท. ได้รับทราบด้วย

2.3.4.2.2 การเลี่ยงความเสี่ยง (Avoidance) คือ การหาหนทางที่เหมาะสมเพื่อหลีกเลี่ยงความเสี่ยงที่พบ นั้น เช่น หากพบว่าการนำทรัพย์สินไปตั้งไว้ในบริเวณที่มีความเสี่ยงต่อการสูญหาย ก็ควรจะหลีกเลี่ยงโดยการนำไป จัดเก็บไว้ในสถานที่ที่ปลอดภัย การตัดสินใจที่จะแลกเปลี่ยนข้อมูลสำคัญกับองค์กรหนึ่งผ่านทางระบบออนไลน์ เมื่อพบว่าองค์กร นั้นยังไม่มีมาตรการความมั่นคงปลอดภัยที่ดีเพียงพอ ก็อาจยับยั้งการตัดสินใจนั้น โดยหลีกเลี่ยงความเสี่ยงไปใช้วิธีการแลกเปลี่ยนแบบ Manual แทน การหาหนทางที่เหมาะสมกว่า ควรพิจารณาว่าความเสี่ยงลดลงมาอยู่ในระดับที่ยอมรับได้หรือไม่ เช่น ตกอยู่ในบริเวณสีเขียวหรือไม่

2.3.4.2.3 การโอนย้ายความเสี่ยง (Transfer) คือ การให้หน่วยงานอื่นเป็นผู้รับความเสี่ยงหรือดำเนินการ แทน บอท. เช่น ควรพิจารณาว่า ผู้ดำเนินการสามารถจัดการความเสี่ยงนั้นได้เป็นอย่างดี หรือไม่ ระดับความเสี่ยงที่เกิดจากผู้ดำเนินการแทน ควรจะอยู่ในระดับที่ บอท. ยอมรับได้ หากผู้ดำเนินการแทนไม่ สามารถทำได้ดี ความเสี่ยงจะตกกลับมาที่ บอท. เอง

2.3.4.2.4 การลดความเสี่ยง (Reduction) คือ การหาทางลดค่าความเสี่ยงที่อาจตกอยู่ในบริเวณสีเหลือง สีส้ม หรือ สีแดงก็ตาม ให้ลงมาอยู่ในระดับที่น้อยลง กรณีที่หน่วยงานหรือฝ่ายสามารถลดความเสี่ยงลงมาอยู่ในบริเวณสีเขียวได้ หน่วยงานสามารถ ยอมรับความเสี่ยงได้ และไม่ต้องทำอะไรเพิ่มเติม แต่หากอยู่ในบริเวณสีเหลือง หน่วยงานยังต้องคอยคุมความเสี่ยง ไว้ (เพื่อป้องกันการเลื่อนระดับไปสู่ระดับที่สูงขึ้น) เมื่อมีการประเมินระดับความเสี่ยงในหัวข้อที่แล้ว หน่วยงานหรือฝ่ายต้องพิจารณาค่าระดับความ เสี่ยงนั้นและตัดสินใจว่าจะใช้ทางเลือกใด เพื่อจัดการกับความเสี่ยงที่ประเมินนั้น

2.3.4.3 กิจกรรมการควบคุม (Control Activities)

ควบคุมดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศ โดยจะควบคุมความเสี่ยง ให้สอดคล้องกับระดับความเสี่ยงองค์กร ที่ได้รับอนุมัติ และดำเนินการควบคุมป้องกันความเสี่ยงด้านเทคโนโลยีสารสนเทศ ให้อยู่ในระดับความเสี่ยงที่ยอมรับ ได้ รวมถึงมีการติดตามและรายงานต่อคณะกรรมการ ผ่านคณะอนุกรรมการต่อไป

2.3.4.4 การรายงานความเสี่ยง (Risk Reporting)

จัดทำรายงานการประเมินการควบคุมความเสี่ยงด้วยตนเอง (Risk and Control Self-Assessment หรือ RCSA) อย่างน้อยปีละ ๑ ครั้ง โดยจุดที่มีความเสี่ยงอยู่ในระดับที่มีนัยสำคัญและ ระดับสูง จะต้องมีการจัดทำ Action Plan เพื่อปิดความเสี่ยงที่เกิดขึ้นกับหน่วยงานต่อไป ดังรายละเอียดต่อไปนี้คือ

2.3.4.4.1 ความเสี่ยงด้านข้อมูล (Information Risk) หมายถึง ความเสี่ยงที่เกิดจากข้อมูลต่าง ๆ ในระบบเทคโนโลยีสารสนเทศ ไม่ถูกต้องครบถ้วนของข้อมูล (Integrity Risk) ซึ่งอาจเกิดจากการถูกแก้ไขเปลี่ยนแปลง โดยบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้อง หรือมีการบันทึกข้อมูล การประเมินผล และการแสดงผลที่ผิดพลาดโดย อาจมีสาเหตุมาจากการที่หน่วยงานไม่ได้ควบคุมเกี่ยวกับการเข้าถึงข้อมูลของระบบคอมพิวเตอร์ โดยบุคคลที่ ไม่มีอำนาจหน้าที่ที่เกี่ยวข้องที่รอบคอบและรัดกุมเพียงพอ (Access risk) ทำให้ข้อมูลที่จัดเก็บรั่วไหล อาจทำให้ เกิดการฟ้องร้องได้ หรือมีความเสี่ยงเกี่ยวกับการที่ไม่สามารถใช้ข้อมูล (Availability Risk) หรือระบบคอมพิวเตอร์ ได้อย่างต่อเนื่องหรือในเวลาที่ต้องการ ซึ่งอาจทำให้การปฏิบัติงานหยุดชะงักได้ โดยความเสี่ยงนี้อาจเกิดจากไม่มี การควบคุมดูแลการ

ทำงานของระบบคอมพิวเตอร์และป้องกันความเสียหายอย่างเพียงพอ ยังรวมไปถึงความเสี่ยง เกี่ยวกับการสำรองข้อมูล โดยวัตถุประสงค์ของการสำรองข้อมูล (Back Up) ที่สำคัญคือ เพื่อไม่ให้ข้อมูล เกิดการสูญหาย ตลอดจนเป็นแนวทางในการปฏิบัติในการบริหารจัดการในการเก็บข้อมูลสำรอง การกู้คืนข้อมูล (Information Recovery) ซึ่งเป็นส่วนหนึ่งของแผนบริหารความต่อเนื่อง (Business Continuity Plan) และแผนกู้คืนข้อมูล (Disaster Recovery Plan)

2.3.4.4.2 ความเสี่ยงด้านอุปกรณ์เทคโนโลยีสารสนเทศ (Hardware Risk) หมายถึง ความเสี่ยงที่เกิดจากความผิดพลาดของอุปกรณ์ การเคลื่อนย้ายตัวเครื่องอุปกรณ์การติดตั้งอุปกรณ์ในพื้นที่ไม่เหมาะสม ความเสี่ยงใน เรื่องของการจัดหาอุปกรณ์เทคโนโลยีสารสนเทศที่เหมาะสมกับลักษณะของงาน และขององค์กร ที่ต้องมีการจัดหา เครื่องคอมพิวเตอร์และอุปกรณ์ต่าง ๆ ให้ได้ตามมาตรฐานของอุปกรณ์คอมพิวเตอร์ จัดหาและติดตั้งอุปกรณ์ เทคโนโลยีสารสนเทศ (Acquisition and Implementation) ให้เหมาะสมตามลักษณะของโครงการ และเหมาะสมกับงบประมาณ หรือความเสี่ยงในเรื่องการบำรุงรักษาอุปกรณ์เทคโนโลยีสารสนเทศ ความเสี่ยงจาก การที่อุปกรณ์เทคโนโลยีสารสนเทศหมดอายุไปเอง ความเสี่ยงจากการไม่ได้กำหนดหรือกำหนดกระบวนการอนุมัติ ใช้อุปกรณ์เทคโนโลยีสารสนเทศไม่ชัดเจน

2.3.4.4.3 ความเสี่ยงด้านโปรแกรมคอมพิวเตอร์ (Software Risk) หมายถึงความเสี่ยงที่เกิดจาก การเลือกใช้หรือความเสี่ยงจากการทำงานของโปรแกรมต่าง ๆ เช่น การใช้โปรแกรมที่ไม่มีลิขสิทธิ์ถูกต้อง การถูกผู้ ไม่หวังดีทำลายระบบ (Hacker) การควบคุมการ Reversion software ไม่เพียงพอ การที่ Software ที่ใช้อยู่ Out of date ความเสี่ยงที่เกิดจากการเลือกใช้ Software platforms ความเสี่ยงที่เกิดจากควบคุม การเปลี่ยนแปลง (Change control) ไม่เหมาะสมเพียงพอ ความเสี่ยงที่ไม่ได้กำหนดขั้นตอนการอนุมัติการใช้งาน Software การไม่ได้จัดทำขั้นตอนการปฏิบัติงานที่เป็นลายลักษณ์อักษร (Document operating procedures) ความเสี่ยงจากการไม่แยกระบบสำหรับการพัฒนา ทดสอบ และการให้บริการออกจากกัน (Separation of development, test and operation facilities) เป็นต้น

2.3.4.4.4 ความเสี่ยงด้านบุคลากร (People Risk) หมายถึง ความเสี่ยงที่เกิดจากบุคลากรที่เกี่ยวข้องกับการดำเนินงานด้านเทคโนโลยีสารสนเทศ ในเรื่องของการกำหนดโครงสร้าง การมอบหมายงานในหน้าที่ให้แก่ บุคลากรด้านเทคโนโลยีสารสนเทศ ที่มีความเหมาะสม คือ มีความรู้ ประสบการณ์ ในระดับที่สามารถรับการ ถ่ายทอดเทคโนโลยีสารสนเทศ และสามารถถ่ายทอดความรู้นั้นให้แก่ผู้ใช้งานด้านเทคโนโลยีสารสนเทศได้อย่างมี ประสิทธิภาพ ทั้งนี้ ยังรวมถึงการที่ขาดแผนการฝึกอบรมด้านเทคโนโลยีสารสนเทศให้กับเจ้าหน้าที่ของ บอท. อย่าง ทั่วถึง ทั้งในส่วนของ

ผู้ดูแลระบบ (Administration) ผู้พัฒนาระบบ (Developer/Programmer) และผู้ใช้งาน ทั่วไป (User) อย่างสม่ำเสมอ

2.3.4.4.5 ความเสี่ยงด้านกายภาพและสิ่งแวดล้อม (Physical and Environment Risk) หมายถึง ความ เสี่ยงที่เกิดจากภัยคุกคามทั้งภัยจากธรรมชาติ และภัยที่มนุษย์ทำขึ้น เช่น วาตภัย อุทกภัย ฟ้าผ่า น้ำท่วม กระแสไฟฟ้าขัดข้อง เพลิงไหม้ การไม่มีระบบรักษาความปลอดภัยห้องคอมพิวเตอร์แม่ข่าย และการก่อการร้าย เป็นต้น

2.3.4.4.6 ความเสี่ยงด้านเครือข่ายสื่อสาร (Network Communication Risk) หมายถึง ความเสี่ยงที่ เกิดจากระบบเครือข่ายสื่อสารขัดข้อง ไม่มีระบบเครือข่ายสื่อสารสำรอง ความเสี่ยงที่เกิดจากไม่ได้กำหนด คุณสมบัติทางด้านความมั่นคงปลอดภัย ระดับการให้บริการ ข้อกำหนดในการบริหารจัดการสำหรับบริหาร เครือข่ายทั้งหมดที่องค์กรใช้บริการอยู่ และต้องกำหนดไว้ในข้อตกลงในการให้บริการเครือข่ายโดยที่บริการ เครือข่ายเหล่านี้อาจจะเป็นบริการเครือข่ายภายในขององค์กรเองหรือบริการที่ได้รับจากหน่วยงานภายนอก การบำรุงรักษาอุปกรณ์เครือข่ายสื่อสารไม่สม่ำเสมอ การไม่มีรายชื่อและข้อมูลสำหรับติดต่อหน่วยงานอื่นกรณีมี ความจำเป็น เช่น บมจ. ทศท คอร์เปอเรชั่น บมจ. กสท. โทรคมนาคม ผู้ให้บริการอินเตอร์เน็ต (Internet Service Provider) ความเสี่ยงที่ผู้ดูแลระบบไม่มีการกำหนดมาตรการเพื่อป้องกันภัยคุกคามต่าง ๆ ทางเครือข่าย และดูแล รักษาความมั่นคงปลอดภัยสำหรับระบบและแอปพลิเคชันที่ใช้งานเครือข่าย รวมทั้งที่ส่งผ่านทาง เครือข่าย เป็นต้น

2.3.4.4.7 ความเสี่ยงจากการว่าจ้างหรือจัดจ้างผู้ให้บริการภายนอก (Information Technology Outsourcing) หมายถึง ความเสี่ยงที่เกิดจากการดำเนินการว่าจ้างหรือจัดจ้างผู้ให้บริการภายนอกเพื่อจัดทำ โครงการด้านเทคโนโลยีสารสนเทศต่าง ๆ เช่น ผู้ให้บริการไม่สามารถดำเนินงานตามรายละเอียดของสัญญาที่ กำหนดไว้ เป็นต้น

บทที่ 3

ยุทธศาสตร์การพัฒนาเทคโนโลยีดิจิทัล ของ บอท.

3.1 ยุทธศาสตร์การพัฒนาเทคโนโลยีดิจิทัล ของ บอท.

ยุทธศาสตร์ที่ 1 พัฒนาโครงสร้างพื้นฐานดิจิทัลประสิทธิภาพสูงให้ครอบคลุมทั้งองค์กร สร้างความเชื่อมั่นในการใช้เทคโนโลยีดิจิทัล จะมุ่งเน้นการมีกฎหมาย กฎระเบียบกติกาและมาตรฐานที่มีประสิทธิภาพ

1.1 พนักงานทุกคนสามารถเข้าถึงและใช้ประโยชน์ได้แบบทุกที่ ทุกเวลา ผลักดันเกิดศูนย์กลาง การเชื่อมต่อและแลกเปลี่ยนข้อมูลขององค์กร จัดให้มีนโยบายและแผนบริหารจัดการโครงสร้างพื้นฐาน เพื่อให้เกิดการใช้ทรัพยากรอย่างมีประสิทธิภาพสูงสุด

1.2 ทันสมัย และสอดคล้องกับหลักเกณฑ์สากล เพื่ออำนวยความสะดวก ลดอุปสรรค เพิ่มประสิทธิภาพในการประกอบกิจกรรมและ ทำธุรกรรมออนไลน์ต่างๆ รวมถึงสร้างความมั่นคงปลอดภัย และความเชื่อมั่น ตลอดจนคุ้มครองสิทธิ์ให้แก่ผู้ใช้งานเทคโนโลยีดิจิทัลในทุกภาคส่วน

เป้าหมาย

1. มีระบบโครงสร้างพื้นฐานที่เหมาะสม เพียงพอ และมีประสิทธิภาพในการบริการ
2. มีการจัดการด้านความมั่นคงปลอดภัยสารสนเทศที่มีประสิทธิภาพและสอดคล้องตามมาตรฐานสากล
3. ปรับเปลี่ยนองค์กรเพื่อรองรับนโยบายรัฐบาลดิจิทัล

กลยุทธ์/แผนงานดำเนินงาน

1. การพัฒนาโครงสร้างพื้นฐานทางด้านเทคโนโลยีสารสนเทศ
2. การพัฒนาระบบการบริหารความมั่นคงปลอดภัยสารสนเทศ (Information Security Management)

ตัวชี้วัด

1. ประสิทธิภาพของระบบโครงสร้างพื้นฐานและความพร้อมใช้งาน
2. มีระบบการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีดิจิทัล จำนวนเหตุการณ์ด้านความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศที่ลดน้อยลง

