



องค์การสุรา
กรมสรรพสามิต
LIQUOR DISTILLERY
ORGANIZATION

นโยบายการกำกับดูแลกิจการที่ดี การบริหารความเสี่ยง และการปฏิบัติตามกฎระเบียบ
(Good Governance, Risk Management and Compliance: GRC)
องค์การสุรา กรมสรรพสามิต ประจำปี ๒๕๖๙

“องค์การสุราฯ คำนึงถึงการปฏิบัติตามหลักธรรมาภิบาล โดยบูรณาการหลักการ
กำกับดูแลกิจการที่ดี การบริหารความเสี่ยงและการปฏิบัติตามกฎระเบียบ
เพื่อการพัฒนาและประโยชน์สูงสุดแก่ผู้มีส่วนได้ส่วนเสีย”

องค์การสุราฯ มีความตระหนักและให้ความสำคัญต่อการเพิ่มประสิทธิภาพประสิทธิผล และยกระดับความโปร่งใสในการดำเนินงาน เพื่อเสริมสร้างภาพลักษณ์ที่ดีให้แก่องค์กร และเพิ่มศักยภาพในการตอบสนองต่อผู้มีส่วนได้ส่วนเสีย คณะกรรมการบริหารกิจการขององค์การสุราฯ ในการประชุมครั้งที่ ๑๒/๒๕๖๗ เมื่อวันที่ ๒๕ ตุลาคม ๒๕๖๗ จึงได้กำหนดนโยบายการกำกับดูแลกิจการที่ดี การบริหารความเสี่ยง และการปฏิบัติตามกฎระเบียบ (Good Governance, Risk Management and Compliance: GRC) ขึ้น โดยการจัดให้มีบุคลากรที่มีความรู้และคุณสมบัติเหมาะสม (People) ขั้นตอนการทำงานที่โปร่งใสและมีการควบคุมภายในที่ดี (Process) มีการบริหารจัดการข้อมูลที่ต้องเหมาะสม ทันเวลา (Information) และมีการใช้เทคโนโลยีอย่างมีประสิทธิภาพ (Technology) เพื่อช่วยให้ องค์การมีการกำกับดูแลกิจการที่ดี โปร่งใส และตรวจสอบได้ มีการบริหารความเสี่ยงอย่างเป็นระบบและ สามารถปฏิบัติตามกฎระเบียบได้อย่างครบถ้วน ส่งผลให้เกิดความน่าเชื่อถือและมั่นใจในการบริหารงานและการให้บริการขององค์กรจากผู้มีส่วนได้ส่วนเสีย (Stakeholder) ซึ่งนโยบายนี้บังคับใช้กับคณะกรรมการ ผู้บริหาร และพนักงานทุกคน

คำนิยาม

“กฎระเบียบ” หมายถึง กฎหมาย ระเบียบ ข้อบังคับ ที่เกี่ยวข้องกับองค์การสุราฯ

โดยมีหลักปฏิบัติดังนี้

คณะกรรมการบริหารกิจการขององค์การสุราฯ คณะอนุกรรมการกำกับดูแลที่ดีและการนำองค์กร คณะอนุกรรมการบริหารความเสี่ยงและการควบคุมภายใน คณะอนุกรรมการเทคโนโลยี นวัตกรรมและดิจิทัล และคณะอื่นที่เกี่ยวข้อง ตลอดจนผู้บริหารและพนักงานขององค์การสุราฯทุกระดับ จะร่วมกันกำกับและ ขับเคลื่อนองค์กรในเชิงการบูรณาการภายใต้หลักการกำกับดูแลกิจการที่ดี การบริหารความเสี่ยงและการควบคุมภายใน กฎหมาย ระเบียบ ข้อบังคับขององค์กร ให้มีการปฏิบัติตามหลักสำคัญ ดังต่อไปนี้

ข้อ ๑ องค์การสุราฯ ร่วมกันกำกับดูแลกิจการที่ดีให้สอดคล้องกับมาตรฐานสากลตามกรอบ หลักการของ Organization for Economic Co-operation and Development (OECD) ปี ๒๕๑๕ และแนวทางการปฏิบัติ ๑๐ หมวด มาใช้ในการปฏิบัติงาน ได้แก่ ๑) การสนองบทบาทของภาครัฐ ๒) บทบาทของรัฐบาลกิจเพื่อการตลาดที่เป็นธรรม ๓) สิทธิและความเท่าเทียมกันของผู้ถือหุ้น ๔) บทบาท

