องค์การสุรา
กรมสรรพสามิต
LIQUOR DISTILLERY ORGANIZATION

2025

กรอบการกำกับดูแล

ด้านการบริหารจัดการเทคโนโลยีดิจิทัล

(DIGITAL GOVERNANCE GUIDING PRINCIPLE)

องค์การสุรา กรมสรรพสามิต

สารบัญ

หน้า

บทที่ 1 บทนำ

องค์การสุรา กรมสรรพสามิต ตระหนักถึงความสำคัญในการใช้เทคโนโลยีดิจิทัลให้มีประสิทธิภาพและเป็นที่ยอมรับ ตอบสนองต่อความต้องการของผู้มีส่วนได้ส่วนเสียในการดำเนินธุรกิจและภารกิจขององค์การสุราฯ มีการกำกับดูแล การบริหารจัดการที่ดีด้านเทคโนโลยีสารสนเทศอย่างต่อเนื่อง ตามหลักการกำกับดูแลกิจการที่ดี รวมทั้งมีการบริหารจัดการที่ดีเลิศและบูรณาการตามแนวทางการกำกับดูแลการบริหารความเสี่ยง และการปฏิบัติตามกฎเกณฑ์ (Integrated GRC: Governance, Risk Management and Compliance)

การกำกับดูแลที่ดีด้านเทคโนโลยีสารสนเทศ (IT Governance, ITG) อย่างเป็นระบบ จะเป็นกลไกสำคัญในการสนับสนุนการกำกับดูแลกิจการที่ดี (Corporate Governance) ทั้งในเรื่องของการกำหนดนโยบายมาตรฐานและแนวปฏิบัติ เพื่อสร้างความเชื่อมั่นในการให้บริการด้านเทคโนโลยีสารสนเทศ การจัดการความเสี่ยงและการสร้างโอกาสทางธุรกิจจากการนำระบบเทคโนโลยีดิจิทัลมาใช้ รวมไปถึงเรื่องของการปฏิบัติงานที่สอดคล้องกับกฎหมาย ข้อบังคับ กฎ ระเบียบ และข้อกำหนดต่าง ๆ อันจะเป็นการสร้างคุณค่าจากการใช้งานเทคโนโลยีดิจิทัลตลอดจนสนับสนุนการดำเนินงานตามแผนงานและยุทธศาสตร์ ขององค์การสุราฯ ให้เป็นไปอย่างมีประสิทธิภาพ

1.1 หลักการและเหตุผล

เนื่องด้วยระบบเทคโนโลยีสารสนเทศเข้ามามีบทบาทสำคัญในการขับเคลื่อนองค์กร และถือเป็นหนึ่งในระบบงานหลักที่หากมีเหตุขัดข้องหรือสถานการณ์ฉุกเฉินเกิดขึ้น จะส่งผลกระทบต่อการดำเนินงานของผู้ประกอบธุรกิจ ผู้ลงทุน และความเชื่อมั่นต่อตลาดทุนโดยรวมได้ ผู้บริหารระดับสูงจึงมีบทบาทสำคัญในการบริหารจัดการในการนำเทคโนโลยีสารสนเทศมาใช้ในการประกอบธุรกิจ รวมถึงมีหน้าที่ในการส่งทอดเป้าหมายทางธุรกิจตามภารกิจ กลยุทธ์ นโยบาย และแผนงานระดับองค์กร ไปสู่เป้าหมายที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ โดยอยู่ภายใต้การกำกับดูแลของคณะกรรมการบริหารกิจการองค์การสุรา และคณะกรรมการ/คณะทำงานที่เกี่ยวข้อง เพื่อทำให้มั่นใจได้ว่าการนำเทคโนโลยีสารสนเทศดังกล่าวมาใช้ในการประกอบธุรกิจ จะช่วยให้ผู้ประกอบธุรกิจสามารถบรรลุเป้าหมายได้ตามที่กำหนดไว้ โดยมีการใช้ทรัพยากรอย่างเหมาะสม และมีการบริหารจัดการความเสี่ยงอย่างมีประสิทธิภาพและเหมาะสม ให้สอดคล้องกับการกำกับดูแลกิจการที่ดี (Corporate Governance)

การกำกับดูแลและบริหารจัดการเทคโนโลยีสารสนเทศระดับองค์กรที่ดี หมายถึง การจัดการโครงสร้างองค์กรและสาธารณูปโภคพื้นฐานทางด้านเทคโนโลยีสารสนเทศเพื่อสนับสนุนกลยุทธ์และเป้าหมายขององค์กร รวมทั้งสนับสนุนการดำเนินงานทางด้านสารสนเทศอย่างมีประสิทธิภาพและประสิทธิผล โดยการกำกับดูแลและบริหารจัดการเทคโนโลยีสารสนเทศระดับองค์กรที่ดี เป็นกระบวนการที่สำคัญที่ช่วยในด้าน

- การจัดสรรทรัพยากรสารสนเทศอย่างมีประสิทธิภาพ ประสิทธิผล สอดคล้องกับเป้าหมาย พันธกิจและวัตถุประสงค์ขององค์กร
- การบริหารความเสี่ยงในกิจกรรมด้านเทคโนโลยีสารสนเทศ ในด้านของผลตอบแทนเปรียบเทียบกับความเสี่ยง และการจัดการกับความเสี่ยงอย่างเหมาะสม
- การสร้างความมั่นใจถึงคุณภาพของเทคโนโลยีสารสนเทศเพื่อใช้ในการตัดสินใจในทุกระดับทั้งการตัดสินใจ ในเชิงกลยุทธ์ ไปจนถึงการตัดสินใจเพื่อบริหารจัดการในการดำเนินธุรกิจ
- การสร้างความมั่นใจในความน่าเชื่อถือของระบบสารสนเทศ

• การพิจารณาความคุ้มค่าของต้นทุนของการให้บริการ และผลตอบแทนที่ได้รับอย่างมีประสิทธิภาพและมีประสิทธิผล

• ความมั่นใจในการปฏิบัติตามกฎหมาย ระเบียบข้อบังคับ หรือมาตรฐานอุตสาหกรรมที่เกี่ยวข้อง

การกำกับดูแลด้านบริหารจัดการเทคโนโลยีดิจิทัล หรือธรรมาภิบาลด้านดิจิทัล (Digital Governance) เป็นการจัดการโครงสร้างองค์กรและโครงสร้างพื้นฐานทางด้านเทคโนโลยีดิจิทัล เพื่อสนับสนุนยุทธศาสตร์ เป้าหมายขององค์กร และยุทธศาสตร์ด้านดิจิทัล รวมทั้งสนับสนุนการดำเนินงานทางด้านเทคโนโลยีดิจิทัล ซึ่งเป็นกระบวนการที่สำคัญที่ช่วยองค์กรในการจัดสรรทรัพยากรสารสนเทศอย่างเหมาะสมสอดคล้องกับเป้าหมายพันธกิจขององค์กร รวมทั้งการบริหารความเสี่ยงด้านเทคโนโลยีดิจิทัล การสร้างความมั่นใจและความน่าเชื่อถือในระบบเทคโนโลยีดิจิทัลเพื่อใช้สนับสนุนการตัดสินใจ และการพิจารณาความคุ้มค่าของต้นทุนของการให้บริการและผลตอบแทนที่ได้รับอย่างมีประสิทธิภาพ และมีประสิทธิผลรวมทั้งสร้างความมั่นใจในการปฏิบัติตามกฎหมาย ระเบียบข้อบังคับที่เกี่ยวข้อง เพื่อให้เกิดการบูรณาการทั้งด้านกระบวนงานทางธุรกิจและเทคโนโลยีดิจิทัลที่เหมาะสมในการดำเนินการต่อไป

1.2 วัตถุประสงค์

การกำกับดูแลด้านการบริหารจัดการเทคโนโลยีดิจิทัล (Digital Governance guiding principle) จัดทำขึ้นเพื่อเป็นแนวทางปฏิบัติในการกำกับดูแลและบริหารจัดการทางด้านเทคโนโลยีสารสนเทศของ องค์กร โดยคำนึงถึงความต้องการของผู้มีส่วนได้ส่วนเสีย (Stakeholder) ในการสร้างคุณค่า (Value creation) จากการนำเทคโนโลยีสารสนเทศมาใช้ในการดำเนินงานขององค์กร

บทที่ 2 บทบาทหน้าที่ โครงสร้างองค์กร และการบริหารจัดการบุคลากรในการกำกับดูแลและบริหารจัดการเทคโนโลยีสารสนเทศระดับองค์กรที่ดี

2.1 บทบาทหน้าที่และความรับผิดชอบ

2.1.1 คณะกรรมการบริหารกิจการขององค์การสุรา

องค์ประกอบ คุณสมบัติ การแต่งตั้งคณะกรรมการบริหารกิจการองค์การสุราฯ

ตามระเบียบกระทรวงการคลังว่าด้วยการจัดตั้งองค์การสุรา กรมสรรพสามิต (ฉบับที่ 2) พ.ศ. 2541 กำหนดให้คณะกรรมการบริหารกิจการขององค์การสุราฯ ประกอบด้วย อธิบดีกรมสรรพสามิตเป็นประธานกรรมการโดยตำแหน่ง รองอธิบดีกรมสรรพสามิตผู้ซึ่งอธิบดีกรมสรรพสามิตมอบหมาย จำนวน 2 คน เป็นรองประธานกรรมการโดยตำแหน่ง ผู้อำนวยการองค์การสุราเป็นกรรมการและเลขานุการโดยตำแหน่ง และกรรมการอื่นอีกไม่น้อยกว่าสามคน แต่ต้องไม่เกินสิบเอ็ดคน ซึ่งในกรรมการอื่นนี้ให้มีผู้แทนกระทรวงการคลังเป็นกรรมการร่วมด้วยหนึ่งคนกรรมการอื่น รวมทั้งผู้แทนกระทรวงการคลังและที่ปรึกษาคณะกรรมการ รัฐมนตรีเป็นผู้แต่งตั้งและถอดถอน

ปัจจุบันคณะกรรมการบริหารกิจการขององค์การสุราฯ มีจำนวน 11 คน ประกอบด้วยผู้ที่มีความรู้ความสามารถ ทักษะและประสบการณ์การทำงานจากหลากหลายสาขาวิชาชีพ ซึ่งเป็นประโยชน์ต่อการดำเนินกิจการขององค์การสุราฯ

บทบาทและหน้าที่ความรับผิดชอบ

คณะกรรมการบริหารกิจการขององค์การสุราฯ มีอำนาจและหน้าที่วางนโยบายและควบคุมดูแลโดยทั่วไปซึ่งกิจการขององค์การสุราฯ และให้มีอำนาจและหน้าที่ ดังต่อไปนี้

1. วางระเบียบข้อบังคับต่าง ๆ เกี่ยวกับการบริหารงาน
2. วางระเบียบข้อบังคับว่าด้วยการบรรจุ การแต่งตั้ง การถอดถอน การเลื่อนขั้นเงินเดือน การตัดเงินเดือนการลดขั้นเงินเดือน และระเบียบวินัยของพนักงานสุรา ตลอดจนกำหนดอัตราตำแหน่ง อัตราเงินเดือนค่าจ้าง และเงินอื่น ๆ ของพนักงานสุรา
3. กำหนดอัตราค่าดอกเบี้ย ค่าภาระ ค่าบริการ และค่าดำเนินธุรกิจต่าง ๆ
4. กำหนดอัตราและดอกเบี้ยเงินสะสมของผู้อำนวยการและพนักงานสุรา และวางระเบียบการจ่ายคืนเงินสะสม
5. กำหนดราคามาตรฐานของผลิตภัณฑ์

ทั้งนี้ ต้องไม่เป็นการขัดต่อหรือนอกเหนือไปจากระเบียบแบบแผนของทางราชการ

2.1.2 คณะอนุกรรมกรรมการกำกับดูแลที่ดี การบริหารความเสี่ยง การปฏิบัติตามกฎ ระเบียบ (Governance Risk and Compliance : GRC)

บทบาทและหน้าที่ความรับผิดชอบ

1. ขับเคลื่อน กำกับ ควบคุม และประเมินผลในการกำกับดูแลที่ดี การบริหารความเสี่ยงและการควบคุมภายใน รวมถึงการจัดการผู้มีส่วนได้ส่วนเสียอย่างครบถ้วนและมีประสิทธิภาพและประสิทธิผล ให้เป็นไปตามโยบายภาครัฐ มติคณะรัฐมนตรี ยุทธศาสตร์ชาติ กฎหมาย ระเบียบ ข้อบังคับและนโยบายของคณะกรรมการบริหารกิจการขององค์การสุรา

2. กลั่นกรอง เสนอแนะ หรือให้คำปรึกษาต่อคณะกรรมการบริหารกิจการขององค์การสุราเกี่ยวกับนโยบายและแนวทางการแก้ปัญหา หรืออุปสรรคอื่นที่เกิดจากการดำเนินงานตามแผนการดำเนินงานและตัวชี้วัดต่อคณะกรรมการบริหารกิจการขององค์การสุรา

3. พิจารณาอนุมัติการจัดทำหรือทบทวนแผนแม่บท แผนปฏิบัติการ แผนการดำเนินงาน คู่มือ นโยบาย และรายละเอียดอื่น ๆ ตามหลักเกณฑ์การประเมินกระบวนการปฏิบัติงานและการจัดการ (Core Business Enablers) ของรัฐวิสาหกิจที่สำนักงานคณะกรรมการนโยบายรัฐวิสาหกิจกำหนดในคู่มือ State Enterprise Assessment Model: SE-AM ในหัวข้อการกำกับดูแลที่ดีและการนำองค์กร หัวข้อการบริหารความเสี่ยงและการควบคุมภายใน หัวข้อการมุ่งเน้นผู้มีส่วนได้ส่วนเสีย ติดตามผลการดำเนินงาน และรายงานผลการดำเนินงานต่อคณะกรรมการบริหารกิจการขององค์การสุราทราบอย่างน้อยเป็นรายไตรมาส

4. พิจารณาให้ความเห็นชอบนโยบายการบูรณาการในเรื่องการกำกับดูแลกิจการที่ดี การบริหารความเสี่ยง และปฏิบัติตามกฎ ระเบียบ (Governance Risk and Compliance: GRC) ก่อนนำเสนอคณะกรรมการบริหารกิจการขององค์การสุราพิจารณาอนุมัติและกำกับดูแลให้มีการดำเนินงานตานตามนโยบาย รวมทั้งทบทวนนโยบายดังกล่าวเป็นประจำทุกปี

5. ทบทวนกฎ ระเบียบ ข้อบังคับ และกฎบัตรที่เกี่ยวข้องกับการกำกับดูแลกิจการที่ดีการบริหารความเสี่ยงและควบคุมภายใน การบริหารจัดการผู้มีส่วนได้ส่วนเสีย

6. ไม่นำข้อมูลการดำเนินงานไปเปิดเผยต่อบุคคลภายนอกโดยไม่ได้รับอนุญาตจากองค์การสุราฯ

7. ดำเนินการอื่น ๆ ตามที่คณะกรรมการบริหารกิจการขององค์การสุรามอบหมาย

2.1.3 คณะอนุกรรมการเทคโนโลยี นวัตกรรม และดิจิทัล

บทบาทและหน้าที่ความรับผิดชอบ

1. ขับเคลื่อน กำกับ ควบคุม และประเมินผลด้านการบริหารจัดการเทคโนโลยี นวัตกรรม การจัดการความรู้ และดิจิทัล ให้เป็นไปตามนโยบายภาครัฐ มติคณะรัฐมนตรี ยุทธศาสตร์ชาติ กฎหมาย ระเบียบ ข้อบังคับ มติและนโยบายของคณะกรรมการบริหารกิจการขององค์การสุรา

2. กลั่นกรอง เสนอแนะ หรือให้คำปรึกษาต่อคณะกรรมการบริหารกิจการขององค์การสุรา เกี่ยวกับนโยบายและแนวทางการแก้ปัญหา หรืออุปสรรคอื่นที่เกิดจาการดำเนินงานตามแผนการดำเนินงานและตัวชี้วัดต่อคณะกรรมการบริหารกิจการขององค์การสุรา

3. ทบทวนกฎ ระเบียบ ข้อบังคับ และกฎบัตรที่เกี่ยวข้องกับเทคโนโลยี นวัตกรรม และดิจิทัล

4. พิจารณาและอนุมัติแผนแม่บท แผนการดำเนินงาน แผนปฏิบัติการ คู่มือ นโยบาย และรายละเอียดอื่น ๆ ตามหลักเกณฑ์การประเมินกระบวนการปฏิบัติงานและการจัดการ (Core Business Enablers) ของรัฐวิสาหกิจที่สำนักงานคณะกรรมการนโยบายรัฐวิสาหกิจกำหนดในคู่มือ State Enterprise Assessment Model : SE-AM ในหัวข้อการพัฒนาเทคโนโลยีดิจิทัล และหัวข้อการจัดการความรู้และนวัตกรรม และรายงานต่อคณะกรรมการบริหารกิจการขององค์การสุราทราบผลการดำเนินงานต่อไป

5. ปฏิบัติหน้าที่อื่นตามที่คณะกรรมการบริหารกิจการขององค์การสุรามอบหมาย

2.1.4 คณะกรรมการระบบบริหารความมั่นคงปลอดภัยสารสนเทศตามมาตรฐาน ISO/IEC 27001:2022 (ISMS Management Steering Committee: ISMC)

<u>บทบาทและหน้าที่ความรับผิดชอบ</u>

1. สนับสนุนการจัดทำระบบบริหารการรักษาความมั่นคงปลอดภัยสารสนเทศ (Information Security Management System: ISMS) ให้มีการดำเนินงานอย่างต่อเนื่อง ตามมาตรฐานISO/IEC 27001:2022

2. พิจารณานโยบายระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ วัตถุประสงค์ของระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ และเกณฑ์การวัดประสิทธิภาพของระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ

3. พิจารณาขอบเขตของระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ

4. พิจารณาเกณฑ์การประเมินความเสี่ยง และระดับความเสี่ยงด้านความมั่นคงปลอดภัยสำหรับสารสนเทศที่ยอมรับได้

5. พิจารณาผลการประเมินความเสี่ยง แผนจัดการความเสี่ยง และมาตรการควบคุมด้านความมั่นคงปลอดภัยสารสนเทศ

6. สนับสนุนทรัพยากรที่จำเป็นและสั่งการ เพื่อให้สามารถดำเนินงานตามมาตรการควบคุม และแผนจัดการความมั่นคงปลอดภัยสารสนเทศได้ตามกรอบที่กำหนด

7. ติดตามและประเมินผลการดำเนินงานของระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ

8. แต่งตั้งคณะทำงานพัฒนาระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศนายทะเบียนเอกสารระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ หรือคณะทำงานย่อยได้ตามความจำเป็นและเหมาะสม

2.1.5 คณะกรรมการกำกับดูแลด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์

<u>บทบาทและหน้าที่ความรับผิดชอบ</u>

1. จัดทำแนวทางในการดำเนินงานด้านการส่งสริมการรักษาความมั่นคงปลอดภัยทางไซเบอร์ วิเคราะห์ความเสี่ยงต่อการถูกคุกคามทางไซเบอร์จากกระบวนการปฏิบัติงานและทรัพย์สินทางสารสนเทศ

2. กำหนดแนวทางและมาตรการการป้องกันต่อการถูกคุกคามทางไซเบอร์ กำหนดแผนการดำเนินงานในการรับมือกับเหตุการณ์ เมื่อเกิดการคุกคามทางไซเบอร์ จะต้องมีแผนการดำเนินการกู้คืนของข้อมูลและทบทวนแผนการดำเนินงานเป็นประจำทุกปีเป็นอย่างน้อย เพื่อปรับแผนให้เหมาะสมกับเทคโนโลยีใหม่ ๆ

3. ติดตามเฝ้าระวังภัยคุกคามไซเบอร์อย่างต่อเนื่อง ติดตามข่าวสารภัยคุกคามที่เกิดขึ้นกับภายนอก เพื่อนำมาปรับใช้กับองค์การ และให้คำแนะนำกับพนักงานองค์การสุราฯ ปฏิบัติตามข้อกำหนดเกี่ยวกับการรักษาความมั่นคงปลอดภัยทางไซเบอร์ อย่างเคร่งครัด

4. ทบทวนกลไกการควบคุม และอนุมัติโครงการที่เกี่ยวข้องกับระบบรักษาความมั่นคงปลอดภัยทางไซเบอร์ โดยกำหนดเป็นคู่มือปฏิบัติกระบวนการหรือการอนุมัติให้ชัดเจน รองรับตามระเบียบปฏิบัติต่าง ๆ

5. ส่งเสริมให้มีการปรับปรุงระบบรักษาความปลอดภัยทางไซเบอร์ขององค์การสุรา กรมสรรพสามิต อย่างจริงจังและต่อเนื่อง

2.1.6 คณะทำงานคุ้มครองข้อมูลส่วนบุคคล องค์การสุรา กรมสรรพสามิต

<u>บทบาทและหน้าที่ความรับผิดชอบ</u>

1. ให้คำแนะนำและตรวจสอบการดำเนินงานให้การประมวลผลข้อมูลส่วนบุคคลเป็นไปตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

2. ประสานงานและให้ความร่วมมือกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

3. รักษาความลับที่ได้มาเนื่องจากการปฏิบัติหน้าที่

2.1.7 คณะทำงานระบบบริหารการรักษาความมั่นคงปลอดภัยสารสนเทศ (ISMS Working Team: IST)

1. จัดทำ พัฒนา ปรับปรุงและทบทวนเอกสารที่เกี่ยวข้องกับการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ

2. ประเมินความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ และจัดทำรายงานผลการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ

3. วิเคราะห์และกำหนดแนวทางในการจัดการความเสี่ยง และจัดทำแผนการจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ

4. สนับสนุนและดูแลบุคลากรให้ปฏิบัติตามแผนการจัดการความเสี่ยงด้านความความมั่นคงปลอดภัยสารสนเทศ

5. จัดทำและทบทวนแนวทางการประเมินผลการดำเนินงาน และวัดผลการดำเนินงานของระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ

6. สนับสนุนและผลักดันให้บุคลากรเข้าใจ และตระหนักถึงความมั่นคงปลอดภัยสารสนเทศ รวมทั้งสามารถปฏิบัติตามนโยบาย ขั้นตอนปฏิบัติงานและเอกสารที่เกี่ยวข้องในระบบบริหารความมั่นคงปลอดภัยสารสนเทศ (Information Security Management System: ISMS)

7. สนับสนุนการตรวจประเมินระบบมาตรฐานภายใน (Internal Audit) ของระบบบริหารความมั่นคงปลอดภัยสารสนเทศ (Information Security Management System: ISMS)

8. กำกับดูแล ติดตาม ให้คำปรึกษาและข้อแนะนำตลอดจนทบทวนประสิทธิภาพของการแก้ไขข้อบกพร่องและการปรับปรุงอย่างต่อเนื่องในระบบบริหารความมั่นคงปลอดภัยสารสนเทศ

9. รายงานผลการดำเนินงานต่อคณะกรรมการระบบบริหารความมั่นคงปลอดภัยสารสนเทศตามมาตรฐาน ISO/IEC 27001:2022 ((SMS Management Steering Committee: ISMC)

10. รายงานผลการดำเนินงานต่อคณะกรรมการกำกับดูแลด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์

2.1.8 คณะทำงานการพัฒนาเทคโนโลยีดิจิทัล

บทบาทและหน้าที่ความรับผิดชอบ

1. จัดทำ/ทบทวนแผนปฏิบัติการดิจิทัลระยะยาวและแผนปฏิบัติการประจำปีขององค์กร เพื่อให้สอดคล้องกับนโยบายของรัฐบาล และแผนพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคม รวมถึงบริบทการเปลี่ยนแปลงด้านดิจิทัลในยุคปัจจุบัน

2. ขับเคลื่อนให้มีการนำเทคโนโลยีดิจิทัลมาปรับใช้กับทุกส่วนขององค์กร และทุกส่วนของธุรกิจ ทั้งในส่วนของกระบวนการทำงาน การสร้างสรรค์ผลิตภัณฑ์ การตลาด วัฒนธรรมองค์กรและการกำหนดเป้าหมายการเติบโตในอนาคต เพื่อให้เกิดประสิทธิภาพในการดำเนินธุรกิจและสามารถรองรับการเปลี่ยนแปลงได้อย่างรวดเร็ว รวมถึงในการสร้างธุรกิจใหม่ ๆ รูปแบบบริการใหม่ ๆ ให้เกิดขึ้น ตลอดจนการบริหารโครงการและการดำเนินงานด้านเทคโนโลยีดิจิทัลอย่างมีประสิทธิภาพ และมีการบริหารจัดการด้านคุณภาพของการนำเทคโนโลยีดิจิทัลมาใช้

3. มีการบูรณาการเชื่อมโยงข้อมูล และการดำเนินงานร่วมกันระหว่างหน่วยงานต่าง ๆ ทั้งการเชื่อมโยงข้อมูลและการดำเนินงาน

4. มีการบริหารจัดการข้อมูลทุกขั้นตอน เพื่อให้การได้มาและการนำข้อมูลของหน่วยงานไปใช้ได้ถูกต้องครบถ้วน เป็นปัจจุบัน และสามารถเชื่อมโยงกันได้อย่างมีประสิทธิภาพและมั่นคงปลอดภัย โดยใช้ข้อมูลเป็นหลักในการขับเคลื่อนองค์กร

5. มีกระบวนการหรือการกระทำทั้งหมดที่จำเป็น เพื่อทำให้องค์กรปราศจากความเสี่ยงและความเสียหายที่มีผลต่อความปลอดภัยของข้อมูลและสารสนเทศ (Data and Information) ในทุกรูปแบบรวมถึงการระวังป้องกันต่อการอาชญากรรม การโจมตี การบ่อนทำลาย การจารกรรม และความผิดพลาดต่าง ๆ โดยคำนึงถึงองค์ประกอบพื้นฐานของความปลอดภัยของข้อมูล

6. มีกระบวนการที่ทำให้ธุรกิจสามารถดำเนินการได้อย่างต่อเนื่อง และการจัดการความเสี่ยงเมื่อเกิดเหตุการณ์ฉุกเฉินอันอาจมีผลกระทบต่อการให้บริการหรือผลิตภัณฑ์ที่สำคัญเพื่อเป็นการสร้างเสถียรภาพและความมั่นคงปลอดภัยเพื่อพร้อมรองรับการปฏิบัติงานได้อย่างต่อเนื่องและมีประสิทธิภาพเตรียมพร้อมรับมือกับเหตุการณ์ฉุกเฉินหรือสถานการณ์ผิดปกติ โดยที่มีการจัดทำแผนตอบสนองกับสถานการณ์ภัยพิบัติ (Incident Management Plan) และแผนกอบกู้สถานการณ์ภัยภัยพิบัติ (Business Continuity Plan) เพื่อการดำเนินธุรกิจอย่างต่อเนื่องและมีประสิทธิภาพ รวมถึงการบริหารจัดการความพร้อมใช้ของระบบต่าง ๆ ตามความต้องการของผู้ใช้บริการเพื่อให้ผู้ใช้บริการเกิดความมั่นใจในการบริการ

