



คู่มือบูรณาการนโยบาย

การกำกับดูแลกิจการที่ดี การบริหารความเสี่ยง
และการปฏิบัติตามกฎหมาย ระเบียบ ข้อบังคับ อ.ส.ค.



จัดทำโดย

กองบริหารจัดการและพัฒนาองค์กร

ฝ่ายนโยบายและยุทธศาสตร์

สารบัญ

	หน้า
คำนำ	
1. หลักการและเหตุผล	1
2. คำนินยาม	2
3. วัตถุประสงค์ของคู่มือ	4
4. นโยบายการบูรณาการ GRC	4
5. โครงสร้าง และบทบาทหน้าที่ความรับผิดชอบในการบูรณาการ GRC	4
6. แนวทางการปฏิบัติการบูรณาการ GRC	6
7. รูปแบบการรายงาน	6
8. อำนาจอนุมัติ และการทบทวนคู่มือการบูรณาการ	8
9. ภาคผนวก ก	8
9.1 คำศัพท์	8
9.2 ตารางประเมินความเสี่ยง (Risk Assessment Matrix)	9
9.2.1 ตารางประเมินโอกาสที่จะเกิดความเสี่ยง (Likelihood)	10
9.2.2 ตารางการประเมินความรุนแรงของผลกระทบ (Impact)	11
9.3 การจัดระดับความเสี่ยง (หลังการจัดการ)	11
9.4 (ตัวอย่าง) การกรอกแบบฟอร์มประเมินความเสี่ยงสำหรับบูรณาการ GRC	12
9.5 กระบวนการ GRC	13

สารบัญภาพ

รูปที่ 1 โครงสร้างองค์กรที่สนับสนุนการบูรณาการตามหลัก GRC	5
รูปที่ 2 แผนภูมิแสดงสายการรายงาน GRC	7

สารบัญตาราง

	หน้า
ตารางที่ 1 ตารางแสดงค่านิยาม GRC	2
ตารางที่ 2 ตารางแสดงโครงสร้าง และบทบาทหน้าที่ความรับผิดชอบในการบูรณาการ GRC	4
ตารางที่ 3 ตารางแสดงคำศัพท์	8
ตารางที่ 4 ตารางแสดงการประเมินความเสี่ยง (Risk Assessment Matrix)	9
ตารางที่ 5 ตารางแสดงความหมายระดับความเสี่ยง (Risk Assessment Matrix)	10
ตารางที่ 6 ตารางแสดงประเมินโอกาสที่จะเกิดความเสี่ยง (Likelihood)	10
ตารางที่ 7 ตารางแสดงประเมินความรุนแรงของผลกระทบ (Impact)	11
ตารางที่ 8 ตารางแสดงการจัดระดับความเสี่ยง (หลังการจัดการ)	11
ตารางที่ 9 ตารางแสดงการคำนวณระดับความเสี่ยง	11

คำนำ

คณะกรรมการ อ.ส.ค. ได้เห็นชอบนโยบายบูรณาการกำกับดูแลกิจการที่ดี การบริหารความเสี่ยง และการกำกับปฏิบัติตามกฎ ระเบียบ ข้อบังคับ และกฎเกณฑ์ที่เกี่ยวข้อง (Integrated Governance Risk and Compliance Policy : GRC Policy) เพื่อใช้เป็นกรอบและแนวทางปฏิบัติสำหรับการบูรณาการนโยบาย GRC ให้เป็นไปในทิศทางเดียวกันทั่วทั้งองค์กร ซึ่งแสดงให้เห็นถึงการบูรณาการฐานข้อมูล และกระบวนการดำเนินงานที่นำไปปฏิบัติได้จริง สามารถวัดและประเมินผลลัพธ์ได้ และเพื่อให้การปฏิบัติเกิดความชัดเจน ทำซ้ำได้ จึงจำเป็นต้องจัดทำคู่มือปฏิบัติการบูรณาการนโยบายการกำกับดูแลกิจการที่ดี การบริหารความเสี่ยง และการปฏิบัติตามกฎหมาย ระเบียบ ข้อบังคับ อ.ส.ค. ปีงบประมาณ 2569

การจัดทำคู่มือบูรณาการนโยบายการกำกับดูแลกิจการที่ดี การบริหารความเสี่ยง และการกำกับปฏิบัติตามกฎ ระเบียบ ข้อบังคับ และกฎเกณฑ์ที่เกี่ยวข้อง ฉบับนี้ เป็นไปตามกรอบการบริหารความเสี่ยงองค์กรตามมาตรฐานสากล COSO 2013 และ 2017 รวมทั้งแนวปฏิบัติของหน่วยงานที่กำกับดูแล เช่น กระทรวงเกษตรและสหกรณ์ สำนักงานคณะกรรมการรัฐวิสาหกิจ กระทรวงการคลัง เป็นต้น เพื่อใช้เป็นแนวทางการบูรณาการ GRC ตามเกณฑ์การประเมินผลการดำเนินงานรัฐวิสาหกิจและมาตรฐานสากลภายใต้บริบทของ อ.ส.ค. ทั้งนี้เพื่อให้ผู้ปฏิบัติงานทุกระดับนำไปใช้ภายในหน่วยงานของตนเอง รวมทั้งส่งเสริม/สนับสนุนการดำเนินงานให้มีประสิทธิภาพ โดยยึดหลักกฎหมาย ระเบียบ ข้อบังคับ รวมทั้งกฎเกณฑ์ต่างๆ อย่างเคร่งครัด