ของผู้มีส่วนได้ส่วนเสีย ๕) การเปิดเผยข้อมูล ๖) คณะกรรมการ ๗) การบริหารความเสี่ยงและการควบคุมภายใน ๘) จรรยาบรรณ ๙) ความยั่งยืนและนวัตกรรม และ ๑๐) การติดตามผลการดำเนินการ

ข้อ ๒ ดำเนินการกำหนดกลยุทธ์ แผนการดำเนินงานตามวัตถุประสงค์และเป้าหมาย เพื่อการป้องกันความเสียหายขององค์กรด้วยระบบการควบคุมภายในและเฝ้าระวังความเสี่ยง (Risk) ในอนาคตที่อาจเกิดขึ้นและส่งผลกระทบต่อองค์กร และสนับสนุนให้มีการบริหารความเสี่ยงอย่างเป็นระบบ รวมทั้งการสื่อสาร เผยแพร่ความรู้ สร้างความตระหนักเกี่ยวกับการบริหารความเสี่ยงและการควบคุมภายใน

ข้อ ๓ จัดให้มีการเสริมสร้างบรรยากาศและพฤติกรรมในการสร้างวัฒนธรรมองค์กร เชิงบูรณาการ (GRC Culture) ที่มุ่งตอบสนองค่านิยมองค์กรและเหมาะสมต่อการสนับสนุนการบริหารจัดการองค์กร และการตัดสินใจในเรื่องสำคัญต่าง ๆ ร่วมกัน เพื่อให้เกิดประสิทธิภาพในการบริหารงาน ด้าน GRC ที่สามารถตอบสนองต่อผู้มีส่วนได้ส่วนเสีย (Stakeholder) อย่างทันทั่วถึง

ข้อ ๔ ดำเนินการกำหนดวัตถุประสงค์และกลยุทธ์ที่มุ่งเน้นความยั่งยืนขององค์กร บนพื้นฐานของหลักธรรมาภิบาล (Governance) ภายใต้แนวคิดขับเคลื่อนธุรกิจคู่สังคม รวมทั้งคำนึงถึงการกำกับด้านกฎหมาย ระเบียบ ข้อบังคับขององค์กร (Compliance) อย่างเป็นระบบ เพื่อสามารถสนับสนุนการกำหนดแนวปฏิบัติได้อย่างมีประสิทธิภาพ