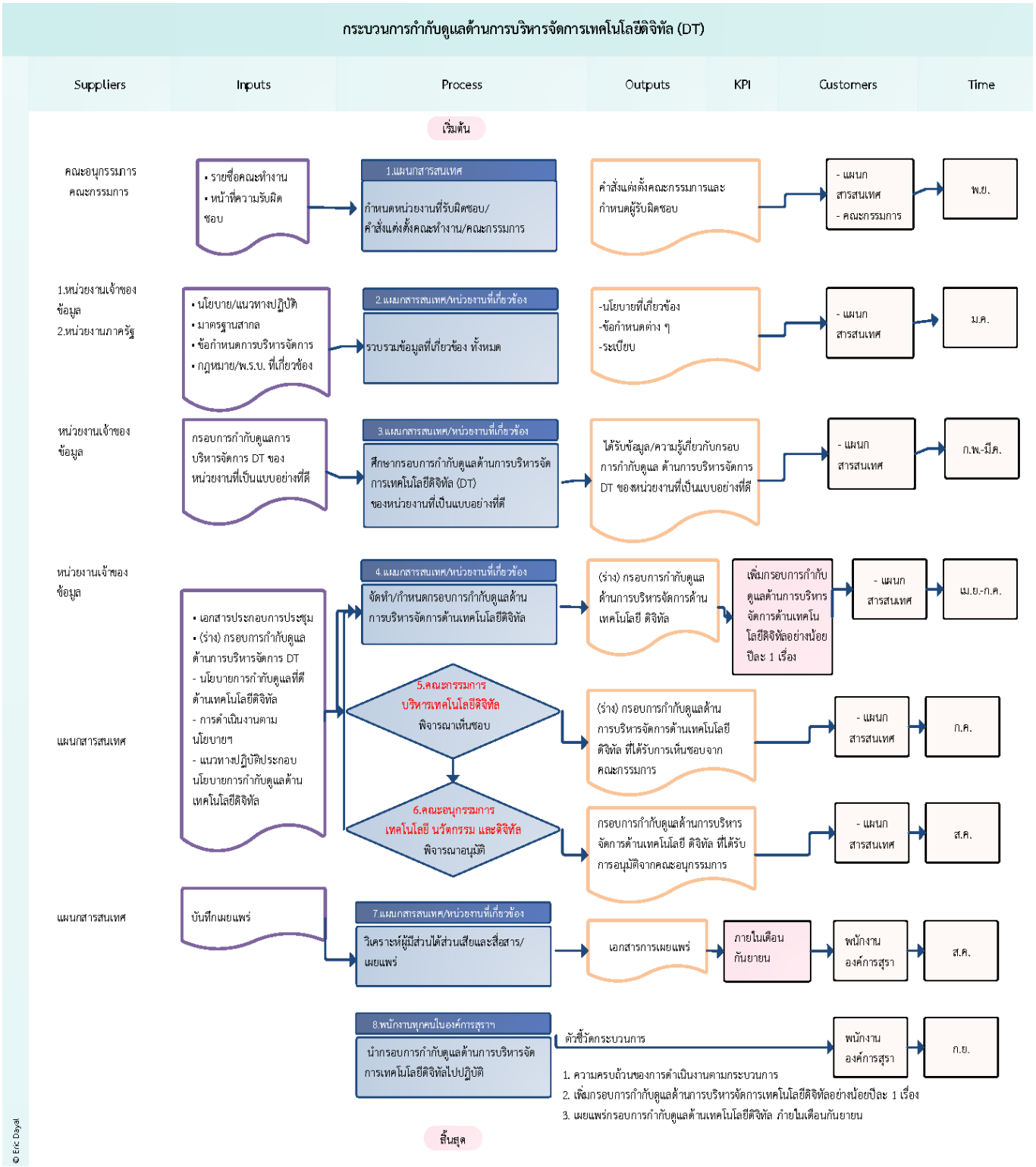
7. จัดให้องค์การสุราฯ มีกระบวนการบริหารจัดการการใช้ทรัพยากรด้านเทคโนโลยีดิจิทัลทั้งในส่วนของบุคลากร กระบวนการ และเทคโนโลยี เพื่อสนับสนุนวัตถุประสงค์ขององค์กรอย่างมีประสิทธิภาพ ด้วย

ต้นทุนที่เหมาะสม และมีความพร้อมต่อการเปลี่ยนแปลงในอนาคต รวมถึงการบริหารจัดการ การเลือกใช้เทคโนโลยีที่เป็นมิตรต่อสิ่งแวดล้อม เพื่อเพิ่มประสิทธิภาพในการจัดการการใช้พลังงานลดการใช้พลังงานลดการปล่อยก๊าซเรือนกระจก ลดการสร้างขยะ รวมถึงการนำขยะอิเล็กทรอนิกส์มารีไซเคิล

8. นำเสนอขออนุมัติงบลงทุนด้านดิจิทัลขององค์กร

9. ติดตาม ประเมิน และรายงานผลการดำเนินงานตามแผนปฏิบัติการต่อคณะอนุกรรมการที่ได้รับมอบหมายกำกับดูแล และคณะกรรมการบริหารกิจการขององค์การสุราฯ อย่างน้อยเป็นรายไตรมาส

บทที่ 3 กระบวนการกำกับดูแลที่ดีด้านเทคโนโลยีดิจิทัล

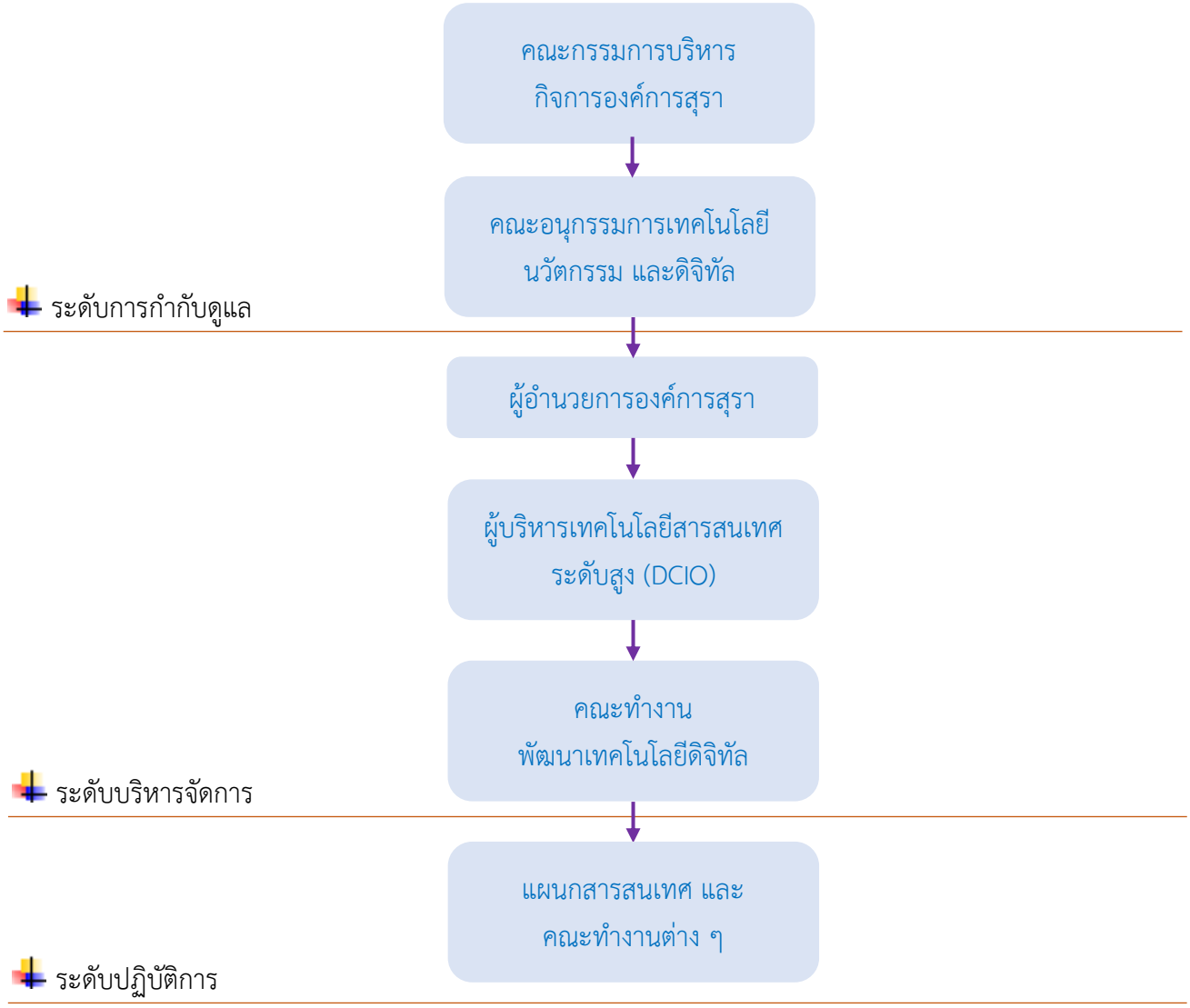


รูปที่ 1 กระบวนการกำกับดูแลด้านการบริหารจัดการเทคโนโลยีดิจิทัล

บทที่ 4 การกำกับดูแลด้านการบริหารจัดการทรัพยากรเทคโนโลยีดิจิทัลอย่างเหมาะสม

4.1 การกำหนดความรับผิดชอบด้านดิจิทัล (Responsibility)

องค์การสุรา กรมสรรพสามิตมีโครงสร้างการกำกับดูแลที่ดีด้านเทคโนโลยีดิจิทัล โดยมีระดับการกำกับดูแล ประกอบด้วย คณะกรรมการบริหารกิจการองค์การสุรา และคณะอนุกรรมการเทคโนโลยี นวัตกรรม และดิจิทัล ระดับบริหารจัดการ ประกอบด้วยผู้อำนวยการองค์การสุรา ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (DCIO) และคณะทำงานพัฒนาเทคโนโลยีดิจิทัล และระดับปฏิบัติงาน ขับเคลื่อนการดำเนินงาน



รูปที่ 2 โครงสร้างการกำกับดูแลที่ดีด้านเทคโนโลยีดิจิทัล

แผนกสารสนเทศ เป็นหน่วยงานหลักรับที่รับผิดชอบงานด้านพัฒนาเทคโนโลยีดิจิทัล ในการวางแผน กำหนดมาตรฐานเทคโนโลยีดิจิทัล กำหนดนโยบาย กลยุทธ์ แนวทางการพัฒนา ปรับปรุง ประยุกต์ใช้ระบบดิจิทัล จัดทำแผนแม่บท และปฏิบัติการด้านดิจิทัลระยะยาว และระยะสั้น จัดทำงบประมาณด้านเทคโนโลยีดิจิทัล พัฒนาระบบสารสนเทศเพื่อสนับสนุนการให้บริการทั้งภายในและภายนอกองค์กร บริหารจัดการด้านโครงสร้างพื้นฐานด้านเทคโนโลยีดิจิทัลและเครือข่ายสื่อสาร และสนับสนุนการใช้เทคโนโลยีสารสนเทศ โดยมีหน้าที่ความรับผิดชอบ คือ ควบคุม กำกับดูแลระบบคอมพิวเตอร์ และระบบเครือข่ายการสื่อสารข้อมูล พัฒนา ดูแล ปรับปรุง ระบบเว็บไซต์ และอินทราเน็ตขององค์การสุรา พัฒนา ดูแล ปรับปรุง ระบบงาน ERP ขององค์การสุรา จัดทำโครงการเกี่ยวกับการบริหารจัดการสารสนเทศ ตรวจสอบงานบริการด้านสารสนเทศ เพื่อนำเทคโนโลยีสารสนเทศมาใช้กับองค์กรได้อย่างเหมาะสมและปลอดภัย นำข้อมูลจากระบบสารสนเทศมาใช้ในการวิเคราะห์ สำหรับการสนับสนุนการตัดสินใจ กำกับดูแลระบบมาตรฐาน ISO/IEC 27001 และระบบมาตรฐานอื่น ๆ ที่เกี่ยวข้อง กำกับดูแลกฎหมายใหม่ ที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ เป็นต้น

องค์การสุรา กรมสรรพสามิต ได้กำหนดโครงสร้างในการกำกับดูแลที่ดีและบริหารจัดการด้านเทคโนโลยีดิจิทัล เพื่อส่งเสริมการบริหารจัดการองค์กรตามหลักธรรมาภิบาล (Corporate Governance) และสนับสนุนการดำเนินงานตามยุทธศาสตร์องค์กรอย่างมีประสิทธิภาพ ทั้งนี้ การดำเนินงานตามแผนงานจะต้องมีการจัดสรรทรัพยากรต่าง ๆ ได้แก่ คน เวลา งบประมาณ และเครื่องมือ เพื่อให้โครงการต่าง ๆ ที่กำหนดไว้ในแผนปฏิบัติการด้านดิจิทัลฯ สามารถสำเร็จลุล่วงได้อย่างมีประสิทธิภาพตลอดระยะเวลาของแผนปฏิบัติการด้านดิจิทัลฯ

4.2 การกำหนดกลยุทธ์ขององค์กรที่สอดคล้องกับความสามารถด้านเทคโนโลยีดิจิทัล (Strategy)

องค์การสุราฯ ตระหนักและให้ความสำคัญต่อการจัดทำแผนแม่บทและแผนปฏิบัติการด้านดิจิทัล องค์การสุรา กรมสรรพสามิต ปีงบประมาณ 2566 – 2570 (ฉบับทบทวนปี 2568) โดยมุ่งเน้นที่จะนำเทคโนโลยีดิจิทัลมาใช้เป็นเครื่องมือในการขับเคลื่อนการดำเนินธุรกิจขององค์กร เพื่อให้องค์การสุราฯ มีกรอบแนวทางในการใช้ประโยชน์จากเทคโนโลยีดิจิทัลอย่างเต็มศักยภาพในการพัฒนาโครงสร้างพื้นฐาน นวัตกรรม ข้อมูล บุคลากรและการให้บริการภาคประชาชนในการขับเคลื่อนการดำเนินงานขององค์กรให้สอดคล้องเป็นไปในทิศทางเดียวกันทั้งองค์กรและเป็นไปตามวิสัยทัศน์และพันธกิจขององค์กร พร้อมทั้งให้มีความสอดคล้องกับแนวทางการดำเนินงานขององค์กรตามแผนยุทธศาสตร์องค์การสุราฯ แผนพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคม และแผนพัฒนารัฐบาลดิจิทัลของประเทศไทย (พ.ศ. 2566 – 2570)

4.2.1 การวิเคราะห์ จุดอ่อน จุดแข็ง โอกาสและอุปสรรค ปัจจัยภายใน ภายนอก (SWOT Analysis)

SWOT ด้านดิจิทัล		คำอธิบาย	หลักฐานประกอบ
จุดแข็ง (Strength)	S1	มีกรอบการดำเนินงานด้านสารสนเทศและดิจิทัล ตามกรอบแผนแม่บทด้านดิจิทัล ระยะ 5 ปี ที่มีการทบทวนอย่างสม่ำเสมอ	มีแผนแม่บทด้านดิจิทัลฯ และแผนปฏิบัติการดิจิทัลฯ ที่มีแนวทางปฏิบัติอย่างเป็นระบบที่สามารถทำซ้ำได้ (Repeatable Practice) และเป็นมาตรฐาน (Standardized Practice) ที่มีความเชื่อมโยงและสอดคล้องกับแผนวิสาหกิจขององค์กร และนโยบายต่าง ๆ ที่สำคัญ โดยได้รับอนุมัติจากคณะกรรมการบริหารกิจการขององค์การสุรา
	S2	การริเริ่มสร้างนวัตกรรมทางธุรกิจ/ นวัตกรรมทางผลิตภัณฑ์ที่สนับสนุนการพัฒนาทางเศรษฐกิจและสังคมของประเทศ ตลอดจนการสร้างนวัตกรรมทางกระบวนการ	แผนวิสาหกิจ องค์การสุรา (SO 2 การเพิ่มขีดความความสามารถองค์กรด้วยเทคโนโลยีและนวัตกรรม)
	S3	มีระบบบริหารจัดการความปลอดภัยของข้อมูล ISO 27001 (Information Security Management System : ISMS)	ได้รับรองมาตรฐานจาก BSI เมื่อวันที่ 20 พฤษภาคม 2022
	S4	มีระบบการบริหารความต่อเนื่องทางธุรกิจ ISO 22301 (Business Continuity Management : BCM)	ได้รับรองมาตรฐานจาก BSI เมื่อวันที่ 20 พฤศจิกายน 2022
	S5	มีระบบบริหารจัดการคุณภาพ ISO 9001, FSSC 22000, GMP/HACCP และ ISO 14001	- ISO 14000 ได้รับรองมาตรฐานจาก SGS เมื่อวันที่ 8 สิงหาคม 2023 - FSSC 22000 ได้รับรองมาตรฐานจาก SGS เมื่อวันที่ 25 กรกฎาคม 2023 - ISO 9001 ได้รับรองมาตรฐานจาก SGS เมื่อวันที่ 15 กันยายน 2023 - GMP/HACCP ได้รับรองมาตรฐานจาก SGS เมื่อวันที่ 2 กันยายน 2022
	S6	การนำเทคโนโลยีดิจิทัลและนวัตกรรมมาเป็นเครื่องมือหลักในการขับเคลื่อน	แผนวิสาหกิจ องค์การสุรา (SO 2 การเพิ่มขีดความความสามารถองค์กรด้วยเทคโนโลยีและนวัตกรรม)
	S7	มีการใช้เครื่องมือในการวิเคราะห์ข้อมูลธุรกิจ (Business Analytics Tool) โดย Power BI	แผนปฏิบัติการ องค์การสุรา กรมสรรพสามิต ภายใต้โครงการพัฒนาศักยภาพการให้บริการด้านเทคโนโลยีสารสนเทศ

SWOT ด้านดิจิทัล		คำอธิบาย	หลักฐานประกอบ
	S8	มีการบูรณาการข้อมูลจากระบบสารสนเทศในระดับปฏิบัติการ เพื่อนำมาจัดทำเป็นรายงานประจำเชิงวิเคราะห์ แบบพลิกแพลงมุมมองหลายมิติ เพื่อสนับสนุนการตัดสินใจสำหรับผู้บริหาร	แผนปฏิบัติการ องค์การสุรา กรมสรรพสามิต ภายใต้โครงการพัฒนาศักยภาพการให้บริการด้านเทคโนโลยีสารสนเทศ
	S9	การพัฒนาระบบ ERP ที่กำหนดให้มีช่องทาง เช่น API เพื่อให้สามารถเชื่อมต่อข้อมูลจาก Sensor/IoT เข้ามาใช้ประกอบการดำเนินงาน รวมทั้งให้สามารถเชื่อมต่อ เพื่อนำข้อมูลจาก ระบบ ERP ออกไปใช้ประโยชน์ แบบ Realtime หรือ Near-Realtime มีลักษณะที่เป็น Workflow Management เพื่อให้สะดวกต่อการปรับเปลี่ยนกระบวนงาน รวมทั้งเพิ่ม-ลดแบบฟอร์มต่าง ๆ ที่เกี่ยวข้องในกระบวนงานตามลักษณะงานที่เปลี่ยนแปลงไป	แผนปฏิบัติการด้านดิจิทัล องค์การสุรา กรมสรรพสามิต
	S10	มีโครงการปรับเปลี่ยนพัฒนาบุคลากรสู่องค์กรดิจิทัล เพื่อส่งเสริมและพัฒนาบุคลากรให้เปิดรับการเปลี่ยนแปลงทางเทคโนโลยี	แผนวิสาหกิจ องค์การสุรา (SO 3 การสร้างคุณค่าให้สังคมและเป็นมิตรกับสิ่งแวดล้อม)
จุดอ่อน (Weakness)	W1	ระบบรักษาความมั่นคงปลอดภัยทางสารสนเทศ ยังจำเป็นต้องมีการพัฒนาเพิ่มเติมให้สามารถรองรับ การโจมตีทางไซเบอร์ในรูปแบบต่าง ๆ รวมทั้งยังจำเป็นต้องยกระดับการจัดการข้อมูลและระบบการบริหารงานให้ต่อเนื่องภายใต้เหตุวิกฤต	เนื่องในปัจจุบันการโจมตีทางไซเบอร์มีการพัฒนาไปพร้อมกับการเปลี่ยนแปลงของเทคโนโลยี จึงมีการนำเครื่องมือใหม่ ๆ หรือคิดค้นกลยุทธ์ใหม่ ๆ เพื่อเข้าถึงระบบโดยไม่ได้รับอนุญาต
	W2	การขาดศักยภาพด้านเทคโนโลยีและนวัตกรรม กฎ ระเบียบ ข้อบังคับต่าง ๆ ภายในองค์การสุราฯ ที่ล้าสมัยและไม่เป็นปัจจุบัน ส่งผลต่อความคล่องตัวและประสิทธิภาพในการดำเนินงาน	พนักงานส่วนมากเป็น Gen X และใกล้เกษียณอายุงาน ไม่สามารถปรับตัวในการใช้เทคโนโลยี รวมถึงพนักงานที่อยู่ในสายการผลิต ไม่มีเวลาเข้าร่วมการอบรม

SWOT ด้านดิจิทัล		คำอธิบาย	หลักฐานประกอบ
	W3	ยังมีขีดความสามารถที่จำกัดในการใช้ประโยชน์จาก Big Data Analytics และ Social Network ในการรับรู้ความต้องการ ความคาดหวัง รวมทั้งการสื่อสารไปยังลูกค้าและกลุ่มเป้าหมาย	พนักงานส่วนใหญ่ยังขาดความรู้ และกระบวนการในนำข้อมูลมาวิเคราะห์ เพื่อเผยแพร่ไปยังผู้มีส่วนได้ส่วนเสีย
	W4	ยังอยู่ในช่วงของการริเริ่มเพื่อพัฒนาระบบ Sensor และระบบเครือข่ายสื่อสารข้อมูลรองรับ Industry 4.0& Smart Office เพื่อให้สามารถนำข้อมูลแบบ Realtime มาเพิ่มศักยภาพในการตัดสินใจ รวมทั้งสามารถนำมาสู่การวิเคราะห์และใช้งานร่วมกันเพื่อสร้างคุณค่าทางการบริหารจัดการ	แผนปฏิบัติการด้านดิจิทัล องค์การสุรา กรมสรรพสามิต เริ่มดำเนินโครงการในปี 2570
	W5	อุปกรณ์สารสนเทศมีอายุการใช้งานมานาน ทำให้ประสิทธิภาพของอุปกรณ์ลดลง	อุปกรณ์สารสนเทศบางรายการมีระยะเวลาในการใช้งานมานาน
	W6	งบประมาณขององค์กรยังไม่เพียงพอต่อการพัฒนางานด้านเทคโนโลยีดิจิทัล	เนื่องจากสภาพคล่องขององค์การสุรา จึงมีการจำกัดงบประมาณในการลงทุนเทคโนโลยีหรือระบบใหม่ ๆ โดยจัดงบประมาณสำหรับที่จำเป็นต้องทำเท่านั้น
	W7	กระบวนการในการวิเคราะห์สถาปัตยกรรมองค์กรยังไม่ชัดเจน	ยังขาดทักษะในการวิเคราะห์สถาปัตยกรรมองค์กร
โอกาส (Opportunity)	O1	นโยบายรัฐ สนับสนุนการพัฒนาทางด้านดิจิทัล เพื่อเศรษฐกิจและสังคม รวมทั้งการพัฒนาทางนวัตกรรม	รัฐบาลมีการขับเคลื่อนการพัฒนาดิจิทัลที่เป็นประโยชน์ต่อธุรกิจขององค์การสุรา ทั้งในเชิงนโยบาย กฎหมายระเบียบรองรับ และแนวปฏิบัติ
	O2	แนวโน้มการเติบโตของอุตสาหกรรมอาหาร อุตสาหกรรมยาและเวชภัณฑ์ รวมทั้งอุตสาหกรรมผลิตภัณฑ์ใช้กับร่างกาย อุตสาหกรรมเครื่องมือ เครื่องจักร อุปกรณ์อิเล็กทรอนิกส์/ห้องแล็บ	นโยบายการพัฒนารัฐบาลดิจิทัลของประเทศไทย ที่ให้ความสำคัญกับการเพิ่มขีดความสามารถทางการแข่งขันทางเศรษฐกิจ
	O3	การสร้างความร่วมมือกับหน่วยงานของรัฐและเอกชน	การลงนามบันทึกข้อตกลงความร่วมมือทางวิชาการ (MOU) ระหว่างหน่วยงานต่าง ๆ
	O4	การเติบโตของธุรกิจ Logistic และ Digital Services ที่สร้างความสะดวกให้กับผู้จำหน่ายและผู้บริโภคมากยิ่งขึ้น	แนวโน้มธุรกิจ/อุตสาหกรรม ปี 2566-2568: ธุรกิจบริการดิจิทัลและซอฟต์แวร์

SWOT ด้านดิจิทัล		คำอธิบาย	หลักฐานประกอบ
ภัยคุกคาม (Threat)	T1	ระบบรักษาความมั่นคงปลอดภัยทางสารสนเทศ ยังจำเป็นต้องมีการพัฒนาเพิ่มเติมให้สามารถรองรับ การโจมตีทางไซเบอร์ในรูปแบบต่าง ๆ รวมทั้งยังจำเป็นต้องยกระดับการจัดการข้อมูลและระบบการบริหารงานให้ต่อเนื่องภายใต้เหตุวิกฤต	เนื่องในปัจจุบันการโจมตีทางไซเบอร์มีการพัฒนาไปพร้อมกับการเปลี่ยนแปลงของเทคโนโลยี จึงมีการนำเครื่องมือใหม่ ๆ หรือคิดค้นกลยุทธ์ใหม่ ๆ เพื่อเข้าถึงระบบโดยไม่ได้รับอนุญาต
	T2	การเปลี่ยนแปลงและพัฒนาที่รวดเร็วของเทคโนโลยี รวมทั้งรูปแบบการลงทุนในแบบต่าง ๆ	Digital Transformation สู่บริบทธุรกิจยุคใหม่
	T3	การเผชิญการแข่งขันจากคู่แข่งในธุรกิจเดียวกันและสินค้านำเข้าที่เข้ามาตีตลาด	SWOT แผนวิสาหกิจ องค์การสุรา พ.ศ. 2566-2570

4.2.2 ผลการวิเคราะห์โดยใช้หลักการ TOWS Matrix

เมื่อนำผลการวิเคราะห์จุดแข็ง จุดอ่อน โอกาส และอุปสรรคดังกล่าว มาวิเคราะห์ด้วยเครื่องมือ TOWS Matrix เพื่อสังเคราะห์และกำหนดแนวทางการพัฒนาเศรษฐกิจ สังคมดิจิทัล และนวัตกรรม องค์การสุรากรมสรรพสามิต โดยจำแนกเป็น

- สถานการณ์ที่ 1 (จุดแข็ง-โอกาส) สถานการณ์นี้เป็นสถานการณ์ที่พึงปรารถนาที่สุดควรกำหนดกลยุทธ์ในเชิงรุก (Aggressive –Strategy) เพื่อดึงเอาจุดแข็งที่มีอยู่มาเสริมสร้างและปรับใช้และฉกฉวยโอกาสต่าง ๆ ที่เปิดมาหาประโยชน์อย่างเต็มที่

- สถานการณ์ที่ 2 (จุดอ่อน-โอกาส) สถานการณ์ที่สะท้อนให้เห็นถึงโอกาสที่เป็นข้อได้เปรียบอยู่หลายประการแต่ติดขัดตรงที่มีปัญหาอุปสรรคจากปัจจัยภายนอกอยู่เช่นกันดังนั้น ทางออก คือ กลยุทธ์การพลิกตัว (Turnaround-oriented Strategy) เพื่อขจัดหรือแก้ไขจุดอ่อนภายในต่าง ๆให้พร้อมที่จะฉกฉวยโอกาสต่าง ๆ ที่เปิดให้

- สถานการณ์ที่ 3 (จุดแข็ง-อุปสรรค) สถานการณ์นี้เกิดขึ้นจากการที่สภาพแวดล้อมไม่เอื้ออำนวยต่อการดำเนินงานแต่ตัวองค์กรมีข้อได้เปรียบที่เป็นจุดแข็งหลายประการดังนั้นแทนที่จะรอจนกระทั่งสภาพแวดล้อมเปลี่ยนแปลงไปก็สามารถที่จะเลือกกลยุทธ์เพื่อใช้ประโยชน์จากจุดแข็งที่มีสร้างโอกาสในระยะยาวด้านอื่น ๆ

- สถานการณ์ที่ 4 (จุดอ่อน-อุปสรรค) สถานการณ์นี้เป็นสถานการณ์ที่เลวร้ายที่สุดเนื่องจากองค์กรกำลังเผชิญอยู่กับอุปสรรคจากภายนอกและมีปัญหาจุดอ่อนภายในหลายประการดังนั้น ทางเลือกที่ดีที่สุด คือ กลยุทธ์การตั้งรับหรือป้องกันตัว (Defensive Strategy) เพื่อพยายามลดหรือหลบหลีกภัยอุปสรรคต่างๆที่คาดว่าจะเกิดขึ้นตลอดจนหามาตรการที่จะทำให้องค์กรเกิดความสูญเสียที่น้อยที่สุด

รูปที่ 3 TOWS Matrix

4.2.3 วิสัยทัศน์ และยุทธศาสตร์ แผนแม่บทด้านดิจิทัล องค์การสุรา ประจำปี 2566-2570

วิสัยทัศน์: “พัฒนานวัตกรรม ยกระดับโครงสร้างพื้นฐานด้านดิจิทัลและประยุกต์ใช้เทคโนโลยีดิจิทัล เพื่อยกระดับองค์กรด้วย Digital Transformation”