แผนกบริหารความเสี่ยงและควบคุมภายใน
กองบริหารจัดการและพัฒนาองค์กร
ฝ่ายนโยบายและยุทธศาสตร์
สิงหาคม 2568

คู่มือบูรณาการนโยบาย การกำกับดูแลกิจการที่ดี การบริหารความเสี่ยง และการปฏิบัติตามกฎหมาย ระเบียบ ข้อบังคับ อ.ส.ค. ปีงบประมาณ 2569

1. หลักการและเหตุผล

สืบเนื่องจากองค์การส่งเสริมกิจการโคนมแห่งประเทศไทย มีนโยบายบูรณาการกำกับดูแลกิจการที่ดี การบริหารความเสี่ยง และการกำกับปฏิบัติตามเกณฑ์ (Integrated Governance Risk and Compliance Policy : GRC) สนับสนุนให้ทุกหน่วยงานของ อ.ส.ค. มีส่วนร่วมในการ บูรณาการ GRC เพื่อให้ดำเนินการกำกับดูแลกิจการที่ดี การบริหารความเสี่ยงและการกำกับปฏิบัติตามกฎหมาย ระเบียบ ข้อบังคับ และกฎเกณฑ์ต่างๆ สอดคล้องกับกรอบการบริหารความเสี่ยงองค์กรตามมาตรฐานสากล COSO และแนวปฏิบัติของ อ.ส.ค. กระทรวงเกษตรและสหกรณ์ เป็นต้น โดยเชื่อมโยงการกำกับดูแลกิจการที่ดีหรือหลักธรรมาภิบาลเข้ากับกระบวนการบริหารความเสี่ยงทั่วทั้งองค์กร และการกำกับปฏิบัติตามกฎหมาย ระเบียบ ข้อบังคับ และกฎเกณฑ์ต่างๆ เพื่อการขับเคลื่อนองค์กรอย่างมีคุณค่าและส่งเสริมการดำเนินงานให้มีประสิทธิภาพ โดยยึดถือหลักกฎหมาย ระเบียบ ข้อบังคับ รวมทั้งกฎเกณฑ์ต่างๆ อย่างเคร่งครัด ทำให้องค์กรมีความน่าเชื่อถือ และเติบโตอย่างยั่งยืน

ดังนั้น เพื่อให้องค์กรมีแนวทางปฏิบัติสำหรับการบูรณาการนโยบาย GRC ให้เป็นไปในทิศทางเดียวกันทั่วทั้งองค์กร ซึ่งแสดงให้เห็นถึงการบูรณาการฐานข้อมูล และกระบวนการดำเนินงานที่สามารถปฏิบัติได้จริง จึงจำเป็นต้องจัดทำคู่มือบูรณาการกำกับดูแลกิจการที่ดี การบริหารความเสี่ยงและการกำกับปฏิบัติตามกฎหมาย ระเบียบ ข้อบังคับ และกฎเกณฑ์ที่เกี่ยวข้อง ตามกรอบการบริหารความเสี่ยงองค์กรตามมาตรฐานสากล COSO 2013 และ 2017 รวมทั้งแนวปฏิบัติของหน่วยงานที่กำกับดูแล เช่น กระทรวงเกษตรและสหกรณ์ สำนักงานคณะกรรมการรัฐวิสาหกิจ กระทรวงการคลัง เป็นต้น เพื่อใช้เป็นแนวทางการบูรณาการ GRC ตามเกณฑ์การประเมินผลการดำเนินงานรัฐวิสาหกิจและมาตรฐานสากลภายใต้บริบทของ อ.ส.ค. เพื่อให้ผู้ปฏิบัติงานทุกระดับสามารถนำไปใช้ภายในหน่วยงานของตนเองได้อย่างถูกต้อง รวมทั้งส่งเสริม/สนับสนุนการดำเนินงานให้มีประสิทธิภาพ โดยยึดหลักกฎหมาย ระเบียบ ข้อบังคับ รวมทั้งกฎเกณฑ์ต่างๆ อย่างเคร่งครัด

2. คำนิยาม

องค์การส่งเสริมกิจการโคนมแห่งประเทศไทย ได้กำหนดนิยามของ Governance (G) Risk (R) และ Compliance (C) โดยมีรายละเอียด ดังนี้