3. มีการประกาศใช้นโยบาย มาตรการตามเกณฑ์มาตรฐานสากลทั่วไป

ยุทธศาสตร์ที่ 2 ขับเคลื่อนธุรกิจหลักด้วยระบบเทคโนโลยีสารสนเทศและดิจิทัล ผลักดันให้ใช้เทคโนโลยีดิจิทัลในการลดต้นทุน การซ่อมสร้างและการบริการ เพิ่มประสิทธิภาพในการดำเนินธุรกิจ ตลอดจนพัฒนาไปสู่การแข่งขันเชิงธุรกิจรูปแบบใหม่ในระยะยาว พัฒนาเทคโนโลยีดิจิทัลขององค์กร ให้มีความเข้มแข็งและสามารถแข่งขันเชิงนวัตกรรมได้ในอนาคต เพิ่มโอกาสทางการตลาดผ่านเทคโนโลยีดิจิทัล โดยดำเนินการร่วมกันระหว่างหน่วยงานจากทั้งภาครัฐและภาคเอกชน

เป้าหมาย

1. มีการพัฒนา Platform เพื่อสนับสนุนงานทั้งภายในและภายนอกองค์กร
2. มีการบูรณาการเชื่อมโยงระบบงานภายในองค์กร กำกับดูแลข้อมูลและการบริหารจัดการข้อมูลขนาดใหญ่ขององค์กร (Data Governance and Big Data Management)
3. มี Platform รองรับนวัตกรรมและการขยายธุรกิจเกี่ยวเนื่องตามสภาพเศรษฐกิจและสังคม รวมถึงปรับเปลี่ยนองค์กรเพื่อรองรับนโยบายรัฐบาลดิจิทัล
4. มีการพัฒนา Platform รองรับระบบการสื่อสารองค์กร เพื่อสนับสนุนผู้มีส่วนได้เสียทั้งภายในและภายนอกองค์กร เช่น การจัดทำ Website หรือ สื่อออนไลน์ที่แพร่หลาย
5. การเปิดเผยและการแลกเปลี่ยนข้อมูลระหว่างองค์กรตามเกณฑ์มาตรฐานและนโยบายภาครัฐ
6. การให้บริการของหน่วยงานและการมีส่วนร่วมของผู้มีส่วนได้เสีย

กลยุทธ์/แผนงานดำเนินงาน

1. การพัฒนา Platform ระบบสารสนเทศเพื่อสนับสนุนผู้บริหาร
2. การพัฒนา Platform ระบบสารสนเทศเพื่อสนับสนุนโครงการหลักของธุรกิจ
3. การพัฒนา Platform รองรับระบบการสื่อสารองค์กรสนับสนุนผู้มีส่วนได้เสียทั้งภายในและภายนอกองค์กร

ตัวชี้วัด

1. จำนวน Platform ที่พัฒนาขึ้นสนับสนุนผู้มีส่วนได้เสียทั้งภายนอกและภายในองค์กร
2. การวัดระดับความพึงพอใจของผู้รับบริการทั้งภายนอกและภายในองค์กร

3. การประเมินประสิทธิภาพและประสิทธิผลในการบริหารโครงการ

ยุทธศาสตร์ที่ 3 พัฒนากำลังคนให้พร้อมเข้าสู่ไทยแลนด์ 4.0 และสังคมดิจิทัล (ให้ความสำคัญกับการพัฒนากำลังคนทุกคนในองค์กรให้มีความรู้ทางด้านเทคโนโลยีดิจิทัล มีความสามารถในการสร้างสรรค์และใช้เทคโนโลยีดิจิทัลอย่างชาญฉลาดในการปฏิบัติงาน และการพัฒนาบุคลากรในสาขาเทคโนโลยีดิจิทัลโดยตรง ให้มีความรู้ความสามารถและความเชี่ยวชาญเฉพาะด้านในระดับมาตรฐานสากล)

เป้าหมาย

1. พัฒนาทักษะความรู้ด้านเทคโนโลยีดิจิทัลที่สอดคล้องตามมาตรฐานอาชีพ และถ่ายทอดความรู้ทั่วทั้งองค์กร

2. การนำเทคโนโลยีดิจิทัลมาปรับใช้กับทุกส่วนขององค์กร (Digital Transformation) การบูรณาการเชื่อมโยงข้อมูลและการดำเนินงานร่วมกันระหว่างหน่วยงาน (Government Integration)

4. การกำกับดูแลข้อมูลและการบริหารจัดการข้อมูลขนาดใหญ่ขององค์กร (Data Governance and Big Data Management)

5. การบริหารจัดการและตรวจสอบความมั่นคงปลอดภัยสารสนเทศ (Information Security Management) การบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ (Information Security Risk Management) ขององค์กร

6. การบริหารความต่อเนื่องทางธุรกิจและความพร้อมใช้ของระบบ (Business Continuity and Availability Management) การบริหารจัดการเหตุการณ์ผิดปกติ การร้องขอการบริการ และปัญหาด้านเทคโนโลยีสารสนเทศ

กลยุทธ์/แผนงานดำเนินงาน

1. การอบรมบุคลากรเพื่อพัฒนาทักษะความรู้ด้านเทคโนโลยีดิจิทัลที่สอดคล้องตามมาตรฐานอาชีพ

2. การอบรมบุคลากรในองค์กรด้านการใช้เทคโนโลยีสารสนเทศในองค์กรอย่างมีประสิทธิภาพ

ตัวชี้วัด

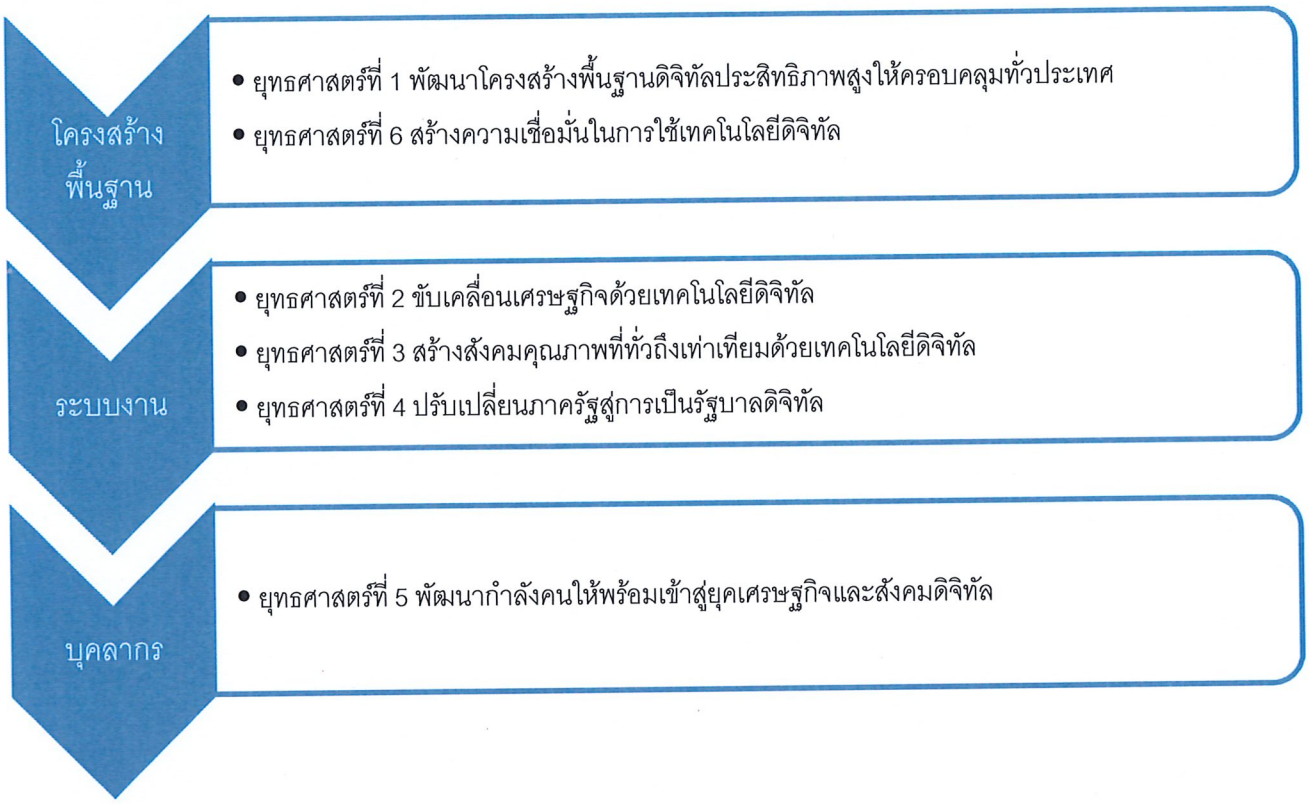
1. การอบรมภายนอก จำนวนหลักสูตรตามแผนปฏิบัติการประจำปี
2. การอบรมภายใน จำนวนบุคลากรที่เข้ารับการอบรมด้านเทคโนโลยีสารสนเทศ คิดเป็น 70% ของพนักงานทั้งหมด

3.2 ตารางความสัมพันธ์ยุทธศาสตร์ด้านการพัฒนาเทคโนโลยีดิจิทัล กับยุทธศาสตร์ต่างๆ

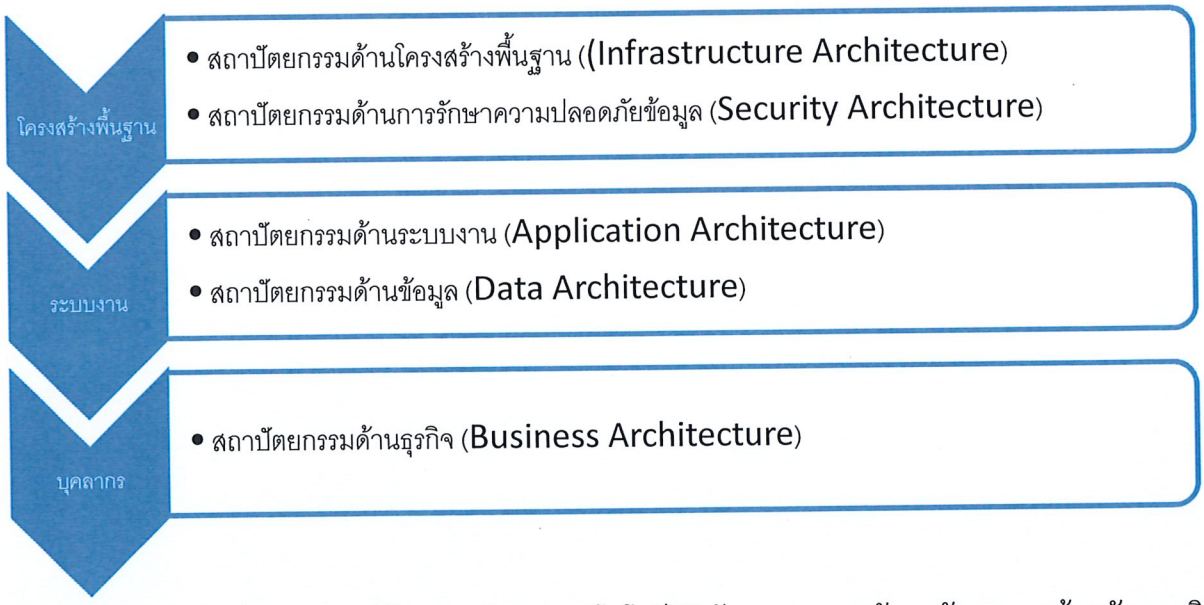
3.2.1 ตารางความสัมพันธ์ยุทธศาสตร์ด้านการพัฒนาเทคโนโลยีดิจิทัล กับแผนวิสาหกิจ ของ บอท. ปี 2568-2572

โครงสร้างพื้นฐาน	• ยุทธศาสตร์ที่ 5.2.1.1 แผนงานพัฒนาโครงสร้างพื้นฐานทางด้านเทคโนโลยีสารสนเทศ
ระบบงาน	• ยุทธศาสตร์ที่ 3.1 พัฒนาระบบสารสนเทศเพื่อสนับสนุนการตัดสินใจผู้บริหาร • ยุทธศาสตร์ที่ 3.2 พัฒนาระบบสารสนเทศเพื่อสนับสนุนการบริหารจัดการโครงการและผู้มีส่วนได้เสียทั้งภายในและภายนอกองค์กร
บุคลากร	• ยุทธศาสตร์ที่ 3.1 ปรับปรุงกระบวนการบริหารจัดการองค์กรให้เป็นไปตามมาตรฐานที่ สคร.กำหนด ทางด้านการพัฒนาเทคโนโลยีดิจิทัล • ยุทธศาสตร์ที่ 5.2.1.2 แผนงานนำเทคโนโลยีสารสนเทศและนวัตกรรมเข้ามาใช้

3.2.2 ตารางแสดงความสัมพันธ์ยุทธศาสตร์ด้านการพัฒนาเทคโนโลยีดิจิทัล ของ บอท.กับแผนพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคม ดังนี้คือ



3.2.3 ตารางแสดงความสัมพันธ์ยุทธศาสตร์ด้านการพัฒนาเทคโนโลยีดิจิทัล ของ บอท.กับสถาปัตยกรรมองค์กร (Enterprise Architecture) ของ บอท. ดังนี้คือ



ตารางแสดงความสัมพันธ์ยุทธศาสตร์ด้านการพัฒนาเทคโนโลยีดิจิทัล ของ บอท.กับระดับความพร้อมรัฐบาลดิจิทัล หน่วยงานภาครัฐ. ดังนี้คือ

โครงสร้างพื้นฐาน

- ตัวชี้วัดที่ 6 โครงสร้างพื้นฐานความมั่นคงปลอดภัยและมีประสิทธิภาพ (Secure and Efficient Infrastructure)

ระบบงาน

- ตัวชี้วัดที่ 2 กระบวนการพัฒนาด้วยข้อมูล (Data-driven Practices)
- ตัวชี้วัดที่ 4 บริการภาครัฐ (Public Services)
- ตัวชี้วัดที่ 5 การบริหารจัดการรูปแบบดิจิทัล (Smart Back Office)
- ตัวชี้วัดที่ 7 เทคโนโลยีดิจิทัลและการนำไปใช้ (Digital Technology Practices)

บุคลากร

- ตัวชี้วัดที่ 1 แนวนโยบายและหลักปฏิบัติ (Policies & Practices)
- ตัวชี้วัดที่ 3 ศักยภาพเจ้าหน้าที่ภาครัฐด้านดิจิทัล (Digital Capability)

บทที่ 4

แผนงาน / โครงการ ด้านเทคโนโลยีสารสนเทศ

การจัดทำแผนงานโครงการด้านเทคโนโลยีสารสนเทศแบ่งออกเป็น 3 ยุทธศาสตร์ โดยกำหนดแผนดำเนินเพื่อเป็นแนวทางการขับเคลื่อนองค์กรเข้าสู่ยุคดิจิทัลอย่างมีประสิทธิภาพและ

ยุทธศาสตร์	ตัวชี้วัด/แผนวิสาหกิจ	ปีงบประมาณ (ล้านบาท)					รวม
รวมงบประมาณทั้งหมด		0.91	6.99	2.1	2.0	2.10	14.10