วัตถุประสงค์เชิงยุทธศาสตร์

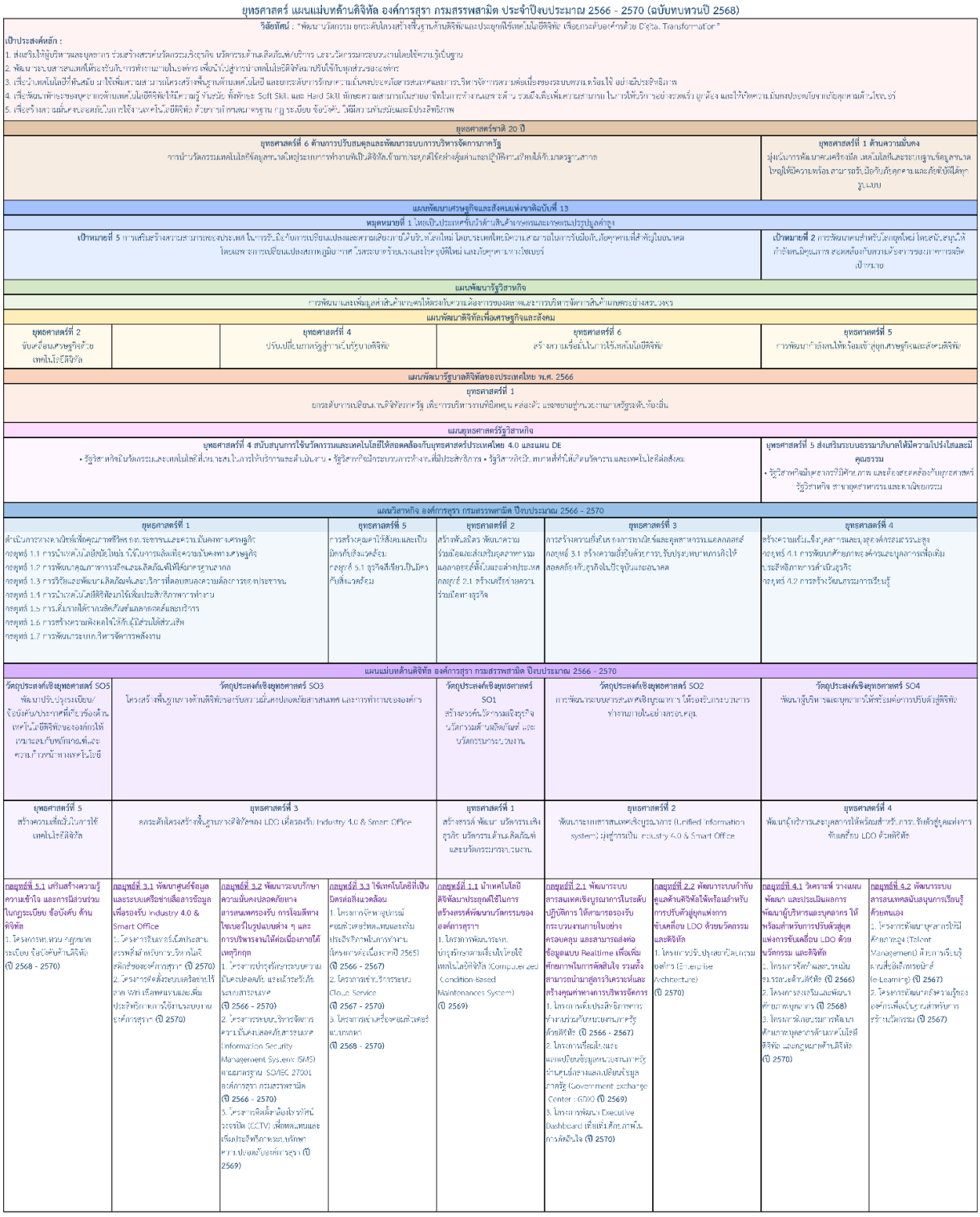
SO 1 สร้างสรรค์นวัตกรรมเชิงธุรกิจ นวัตกรรมด้านผลิตภัณฑ์ และนวัตกรรมกระบวนงาน

SO 2 การพัฒนาระบบสารสนเทศเชิงบูรณาการ ให้รองรับกระบวนการทำงานภายในอย่างครอบคลุม

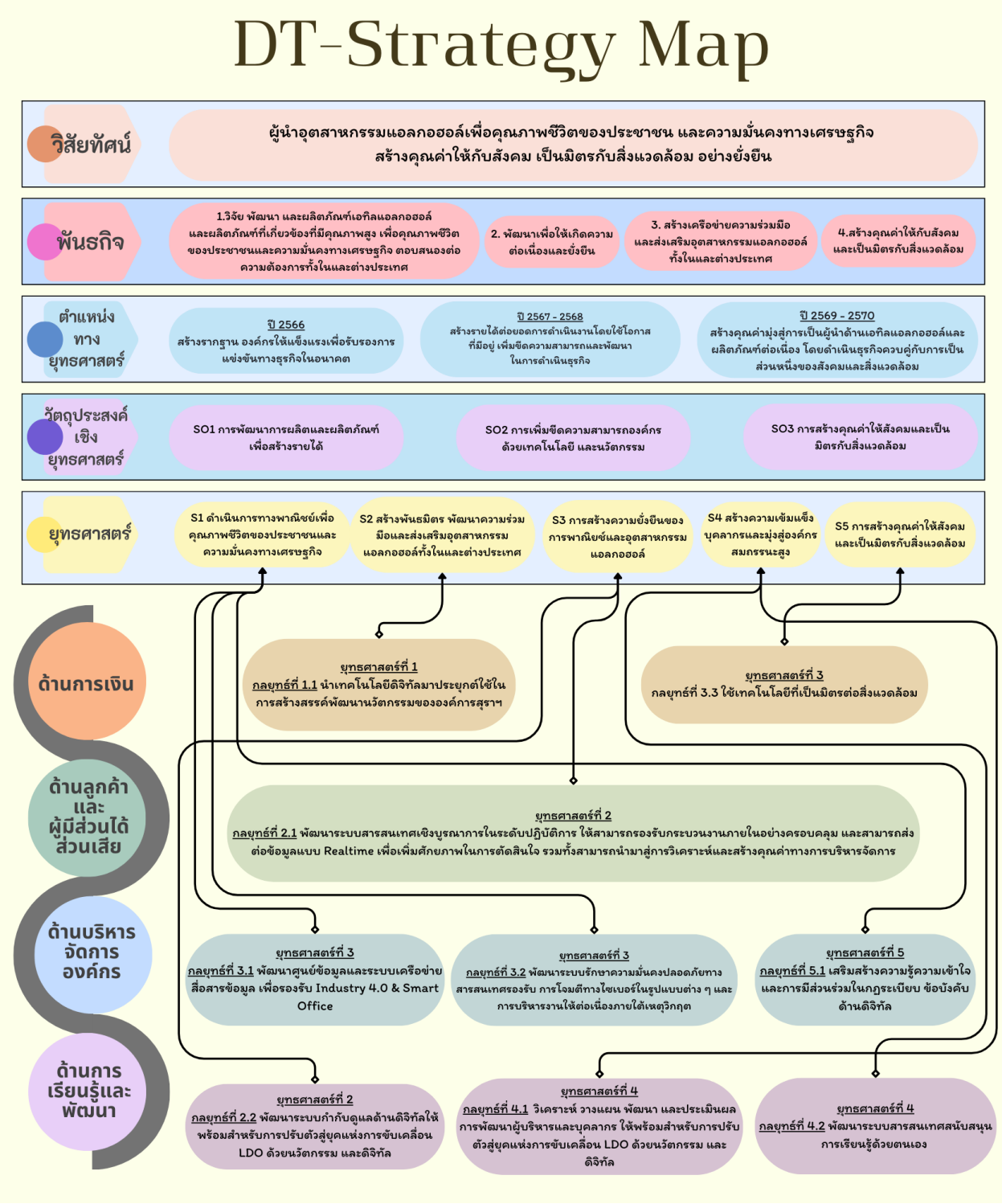
SO 3 โครงสร้างพื้นฐานทางด้านดิจิทัลรองรับความมั่นคงปลอดภัยสารสนเทศ และการทำงานขององค์กร

SO 4 พัฒนาผู้บริหารและบุคลากรให้พร้อมต่อการปรับตัวสู่ดิจิทัล

SO 5 พัฒนาปรับปรุงระเบียบ/ข้อบังคับ/ประกาศที่เกี่ยวข้องด้านเทคโนโลยีดิจิทัลขององค์กรให้เหมาะสมกับหลักเกณฑ์และความก้าวหน้าทางเทคโนโลยี



รูปที่ 3 แผนยุทธศาสตร์ของแผนแม่บทด้านดิจิทัล องค์การสุรา กรมสรรพสามิต พ.ศ. 2566-2570 (ฉบับทบทวนประจำปีงบประมาณ 2568)



รูปที่ 4 Strategy Map แผนแม่บทด้านดิจิทัลที่มีความเชื่อมโยงและความสอดคล้องในระดับกลยุทธ์ของแผนวิสาหกิจ องค์การสุรา พ.ศ. 2566-2570 ฉบับทบทวนประจำปีงบประมาณ 2568

4.3 การจัดซื้อจัดหา (Acquisition)

ตามที่ได้มีพระราชบัญญัติการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐ พ.ศ. 2560 และระเบียบกระทรวงการคลังว่าด้วยการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐ พ.ศ. 2560 เพื่อให้การดำเนินการจัดซื้อจัดจ้างของหน่วยงานภาครัฐเป็นไปตามหลักธรรมาภิบาล ส่งเสริมให้ภาคประชาชนมีการตรวจสอบการจัดซื้อจัดจ้างภาครัฐ มีแนวทางการจัดซื้อจัดจ้างมีความชัดเจนและรัดกุม และเพื่อรองรับการดำเนินงานให้เป็นไปตามกฎหมาย ระเบียบที่เกี่ยวข้อง องค์การสุราจึงได้กำหนดขั้นตอนการดำเนินงานจัดซื้อจัดจ้าง โดยมีวัตถุประสงค์เพื่อใช้เป็นแนวทางในการปฏิบัติเกี่ยวกับการจัดซื้อจัดจ้าง เพื่อให้การจัดซื้อจัดจ้างเกิดประโยชน์สูงสุด และเพื่อให้เป็นไปตามพระราชบัญญัติการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐ พ.ศ. 2560 ด้วยความคุ้มค่าโปร่งใส มีประสิทธิภาพและประสิทธิผล ตรวจสอบได้ ซึ่งประกอบด้วย การจัดทำแผนการจัดซื้อจัด การจัดทำร่างขอบเขตของงานฯ รายงานขอซื้อหรือขอจ้าง แต่งตั้งคณะกรรมการซื้อหรือจ้าง วิธีการซื้อหรือจ้าง การทำสัญญา เป็นต้น

ในการจัดซื้อจัดหา องค์การสุราพิจารณาถึงขีดความสามารถและแผนการดำเนินงานด้านเทคโนโลยีดิจิทัล ทั้งในปัจจุบันและอนาคต เพื่อตอบสนองความต้องการตามยุทธศาสตร์ขององค์กร โดยผู้รับผิดชอบการกำกับดูแลมอบหมาย สั่งการให้มีการพัฒนาด้านเทคโนโลยีดิจิทัล ให้สอดคล้องกับยุทธศาสตร์ แผนแม่บทและแผนปฏิบัติการด้านดิจิทัลขององค์การสุราไปใช้ในการปฏิบัติงานจริง เพื่อให้มั่นใจได้ว่าองค์กรได้รับประโยชน์สูงสุดจากการพัฒนาด้านเทคโนโลยีดิจิทัล รวมทั้งคณะอนุกรรมการเทคโนโลยีฯ ต้องมีการอนุมัติเห็นชอบแผนแม่บทและแผนปฏิบัติการด้านดิจิทัลฯ เพื่อให้แผนกสารสนเทศสามารถดำเนินการของบประมาณประจำปีได้ตามแผนที่ได้รับการอนุมัติ พร้อมทั้งส่งเสริมให้แผนกสารสนเทศซึ่งมีหน้าที่รับผิดชอบด้านการจัดการเทคโนโลยีดิจิทัล นำเสนอแผนการดำเนินงานการพัฒนาด้านเทคโนโลยีดิจิทัล เพื่อให้ทันต่อการเปลี่ยนแปลงของเทคโนโลยี และติดตามผลการดำเนินงานด้านเทคโนโลยีดิจิทัล ให้เป็นไปตามเป้าหมายที่กำหนดไว้ในข้อเสนอตามแผนงาน โดยมีการประชุมคณะอนุกรรมการเทคโนโลยีฯ ที่เพื่อรายงานผลการดำเนินงาน ติดตามสถานะความคืบหน้าของแผนงานด้านเทคโนโลยีดิจิทัลตามที่ได้รับอนุมัติอย่างต่อเนื่อง เพื่อให้มั่นใจได้ว่าข้อเสนอแผนงานนั้นได้ดำเนินการตามวัตถุประสงค์ภายใต้กรอบเวลาและทรัพยากรตามที่ได้รับจัดสรรไว้อย่างเหมาะสม

ในการจัดหา การพัฒนา และการบำรุงรักษาระบบสารสนเทศ แผนกสารสนเทศจะต้องดำเนินการตาม ขั้นตอนการดำเนินงานจัดซื้อจัดจ้าง (P-SPS-001) อาทิเช่น การจัดทำร่างขอบเขตของงานหรือรายละเอียดคุณลักษณะเฉพาะของพัสดุหรือแบบรูปรายงานก่อสร้าง ต้องดำเนินการตามพระราชบัญญัติการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐ พ.ศ.2560 และระเบียบกระทรวงการคลังว่าด้วยการจัดซื้อจัดจ้างและการบริหารพัสดุภาครัฐ พ.ศ.2560 เพื่อให้การดำเนินการจัดซื้อจัดจ้างของหน่วยงานภาครัฐเป็นไปตามหลักธรรมาภิบาล ส่งเสริมให้ภาคประชาชนมีการตรวจสอบการจัดซื้อจัดจ้างภาครัฐ มีแนวทางการจัดซื้อจัดจ้างมีความชัดเจนและรัดกุม และเพื่อรองรับการดำเนินงานให้เป็นไปตามกฎหมายระเบียบที่เกี่ยวข้อง

4.3.1 โครงสร้างการลงทุนด้านดิจิทัล

วัตถุประสงค์เชิงยุทธศาสตร์ (SO)	ยุทธศาสตร์ (S)	กลยุทธ์ (Tactic)
SO 1 สร้างสรรค์นวัตกรรมเชิงธุรกิจ นวัตกรรมด้านผลิตภัณฑ์ และนวัตกรรมกระบวนงาน	**ยุทธศาสตร์ที่ 1** สร้างสรรค์ พัฒนานวัตกรรมเชิงธุรกิจ นวัตกรรมด้านผลิตภัณฑ์ และนวัตกรรมกระบวนงาน	กลยุทธ์ 1.1 นำเทคโนโลยีดิจิทัลมาประยุกต์ใช้ในการสร้างสรรค์พัฒนานวัตกรรมขององค์การสุราฯ
SO 2 การพัฒนาระบบสารสนเทศเชิงบูรณาการ ให้รองรับกระบวนการทำงานภายในอย่างครอบคลุม	**ยุทธศาสตร์ที่ 2** พัฒนาระบบสารสนเทศเชิงบูรณาการ (Unified information system) มุ่งสู่การเป็น Industry 4.0 & Smart Office	กลยุทธ์ 2.1 พัฒนาระบบสารสนเทศเชิงบูรณาการในระดับปฏิบัติการ ให้สามารถรองรับกระบวนงานภายในอย่างครอบคลุม และสามารถส่งต่อข้อมูลแบบ Realtime เพื่อเพิ่มศักยภาพในการตัดสินใจ รวมทั้งสามารถนำมาสู่การวิเคราะห์และสร้างคุณค่าทางการบริหารจัดการ กลยุทธ์ 2.2 พัฒนาระบบกำกับดูแลด้านดิจิทัลให้พร้อมสำหรับการปรับตัวสู่ยุคแห่งการขับเคลื่อน LDO ด้วยนวัตกรรม และดิจิทัล
SO 3 โครงสร้างพื้นฐานทางด้านดิจิทัลรองรับความมั่นคงปลอดภัยสารสนเทศและการทำงานขององค์กร	**ยุทธศาสตร์ที่ 3** ยกระดับโครงสร้างพื้นฐานทางดิจิทัลของ LDO เพื่อรองรับ Industry 4.0 & Smart Office	กลยุทธ์ 3.1 พัฒนาศูนย์ข้อมูลและระบบเครือข่ายสื่อสารข้อมูล เพื่อรองรับ Industry 4.0 & Smart Office กลยุทธ์ 3.2 พัฒนาระบบรักษาความมั่นคงปลอดภัยทางสารสนเทศรองรับ การโจมตีทางไซเบอร์ในรูปแบบต่าง ๆ และการบริหารงานให้ต่อเนื่องภายใต้เหตุวิกฤต กลยุทธ์ 3.3 ใช้เทคโนโลยีที่เป็นมิตรต่อสิ่งแวดล้อม
SO 4 พัฒนาผู้บริหารและบุคลากรให้พร้อมต่อการปรับตัวสู่ดิจิทัล	**ยุทธศาสตร์ที่ 4** พัฒนาผู้บริหารและบุคลากรให้พร้อมสำหรับการปรับตัวสู่ยุคแห่งการขับเคลื่อน LDO ด้วยดิจิทัล	กลยุทธ์ 4.1 วิเคราะห์ วางแผน พัฒนา และประเมินผลการพัฒนาผู้บริหารและบุคลากรให้พร้อมสำหรับการปรับตัวสู่ยุคแห่งการขับเคลื่อน LDO ด้วยนวัตกรรม และดิจิทัล กลยุทธ์ 4.2 พัฒนาระบบสารสนเทศสนับสนุนการเรียนรู้ด้วยตนเอง
SO 5 พัฒนาปรับปรุงระเบียบ/ข้อบังคับ/ประกาศที่เกี่ยวข้องด้านเทคโนโลยีดิจิทัลขององค์กรให้เหมาะสมกับหลักเกณฑ์และความก้าวหน้าทางเทคโนโลยี	**ยุทธศาสตร์ที่ 5** สร้างความเชื่อมั่นในการใช้เทคโนโลยีดิจิทัล	กลยุทธ์ 5.1 เสริมสร้างความรู้ความเข้าใจและการมีส่วนร่วมในกฎระเบียบ ข้อบังคับด้านดิจิทัล

4.3.2 เกณฑ์การพิจารณาการจัดสรรทรัพยากร

ลำดับที่	หัวข้อเกณฑ์	ค่าน้ำหนัก	ระดับต่ำ (1)	ระดับกลาง (2)	ระดับสูง (3)
ทรัพยากรที่ไม่ใช่การเงินและอื่น ๆ ที่ต้องสนับสนุนแผนงาน / โครงการให้บรรลุเป้าหมาย					
1	ความสอดคล้องกับยุทธศาสตร์	25	อาจไม่สอดคล้องกับเป้าหมายหลักขององค์กรโดยตรง แต่ช่วยอำนวยความสะดวกในการทำงานส่วนบุคคล	สนับสนุนเป้าหมายรองหรือแผนปฏิบัติการของแผนกต่าง ๆ (Operational Plan)	เป็นโครงการเชิงยุทธศาสตร์ที่สนับสนุนเป้าหมายหลักขององค์กร (Strategic Goals) โดยตรง หรือเป็นโครงการที่จำเป็นเพื่อการเปลี่ยนแปลงองค์กร (Transformation)
2	ความเร่งด่วน	25	ไม่มีความเร่งด่วน สามารถรอได้ หรือนำไปพิจารณาเมื่อมีทรัพยากรเหลือ	มีความต้องการใช้งานแต่ยังสามารถรอได้ภายใน 3-6 เดือน โดยไม่เกิดความเสียหายร้ายแรงสามารถวางแผนดำเนินการในรอบการจัดสรรทรัพยากรปกติได้	ต้องดำเนินการทันทีหากล่าช้าจะสร้างความเสียหายร้ายแรงต่อองค์กร เช่น ภารกิจหลัก, ระบบงานหลักล่ม, การละเมิดความปลอดภัยของข้อมูล, หรือเกี่ยวข้องกับข้อบังคับทางกฎหมายที่ต้องปฏิบัติตาม
3	ผลกระทบที่ไม่ใช่ตัวเงิน	25	โดยพิจารณาจากการสอดคล้องไม่น้อยกว่า 1 หัวข้อ		
	ความปลอดภัยของพนักงาน	5	อุบัติเหตุจากการทำงาน	การเจ็บป่วยทุพพลภาพ	การเสียชีวิตของพนักงาน
	การรักษาระบบมาตรฐาน	5	มีข้อสังเกต	แก้ไข Minor Car	แก้ไข Major Car
	การผิดกฎหมาย/การผิดระเบียบ	5	ตรวจพบและสามารถแก้ไขได้เอง	ผิดกฎหมายหรือถูกลงโทษตามระเบียบของหน่วยงาน	ถูกฟ้องคดีหรือถูกปรับ
	การป้องกันข้อร้องเรียน	5	ป้องกันข้อร้องเรียนจากหน่วยงานภายงานภายในองค์กร	ป้องกันข้อร้องเรียนจากหน่วยงานภายนอก	ป้องกันข้อร้องเรียนจากผู้มีส่วนได้ส่วนเสีย (ภายในภายนอก)

ลำดับที่	หัวข้อเกณฑ์	ค่าน้ำหนัก	ระดับต่ำ (1)	ระดับกลาง (2)	ระดับสูง (3)
	ระยะเวลา	5	ช่วยให้การทำงานสำเร็จล่าช้าหรือไม่สำเร็จตามระยะเวลาที่กำหนด	ช่วยให้การทำงานสำเร็จตามระยะเวลาที่กำหนด	ช่วยให้การทำงานสำเร็จเร็วกว่าระยะเวลาที่กำหนด
4	ความรู้/ทักษะในปัจจุบันเพียงพอในการดำเนินแผนงาน/โครงการให้บรรลุ (ด้านทรัพยากรบุคคล)	5	พนักงานมีความเชี่ยวชาญและมีองค์ความรู้ไม่เพียงพอ	พนักงานมีความเชี่ยวชาญและมีองค์ความรู้ปานกลาง	พนักงานมีความเชี่ยวชาญและมีองค์ความรู้เพียงพอ
5	Hardware/Software ในปัจจุบันเพียงพอในการดำเนินแผนงาน/โครงการให้บรรลุ (ด้านเทคโนโลยี)	5	เป็นการนำเทคโนโลยีมาใช้เพื่อสนับสนุนการดำเนินงานขั้นพื้นฐาน โดยไม่มีการเปลี่ยนแปลงกระบวนการทำงานหลักอย่างมีนัยสำคัญ เช่น การใช้ซอฟต์แวร์สำนักงานสำหรับงานเอกสารทั่วไป, การใช้อีเมลและแอปพลิเคชันพื้นฐานเพื่อการสื่อสาร	เป็นการนำเทคโนโลยีมาใช้เพื่อปรับปรุงกระบวนการทำงานเดิมให้มีประสิทธิภาพมากขึ้น เช่น การใช้ระบบฐานข้อมูล (Database), การใช้ระบบเพื่อติดตามความคืบหน้าของงาน, การใช้แพลตฟอร์มการทำงานร่วมกัน (Collaboration Platform)	เป็นการใช้เทคโนโลยีเพื่อสร้างกระบวนการใหม่ ขององค์กร/โครงการ โดยเกี่ยวข้องกับการบูรณาการระบบที่ซับซ้อนและใช้เทคโนโลยีขั้นสูง เช่น การพัฒนาแอปพลิเคชันใหม่, การใช้ระบบ ERP เพื่อเชื่อมโยงหน่วยงานภายในองค์กรเข้าด้วยกัน, เพื่อความปลอดภัยขององค์กร, ปัญญาประดิษฐ์ (AI)
6	ความพร้อมของโครงการด้านกายภาพ	5	ต้องมีโครงการ/แผนงานที่เกี่ยวข้องด้านกายภาพเริ่มต้นก่อน	มีแผนงานที่เกี่ยวข้องด้านกายภาพดำเนินการและคาดการณ์เสร็จสิ้นตามแผนงาน	ดำเนินการได้ทันที
7	การควบคุมภายในและการประเมินความเสี่ยงระดับกิจกรรมของแผนดำเนินงาน (ด้านความเสี่ยงและควบคุมภายใน)	5	การประเมินกิจกรรมที่ไม่เพียงพอตั้งแต่ 5 กิจกรรมขึ้นไป	การประเมินกิจกรรมที่ไม่เพียงพอจำนวน 3-4 กิจกรรม	การประเมินกิจกรรมที่ไม่เพียงพอไม่เกิน 2 กิจกรรม

ลำดับที่	หัวข้อเกณฑ์	ค่าน้ำหนัก	ระดับต่ำ (1)	ระดับกลาง (2)	ระดับสูง (3)
8	แผนงานและโครงการที่มีผลกระทบต่อผู้มีส่วนได้ส่วนเสียและภาพลักษณ์องค์กร	5	ไม่ส่งผลกระทบต่อภาพลักษณ์ในสายตาสาธารณชนเลย หรืออาจมีเสียงวิจารณ์เชิงลบในกลุ่มปิดขนาดเล็กมาก ๆ ที่ไม่มีนัยสำคัญ	สร้างผลกระทบเชิงลบต่อภาพลักษณ์ในวงจำกัดอาจถูกพูดถึงในสื่อเฉพาะกลุ่ม (Niche Media) หรือในโซเชียลมีเดียแต่ไม่ขยายเป็นวงกว้าง สามารถแก้ไขได้ด้วยการสื่อสารและประชาสัมพันธ์ที่เหมาะสม	ทำให้ภาพลักษณ์และความน่าเชื่อถือขององค์กรเสียหายอย่างหนัก ข่าวถูกเผยแพร่ในสื่อกระแสหลัก (Mainstream Media) หรือกลายเป็นไวรัลในโซเชียลมีเดียในเชิงลบ ส่งผลกระทบต่อความสามารถในการแข่งขันและการดำเนินธุรกิจโดยตรง

ทั้งนี้ การดำเนินงานภายใต้ยุทธศาสตร์ปี 2566-2570 (ฉบับปรับปรุงปี 2568) ได้รับการอนุมัติเห็นชอบแผนแม่บทและแผนปฏิบัติการด้านดิจิทัลฯ จากคณะอนุกรรมการเทคโนโลยี นวัตกรรม และดิจิทัล ในการประชุมครั้งที่ 4/2567 เมื่อวันที่ 21 สิงหาคม 2567 และได้นำเสนอคณะกรรมการบริหารกิจการองค์การสุรา ในการประชุมครั้งที่ 11/2567 เมื่อวันที่ 30 กันยายน 2567 เป็นที่เรียบร้อย

4.3.3 การประเมินประสิทธิผล/คุ้มค่าของการลงทุนด้านเทคโนโลยีดิจิทัล

องค์การสุรา กำหนดให้มีการประเมินประสิทธิผลระบบสารสนเทศ และบริการงานของเทคโนโลยีสารสนเทศ เป็นประจำทุกปี โดยการประเมินประสิทธิผลระบบสารสนเทศ เพื่อวัดระบบสารสนเทศในมิติประสิทธิภาพการใช้งานระบบสารสนเทศ ความพร้อมใช้งาน ความถี่ และวัดความพึงพอใจการใช้งานระบบสารสนเทศ ส่วนการประเมินประสิทธิผลบริการด้านเทคโนโลยีสารสนเทศและการสื่อสาร วัดความพึงพอใจงานด้านการบริการ งานเครือข่ายสื่อสาร งานส่งมอบเครื่องคอมพิวเตอร์และอุปกรณ์คอมพิวเตอร์ งานซ่อมเครื่องคอมพิวเตอร์และอุปกรณ์ และงานสนับสนุนการใช้งระบบเทคโนโลยีสารสนเทศ

ในการประเมินความคุ้มค่าของการลงทุนด้านเทคโนโลยีดิจิทัล จะมีการประเมินการดำเนินโครงการตามเกณฑ์ในการพิจารณาการลงทุน พร้อมดำเนินการจัดลำดับความสำคัญของโครงการภายใต้แผนแม่บทด้านดิจิทัลฯ หรือแผนปฏิบัติการด้านดิจิทัลฯ ซึ่งเป็นขั้นตอนการพิจารณาถึงความสำคัญของโครงการที่ระบุไว้ในแผนแม่บทด้านดิจิทัลฯ โดยในแต่ละโครงการนั้นจะมีความสำคัญที่แตกต่างกันออกไป ประกอบกับทรัพยากรขององค์กรมีอยู่อย่างจำกัด ดังนั้น จึงต้องพิจารณาถึงความสำคัญที่มีความจำเป็นเร่งด่วนเพื่อคัดเลือกมาดำเนินงานก่อน โดยมีนิยามระดับความสำคัญ ดังนี้