คำว่า	ความหมาย
- คณะอนุกรรมการบริหารงาน การกำกับดูแลที่ดีและการนำองค์กร - คณะอนุกรรมการด้านการบริหารทรัพยากรมนุษย์ การจัดการความรู้และนวัตกรรม	คณะอนุกรรมการบริหารงาน การกำกับดูแลที่ดีและการนำองค์กร และคณะอนุกรรมการด้านการบริหารทรัพยากรมนุษย์ การจัดการความรู้และนวัตกรรม ที่ได้รับการแต่งตั้งจากคณะกรรมการ อ.ส.ค. ได้มีการทบทวนแนวทางการกำกับดูแลกิจการที่ดีของ อ.ส.ค. ให้สอดคล้องกับมาตรฐานสากลตามกรอบหลักการของ Organization for Economic Co-operation and Development (OECD) ปี 2515, สำนักงานคณะกรรมการนโยบายรัฐวิสาหกิจ (สคร.) และแผนยุทธศาสตร์ชาติว่าด้วยการป้องกันและปราบปรามการทุจริต ระยะที่ 3 (พ.ศ. 2560 - 2564) ตามกรอบวิสัยทัศน์ “ประเทศไทยใสสะอาด ไทยทั้งชาติต้านทุจริต” (Zero Tolerance Clean Thailand) รวมถึงการสร้างประโยชน์สูงสุดให้แก่องค์กร ผู้มีส่วนได้ส่วนเสียที่สำคัญทุกฝ่าย⁴ และดำเนินธุรกิจด้วยความรับผิดชอบต่อสังคมและสิ่งแวดล้อม อ.ส.ค.ยึดหลักการตามกรอบมาตรฐานสากล ได้แก่ 1. หลักการของ Organization for Economic Co-operation and Development (OECD) 2. ตามกรอบของสำนักงานคณะกรรมการนโยบายรัฐวิสาหกิจ (สคร.) ทั้ง 9 หมวด - หมวด 1 บทบาทของภาครัฐ - หมวด 2 สิทธิและความเท่าเทียมกันของผู้ถือหุ้น - หมวด 3 คณะกรรมการ อ.ส.ค. - หมวด 4 บทบาทของผู้มีส่วนได้เสีย - หมวด 5 ความยั่งยืนและนวัตกรรม - หมวด 6 การเปิดเผยข้อมูล - หมวด 7 การบริหารความเสี่ยงและการควบคุมภายใน - หมวด 8 จรรยาบรรณ - หมวด 9 การติดตามผลการดำเนินงาน

ตารางที่ 1 ตารางแสดงคำนิยาม GRC

คำว่า	ความหมาย					
คณะกรรมการบริหารความเสี่ยงและควบคุมภายใน	คณะกรรมการบริหารความเสี่ยงและควบคุมภายใน อ.ส.ค. ที่ได้รับการแต่งตั้งจากคณะกรรมการ อ.ส.ค. มีความตระหนักถึงความสำคัญในการเตรียมการหรือป้องกันต่อความเสี่ยงและควบคุมภายในที่ทำให้งานไม่ประสบความสำเร็จตามเป้าหมายและวัตถุประสงค์ขององค์กรจึงมุ่งมั่นดำเนินการบริหารความเสี่ยงและควบคุมภายในให้ครอบคลุมความเสี่ยงด้านกลยุทธ์ การดำเนินงาน การเงิน และการปฏิบัติตามกฎระเบียบ/กฎหมาย รวมถึงเหตุการณ์ใดๆ ที่มีโอกาสเกิดขึ้นและส่งผลกระทบต่อผลการบรรลุผลสำเร็จตามแผนกลยุทธ์และเป้าหมายทางธุรกิจของ อ.ส.ค. หรือเหตุการณ์ใดๆ ที่มีโอกาสเกิดขึ้นและส่งผลกระทบต่อผลลัพธ์ที่เกิดขึ้นจริงแตกต่างจากผลลัพธ์ที่คาดการณ์ไว้ โดย อ.ส.ค. เน้นกระบวนการบริหารความเสี่ยงตามหลัก COSO ERM⁶ ดังนี้ MISSION, VISION & CORE VALUES STRATEGY DEVELOPMENT BUSINESS OBJECTIVE FORMULATION IMPLEMENTATION & PERFORMANCE ENHANCED VALUE <table><tr><td> Governance & Culture 1. Exercises Board Risk Oversight 2. Establishes Operating Structures 3. Defines Desired Culture 4. Demonstrates Commitment to Core Values 5. Attracts, Develops, and Retains Capable Individuals </td><td> Strategy & Objective-Setting 6. Analyzes Business Context 7. Defines Risk Appetite 8. Evaluates Alternative Strategies 9. Formulates Business Objectives </td><td> Performance 10. Identifies Risk 11. Assesses Severity of Risk 12. Prioritizes Risks 13. Implements Risk Responses 14. Develops Portfolio View </td><td> Review & Revision 15. Assesses Substantial Change 16. Reviews Risk and Performance 17. Pursues improvement in Enterprise Risk Management </td><td> Information, Communication, & Reporting 18. Leverages Information and Technology 19. Communicates Risk Information 20. Reports on Risk, Culture, and Performance </td></tr></table>	Governance & Culture 1. Exercises Board Risk Oversight 2. Establishes Operating Structures 3. Defines Desired Culture 4. Demonstrates Commitment to Core Values 5. Attracts, Develops, and Retains Capable Individuals	Strategy & Objective-Setting 6. Analyzes Business Context 7. Defines Risk Appetite 8. Evaluates Alternative Strategies 9. Formulates Business Objectives	Performance 10. Identifies Risk 11. Assesses Severity of Risk 12. Prioritizes Risks 13. Implements Risk Responses 14. Develops Portfolio View	Review & Revision 15. Assesses Substantial Change 16. Reviews Risk and Performance 17. Pursues improvement in Enterprise Risk Management	Information, Communication, & Reporting 18. Leverages Information and Technology 19. Communicates Risk Information 20. Reports on Risk, Culture, and Performance
Governance & Culture 1. Exercises Board Risk Oversight 2. Establishes Operating Structures 3. Defines Desired Culture 4. Demonstrates Commitment to Core Values 5. Attracts, Develops, and Retains Capable Individuals	Strategy & Objective-Setting 6. Analyzes Business Context 7. Defines Risk Appetite 8. Evaluates Alternative Strategies 9. Formulates Business Objectives	Performance 10. Identifies Risk 11. Assesses Severity of Risk 12. Prioritizes Risks 13. Implements Risk Responses 14. Develops Portfolio View	Review & Revision 15. Assesses Substantial Change 16. Reviews Risk and Performance 17. Pursues improvement in Enterprise Risk Management	Information, Communication, & Reporting 18. Leverages Information and Technology 19. Communicates Risk Information 20. Reports on Risk, Culture, and Performance		
คณะกรรมการด้านกฎหมาย	คณะกรรมการด้านกฎหมาย อ.ส.ค. ที่ได้รับการแต่งตั้งจากคณะกรรมการ อ.ส.ค. ดำเนินการออกแนวนโยบายหลักการกำกับดูแลการปฏิบัติงานให้เป็นไปตามมีตามกฎหมาย ข้อบังคับ ระเบียบ คำสั่ง ประกาศ และแนวปฏิบัติที่บังคับใช้กับธุรกรรมต่างๆ ของ อ.ส.ค. ทั้งภายในและภายนอก เพื่อป้องกันไม่ให้เกิดความเสียหายต่อทรัพย์สิน และชื่อเสียงของ อ.ส.ค. หรือการถูกเข้าแทรกแซงจากกลุ่มผลประโยชน์					