ยุทธศาสตร์ที่ 1 พัฒนาโครงสร้างพื้นฐานทางด้านเทคโนโลยีสารสนเทศ

ยุทธศาสตร์ แผนงาน/โครงการ	ตัวชี้วัด/แผนวิสาหกิจ	ปีงบประมาณ (ล้านบาท)					รวม (ล้านบาท)
		69	70	71	72	73	
ยุทธศาสตร์ที่ 1 พัฒนาโครงสร้างพื้นฐานดิจิทัลและความปลอดภัย ประสิทธิภาพสูงให้ครอบคลุมทั้งองค์กร							
กลยุทธ์ 1.1 การพัฒนาโครงสร้างพื้นฐานทางด้านคอมพิวเตอร์และอุปกรณ์ต่อพ่วง	ความสำเร็จในการดำเนินการตามโครงการพัฒนาเทคโนโลยีองค์ความรู้และการเชื่อมต่อยุคสมัยใหม่ (1) แผนงานพัฒนาโครงสร้างพื้นฐานทางด้านเทคโนโลยีสารสนเทศ						
แผนงาน 1.1.1 จัดหาเครื่องแม่ข่าย		-	3	-	-	-	3.0
แผนงาน 1.1.2 จัดหาเครื่องสำรองไฟเครื่องแม่ข่าย		-	0.5	-	-	-	0.50
แผนงาน 1.1.3 จัดหาอุปกรณ์สำรองข้อมูล		-	0.10				0.1
แผนงาน 1.1.4 จัดหาเครื่องลูกข่าย		-	0.28	0.14	0.14	0.14	0.70
กลยุทธ์ 1.2 การพัฒนาโครงสร้างพื้นฐานระบบเครือข่าย และระบบประชุมออนไลน์							
แผนงาน 1.2.1 จัดหาอุปกรณ์ระบบเครือข่าย (Network) ภายในองค์กร		-	0.2	0.1	-	0.1	0.4
แผนงาน 1.2.2 จัดหาอุปกรณ์รองรับการประชุมออนไลน์		-	0.15	-	-	-	0.15
แผนงาน 1.2.3 เช่าใช้สัญญาณอินเตอร์เนทจาก ISP.		-	0.30	0.30	0.30	0.30	1.20
แผนงาน 1.2.4 ระบบกล้องวงจรปิด		-	0.5	-	-	-	0.5

กลยุทธ์ 1.3 การพัฒนาโครงสร้างพื้นฐานด้านระบบความปลอดภัยในองค์กร	(2) แผนงานนำเทคโนโลยีและนวัตกรรมเข้ามาใช้ เป้าหมายอย่างน้อย 1 โครงการ						
แผนงาน 1.3.1 จัดหาอุปกรณ์ Firewall และระบบการโจมตีทางไซเบอร์		0.30	0.30	0.30	0.30	0.30	1.50
แผนงาน 1.3.2 จัดหาระบบป้องกันไวรัส		0.20	0.20	0.20	0.20	0.20	1.00
รวมงบประมาณยุทธศาสตร์ที่ 1		0.76	5.79	1.30	1.20	1.30	10.35

ยุทธศาสตร์ที่ 2 พัฒนาระบบสารสนเทศเพื่อสนับสนุนการบริหารจัดการ

ยุทธศาสตร์ แผนงาน/โครงการ	ตัวชี้วัด/แผนวิสาหกิจ	ปีงบประมาณ (ล้านบาท)					รวม (ล้านบาท)
		69	70	71	72	73	
ยุทธศาสตร์ที่ 2.1 การพัฒนาระบบงานด้านเทคโนโลยีสารสนเทศและดิจิทัล							
แผนงาน 2.1.1 สนับสนุนเทคโนโลยีสารสนเทศ สำหรับผู้บริหาร	1 โครงการ	-	0.02	0.02	0.02	0.02	0.08
แผนงาน 2.1.2 สนับสนุนเทคโนโลยีสารสนเทศสำหรับผู้มีส่วนได้เสียภายในและภายนอกองค์กร เช่น ระบบอินทราเนท สนับสนุนหน่วยในองค์กร หรือ Website สนับสนุนภายนอกองค์กร	1 โครงการ	-	0.01	0.01	0.01	0.01	0.05
แผนงาน 2.1.3 สนับสนุนเทคโนโลยีสารสนเทศสำหรับนวัตกรรม	1 โครงการ	-	0.01	0.01	0.01	0.01	0.04
ยุทธศาสตร์ที่ 2.2 ระบบสนับสนุนงานด้านเทคโนโลยีสารสนเทศและดิจิทัล							
แผนงาน 2.2.1 ค่าจดโดเมน Bangkokdock.co.th ประจำปี	ต่ออายุการเช่ารายปี	0.01	0.01	0.01	0.01	0.01	0.05
แผนงาน 2.2.2 ค่าบริการ Line OA รายปี		0.02	0.02	0.02	0.02	0.02	0.10
แผนงาน 2.2.3 ค่าบริการ Canva รายปี		0.02	0.02	0.02	0.02	0.02	0.10
แผนงาน 2.3.4 จัดหา Platform รองรับงานสนับสนุนงานด้านเทคโนโลยีสารสนเทศ		0.04	0.04	0.04	0.04	0.04	0.20
รวมงบประมาณยุทธศาสตร์ที่ 2		0.05	1.10	0.7	0.7	0.7	3.25

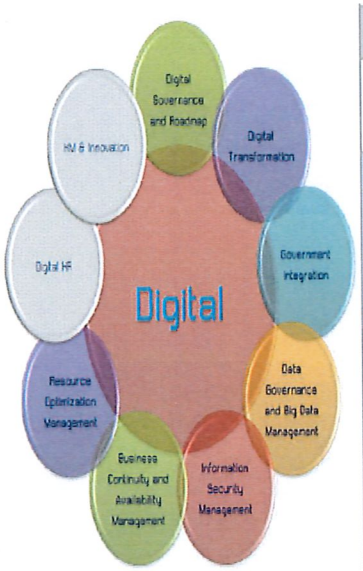
ยุทธศาสตร์ที่ 3 พัฒนากำลังคนให้พร้อมเข้าสู่ไทยแลนด์ 4.0 และสังคมดิจิทัล

ยุทธศาสตร์ แผนงาน/โครงการ	ตัวชี้วัด/แผนวิสาหกิจ	ปีงบประมาณ (ล้านบาท)					รวม (ล้านบาท)
		69	70	71	72	73	
ยุทธศาสตร์ที่ 3 พัฒนากำลังคนให้พร้อมเข้าสู่ไทยแลนด์ 4.0 และสังคมดิจิทัล							
กลยุทธ์ 3.1 การพัฒนาความรู้ความสามารถการพัฒนาระบบงานด้านเทคโนโลยีดิจิทัล	ร้อยละความสำเร็จในการดำเนินการตามโครงการพัฒนาองค์ความรู้ และขีดความสามารถของบุคลากร (1) โครงการพัฒนาองค์ความรู้และขีดความสามารถของบุคลากร						
แผนงาน 3.1.1 อบรมการบริหารจัดการระบบแม่ข่าย Server		0.02	0.02	0.02	0.02	0.02	0.1
แผนงาน 3.1.2 อบรมหลักสูตรการบริหารจัดการเครือข่าย (Network)		0.02	0.02	0.02	0.02	0.02	0.1
แผนงาน 3.1.3 อบรมหลักสูตรการบริหารความมั่นคงปลอดภัยของสารสนเทศ		0.02	0.02	0.02	0.02	0.02	0.1
แผนงาน 3.1.4 อบรมการพัฒนาระบบงานรองรับการพัฒนารัฐบาลดิจิทัล		0.1	0.1	0.1	0.1	0.1	0.5
กลยุทธ์ 3.2 การพัฒนาความรู้ความสามารถการใช้เทคโนโลยีดิจิทัล ของพนักงานในองค์กร							
แผนงาน 3.2.1 จัดอบรมการใช้งานระบบงานเทคโนโลยีสารสนเทศและดิจิทัลให้พนักงานทุกคนในองค์กร		0.1	0.1	0.1	0.1	0.1	0.5
รวมงบประมาณยุทธศาสตร์ที่ 3		0.76	5.79	1.30	1.20	1.30	10.35

บทที่ 5

การบริหารจัดการและการติดตามประเมินผลการบริหารจัดการสารสนเทศ

การวัดผลการดำเนินงานตามแผนปฏิบัติการดิจิทัลประสบความสำเร็จดังเป้าหมายที่ตั้งไว้หรือไม่นั้น ต้องมีการบริหารจัดการและระบบติดตามประเมินผลเพื่อใช้เป็นเครื่องมือในการบริหารแผนงานฯ และการประเมินผลอย่างมีประสิทธิภาพโดยอาศัยตัวชี้วัดความสำเร็จในหลายระดับ



ประเด็นพิจารณา	ประเด็นย่อย
1. การกำกับดูแลด้านเทคโนโลยีดิจิทัล และแผนปฏิบัติการดิจิทัลขององค์กร (Digital Governance and Roadmap)	1.1 กำหนดกรอบทิศทางการกำกับดูแลด้านการบริหารจัดการเทคโนโลยีดิจิทัล (Digital Governance) 1.2 แผนปฏิบัติการดิจิทัลระยะ 3- 5 ปี (Digital Roadmap)
2. การนำเทคโนโลยีดิจิทัลมาปรับใช้กับทุกส่วนขององค์กร (Digital Transformation)	2.1 การวิเคราะห์และจัดทำสถาปัตยกรรมองค์กร (Enterprise Architecture) 2.2 การบริหารโครงการและการดำเนินงานด้านเทคโนโลยีดิจิทัลอย่างมีประสิทธิภาพ (Project Management) 2.3 การจัดการด้านคุณภาพ (Quality Management)
3. การบูรณาการเชื่อมโยงข้อมูลและการดำเนินงานร่วมกันระหว่างหน่วยงาน (Government Integration)	3.1 การออกแบบความเชื่อมโยงและการทำงานร่วมกัน การบูรณาการเชื่อมโยงข้อมูลและการดำเนินงานร่วมกัน (Enterprise Collaboration and Interoperability Design & Data and System Integration)
4. การกำกับดูแลข้อมูลและการบริหารจัดการข้อมูลขนาดใหญ่ขององค์กร (Data Governance and Big Data Management)	4.1 การดำเนินการด้านการกำกับดูแลข้อมูลและการบริหารจัดการข้อมูลขนาดใหญ่ขององค์กร (Data Governance and Big Data Management Implementation)
5. การบริหารความมั่นคงปลอดภัยของสารสนเทศ (Information Security Management)	5.1 การบริหารจัดการความมั่นคงปลอดภัยสารสนเทศขององค์กร (Information Security Management) 5.2 การบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศขององค์กร (Information Security Risk Management) 5.3 การตรวจสอบการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศขององค์กร (ISMS Audit)
6. การบริหารความต่อเนื่องทางธุรกิจและความพร้อมใช้ของระบบ (Business Continuity and Availability Management)	6.1 การบริหารจัดการทรัพย์สินด้านเทคโนโลยีสารสนเทศ (IT Asset Management) 6.2 การบริหารจัดการคอนฟิกูเรชั่น (Configuration Management) 6.3 การบริหารจัดการเหตุการณ์ผิดปกติ การร้องขอการบริการ และปัญหาด้านเทคโนโลยีสารสนเทศ (IT Incident, Service Requests and Problem Management) 6.4 การบริหารจัดการความต่อเนื่องทางธุรกิจ (Business Continuity Management)
7. การดำเนินการด้านการบริหารจัดการการใช้ทรัพยากรอย่างเหมาะสม (Resource Optimization Management)	7.1 การดำเนินการด้านการบริหารจัดการการใช้ทรัพยากรอย่างเหมาะสม (Resource Optimization Management Implementation) 7.2 การบริหารจัดการการเลือกใช้เทคโนโลยีที่เป็นมิตรต่อสิ่งแวดล้อม (Green IT Management)

ระบบประเมินผลการดำเนินงานรัฐวิสาหกิจปรับปรุงใหม่ จะเริ่มใช้ประเมินในปี พ.ศ. 2563 โดยเปลี่ยนจากระบบเดิมที่ใช้ 2 ระบบ คือ ระบบประเมินคุณภาพรัฐวิสาหกิจ (SEPA) และระบบการบริหารจัดการองค์กร (ข้อ 3) เปลี่ยนเป็นระบบประเมินผลการดำเนินงานรัฐวิสาหกิจใหม่ ที่ประกอบด้วย Key

result และ Core Business Enablers 8 ด้าน ทาง บอท.จึงดำเนินการปรับปรุงแผนปฏิบัติการดิจิทัล เพื่อรองรับแนวทางระบบประเมินผลการดำเนินงานรัฐวิสาหกิจใหม่ ดังมีรายละเอียดดังนี้คือ

5.1 Digital Governance and Roadmap การกำกับดูแลด้านเทคโนโลยีดิจิทัล และแผนปฏิบัติการดิจิทัลขององค์กร ประเด็นพิจารณา

5.1.1 กำหนดกรอบทิศทางการกำกับดูแลด้านการบริหารจัดการเทคโนโลยีดิจิทัล

- กำหนดกรอบการกำกับดูแลด้านการบริหารจัดการทรัพยากรเทคโนโลยีสารสนเทศอย่างเหมาะสม (Benefits Delivery and Resource Optimization Framework Setting) เช่น การลงทุนด้าน IT ที่เหมาะสมคุณภาพในการปฏิบัติงานของระบบ IT
- กำหนดกรอบการกำกับดูแลด้านการดำเนินงานให้มีประสิทธิภาพและมีความโปร่งใส (Performance Measurement and Stakeholder Transparency Framework Setting) เช่น การปฏิบัติตาม กฎหมาย ระเบียบข้อบังคับ ที่เกี่ยวข้องกับระบบ IT
- การกำหนดกรอบการกำกับดูแลการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ (IT Risk Optimization Framework Setting) เช่น ความเสี่ยงด้าน IT ที่กระทบต่อองค์กร

5.1.2 แผนปฏิบัติการดิจิทัลระยะ 3- 5 ปี (Digital Roadmap)

5.1.3 แผนปฏิบัติการประจำปี (Action Plan)

5.2 Digital Transformation การนำเทคโนโลยีดิจิทัลมาปรับใช้กับทุกส่วนขององค์กร

การนำเทคโนโลยีดิจิทัลมาปรับใช้กับทุกส่วนขององค์กรมาปรับใช้กับทุกส่วนของธุรกิจ ทั้งในส่วนของกระบวนการทำงาน การสร้างสรรค์ผลิตภัณฑ์ การตลาด วัฒนธรรมองค์กร และการกำหนดเป้าหมายการเติบโตในอนาคต เพื่อให้เกิดประสิทธิภาพในการดำเนินธุรกิจและสามารถรองรับการเปลี่ยนแปลงได้อย่างรวดเร็ว รวมถึงในการสร้างธุรกิจใหม่ๆ รูปแบบบริการใหม่ๆ ให้เกิดขึ้น ตลอดจนการบริหารโครงการและการดำเนินงานด้านเทคโนโลยีดิจิทัลอย่างมีประสิทธิภาพ และมีการบริหารจัดการด้านคุณภาพของการนำเทคโนโลยีดิจิทัลมาใช้ ประเด็นพิจารณา

5.2.1การวิเคราะห์และจัดทำ Enterprise Architecture สถาปัตยกรรมองค์กร เพื่อมุ่งเน้นการนำเทคโนโลยีดิจิทัลมาปรับใช้กับทุกส่วนขององค์กรมาปรับใช้กับทุกส่วนของธุรกิจ ทั้งในส่วนของกระบวนการทำงาน การสร้างสรรค์ผลิตภัณฑ์ การตลาด วัฒนธรรมองค์กร และการกำหนดเป้าหมายการเติบโตในอนาคต เช่น Business Architecture/ Information Architecture/ Application Architecture/ Technology/Infrastructure/ Architecture Security Architecture

5.2.2 การบริหารโครงการและการดำเนินงานด้านเทคโนโลยีดิจิทัลอย่างมีประสิทธิภาพ และ

มี

การบริหารจัดการด้านคุณภาพของการนำเทคโนโลยีดิจิทัลมาใช้ เช่น Project Management การบริหารจัดการโครงการ

- การบริหารจัดการแผนงานและโครงการ (Programmes and Projects)
- การบริหารจัดการข้อกำหนดและความต้องการ (Requirements Definition)
- การบริหารจัดการการระบุและการจัดสร้างกระบวนการแก้ปัญหาแบบเบ็ดเสร็จ (Solutions Identification and Build)
- การบริหารจัดการเพื่อให้การเปลี่ยนแปลงองค์กรสัมฤทธิ์ผล (Organizational Change Enablement)
- การบริหารจัดการการเปลี่ยนแปลง (Changes)
- การบริหารจัดการการยอมรับการเปลี่ยนแปลงและการปรับเปลี่ยน (Change Acceptance and Transitioning)

5.2.3 การจัดการด้านคุณภาพ (Quality Management)