- จำเป็นมาก : คะแนนรวมตามเกณฑ์พิจารณางบลงทุนตั้งแต่ 75 คะแนนขึ้นไป
- จำเป็น : คะแนนรวมตามเกณฑ์พิจารณางบลงทุนอยู่ระหว่าง 60 ถึง 74 คะแนน
- ควรดำเนินการ : คะแนนรวมตามเกณฑ์พิจารณางบลงทุน อยู่ระหว่าง 50 ถึง 59 คะแนน

4.4 หลักการจัดสรรทรัพยากรและขีดความสามารถขององค์กร

แผนปฏิบัติการด้านดิจิทัล องค์การสุราฯ ในแต่ละโครงการมีการใช้ทรัพยากรต่าง ๆ เช่น บุคลากร (เชิงปริมาณและคุณภาพ) งบประมาณ ฮาร์ดแวร์ ซอฟต์แวร์ รวมถึงระยะเวลาที่ใช้ในการพัฒนาและดำเนินโครงการไม่เท่ากัน ดังนั้น จึงกำหนดให้มีการจัดลำดับความสำคัญของโครงการ และการจัดสรรทรัพยากรด้านต่าง ๆ ดังนี้

1. <u>หลักเกณฑ์การจัดลำดับความสำคัญของโครงการตามแผนปฏิบัติการด้านดิจิทัล องค์การสุรากรมสรรพสามิต ประจำปี 2566 – 2570 (ฉบับทบทวนปี 2568)</u>

ใช้หลักเกณฑ์การพิจารณาการลงทุนในการประเมินโครงการทุกโครงการในแผน โดยนำคะแนนรวมที่ได้จากการประเมิน แบ่งออกเป็น 3 ระดับ คือ

- จำเป็นเป็นมาก: คะแนนรวมตามเกณฑ์พิจารณางบลงทุนตั้งแต่ 75 คะแนนขึ้นไป
- จำเป็น: คะแนนรวมตามเกณฑ์พิจารณางบลงทุนอยู่ระหว่าง 60 ถึง 74 คะแนน
- ควรดำเนินการ: คะแนนรวมตามเกณฑ์พิจารณางบลงทุนอยู่ระหว่าง 50 ถึง 59 คะแนน

ซึ่งเมื่อได้คะแนนจากการประเมินเป็นที่เรียบร้อยแล้ว จะนำข้อมูลที่ได้มาจัดลำดับความสำคัญของโครงการในการดำเนินการก่อน - หลัง รวมถึงจัดลำดับตามทิศทางการดำเนินงานของแผนวิสาหกิจขององค์การสุรา

ปี 2566	ปี 2567	ปี 2568	ปี 2569	ปี 2570
❖ มีการนำเทคโนโลยีดิจิทัลและนวัตกรรมมาใช้ในการจำหน่ายและการเชื่อมต่อระหว่างหน่วยงานภาครัฐ ❖ มีการนำเทคโนโลยีมาใช้เพื่อการพัฒนาผลิตภัณฑ์และกระบวนการผลิต ❖ มีการนำระบบ Lean Management มาปรับกระบวนการทำงานเพื่อเพิ่มประสิทธิภาพและลดต้นทุน ❖ นำเทคโนโลยีดิจิทัลและนวัตกรรมมาสร้างความสัมพันธ์อันดีกับผู้มีส่วนได้ส่วนเสีย ❖ รับเป็นผู้ตรวจสอบผลิตภัณฑ์เอทานอลจากหน่วยงานภาครัฐ ❖ ปรับปรุงกระบวนการผลิตเพื่อลดต้นทุน	❖ พัฒนาระบบเทคโนโลยีดิจิทัลเพื่อปรับปรุงการทำงานและเพิ่มประสิทธิภาพในการให้บริการ ❖ บริหารจัดการการจำหน่ายผ่านช่องทางออนไลน์อย่างมีประสิทธิภาพ ❖ ขยายความร่วมมือกับหน่วยงานต่าง ๆ ในการพัฒนาสินค้าและบริการรวมถึงการสร้างสินค้าใหม่ที่ตอบสนองตลาด ❖ บริหารจัดการตลาดเชิงรุกในแนวราบและแนวตั้งอย่างสมดุล ❖ สร้างและสื่อสารแบรนด์ LDO ด้านการดูแลสังคมและสิ่งแวดล้อม	❖ พัฒนาระบบเทคโนโลยีดิจิทัลเพื่อปรับปรุงการทำงานและเพิ่มประสิทธิภาพในการให้บริการ ❖ พัฒนาธุรกิจโดยทำความร่วมมือทางการค้ากับหน่วยงานภาครัฐและเอกชน ❖ การขอเพิ่มชื่อหน่วยงานในกฎกระทรวงพัสดุที่รัฐต้องการส่งเสริมหรือสนับสนุน พ.ศ. ... ❖ พัฒนาระบบคุณภาพการผลิตแอลกอฮอล์ให้เป็นไปตามมาตรฐาน PIC/S GMP สำหรับโรงงานผลิตสารตั้งต้นทางยา (API) ❖ บริการวิเคราะห์ทดสอบแอลกอฮอล์และสุราบางชนิด ❖ มีผลการศึกษาวิจัยการผลิตแอลกอฮอล์จากวัตถุดิบทางเลือก	❖ มีการบูรณาการข้อมูลระหว่างหน่วยงานรัฐเพื่อเพิ่มประสิทธิภาพในการบริหารงาน ❖ กระบวนการผลิตได้รับรองมาตรฐานยา (GMP PIC/s) ❖ มีสินค้าใหม่ที่ได้รับการขึ้นทะเบียนเป็นสารตั้งต้นทางยา และเภสัชเคมีภัณฑ์ ❖ ต่อยอดการให้บริการวิเคราะห์ทดสอบแอลกอฮอล์และสุรา ❖ มีการปรับปรุงระบบผลิตแอลกอฮอล์ทำให้ได้ความบริสุทธิ์สูงขึ้น มีเสถียรภาพในฐานะธุรกิจต้นน้ำ ❖ เปลี่ยนชื่อองค์กรให้สอดคล้องกับภารกิจสำคัญทำให้ภาพลักษณ์องค์กรดีขึ้น ❖ ลดการปล่อยก๊าซเรือนกระจกจากการลดการใช้พลังงาน	❖ ปรับให้มีสภาพนิติบุคคลผ่านพระราชกฤษฎีกา ❖ เพิ่มบทบาทด้านการบริการสาธารณะ ❖ บริการรับรองคุณภาพสุราและแอลกอฮอล์ครอบคลุมทุกมาตรฐาน ❖ การประชาสัมพันธ์ภาพลักษณ์และผลิตภัณฑ์ ในกลุ่มอุตสาหกรรมยาและเวชภัณฑ์ ❖ ขยายช่องทางการขนส่งให้ครอบคลุมกลุ่มลูกค้า ❖ มีผลการศึกษาความเป็นไปได้ในการลงทุนผลิตแอลกอฮอล์จากวัตถุดิบทางเลือกและเข้าสู่ตลาดอุตสาหกรรมโลกใหม่

รูปที่ 5 ทิศทางการดำเนินงานตามแผนวิสาหกิจ 2566 - 2570

2. หลักเกณฑ์พิจารณาการขอตั้งงบประมาณครุภัณฑ์คอมพิวเตอร์ประจำปีงบประมาณ 2568

ทุกหน่วยงานต้องทำหนังสือบันทึกข้อความในการขอมีเครื่องคอมพิวเตอร์และอุปกรณ์ต่าง ๆ โดยดำเนินการขออนุมัติตามสายงาน ซึ่งมีเกณฑ์ที่ทุกหน่วยงานต้องพิจารณาเบื้องต้น ดังนี้

1. การขอมีเครื่องคอมพิวเตอร์ (PC / Notebook / Tablet) ประจำโต๊ะทำงานพิจารณาให้เฉพาะพนักงานที่ได้รับการบรรจุแต่งตั้งเป็นพนักงานองค์การสุราเท่านั้น ดังนี้

1.1 ผู้บริหารระดับ 8 ขึ้นไป (หัวหน้ากอง หัวหน้าฝ่าย รองผู้อำนวยการ และผู้อำนวยการ) ให้ใช้เครื่อง Tablet และคอมพิวเตอร์พกพา เพื่อให้สอดคล้องกับนโยบาย digital transformation และนโยบายรัฐบาลอิเล็กทรอนิกส์ โดยเริ่มใช้งานในปี 2565

1.2 พนักงานระดับ 1 – 7 พิจารณาจากสัดส่วนพนักงาน 1 คน ต่อเครื่อง (PC / Notebook) 1 เครื่อง ยกเว้น สายงานที่เกี่ยวกับงานด้านบริการ เช่น ซ่อมบำรุง ไอน้ำประปา เป็นต้น

1.3 มอบหมายให้แผนกสารสนเทศ กำกับดูแลและตรวจสอบทรัพย์สิน ICT และผู้ที่ได้รับอุปกรณ์ ICT ทุกท่าน จะต้องรับผิดชอบต่ออุปกรณ์และหากมีการสูญหายจะต้องรับผิดชอบภายใน 7 วัน โดยจะต้องนำอุปกรณ์ที่เทียบเท่าหรือดีกว่าส่งคืน

1.4 หากมีพนักงานลาออก ต้องดำเนินการจัดทำบันทึกข้อความสำหรับส่งคืนเครื่องคอมพิวเตอร์ทั้งหมด พร้อมนำเครื่องคอมพิวเตอร์มาส่งคืนยังแผนกสารสนเทศ

2. การขอมีอุปกรณ์คอมพิวเตอร์ต่าง ๆ (ขอใหม่) ต้องพิจารณาจากจำนวนอุปกรณ์เดิมที่หน่วยงาน มีใช้งาน ลักษณะงาน และ/หรือปริมาณงานที่เพิ่มขึ้น

3. การขอทดแทนเครื่องคอมพิวเตอร์และอุปกรณ์คอมพิวเตอร์เดิม จะต้องมีอายุการใช้งานมาแล้ว ไม่น้อยกว่า 5 ปี หรือกรณีที่เครื่องฯ เสีย/ชำรุดและมีการแจ้งซ่อมในระบบซึ่งแผนกสารสนเทศประเมินว่าไม่คุ้มค่าในการซ่อม รวมถึงปัจจุบัน ไม่มีอะไหล่ในการซ่อมและ/บริษัทฯ หยุดสายการผลิต

4. การขอมีโปรแกรมสำเร็จรูปเพิ่มเติม เพื่อใช้งานนอกเหนือจากโปรแกรมสำเร็จรูปในการผลิตเอกสาร หน่วยงานจะต้องชี้แจงเหตุผลความจำเป็นและลักษณะงานที่ต้องใช้โปรแกรมดังกล่าว พร้อมรายละเอียดของโปรแกรม รุ่น และราคา (โบว์ชัวร์/แผ่นพับ) เพื่อประกอบการพิจารณาในเบื้องต้น

5. ในกรณีที่มีการขอมีอุปกรณ์คอมพิวเตอร์ต่าง ๆ (ขอใหม่) การขอทดแทนเครื่องคอมพิวเตอร์และอุปกรณ์คอมพิวเตอร์เดิม และการขอมีโปรแกรมสำเร็จรูปเพิ่มเติม จะต้องผ่านการอนุมัติเห็นชอบจากคณะทำงานพัฒนาเทคโนโลยีดิจิทัล

3. หลักเกณฑ์การกำหนดมาตรฐานเครื่องคอมพิวเตอร์และอุปกรณ์ ICT

ใช้หลักเกณฑ์ราคากลางและคุณลักษณะพื้นฐานการจัดหาอุปกรณ์และระบบคอมพิวเตอร์ จากกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม

4.5 หลักเกณฑ์การจัดทำและการกำกับดูแลสถาปัตกรรมองค์กร

สถาปัตยกรรมองค์กร (Enterprise Architecture) หรือ EA คือแผนผังในภาพรวมขององค์กร เป็น การบูรณาการเทคโนโลยีดิจิทัลให้สอดคล้องกับกระบวนการการทำงาน (Business Process) หรือภารกิจขององค์กรอย่างเป็นระบบ ตั้งแต่ในระดับระดับนโยบาย ยุทธศาสตร์ นำไปสู่ทิศทางการขับเคลื่อน (Roadmap) ของ

องค์กร เพื่อเป็นเครื่องมือให้องค์กรสามารถวางแผนกลยุทธ์ หรือกำหนดแผนงานให้บรรลุตามวิสัยทัศน์ที่กำหนดไว้อย่างมีประสิทธิภาพ ประกอบด้วย 5 ด้าน ดังนี้

1. สถาปัตยกรรมด้านธุรกิจ (Business Architecture)
2. สถาปัตยกรรมด้านข้อมูล (Data Architecture)
3. สถาปัตยกรรมด้านระบบงาน (Application Architecture)
4. สถาปัตยกรรมด้านเทคโนโลยี (Technology Architecture)
5. สถาปัตยกรรมด้านการรักษาความปลอดภัย (Security Architecture)

สถาปัตยกรรมองค์กร (Enterprise Architecture) เป็นการนำหลักการปรับปรุงและพัฒนาองค์กรมาประยุกต์ใช้ ทั้งในด้านกระบวนการปฏิบัติงาน (Business Process) ระบบสารสนเทศ (Information Systems) และเทคโนโลยี (Technology) เพื่อขับเคลื่อนนโนบายและยุทธศาสตร์ไปสู่ภาคปฏิบัติ (Strategic Execution) ให้สัมฤทธิ์ผล ทั้งนี้การดำเนินงานตามสถาปัตยกรรมองค์กร ต้องมีการพัฒนาอย่างต่อเนื่องและปรับเปลี่ยนได้ตามบริบทการดำเนินงานที่สำคัญขององค์กร (Continuous Improvement)

4.6 การกำหนดนโยบายสนับสนุนการพัฒนาความรู้ความสามารถด้านดิจิทัลของบุคลากรในองค์กรและการสร้างวัฒนธรรมองค์กร

1. <u>แผนวิสาหกิจองค์การสุรา กรมสรรพสามิต ประจำปี 2566 – 2570 (ฉบับทบทวนปี 2568)</u>

ยุทธศาสตร์ที่ 4 สร้างความเข้มแข็งบุคลากรและมุ่งสู่องค์กรสมรรถนะสูง

กลยุทธ์ 4.1 การพัฒนาศักยภาพองค์กรและบุคลากรเพื่อเพิ่มประสิทธิภาพการดำเนินธุรกิจ

กลยุทธ์ 4.2 การสร้างวัฒนธรรมการเรียนรู้

2. <u>แผนแม่บทด้านดิจิทัล องค์การสุรา กรมสรรพสามิต ประจำปี 2566 – 2570 (ฉบับทบทวนปี 2568)</u>

ยุทธศาสตร์ที่ 4 พัฒนาผู้บริหารและบุคลากรให้พร้อมสำหรับการปรับตัวสู่ยุคแห่งการขับเคลื่อน LDO ด้วยดิจิทัล

กลยุทธ์ 4.1 วิเคราะห์ วางแผน พัฒนา และประเมินผลการพัฒนาผู้บริหารและบุคลากร ให้พร้อมสำหรับการปรับตัวสู่ยุคแห่งการขับเคลื่อน LDO ด้วยนวัตกรรม และดิจิทัล

กลยุทธ์ 4.2 พัฒนาระบบสารสนเทศสนับสนุนการเรียนรู้ด้วยตนเอง

ตัวชี้วัดที่ 1 จำนวนผู้บริหารและบุคลากรได้รับการพัฒนาตามแผนงาน อย่างน้อยร้อยละ 80

ตัวชี้วัดที่ 2 จำนวนผู้บริหารและบุคลากรผ่านการประเมิน/วัดผล อย่างน้อยร้อยละ 80

<u>3. แผนแม่บทด้านการบริหารและพัฒนาทุนมนุษย์ ปีงบประมาณ 2566–2570</u>

ยุทธศาสตร์ที่ 2 การสร้างและการพัฒนาทรัพยากรมนุษย์ เพื่อมุ่งสู่องค์กรที่มีสมรรถนะสูงอย่างยั่งยืน

กลยุทธ์ 2.1 ปรับรูปแบบการพัฒนาบุคลากร เพื่อสร้างมูลค่าเพิ่มและความได้เปรียบในการแข่งขัน

ตัวชี้วัดที่ 1 ร้อยละ 80 ของบุคลากรที่ผ่านประเมินสมรรถนะ

บทที่ 5 กรอบการกำกับดูแลด้านการดำเนินงานให้มีประสิทธิภาพและมีความโปร่งใส

องค์การสุราฯ ยึดหลักธรรมาภิบาล 6 ข้อ ในการดำเนินงาน การบริหารจัดการและปฏิบัติงานขององค์การสุราฯ ได้แก่

- หลักนิติธรรม
- หลักคุณธรรม
- หลักความโปร่งใส
- หลักความมีส่วนร่วม
- หลักความรับผิดชอบ
- หลักความคุ้มค่า

และให้กรรมการ ผู้บริหาร พนักงานและลูกจ้าง ยึดมั่นในหลักสำคัญของการกำกับดูแลกิจการที่ดีและการนำองค์กร ตามแนวทางของสำนักงานคณะกรรมการนโยบายรัฐวิสาหกิจ (สคร) ดังนี้

- ให้มีการกำกับดูแลกิจการที่ดี
- ให้มีการประกอบธุรกิจด้วยความเป็นธรรม
- ให้มีการเคารพสิทธิมนุษยชนและการปฏิบัติต่อผู้ปฏิบัติงานอย่างเป็นธรรม
- ให้มีความรับผิดชอบต่อผู้เข้าชมและผู้มาใช้บริการ
- ให้มีการร่วมพัฒนาชุมชนและสังคม
- ให้มีการดูแลรักษาอาคารสถานที่และสิ่งแวดล้อมโดยรอบ
- ให้มีการจัดทำรายงานด้านการช่วยเหลือสังคมและอนุรักษ์สิ่งแวดล้อม

และนำหลักปรัชญาเศรษฐกิจพอเพียงมาปรับใช้อย่างบูรณาการ โดยคำนึงถึงการดำเนินงานบนทางสายกลาง กล่าวคือ มีความพอประมาณ มีเหตุผล และมีภูมิคุ้มกันในตัวที่ดี บนพื้นฐานของความรู้ รอบคอบ ระมัดระวัง การมีคุณธรรม ซื้อสัตย์ สุจริต ขยัน อดทน มีสติปัญญา และแบ่งปัน

5.1 ความโปร่งใสต่อผู้มีส่วนได้ส่วนเสีย (Stakeholder Transparency)

เพื่อให้มั่นใจว่าการรายงานและการสื่อสารผลการดำเนินงานและบริหารจัดการเทคโนโลยีสารสนเทศกับผู้มีส่วนได้ส่วนเสียมีประสิทธิผลและทันเวลา การดำเนินงานโดยรวมควรมีการพัฒนาอย่างต่อเนื่องและวัตถุประสงค์รวมทั้งกลยุทธ์ ที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศมีความสอดคล้องกับแผนกลยุทธ์ขององค์กร ซึ่งแนวทางปฏิบัติที่ควรพิจารณามีดังนี้

(1) การประเมินความต้องการของผู้มีส่วนได้ส่วนเสียในการรายงานผลการดำเนินงานและบริหารจัดการเทคโนโลยีสารสนเทศ

- องค์กรควรพิจารณาข้อกำหนดด้านการรายงานภาคบังคับ (Mandatory Reporting) ทั้งในปัจจุบัน และอนาคตที่เกี่ยวข้องกับการใช้เทคโนโลยีสารสนเทศภายในองค์กร รวมทั้งขอบเขตและรอบระยะเวลา ในการรายงานที่เหมาะสม

- นอกเหนือจากประเด็นข้างต้น การรายงานยังอาจต้องพิจารณาถึงความต้องการด้านการรายงานสำหรับ ผู้มีส่วนได้ส่วนเสียอื่น ๆ ทั้งในปัจจุบันและอนาคต ที่เกี่ยวข้องกับการใช้เทคโนโลยีสารสนเทศในองค์กร รวมถึงขอบเขตและเงื่อนไขในการรายงานที่แตกต่างกัน

- องค์กรควรจัดให้มีหลักเกณฑ์การรายงานต่อผู้มีส่วนได้ส่วนเสียทั้งภายในและภายนอกองค์กร รวมทั้งรูปแบบและช่องทางการสื่อสารอย่างเหมาะสม

(2) การสื่อสารผลการดำเนินงานและบริหารจัดการเทคโนโลยีสารสนเทศที่เหมาะสม

- องค์กรควรมีการกำหนดกลยุทธ์ในการสื่อสารกับผู้มีส่วนได้ส่วนเสียทั้งภายในและภายนอกองค์กร

- ควรมีการกำหนดวิธีการสอบทานเพื่อให้มั่นใจว่าข้อมูลการรายงานเป็นไปตามหลักเกณฑ์สำหรับข้อกำหนด ของการรายงานภาคบังคับขององค์กรทั้งหมด

- ควรมีกระบวนการในการตรวจสอบความถูกต้องและอนุมัติรายงานภาคบังคับ

- มีกระบวนการ และลำดับชั้นการรายงาน

(3) การติดตามการสื่อสารกับผู้มีส่วนได้ส่วนเสีย

- องค์กรควรมีการประเมินความมีประสิทธิผลของการรายงานผลอย่างสม่ำเสมอเพื่อให้มั่นใจ ในความถูกต้องและความน่าเชื่อถือของรายงานภาคบังคับที่จัดทำขึ้น

- องค์กรควรมีการประเมินความมีประสิทธิผลของวิธีการสื่อสารและผลลัพธ์ของการสื่อสารกับผู้มีส่วนได้ส่วนเสียทั้งภายในและภายนอกองค์กร และประเมินว่าการสื่อสารดังกล่าวสามารถตอบสนอง ความต้องการของผู้มีส่วนได้ส่วนเสียที่หลากหลายอย่างครบถ้วน

5.2 การปฏิบัติตามกฎหมายระเบียบข้อบังคับที่เกี่ยวข้องกับการพัฒนาเทคโนโลยีดิจิทัล (Conformance)

องค์กรได้ปฏิบัติตามกฎหมาย ระเบียบข้อบังคับที่เกี่ยวข้องกับการพัฒนาเทคโนโลยีดิจิทัลทั้งภายในและภายนอกองค์กร เพื่อให้เกิดเป็นบรรทัดฐาน และแนวทางปฏิบัติร่วมกันอย่างเหมาะสม ดังนี้

(1) พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562

เนื่องจากปัจจุบันปัญหาเรื่องภัยคุกคามทางไซเบอร์ (Cyber Security) จะยังคงเติบโตอย่างต่อเนื่องตามเทคโนโลยีที่ทันสมัยมากขึ้น หน่วยงานภาครัฐจะยังคงเป็นเป้าหมายสำคัญในการโจมตีทางไซเบอร์จากผู้ไม่หวังดี ทั้งจากการโจมตีเพื่ออาศัยความน่าเชื่อถือของหน่วยงานภาครัฐมาใช้หลอกลวงประชาชนอีกต่อหนึ่ง และการโจมตีเพื่อทำลายความน่าเชื่อถือของหน่วยงาน ดังนั้น องค์กรจะต้องตระหนักถึงความสำคัญการเฝ้าระวัง และการปฏิบัติให้ถูกต้องตามมาตรการรักษาความมั่นคงปลอดภัยทางไซเบอร์ของหน่วยงานเพื่อป้องกันตนเองและหน่วยงานให้ปลอดภัยจากการถูกโจมตี นอกจากนี้การติดตามสถานการณ์ ด้านความมั่นคงปลอดภัยทางไซเบอร์ก็มีความสำคัญที่จะช่วยให้สามารถพร้อมรับมือกับภัยคุกคามใหม่ ๆ ที่เกิดขึ้นได้อย่างทันท่วงที

(2) พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลเป็นกฎหมายที่มีวัตถุประสงค์เพื่อการคุ้มครองสิทธิเกี่ยวกับข้อมูลส่วนบุคคลของประชาชนในฐานะเจ้าของข้อมูลส่วนบุคคล โดยกำหนดหน้าที่และความรับผิดชอบให้องค์กรปฏิบัติตามกฎหมาย บทบัญญัติใน พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล มีลักษณะพิเศษแตกต่างจากกฎหมายฉบับอื่น กล่าวคือ ไม่ได้มุ่งเน้นเพียงสภาพบังคับให้กระทำหรือไม่กระทำเท่านั้น แต่บทบัญญัติส่งเสริมการสร้างความตระหนักรู้ และการทบทวนกระบวนการทำงาน เพื่อให้การกระทำใดก็ตามที่เกี่ยวข้องกับข้อมูลส่วนบุคคลเป็นไปอย่างเหมาะสม โดยตระหนักถึงมาตรการด้านความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล ความเป็นธรรมในการใช้ข้อมูล และความโปร่งใสต่อเจ้าของข้อมูลส่วนบุคคล สอดคล้องกับวัตถุประสงค์ของกฎหมายในการคุ้มครองสิทธิความเป็นส่วนตัวภายใต้หลักการของรัฐธรรมนูญ

(3) พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2562

พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2562 ได้ประกาศใช้เมื่อวันที่ 15 เมษายน พ.ศ. 2562 เป็นพระราชบัญญัติที่ได้ทำการปรับปรุงเนื้อหาจากพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ (ฉบับที่ 1) พ.ศ. 2544 และพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ (ฉบับที่ 2) พ.ศ. 2551 โดยมีการเพิ่มอำนาจให้สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน)” หรือ ETDA ดำเนินการต่อธุรกิจบริการด้านธุรกิจกรรมอิเล็กทรอนิกส์ได้มากขึ้น ช่วยสนับสนุนการดูแลกิจการธุรกิจธุรกรรมดิจิทัล โดยมีสิทธิ์ออกใบอนุญาตประกอบกิจการธุรกรรมดิจิทัล ให้คำแนะนำในฐานะผู้กำกับดูแล รวมถึงมีหน้าที่ช่วยเพิ่มศักยภาพการบริการในธุรกิจนี้ผ่านการทำ Sandbox เพื่อพัฒนาเทคโนโลยีและกระบวนการใหม่ ๆ

(4) พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ.2560

เทคโนโลยีสารสนเทศแม้จะมีประโยชน์มากมายหากมีการนำมาใช้อย่างสร้างสรรค์ แต่ก็สามารถสร้างความเสียหายได้อย่างมากเช่นกัน หากมีการนำมาใช้อย่างไม่เหมาะสมและปัญหานี้มีแนวโน้มเพิ่มสูงขึ้นอย่างต่อเนื่อง เช่น การเจาะระบบ การส่งไวรัส การโจมตีระบบ การลงข้อมูลในระบบคอมพิวเตอร์ที่กระทบต่อความมั่นคงประเทศ เป็นต้น และหากการกระทำดังกล่าว มุ่งหวังสร้างความเสียหายต่อระบบคอมพิวเตอร์ภาครัฐด้วยแล้ว ผลกระทบจะไม่ได้จำกัดเพียงแค่ความเสียหายต่อบุคคลใดบุคคลหนึ่งเท่านั้น แต่อาจร้ายแรงและสร้างความเสียหายต่อเศรษฐกิจ สังคม และความมั่นคงของประเทศได้ พระราชบัญญัติฉบับนี้จึงมีวัตถุประสงค์เพื่อป้องกันควบคุมการกระทำผิดที่จะเกิดขึ้นได้จากการใช้คอมพิวเตอร์ และเนื่องจากพระราชบัญญัติฉบับเดิม มีการบังคับใช้เป็นเวลากว่า 10 ปี ที่ผ่านมาพบว่ากฎหมายมีปัญหาในการตีความ จนกระทบกับการบังคับใช้ เช่น การนำฐานความผิดที่ใช้กับเรื่องฉ้อโกงปลอมแปลงทางออนไลน์ ไปใช้กับการหมิ่นประมาท ทำให้กระทบต่อสิทธิเสรีภาพในการแสดงความคิดเห็น จนทำให้เกิดการโจมตีจากประชาคมโลก และเกิดกระแสสังคมเรียกร้องหลักประกันสิทธิเสรีภาพในการแสดงความคิดเห็นขึ้น

ทั้งนี้ สาระสำคัญของพระราชบัญญัติมีดังนี้

1. การฝากร้านใน Facebook, IG ถือเป็นสแปม

2. การส่ง SMS โฆษณา โดยไม่รับความยินยอม ให้ผู้รับสามารถปฏิเสธข้อมูลนั้นได้ ไม่เช่นนั้นถือเป็นสแปม