ตารางที่ 1 ตารางแสดงคำนิยาม GRC

3. วัตถุประสงค์ของคู่มือ

3.1 เพื่อสนับสนุนให้ทุกหน่วยงานของ อ.ส.ค. สามารถใช้เป็นกรอบแนวทางการปฏิบัติ การบูรณาการ GRC ให้เป็นมาตรฐานเดียวกันทั่วทั้งองค์กร

3.2 เพื่อสนับสนุนให้ทุกหน่วยงานของ อ.ส.ค. สามารถดำเนินการบูรณาการ GRC ให้สอดคล้องกับแนวปฏิบัติที่ดีตามกรอบการบริหารความเสี่ยงตามมาตรฐานสากลของ Committee of Sponsoring Organizations of the Tread way Commission : COSO 2017 /2013 รวมถึง ISO 27001/27005/38500 และแนวปฏิบัติของหน่วยงานที่กำกับดูแล เช่น กระทรวงเกษตรและสหกรณ์ เป็นต้น

3.3 เพื่อเผยแพร่แนวทางการบูรณาการกำกับดูแลกิจการที่ดี บริหารความเสี่ยงและการกำกับการปฏิบัติตามกฎหมายให้ผู้บริหารและผู้ปฏิบัติงานทุกระดับทราบและนำไปปฏิบัติใช้

3.4 เพื่อส่งเสริมความรู้ความเข้าใจ และการสร้างวัฒนธรรมที่สนับสนุนการบริหารความเสี่ยง และการควบคุมภายในเพื่อให้การบริหารความเสี่ยงและการควบคุมภายในเป็นส่วนหนึ่งของวัฒนธรรมองค์กร

4. นโยบายการบูรณาการ GRC

การบูรณาการ GRC หมายถึง การทำให้คณะกรรมการ อ.ส.ค. สามารถกำกับดูแลองค์กรและให้คำแนะนำแก่ผู้บริหารเพื่อให้ดำเนินงานเป็นไปตามกฎหมาย ข้อบังคับ ระเบียบที่เกี่ยวข้องสอดคล้องกับ มาตรฐานสากล และแนวทางปฏิบัติที่ดีได้อย่างมั่นใจ ซึ่งสะท้อนได้จากการที่ผู้บริหารนำหลักการกำกับดูแล กิจการที่ดีมาใช้ในการบริหารจัดการ มีการบริหารความเสี่ยงที่เป็นระบบครบถ้วนและตรงประเด็น และสามารถจัดกระบวนการทำงานเพื่อให้มีการปฏิบัติตามกฎหมายและกฎระเบียบหรือการควบคุมภายในได้ อย่างเหมาะสม ภายใต้ผลตอบแทนและต้นทุนการจัดการที่สมเหตุผล และให้ความสำคัญกับการนำเทคโนโลยี มาสนับสนุนการทำงานให้มีประสิทธิภาพและการสื่อสารข้อมูลสารสนเทศอย่างถูกต้องเหมาะสม ทันเวลาต่อ การตัดสินใจของผู้เกี่ยวข้องในทุกระดับเพื่อมุ่งสู่การดำเนินที่ดีได้อย่างยั่งยืน