- การสร้างระบบบริหารคุณภาพ (Quality Management System)
- การบริหารจัดการกระบวนการ Computer Audit

5.3 Government Integration การบูรณาการเชื่อมโยงข้อมูลและดำเนินงานร่วมกันระหว่างหน่วยงาน

การบูรณาการเชื่อมโยงข้อมูล และการดำเนินงานร่วมกันระหว่างหน่วยงานต่างๆ ทั้งการเชื่อมโยง

ข้อมูลและการดำเนินงาน เพื่อสามารถเห็นข้อมูลประชาชนเป็นภาพเดียวที่สมบูรณ์ เกิดใช้บริการทางเทคโนโลยีร่วมกัน รวมถึงการให้บริการภาครัฐแบบครบวงจร ณ จุดเดียว ประเด็นพิจารณา

i. Enterprise Collaboration and Interoperability Design การออกแบบความเชื่อมโยง

การนำข้อมูลและการดำเนินการทั้งหมดที่ได้ออกแบบกิจกรรม กระบวนการ ทรัพยากร ให้มีความชัดเจนเกี่ยวกับการเชื่อมโยง และการทำงานร่วมกัน ทั้งระบบสารสนเทศ โครงสร้างสถาปัตยกรรม กระบวนการข้อมูล และตารางวัดผล โดยเป็นการเชื่อมโยงกับกระบวนการต่างๆ

5.3.2 Data and System Integration การบูรณาการเชื่อมโยงข้อมูลและการดำเนินงานร่วมกัน

b. Data Governance and Big Data Management ธรรมภิบาลข้อมูลและ การบริหารจัดการ

ข้อมูล ขนาดใหญ่ขององค์กรการกำหนดสิทธิ หน้าที่ และความรับผิดชอบของผู้มีส่วนได้ส่วนเสียในการบริหารจัดการข้อมูลทุกขั้นตอน เพื่อให้การได้มาและการนำไปใช้ข้อมูลของหน่วยงาน ได้ถูกต้อง ครบถ้วน เป็นปัจจุบัน และสามารถเชื่อมโยงกันได้อย่างมีประสิทธิภาพและมั่นคงปลอดภัย โดยใช้ข้อมูลเป็นหลักในการขับเคลื่อนองค์กร เช่น การใช้ข้อมูลในการวิเคราะห์การตัดสินใจเชิงนโยบาย และการบริหารจัดการองค์กร การเพิ่มประสิทธิภาพในการบริการประชาชน การเสริมสร้างและผลักดันธุรกิจที่เกิดจากการใช้นวัตกรรมข้อมูลประเด็นพิจารณา การดำเนินการด้านการกำกับดูแลข้อมูลและการบริหารจัดการข้อมูลขนาดใหญ่ขององค์กร (Data Governance and Big Data Management Implementation)

- กระบวนการกำกับดูแลข้อมูล
- โครงสร้างการกำกับดูแลข้อมูล
- นโยบายข้อมูลและการตรวจสอบ
- การวัดประสิทธิภาพกระบวนการและคุณภาพข้อมูล
- การวัดความคุ้มทุนและการปรับปรุงอย่างต่อเนื่อง

การกำหนดข้อมูลและสารสนเทศที่สำคัญขององค์กร รวมถึงการกำหนดสิทธิ หน้าที่ และความรับผิดชอบของผู้มีส่วนได้ส่วนเสียในการบริหารจัดการข้อมูลทุกขั้นตอน เพื่อให้การได้มาและการนำไปใช้ข้อมูลของหน่วยงาน ได้ถูกต้อง แม่นยำ ครบถ้วน เป็นปัจจุบัน และใช้งานง่าย

5.5 Information Security Management การบริหารความมั่นคงปลอดภัยของสารสนเทศ

กระบวนการหรือการกระทาทั้งหมดที่จาเป็น เพื่อทำให้องค์กรปราศจากความเสี่ยง และความเสียหายที่มีผลต่อความปลอดภัยของข้อมูล และสารสนเทศ (Data and Information) ในทุกรูปแบบ รวมถึงการระวังป้องกันต่อการอาชญากรรม การโจมตี การบ่อนทาลาย การจารกรรม และความผิดพลาดต่างๆ โดยคำนึงถึงองค์ประกอบพื้นฐานของความปลอดภัยของข้อมูล ได้แก่ การรักษาความลับของข้อมูล (Confidentiality) การรักษาความคงสภาพของข้อมูลหรือความสมบูรณ์ของข้อมูล (Integrity) และความพร้อมใช้งานของข้อมูล (Availability) ประเด็นพิจารณา

i. Information Security Management System การกำหนดแนวทางมาตรฐานของการบริหารความมั่นคงปลอดภัยของสารสนเทศ

- ความมั่นคงปลอดภัยทางกายภาย (Physical Security)
- ความมั่นคงปลอดภัยส่วนบุคคล (Personal Security)
- ความมั่นคงปลอดภัยในการปฏิบัติงาน (Operations Security)
- ความมั่นคงปลอดภัยในการติดต่อสื่อสาร (Communication Security)
- ความมั่นคงปลอดภัยของเครือข่าย (Network Security)
- ความมั่นคงปลอดภัยของสารสนเทศ (Information Security)

ii. Measurement for Information Security Management การวัดประสิทธิผล ของการบริหารความมั่นคงปลอดภัยของสารสนเทศ

b. Business Continuity and Availability Management การบริหารความต่อเนื่องทางธุรกิจและความพร้อมใช้ของระบบ

กระบวนการที่ทาให้ธุรกิจสามารถดาเนินการได้อย่างต่อเนื่อง และการบริหารจัดการความเสี่ยงเมื่อเกิดเหตุการณ์ฉุกเฉินอันอาจมีผลกระทบต่อการให้บริการหรือผลิตภัณฑ์ที่สำคัญ เพื่อเป็นการสร้างเสถียรภาพและความมั่นคงปลอดภัยเพื่อพร้อมรองรับการปฏิบัติงานได้อย่างต่อเนื่องและมีประสิทธิภาพ เตรียมพร้อมรับมือกับเหตุการณ์ฉุกเฉินหรือสถานการณ์ผิดปกติ โดยที่มีการจัดทาแผนตอบสนองกับสถานการณ์ภัยพิบัติ (Incident Management Plan) และแผนกอบกู้สถานการณ์ภัยพิบัติ (Business Continuity Plan) เพื่อการดำเนินธุรกิจอย่างต่อเนื่องและมีประสิทธิภาพ รวมถึงการบริหารจัดการความพร้อมใช้ของระบบต่างๆ ตามความต้องการของผู้ใช้บริการเพื่อให้ผู้ใช้บริการเกิดความมั่นใจในการบริการ

ประเด็นพิจารณา

5.6.1 การบริหารจัดการทรัพย์สินด้านเทคโนโลยีสารสนเทศ (IT Asset Management)

5.6.2 การบริหารจัดการคอนฟิกูเรชั่น (Configuration Management)

5.6.3 การบริหารจัดการเหตุการณ์ผิดปกติ (IT Incident) การร้องขอการบริการ (Service Requests) และปัญหาด้านเทคโนโลยีสารสนเทศ (Problem Management)

5.6.4 การบริหารจัดการความต่อเนื่องทางธุรกิจ (Business Continuity Management)

5.7. Resource Optimization Management การบริหารจัดการการใช้ทรัพยากรอย่างเหมาะสม

กระบวนการบริหารจัดการการใช้ทรัพยากรด้านเทคโนโลยีดิจิทัล ทั้งในส่วนของ บุคลากร กระบวนการ และเทคโนโลยี เพื่อสนับสนุนวัตถุประสงค์ขององค์กรอย่างมีประสิทธิภาพด้วยต้นทุนที่เหมาะสม และมีความพร้อมต่อการเปลี่ยนแปลงในอนาคต รวมถึงการบริหารจัดการการเลือกใช้เทคโนโลยีที่เป็นมิตรต่อสิ่งแวดล้อม เพื่อเพิ่มประสิทธิภาพในการจัดการการใช้พลังงาน ลดการใช้พลังงาน ลดการปล่อยก๊าซเรือนกระจก ลดการสร้างขยะ รวมถึงการนำขยะอิเลคทรอนิคส์มารีไซเคิล ประเด็นพิจารณา

5.7.1 Resource Optimization Management Implementation การดำเนินการด้านการบริหารจัดการการใช้ทรัพยากรอย่างเหมาะสม

- Resource Efficiency
- Process Accountability
- Product Effectiveness 7.2 Green IT Management การบริหารจัดการการเลือกใช้

เทคโนโลยีที่เป็นมิตรต่อสิ่งแวดล้อม

- Green IT Implementation
- Paperless Organization องค์กรไร้กระดาษ

5.8 Digital HR เกณฑ์ HCM

5.9 Knowledge Management & Learning Organization and Innovation & Technology เกณฑ์ Knowledge Management & Innovation Manageme

บทที่ 1 บททั่วไป

1.1 ความเป็นมา

บริษัท อู่กรุงเทพ จำกัด เป็นรัฐวิสาหกิจ ในความควบคุมของกองทัพเรือ สังกัดกระทรวงกลาโหม จัดเป็นรัฐวิสาหกิจประเภทนโยบายพิเศษของรัฐประเภทยุทธปัจจัย ประกอบกิจการอุตสาหกรรมอู่เรือ และอุตสาหกรรมต่อเนื่องกับกิจการพาณิชยนาวี และเป็นอุตสาหกรรมพื้นฐานในการพัฒนาอุตสาหกรรมต่อเนื่องหลายประเภท ซึ่งอุตสาหกรรมอู่เรือภายในประเทศเป็นส่วนประกอบที่สำคัญของสมุทานุภาพ เป็นอุตสาหกรรมที่ก่อให้เกิดการจ้างแรงงานฝีมือจำนวนมาก เป็นอุตสาหกรรมที่สนับสนุนและส่งเสริมการขนส่งทางทะเล การค้าระหว่างประเทศส่งเสริมอุตสาหกรรมปิโตรเคมีและอุตสาหกรรมเหล็ก และประการที่สำคัญที่สุดคือ เป็นอุตสาหกรรมที่ทำให้เกิดความมั่นคงทางการทหารและเพิ่มศักย์สงครามให้แก่ประเทศ

บริษัท อู่กรุงเทพ จำกัด (สำนักงานใหญ่) ตั้งอยู่ริมแม่น้ำเจ้าพระยาฝั่งตะวันออกบนถนนเจริญกรุง ระหว่างสะพานกรุงเทพ และสะพานตากสิน มีพื้นที่ทั้งหมด 20 ไร่ 1 งาน 82 ตารางวา มีอาณาเขตติดกับวัดยานนาวา มีลักษณะเป็นอู่แห้งทั้งหมด 2 อู่ ในส่วนของสำนักงานสาขาสัตหีบ (สำนักงานธุรกิจสัตหีบ) ตั้งอยู่ในพื้นที่ราชพัสดุกรมธนารักษ์ (บริเวณอู่ราชนาวีมหิดลอดุลยเดช กรมอู่ทหารเรือ) ตำบลสัตหีบ อำเภอสัตหีบ จังหวัดชลบุรี พื้นที่ 44 ไร่ 2 งาน มีระบบเชื่อมโยงเครือข่ายผ่านระบบ VPN โดยสายสัญญาณอินเตอร์เน็ตเพื่อสามารถใช้ทรัพยากรต่างๆ ที่สำนักงานใหญ่ได้เช่น Data Center ผ่านระบบอินทราเนท หรือระบบงานต่าง ๆ

การกำหนดทิศทางการกำกับดูแลการบริหารจัดการเทคโนโลยีดิจิทัล ของสำนักงานคณะกรรมการนโยบายรัฐวิสาหกิจ (สคร.) รัฐวิสำหกิจส่วนใหญ่ มีการกำหนดกระบวนการกำกับดูแลด้านเทคโนโลยีดิจิทัล ที่ครอบคลุมถึงการบริหารจัดการทรัพยากรเทคโนโลยีดิจิทัลอย่างเหมาะสม มีประสิทธิภาพและมีความโปร่งใส และการกำกับดูแลการบริหารความเสี่ยงด้านเทคโนโลยีดิจิทัล แผนปฏิบัติการดิจิทัลระยะ 3-5 ปี รัฐวิสาหกิจบางแห่ง เริ่มมีการกำหนดรายละเอียดที่ชัดเจนในส่วนของเป้าหมายการนำเทคโนโลยีดิจิทัลมาปรับใช้กับทุกส่วนขององค์กร (Digital Transformation) ที่แสดงให้เห็นถึงการปรับเปลี่ยนทั้งส่วนของกระบวนการ (Process) บุคลากร (People) และเทคโนโลยี (Technology) มีกระบวนการจัดการคุณภาพให้มีแนวทำงปฏิบัติอย่างเป็นระบบที่สามารถทำซ้ำได้ มีการกำหนดขอบเขตและแนวทางในการสร้างระบบบริหารคุณภาพที่ชัดเจน มีการตรวจสอบด้านเทคโนโลยีดิจิทัล (Digital Audit หรือ Computer Audit)

ทั้งนี้ เพื่อให้การดำเนินการแผนปฏิบัติการดิจิทัล ประจำปี 2568 – 2572 ของบริษัท อู่กรุงเทพ จำกัด สอดคล้องสถานการณ์ปัจจุบัน และเป็นประโยชน์สุงสุดต่อการบริหารจัดการด้านการัฒนาเทคโนโลยีดิจิทัลต่อไป

1.2 วิสัยทัศน์

“เป็นอู่เรือที่มีศักยภาพในการบริหารจัดการระดับสากล เติบโต และเป็นกลไกสำคัญในอุตสาหกรรมป้องกันประเทศและพาณิชย์นาวีของไทย สามารถพึ่งพาตนเองอย่างยั่งยืน”

1.3 พันธกิจ

(1) ให้บริการต่อเรือและซ่อมเรือ ซ่อมบำรุงยุทธโธปกรณ์ และจัดส่งพัสดุให้แก่กองทัพเรือ

(2) ให้บริการต่อเรือและซ่อมเรือ หน่วยข้าราชการ รัฐวิสาหกิจ และ เอกชน

(3) ขยายกิจการโดยการสร้างอู่เรือแห่งใหม่บริเวณชายทะเล

(4) ขยายกิจการในอุตสาหกรรมป้องกันประเทศ การต่อเรือเฉพาะทาง การพัฒนาอสังหาริมทรัพย์ เพื่อความมั่นคงทางการเงินในระยะยาว

(5) บริหารจัดการเพื่อมุ่งสู่การเป็นองค์กรแห่งความเป็นเลิศ

(6) ดำเนินกิจการตามหลักการกำกับดูแลที่ดี และมีความ รับผิดชอบต่อสังคม และสิ่งแวดล้อม รวมถึง การป้องกันและปราบปรามการทุจริต และประพฤติมิชอบอย่างเคร่งครัด

1.4 ค่านิยมและวัฒนธรรมองค์กร

(1) ค่านิยม

“แสวงหาโอกาสทางธุรกิจ สั่งสมความเชี่ยวชาญทางอาชีพ สร้างสรรค์ นวัตกรรมสู่ความยั่งยืน”

(2) วัฒนธรรมองค์กร

“อุทิศตนเพื่อให้ความต้องการของลูกค้าบรรลุผลสำเร็จ และดำเนินการปรับปรุงองค์กรเพื่อ สร้างความประทับใจให้ลูกค้าอย่างต่อเนื่อง”