3. ส่ง Email ขายของ ถือเป็นสแปม

4. กด Like ได้ไม่ผิด พ.ร.บ.คอมพิวเตอร์ยกเว้นการกดไลค์ เป็นเรื่องเกี่ยวกับสถาบัน เสี่ยงเข้าข่ายความผิดมาตรา 112 หรือมีความผิดร่วม

5. กด Share ถือเป็นการเผยแพร่ หากข้อมูลที่แชร์มีผลกระทบต่อผู้อื่น อาจเข้าข่ายความผิดตามพ.ร.บ.คอมพิวเตอร์ฯ โดยเฉพาะที่กระทบต่อบุคคลที่ 3

6. พบข้อมูลผิดกฎหมายอยู่ในระบบคอมพิวเตอร์ของเรา แต่ไม่ใช่สิ่งที่เจ้าของคอมพิวเตอร์กระทำเองสามารถแจ้งไปยังหน่วยงานที่รับผิดชอบได้ หากแจ้งแล้วลบข้อมูลออกเจ้าของก็จะไม่มีความผิดตามกฎหมาย เช่น ความเห็นในเว็บไซต์ต่าง ๆ รวมไปถึง Facebook ที่ให้แสดงความคิดเห็น หากพบว่าการแสดงความเห็นผิดกฎหมาย เมื่อแจ้งไปที่หน่วยงานที่รับผิดชอบเพื่อลบได้ทันที เจ้าของระบบเว็บไซต์จะไม่มีความผิด

7. สำหรับ แอดมินเพจ ที่เปิดให้มีการแสดงความเห็น เมื่อพบข้อความที่ผิด พ.ร.บ.คอมฯ เมื่อลบออกจากพื้นที่ที่ตนดูแลแล้ว จะถือเป็นผู้พ้นผิด

8. ไม่โพสต์สิ่งลามกอนาจาร ที่ทำให้เกิดการเผยแพร่สู่ประชาชนได้

9. การโพสเกี่ยวกับเด็ก เยาวชน ต้องปิดบังใบหน้า ยกเว้นเมื่อเป็นการเชิดชู ชื่นชม อย่างให้เกียรติ

10. การให้ข้อมูลเกี่ยวกับผู้เสียชีวิต ต้องไม่ทำให้เกิดความเสื่อมเสียเชื่อเสียง หรือถูกดูหมิ่นเกลียดชัง ญาติสามารถฟ้องร้องได้ตามกฎหมาย

11. การโพสต์ด่าว่าผู้อื่น มีกฎหมายอาญาอยู่แล้ว ไม่มีข้อมูลจริง หรือถูกตัดต่อ ผู้ถูกกล่าวหา เอาผิดผู้โพสต์ได้ และมีโทษจำคุกไม่เกิน 3 ปี ปรับไม่เกิน 200,000 บาท

12. ไม่ทำการละเมิดลิขสิทธิ์ผู้ใด ไม่ว่าข้อความ เพลง รูปภาพ หรือวิดีโอ

13. ส่งรูปภาพแชร์ของผู้อื่น เช่น สวัสดี อวยพร ไม่ผิด ถ้าไม่เอาภาพไปใช้ในเชิงพาณิชย์หารายได้

5.3 การตรวจติดตามการนำไปปฏิบัติตามกระบวนการและการให้ความเป็นอิสระในการตรวจสอบ (Performance)

องค์การสุราฯ พิจารณาให้มีการประเมินแผนงานว่า มีความสอดคล้องกับการดำเนินงานและการกำกับดูแลที่ดีด้านเทคโนโลยีดิจิทัลอย่างไร รวมทั้งประเมินความเสี่ยงที่เกิดจากการจัดการเทคโนโลยีดิจิทัลอย่างสม่ำเสมอ เพื่อป้องกันมิให้ทรัพยากรเทคโนโลยีดิจิทัลถูกนำไปใช้อย่างไม่เหมาะสม

ระบบควบคุมภายในขององค์การสุราฯ เป็นกระบวนการปฏิบัติงานที่จัดให้มีขึ้น เพื่อสร้างความมั่นใจว่าการดำเนินงานขององค์กรจะบรรลุวัตถุประสงค์ของการควบคุมภายใน ทั้งในด้านประสิทธิภาพประสิทธิผลของการดำเนินงาน ซึ่งรวมถึงการดูแลทรัพย์สินการป้องกันหรือ ลดความผิดพลาดความเสียหาย การรั่วไหล การสิ้นเปลือง หรือการทุจริตในหน่วยงาน ความเชื่อถือได้ของรายงาน การเงินและรายงานที่มิใช่การเงินการปฏิบัติตามกฎหมายระเบียบ ข้อบังคับ มติคณะรัฐมนตรี การดำเนินงานการควบคุมภายในขององค์การสุราฯ เป็นไปตามหลักเกณฑ์กระทรวงการคลังว่าด้วย มาตรฐานและหลักเกณฑ์ปฏิบัติการควบคุมภายในสำหรับหน่วยงานของรัฐ พ.ศ. 2561 และหลักเกณฑ์กระทรวงการคลังว่าด้วยมาตรฐานและหลักเกณฑ์ปฏิบัติการ

บริหารจัดการความเสี่ยงสำหรับ หน่วยงานของรัฐ พ.ศ. 2562 ทั้งนี้ องค์การสุราฯ ได้มีการกำหนดคู่มือการควบคุมภายใน โดยมีรายละเอียดดังนี้

องค์ประกอบของมาตรฐานการควบคุมภายใน

ในการดำเนินงานเพื่อให้บรรลุวัตถุประสงค์ของการควบคุมภายใน ผู้กำกับดูแลและฝ่ายบริหารจะต้องจัดให้การดำเนินงานภายในองค์การสุราฯ ประกอบไปด้วยองค์ประกอบของมาตรฐานการควบคุมภายในตามแนวทางของ Committee of Sponsoring Organization of the Treadway Commission (COSO) จะประกอบไปด้วย 5 องค์ประกอบ 17 หลักการ ดังนี้

1) สภาพแวดล้อมของการควบคุม (Control Environment) สภาพแวดล้อมของการควบคุมเป็นปัจจัยพื้นฐานในการดำเนินงานที่ส่งผลให้มีการนำ การควบคุมภายในมาปฏิบัติทั่วทั้งหน่วยงานของรัฐ ทั้งนี้ ผู้กำกับดูแลและฝ่ายบริหารจะต้องสร้าง บรรยากาศให้ทุกระดับตระหนักถึงความสำคัญของการควบคุมภายในรวมทั้งการดำเนินงานที่ คาดผู้หวังของผู้กำกับดูแลและฝ่ายบริหาร ทั้งนี้ สภาพแวดล้อมการควบคุมดังกล่าวเป็นพื้นฐานสำคัญ ที่จะส่งผลกระทบต่อองค์ประกอบของการควบคุมภายในอื่น ๆ ซึ่งสภาพแวดล้อมการควบคุมประกอบด้วย 5 หลักการ ดังนี้

- หน่วยงานของรัฐแสดงให้เห็นถึงการยึดมั่นในคุณค่าของความซื่อตรงและจริยธรรม
- ผู้กำกับดูแลของหน่วยงานของรัฐ แสดงให้เห็นถึงความเป็นอิสระจากฝ่ายบริหารและมีหน้าที่กำกับดูแลให้มีการพัฒนาหรือปรับปรุงการควบคุมภายใน รวมถึงดำเนินการเกี่ยวกับการควบคุมภายใน
- หัวหน้าหน่วยงานของรัฐจัดให้มีโครงสร้างองค์กร สายการบังคับบัญชา อำนาจหน้าที่และความรับผิดชอบที่เหมาะสมในการบรรลุวัตถุประสงค์ของหน่วยงานของรัฐภายใต้การ กำกับดูลของผู้กำกับดูแล
- หน่วยงานของรัฐแสดงให้เห็นถึงความมุ่งมั่นในการสร้างแรงจูงใจ พัฒนาและรักษาบุคลากรที่มีความรู้ความสามารถที่สอดคล้องกับวัตถุประสงค์ของหน่วยงานของรัฐ
- หน่วยงานของรัฐกำหนดให้บุคลากรมีหน้าที่และความรับผิดชอบต่อผลการปฏิบัติงานตามระบบการควบคุมภายใน เพื่อให้บรรลุวัตถุประสงค์ของหน่วยงานของรัฐ

2) การประเมินความเสี่ยง (Risk Assessment) การประเมินความเสี่ยงเป็นกระบวนการที่มีการดำเนินการอย่างต่อเนื่องและเป็นประจำเพื่อระบุและวิเคราะห์ความเสี่ยงที่มีผลกระทบต่อการบรรลุวัตถุประสงค์ของหน่วยงานของรัฐ รวมถึงกำหนดวิธีการจัดการความเสี่ยงนั้น ฝ่ายบริหารควรคำนึงถึงการเปลี่ยนแปลงของสภาพแวดล้อมภายนอกและภารกิจภายในทั้งหมดที่มีผลต่อการบรรลุวัตถุประสงค์ของหน่วยงานของรัฐ การประเมินความเสี่ยงประกอบด้วย 4 หลักการ ดังนี้

- หน่วยงานของรัฐระบุวัตถุประสงค์การควบคุมภายในของการปฏิบัติงานให้สอดคล้องกับวัตถุประสงค์ขององค์กรไว้อย่างชัดเจนและเพียงพอที่จะสามารถระบุและประเมินความเสี่ยงที่เกี่ยวข้องกับวัตถุประสงค์
- หน่วยงานของรัฐระบุความเสี่ยงที่มีผลต่อการบรรลุวัตถุประสงค์การควบคุมภายในอย่างครอบคลุมทั้งหน่วยงานของรัฐ และวิเคราะห์ความเสี่ยงเพื่อกำหนดวิธีการจัดการความเสี่ยงนั้น

- หน่วยงานของรัฐพิจารณาโอกาสที่อาจเกิดการทุจริต เพื่อประกอบการประเมินความเสี่ยงที่ส่งผลต่อการบรรลุวัตถุประสงค์

- หน่วยงานของรัฐระบุและประเมินการเปลี่ยนแปลงที่อาจมีผลกระทบอย่างมีนัยสำคัญต่อระบบการควบคุมภายใน

3) กิจกรรมการควบคุม (Control Activities) กิจกรรมการควบคุมเป็นการปฏิบัติที่กำหนดไว้ในนโยบายและกระบวนการดำเนินงานเพื่อให้มั่นใจว่าการปฏิบัติตามการสั่งการของฝ่ายบริหารจะลดหรือควบคุมความเสี่ยงให้ สามารถบรรลุวัตถุประสงค์กิจกรรมการควบคุมควรได้รับการการนำไปปฏิบัติทั่วทุกระดับของหน่วยงานของรัฐ ในกระบวนการปฏิบัติงาน ขั้นตอนการดำเนินงานต่างๆ รวมถึงการนำเทคโนโลยีมาใช้ในการดำเนินงาน

- หน่วยงานของรัฐระบุและพัฒนากิจกรรมการควบคุม เพื่อลดความเสี่ยงในการบรรลุวัตถุประสงค์ให้อยู่ในระดับที่ยอมรับได้

- หน่วยงานของรัฐระบุและพัฒนากิจกรรมการควบคุมทั่วไปด้านเทคโนโลยี เพื่อสนับสนุนการบรรลุวัตถุประสงค์

- หน่วยงานของรัฐจัดให้มีกิจกรรมการควบคุม โดยกำหนดไว้ในนโยบายประกอบด้วยผลสำเร็จที่คาดหวังและขั้นตอนการปฏิบัติงาน เพื่อนำนโยบายไปสู่การปฏิบัติจริง

4) สารสนเทศและการสื่อสาร (Information and Communications) ระบบสารสนเทศเป็นสิ่งจำเป็นสำหรับหน่วยงานของรัฐที่จะช่วยให้มีการดำเนินการตาม การควบคุมภายในที่กำหนด เพื่อสนับสนุนให้บรรลุวัตถุประสงค์ของหน่วยงานของรัฐ การสื่อสาร เกิดขึ้นได้ทั้งจากภายในและภายนอก และเป็นช่องทางเพื่อให้ทราบถึงสารสนเทศที่สำคัญในการควบคุมการดำเนินงานของหน่วยงานของรัฐ การสื่อสารจะช่วยให้บุคลากรในหน่วยงานมีความเข้าใจ ถึงความรับผิดชอบและความสำคัญของการควบคุมภายในที่มีต่อการบรรลุวัตถุประสงค์ด้านสารสนเทศและการสื่อสารประกอบด้วย 3 หลักการ ดังนี้

- หน่วยงานของรัฐจัดทำหรือจัดหาและใช้สารสนเทศที่เกี่ยวข้องและมีคุณภาพเพื่อสนับสนุนให้มีการปฏิบัติตามการควบคุมภายในที่กำหนด

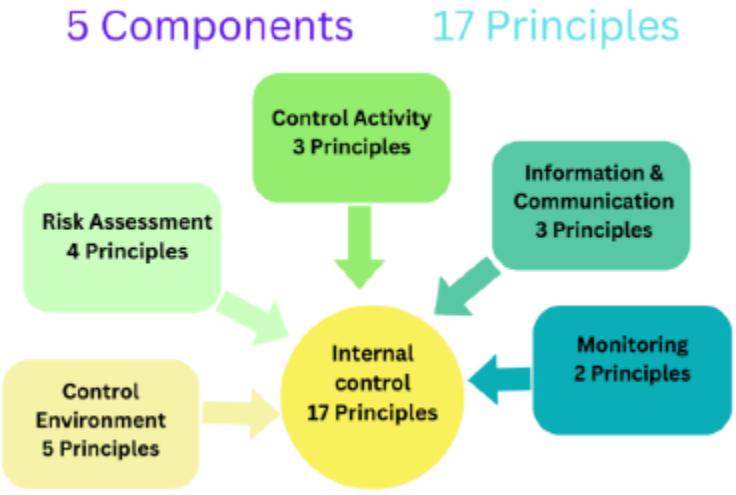
- หน่วยงานของรัฐมีการสื่อสารภายในเกี่ยวกับสารสนเทศ รวมถึงวัตถุประสงค์และความรับผิดชอบที่มีต่อการควบคุมภายในซึ่งมีความจำเป็นในการสนับสนุนให้มีการปฏิบัติตามการ ควบคุมภายในที่กำหนด

- หน่วยงานของรัฐมีการสื่อสารกับบุคคลภายนอกเกี่ยวกับเรื่องที่มีผลกระทบต่อการปฏิบัติตามการควบคุมภายในที่กำหนด

5) การติดตามประเมินผล (Monitoring) กิจกรรมการติดตามผลเป็นการประเมินผลระหว่างการปฏิบัติงาน การประเมินผลเป็น รายครั้งหรือเป็นการประเมินผลทั้งสองวิธีร่วมกัน เพื่อให้เกิดความมั่นใจว่าได้มีการปฏิบัติตามหลักการในแต่ละองค์ประกอบของการควบคุมภายในจะก่อให้เกิดความเสียหายต่อหน่วยงานของรัฐให้รายงานต่อฝ่ายบริหารและผู้กำกับดูแล อย่างทันเวลา กิจกรรมการติดตามผลประกอบด้วย 2 หลักการ ดังนี้

- หน่วยงานของรัฐระบุ พัฒนาและดำเนินการประเมินผลระหว่างการปฏิบัติงานและหรือการประเมินผลเป็นรายครั้งตามที่กำหนด เพื่อให้เกิดความมั่นใจว่าได้มีการปฏิบัติตามองค์ประกอบของการควบคุมภายใน

- หน่วยงานของรัฐประเมินผลและสื่อสารข้อบกพร่อง หรือจุดอ่อนของการควบคุมภายในอย่างทันเวลา ต่อฝ่ายบริหารและผู้กำกับดูแล เพื่อให้ผู้รับผิดชอบสามารถสั่งการแก้ไขได้อย่างเหมาะสม



รูปที่ 6 มาตรฐานการควบคุมภายในตามแนวทางของ
Committee of Sponsoring Organization of the Treadway Commission (COSO)

บทที่ 6 กรอบการกำกับดูแลการบริหารความเสี่ยงด้านเทคโนโลยีดิจิทัล

6.1 นโยบายการกำกับดูแลกิจการที่ดี การบริหารความเสี่ยง และการปฏิบัติตามกฎระเบียบ (Governance, Risk Management and Compliance: GRC)

องค์การสุราฯ มีความตระหนักและให้ความสำคัญต่อการเพิ่มประสิทธิภาพประสิทธิผลและยกระดับความโปร่งใสในการดำเนินงาน เพื่อเสริมสร้างภาพลักษณ์ที่ดีให้แก่องค์กรและเพิ่มศักยภาพในการตอบสนองต่อผู้มีส่วนได้ส่วนเสีย คณะกรรมการบริหารกิจการขององค์การสุราในการประชุมครั้งที่ 12/2567 เมื่อวันที่ 25 ตุลาคม 2567 จึงได้กำหนดนโยบายการกำกับดูแลกิจการที่ดี การบริหารความเสี่ยง และการปฏิบัติตามกฎระเบียบ (Good Governance, Risk Management and Compliance: GRC) ขึ้น โดยการจัดให้มีบุคลากรที่มีความรู้และคุณสมบัติเหมาะสม (People) ขั้นตอนการทำงานที่โปร่งใสและมีการควบคุมภายในที่ดี (Process) มีการบริหารจัดการข้อมูลที่ถูกต้อง เหมาะสม ทันเวลา (Information) และมีการใช้เทคโนโลยีอย่างมีประสิทธิภาพ (Technology) เพื่อช่วยให้องค์กรมีการกำกับดูแลกิจการที่ดี โปร่งใส และตรวจสอบได้ มีการบริหารความเสี่ยงอย่างเป็นระบบและสามารถปฏิบัติตามกฎระเบียบได้อย่างครบถ้วน ส่งผลให้เกิดความน่าเชื่อถือและมั่นใจในการบริหารงานและการให้บริการขององค์กรจากผู้มีส่วนได้ส่วนเสีย (Stakeholder) ซึ่งนโยบายนี้บังคับใช้กับคณะกรรมการ ผู้บริหาร และพนักงานทุกคน

<u>คำนิยาม</u>

“กฎระเบียบ” หมายถึง กฎหมาย ระเบียบ ข้อบังคับ ที่เกี่ยวข้องกับองค์การสุราฯ

<u>โดยมีหลักปฏิบัติดังนี้</u>

คณะกรรมการบริหารกิจการขององค์การสุรา คณะอนุกรรมการกำกับดูแลที่ดีและการนำองค์กร คณะอนุกรรมการบริหารความเสี่ยงและการควบคุมภายใน คณะอนุกรรมการเทคโนโลยี นวัตกรรมและดิจิทัล และคณะอื่นที่เกี่ยวข้อง ตลอดจนผู้บริหารและพนักงานขององค์การสุราทุกระดับ จะร่วมกันกำกับและขับเคลื่อนองค์กรในเชิงการบูรณาการภายใต้หลักการกำกับดูแลกิจการที่ดี การบริหารความเสี่ยงและการควบคุมภายในกฎหมาย ระเบียบ ข้อบังคับขององค์กร ให้มีการปฏิบัติตามหลักสำคัญ ดังต่อไปนี้

ข้อ 1 องค์การสุราฯ ร่วมกันกำกับดูแลกิจการที่ดีให้สอดคล้องกับมาตรฐานสากลตามกรอบหลักการของ Organization for Economic Co-operation and Development (OECD) ปี 2515 และแนวทางการปฏิบัติ 10 หมวด มาใช้ในการปฏิบัติงาน ได้แก่ 1) การสนองบทบาทของภาครัฐ 2) บทบาทของรัฐวิสาหกิจเพื่อการตลาดที่เป็นธรรม 3) สิทธิและความเท่าเทียมกันของผู้ถือหุ้น 4) บทบาทของผู้มีส่วนได้ส่วนเสีย 5) การเปิดเผยข้อมูล 6) คณะกรรมการ 7) การบริหารความเสี่ยงและการควบคุมภายใน 8) จรรยาบรรณ 9) ความยั่งยืนและนวัตกรรม และ 10) การติดตามผลการดำเนินการ

ข้อ 2 ดำเนินการกำหนดกลยุทธ์ แผนการดำเนินงานตามวัตถุประสงค์และเป้าหมายเพื่อการป้องกันความเสียหายขององค์กรด้วยระบบการควบคุมภายในและเฝ้าระวังความเสี่ยง (Risk) ในอนาคตที่อาจเกิดขึ้นและส่งผลกระทบต่อองค์กร และสนับสนุนให้มีการบริหารความเสี่ยงอย่างเป็นระบบ รวมทั้งการสื่อสาร เผยแพร่ความรู้ สร้างความตระหนักเกี่ยวกับการบริหารความเสี่ยงและการควบคุมภายใน

ข้อ 3 จัดให้มีการเสริมสร้างบรรยากาศและพฤติกรรมในการสร้างวัฒนธรรมองค์กรเชิงบูรณาการ (GRC Culture) ที่มุ่งตอบสนองค่านิยมองค์กรและเหมาะสมต่อการสนับสนุนการบริหารจัดการ

องค์กร และการตัดสินใจในเรื่องสำคัญต่าง ๆ ร่วมกัน เพื่อให้เกิดประสิทธิภาพในการบริหารงานด้าน GRC ที่สามารถตอบสนองต่อผู้มีส่วนได้ส่วนเสีย (Stakeholder) อย่างทันท่วงที

ข้อ 4 ดำเนินการกำหนดวัตถุประสงค์และกลยุทธ์ที่มุ่งเน้นความยั่งยืนขององค์กร บนพื้นฐานของหลักธรรมาภิบาล (Governance) ภายใต้แนวคิดขับเคลื่อนธุรกิจคู่สังคม รวมทั้งคำนึงถึงการกำกับด้านกฎหมายระเบียบ ข้อบังคับขององค์กร (Compliance) อย่างเป็นระบบ เพื่อสามารถสนับสนุนการกำหนดแนวปฏิบัติได้อย่างมีประสิทธิภาพ

ข้อ 5 นำเทคโนโลยีดิจิทัลมาปรับใช้เป็นเครื่องมือในการสนับสนุนการปฏิบัติงาน เพื่อให้การดำเนินกิจการขององค์กรบรรลุผลสัมฤทธิ์ ตามเป้าประสงค์ที่กำหนดด้วยการบริหารจัดการที่ดีด้านเทคโนโลยีสารสนเทศครอบคลุมทั่วทั้งองค์กร และผู้มีส่วนได้ส่วนเสีย เพื่อสร้างคุณค่าจากการใช้เทคโนโลยีสารสนเทศที่มีความโปร่งใสและตรวจสอบได้ ควบคู่กับการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศที่เหมาะสม เพื่อลดภัยคุกคามต่าง ๆ ที่อาจเกิดขึ้นและกระทบการดำเนินกิจการที่สำคัญขององค์กร อาทิ การโจมตีทางไซเบอร์ (Cyber Attack) รวมทั้งการบริหารความต่อเนื่องทางธุรกิจ (Business Continuity Management: BCM) เพื่อสร้างความต่อเนื่องในการดำเนินการและให้บริการขององค์กรในขณะเกิดภาวะวิกฤตหรือเหตุการณ์ฉุกเฉิน

ข้อ 6 จัดให้มีการบูรณาการร่วมกันระหว่างหน่วยงานในการติดตามความคืบหน้า สอบทาน และตรวจสอบกระบวนการทำงานต่าง ๆ อย่างสม่ำเสมอ เพื่อปรับปรุงแก้ไขการดำเนินงานให้มีประสิทธิภาพและมุ่งสู่การพัฒนาอย่างยั่งยืน (Sustainable Development) ตลอดจนการสื่อสารข้อมูลต่าง ๆ ร่วมกับผู้บริหารและพนักงานทุกระดับ เพื่อสนับสนุนให้เกิดการแลกเปลี่ยนองค์ความรู้ (Knowledge Sharing) ภายใต้การสื่อสารข้อมูลทั่วทั้งองค์กรจนเกิดการบูรณาการร่วมกัน

องค์การสุรา กรมสรรพสามิต จึงได้กำหนดแนวทางในการนำนโยบายการกำกับดูแลกิจการที่ดี การบริหารความเสี่ยง และการปฏิบัติตามกฎระเบียบ (GRC) ประจำปี 2568 เพื่อการปฏิบัติอย่างชัดเจน โดยได้กำหนดแนวทางการดำเนินการตาม GRC Capability Model Version 3.0 ดังนี้

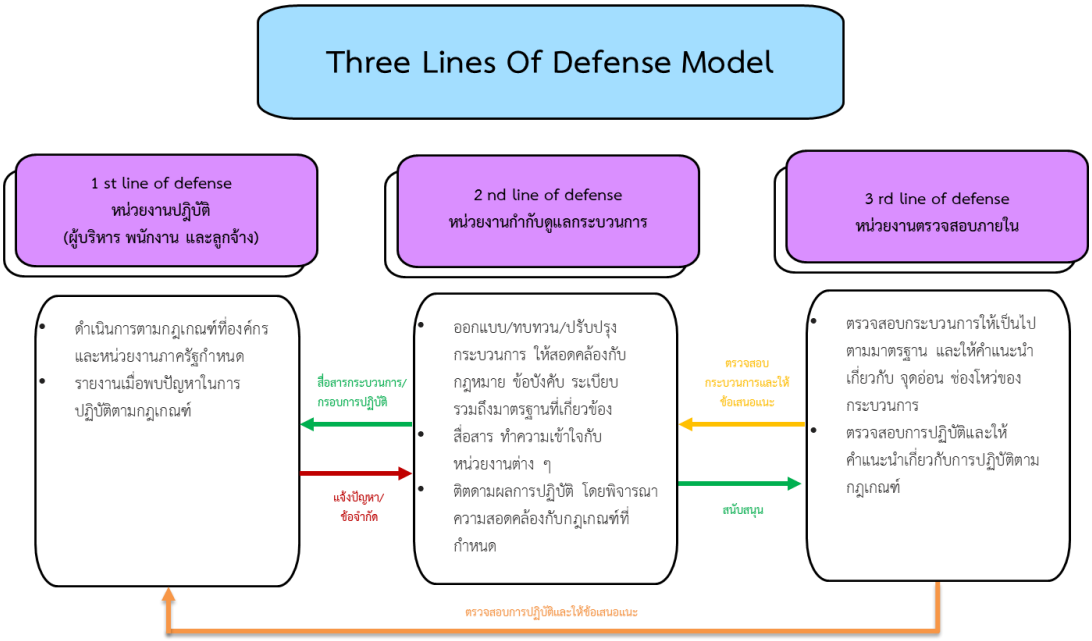
1. Learn หมายถึง การเรียนรู้และเข้าใจอย่างถ่องแท้ถึงบริบทในการดำเนินธุรกิจ วัฒนธรรมองค์กรและความคาดหวังของผู้มีส่วนได้เสีย

2. Align หมายถึง การนำสิ่งที่ได้เรียนรู้มากำหนดวัตถุประสงค์ของบริษัท แล้วจึงระบุความเสี่ยงที่อาจเกิดขึ้น ซึ่งทำให้บริษัทไม่บรรลุวัตถุประสงค์

3. Perform หมายถึง การขับเคลื่อนให้บริษัทไปสู่เป้าหมายหรือวัตถุประสงค์ ด้วยกระบวนการทำงานที่มีประสิทธิภาพ ถูกต้องตามกฎระเบียบ และมีระบบการควบคุมภายในที่ดี

4. Monitor หมายถึง มีระบบติดตามดูแลการปฏิบัติงานอย่างเพียงพอ เหมาะสม เพื่อให้เป็นไปตามวัตถุประสงค์ที่ตั้งไว้

ปัจจัยสนับสนุนและขับเคลื่อน GRC (GRC Supports)