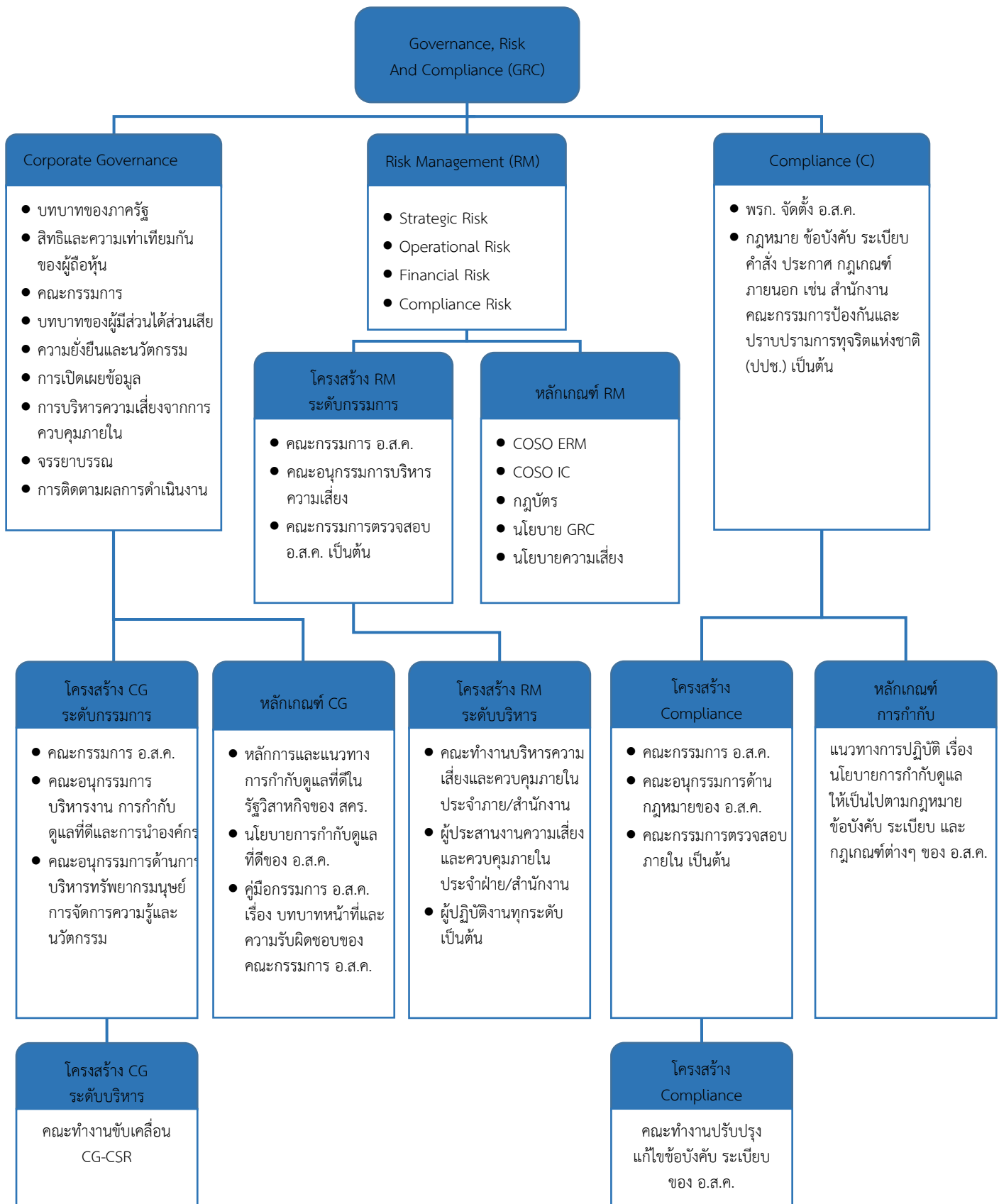
5. โครงสร้าง และบทบาทหน้าที่ความรับผิดชอบในการบูรณาการ GRC

อ.ส.ค. ได้มีการจัดโครงสร้างการกำกับดูแลกิจการบูรณาการ GRC อย่างเหมาะสม เพื่อสนับสนุนและส่งเสริมการบูรณาการ GRC ให้มีประสิทธิภาพ และให้ทุกหน่วยงานของ อ.ส.ค. ใช้เป็นกรอบ และแนวทางปฏิบัติการบูรณาการ GRC ให้เป็นมาตรฐานเดียวกันทั่วทั้งองค์กรได้ตามนโยบายบูรณาการ GRC โดยมีโครงสร้างการบูรณาการ GRC ดังนี้