บทที่ 2

กระบวนการจัดทำแผนปฏิบัติการดิจิทัล

2.1 ขั้นตอนศึกษา ทบทวนเอกสารต่าง ๆ ที่เกี่ยวข้อง

2.1.1 ทบทวนแผนยุทธศาสตร์ชาติ 20 ปี พ.ศ.2561 - 2580

โดยที่รัฐธรรมนูญแห่งราชอาณาจักรไทย มาตรา ๖๕ กำหนดให้รัฐ พึงจัดให้มียุทธศาสตร์ชาติเป็นเป้าหมายการพัฒนาประเทศอย่างยั่งยืน ตามหลัก ธรรมาภิบาลเพื่อใช้เป็นกรอบในการจัดทำแผนต่าง ๆ ให้สอดคล้องและบูรณาการกันเพื่อให้เกิดเป็นพลังผลักดันร่วมกันไปสู่เป้าหมายดังกล่าว โดยให้เป็นไปตามที่ กำหนดในกฎหมายว่าด้วยการจัดทำยุทธศาสตร์ชาติ และต่อมาได้มีการตรา พระราชบัญญัติการจัดทำยุทธศาสตร์ชาติ พ.ศ. ๒๕๖๐ โดยกำหนดให้มีการแต่งตั้ง คณะกรรมการยุทธศาสตร์ชาติ เพื่อรับผิดชอบในการจัดทำร่างยุทธศาสตร์ชาติ กำหนดวิธีการการมีส่วนร่วมของประชาชนในการจัดทำร่างยุทธศาสตร์ชาติ ในการติดตาม การตรวจสอบ และการประเมินผล รวมทั้ง กำหนดมาตรการส่งเสริม และสนับสนุนให้ประชาชนทุกภาคส่วนดำเนินการให้สอดคล้องกับยุทธศาสตร์ชาติ เพื่อให้เป็นไปตามที่กำหนดในพระราชบัญญัติการจัดทำยุทธศาสตร์ชาติ พ.ศ. ๒๕๖๐ คณะกรรมการยุทธศาสตร์ชาติได้แต่งตั้งคณะกรรมการจัดทำยุทธศาสตร์ชาติด้านต่าง ๆ รวม ๖ คณะ เพื่อรับผิดชอบในการดำเนินการจัดทำ ร่างยุทธศาสตร์ชาติให้เป็นไปตามหลักเกณฑ์ วิธีการ และเงื่อนไขที่กำหนด ตลอดจนได้จัดให้มีการรับฟังความคิดเห็นของประชาชนและหน่วยงานของรัฐที่เกี่ยวข้องอย่างกว้างขวาง เพื่อประกอบการจัดทำร่างยุทธศาสตร์ชาติตามที่ กฎหมายกำหนด ยุทธศาสตร์ชาติ ๒๐ ปี (พ.ศ. ๒๕๖๑-๒๕๘๐) เป็นยุทธศาสตร์ชาติ ฉบับแรกของประเทศไทยตามรัฐธรรมนูญแห่งราชอาณาจักรไทย ซึ่งจะต้องนำไปสู่ การปฏิบัติเพื่อให้ประเทศไทยบรรลุวิสัยทัศน์ “ประเทศไทยมีความมั่นคง มั่งคั่ง ยั่งยืน เป็นประเทศพัฒนาแล้วด้วยการพัฒนาตามหลักปรัชญาของเศรษฐกิจ พอเพียง” เพื่อความสุขของคนไทยทุกคน

http://nscr.nesdc.go.th/ns/

ยุทธศาสตร์ชาติ 20 ปี เป็นแผนการพัฒนาประเทศ ที่จะกำหนดกรอบและแนวทางการพัฒนาให้หน่วยงานของรัฐทุกภาคส่วนต้องทำตาม เพื่อให้บรรลุวิสัยทัศน์ "ประเทศไทยมีความมั่นคง มั่งคั่ง ยั่งยืน เป็นประเทศที่พัฒนาแล้วด้วยการพัฒนาตามหลักปรัชญาของเศรษฐกิจพอเพียง" หรือตามคติพจน์ "มั่นคง มั่งคั่ง ยั่งยืน" โดยมีระยะเวลาบังคับนานถึง 20 ปี ตั้งแต่ปี 2560-2579 แบ่งยุทธศาสตร์ออกเป็น 6 ด้าน คือ

1. ยุทธศาสตร์ด้านความมั่นคง
2. ยุทธศาสตร์ด้านการสร้างความสามารถในการแข่งขัน
3. ยุทธศาสตร์การพัฒนาและเสริมสร้างศักยภาพคน
4. ยุทธศาสตร์ด้านการสร้างโอกาสความเสมอภาคและเท่าเทียมกันทางสังคม
5. ยุทธศาสตร์ด้านการสร้างการเติบโตบนคุณภาพชีวิตที่เป็นมิตรกับสิ่งแวดล้อม
6. ยุทธศาสตร์ด้านการปรับสมดุลและพัฒนาระบบการบริหารจัดการภาครัฐ

ยุทธศาสตร์ชาติ 20 ปี (พ.ศ. 2561-2580) มุ่งเน้นการพัฒนาประเทศไทยให้มีความมั่นคงและเป็นประชาชนมีความสุขการจัดทำแผนการพัฒนานี้เป็นกรอบและแนวทางที่หน่วยงานของรัฐต้องปฏิบัติตาม

2.1.2 แผนพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคม พ.ศ.2561 - 2580

ตามแผนพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคม ซึ่งจัดทำโดยกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร ได้รับความเห็นชอบจากคณะรัฐมนตรีเมื่อวันที่ 5 เมษายน พ.ศ. 2559 โดยแผนฉบับนี้ได้กำหนดวิสัยทัศน์ในการปฏิรูปประเทศไทยสู่ดิจิทัลไทยแลนด์ (Digital Thailand) ซึ่งหมายถึง ประเทศไทยที่สามารถสร้างสรรค์และใช้ประโยชน์จากเทคโนโลยีดิจิทัลอย่างเต็มศักยภาพในการพัฒนาโครงสร้างพื้นฐาน นวัตกรรม ข้อมูล ทุนมนุษย์ และทรัพยากรอื่นใด เพื่อขับเคลื่อนประเทศไปสู่ความมั่นคง มั่งคั่ง และยั่งยืน โดยมีเป้าหมายหลัก 4 ประการคือ

1) เพิ่มขีดความสามารถในการแข่งขันทางเศรษฐกิจของประเทศด้วยการใช้นวัตกรรมและเทคโนโลยีดิจิทัล เป็นเครื่องมือหลักในการสร้างสรรค์นวัตกรรมการผลิต การบริการ
2) สร้างโอกาสทาง สังคมอย่างเท่าเทียม ด้วยข้อมูลข่าวสารและบริการต่าง ๆ ผ่านสื่อดิจิทัลเพื่อยกระดับคุณภาพชีวิตของประชาชน
3) เตรียมความพร้อมให้บุคลากรทุกกลุ่ม มีความรู้และทักษะที่เหมาะสมต่อการดำเนินชีวิตและการประกอบอาชีพในยุคดิจิทัล
4) ปฏิรูปกระบวนทัศน์การทำงานและการให้บริการของภาครัฐ ด้วยเทคโนโลยีดิจิทัลและการใช้ประโยชน์จากข้อมูล เพื่อให้การปฏิบัติงานเกิดความโปร่งใส มีประสิทธิภาพ และประสิทธิผล

ยุทธศาสตร์แผนพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคม กำหนดภูมิทัศน์ดิจิทัล เพื่อกำหนดทิศทางการพัฒนาและเป้าหมายใน 4 ระยะ ภายในเวลา 20 ปี (2561 – 2580) และกำหนดยุทธศาสตร์ในการดำเนินงานเพื่อไปสู่เป้าหมาย 6 ยุทธศาสตร์ ประกอบด้วย

ยุทธศาสตร์ที่ 1 พัฒนาโครงสร้างพื้นฐานดิจิทัลประสิทธิภาพสูงให้ครอบคลุมทั่วประเทศ

ยุทธศาสตร์ที่ 2 ขับเคลื่อนเศรษฐกิจด้วยเทคโนโลยีดิจิทัล

ยุทธศาสตร์ที่ 3 สร้างสังคมคุณภาพที่ทั่วถึงเท่าเทียมด้วยเทคโนโลยีดิจิทัล

ยุทธศาสตร์ที่ 4 ปรับเปลี่ยนภาครัฐสู่การเป็นรัฐบาลดิจิทัล

ยุทธศาสตร์ที่ 5 พัฒนากำลังคนให้พร้อมเข้าสู่ยุคเศรษฐกิจและสังคมดิจิทัล

ยุทธศาสตร์ที่ 6 สร้างความเชื่อมั่นในการใช้เทคโนโลยีดิจิทัล

ตามแผนพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคม พ.ศ.2561 - 2580 ที่ได้รับการกำหนดจากกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมและสำนักงานคณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งชาติ (สดช.) แผนนี้มุ่งเน้นการส่งเสริมให้เทคโนโลยีดิจิทัลเข้าสู่การใช้งานทั่วไปในด้านต่างๆ เพื่อเพิ่มประสิทธิภาพในเศรษฐกิจและชีวิตสังคม

2.1.3 ทบทวนผลการประเมินและข้อเสนอแนะของสำนักงานคณะกรรมการนโยบายรัฐวิสาหกิจ (สคร.)

หลักเกณฑ์ระบบประเมินผลการดำเนินงานรัฐวิสาหกิจ โดยเปลี่ยนแนวคิดในการกำกับรัฐวิสาหกิจจากการควบคุมขั้นตอนในการทำงานมาเป็นการควบคุมผลการดำเนินงานแทน และให้อำนาจแก่คณะกรรมการรัฐวิสาหกิจในการบริหารจัดการภายในองค์กรได้เอง โดยให้เริ่มนำระบบประเมินผลฯ มาใช้วัดประสิทธิภาพการ

บทที่ 1 บททั่วไป

1.1 ความเป็นมา

บริษัท อู่กรุงเทพ จำกัด เป็นรัฐวิสาหกิจ ในความควบคุมของกองทัพเรือ สังกัดกระทรวงกลาโหม จัดเป็นรัฐวิสาหกิจประเภทนโยบายพิเศษของรัฐประเภทยุทธปัจจัย ประกอบกิจการอุตสาหกรรมอู่เรือ และอุตสาหกรรมต่อเนื่องกับกิจการพาณิชยนาวี และเป็นอุตสาหกรรมพื้นฐานในการพัฒนาอุตสาหกรรมต่อเนื่องหลายประเภท ซึ่งอุตสาหกรรมอู่เรือภายในประเทศเป็นส่วนประกอบที่สำคัญของสมุทานุภาพ เป็นอุตสาหกรรมที่ก่อให้เกิดการจ้างแรงงานฝีมือจำนวนมาก เป็นอุตสาหกรรมที่สนับสนุนและส่งเสริมการขนส่งทางทะเล การค้าระหว่างประเทศส่งเสริมอุตสาหกรรมปิโตรเคมีและอุตสาหกรรมเหล็ก และประการที่สำคัญที่สุดคือ เป็นอุตสาหกรรมที่ทำให้เกิดความมั่นคงทางการทหารและเพิ่มศักย์สงครามให้แก่ประเทศ

บริษัท อู่กรุงเทพ จำกัด (สำนักงานใหญ่) ตั้งอยู่ริมแม่น้ำเจ้าพระยาฝั่งตะวันออกบนถนนเจริญกรุง ระหว่างสะพานกรุงเทพ และสะพานตากสิน มีพื้นที่ทั้งหมด 20 ไร่ 1 งาน 82 ตารางวา มีอาณาเขตติดกับวัดยานนาวา มีลักษณะเป็นอู่แห้งทั้งหมด 2 อู่ ในส่วนของสำนักงานสาขาสัตหีบ (สำนักงานธุรกิจสัตหีบ) ตั้งอยู่ในพื้นที่ราชพัสดุกรมธนารักษ์ (บริเวณอู่ราชนาวีมหิดลอดุลยเดช กรมอู่ทหารเรือ) ตำบลสัตหีบ อำเภอสัตหีบ จังหวัดชลบุรี พื้นที่ 44 ไร่ 2 งาน มีระบบเชื่อมโยงเครือข่ายผ่านระบบ VPN โดยสายสัญญาณอินเตอร์เน็ตเพื่อสามารถใช้ทรัพยากรต่างๆ ที่สำนักงานใหญ่ได้เช่น Data Center ผ่านระบบอินทราเนท หรือระบบงานต่าง ๆ

การกำหนดทิศทางการกำกับดูแลการบริหารจัดการเทคโนโลยีดิจิทัล ของสำนักงานคณะกรรมการนโยบายรัฐวิสาหกิจ (สคร.) รัฐวิสำหกิจส่วนใหญ่ มีการกำหนดกระบวนการกำกับดูแลด้านเทคโนโลยีดิจิทัล ที่ครอบคลุมถึงการบริหารจัดการทรัพยากรเทคโนโลยีดิจิทัลอย่างเหมาะสม มีประสิทธิภาพและมีความโปร่งใส และการกำกับดูแลการบริหารความเสี่ยงด้านเทคโนโลยีดิจิทัล แผนปฏิบัติการดิจิทัลระยะ 3-5 ปี รัฐวิสาหกิจบางแห่ง เริ่มมีการกำหนดรายละเอียดที่ชัดเจนในส่วนของเป้าหมายการนำเทคโนโลยีดิจิทัลมาปรับใช้กับทุกส่วนขององค์กร (Digital Transformation) ที่แสดงให้เห็นถึงการปรับเปลี่ยนทั้งส่วนของกระบวนการ (Process) บุคลากร (People) และเทคโนโลยี (Technology) มีกระบวนการจัดการคุณภาพให้มีแนวทำงปฏิบัติอย่างเป็นระบบที่สามารถทำซ้ำได้ มีการกำหนดขอบเขตและแนวทางในการสร้างระบบบริหารคุณภาพที่ชัดเจน มีการตรวจสอบด้านเทคโนโลยีดิจิทัล (Digital Audit หรือ Computer Audit)

ทั้งนี้ เพื่อให้การดำเนินการแผนปฏิบัติการดิจิทัล ประจำปี 2568 – 2572 ของบริษัท อู่กรุงเทพ จำกัด สอดคล้องสถานการณ์ปัจจุบัน และเป็นประโยชน์สุงสุดต่อการบริหารจัดการด้านการัฒนาเทคโนโลยีดิจิทัลต่อไป

1.2 วิสัยทัศน์

“เป็นอู่เรือที่มีศักยภาพในการบริหารจัดการระดับสากล เติบโต และเป็นกลไกสำคัญในอุตสาหกรรมป้องกันประเทศและพาณิชย์นาวีของไทย สามารถพึ่งพาตนเองอย่างยั่งยืน”

1.3 พันธกิจ

(1) ให้บริการต่อเรือและซ่อมเรือ ซ่อมบำรุงยุทธโธปกรณ์ และจัดส่งพัสดุให้แก่กองทัพเรือ

(2) ให้บริการต่อเรือและซ่อมเรือ หน่วยข้าราชการ รัฐวิสาหกิจ และ เอกชน

(3) ขยายกิจการโดยการสร้างอู่เรือแห่งใหม่บริเวณชายทะเล

(4) ขยายกิจการในอุตสาหกรรมป้องกันประเทศ การต่อเรือเฉพาะทาง การพัฒนาอสังหาริมทรัพย์ เพื่อความมั่นคงทางการเงินในระยะยาว

(5) บริหารจัดการเพื่อมุ่งสู่การเป็นองค์กรแห่งความเป็นเลิศ

(6) ดำเนินกิจการตามหลักการกำกับดูแลที่ดี และมีความ รับผิดชอบต่อสังคม และสิ่งแวดล้อม รวมถึง การป้องกันและปราบปรามการทุจริต และประพฤติมิชอบอย่างเคร่งครัด

1.4 ค่านิยมและวัฒนธรรมองค์กร

(1) ค่านิยม

“แสวงหาโอกาสทางธุรกิจ สั่งสมความเชี่ยวชาญทางอาชีพ สร้างสรรค์ นวัตกรรมสู่ความยั่งยืน”

(2) วัฒนธรรมองค์กร

“อุทิศตนเพื่อให้ความต้องการของลูกค้าบรรลุผลสำเร็จ และดำเนินการปรับปรุงองค์กรเพื่อ สร้างความประทับใจให้ลูกค้าอย่างต่อเนื่อง”