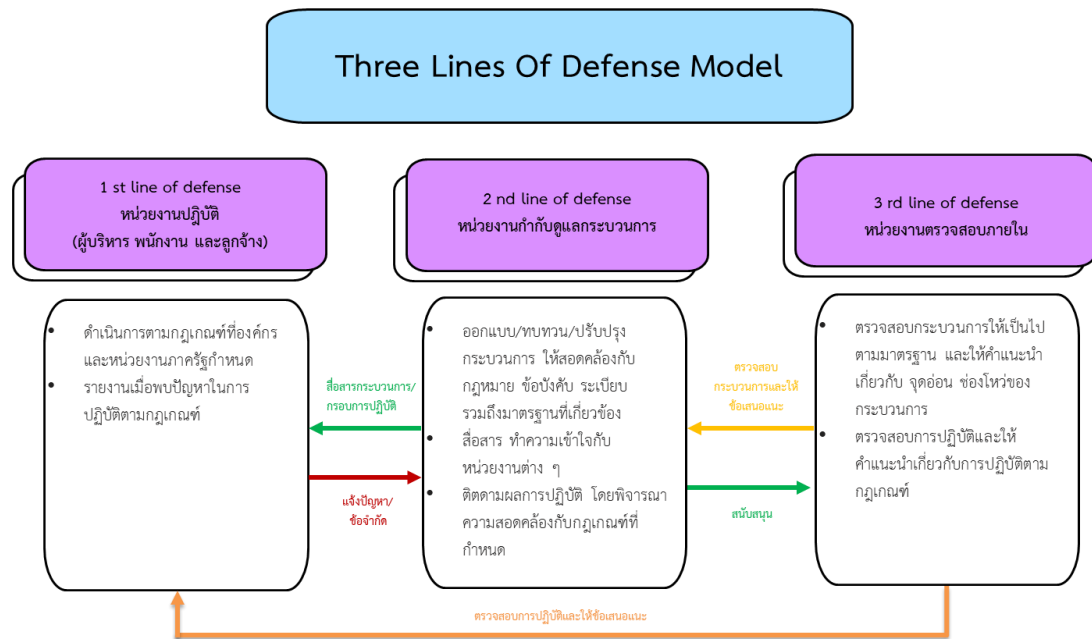
ข้อ ๕ นำเทคโนโลยีดิจิทัลมาปรับใช้เป็นเครื่องมือในการสนับสนุนการปฏิบัติงาน เพื่อให้การดำเนินกิจการขององค์กรบรรลุผลสัมฤทธิ์ ตามเป้าประสงค์ที่กำหนดด้วยการบริหารจัดการที่ดีด้านเทคโนโลยีสารสนเทศครอบคลุมทั่วทั้งองค์กร และผู้มีส่วนได้ส่วนเสีย เพื่อสร้างคุณค่าจากการใช้เทคโนโลยีสารสนเทศที่มีความโปร่งใสและตรวจสอบได้ ควบคู่กับการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศที่เหมาะสม เพื่อลดภัยคุกคามต่าง ๆ ที่อาจเกิดขึ้นและกระทบการดำเนินกิจการที่สำคัญขององค์กร อาทิ การโจมตีทางไซเบอร์ (Cyber Attack) รวมทั้งการบริหารความต่อเนื่องทางธุรกิจ (Business Continuity Management: BCM) เพื่อสร้างความต่อเนื่องในการดำเนินการและให้บริการขององค์กร ในขณะเกิดภาวะวิกฤตหรือเหตุการณ์ฉุกเฉิน

ข้อ ๖ จัดให้มีการบูรณาการร่วมกันระหว่างหน่วยงานในการติดตามความคืบหน้า สอบทาน และตรวจสอบกระบวนการทำงานต่าง ๆ อย่างสม่ำเสมอ เพื่อปรับปรุงแก้ไขการดำเนินงานให้มีประสิทธิภาพและมุ่งสู่การพัฒนาอย่างยั่งยืน (Sustainable Development) ตลอดจนการสื่อสารข้อมูลต่าง ๆ ร่วมกับผู้บริหารและพนักงานทุกระดับ เพื่อสนับสนุนให้เกิดการแลกเปลี่ยนองค์ความรู้ (Knowledge Sharing) ภายใต้การสื่อสารข้อมูลทั่วทั้งองค์กรจนเกิดการบูรณาการร่วมกัน

องค์การสุรา กรมสรรพสามิต จึงได้กำหนดแนวทางในการนำนโยบายการกำกับดูแลกิจการที่ดี การบริหารความเสี่ยง และการปฏิบัติตามกฎระเบียบ (GRC) ประจำปี 2567 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 ถูกต้องตามกฎหมาย และมีระบบการควบคุมภายในที่ดี
4. Monitor หมายถึง มีระบบติดตามดูแลการปฏิบัติงานอย่างเพียงพอ เหมาะสม เพื่อให้เป็นไปตามวัตถุประสงค์ที่ตั้งไว้

ปัจจัยสนับสนุนและขับเคลื่อน GRC (GRC Supports)



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

การบูรณาการนโยบาย

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

ข้อ 1 องค์กรสุราฯ ร่วมกันการค้ากับดูแลกิจการที่ดีให้สอดคล้องกับมาตรฐานสากลตามกรอบหลักการของ 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. องค์กรสุราฯ มีการปฏิบัติหน้าที่ตามความรับผิดชอบอย่างครบถ้วนและมีประสิทธิผลโดยคณะกรรมการบริหารกิจการขององค์กรสุราฯ ตระหนักถึงบทบาท หน้าที่ ในการกำหนดให้มีทิศทางนโยบายแผนงาน 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 กำกับดูแลและสอบทานการปฏิบัติงานของพนักงานและลูกจ้างให้เป็นไปตามแผนการดำเนินงาน โดยให้ดำเนินงานอย่างโปร่งใสและตรวจสอบได้