ระดับ	หมายถึง	หน้าที่/ความรับผิดชอบ
1st Line	หน่วยงานผู้ปฏิบัติทุกหน่วยงานภายในองค์กร หรือ Risk Owner เป็นหน่วยงานเจ้าของความเสี่ยงที่เข้าใจในธุรกิจ และความเสี่ยงที่มีกับงานของตนเอง (ผู้บริหารฯ และพนักงานทั้งหมด)	- ปฏิบัติงานให้เป็นไปตามเกณฑ์ที่ Second Line กำหนด เพื่อให้มีการควบคุมภายในและการบริหารจัดการความเสี่ยงที่เหมาะสม - รายงานเมื่อพบปัญหาในการปฏิบัติงานตามกฎเกณฑ์
2nd Line	หน่วยงานกำกับดูแลระบบงานหรือเจ้าของระบบงานภายในองค์กร (คณะกรรมการฯ คณะอนุกรรมการฯ คณะทำงานฯ)	- กำกับดูแลระบบงานและวางกรอบแนวทางการดำเนินงานของระบบงานที่รับผิดชอบให้ First Line ดำเนินการโดย 1. ออกแบบ/ทบทวน/ปรับปรุงกระบวนการให้สอดคล้องกับกฎหมาย ข้อบังคับ ระเบียบ รวมถึงมาตรฐานที่เกี่ยวข้อง 2. สื่อสารทำความเข้าใจกับหน่วยงานต่าง ๆ 3. ติดตามผลการปฏิบัติโดยพิจารณาความสอดคล้องกับกฎเกณฑ์ที่กำหนด
3rd Line	หน่วยงานตรวจสอบภายใน	- สอบทานการปฏิบัติงานของ Frist Line และ Second Line โดยดำเนินการดังนี้ 1. ตรวจสอบกระบวนการให้เป็นไปตามมาตรฐาน และให้คำแนะนำเกี่ยวกับจุดอ่อน 2. ตรวจสอบการปฏิบัติงานและให้คำแนะนำเกี่ยวกับการปฏิบัติตามกฎเกณฑ์ เพื่อให้มั่นใจว่า การดำเนินงานของทุกหน่วยงานมีประสิทธิภาพ ประสิทธิผล เป็นไปตามวัตถุประสงค์/เป้าหมายขององค์กร และข้อกำหนด/กฎเกณฑ์ต่าง ๆ

การบูรณาการนโยบาย

การบูรณาการระหว่างการกำกับดูแลกิจการที่ดี การบริหารความเสี่ยง และการปฏิบัติตามกฎระเบียบ (Governance, Risk Management and Compliance: GRC) คือ การจัดให้มีบุคลากรที่มีความรู้และมีคุณสมบัติเหมาะสม (People) ขั้นตอนการทำงานที่โปร่งใสและมีการควบคุมภายในที่ดี (Process) มีการบริหารจัดการข้อมูลที่ถูกต้อง เหมาะสม ทันเวลา (Information) และมีการใช้เทคโนโลยีอย่างมีประสิทธิภาพ (Technology) เพื่อช่วยให้องค์กรมีการกำกับดูแลกิจการที่ดี โปร่งใสและตรวจสอบได้ มีการบริหารความเสี่ยงอย่างเป็นระบบ และสามารถปฏิบัติตามกฎระเบียบที่เกี่ยวข้องได้อย่างครบถ้วน ส่งผลให้เกิดความน่าเชื่อถือและมั่นใจในการบริหารงาน และการให้บริการขององค์กรจากผู้มีส่วนได้ส่วนเสีย (Stakeholder) ทั้งนี้ เพื่อช่วยเพิ่มความมั่นใจว่าองค์กรจะสามารถบรรลุวัตถุประสงค์หรือเป้าหมายที่ตั้งไว้อย่างสมเหตุสมผล ดังนี้

ข้อ 1 องค์การสุราฯ ร่วมกันกำกับดูแลกิจการที่ดีให้สอดคล้องกับมาตรฐานสากลตามกรอบหลักการของ Organization for Economic Co-operation and Development (OECD) ปี 2515 และแนวทางการปฏิบัติ 10 หมวด มาใช้ในการปฏิบัติงาน ได้แก่ 1) การสนองบทบาทของภาครัฐ 2) บทบาทของรัฐวิสาหกิจเพื่อการตลาดที่เป็นธรรม 3) สิทธิและความเท่าเทียมกันของผู้ถือหุ้น 4) บทบาทของผู้มีส่วนได้ส่วนเสีย 5) การเปิดเผยข้อมูล 6) คณะกรรมการ 7) การบริหารความเสี่ยงและการควบคุมภายใน 8) จรรยาบรรณ 9) ความยั่งยืนและนวัตกรรม และ 10) การติดตามผลการดำเนินการ

หลักการพื้นฐาน

1. องค์การสุราฯ มีการปฏิบัติหน้าที่ตามความรับผิดชอบอย่างครบถ้วนและมีประสิทธิผลโดยคณะกรรมการบริหารกิจการขององค์การสุราฯ ตระหนักถึงบทบาท หน้าที่ ในการกำหนดให้มีทิศทาง นโยบาย แผนงาน กลยุทธ์ และเป้าหมายที่ชัดเจนเป็นรูปธรรม รวมทั้งสร้างความมั่นใจในความเพียงพอของระบบการบริหารจัดการองค์กรที่สำคัญ ตลอดจน กำกับ ควบคุม ดูแล ติดตามผลการดำเนินงานขององค์กรให้สอดคล้องกับมาตรฐานสากลตามกรอบหลักการของ Organization for Economic Co-operation and Development (OECD) ปี 2515 และตามหลักเกณฑ์ของสำนักงานคณะกรรมการนโยบายรัฐวิสาหกิจ (สคร.) ให้บรรลุเป้าหมายตามที่กำหนดไว้

แนวทางปฏิบัติ

หน่วยงานปฏิบัติ (1st Line)

1. ผู้บริหาร พนักงาน และลูกจ้าง ดำเนินการศึกษาและทำความเข้าใจกับนโยบาย กลยุทธ์ และปัจจัยต่าง ๆ ตามแผนการดำเนินงานขององค์กร พร้อมทั้งกำหนดแผนการทำงานและควรจัดสรรทรัพยากรอย่างเพียงพอและเหมาะสม เพื่อให้เกิดประสิทธิผลและประสิทธิภาพในการดำเนินงาน

2. ผู้บังคับบัญชา กำกับดูแลและสอบทางการปฏิบัติงานของพนักงานและลูกจ้างให้เป็นไปตามแผนการดำเนินงาน โดยให้ดำเนินงานอย่างโปร่งใสและตรวจสอบได้

3. ผู้บริหาร พนักงาน และลูกจ้าง ต้องตระหนักและปฏิบัติงานอย่างโปร่งใส่ถูกต้องตามหลักจริยธรรมและจรรยาบรรณตามคู่มือจริยธรรมและจรรยาบรรณการดำเนินธุรกิจขององค์การสุรา กรมสรรพสามิตอย่างเคร่งครัด พร้อมทั้งสอดส่องดูแลให้ไม่เกิดช่องทางการทุจริตในการดำเนินงาน รวมถึงการกำหนดวิธีการควบคุมและป้องกันปราบปรามการทุจริตและคอร์รัปชั่นทุกรูปแบบ

หน่วยงานกำกับดูแลกระบวนการ (2nd Line)

1. กำหนดกรอบและแนวทางในการปฏิบัติตามนโยบายทั้งภายในและภายนอก ให้สอดคล้องและเหมาะสมกับองค์กร รวมทั้งควรมีการทบทวน และปรับปรุงให้สามารถดำเนินงานได้ทันท่วงทีและถูกต้องตามสถานการณ์ในปัจจุบัน

2. ติดตามผลการปฏิบัติงานของแต่ละหน่วยงานต่าง ๆ โดยพิจารณาถึงความสอดคล้องกับแนวปฏิบัติและแผนการดำเนินงานที่กำหนดไว้ รวมทั้งวิเคราะห์และประเมินผลการดำเนินงาน และรายงานให้ผู้บริหารระดับสูงทราบเป็นไตรมาส

3. สื่อสาร และทำความเข้าใจเกี่ยวกับการปฏิบัติตามแนวทางปฏิบัติ และแผนการดำเนินงาน รวมทั้งผลการวิเคราะห์ประเมินช่องโหว่และความเสี่ยงให้กับพนักงานและหน่วยงานต่าง ๆ ได้รับทราบอย่างถูกต้อง

หน่วยงานตรวจสอบภายใน (3rd Line)

1. ตรวจสอบกระบวนการทำงานของหน่วยงานต่าง ๆ และให้คำแนะนำ ชี้แจงเกี่ยวกับการปฏิบัติงานตามแนวปฏิบัติ และแผนการดำเนินงานอย่างมีประสิทธิภาพและประสิทธิผล

ข้อ 2 ดำเนินการกำหนดกลยุทธ์ แผนการดำเนินงานตามวัตถุประสงค์และเป้าหมายเพื่อการป้องกันความเสียหายขององค์กรด้วยระบบการควบคุมภายในและเฝ้าระวังความเสี่ยง (Risk) ในอนาคตที่อาจเกิดขึ้นและส่งผลกระทบต่อองค์กร และสนับสนุนให้มีการบริหารความเสี่ยงอย่างเป็นระบบ รวมทั้งการสื่อสาร เผยแพร่ความรู้ สร้างความตระหนักเกี่ยวกับการบริหารความเสี่ยงและการควบคุมภายใน

หลักการพื้นฐาน

1. องค์การสุราฯ มีกระบวนการบริหารจัดการความเสี่ยงองค์กรที่สอดคล้องกับระบบการบริหารความเสี่ยงตามมาตรฐานสากล COSO ERM 2017 โดยเป็นการบริหารความเสี่ยงลักษณะเชิงรุก กำหนดกลยุทธ์การบริหารความเสี่ยงที่เชื่อมโยงกับแผนยุทธศาสตร์/กลยุทธ์/การวางแผน/การจัดสรรทรัพยากร/การลงทุน/ผู้มีส่วนได้ส่วนเสีย ทั้งนี้พิจารณาประเด็นความเสี่ยงทางการเงินและไม่ใช่การเงินที่ครอบคลุมทั้งในด้านกลยุทธ์ (Strategy) ด้านการเงิน (Finance) ด้านการปฏิบัติงาน (Operation) และการปฏิบัติตามกฎหมาย (Compliance) โดยมีการประเมินความเสี่ยงผ่านมุมมองของโอกาส(Likelihood) และผลกระทบ (Impact) และกำหนดมาตรการจัดการความเสี่ยง (Mitigation) รวมถึงค่าดัชนีชี้วัดความเสี่ยง (Key Risk Indicator : KRI) ระดับความเสี่ยงที่ยอมรับได้ผ่านค่าความเสี่ยงที่ยอมรับได้ (Risk Appetite : RA) และ ค่าช่วงเบี่ยงเบนของระดับความเสี่ยงที่ยอมรับได้ (Risk Tolerance : RT) พร้อมทั้งมีการติดตามรายงานผลการบริหารความเสี่ยง และมีการทบทวนการบริหารความเสี่ยงทุกไตรมาส

2. องค์การสุราฯ จัดให้มีการควบคุมภายในตามภารกิจของหน่วยงานอย่างเพียงพอและเหมาะสมทุกขั้นตอนของการปฏิบัติงาน เป็นไปตามหลักเกณฑ์กระทรวงการคลังว่าด้วยมาตรฐานและหลักเกณฑ์ปฏิบัติการควบคุมภายในสาหรับหน่วยงานของรัฐ พ.ศ. 2561 และสอดคล้องกับหลักการตามกรอบดำเนินงานด้าน Governance, Risk and Compliance (GRC) รวมทั้งกำกับดูแลให้มีการปฏิบัติตามอย่างเคร่งครัด

3. สนับสนุนให้มีบรรยากาศและวัฒนธรรมที่สนับสนุนการบริหารความเสี่ยงอย่างต่อเนื่องทั่วทั้งองค์กร โดยมีการสื่อสารทำความเข้าใจและสร้างความตระหนักให้แก่พนักงานทุกระดับให้มีส่วนร่วมในการบริหารความเสี่ยง และการควบคุมภายใน โดยเชื่อมโยงกับพฤติกรรมด้านที่ส่งเสริมค่านิยมขององค์กร

แนวทางปฏิบัติ

หน่วยงานปฏิบัติ (1st Line)

1. ผู้บริหาร พนักงาน และลูกจ้าง ดำเนินการศึกษาและทำความเข้าใจกับหลักการในการบริหารความเสี่ยงตามมาตรฐานสากล COSO ERM 2017 และปฏิบัติตามคู่มือการบริหารความเสี่ยง คู่มือการควบคุมภายใน แนวทางการควบคุมภายใน และแนวทางปฏิบัติงานให้เป็นไปตามกฎเกณฑ์ขององค์กร

2. ผู้บังคับบัญชา กำกับดูแลและสอบทานการดำเนินการของพนักงานและลูกจ้าง ให้เป็นไปตามแผนการบริหารความเสี่ยงและการควบคุมภายในที่กำหนดอย่างครบถ้วน พร้อมทั้งสอบทาน การปฏิบัติงานให้สอดคล้องกับกฎเกณฑ์ที่เกี่ยวข้องอย่างเคร่งครัด หรือละเมิด

3. ผู้บริหาร พนักงาน และลูกจ้าง ต้องตระหนักถึงการบริหารความเสี่ยงและการควบคุมภายใน และประเมินความเสี่ยงในการปฏิบัติงาน พร้อมทั้งสอบทานการดำเนินการให้สอดคล้องกับกฎเกณฑ์อยู่เสมอ เพื่อให้บรรลุผลสำเร็จตามวัตถุประสงค์ การดำเนินงานขององค์กร

หน่วยงานกำกับดูแลกระบวนการ (2nd Line)

1. กำหนดกรอบ แผนการดำเนินงาน และแนวทางในการปฏิบัติด้านการบริหารความเสี่ยง การควบคุมภายใน และการปฏิบัติงานให้เป็นไปตามกฎเกณฑ์ขององค์กร ให้สอดคล้องและเหมาะสมกับองค์กร รวมทั้งควรมีการทบทวนและปรับปรุงให้มีความถูกต้องอย่างสม่ำเสมอ

2. ติดตามผลการปฏิบัติของหน่วยงานต่างๆ โดยพิจารณาถึงความสอดคล้องกับแนวทางปฏิบัติ และแผนการดำเนินงานที่กาหนดไว้ ควรมีการทบทวนและประเมินช่องโหว่และความเสี่ยงในการดำเนินงาน และควรมีการแจ้งเตือนเหตุล่วงหน้าให้ผู้ปฏิบัติได้มีการแก้ไขได้ทันกาล รวมทั้งควรทบทวนข้อมูลให้เป็นปัจจุบันอยู่เสมอ เพื่อให้ผู้รับผิดชอบและผู้บริหารได้ใช้ประกอบการตัดสินใจได้

3. สื่อสาร เผยแพร่ความรู้ สร้างความตระหนักเกี่ยวกับการบริหารความเสี่ยงและการควบคุมภายใน และประชาสัมพันธ์และทำความเข้าใจเกี่ยวกับการปฏิบัติตามแนวปฏิบัติ และแผนการดำเนินงานให้กับพนักงานและหน่วยงานต่างๆ ได้รับทราบอย่างถูกต้องและมีประสิทธิภาพ รวมถึงควรสร้างความตระหนักรับรู้อย่างทั่วถึงทั่วทั้งองค์กร

หน่วยงานตรวจสอบภายใน (3rd Line)

1. ตรวจสอบกระบวนการทำงานของหน่วยงานต่าง ๆ และให้คำแนะนำ ชี้แจงเกี่ยวกับประเด็นความเสี่ยงที่ตรวจพบ ในการดำเนินการที่ไม่สอดคล้องตามแนวทางและแผนการดำเนินงาน อย่างมีประสิทธิภาพและประสิทธิผล

ข้อ 3 จัดให้มีการเสริมสร้างบรรยากาศและพฤติกรรมในการสร้างวัฒนธรรมองค์กรเชิงบูรณาการ (GRC Culture) ที่มุ่งตอบสนองค่านิยมองค์กรและเหมาะสมต่อการสนับสนุนการบริหารจัดการองค์กร และการตัดสินใจในเรื่องสำคัญต่าง ๆ ร่วมกัน เพื่อให้เกิดประสิทธิภาพในการบริหารงานด้าน GRC ที่สามารถตอบสนองต่อผู้มีส่วนได้ส่วนเสีย (Stakeholder) อย่างทันท่วงที

หลักการพื้นฐาน

1. มุ่งมั่นดูแลบุคลากรอย่างเท่าเทียม โดยให้ความสำคัญตั้งแต่กระบวนการวางแผนกำลังคน และการสรรหาคัดเลือกบุคลากรด้วยความโปร่งใส เพื่อให้ได้บุคลากรที่มีความรู้ ความสามารถมีความมุ่งมั่น และมีศักยภาพในการขับเคลื่อนองค์กรไปสู่ความยั่งยืน รวมทั้งคำนึงถึงการบริหารค่าตอบแทนและการรักษาบุคลากร รวมถึงการ

สร้างสภาพแวดล้อมที่ปลอดภัยและเอื้อต่อการมีคุณภาพชีวิตที่ดี เพื่อตอบสนองต่อความต้องการและความคาดหวังของบุคลากร เพื่อให้มีขวัญและกำลังใจในการปฏิบัติงานจวบจนเกษียณอายุงาน และเสริมสร้างระดับความพึงพอใจและความผูกพันที่ดีต่อสังคม

2. มีความมุ่งมั่นพัฒนาองค์กรอย่างมีประสิทธิภาพ และตอบสนองความต้องการ ความคาดหวัง ของผู้มีส่วนได้ส่วนเสีย โดยได้นำหลักการ Governance Risk Management and Compliance (GRC) ตามมาตรฐานสากลมาประยุกต์ และบูรณาการระหว่าง การกำกับดูแลกิจการที่ดี การบริหารความเสี่ยงการปฏิบัติตามกฎหมายและกฎระเบียบ เพื่อสนับสนุนให้เกิดระบบบริหารจัดการองค์กรที่มีประสิทธิภาพ ภายใต้หลักธรรมาภิบาล มีความโปร่งใส เป็นธรรม ตรวจสอบได้

<u>แนวทางปฏิบัติ</u>

<u>หน่วยงานปฏิบัติ (1st Line)</u>

1. ผู้บริหาร พนักงาน และลูกจ้าง ตระหนัก รวมถึงศึกษาทำความความเข้าใจ และนำนโยบาย GRC ไปปฏิบัติตาม โดยสามารถศึกษาในแนวทางปฏิบัติได้ในคู่มือการบริหารความสี่ยง เพื่อเสริมสร้างบรรยากาศรวมถึงสภาพแวดล้อมให้เหมาะสม ในการส่งเสริมการกำกับดูแลกิจการที่ดี การบริหารความเสี่ยง และการปฏิบัติตามกฎระเบียบภายในองค์กร

2. ผู้บังคับบัญชา ศึกษาทำความเข้าใจกฎระเบียบข้อบังคับ พร้อมทั้งสอบทาน การดำเนินการของบุคลากรในสายบังคับบัญชา ให้สอดคล้องกับกฎเกณฑ์อยู่เสมอ เพื่อให้บรรลุผลสำเร็จตามวัตถุประสงค์การดำเนินงานขององค์กร

3. ผู้ปฏิบัติ ศึกษาทำความเข้าใจกฎระเบียบข้อบังคับ พร้อมทั้งดำเนินงาน ให้สอดคล้องกับกฎเกณฑ์อยู่เสมอ รวมถึงวิเคราะห์การดำเนินงานที่ไม่สอดคล้องกับกฎเกณฑ์ เพื่อรายงานให้ผู้บังคับบัญชา รวมถึงหน่วยงานที่เกี่ยวข้องในกระบวนการทราบ และร่วมกันพัฒนาปรับปรุงแก้ไขต่อไป

<u>หน่วยงานกำกับดูแลกระบวนการ (2nd Line)</u>

1. กำหนดกรอบ นโยบาย แนวทางในการปฏิบัติ และจัดทำระเบียบ/ข้อปฏิบัติ ให้สอดคล้อง และเหมาะสมกับองค์กร รวมทั้งควรมีการทบทวน และปรับปรุงให้มีความถูกต้องอย่างสม่ำเสมอ

2. ติดตามผลการการบังคับใช้ ระเบียบ/ข้อปฏิบัติ รวมถึงประเมินและวิเคราะห์การดำเนินงานที่ไม่สอดคล้อง และพิจารณาการปรับปรุงระเบียบ/ข้อปฏิบัติ หรือกระบวนการ เพื่อให้มีความสอดคล้องและเหมาะสมกับสภาพแวดล้อมและวัฒนธรรมองค์กร

3. สื่อสาร ประชาสัมพันธ์และทำความเข้าใจเกี่ยวกับการปฏิบัติตามระเบียบ/ข้อปฏิบัติ ให้กับพนักงานและหน่วยงานต่าง ๆ ได้รับทราบและปฏิบัติได้อย่างถูกต้อง

<u>ข้อ 4 ดำเนินการกำหนดวัตถุประสงค์และกลยุทธ์ที่มุ่งเน้นความยั่งยืนขององค์กรบนพื้นฐานของหลักธรรมาภิบาล (Governance) ภายใต้แนวคิดขับเคลื่อนธุรกิจคู่สังคม รวมทั้งคำนึงถึงการกำกับด้านกฎหมาย ระเบียบข้อบังคับขององค์กร (Compliance) อย่างเป็นระบบ เพื่อสามารถสนับสนุน การกำหนดแนวปฏิบัติได้อย่างมีประสิทธิภาพ</u>

<u>หลักการพื้นฐาน</u>

1. มุ่งเน้นความยั่งยืนขององค์กร บนพื้นฐานของหลักธรรมาภิบาล (Governance) ภายใต้แนวคิดขับเคลื่อนธุรกิจคู่สังคม และพัฒนาระบบบริหารจัดการด้านการกำกับดูแลการปฏิบัติตามกฎระเบียบ

(Compliance Management System) โดยปรับปรุงกระบวนการดำเนินงานเพื่อวิเคราะห์ ประเมินความเสี่ยงต่อความไม่สอดคล้องกับกฎหมาย และกฎระเบียบ (Compliance Risk) ทั้งในด้านการเปลี่ยนแปลงกฎหมาย (Regulatory Risk) และด้านการปฏิบัติที่ไม่ถูกต้อง ไม่สอดคล้องกับกฎหมายและกฎระเบียบ เกี่ยวกับด้านดำเนินงาน (Operational Risk) เพื่อกำหนดมาตรการปรับปรุง แก้ไขต่อความไม่สอดคล้องกับกฎหมายและกฎระเบียบ (Compliance Risk) และสามารถสนับสนุนการกำหนดแนวปฏิบัติได้อย่างมีประสิทธิภาพ

แนวทางปฏิบัติ

หน่วยงานปฏิบัติ (1st Line)

1. ผู้บริหาร พนักงาน และลูกจ้าง ดำเนินการศึกษาและทำความเข้าใจกับหลักธรรมาภิบาล (Governance) การกำกับด้านกฎหมาย ระเบียบ ข้อบังคับขององค์กร (Compliance) และแนวทางปฏิบัติงานให้เป็นไปตามกฎเกณฑ์ขององค์กร

2. ผู้บังคับบัญชา กำกับดูแลและสอบทานการดำเนินการของพนักงานและลูกจ้าง ให้เป็นไปตามหลักธรรมาภิบาล (Governance) การกำกับด้านกฎหมาย ระเบียบ ข้อบังคับขององค์กร (Compliance) พร้อมทั้งสอบทานการปฏิบัติงานให้สอดคล้องกับกฎเกณฑ์ที่เกี่ยวข้องอย่างเคร่งครัด หรือละเมิด

3. ผู้บริหาร พนักงาน และลูกจ้าง ต้องตระหนักถึงหลักธรรมาภิบาล (Governance) การกำกับด้านกฎหมาย ระเบียบ ข้อบังคับขององค์กร (Compliance) พร้อมทั้งสอบทานการดำเนินการให้สอดคล้องกับกฎเกณฑ์อยู่เสมอ เพื่อให้บรรลุผลสำเร็จตามวัตถุประสงค์การดำเนินงานขององค์กร

หน่วยงานกำกับดูแลกระบวนการ (2nd Line)

1. กำหนดกรอบ แผนการดำเนินงาน และแนวทางในการปฏิบัติตามหลักธรรมาภิบาล (Governance) การกำกับด้านกฎหมาย ระเบียบ ข้อบังคับขององค์กร (Compliance) และแนวทางปฏิบัติงานให้เป็นไปตามกฎเกณฑ์ขององค์กรให้สอดคล้องและเหมาะสมกับองค์กร รวมทั้งควรมีการทบทวนและปรับปรุงให้มีความถูกต้องอย่างสม่ำเสมอ

2. ติดตามผลการปฏิบัติของหน่วยงานต่างๆ โดยพิจารณาถึงความสอดคล้องกับแนวทางปฏิบัติ ปฏิบัติตามหลักธรรมาภิบาล (Governance) การกำกับด้านกฎหมาย ระเบียบ ข้อบังคับขององค์กร (Compliance) และแนวทางปฏิบัติงานให้เป็นไปตามกฎเกณฑ์ขององค์กร

3. สื่อสาร ประชาสัมพันธ์และทำความเข้าใจเกี่ยวกับการปฏิบัติตามแนวปฏิบัติ ตามหลักธรรมาภิบาล (Governance) การกำกับด้านกฎหมาย ระเบียบ ข้อบังคับขององค์กรให้กับพนักงานและหน่วยงานต่างๆ ได้รับทราบอย่างถูกต้องและมีประสิทธิภาพ รวมถึงควรสร้างความตระหนักรับรู้อย่างทั่วถึงทั่วทั้งองค์กร

ข้อ 5 นำเทคโนโลยีดิจิทัลมาปรับใช้เป็นเครื่องมือในการสนับสนุนการปฏิบัติงาน เพื่อให้การดำเนินกิจการขององค์กรบรรลุผลสัมฤทธิ์ ตามเป้าประสงค์ที่กำหนดด้วยการบริหารจัดการที่ดีด้านเทคโนโลยีสารสนเทศครอบคลุมทั่วทั้งองค์กร และผู้มีส่วนได้ส่วนเสีย เพื่อสร้างคุณค่าจากการใช้เทคโนโลยีสารสนเทศที่มีความโปร่งใสและตรวจสอบได้ ควบคู่กับการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศที่เหมาะสม เพื่อลดภัยคุกคามต่าง ๆ ที่อาจเกิดขึ้นและกระทบการดำเนินกิจการที่สำคัญขององค์กร อาทิ การโจมตีทางไซเบอร์ (Cyber Attack) รวมทั้งการบริหารความต่อเนื่องทางธุรกิจ (Business Continuity Management: BCM) เพื่อสร้างความต่อเนื่องในการดำเนินการและให้บริการขององค์กรในขณะเกิดภาวะวิกฤตหรือเหตุการณ์ฉุกเฉิน

หลักการพื้นฐาน

1. มุ่งเน้นการพัฒนาระบบเทคโนโลยีดิจิทัล เพื่อสนับสนุนให้องค์กรก้าวสู่การเปลี่ยนแปลงและจัดให้มีกระบวนการบริหารจัดการระบบรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศตามมาตรฐาน ISO/IEC 27001 ซึ่งมีขอบเขตงานที่ครอบคลุมโครงสร้างพื้นฐานขององค์กรที่สำคัญ (Critical Infrastructure) โดยเฉพาะด้านสารสนเทศของศูนย์คอมพิวเตอร์ รวมทั้งการดาเนินการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศตามมาตรฐานสากล ISO/IEC27001 หรือมาตรฐานสากลอื่น ๆ อย่างต่อเนื่อง

2 . มุ่งมั่นพัฒนาองค์กรอย่างมีประสิทธิภาพ และตอบสนองความต้องการ ความคาดหวังของ ผู้มีส่วนได้ส่วนเสีย โดยกำหนดหลักการกระบวนการบริหารความต่อเนื่องทางธุรกิจ (Business Continuity Management: BCM) และแผนการบริหารความต่อเนื่องทางธุรกิจ (BCP) เพื่อสร้างความต่อเนื่องในการดำเนินการและให้บริการขององค์กรในขณะเกิดภาวะวิกฤตหรือเหตุการณ์ฉุกเฉิน

แนวทางปฏิบัติ

หน่วยงานปฏิบัติ (1st Line)

1. ผู้บริหาร พนักงาน และลูกจ้าง ตระหนักและดำเนินการตามระบบการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ อย่างเคร่งครัด รวมถึงการไม่ดำเนินการใดๆ ที่เสี่ยงต่อการละเมิดการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศขององค์กร

2. ผู้บริหาร พนักงาน และลูกจ้าง ดำเนินการศึกษา ทำความเข้าใจ และฝึกซ้อมสถานการณ์ที่อาจจะเกิดขึ้นตามการกระบวนการบริหารความต่อเนื่องทางธุรกิจ (Business Continuity Management: BCM) และแผนการบริหารความต่อเนื่องทางธุรกิจ (BCP) เพื่อสร้างความต่อเนื่องในการดำเนินการและให้บริการขององค์กรในขณะเกิดภาวะวิกฤตหรือเหตุการณ์ฉุกเฉิน