ยุทธศาสตร์ชาติ 20 ปี เป็นแผนการพัฒนาประเทศ ที่จะกำหนดกรอบและแนวทางการพัฒนาให้หน่วยงานของรัฐทุกภาคส่วนต้องทำตาม เพื่อให้บรรลุวิสัยทัศน์ "ประเทศไทยมีความมั่นคง มั่งคั่ง ยั่งยืน เป็นประเทศที่พัฒนาแล้วด้วยการพัฒนาตามหลักปรัชญาของเศรษฐกิจพอเพียง" หรือตามคติพจน์ "มั่นคง มั่งคั่ง ยั่งยืน" โดยมีระยะเวลาบังคับนานถึง 20 ปี ตั้งแต่ปี 2560-2579 แบ่งยุทธศาสตร์ออกเป็น 6 ด้าน คือ

1. ยุทธศาสตร์ด้านความมั่นคง
2. ยุทธศาสตร์ด้านการสร้างความสามารถในการแข่งขัน
3. ยุทธศาสตร์การพัฒนาและเสริมสร้างศักยภาพคน
4. ยุทธศาสตร์ด้านการสร้างโอกาสความเสมอภาคและเท่าเทียมกันทางสังคม
5. ยุทธศาสตร์ด้านการสร้างการเติบโตบนคุณภาพชีวิตที่เป็นมิตรกับสิ่งแวดล้อม
6. ยุทธศาสตร์ด้านการปรับสมดุลและพัฒนาระบบการบริหารจัดการภาครัฐ

ยุทธศาสตร์ชาติ 20 ปี (พ.ศ. 2561-2580) มุ่งเน้นการพัฒนาประเทศไทยให้มีความมั่นคงและเป็นประชาชนมีความสุขการจัดทำแผนการพัฒนานี้เป็นกรอบและแนวทางที่หน่วยงานของรัฐต้องปฏิบัติตาม

2.1.2 แผนพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคม พ.ศ.2561 - 2580

ตามแผนพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคม ซึ่งจัดทำโดยกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร ได้รับความเห็นชอบจากคณะรัฐมนตรีเมื่อวันที่ 5 เมษายน พ.ศ. 2559 โดยแผนฉบับนี้ได้กำหนดวิสัยทัศน์ในการปฏิรูปประเทศไทยสู่ดิจิทัลไทยแลนด์ (Digital Thailand) ซึ่งหมายถึง ประเทศไทยที่สามารถสร้างสรรค์และใช้ประโยชน์จากเทคโนโลยีดิจิทัลอย่างเต็มศักยภาพในการพัฒนาโครงสร้างพื้นฐาน นวัตกรรม ข้อมูล ทุนมนุษย์ และทรัพยากรอื่นใด เพื่อขับเคลื่อนประเทศไปสู่ความมั่นคง มั่งคั่ง และยั่งยืน โดยมีเป้าหมายหลัก 4 ประการคือ

1) เพิ่มขีดความสามารถในการแข่งขันทางเศรษฐกิจของประเทศด้วยการใช้นวัตกรรมและเทคโนโลยีดิจิทัล เป็นเครื่องมือหลักในการสร้างสรรค์นวัตกรรมการผลิต การบริการ
2) สร้างโอกาสทาง สังคมอย่างเท่าเทียม ด้วยข้อมูลข่าวสารและบริการต่าง ๆ ผ่านสื่อดิจิทัลเพื่อยกระดับคุณภาพชีวิตของประชาชน
3) เตรียมความพร้อมให้บุคลากรทุกกลุ่ม มีความรู้และทักษะที่เหมาะสมต่อการดำเนินชีวิตและการประกอบอาชีพในยุคดิจิทัล
4) ปฏิรูปกระบวนทัศน์การทำงานและการให้บริการของภาครัฐ ด้วยเทคโนโลยีดิจิทัลและการใช้ประโยชน์จากข้อมูล เพื่อให้การปฏิบัติงานเกิดความโปร่งใส มีประสิทธิภาพ และประสิทธิผล

ยุทธศาสตร์แผนพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคม กำหนดภูมิทัศน์ดิจิทัล เพื่อกำหนดทิศทางการพัฒนาและเป้าหมายใน 4 ระยะ ภายในเวลา 20 ปี (2561 – 2580) และกำหนดยุทธศาสตร์ในการดำเนินงานเพื่อไปสู่เป้าหมาย 6 ยุทธศาสตร์ ประกอบด้วย

ยุทธศาสตร์ที่ 1 พัฒนาโครงสร้างพื้นฐานดิจิทัลประสิทธิภาพสูงให้ครอบคลุมทั่วประเทศ

ยุทธศาสตร์ที่ 2 ขับเคลื่อนเศรษฐกิจด้วยเทคโนโลยีดิจิทัล

ยุทธศาสตร์ที่ 3 สร้างสังคมคุณภาพที่ทั่วถึงเท่าเทียมด้วยเทคโนโลยีดิจิทัล

ยุทธศาสตร์ที่ 4 ปรับเปลี่ยนภาครัฐสู่การเป็นรัฐบาลดิจิทัล

ยุทธศาสตร์ที่ 5 พัฒนากำลังคนให้พร้อมเข้าสู่ยุคเศรษฐกิจและสังคมดิจิทัล

ยุทธศาสตร์ที่ 6 สร้างความเชื่อมั่นในการใช้เทคโนโลยีดิจิทัล

ตามแผนพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคม พ.ศ.2561 - 2580 ที่ได้รับการกำหนดจากกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมและสำนักงานคณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งชาติ (สดช.) แผนนี้มุ่งเน้นการส่งเสริมให้เทคโนโลยีดิจิทัลเข้าสู่การใช้งานทั่วไปในด้านต่างๆ เพื่อเพิ่มประสิทธิภาพในเศรษฐกิจและชีวิตสังคม

2.1.3 ทบทวนผลการประเมินและข้อเสนอแนะของสำนักงานคณะกรรมการนโยบายรัฐวิสาหกิจ (สคร.)

หลักเกณฑ์ระบบประเมินผลการดำเนินงานรัฐวิสาหกิจ โดยเปลี่ยนแนวคิดในการกำกับรัฐวิสาหกิจจากการควบคุมขั้นตอนในการทำงานมาเป็นการควบคุมผลการดำเนินงานแทน และให้อำนาจแก่คณะกรรมการรัฐวิสาหกิจในการบริหารจัดการภายในองค์กรได้เอง โดยให้เริ่มนำระบบประเมินผลฯ มาใช้วัดประสิทธิภาพการ

บทที่ 2

กระบวนการจัดทำแผนปฏิบัติการดิจิทัล

2.1 ขั้นตอนศึกษา ทบทวนเอกสารต่าง ๆ ที่เกี่ยวข้อง

2.1.1 ทบทวนแผนยุทธศาสตร์ชาติ 20 ปี พ.ศ.2561 - 2580

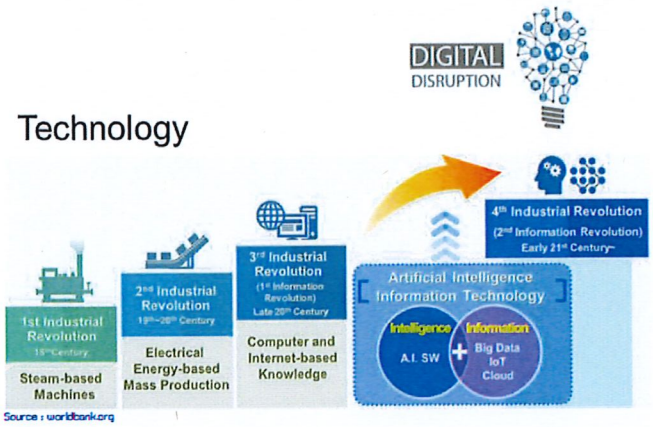
โดยที่รัฐธรรมนูญแห่งราชอาณาจักรไทย มาตรา ๖๕ กำหนดให้รัฐ พึงจัดให้มียุทธศาสตร์ชาติเป็นเป้าหมายการพัฒนาประเทศอย่างยั่งยืน ตามหลัก ธรรมาภิบาลเพื่อใช้เป็นกรอบในการจัดทำแผนต่าง ๆ ให้สอดคล้องและบูรณาการกันเพื่อให้เกิดเป็นพลังผลักดันร่วมกันไปสู่เป้าหมายดังกล่าว โดยให้เป็นไปตามที่ กำหนดในกฎหมายว่าด้วยการจัดทำยุทธศาสตร์ชาติ และต่อมาได้มีการตรา พระราชบัญญัติการจัดทำยุทธศาสตร์ชาติ พ.ศ. ๒๕๖๐ โดยกำหนดให้มีการแต่งตั้ง คณะกรรมการยุทธศาสตร์ชาติ เพื่อรับผิดชอบในการจัดทำร่างยุทธศาสตร์ชาติ กำหนดวิธีการการมีส่วนร่วมของประชาชนในการจัดทำร่างยุทธศาสตร์ชาติ ในการติดตาม การตรวจสอบ และการประเมินผล รวมทั้ง กำหนดมาตรการส่งเสริม และสนับสนุนให้ประชาชนทุกภาคส่วนดำเนินการให้สอดคล้องกับยุทธศาสตร์ชาติ เพื่อให้เป็นไปตามที่กำหนดในพระราชบัญญัติการจัดทำยุทธศาสตร์ชาติ พ.ศ. ๒๕๖๐ คณะกรรมการยุทธศาสตร์ชาติได้แต่งตั้งคณะกรรมการจัดทำยุทธศาสตร์ชาติด้านต่าง ๆ รวม ๖ คณะ เพื่อรับผิดชอบในการดำเนินการจัดทำ ร่างยุทธศาสตร์ชาติให้เป็นไปตามหลักเกณฑ์ วิธีการ และเงื่อนไขที่กำหนด ตลอดจนได้จัดให้มีการรับฟังความคิดเห็นของประชาชนและหน่วยงานของรัฐที่เกี่ยวข้องอย่างกว้างขวาง เพื่อประกอบการจัดทำร่างยุทธศาสตร์ชาติตามที่ กฎหมายกำหนด ยุทธศาสตร์ชาติ ๒๐ ปี (พ.ศ. ๒๕๖๑-๒๕๘๐) เป็นยุทธศาสตร์ชาติ ฉบับแรกของประเทศไทยตามรัฐธรรมนูญแห่งราชอาณาจักรไทย ซึ่งจะต้องนำไปสู่ การปฏิบัติเพื่อให้ประเทศไทยบรรลุวิสัยทัศน์ “ประเทศไทยมีความมั่นคง มั่งคั่ง ยั่งยืน เป็นประเทศพัฒนาแล้วด้วยการพัฒนาตามหลักปรัชญาของเศรษฐกิจ พอเพียง” เพื่อความสุขของคนไทยทุกคน

http://nscr.nesdc.go.th/ns/

ดำเนินงานของรัฐวิสาหกิจใหม่ โดยคณะกรรมการประเมินผลงานรัฐวิสาหกิจได้พิจารณาปรับปรุงระบบประเมินผลฯ เพื่อให้มีความเหมาะสมกับการดำเนินงานของรัฐวิสาหกิจเป็นระยะในปี 2547 คณะกรรมการประเมินผลฯ ได้กำหนดเกณฑ์การประเมินผลในหัวข้อการบริหารจัดการองค์กร (ข้อ 3.) ขึ้น เพื่อผลักดันให้รัฐวิสาหกิจพัฒนาระบบการบริหารจัดการองค์กรในด้านต่างๆ ให้ทัดเทียมกับมาตรฐานสากล โดยการคัดเลือกกระบวนงานหลัก 6 ด้าน ซึ่งมีความสำคัญและเป็นพื้นฐานของการบริหารจัดการที่ดีมาเป็นหัวข้อการประเมินหลัก ได้แก่ บทบาทคณะกรรมการรัฐวิสาหกิจ การบริหารความเสี่ยง การควบคุมภายใน การตรวจสอบภายใน การบริหารจัดการสารสนเทศ และการบริหารทรัพยากรบุคคล

พระราชบัญญัติการพัฒนาการกำกับดูแลและบริหารรัฐวิสาหกิจ (พ.ร.บ. พัฒนารัฐวิสาหกิจฯ) เมื่อวันที่ 19 พฤษภาคม 2562 ซึ่งถือเป็นหัวใจสำคัญของการปฏิรูปรัฐวิสาหกิจไทย โดย พ.ร.บ. พัฒนารัฐวิสาหกิจฯ ดังกล่าวได้กำหนดวัตถุประสงค์สำคัญในการพัฒนาการกำกับดูแลและบริหารรัฐวิสาหกิจไว้ 4 ประเด็นซึ่งรวมถึงการส่งเสริมให้รัฐวิสาหกิจดำเนินการอย่างมีประสิทธิภาพ โปร่งใส สอดคล้องกับหลักการกำกับดูแลกิจการที่ดีและมีการประเมินผลการดำเนินการอย่างต่อเนื่อง สคร.เห็นถึงความจำเป็นของการพัฒนาระบบประเมินผลเพื่อพัฒนาต่อยอดจากโครงการระบบประเมินผลเดิมที่สามารถใช้เป็นเครื่องมือในการกำกับ ติดตาม ประเมินผลการดำเนินงานรัฐวิสาหกิจที่มีความเหมาะสมเป็นรูปธรรม และสามารถสะท้อนถึงความมีประสิทธิภาพในการดำเนินงานได้อย่างแท้จริง โดยได้พิจารณานำข้อดี/จุดแข็งของระบบปัจจุบันที่มีมาใช้ ปรับปรุงข้อด้อยของระบบปัจจุบัน รวมทั้งปรับปรุง เพิ่มเติมประเด็นของการจัดการสมัยใหม่และ Update ให้เป็นปัจจุบัน และจะนำมาใช้ในการประเมินผลรัฐวิสาหกิจในปี 2563 โดยมีรายละเอียดดังนี้คือ

เหตุผลและความจำเป็นในการพัฒนาระบบประเมินผลฯ ใหม่



วัตถุประสงค์

เพื่อส่งเสริมให้ รส. ตอบสนองกับสภาพแวดล้อมในการดำเนินภารกิจ/ธุรกิจ การแข่งขัน ความต้องการของผู้ใช้บริการ และ บริบทที่เปลี่ยนแปลงไป เช่น การเปลี่ยนแปลงของเทคโนโลยีดิจิทัล เป็นต้น รวมถึงนโยบายสำคัญไทยแลนด์ 4.0 ที่ต้องการขับเคลื่อนประเทศด้วยความคิดสร้างสรรค์และนวัตกรรม ทั้งหมดนี้ด้วยการดำเนินงานที่มีประสิทธิภาพ โปร่งใส ตรวจสอบได้

หลักการ

1. รักษาข้อดี/จุดแข็ง ของระบบปัจจุบัน
2. ปรับปรุงข้อด้อย ของระบบปัจจุบัน
3. ปรับปรุง เพิ่มเติม ประเด็นของการจัดการสมัยใหม่/Update ให้เป็นปัจจุบัน พร้อมข้อสังเกต/ข้อเสนอแนะที่ได้รับ