3. ผู้บริหาร พนักงาน และลูกจ้าง ต้องตระหนักและปฏิบัติงานอย่างโปร่งใสถูกต้องตามหลักจริยธรรมและจรรยาบรรณตามคู่มือจริยธรรมและจรรยาบรรณการดำเนินธุรกิจขององค์กรสุราฯ กรมสรรพสามิต อย่างเคร่งครัด พร้อมทั้งสอดส่องดูแลให้ไม่เกิดช่องทางการทุจริตในการดำเนินงาน รวมถึงการกำหนดวิธีการควบคุมและป้องกันปราบปรามการทุจริตและคอร์รัปชันทุกรูปแบบ

หน่วยงานกำกับดูแลกระบวนการ (2nd Line)

1. กำหนดกรอบและแนวทางในการปฏิบัติตามนโยบายทั้งภายในและภายนอก ให้สอดคล้องและเหมาะสมกับองค์กร รวมทั้งควรมีการทบทวน และปรับปรุงให้สามารถดำเนินงานได้ทันทั่วถึงและถูกต้องตามสถานการณ์ในปัจจุบัน

2. ติดตามผลการปฏิบัติงานของแต่ละหน่วยงานต่าง ๆ โดยพิจารณาถึงความสอดคล้องกับแนวปฏิบัติและแผนการดำเนินงานที่กำหนดไว้ รวมทั้งวิเคราะห์และประเมินผลการดำเนินงาน และรายงานให้ผู้บริหารระดับสูงทราบเป็นไตรมาส

3. สื่อสาร และทำความเข้าใจเกี่ยวกับการปฏิบัติตามแนวทางปฏิบัติ และแผนการดำเนินงาน รวมทั้งผลการวิเคราะห์ประเมินช่องโหว่และความเสี่ยงให้กับพนักงานและหน่วยงานต่าง ๆ ได้รับความเข้าใจอย่างถูกต้อง

หน่วยงานตรวจสอบภายใน (3rd Line)

1. ตรวจสอบกระบวนการทำงานของหน่วยงานต่าง ๆ และให้คำแนะนำ ชี้แจงเกี่ยวกับการปฏิบัติงานตามแนวปฏิบัติ และแผนการดำเนินงานอย่างมีประสิทธิภาพและประสิทธิผล

ข้อ 2 ดำเนินการกำหนดกลยุทธ์ แผนการดำเนินงานตามวัตถุประสงค์และเป้าหมาย เพื่อการป้องกันความเสียหายขององค์กรด้วยระบบการควบคุมภายในและเฝ้าระวังความเสี่ยง (Risk) ในอนาคตที่อาจเกิดขึ้นและส่งผลกระทบต่อองค์กร และสนับสนุนให้มีการบริหารความเสี่ยงอย่างเป็นระบบ รวมทั้งการสื่อสาร เผยแพร่ความรู้ สร้างความตระหนักเกี่ยวกับการบริหารความเสี่ยงและการควบคุมภายใน

หลักการพื้นฐาน

1. องค์กรสุราษฎร์ มีกระบวนการบริหารจัดการความเสี่ยงองค์กรที่สอดคล้องกับระบบการบริหารความเสี่ยงตามมาตรฐานสากล COSO ERM 2017 โดยเป็นการบริหารความเสี่ยงลักษณะเชิงรุก กำหนดกลยุทธ์การบริหารความเสี่ยงที่เชื่อมโยงกับแผนยุทธศาสตร์/กลยุทธ์/การวางแผน/การจัดสรรทรัพยากร/การลงทุน/ผู้มีส่วนได้ส่วนเสีย ทั้งนี้พิจารณาประเด็นความเสี่ยงทางการเงินและไม่ใช่การเงิน ที่ครอบคลุมทั้งในด้านกลยุทธ์ (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. องค์กรสุราษฎร์ จัดให้มีการควบคุมภายในตามภารกิจของหน่วยงานอย่างเพียงพอและเหมาะสม ทุกขั้นตอนของการปฏิบัติงาน เป็นไปตามหลักเกณฑ์กระทรวงการคลังว่าด้วยมาตรฐานและหลักเกณฑ์ปฏิบัติการควบคุมภายในสำหรับหน่วยงานของรัฐ 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 พร้อมทั้งสอบทานการปฏิบัติงานให้สอดคล้องกับกฎเกณฑ์ที่เกี่ยวข้องอย่างเคร่งครัด หรือละเมิด