3. ผู้บริหาร พนักงาน และลูกจ้าง ตระหนักและดำเนินการตามระบบการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (ภัยคุกคามทางไซเบอร์) อย่างเคร่งครัด รวมถึงการไม่ดำเนินการใด ๆ ที่เสี่ยงต่อการละเมิดการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศขององค์กร

หน่วยงานกำกับดูแลกระบวนการ (2nd Line)

1. กำหนดกรอบ และแนวทางในการปฏิบัติและบริหารจัดการระบบรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ ตามมาตรฐาน ISO/IEC 27001 รวมทั้งการดำเนินการบริหารจัดการความเสี่ยง ด้านความมั่นคงปลอดภัยสารสนเทศตามมาตรฐานสากล ISO/IEC27001 อย่างต่อเนื่อง และการบริหารความต่อเนื่องทางธุรกิจ (Business Continuity Management: BCM) เพื่อสร้างความต่อเนื่องในการดำเนินการและให้บริการขององค์กรในขณะเกิดภาวะวิกฤตหรือเหตุการณ์ฉุกเฉิน

2. ติดตามผลการปฏิบัติของหน่วยงานต่าง ๆ โดยพิจารณาถึงความสอดคล้องกับแนวปฏิบัติ และแผนการดำเนินงานที่กำหนดไว้ โดยควรมีการทบทวนเพื่อให้ข้อมูลเป็นปัจจุบัน พร้อมทั้งมีการจัดทำแผนเฝ้าระวังและฝึกซ้อมเพื่อให้มีการป้องกันแก้ไขได้ทันกาลอยู่เสมอ

3. สื่อสาร ประชาสัมพันธ์และทำความเข้าใจเกี่ยวกับการปฏิบัติตามแนวปฏิบัติ และแผนการดำเนินงานให้กับพนักงานและหน่วยงานต่างๆ ได้รับทราบอย่างถูกต้องมีประสิทธิภาพและประสิทธิผล

ข้อ 6 จัดให้มีการบูรณาการร่วมกันระหว่างหน่วยงานในการติดตามความคืบหน้า สอบทาน และตรวจสอบกระบวนการทำงานต่าง ๆ อย่างสม่ำเสมอ เพื่อปรับปรุงแก้ไขการดำเนินงานให้มีประสิทธิภาพและมุ่งสู่

การพัฒนาอย่างยั่งยืน (Sustainable Development) ตลอดจนการสื่อสารข้อมูลต่าง ๆ ร่วมกับผู้บริหารและพนักงานทุกระดับ เพื่อสนับสนุนให้เกิดการแลกเปลี่ยนองค์ความรู้ (Knowledge Sharing) ภายใต้การสื่อสารข้อมูลทั่วทั้งองค์กรจนเกิดการบูรณาการร่วมกัน

หลักการพื้นฐาน

1. มุ่งเน้นให้องค์กรเกิดการบูรณาการร่วมกันระหว่างหน่วยงานต่าง ๆ ในการติดตามความคืบหน้า สอบทาน และตรวจสอบกระบวนการทำงานต่าง ๆ อย่างสม่ำเสมอ เพื่อปรับปรุงแก้ไขการดำเนินงานให้มีประสิทธิภาพและมุ่งสู่การพัฒนาอย่างยั่งยืน (Sustainable Development) ตลอดจนการสื่อสารข้อมูลต่าง ๆ ร่วมกับผู้บริหารและพนักงานทุกระดับ เพื่อสนับสนุนให้เกิดการแลกเปลี่ยนองค์ความรู้ (Knowledge Sharing) ภายใต้การสื่อสารข้อมูลทั่วทั้งองค์กร

แนวทางปฏิบัติ

หน่วยงานปฏิบัติ (1st Line)

1. ผู้บริหาร พนักงาน และลูกจ้าง ดำเนินการบูรณาการร่วมกันระหว่างหน่วยงานต่าง ๆ เพื่อปรับปรุงแก้ไขการดำเนินงานให้มีประสิทธิภาพและมุ่งสู่การพัฒนาอย่างยั่งยืน (Sustainable Development) และเกิดองค์ความรู้และนวัตกรรมใหม่ ๆ ขึ้น

2. ผู้บังคับบัญชา กำกับดูแลและสอบทานการดำเนินการของพนักงานและลูกจ้างให้เกิดการแลกเปลี่ยนองค์ความรู้และเกิดการสร้างนวัตกรรมที่สามารถผลักดันเป้าหมายหรือความท้าทายขององค์กรให้บรรลุเป้าหมาย

3. ผู้บริหาร พนักงาน และลูกจ้าง ต้องตระหนักและเกิดการแลกเปลี่ยนองค์ความรู้และเกิดการสร้างนวัตกรรมภายในองค์กร

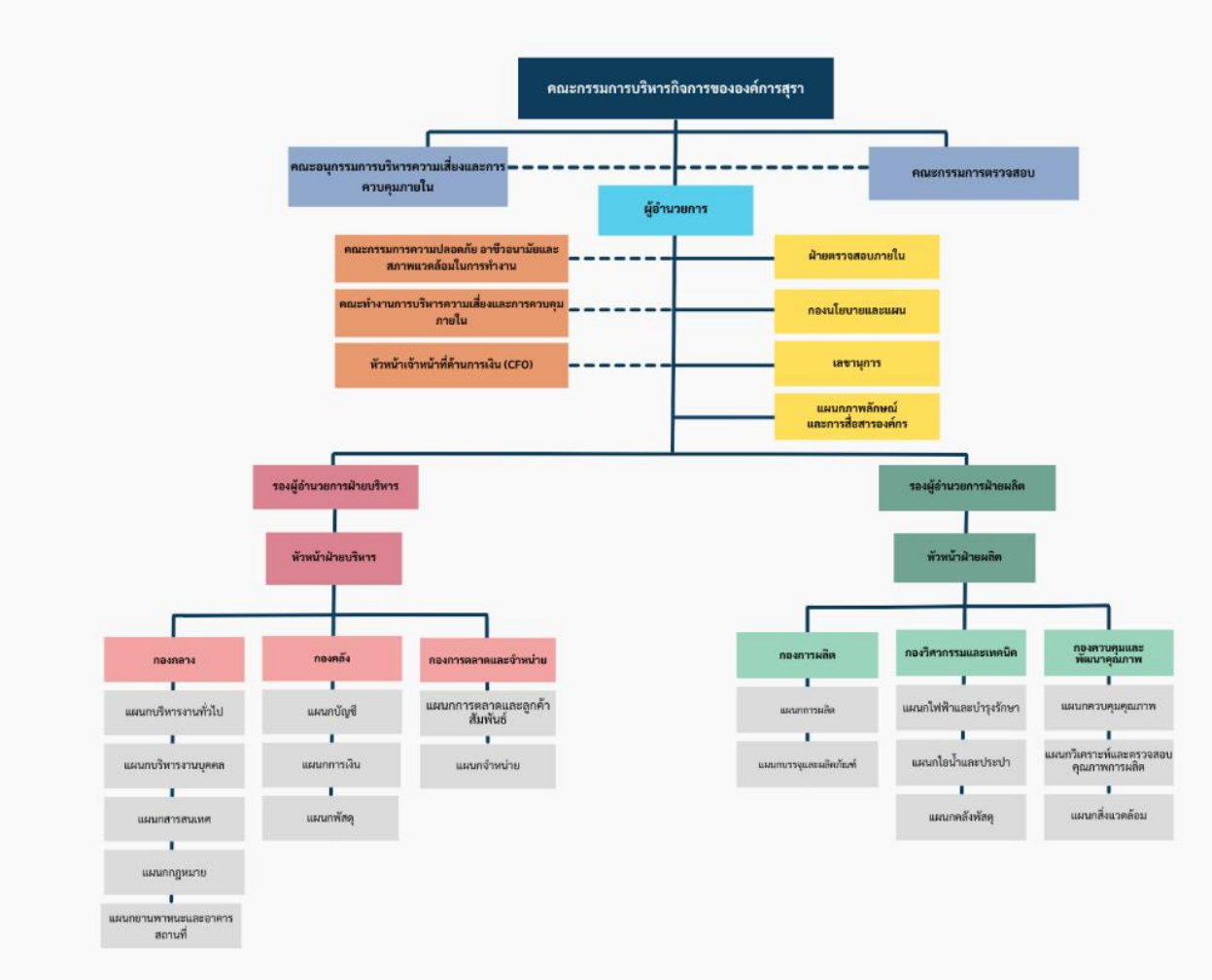
หน่วยงานกำกับดูแลกระบวนการ (2nd Line)

1. กำหนดกรอบ นโยบาย แผนการดำเนินงาน และแนวทางในการปฏิบัติในการมุ่งสู่การพัฒนาอย่างยั่งยืน (Sustainable Development) และผลักดันการสร้างองค์ความรู้และนวัตกรรมใหม่ ๆ

2. ติดตามผลการปฏิบัติของหน่วยงานต่างๆ โดยพิจารณาถึงความสอดคล้องกับแนวทางปฏิบัติ และแผนการดำเนินงานที่กาหนดไว้ และสอบทานการดำเนินงานที่เกิดการแลกเปลี่ยนองค์ความรู้และเกิดการสร้างนวัตกรรมที่สามารถผลักดันเป้าหมายหรือความท้าทายขององค์กรให้บรรลุเป้าหมาย และควรมีการทบทวนและประเมินช่องโหว่และความเสี่ยงในการดำเนินงานที่อาจจะเกิดขึ้น เพื่อให้ผู้รับผิดชอบและผู้บริหารได้ใช้ประกอบการตัดสินใจได้

3. สื่อสาร ประชาสัมพันธ์และทำความเข้าใจและสร้างความตระหนักรับรู้เกี่ยวกับการบูรณาการร่วมกันระหว่างหน่วยงานต่าง ๆ เพื่อปรับปรุงแก้ไขการดำเนินงานให้มีประสิทธิภาพและมุ่งสู่การพัฒนาอย่างยั่งยืน (Sustainable Development) อย่างทั่วถึงทั้งองค์กร

6.2 โครงสร้างการบริหารความเสี่ยงและการควบคุมภายในขององค์การสุรา กรมสรรพสามิต



รูปที่ 7 โครงสร้างการบริหารความเสี่ยงและการควบคุมภายในขององค์การสุรา กรมสรรพสามิต

องค์การสุราฯ ตระหนักว่าการบริหารความเสี่ยงมีความสำคัญต่อการดำเนินธุรกิจ เนื่องจากระบบการบริหารความเสี่ยง ที่มีประสิทธิภาพและประสิทธิผล จะเป็นส่วนหนึ่งของการกำกับดูแลกิจการที่ดี ป้องกันการเกิดความเสี่ยงระดับองค์กร ซึ่งจะนำองค์กรไปสู่การเติบโตทางธุรกิจ อย่างมั่นคงและยั่งยืน ดังนั้นคณะกรรมการ คณะอนุกรรมการ ผู้บริหาร และคณะทำงาน จึงได้ปรับปรุงกระบวนการบริหารความเสี่ยงขององค์การสุราฯ ให้เป็นไปตามมาตรฐานในระดับสากล โดยยึดตามกรอบการบริหารความเสี่ยงของ Committee of Sponsoring Organizations of The Treadway Commission (COSO ERM) เป็นแนวทางในการดำเนินการ ซึ่งประกอบตามแผนภาพนี้

รูปที่ 8 กรอบการบริหารความเสี่ยงของ Committee of Sponsoring Organizations of The Treadway Commission (COSO ERM)

<u>องค์ประกอบการบริหารความเสี่ยง COSO ERM ประกอบไปด้วย</u>

1. การกำกับดูแลกิจการและวัฒนธรรมองค์กร ประกอบด้วยบทบาทของคณะกรรมการ โครงสร้างการดำเนินงานตามเป้าหมายกลยุทธ์ การกำหนดวัฒนธรรมที่พึงประสงค์ การยึดมั่นต่อค่านิยมองค์กร และการสร้างความเข้มแข็งด้านทุนมนุษย์โดยบุคลากรในองค์กรต้องให้ความสำคัญและมีความรับผิดชอบร่วมกันในการทำให้เกิดการบริหารความเสี่ยง ทั่วทั้งองค์กรที่เป็นระบบและมีประสิทธิผล

2. กลยุทธ์และวัตถุประสงค์องค์กร ประกอบด้วย การวิเคราะห์บริบทของธุรกิจ การกำหนดระดับความสามารถในการรับความเสี่ยง การประเมินทางเลือกของกลยุทธ์จัดการความเสี่ยงองค์กร และการวางเป้าประสงค์ทางธุรกิจภายใต้ความเสี่ยง เพื่อส่งผลให้กระบวนการบริหารความเสี่ยงทั่วทั้งองค์กรให้เกิดประสิทธิภาพ

3. เป้าหมายผลการดำเนินงาน ประกอบด้วย การระบุความเสี่ยง การประเมินระดับความรุนแรง การจัดลำดับความเสี่ยง การตอบสนอง ความเสี่ยง และการพิจารณาภาพรวมของความเสี่ยงองค์กรทั้งหมด

4. การทบทวน และ ปรับปรุง ประกอบด้วย การประเมินความเปลี่ยนแปลงที่เกิดขึ้นจากการบริหารความเสี่ยงการทบทวนความสามารถในการจัดการและระดับความเสี่ยง และการปรับปรุงพัฒนาระบบการบริหารความเสี่ยงองค์กร

5. สารสนเทศการสื่อสาร และการรายงาน ประกอบด้วย การใช้สารสนเทศสนับสนุนการบริหารความเสี่ยงการใช้ช่องทางการสื่อสารต่างๆ สนับสนุนการบริหารความเสี่ยง และการรายงานความสำเร็จการดำเนินการรวมทั้งวัฒนธรรม ความเสี่ยงที่เกิดขึ้น

เพื่อส่งเสริมและผลักดันให้องค์กรมีแนวทางการบริหารความเสี่ยงที่มีประสิทธิภาพและสามารถสร้างมูลค่าเพิ่ม (Value Enhancement) ให้กับองค์กรได้ โดยการกำหนดระดับที่สะท้อน การพัฒนาการของการบริหารความเสี่ยง ตั้งแต่การกำกับดูแลที่ดีและสร้างวัฒนธรรมความเสี่ยง การกำหนดนโยบาย/ กลยุทธ์ขององค์กรในการบริหารความเสี่ยง การกำหนดวัตถุประสงค์และยุทธศาสตร์องค์กรที่ชัดเจน กระบวนการในการจัดการความ

เสี่ยงที่เป็นระบบตั้งแต่การระบุความเสี่ยง การประเมินความเสี่ยงและการบริหารความเสี่ยงในแต่ละประเภท จนถึงระดับที่การบริหารความเสี่ยงแบบบูรณาการ รวมทั้งประเด็นสำคัญของการบริหารความเสี่ยง ตั้งแต่การสร้างความรู้ ความเข้าใจ ความตระหนักเรื่องการบริหารความเสี่ยง การบริหารเทคโนโลยีสารสนเทศเพื่อการจัดการที่ดี (IT Governance) ผลลัพธ์ของการบริหารความเสี่ยง และการพิจารณา การบริหารความเสี่ยงเป็นส่วนหนึ่งของการพิจารณาผลตอบแทน ของผู้ที่เกี่ยวข้อง

ประเภทของความเสี่ยง

องค์การสุราฯ แบ่งความเสี่ยงออกเป็น 4 ประเภท ตามกรอบการบริหารความเสี่ยงของ COSO ดังนี้

1) ความเสี่ยงด้านกลยุทธ์ (Strategic Risks: S) คือ ความเสี่ยงที่เกิดจากการกำหนดแผนกลยุทธ์ แผนดำเนินงานที่นำไปปฏิบัติไม่เหมาะสมหรือไม่สอดคล้องกับปัจจัยภายในและสภาพแวดล้อมภายนอก อันส่งผลกระทบต่อการบรรลุวิสัยทัศน์ พันธกิจหรือสถานะขององค์กร

2) ความเสี่ยงด้านการปฏิบัติงาน (Operational Risks: O) คือ ความเสี่ยงที่เกิดจากการดำเนินงานทุก ๆ ขั้นตอนโดยครอบคลุมถึงปัจจัยที่เกี่ยวข้องกับกระบวนการ อุปกรณ์ เทคโนโลยีสารสนเทศหรือแม้แต่บุคลากรในการปฏิบัติงาน

3) ความเสี่ยงด้านการเงิน (Financial Risks: F) คือ ความเสี่ยงที่เกิดจากการเบิกจ่ายงบประมาณไม่เป็นไปตามแผนงบประมาณถูกตัด งบประมาณที่ได้รับไม่สอดคล้องกับสถานการณ์ของภารกิจที่เปลี่ยนแปลงไป ทำให้การจัดสรรไม่เพียงพอ

4) ความเสี่ยงด้านกฎ ระเบียบ ข้อบังคับ (Compliance Risks: C) คือ ความเสี่ยงที่เกิดจากการไม่สามารถปฏิบัติตามกฎระเบียบ หรือกฎหมายที่เกี่ยวข้องได้

การระบุความเสี่ยง

การระบุปัจจัยเสี่ยงในระดับองค์กร เป็นการระบุปัจจัยที่มีผลกระทบในเชิงลบต่อยุทธศาสตร์ เป้าหมายและการปฏิบัติงานในระดับองค์กร รวมทั้งปัจจัยที่จะทำให้สูญเสียโอกาสทางธุรกิจ และ Intelligent Risk โดยมีประเด็นสำคัญที่นำมาพิจารณาในการระบุปัจจัยเสี่ยงให้ครอบคลุมหัวข้อดังต่อไปนี้

1. นโยบายภาครัฐ
2. แผนวิสาหกิจ แผนปฏิบัติการ
3. SWOT ขององค์กร
4. Supply Chain
5. นโยบายของผู้อำนวยการ/คณะกรรมการบริหารฯ
6. กฎหมายที่เกี่ยวข้อง
7. ความต้องการความคาดหวังของผู้มีส่วนได้ส่วนเสีย
8. ตัวชี้วัดองค์กร
9. ความเสี่ยงคงเหลือจากปีที่ผ่านมา และความเสี่ยงคงเหลือจากการควบคุมภายในที่ไม่เพียงพอ
10. การการควบคุมภายในที่ไม่เพียงพอ
11. Value Creation และ Value Enhancement

ทั้งนี้ จะต้องมีการศึกษาและพิจารณาถึงเหตุการณ์ที่จะทำให้องค์กรไม่บรรลุวัตถุประสงค์ต่าง ๆ ตามที่กำหนดเบื้องต้นไว้ในแผน โดยพิจารณาทั้งปัจจัยภายใน ปัจจัยภายนอก เหตุการณ์ที่เกิดขึ้นแล้ว เหตุการณ์ปัจจุบันและเหตุการณ์ที่คาดว่าจะเกิดขึ้นในอนาคต

ในการระบุความเสี่ยง ควรพิจารณาปัจจัยความเสี่ยงต่าง ๆ ให้ครบถ้วนและครอบคลุม ตัวอย่างเช่น

• ปัจจัยภายในและภายนอก ที่อาจส่งผลกระทบต่อการดำเนินงาน เช่น

- ปัจจัยภายใน ได้แก่ ทรัพยากรบุคคล ระบบเทคโนโลยีสารสนเทศ กระบวนการ และระบบงานสนับสนุนต่าง ๆ

- ปัจจัยภายนอก ได้แก่ การเมือง กฎระเบียบ กฎหมาย สภาวะตลาด เทคโนโลยี ความไม่สงบทางการเมือง และภัยธรรมชาติ เป็นต้น

• เหตุการณ์ในอดีต ความเสี่ยงที่มีอยู่ในปัจจุบัน และแนวโน้มของเหตุการณ์ที่อาจจะเกิดขึ้นในอนาคต

• เหตุการณ์ปัจจุบัน อาทิเช่น เหตุฉุกเฉิน สถานการณ์เฉพาะหน้าที่กำลังเกิด สังคมและวิถีชีวิตของสังคมปัจจุบัน เทคโนโลยีปัจจุบัน

• เหตุการณ์อนาคต อาทิเช่น สิ่งที่มีแนวโน้มจะเกิดขึ้นตามกาลเวลาหรือจากเหตุการณ์ปัจจุบันเป็นสาเหตุให้เกิดเหตุการในอนาคตได้

• นวัตกรรม ผลิตภัณฑ์ และบริการใหม่ ๆ ที่องค์กรต้องการพัฒนา

• โอกาสหรือกิจกรรมใหม่ ๆ ที่อาจเพิ่มคุณค่าให้กับองค์กร

สรุปประเด็นเหตุการณ์ที่อาจเกิดขึ้นซึ่งมีผลกระทบต่อการบรรลุวัตถุประสงค์ และสาเหตุของเหตุการณ์หรือความเสี่ยงดังกล่าวให้เป็นลายลักษณ์อักษร เพื่อหารือร่วมกันระหว่างผู้บริหารระดับสูง หากเหตุการณ์ที่มีผลกระทบในเชิงลบถือเป็นความเสี่ยงที่ผู้บริหารต้องประเมินและจัดการความเสี่ยงนั้น สำหรับเหตุการณ์ที่มีผลกระทบในเชิงบวกเป็นโอกาสซึ่งผู้บริหารควรนำไปพิจารณาอีกครั้งในกระบวนการกำหนดวัตถุประสงค์ และกลยุทธ์ในการดำเนินงานต่อไป

<u>การกำหนดค่า Risk Appetite และ Risk Tolerance</u>

ค่าระดับความเสี่ยงที่ยอมรับได้ (Risk Appetite : RA) หมายถึง เกณฑ์ของความเสี่ยงที่องค์การสุรา กรมสรรพสามิต ยอมรับได้เพื่อช่วยให้องค์การสุราฯ บรรลุเป้าหมายที่กำหนดนั้น จะระบุเป็นเป้าหมายค่าเดียว หรือระบุเป็นช่วงก็ได้ ซึ่งขึ้นอยู่กับความเหมาะสมของแต่ละปัจจัยเสี่ยง

ปัจจัยที่ใช้กำหนดระดับความเสี่ยงที่ยอมรับได้ ได้แก่

• ความต้องการของผู้มีส่วนได้ส่วนเสีย

• วัตถุประสงค์ เป้าหมาย วิสัยทัศน์ พันธกิจ

• ความเสี่ยงในการดำเนินงาน

• ปัจจัยภายในองค์กร ที่มีมุมมองต่อความเสี่ยงรับความเสี่ยงได้หรือไม่ยอมรับความเสี่ยง (Risk Taker vs Risk Averse)

• ปัจจัยภายนอกองค์กร ได้แก่ สภาพแวดล้อมต่าง ๆ ที่เกี่ยวข้องกับการดำเนินธุรกิจ

• ระดับความเสี่ยงที่ยอมรับได้ สามารถกำหนดได้ทั้งเชิงปริมาณและเชิงคุณภาพ

ขั้นตอนการกำหนดระดับความเสี่ยงที่ยอมรับได้ ประกอบด้วย

1. การวิเคราะห์ความคาดหวังของผู้มีส่วนได้ส่วนเสีย ทั้งจากภายในและภายนอกเกี่ยวกับระดับความเสี่ยงที่ยอมรับได้

2. การกำหนดระดับความเสี่ยงที่ยอมรับได้จากระดับบนลงสู่ระดับล่าง (Top – down) โดยเชื่อมโยงเข้ากับกลยุทธ์และวัตถุประสงค์การดำเนินงาน

3. การกำหนดระดับความเสี่ยงที่ยอมรับได้จากระดับล่างขึ้นสู่ระดับบน (Bottom – up) จากการวิเคราะห์ข้อมูลความเสี่ยงในแต่ละด้าน

ประเภทของความเสี่ยง	ระดับที่ยอมรับได้	คำอธิบาย/แนวทางปฏิบัติ
กลยุทธ์ (Strategic)	ต่ำ	• จัดให้มีเงินลงทุนเพื่อดำเนินโครงการใหม่ ๆ เพื่อการวิจัยและพัฒนา
ปฏิบัติการ (Operational)	ต่ำ	• ยอมรับความเสี่ยงได้ต่ำ สำหรับเรื่องความปลอดภัยและอาชีวอนามัย • ยอมรับความเสี่ยงได้ต่ำ สำหรับการปฏิบัติงานในกระบวนการทำงานที่ทำอยู่เป็นประจำ
การเงิน (Finance)	ต่ำ	• ยอมรับความเสี่ยงได้ต่ำ สำหรับผลขาดทุนจากการบริหารเงิน (Treasury Operations) • การทำธุรกรรมเพื่อการเก็งกำไร (Speculative) สามารถทำได้ตามความจำเป็นเท่านั้น
การปฏิบัติตามกฎระเบียบ (Compliance)	ต่ำ	• ยอมรับความเสี่ยงระดับต่ำ ผู้มีส่วนได้ส่วนเสีย มีการแจ้งข้อร้องเรียนที่ไม่รุนแรงสามารถดำเนินการแก้ไขหรือชี้แจงได้ ภายใต้กฎ ระเบียบ ข้อบังคับ นโยบายของรัฐ หน่วยงานที่กำกับดูแล และหน่วยงานที่เกี่ยวข้อง

รูปที่ 9 ตัวอย่างการกำหนดระดับความเสี่ยงที่ยอมรับได้เชิงคุณภาพ

ช่วงเบี่ยงเบนของระดับความเสี่ยงที่ยอมรับได้ (Risk Tolerance : RT) หมายถึง ระดับความเบี่ยงเบนจากเกณฑ์ หรือประเภทของความเสี่ยงที่ยอมรับได้ โดยดำเนินการบริหารความเสี่ยงให้อยู่ภายในเกณฑ์ที่ยอมรับได้ (Risk Appetite) และช่วงเบี่ยงเบนที่องค์การสุราฯ ยอมรับได้ (Risk Tolerance) โดยเชื่อมโยงกับวัตถุประสงค์ ตัวชี้วัด และเป้าหมายขององค์การสุราฯ เพื่อทำให้มั่นใจได้ว่าสามารถดำเนินการให้บรรลุเป้าหมายและวัตถุประสงค์ขององค์การสุราฯ ได้

6.3 การบริหารความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ (Information Security Risk Management Procedure)

เพื่อให้ความเสี่ยงทางด้านเทคโนโลยีสารสนเทศอยู่ในระดับความเสี่ยงที่องค์กรสามารถยอมรับได้ (Risk Appetite) และลดความผิดพลาดที่อาจเกิดขึ้นจากการดำเนินงานทางด้านเทคโนโลยีสารสนเทศ จึงได้มีการการกำหนดกระบวนการการบริหารความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ (Information Security Risk Management Procedure) ซึ่งเป็นไปตามขั้นตอนการประเมินผลและการบริหารจัดการความเสี่ยง ตามมาตรฐาน ISO27001 โดยมีรายละเอียดดังต่อไปนี้

6.3.1 หน้าที่ความรับผิดชอบ

บทบาท	หน้าที่ความรับผิดชอบ
คณะกรรมการระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (ISMS Committee)	■ พิจารณาอนุมัติขั้นตอนการดำเนินงานสำหรับบริหารความเสี่ยงและเกณฑ์การประเมินความเสี่ยง ■ พิจารณาอนุมัติขั้นตอนการดำเนินงานสำหรับบริหารความเสี่ยงและแผนจัดการความเสี่ยง ■ พิจารณาอนุมัติผลการจัดการความเสี่ยง
คณะทำงานระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (ISMS Working Team)	■ จัดทำขั้นตอนการด้าเนินงานส้าหรับบริหารความเสี่ยงและเกณฑ์การประเมินความเสี่ยง ■ กำหนดสถานการณ์ความเสี่ยง ■ ดำเนินการประเมินความเสี่ยง ■ จัดทำรายงานผลการประเมินความเสี่ยง ■ จัดทำแผนปฏิบัติตามแผนจัดการความเสี่ยง ■ ติดตามความคืบหน้าของการดำเนินการตามแผนจัดการความเสี่ยง ■ นำเสนอความคืบหน้าของแผนจัดการความเสี่ยงในการประชุม
เจ้าของความเสี่ยง (Risk Owner)	■ พิจารณาความถูกต้องเหมาะสมของผลการประเมินความเสี่ยงและแผนการจัดการความเสี่ยง
ผู้รับผิดชอบแผนจัดการความเสี่ยง (Risk Responsible person)	■ สรุปและจัดทำรายงานความคืบหน้าของการดำเนินการตามแผนจัดการความเสี่ยง ■ ตรวจสอบความถูกต้องเหมาะสมของแผนจัดการความเสี่ยง
ระบบสารสนเทศ	■ ระบบที่ให้บริการภายในศูนย์คอมพิวเตอร์หลักขององค์การสุราฯ ได้แก่ ● ระบบเครือข่าย (Network) ● เครื่องคอมพิวเตอร์แม่ข่ายระบบ ERP (Server)