โครงสร้างการบูรณาการ GRC	บทบาทและหน้าที่
- คณะอนุกรรมการบริหารงาน การกำกับดูแลที่ดี และการนำองค์กร - คณะอนุกรรมการด้านการบริหารทรัพยากรมนุษย์ การจัดการความรู้และนวัตกรรม	- ตามคำสั่ง อ.ส.ค. ที่ 3/2568 เรื่องแต่งตั้งคณะอนุกรรมการบริหารงาน การกำกับดูแลที่ดีและการนำองค์กร - ตามคำสั่ง อ.ส.ค. ที่ 4/2568 เรื่องแต่งตั้งคณะอนุกรรมการด้านการบริหารทรัพยากรมนุษย์ การจัดการความรู้และนวัตกรรม
คณะอนุกรรมการบริหารความเสี่ยงและควบคุมภายใน อ.ส.ค.	ตามคำสั่ง อ.ส.ค. ที่ 5/2568 เรื่องแต่งตั้งคณะอนุกรรมการบริหารความเสี่ยงและควบคุมภายใน อ.ส.ค.
คณะอนุกรรมการด้านกฎหมาย อ.ส.ค.	ตามคำสั่ง อ.ส.ค. ที่ 6/2567 เรื่องแต่งตั้งคณะอนุกรรมการด้านกฎหมาย อ.ส.ค.

ตารางที่ 2 ตารางแสดงโครงสร้าง และบทบาทหน้าที่ความรับผิดชอบในการบูรณาการ GRC

โครงสร้างองค์กรที่สนับสนุนการบูรณาการตามหลัก GRC



รูปที่ 1 โครงสร้างองค์กรที่สนับสนุนการบูรณาการตามหลัก GRC

6. แนวทางการปฏิบัติการบูรณาการ GRC

อ.ส.ค. มีการบูรณาการ GRC โดยนำหลักเกณฑ์การประเมินผลการดำเนินงานรัฐวิสาหกิจตามระบบการประเมินใหม่ : หลักเกณฑ์ Enabler 3 ด้าน การบริหารความเสี่ยงและการควบคุมภายใน (Risk Management & Internal Control) เรื่อง ธรรมาภิบาลและวัฒนธรรมองค์กร (Governance and Culture) โดยมีแนวปฏิบัติดังนี้

6.1 กำหนดบทบาทคณะกรรมการบริหารความเสี่ยงฯ ในการกำกับติดตามการบริหารความเสี่ยงและการควบคุมภายใน อ.ส.ค. มุ่งเน้นการจัดให้มีนโยบายที่บูรณาการในเรื่องการกำกับดูแลกิจการที่ดี การบริหารความเสี่ยงและการควบคุมภายใน การปฏิบัติตามกฎหมาย ระเบียบ ข้อบังคับที่เกี่ยวข้อง สอดคล้องกับมาตรฐานสากล (Integrated Governance Risk and Compliance : GRC)

6.2 มีโครงสร้างและบทบาทหน้าที่ มุ่งเน้นการกำหนดโครงสร้างและบทบาทหน้าที่ของการบริหารจัดการความเสี่ยงและการควบคุมภายในที่ชัดเจน เป็นรูปธรรม รวมทั้งการจัดทำคู่มือให้สอดคล้องกับนโยบายบูรณาการการกำกับดูแลกิจการที่ดี การบริหารความเสี่ยง และการกำกับการปฏิบัติตามกฎหมาย

6.3 สร้างบรรยากาศและวัฒนธรรมในการบูรณาการ GRC รวมถึงการกำหนดกระบวนการ/การดำเนินการสร้างความตระหนักรู้ ความเข้าใจ ในเรื่องการบริหารความเสี่ยงและการควบคุมภายใน

6.4 จัดกิจกรรมที่ส่งเสริมให้เกิดความมุ่งมั่นต่อค่านิยมองค์กร และสร้างวัฒนธรรมองค์กรด้านการบริหารความเสี่ยงและการควบคุมภายในที่ตอบสนอง และส่งเสริมค่านิยมองค์กร