3. ผู้บริหาร พนักงาน และลูกจ้าง ต้องตระหนักถึงการบริหารความเสี่ยงและการควบคุมภายใน และประเมินความเสี่ยงในการปฏิบัติงาน พร้อมทั้งสอบทานการดำเนินการให้สอดคล้องกับกฎเกณฑ์อยู่เสมอ เพื่อให้บรรลุผลสำเร็จตามวัตถุประสงค์ การดำเนินงานขององค์กร

หน่วยงานกำกับดูแลกระบวนการ (2nd Line)

1. กำหนดกรอบ แผนการดำเนินงาน และแนวทางในการปฏิบัติด้านการบริหารความเสี่ยง การควบคุมภายใน และการปฏิบัติงานให้เป็นไปตามกฎเกณฑ์ขององค์กร ให้สอดคล้องและเหมาะสมกับองค์กร รวมทั้งควรมีการทบทวนและปรับปรุงให้มีความถูกต้องอย่างสม่ำเสมอ

2. ติดตามผลการปฏิบัติของหน่วยงานต่างๆ โดยพิจารณาถึงความสอดคล้องกับแนวทางปฏิบัติ และแผนการดำเนินงานที่กำหนดไว้ ควรมีการทบทวนและประเมินช่องโหว่และความเสี่ยงในการดำเนินงาน และควรมีการแจ้งเตือนเหตุล่วงหน้าให้ผู้ปฏิบัติได้มีการแก้ไขได้ทันกาล รวมทั้งควรทบทวนข้อมูลให้เป็นปัจจุบันอยู่เสมอ เพื่อให้ผู้รับผิดชอบและผู้บริหารได้ใช้ประกอบการตัดสินใจได้

3. สื่อสาร เผยแพร่ความรู้ สร้างความตระหนักเกี่ยวกับการบริหารความเสี่ยงและการควบคุมภายใน และประชาสัมพันธ์และทำความเข้าใจเกี่ยวกับการปฏิบัติตามแนวปฏิบัติ และแผนการดำเนินงานให้กับพนักงานและหน่วยงานต่างๆ ได้รับทราบอย่างถูกต้องและมีประสิทธิภาพ รวมถึงควรสร้างความตระหนักรู้อย่างทั่วถึงทั่วทั้งองค์กร

หน่วยงานตรวจสอบภายใน (3rd Line)

1. ตรวจสอบกระบวนการทำงานของหน่วยงานต่าง ๆ และให้คำแนะนำ ชี้แจงเกี่ยวกับประเด็นความเสี่ยงที่ตรวจพบ ในการดำเนินการที่ไม่สอดคล้องตามแนวทางและแผนการดำเนินงาน อย่างมีประสิทธิภาพและประสิทธิผล

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

หลักการพื้นฐาน

1. มุ่งมั่นดูแลบุคลากรอย่างเท่าเทียม โดยให้ความสำคัญตั้งแต่กระบวนการวางแผนกำลังคน และการสรรหาคัดเลือกบุคลากรด้วยความโปร่งใส เพื่อให้ได้บุคลากรที่มีความรู้ ความสามารถ มีความมุ่งมั่น และมีศักยภาพในการขับเคลื่อนองค์กรไปสู่ความยั่งยืน รวมทั้งคำนึงถึงการบริหารค่าตอบแทนและการรักษาบุคลากร รวมถึงการสร้างสภาพแวดล้อมที่ปลอดภัยและเอื้อต่อการมีคุณภาพ

ชีวิตที่ดี เพื่อตอบสนองต่อความต้องการและความคาดหวังของบุคลากร เพื่อให้มีขวัญและกำลังใจในการปฏิบัติงานจวบจนเกษียณอายุงาน และเสริมสร้างระดับความพึงพอใจและความผูกพันที่ดีต่อสังคม