10

ผลการดำเนินงาน ประจำปีบัญชี 2567
ด้าน Core Business Enablers

สรุปข้อเสนอแนะด้านการพัฒนาเทคโนโลยีดิจิทัล

1. รัฐวิสาหกิจต้องนำเทคโนโลยีดิจิทัลมาปรับใช้กับทุกส่วนขององค์กรโดยสามารถกำหนดเป้าหมายที่สะท้อนถึงการเปลี่ยนแปลง People Process Technology ออกมาได้อย่างชัดเจนเป็นรูปธรรม ตลอดจนสามารถประเมินและติดตามผลได้ รวมถึงมีการวัดผลลัพธ์ (Outcome) ในเชิงปริมาณที่สะท้อนให้เห็นผลดำเนินงานที่สำคัญของรัฐวิสาหกิจที่ดียิ่งขึ้น เช่น การให้บริการประชาชน การอำนวยความสะดวกให้กับผู้มีส่วนได้ส่วนเสีย เป็นต้น เพื่อยกระดับการดำเนินงานขององค์กร เช่น ทอท. กปน. กปภ. กทท. กคช. อภ. บวท. กนอ. รฟม. กทพ. ททท. รฟท. ขสมก. บขส. เป็นต้น
2. รัฐวิสาหกิจต้องดำเนินการป้องกันความเสี่ยงด้านเทคโนโลยีดิจิทัล ที่ปัจจุบันมีภัยคุกคามจากหลากหลายรูปแบบ เช่น Cyber Security Hacking the home Beware of the 'wares' Application-Based or Web-based Threats อาชญากรรมจากคอมเซ็นเตอร์ เป็นต้น โดยต้องมีการกำหนดเป็นแผนการรองรับที่ชัดเจน มีการนำเครื่องมือป้องกันหรือเทคโนโลยีที่เหมาะสมเข้ามาใช้ รวมถึงมีการติดตามผลการดำเนินงานอย่างต่อเนื่อง เช่น อภ. กปน. กปภ. ททท. ทอท. กนอ. รฟม. กทพ. กทท. กกท กคช. รฟท. สบพ. ขสมก. บขส. เป็นต้น
3. รัฐวิสาหกิจต้องนำเทคโนโลยีดิจิทัลที่ทันสมัยมาประยุกต์ใช้กับการดำเนินงานให้มีประสิทธิภาพ เช่น การใช้ Cloud Computing Services เพื่อลดการลงทุน Data Center การใช้ Big Data, Data Analytics และ AI เพื่อให้เกิดการใช้ประโยชน์ข้อมูลอย่างมีประสิทธิภาพ การบริหารจัดการ Digital Outsource เพื่อลดปัญหาการขาดแคลนทรัพยากรและบุคลากรด้านเทคโนโลยีดิจิทัล เป็นต้น โดยต้องคำนึงถึงความคุ้มค่าการลงทุน ความมั่นคงปลอดภัย และเทคโนโลยีที่เหมาะสม
4. รัฐวิสาหกิจต้องดำเนินการให้มีการประกอบธุรกิจ หรือการปฏิบัติที่มีความสอดคล้องกับกฎหมาย ระเบียบ ข้อบังคับ และมาตรฐานต่างๆ ที่เกี่ยวข้องกับการพัฒนาเทคโนโลยีดิจิทัล เช่น พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล 2562 และ พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 เป็นต้น โดยแสดงให้เห็นถึงแผนงาน/โครงการที่ชัดเจนเป็นรูปธรรม เพื่อลดช่องว่าง (GAP) การปฏิบัติที่ยังไม่มีความสอดคล้อง โดยเฉพาะรัฐวิสาหกิจที่จัดเป็นหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Critical Information Infrastructure: CII) ที่ สกมช. มีการใช้ NIST2.0 เป็นแนวทางในการประเมินผลกับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Critical Information Infrastructure: CII) ซึ่งแบ่งตามลักษณะการให้บริการ ได้ดังต่อไปนี้
   หมวด 2 ด้านบริการภาครัฐที่สำคัญ ได้แก่ อจน. อสมท.
   หมวด 3 ด้านการเงินการธนาคาร ได้แก่ ธกส. ธสน. ธพว. ออมสิน ธอส. ธอท. บสย.
   หมวด 4 ด้านเทคโนโลยีสารสนเทศและคมนาคม ได้แก่ ปณท. เอ็นที
   หมวด 5 ด้านขนส่งและโลจิสติกส์ ได้แก่ กทพ. บขส. ขสมก. รฟท. รฟม. ทอท. บวท.
   หมวด 6 ด้านพลังงานและสาธารณูปโภค ได้แก่ กฟน. กฟผ. กฟภ. ปตท. กปน. กปภ.
   หมวด 7 ด้านสาธารณสุข ได้แก่ อภ.
   รวมถึงควรมีการกำหนดบทบาทความร่วมมือกับหน่วยงานกำกับดูแลต่างๆ อย่างไกล้ชิด

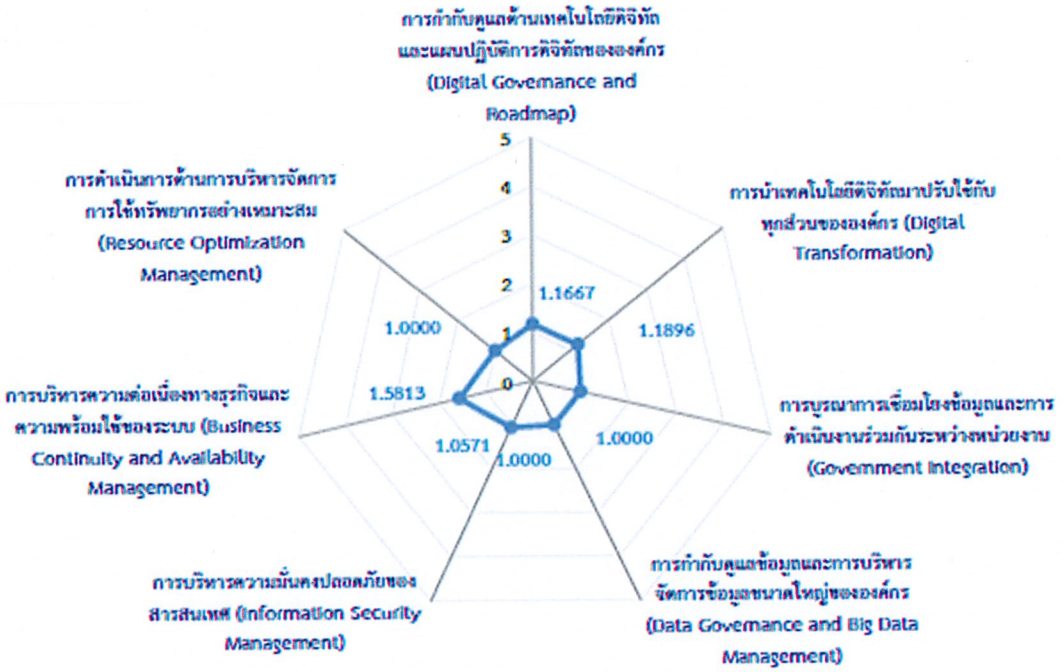
2.1.4 แผนพัฒนารัฐบาลดิจิทัลของประเทศไทย พ.ศ. 2566-2570

แผนพัฒนารัฐบาลดิจิทัลบับนี้มุ่งยกระดับภาครัฐไทยสู่เป้าหมายการให้บริการตอบสนองประชาชน และลดความเหลื่อมล้ำการเพิ่มความสามารถและศักยภาพในการแข่งขันของภาคธุรกิจ การสร้างความโปร่งใส ที่เน้นการเปิดเผยข้อมูลแก่ประชาชนโดยไม่ต้องร้องขอและการสนับสนุนการมีส่วนร่วมของประชาชน และการเป็นภาครัฐที่

ผลการดำเนินงาน ประจำปีบัญชี 2567
ด้าน Core Business Enablers

(outcome) ของกระบวนการประเมินประสิทธิผลของกระบวนการที่สอดคล้องตามเกณฑ์ โดยแสดงให้เห็นว่าผลลัพธ์ (outcome) ของกระบวนการครบถ้วนตามเกณฑ์ รวมถึงควรมีการนำผลลัพธ์ที่สำคัญของกระบวนการ เข้าสู่กระบวนการทบทวน ปรับปรุงและพัฒนากระบวนการอย่างต่อเนื่อง

กราฟสรุปผลการประเมิน	หัวข้อ "การพัฒนาเทคโนโลยีดิจิทัล"	อยู่ที่ระดับคะแนน 1.1529



ปฏิบัติที่ดีด้านการพัฒนาเทคโนโลยีดิจิทัลของภาครัฐและภาคเอกชน ที่เป็นที่ยอมรับทั้งในและต่างประเทศ ตลอดจนสอดคล้องกับทิศทาง นโยบาย กรอบการดำเนินงานของประเทศ เช่น นโยบายไทยแลนด์ 4.0 แผนดิจิทัลเพื่อเศรษฐกิจและสังคม

ประเมินความเสี่ยงและความร้ายแรงของ

- Data Protection Officer: เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO) กำหนดลักษณะขององค์กรที่ต้องจัดให้มีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO
- Security Measures for Historical Research for Public Task: มาตรการปกป้องข้อมูลส่วนบุคคลสำหรับการจัดทำเอกสารประวัติศาสตร์หรือจดหมายเหตุเพื่อประโยชน์
- Security Measures for Scientific Research and Statistical Purposes: มาตรการที่เหมาะสมสำหรับการเก็บรวบรวมข้อมูลส่วนบุคคลเพื่อให้บรรลุวัตถุประสงค์ที่เกี่ยวกับการศึกษาวิจัยหรือสถิติกำหนดมาตรการปกป้องที่เหมาะสมเพื่อคุ้มครองสิทธิและเสรีภาพของเจ้าของข้อมูลส่วน
- Cross-Border Transfer: หลักเกณฑ์การให้ความคุ้มครองข้อมูลส่วนบุคคลที่ส่งหรือโอนไปยังต่างประเทศ
- Security Measures for Criminal Record: มาตรการคุ้มครองข้อมูลส่วนบุคคลเกี่ยวกับประวัติอาชญากรรม

2.1.6.2 พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562

พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 (Cybersecurity Act, B.E. 2562) ของประเทศไทยมีข้อกำหนดหลายประการในการรักษาความมั่นคงปลอดภัยทางไซเบอร์ของประเทศ ทั้งนี้เพื่อป้องกันและลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ และเพื่อรักษาความมั่นคงของระบบสารสนเทศในภาคส่วนต่างๆ

ตามพระราชบัญญัตินี้เน้นการปฏิบัติตามและมาตรการที่ต้องดำเนินการโดยองค์กรต่างๆ เพื่อให้มั่นใจว่ามีการรักษาความมั่นคงปลอดภัยทางไซเบอร์ตามมาตรฐานที่กำหนดสิ่งที่สำคัญในมาตรา 2.5 ประกอบด้วย:

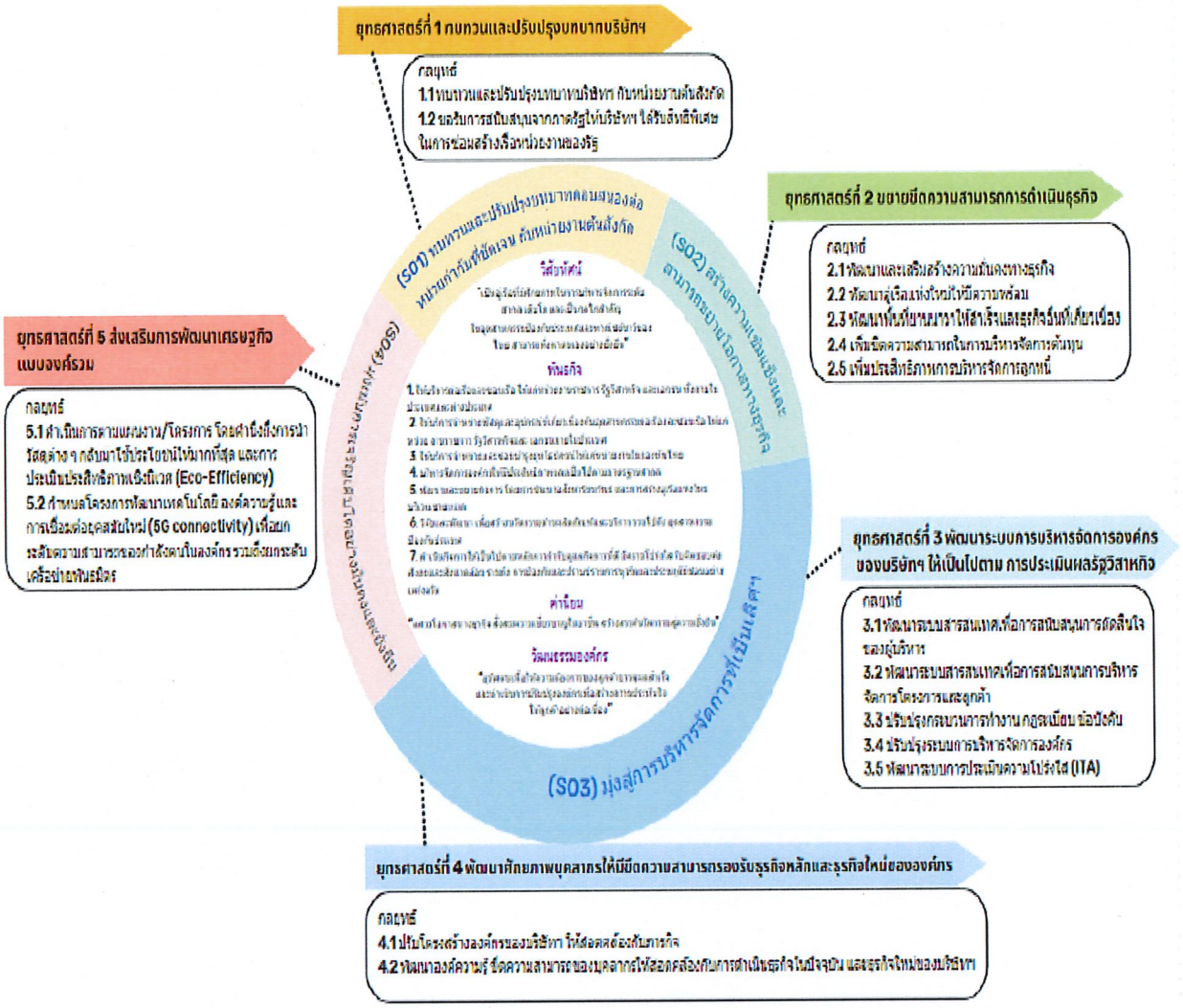
1. **การประเมินและจัดการความเสี่ยง**: องค์กรต่างๆ ต้องดำเนินการประเมินความเสี่ยงที่อาจเกิดขึ้นจากภัยคุกคามทางไซเบอร์ และจัดการความเสี่ยงนั้นอย่างมีประสิทธิภาพ
2. **การพัฒนานโยบายและแผนการรักษาความมั่นคงปลอดภัยไซเบอร์**: องค์กรต้องมีนโยบายและแผนการที่ชัดเจนในการรักษาความมั่นคงปลอดภัยไซเบอร์ รวมถึงการปรับปรุงและทบทวนนโยบายและแผนการดังกล่าวอย่างสม่ำเสมอ
3. **การป้องกันและตรวจจับภัยคุกคามทางไซเบอร์**: องค์กรต้องมีมาตรการที่เหมาะสมในการป้องกันและตรวจจับภัยคุกคามทางไซเบอร์ รวมถึงการใช้เทคโนโลยีที่ทันสมัยในการตรวจจับและตอบโต้ภัยคุกคาม
4. **การบริหารจัดการเหตุการณ์**: องค์กรต้องมีแผนการบริหารจัดการเหตุการณ์ที่เกี่ยวข้องกับภัยคุกคามทางไซเบอร์อย่างมีประสิทธิภาพ รวมถึงการรายงานและการตอบสนองต่อเหตุการณ์อย่างรวดเร็ว

5. **การฝึกอบรมและสร้างความตระหนักรู้**: องค์กรต้องจัดการฝึกอบรมและสร้างความตระหนักรู้ให้กับบุคลากรในองค์กรเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์การปฏิบัติตามข้อกำหนดเหล่านี้จะช่วยให้องค์กรสามารถป้องกันและตอบโต้ภัยคุกคามทางไซเบอร์ได้อย่างมีประสิทธิภาพ และรักษาความมั่นคงของระบบสารสนเทศในองค์กรได้อย่างยั่งยืนความตระหนักถึงบทบาทหน้าที่ตามกฎหมายในเรื่องของการรักษาความมั่นคงปลอดภัย มีความรู้ความเข้าใจในการจัดการเกี่ยวกับภัยคุกคามด้านความมั่นคงปลอดภัยและความเสี่ยงทางด้านเทคโนโลยีดิจิทัล ที่กำลังเป็นปัญหาในการทำงานในยุคดิจิทัลได้อย่างมีประสิทธิภาพตามแนวทางของ NIST Cybersecurity Framework โดยแบ่งออกเป็น 5 ขั้นตอนสำคัญ คือ Identity, Protect, Detect, Response และ Recovery สำหรับช่วยให้องค์กรสามารถวางแผนป้องกัน ตรวจจับ และตอบสนองต่อภัยคุกคามได้อย่างรวดเร็วและเป็นระบบ และเข้าใจในกระบวนการในการวางแผนรับมือกับภัยคุกคามและความเสี่ยงทางด้านเทคโนโลยีดิจิทัล การเข้าใจในกระบวนการจะทำให้เกิดการวางแผนที่ดีและยั่งยืนในการรับมือกับความเสี่ยงรูปแบบต่าง ๆ ที่เกิดขึ้นทั้งในปัจจุบันและอนาคตที่มีการเปลี่ยนแปลงทางด้านเทคโนโลยีอย่างรวดเร็วเพื่อช้ในการวางแผนการรับมือกับภัยคุกคามและความเสี่ยงทางด้านดิจิทัลในองค์กรได้อย่างมีประสิทธิภาพ