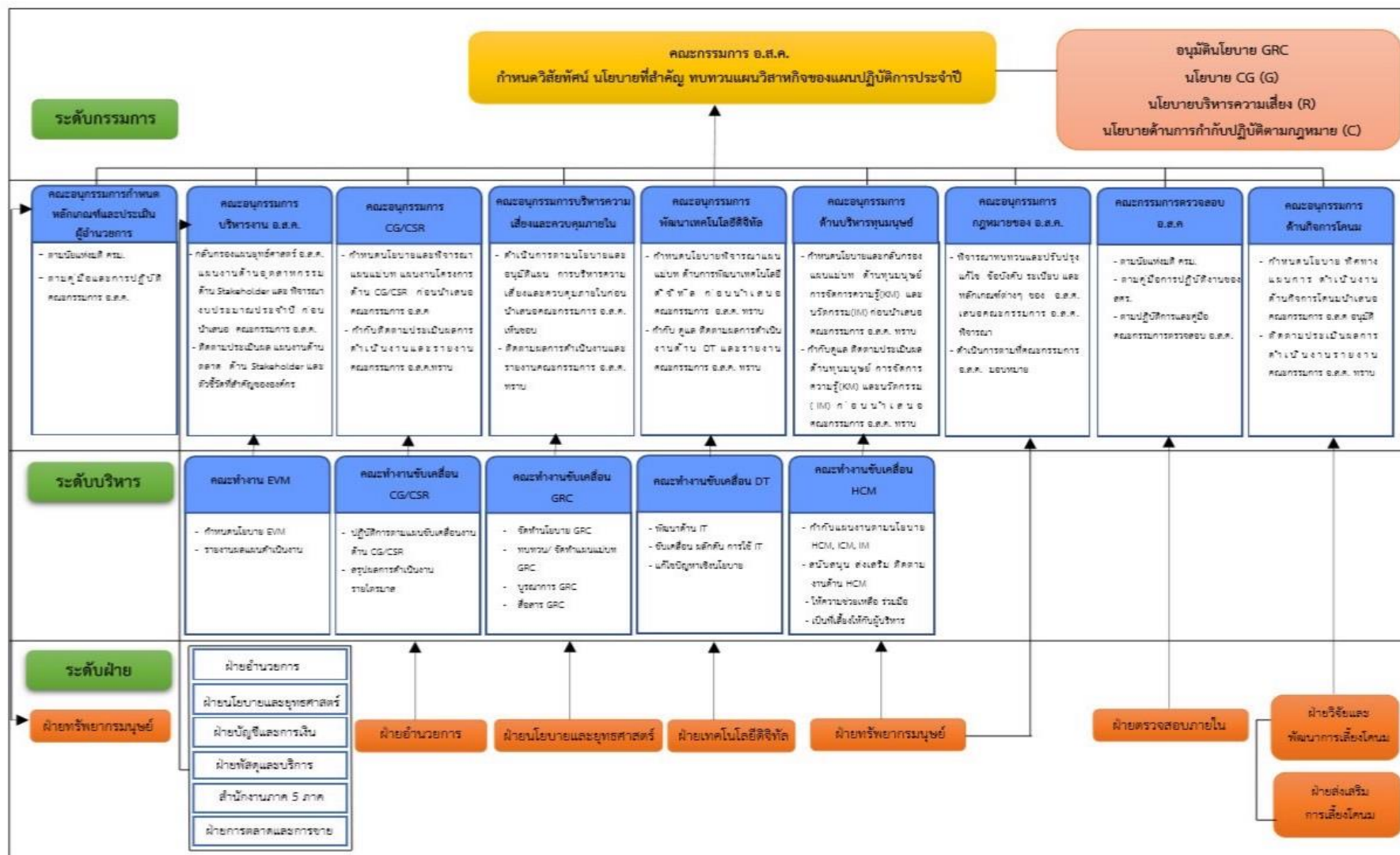
6.5 สร้างแรงจูงใจในการพัฒนาและการรักษาบุคลากร โดยการเชื่อมโยงผลการประเมินระดับบุคคลเฉพาะการบริหารความเสี่ยงและการควบคุมภายใน เข้ากับผลตอบแทน/แรงจูงใจ (Incentive)

7. รูปแบบการรายงาน

อ.ส.ค. กำหนดให้มีการรายงานและติดตามผลการบูรณาการ GRC อย่างน้อยไตรมาสละ 1 ครั้ง เพื่อให้เกิดความมั่นใจว่า ผลการดำเนินการถูกต้อง/เหมาะสมและมีประสิทธิภาพ โดยแผนกบริหารความเสี่ยงและควบคุมภายใน รวบรวมข้อมูลจัดทำวาระและประเมินระดับความเสี่ยง (ภาคผนวก ก) และนำเสนอคณะกรรมการบริหารความเสี่ยงฯ เพื่อพิจารณากลับกรองการบูรณาการ GRC และเสนอคณะกรรมการ อ.ส.ค. เพื่อทราบการบูรณาการ GRC ในกรณีที่มียุทธศาสตร์**รวมทั้งนำเสนอคณะกรรมการตรวจสอบเพื่อทราบ ทั้งนี้เพื่อพิจารณาให้ข้อเสนอแนะ รวมถึงมีการติดตามประเด็นความเสี่ยงและการควบคุมภายใน

หมายเหตุ : กรณีที่มีนัยสำคัญ** หมายถึง กรณีที่มีผลกระทบต่อผลิตภัณฑ์ ผลการดำเนินงาน ชื่อเสียงและภาพลักษณ์ของ อ.ส.ค. อย่างรุนแรงโดยเร็ว

แผนภูมิแสดงสายการรายงาน GRC



รูปที่ 2 แผนภูมิแสดงสายการรายงาน GRC

8. อำนาจอนุมัติ และการทบทวนคู่มือการบูรณาการ GRC

8.1 คณะอนุกรรมการบริหารความเสี่ยงและควบคุมภายใน อ.ส.ค. เป็นผู้ที่มีอำนาจอนุมัติคู่มือการบูรณาการ GRC

8.2 แผนกบริหารความเสี่ยงและควบคุมภายใน จะทบทวนคู่มือการบูรณาการ GRC ทุกปี (หากมีการเปลี่ยนแปลงเกณฑ์ประเมิน หรือ มีเหตุการณ์ที่เปลี่ยนแปลง) และนำเสนอต่ออนุกรรมการบริหารความเสี่ยงและควบคุมภายในเพื่อพิจารณา เพื่อให้มั่นใจว่าคู่มือดังกล่าวยังเหมาะสมกับสภาพแวดล้อมการดำเนินงานของ อ.ส.ค. และเสนอต่อคณะกรรมการ อ.ส.ค. เพื่อทราบ