6.3.2 ขั้นตอนการดำเนินการ

องค์การสุราฯ ได้นำเทคโนโลยีสารสนเทศมาใช้งานเพื่อช่วยประสิทธิภาพการดำเนินงานและให้บริการประชาชนได้รับความสะดวก รวดเร็ว ขณะเดียวกันระบบเทคโนโลยีสารสนเทศ อาจได้รับความเสียหายจากการถูกโจมตีจากไวรัสคอมพิวเตอร์ จากบุคลากร จากปัญหาไฟฟ้า จากอัคคีภัย หรือปัจจัยทั้งภายในและภายนอก ส่งผลกระทบต่อการดำเนินการขององค์การ ดังนั้น เพื่อให้ระบบเทคโนโลยีสารสนเทศมีความมั่นคงปลอดภัย ซึ่งมีขั้นตอนการดำเนินการประเมินความเสี่ยงของระบบเทคโนโลยีสารสนเทศ ดังนี้

6.3.2.1 การบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ

การจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ คือ กระบวนการทำงานที่ช่วยให้แผนกสารสนเทศสามารถประเมินความเสี่ยงและโอกาสของเหตุการณ์ต่าง ๆ เพื่อนำข้อมูลของการประเมินความเสี่ยงที่ได้มาวิเคราะห์และจัดระดับความสำคัญ เพื่อวางแผนป้องกันความเสี่ยงหรือสร้างโอกาสและนำไปสร้างมาตรการเพื่อให้แผนกสารสนเทศบรรลุผลสำเร็จของพันธกิจที่ตั้งไว้

6.3.2.2 การระบุเหตุการณ์ความเสี่ยง

การระบุเหตุการณ์ความเสี่ยง (Risk Scenario) คือ เป็นการค้นหาและระบุเหตุการณ์ที่อาจเกิดขึ้นและส่งผลกระทบต่อองค์การทั้งภายในและภายนอก ทั้งเหตุการณ์ที่เคยเกิดขึ้นมาแล้วในอดีต และการคาดการณ์ในอนาคต ส่งผลให้การดำเนินงานไม่บรรลุผลสำเร็จตามวัตถุประสงค์ที่กำหนดไว้ โดยระบุเหตุการณ์ความเสี่ยงที่คาดว่าจะส่งผลทำให้สารสนเทศสูญเสียความลับ (Confidentiality) ความถูกต้องสมบูรณ์ (Integrity) และความพร้อมใช้ (Availability) เพื่อให้สามารถกำหนดแผนจัดการความเสี่ยงได้ตรงตามสาเหตุและสามารถลดความเสี่ยงลงได้อย่างมีประสิทธิผล

6.3.2.3 การระบุมาตรการควบคุมปัจจุบัน

มาตรการควบคุมปัจจุบัน (Existing Control) เป็นมาตรการที่ใช้หรือมีการดำเนินการอยู่เพื่อจัดการกับความเสี่ยงที่อาจเกิดขึ้นจากภัยคุกคามที่อาศัยประโยชน์จากช่องโหว่มาสร้างความเสียหายต่อทรัพย์สินสารสนเทศที่มีอยู่ โดยที่มาตรการควบคุมปัจจุบันอาจเป็นได้ทั้ง วิธีการควบคุม การจ้างบริการ การใช้อุปกรณ์มาควบคุม เป็นต้น

6.3.2.4 การประเมินผลกระทบ

ผลกระทบ (Impact) คือ ผลลัพธ์ของเหตุการณ์ที่เกิดขึ้นจากภัยคุกคามต่าง ๆ ที่เกิดขึ้น ซึ่งมีผลกระทบกับระบบสารสนเทศหรือต่อธุรกิจและองค์กร โดยอาจสร้างความเสียหายกับระบบสารสนเทศ ทรัพย์สินสารสนเทศ ทรัพยากรหรือองค์การในด้านต่าง ๆ ทำให้ต้องดำเนินการพิจารณามาตรการควบคุมที่เป็นปัจจุบันประกอบว่ามาตรการดังกล่าวสามารถลดผลกระทบที่เกิดขึ้นได้หรือไม่ และระบุระดับผลกระทบขององค์การสุราฯ ได้ให้ความสำคัญต่อผลกระทบ 5 ด้าน คือ 1. ด้านกลยุทธ์ 2. ด้านการเงิน 3. ด้านการดำเนินงาน 4. ด้านภาพลักษณ์และชื่อเสียงขององค์การสุราฯ และ 5. ด้านกฎหมาย ระเบียบ ข้อบังคับ

6.3.2.5 การประเมินโอกาสเกิดของเหตุการณ์

โอกาสเกิดของเหตุการณ์ (Likelihood) คือ โอกาสหรือความถี่ของการเกิดเหตุการณ์ที่ก่อให้เกิดความสูญเสีย โดยจำแนกเป็นระดับน้อยมาก น้อย ปานกลาง สูง สูงมาก หรือร้อยละของโอกาสที่จะเกิดขึ้นได้ อย่างไรก็ตามการประเมินความสูญเสียที่ไม่เคยเกิดขึ้นในอดีตเป็นเรื่องยาก ดังนั้น จึงไม่ควรใช้ข้อมูลในอดีตอ้างอิงเพียงอย่างเดียว แต่ควรใช้การวิเคราะห์ปัจจัยเสี่ยงขององค์การด้วยการวิเคราะห์ความเสี่ยงภายใต้สถานการณ์ที่เป็นไปได้ทั้งหมด การศึกษาข้อมูลเพิ่มเติมจากองค์การอื่น ๆ หรือผู้เชียวชาญด้านการบริหารความเสี่ยงอื่น ซึ่งจะช่วยให้การประเมินความเสี่ยงสมเหตุสมผลมากขึ้น ในการระบุระดับโอกาสเกิดของเหตุการณ์

6.3.2.6 การประเมินค่าระดับความเสี่ยง

ค่าระดับความเสี่ยง (Risk Level) เกิดจากการคำนวณโดยนำเอาค่าคะแนนของโอกาสที่จะเกิดความเสี่ยง x ค่าคะแนนของผลกระทบจากความเสี่ยงที่เกิดขึ้น

ค่าระดับความเสี่ยง = ค่าคะแนนของโอกาสที่จะเกิดความเสี่ยง x ค่าคะแนนของผลกระทบจากความเสี่ยงที่เกิดขึ้น

ค่าระดับความเสี่ยง (Risk Level) ที่คำนวณได้นำมาเปรียบเทียบตารางการจัดระดับความเสี่ยงเพื่อจัดระดับความสำคัญ สำหรับจัดการความเสี่ยงที่ประเมินได้ โดยพิจารณาจากตารางการจัดระดับความเสี่ยง ดังนี้

ตารางจัดระดับความเสี่ยง (Risk Matrix) ขององค์การสุรา กรมสรรพสามิต

ค่าคะแนนผลกระทบจากความเสี่ยง (Impact)						
5	5 (1x5)	10 (2x5)	15 (3x5)	20 (4x5)	25 (5x5)	
4	4 (1x4)	8 (2x4)	12 (3x4)	16 (4x4)	20 (5x4)	
3	3 (1x3)	6 (2x3)	9 (3x3)	12 (4x3)	15 (5x3)	
2	2 (1x2)	4 (2x2)	6 (3x2)	8 (4x2)	10 (5x2)	
1	1 (1x1)	2 (2x1)	3 (3x1)	4 (4x1)	5 (5x1)	Risk Boundary
	1	2	3	4	5	

ค่าคะแนนโอกาสเกิดความเสี่ยง (Likelihood)

รูปที่ 10 ตารางจัดระดับความเสี่ยง (Risk Matrix)

6.3.2.7 พิจารณาระดับความเสี่ยงกับเกณฑ์การยอมรับความเสี่ยง

เมื่อได้ค่าของระดับความเสี่ยงแล้ว ผู้มีอำนาจตัดสินใจจะต้องพิจารณาระดับความเสี่ยงที่ยอมรับได้ เพื่อหาแนวทางในการตอบสนองความเสี่ยงโดยมีทางเลือกสำหรับตอบสนองความเสี่ยง

ระดับ ความเสี่ยง	ระดับสี ความเสี่ยง	ความหมาย
ต่ำ (1-3 คะแนน)	ความเสี่ยงต่ำ	หมายถึง ระดับที่**ยอมรับได้โดยไม่ต้องควบคุมไม่ต้องมีการจัดการเพิ่มเติม**
ปานกลาง (4-6 คะแนน)	ความเสี่ยงปานกลาง	หมายถึง ระดับที่พอ**ยอมรับได้ แต่ต้องมีการควบคุมเพื่อป้องกัน** ไม่ให้ความเสี่ยงเคลื่อนย้ายไปยังระดับที่รับไม่ได้
สูง (7-12 คะแนน)	ความเสี่ยงสูง	หมายถึง ระดับที่ไม่สามารถยอมรับได้ โดยต้องจัดการความเสี่ยงเพื่อให้อยู่ในระดับที่ยอมรับได้
สูงมาก (13-25 คะแนน)	ความเสี่ยงสูงมาก	หมายถึง ระดับที่ไม่สามารถยอมรับได้ จำเป็นต้องเร่งจัดการความเสี่ยงให้อยู่ในระดับที่ยอมรับได้ทันที

หมายเหตุ ผลกระทบ (Impact) ที่มีคะแนนความเสี่ยงอยู่ในระดับสูง ต้องบริหารความเสี่ยงทั้งหมดโดยคะแนนรวมจะพิจารณาจากผลกระทบเป็นหลัก

6.3.2.8 การเลือกแนวทางการตอบสนองความเสี่ยง

การเลือกแนวทางตอบสนองความเสี่ยงเป็นการพิจารณาว่าความเสี่ยงที่วิเคราะห์ได้อยู่ในระดับที่ยอมรับได้หรือไม่ และหากยอมรับไม่ได้ก็ต้องเลือกแนวทางในการตอบสนองความเสี่ยง โดยแนวทางการตอบสนองความเสี่ยงแบ่งเป็น 4 แนวทาง และสัมพันธ์กับระดับความเสี่ยง คือ

1) การถ่ายโอนความเสี่ยง (Transfer) คือ เป็นความเสี่ยงที่ต้องมีการถ่ายโอนหรือแบ่งความเสี่ยงบางส่วนไปยังบุคคลหรือองค์กรอื่น เพื่อลดโอกาสเกิดความเสี่ยงหรือผลกระทบ เช่น การซื้อประกัน หรือจัดจ้างผู้ให้บริการ เป็นต้น

2) การลดความเสี่ยง (Reduction) คือ เป็นความเสี่ยงที่ไม่สามารถยอมรับความเสี่ยงได้ต้องดำเนินการเพื่อลดโอกาสเกิดหรือผลกระทบของความเสี่ยงให้อยู่ในระดับที่ยอมรับได้ หรือทั้งสองอย่าง โดยจัดทำแผนจัดการความเสี่ยงเพื่อเพิ่มประสิทธิภาพและประสิทธิผลในการลดความเสี่ยง

3) การหลีกเลี่ยงความเสี่ยง (Avoidance) คือ เป็นความเสี่ยงที่จะต้องหลีกเลี่ยงไม่ให้มีการกระทำหรือการปฏิบัติที่จะนำไปสู่ความเสี่ยง

4) การยอมรับความเสี่ยง (Accept) คือ เป็นความเสี่ยงที่ยอมรับให้เกิดขึ้นได้และไม่ต้องดำเนินกิจกรรมใด ๆ เพิ่มเติม เพื่อลดโอกาสเกิดหรือผลกระทบของความเสี่ยง แต่ต้องมีการเฝ้าระวังติดตาม เพื่อไม่ให้ความเสี่ยงเลื่อนระดับสูงขึ้น

6.3.2.9 การกำหนดเจ้าของความเสี่ยง

ความเสี่ยงในแต่ละระดับจะต้องได้รับการกำหนดให้ผู้ที่เป็นเจ้าของความเสี่ยง (Risk Owner) เป็นผู้รับผิดชอบในการดำเนินการจัดการความเสี่ยงให้อยู่ในระดับที่ยอมรับได้ แสดงให้เห็นถึงระดับความเสี่ยงและเจ้าของความเสี่ยงแต่ละระดับ

6.3.2.10 กำหนดแผนจัดการความเสี่ยง

สำหรับระดับความเสี่ยงที่ได้กำหนดให้มีการควบคุมความเสี่ยง (Control) ให้กำหนดแผนจัดการความเสี่ยง (Risk Treatment Plan) โดยมีรายละเอียดที่สำคัญ ประกอบด้วย กิจกรรมหรือวิธีในการดำเนินการจัดการความเสี่ยง ทรัพยากรที่ต้องใช้ ระยะเวลาที่คาดว่าจะใช้ในการดำเนินการจัดการตามแผนลดความเสี่ยง ทรัพยากรที่ต้องใช้ ระยะเวลาที่คาดว่าจะใช้ในการดำเนินการจัดการตามแผนลดความเสี่ยง และผู้รับผิดชอบในแต่ละแผน

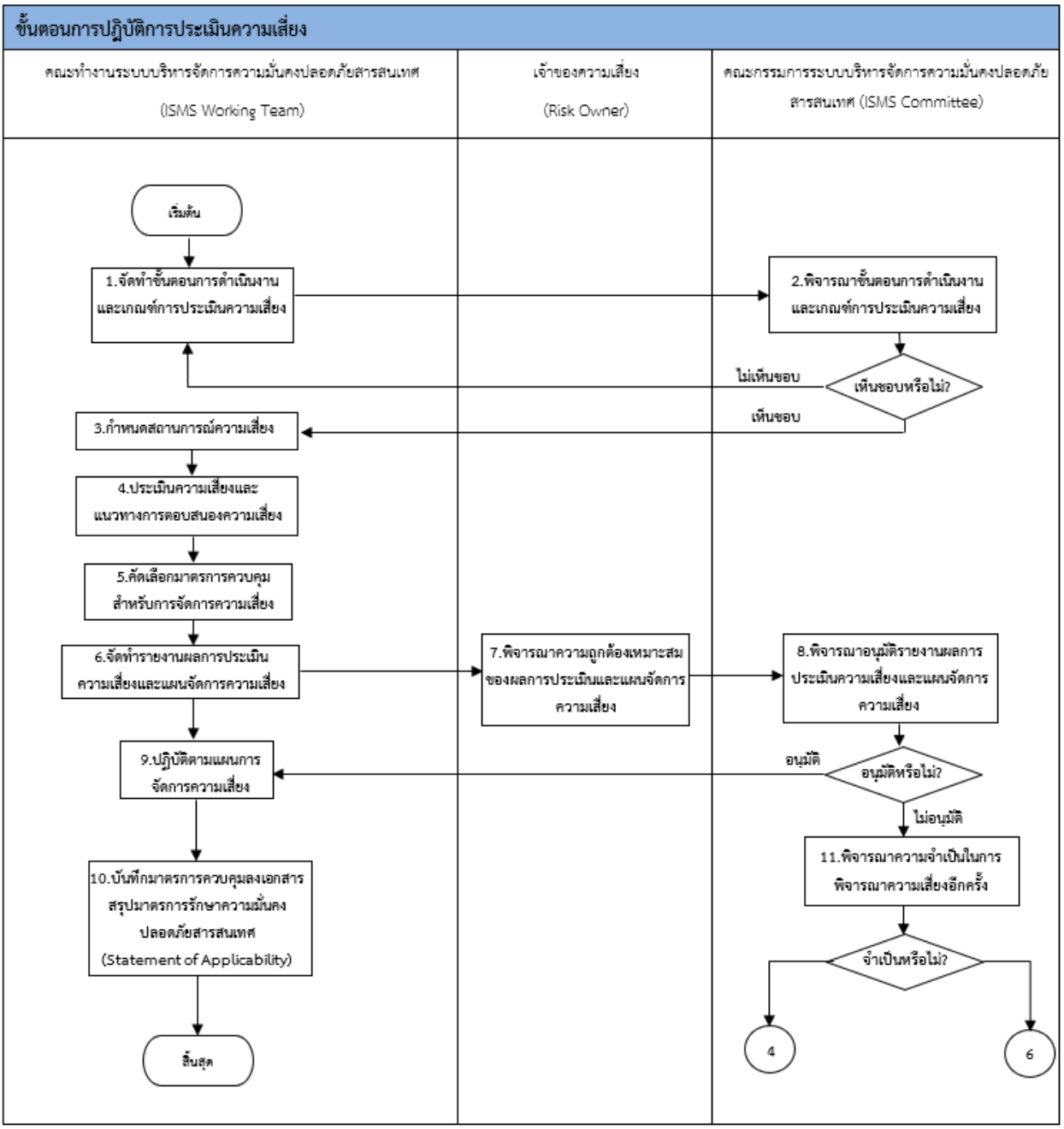
ทั้งนี้ สำหรับระดับความเสี่ยงใดที่ไม่ได้กำหนดให้ต้องมีการควบคุม ไม่จำเป็นต้องกำหนดแผนการควบคุมความเสี่ยงและไม่ต้องวัดระดับความเสี่ยงคงเหลือ

6.3.2.11 วัดระดับความเสี่ยง

กรณีที่มีการจัดการความเสี่ยงด้วยการควบคุม (Control) ภายหลังจากการกำหนดแผนการจัดการความเสี่ยงและดำเนินการตามแผนดังกล่าวเสร็จสิ้น ให้ทำการประเมินความเสี่ยงอีกครั้ง เพื่อหาค่าความเสี่ยงคงเหลือ (Residual Risk) โดยพิจารณาจากเงื่อนไขที่ต้องนำมาพิจารณาในการประเมินความเสี่ยงดังนี้ มาตรการควบคุมที่เพิ่มขึ้นเพื่อควบคุมความเสี่ยง (New Control) ระดับผลกระทบ (Impact) และโอกาสเกิดของเหตุการณ์ (Likelihood) หลังเพิ่มมาตรการควบคุมความเสี่ยง

หากภายหลังการควบคุมความเสี่ยงแล้ว ให้เจ้าของความเสี่ยงพิจารณาระดับความเสี่ยงเหลืออยู่ เพื่อพิจารณาการดำเนินการดูแลความเสี่ยงนั้น ๆ ผลการประเมินความเสี่ยงจะเสนอคณะผู้บริหารระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ เพื่อพิจารณาและรับทราบต่อไป

6.3.3 ขั้นตอนการปฏิบัติการดำเนินการประเมินความเสี่ยง

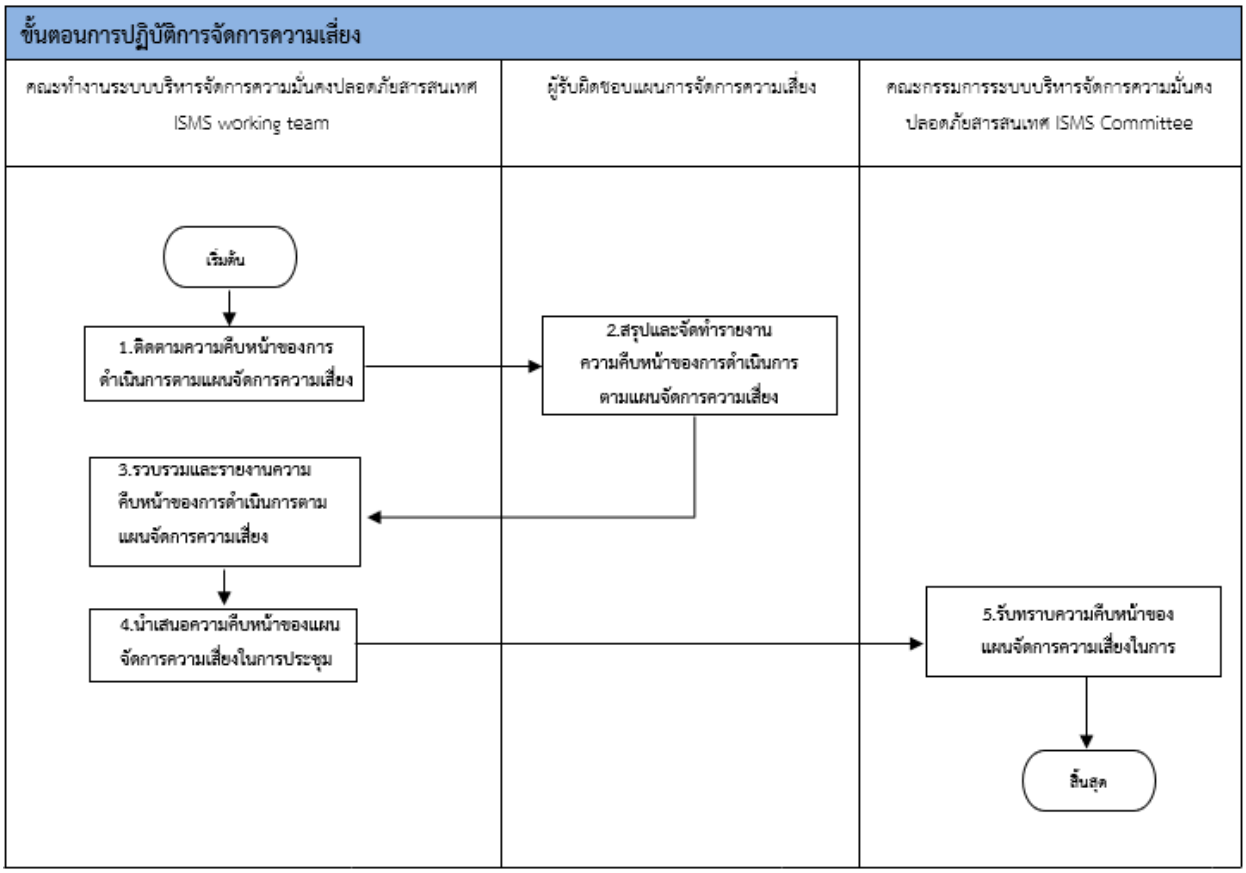


6.3.3.1 คำอธิบายขั้นตอนปฏิบัติการประเมินความเสี่ยง

ลำดับ	ขั้นตอนและกระบวนการ	คำอธิบาย
1.	จัดทำขั้นตอนการดำเนินงานและเกณฑ์การประเมินความเสี่ยง	คณะทำงานระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ ดำเนินการดังนี้ ■ จัดทำขั้นตอนการดำเนินงานสำหรับการบริหารความเสี่ยง ■ กำหนดเกณฑ์การประเมินความเสี่ยง ■ กำหนดรอบการประเมินความเสี่ยงหรือเมื่อมีการเปลี่ยนแปลงที่สำคัญ
2.	พิจารณาขั้นตอนการดำเนินงานสำหรับบริหารความเสี่ยงและเกณฑ์การประเมินความเสี่ยง	คณะกรรมการระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ ดำเนินการพิจารณาอนุมัติ ขั้นตอนการดำเนินงานสำหรับบริหารความเสี่ยงและเกณฑ์การประเมินความเสี่ยง ■ เห็นชอบ ให้ดำเนินการตามขั้นตอนที่ 3 ■ ไม่เห็นชอบ ให้ดำเนินการตามขั้นตอน ลำดับที่ 1
3.	กำหนดสถานการณ์ความเสี่ยง	คณะทำงานระบบบริหารจัดการความมั่นคงปลอดภัย สารสนเทศ ดำเนินการรวบรวมทรัพย์สินสารสนเทศ และกำหนดสถานการณ์ความเสี่ยงที่มีผลกระทบต่อองค์การทั้งภายในและภายนอก ทั้งเหตุการณ์ที่เคยเกิดขึ้นมาแล้วในอดีตและคาดการณ์ในอนาคต
4.	ประเมินความเสี่ยงและแนวทางการตอบสนองความเสี่ยง	คณะทำงานระบบบริหารจัดการความมั่นคงปลอดภัสารสนเทศ ดำเนินการประเมินความเสี่ยง ดังนี้ ประเมินระดับผลกระทบแต่ละด้านโดยนำค่าสูงสุด (Max of Impact) ของผลกระทบทั้งหมดมาใช้พิจารณา 1) ประเมินโอกาสเกิด (Likelihood) เพื่อหาค่าระดับความเสี่ยง (Risk Level) 2) จัดลำดับความเสี่ยง พิจารณาระดับความเสี่ยงกับเกณฑ์การยอมรับความเสี่ยง
5.	คัดเลือกมาตรการควบคุมสำหรับจัดการความเสี่ยง	คณะทำงานระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ ดำเนินการคัดเลือกมาตารการควบคุมสำหรับจัดการความเสี่ยงจาก Annex A ของมาตรฐาน ISO/IEC 27001:2013 และ/หรือจากแหล่งอื่นๆ

ลำดับ	ขั้นตอนและกระบวนการ	คำอธิบาย
6.	จัดทำรายงานผลการประเมินความเสี่ยงและแผนจัดการความเสี่ยง	คณะทำงานระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ ดำเนินการจัดทำรายงานผลการประเมินความเสี่ยงและแผนจัดการความเสี่ยง
7.	พิจารณาความถูกต้องเหมาะสมของผลการประเมินความเสี่ยงและแผนจัดการความเสี่ยง	เจ้าของความเสี่ยงดำเนินการพิจารณาความถูกต้องเหมาะสมของผลการประเมินความเสี่ยงและแผนจัดการความเสี่ยง
8.	พิจารณารายงานผลการประเมินความเสี่ยงและแผนจัดการความเสี่ยง	คณะกรรมการระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ พิจารณาอนุมัติรายงานผลการประเมินความเสี่ยงและแผนการจัดการความเสี่ยง โดยแบ่งเป็น ▪ อนุมัติ ให้ดำเนินการตามขั้นตอนลำดับที่ 9 ไม่อนุมติ ให้ดำเนินการตามขั้นตอนลำดับที่ 10
9.	ปฏิบัติตามแผนจัดการความเสี่ยง	คณะทำงานระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ ดำเนินการปฏิบัติตามแผนการจัดการความเสี่ยงที่ได้รับอนุมัติจากผู้อำนวยการองค์การสุราฯ
10.	บันทึกมาตรการควบคุมลงเอกสารสรุปมาตรการรักษาความมั่นคงปลอดภัยสารสนเทศ	คณะทำงานระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ ดำเนินการบันทึกมาตรการควบคุมลงเอกสารสรุปมาตรการรักษาความมั่นคงปลอดภัยสารสนเทศ
11.	จำเป็นต้องประเมินความเสี่ยงใหม่หรือไม่	คณะกรรมการระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ ดำเนินการพิจารณาความจำเป็น ในการพิจารณาความเสี่ยงอีกครั้ง ▪ จำเป็น ต้องประเมินความเสี่ยงใหม่ ให้ดำเนินการตามขั้นตอนลำดับที่ 4 ▪ ไม่จำเป็น ต้องประเมินความเสี่ยงใหม่ ให้ดำเนินการตามขั้นตอนลำดับที่ 6

6.3.4 ขั้นตอนปฏิบัติการบริหารจัดการความเสี่ยง



6.3.4.1 คำอธิบายขั้นตอนปฏิบัติการบริหารจัดการความเสี่ยง

ลำดับ	ขั้นตอนและกระบวนการ	คำอธิบาย
1.	ติดตามความคืบหน้าของการดำเนินการตามแผนจัดการความเสี่ยง	คณะทำงานระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ ติดตามความคืบหน้าของการดำเนินการตามแผนจัดการความเสี่ยง
2.	สรุปและจัดทำรายงานความคืบหน้าของการดำเนินการตามแผนจัดการความเสี่ยง	ผู้รับผิดชอบแผนจัดการความเสี่ยงดำเนินการสรุปและจัดทำรายงานความคืบหน้าของการดำเนินการ ตามแผนจัดการความเสี่ยง
3.	รวบรวมและรายงานความคืบหน้าของการดำเนินการตามแผนจัดการความเสี่ยง	คณะทำงานระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ ดำเนินการรวบรวม และรายงานความคืบหน้าของการดำเนินการตามแผนจัดการความเสี่ยงในการประชุม
4.	นำเสนอความคืบหน้าของการดำเนินการตามแผนจัดการความเสี่ยงในการประชุม	คณะทำงานระบบบริหารจัดการด้านความมั่นคงปลอดภัยสารสนเทศ ดำเนินการนำเสนอความคืบหน้าของการดำเนินการตามแผนจัดการความเสี่ยงในการประชุม
5.	รับทราบความคืบหน้าของการดำเนินการตามแผนจัดการความเสี่ยง	คณะกรรมการระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ รับทราบความคืบหน้าของการดำเนินการตามแผนการจัดการความเสี่ยง