2. มีความมุ่งมั่นพัฒนาองค์กรอย่างมีประสิทธิภาพ และตอบสนองความต้องการ ความคาดหวังของผู้มีส่วนได้ส่วนเสีย โดยได้นำหลักการ Governance Risk Management and Compliance (GRC) ตามมาตรฐานสากลมาประยุกต์ และบูรณาการระหว่าง การกำกับดูแลกิจการที่ดี การบริหารความเสี่ยง การปฏิบัติตามกฎหมายและกฎระเบียบ เพื่อสนับสนุนให้เกิดระบบบริหารจัดการองค์กรที่มีประสิทธิภาพ ภายใต้หลักธรรมาภิบาล มีความโปร่งใส เป็นธรรม ตรวจสอบได้

แนวทางปฏิบัติ

หน่วยงานปฏิบัติ (1st Line)

1. ผู้บริหาร พนักงาน และลูกจ้าง ตระหนัก รวมถึงศึกษาทำความเข้าใจ และนำนโยบาย GRC ไปปฏิบัติตาม โดยสามารถศึกษาในแนวทางปฏิบัติได้ในคู่มือการบริหารความเสี่ยง เพื่อเสริมสร้างบรรยากาศรวมถึงสภาพแวดล้อมให้เหมาะสม ในการส่งเสริมการกำกับดูแลกิจการที่ดี การบริหารความเสี่ยง และการปฏิบัติตามกฎระเบียบภายในองค์กร

2. ผู้บังคับบัญชา ศึกษาทำความเข้าใจกฎระเบียบข้อบังคับ พร้อมทั้งสอบทาน การดำเนินการของบุคลากรในสายบังคับบัญชา ให้สอดคล้องกับกฎเกณฑ์อยู่เสมอ เพื่อให้บรรลุผลสำเร็จตามวัตถุประสงค์ การดำเนินงานขององค์กร

3. ผู้ปฏิบัติ ศึกษาทำความเข้าใจกฎระเบียบข้อบังคับ พร้อมทั้งดำเนินงาน ให้สอดคล้องกับกฎเกณฑ์อยู่เสมอ รวมถึงวิเคราะห์การดำเนินงานที่ไม่สอดคล้องกับกฎเกณฑ์ เพื่อรายงานให้ผู้บังคับบัญชา รวมถึงหน่วยงานที่เกี่ยวข้องในกระบวนการทราบ และร่วมกันพัฒนาปรับปรุงแก้ไขต่อไป

หน่วยงานกำกับดูแลกระบวนการ (2nd Line)

1. กำหนดกรอบ นโยบาย แนวทางในการปฏิบัติ และจัดทำระเบียบ/ข้อปฏิบัติ ให้สอดคล้องและเหมาะสมกับองค์กร รวมทั้งควรมีการทบทวน และปรับปรุงให้มีความถูกต้องอย่างสม่ำเสมอ

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

3. สื่อสาร ประชาสัมพันธ์และทำความเข้าใจเกี่ยวกับการปฏิบัติตามระเบียบ/ข้อปฏิบัติ ให้กับพนักงานและหน่วยงานต่าง ๆ ได้รับทราบและปฏิบัติได้อย่างถูกต้อง

ข้อ 4 ดำเนินการกำหนดวัตถุประสงค์และกลยุทธ์ที่มุ่งเน้นความยั่งยืนขององค์กรบนพื้นฐานของหลักธรรมาภิบาล (Governance) ภายใต้แนวคิดขับเคลื่อนธุรกิจสู่สังคม รวมทั้งคำนึงถึงการกำกับด้านกฎหมาย ระเบียบ ข้อบังคับขององค์กร (Compliance) อย่างเป็นระบบ เพื่อสามารถสนับสนุน การกำหนดแนวปฏิบัติได้อย่างมีประสิทธิภาพ