   5.1 ภาพรวมความมั่นคงปลอดภัยไซเบอร์ (Security Overview) เป็นการเรียนรู้ Security Awareness การรู้เท่าทันการโจมตีและความมั่นคงปลอดภัยทางไซเบอร์ สถานการณ์ต่าง ๆ ที่เกิดขึ้นในการองค์กรทั้งภาครัฐและเอกชนกรณีศึกษาต่าง ๆ ที่เกิดขึ้นทั้งในประเทศและต่างประเทศ การเรียนรู้ถึงความเสียหายที่เกิดขึ้นจากภัยคุกคามไซเบอร์ Security Trend แนวโน้มของภัยคุกคามต่าง ๆ แนวโน้มของความมั่นคงปลอดภัย ไซเบอร์ Information security Concept: CIA แนวคิดพื้นฐานของความมั่นคงปลอดภัยไซเบอร์ Confidentiality คือ การรักษาความลับของ ไซเบอร์ Integrity คือความถูกต้องของข้อมูลไซเบอร์ Availability คือความพร้อมใช้งานของ เทคโนโลยีไซเบอร์

   5.2 กฎหมายที่เกี่ยวข้องกับความมั่นคงปลอดภัย ไซเบอร์ (Laws and Regulation) พ.ร.บ. ว่าด้วยการกระทาความผิดเกี่ยวกับคอมพิวเตอร์ 2560 พ.ร.บ.การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.2562 พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 กรณีศึกษาที่เกี่วข้องกับกฎหมายที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์

   5.3 การระบุความเสี่ยงด้านความมั่นคงปลอดภัย ไซเบอร์ (Identify) การศึกษาทำความเข้าใจบริบท ทรัพยากรและกิจกรรมงานสาคัญเพื่อบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ที่มีต่อระบบทรัพย์สิน ข้อมูล และขีดความสามารถ Identity: Assessment and Auditing แนวทางและกรอบในการการประเมินองค์กรด้านความมั่นคงปลอดภัยไซเบอร์ และความเสี่ยง เพื่อวิเคราะห์ช่องว่าง (Gap Analysis) หรือจุดอ่อนของกระบวนการในการรักษาความมั่นคงปลอดภัยทางไซเบอร์ขององค์กร ตัวอย่าง ของ Framework ในการประเมินขององค์กรต่าง ๆ



ภาพที่ 1 ความสอดคล้องระหว่างยุทธศาสตร์ แผนวิสาหกิจ และแผนปฏิบัติการ ของ บริษัท อู่กรุงเทพ จำกัด ปีงบประมาณ พ.ศ.2568 – 2572

ซึ่งผลการสำรวจดังกล่าวจะสามารถใช้เป็นข้อมูลประกอบการจัดทำนโยบายและแผนการขับเคลื่อนภาครัฐไปสู่การเป็นรัฐบาลดิจิทัล (Digital Government) ให้มีประสิทธิภาพและเป็นเอกภาพมากยิ่งขึ้น นอกจากนี้ เพื่อเป็นการให้เกียรติและเชิดชูหน่วยงานที่มีความมุ่งมั่นที่จะพัฒนาองค์กรไปสู่การเป็นรัฐบาลดิจิทัล บอท. จะนำผลการสำรวจดังกล่าว มาพิจารณามอบรางวัลรัฐบาลดิจิทัล ประจำปี 2567 (Digital Government Awards 2024) ให้แก่หน่วยงานภาครัฐที่มีการปรับเปลี่ยนองค์กรสู่การเป็นรัฐบาลดิจิทัลในระดับสูง เพื่อเป็นแบบอย่างที่ดีให้กับส่วนราชการและหน่วยงานของรัฐต่อไป

ตัวชี้วัดที่ 1 แนวนโยบายและหลักปฏิบัติ (Policies & Practices)

ตัวชี้วัด	วัตถุประสงค์
1.1 Digital Policy	สำรวจความสอดคล้องของการจัดทำแผนปฏิบัติการหรือแผนงานของหน่วยงานที่สอดคล้องกับแผนพัฒนารัฐบาลดิจิทัลของประเทศไทย ปี พ.ศ. 2566 - 2570
1.2 Cyber Security Policy	สำรวจการดำเนินการที่สอดคล้องกับพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 และกฎหมายลำดับรองที่เกี่ยวข้อง
1.3 Legal & Regulatory Mechanism	สำรวจการดำเนินการตามกฎหมายที่เกี่ยวข้อง และการปฏิบัติตามพระราชบัญญัติการปฏิบัติราชการทางอิเล็กทรอนิกส์ พ.ศ. 2565
1.4 Data Policy	สำรวจการจัดทำแผนปฏิบัติการหรือแผนงานสำหรับ ธรรมาภิบาลข้อมูลภาครัฐ (Data Governance) การเปิดเผยข้อมูล (Open Data) และ การคุ้มครองข้อมูลส่วนบุคคล (PDPA)

ตัวชี้วัดที่ 2 กระบวนการพัฒนาด้วยข้อมูล (Data-driven Practices)

ตัวชี้วัด	วัตถุประสงค์
2.1 Data Governance	สำรวจการดำเนินการและปฏิบัติการด้านธรรมาภิบาลข้อมูลภาครัฐ
2.2 Open Data & Sharable Data	สำรวจการดำเนินการและปฏิบัติการด้านข้อมูลเปิดภาครัฐ และด้านการแลกเปลี่ยนข้อมูล
2.3 Data Privacy	สำรวจการดำเนินการและปฏิบัติการด้านการคุ้มครองข้อมูลส่วนบุคคล

ตัวชี้วัดที่ 3 ศักยภาพเจ้าหน้าที่ภาครัฐด้านดิจิทัล (Digital Capability)

ตัวชี้วัด	วัตถุประสงค์

	เทคโนโลยีดิจิทัลมาใช้เพื่อให้ประชาชนสามารถเสนอทางเลือกและร่วมตัดสินใจเกี่ยวกับนโยบายหรือการบริการจากภาครัฐ

ตัวชี้วัดที่ 5 การบริหารจัดการรูปแบบดิจิทัล (Smart Back Office)

ตัวชี้วัด	วัตถุประสงค์
5.1 Integrated Enterprise	สำรวจประสิทธิภาพในการนำเอาระบบดิจิทัลมาบริหารงานในหน่วยงาน และการเชื่อมโยงกับระบบอื่น
5.2 Process Optimization	สำรวจประสิทธิภาพของกระบวนการทำงานด้วยการนำเทคโนโลยีดิจิทัลและแพลตฟอร์มมาประยุกต์ใช้
5.2.1 Administration	สำรวจการนำเทคโนโลยีดิจิทัลมาเพิ่มประสิทธิภาพในการบริหารจัดการภายในองค์กร
5.2.2 Platform for Communication and Collaboration	สำรวจกระบวนการติดต่อสื่อสาร การทำงานระหว่างหน่วยงานภายในองค์กรและ ข้ามองค์กร

ตัวชี้วัดที่ 6 โครงสร้างพื้นฐานความมั่นคงปลอดภัยและมีประสิทธิภาพ (Secure and Efficient Infrastructure)

ตัวชี้วัด	วัตถุประสงค์
6.1 Reliable Infrastructure	สำรวจการนำโครงสร้างพื้นฐานกลางภาครัฐที่มีเสถียรภาพและมีประสิทธิภาพมาปรับใช้ในหน่วยงาน
6.2 Cybersecurity (Cybersecurity Standard and Procedure)	สำรวจการมีมาตรฐานและแนวทางในการดำเนินการด้านความมั่นคงปลอดภัยทางไซเบอร์

ยุทธศาสตร์ของบริษัท อู่กรุงเทพ จำกัด ตามแผนวิสาหกิจ ปีงบประมาณ พ.ศ.2569 - พ.ศ.2573 เกี่ยวกับการพัฒนาเทคโนโลยีดิจิทัล มีรายละเอียดดังนี้

ยุทธศาสตร์	วัตถุประสงค์เชิงยุทธศาสตร์	กลยุทธ์การดำเนินการ	ตัวชี้วัด/แผนงาน	เป้าหมาย				
				2569	2570	2571	2572	2573
ยุทธศาสตร์ที่ 3 พัฒนาระบบการบริหารจัดการองค์กรของบริษัทฯ ให้เป็นไปตามการประเมินผลรัฐวิสาหกิจ	3.1 พัฒนาระบบสารสนเทศเพื่อสนับสนุนการตัดสินใจของผู้บริหารและการบริหารจัดการโครงการ	3.1 พัฒนาระบบสารสนเทศเพื่อการสนับสนุนการตัดสินใจของผู้บริหาร	3.1.1 ความสำเร็จในการดำเนินการตามโครงการ (1) แผนงานพัฒนาระบบสารสนเทศเพื่อการสนับสนุนการตัดสินใจของผู้บริหาร - ระบบวิเคราะห์เชิงลึก (BI) ตัดสินใจแบบ Real-Time	>1 โครงการ	>1 โครงการ	>1 โครงการ	>1 โครงการ	>1 โครงการ
		3.2 พัฒนาระบบสารสนเทศเพื่อการสนับสนุนการบริหารจัดการโครงการและลูกค้า	3.2.1 ความสำเร็จในการดำเนินการตามโครงการ (1) แผนงานพัฒนาระบบสารสนเทศเพื่อการสนับสนุนการบริหารจัดการโครงการและผู้มีส่วนได้เสียทั้งภายในและภายนอก - จัดทำแพลตฟอร์มจอง/ติดตามงานซ่อมแบบออนไลน์	>1 โครงการ	>1 โครงการ	>1 โครงการ	>1 โครงการ	>1 โครงการ
	3.2 ปรับปรุงกระบวนการทำงาน กฎระเบียบ และข้อบังคับให้สอดคล้องกับการดำเนินธุรกิจในปัจจุบัน	3.3 ปรับปรุงกระบวนการทำงาน กฎระเบียบข้อบังคับให้สอดคล้อง เหมาะสมกับการดำเนินธุรกิจของบริษัทฯ ในปัจจุบันที่ต้องแข่งขันกับภาคเอกชน	3.3.1 จำนวนกระบวนการทำงาน/ระเบียบ/ข้อบังคับบริษัทฯ ที่ได้รับการทบทวนปรับปรุงแก้ไข /การอนุมัติยกเว้นการปฏิบัติตามระเบียบกระทรวงการคลังว่าด้วยการจัดซื้อจัดจ้างและการบริหารพัสดุ ภาครัฐ พ.ศ. 2560 ให้สอดคล้องกับการดำเนินธุรกิจในปัจจุบันที่ต้องแข่งขันกับภาคเอกชน (1) แผนงานปรับปรุงเพิ่มเติมกฎระเบียบข้อบังคับให้หน่วยงานมีมาตรฐานสากลมีความคล่องตัวโปร่งใสและสามารถตรวจสอบได้	>2	>2	>2	>2	>2
	3.3 เสริมสร้างความโปร่งใสและธรรมาภิบาลในการดำเนินงานของบริษัทฯ	3.4 ปรับปรุงระบบการบริหารจัดการองค์กรให้เป็นไปตามมาตรฐานที่ สคร. กำหนด	3.4.1 คะแนนผลประเมินด้านการบริหารจัดการองค์กร (1) การกำกับดูแลที่ดีและการนำองค์กร (2) การวางแผนเชิงกลยุทธ์ (3) การบริหารความเสี่ยงและการควบคุม	>1.70	>1.80	>1.90	>2.20	>2.50

- ต้องได้รับความยินยอมจากเจ้าของข้อมูลก่อนการเปิดเผย ยกเว้นในกรณีที่กฎหมายอนุญาต
- ต้องมีการป้องกันและรักษาความลับของข้อมูลในกรณีที่มีการเปิดเผย

4. **การรักษาความปลอดภัยของข้อมูลส่วนบุคคล:**
   - ต้องมีมาตรการรักษาความปลอดภัยที่เหมาะสมเพื่อป้องกันการสูญหาย การเข้าถึง การใช้ การเปลี่ยนแปลง หรือการเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต
   - ต้องทำการทบทวนและปรับปรุงมาตรการรักษาความปลอดภัยอย่างสม่ำเสมอ
5. **สิทธิของเจ้าของข้อมูลส่วนบุคคล:**
   - เจ้าของข้อมูลมีสิทธิในการเข้าถึงข้อมูลส่วนบุคคลของตนเอง
   - มีสิทธิในการขอแก้ไขหรือปรับปรุงข้อมูลส่วนบุคคลที่ไม่ถูกต้องหรือไม่เป็นปัจจุบัน
   - มีสิทธิในการขอให้ลบหรือทำลายข้อมูลส่วนบุคคลเมื่อไม่ต้องการให้เก็บข้อมูลต่อไป
6. **การจัดตั้งผู้ควบคุมข้อมูลและผู้ประมวลผลข้อมูล:**
   - องค์กรต้องจัดตั้งบุคคลหรือหน่วยงานที่มีหน้าที่ในการควบคุมและประมวลผลข้อมูลส่วนบุคคล
   - ต้องมีการอบรมและสร้างความตระหนักรู้ให้กับบุคลากรในองค์กรเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล
7. **การแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล:**
   - หากเกิดเหตุการละเมิดข้อมูลส่วนบุคคล ต้องแจ้งเหตุการละเมิดไปยังสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลภายใน 72 ชั่วโมง
   - ต้องแจ้งเจ้าของข้อมูลถึงเหตุการละเมิดหากมีความเสี่ยงที่จะกระทบสิทธิและเสรีภาพของเจ้าของข้อมูล

การปฏิบัติตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลอย่างเคร่งครัดจะช่วยให้การจัดการข้อมูลส่วนบุคคลเป็นไปอย่างมีประสิทธิภาพและถูกต้องตามกฎหมาย รวมถึงปกป้องสิทธิและความเป็นส่วนตัวของเจ้าของข้อมูลส่วนบุคคลจากที่กฎหมาย PDPA เริ่มบังคับใช้ตั้งแต่วันที่ 1 มิถุนายน 2565 นับจนถึงปัจจุบัน คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (PDPC) ได้ออกประกาศกฎหมายลำดับรองของกฎหมาย PDPA เพิ่มเติมอีกหลายฉบับตามมา เพื่อยกระดับมาตรฐานการคุ้มครองข้อมูลส่วนบุคคลให้มีประสิทธิภาพยิ่งขึ้น เรามาดูกันว่ามีอะไรเปลี่ยนแปลง แล้วองค์กรควรต้องปรับตัวอย่างไรบ้างเนื้อหาตามประกาศหลัก ๆ ที่สำคัญมีดังนี้

- Security Measures of Data Controller: มาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล2.) Record of Processing Activities (ROPA): บันทึกรายการของกิจกรรมการประมวลผลข้อมูลส่วนบุคคล (ROPA) กำหนดวิธีการจัดทำและเก็บรักษาบันทึกรายละเอียดเกี่ยวกับกิจกรรมการประมวลผลข้อมูลส่วน
- Data Breach Notification: การแจ้งเหตุการละเมิดข้อมูลส่วนบุคคล กำหนดแนวทางการ