หลักการพื้นฐาน

1. มุ่งเน้นความยั่งยืนขององค์กร บนพื้นฐานของหลักธรรมาภิบาล (Governance) ภายใต้แนวคิดขับเคลื่อนธุรกิจสู่สังคม และพัฒนาระบบบริหารจัดการด้านการกำกับดูแลการปฏิบัติตามกฎระเบียบ (Compliance Management System) โดยปรับปรุงกระบวนการดำเนินงานเพื่อวิเคราะห์ประเมินความเสี่ยงต่อความไม่สอดคล้องกับกฎหมาย และกฎระเบียบ (Compliance Risk) ทั้งในด้านการเปลี่ยนแปลงกฎหมาย (Regulatory Risk) และด้านการปฏิบัติที่ไม่ถูกต้อง ไม่สอดคล้องกับกฎหมาย และกฎระเบียบ เกี่ยวกับด้านดำเนินงาน (Operational Risk) เพื่อกำหนดมาตรการปรับปรุง แก้ไขต่อ

ความไม่สอดคล้องกับกฎหมายและกฎระเบียบ (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 หรือละเอียด

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 โดยพิจารณาถึงความสอดคล้องกับแนวทางปฏิบัติปฏิบัติตามหลักธรรมาภิบาล (Governance) การกำกับด้านกฎหมาย ระเบียบ ข้อบังคับขององค์กร (Compliance) และแนวทางปฏิบัติงานให้เป็นไปตามกฎเกณฑ์ขององค์กร

3. สื่อสาร ประชาสัมพันธ์และทำความเข้าใจเกี่ยวกับการปฏิบัติตามแนวปฏิบัติตามหลักธรรมาภิบาล (Governance) การกำกับด้านกฎหมาย ระเบียบ ข้อบังคับขององค์กรให้กับพนักงานและหน่วยงานต่างๆ ได้รับทราบอย่างถูกต้องและมีประสิทธิภาพ รวมถึงควรสร้างความตระหนักรู้อย่างทั่วถึงทั่วทั้งองค์กร

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

หลักการพื้นฐาน

1. มุ่งเน้นการพัฒนากระบวนการเทคโนโลยีดิจิทัล เพื่อสนับสนุนให้องค์กรก้าวสู่การเปลี่ยนแปลงและจัดให้มีกระบวนการบริหารจัดการระบบรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศตามมาตรฐาน ISO/IEC 27001 ซึ่งมีขอบเขตงานที่ครอบคลุมโครงสร้างพื้นฐานขององค์กรที่สำคัญ (Critical Infrastructure) โดยเฉพาะด้านสารสนเทศของศูนย์คอมพิวเตอร์ รวมทั้งการดำเนินการบริหาร

จัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศตามมาตรฐานสากล ISO/IEC27001 หรือ มาตรฐานสากลอื่น ๆ อย่างต่อเนื่อง

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

แนวทางปฏิบัติ

หน่วยงานปฏิบัติ (1st Line)

1. ผู้บริหาร พนักงาน และลูกจ้าง ตระหนักและดำเนินการตามระบบการรักษาความมั่นคง ปลอดภัยด้านเทคโนโลยีสารสนเทศ อย่างเคร่งครัด รวมถึงการไม่ดำเนินการใดๆ ที่เสี่ยงต่อการละเมิด การรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศขององค์กร

2. ผู้บริหาร พนักงาน และลูกจ้าง ดำเนินการศึกษา ทำความเข้าใจ และฝึกซ้อมสถานการณ์ที่ อาจเกิดขึ้นตามการกระบวนการบริหารความต่อเนื่องทางธุรกิจ (Business Continuity Management: BCM) และแผนการบริหารความต่อเนื่องทางธุรกิจ (BCP) เพื่อสร้างความต่อเนื่องในการดำเนินการและให้บริการ ขององค์กรในขณะเกิดภาวะวิกฤตหรือเหตุการณ์ฉุกเฉิน

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

หน่วยงานกำกับดูแลกระบวนการ (2nd Line)

1. กำหนดกรอบ และแนวทางในการปฏิบัติและบริหารจัดการระบบรักษาความมั่นคงปลอดภัย ด้านเทคโนโลยีสารสนเทศ ตามมาตรฐาน ISO/IEC 27001 รวมทั้งการดำเนินการบริหารจัดการความเสี่ยง ด้านความมั่นคงปลอดภัยสารสนเทศตามมาตรฐานสากล ISO/IEC27001 อย่างต่อเนื่อง และการบริหาร ความต่อเนื่องทางธุรกิจ (Business Continuity Management: BCM) เพื่อสร้างความต่อเนื่องใน การดำเนินการและให้บริการขององค์กรในขณะเกิดภาวะวิกฤตหรือเหตุการณ์ฉุกเฉิน

3. ติดตามผลการปฏิบัติของหน่วยงานต่างๆ โดยพิจารณาถึงความสอดคล้องกับแนวปฏิบัติ และแผนการดำเนินงานที่กำหนดไว้ โดยควรมีการทบทวนเพื่อให้ข้อมูลเป็นปัจจุบัน พร้อมทั้งมีการจัดทำ แผนเผื่อสำรองและฝึกซ้อมเพื่อให้มีการป้องกันแก้ไขได้ทันกาลอยู่เสมอ

4. สื่อสาร ประชาสัมพันธ์และทำความเข้าใจเกี่ยวกับการปฏิบัติตามแนวปฏิบัติ และ แผนการดำเนินงานให้กับพนักงานและหน่วยงานต่างๆ ได้รับทราบอย่างถูกต้องมีประสิทธิภาพและ ประสิทธิภาพ

ข้อ 6 จัดให้มีการบูรณาการร่วมกันระหว่างหน่วยงานในการติดตามความคืบหน้า สอบทาน และตรวจสอบกระบวนการทำงานต่าง ๆ อย่างสม่ำเสมอ เพื่อปรับปรุงแก้ไขการดำเนินงาน ให้มีประสิทธิภาพและมุ่งสู่การพัฒนาอย่างยั่งยืน (Sustainable Development) ตลอดจนการสื่อสาร ข้อมูลต่าง ๆ ร่วมกับผู้บริหารและพนักงานทุกระดับ เพื่อสนับสนุนให้เกิดการแลกเปลี่ยนองค์ความรู้ (Knowledge Sharing) ภายใต้การสื่อสารข้อมูลทั่วทั้งองค์กรจนเกิดการบูรณาการร่วมกัน

หลักการพื้นฐาน

1. มุ่งเน้นให้องค์กรเกิดการบูรณาการร่วมกันระหว่างหน่วยงานต่าง ๆ ในการติดตาม ความคืบหน้า สอบทาน และตรวจสอบกระบวนการทำงานต่าง ๆ อย่างสม่ำเสมอ เพื่อปรับปรุงแก้ไข การดำเนินงานให้มีประสิทธิภาพและมุ่งสู่การพัฒนาอย่างยั่งยืน (Sustainable Development) ตลอดจน

การสื่อสารข้อมูลต่าง 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. ติดตามผลการปฏิบัติของหน่วยงานต่าง ๆ โดยพิจารณาถึงความสอดคล้องกับแนวทางปฏิบัติและแผนการดำเนินงานที่กำหนดไว้ และสอบทานการดำเนินงานที่เกิดการแลกเปลี่ยนองค์ความรู้และเกิดการสร้างนวัตกรรมที่สามารถผลักดันเป้าหมายหรือความท้าทายขององค์กรให้บรรลุเป้าหมาย และควรมีการทบทวนและประเมินช่องโหว่และความเสี่ยงในการดำเนินงานที่อาจจะเกิดขึ้น เพื่อให้ผู้รับผิดชอบและผู้บริหารได้ใช้ประกอบการตัดสินใจได้
3. สื่อสาร ประชาสัมพันธ์และทำความเข้าใจและสร้างความตระหนักรู้เกี่ยวกับการบูรณาการร่วมกันระหว่างหน่วยงานต่าง ๆ เพื่อปรับปรุงแก้ไขการดำเนินงานให้มีประสิทธิภาพและมุ่งสู่การพัฒนาอย่างยั่งยืน (Sustainable Development) อย่างทั่วถึงทั้งองค์กร

จึงประกาศให้ทราบโดยทั่วกัน

ประกาศ ณ วันที่ 12 พฤศจิกายน พ.ศ. ๒๕๖๘



(นายณัฐกร อุเทนสุต)

ประธานกรรมการบริหารกิจการขององค์การสุรา