9. ภาคผนวก ก

9.1 คำศัพท์

9.2 ตารางการประเมินความเสี่ยง (Risk Assessment Matrix : ก่อนการจัดการ)

9.2.1 ตารางประเมินโอกาสที่จะเกิดความเสี่ยง (Likelihood)

9.2.2 ตารางการประเมินความรุนแรงของผลกระทบ (Impact)

9.3 การจัดระดับความเสี่ยง (หลังการจัดการ)

9.4 (ตัวอย่าง) การกรอกแบบฟอร์มประเมินความเสี่ยงสำหรับการบูรณาการ GRC (Integrated GRC)

9.1 คำศัพท์

คำศัพท์	ความหมาย
ความเสี่ยง (Risk)	เหตุการณ์หรือสถานการณ์ที่มีความไม่แน่นอน ซึ่งอาจเกิดขึ้นและทำให้เกิดความผิดพลาด ความเสียหาย การรั่วไหล ความสูญเสีย ไม่สามารถดำเนินงานให้บรรลุผลสำเร็จตามวัตถุประสงค์หรือเป้าหมายที่ตั้งไว้ได้
การประเมินความเสี่ยง (Risk Assessment)	กระบวนการที่สำคัญที่ใช้ในการระบุและวิเคราะห์ความเสี่ยงที่มีผลกระทบต่อ การบรรลุวัตถุประสงค์ รวมทั้งการค้นหาและการนำเอาวิธีการควบคุมเพื่อ ป้องกันหรือลดความเสี่ยงมาใช้ให้เกิดประสิทธิภาพและประสิทธิผล
โอกาสที่จะเกิดความเสี่ยง (Likelihood)	ความถี่หรือความเป็นไปได้ที่เหตุการณ์/ความเสี่ยงจะเกิดขึ้น
ผลกระทบ (Impact)	ผลกระทบจากเหตุการณ์/ความเสี่ยงจะเกิดขึ้น
ปัจจัยเสี่ยง (Risk Factor)	ต้นเหตุหรือสาเหตุที่มาของความเสี่ยงที่จะทำให้ไม่บรรลุวัตถุประสงค์ที่กำหนดไว้ โดยต้องระบุได้ด้วยว่าเหตุการณ์นั้นจะเกิดที่ไหน เมื่อใด และเกิดขึ้นได้อย่างไร และทำไม ทั้งนี้สาเหตุที่ระบุควรเป็นสาเหตุที่แท้จริง เพื่อจะได้วิเคราะห์และกำหนดมาตรการลดความเสี่ยงในภายหลังได้อย่างถูกต้อง

ตารางที่ 3 ตารางแสดงคำศัพท์

คำศัพท์	ความหมาย
ความเปี่ยงเบนของระดับความเสี่ยงที่ยอมรับได้ (Risk Tolerance)	ระดับเปี่ยงเบนจากเกณฑ์หรือประเภทของความเสี่ยงที่ยอมรับได้ ซึ่งค่าเปี่ยงเบนจะเป็นช่วงที่ยอมให้ผลการดำเนินงานเปี่ยงเบนหรือคลาดเคลื่อนไปจากเป้าหมายที่กำหนดโดยจะต้องมีความสัมพันธ์กับระดับความเสี่ยงที่ยอมรับได้
ความเสี่ยงที่ยอมรับได้ (Risk Appetite)	ประเภทและเกณฑ์ของความเสี่ยงหรือความไม่แน่นอนโดยรวมที่องค์กรยอมรับได้โดยยังคงให้องค์กรสามารถบรรลุเป้าหมาย ซึ่งความเสี่ยงที่ยอมรับได้นั้น จะต้องสอดคล้องกับเป้าหมายองค์กร ไม่ด้อยกว่าค่าเป้าหมายค่าเดียวหรือระบุเป็นช่วงก็ได้ ทั้งนี้ขึ้นอยู่กับความเหมาะสมของปัจจัยเสี่ยงแต่ละตัว

ตารางที่ 3 ตารางแสดงคำศัพท์

9.2 ตารางการประเมินความเสี่ยง (Risk Assessment Matrix)

Risk Assessment Matrix		ความน่าจะเป็น				
		ยากที่จะเกิด	ไม่น่าจะเกิด	เป็นไปได้ที่จะเกิด	น่าจะเกิด	ค่อนข้างแน่นอน
		1	2	3	4	5
ผลกระทบ	สูงมาก	5 (5x1)	10 (5x2)	15 (5x3)	20 (5x4)	25 (5x5)
	สูง	4 (4x1)	8 (4x2)	12 (4x3)	16 (4x4)	20 (4x5)
	ปานกลาง	3 (3x1)	6 (3x2)	9 (3x3)	12 (3x4)	15 (3x5)
	ต่ำ	2 (2x1)	4 (2x2)	6 (2x3)	8 (2x4)	10 (2x5)
	ต่ำมาก	1 (1x1)	2 (1x2)	6 (1x3)	4 (1x4)	5 (1x5)
ระดับของความเสี่ยง						

ตารางที่ 4 ตารางแสดงการประเมินความเสี่ยง (Risk Assessment Matrix)

ตารางแสดงความหมายระดับความเสี่ยง (Risk Assessment Matrix)

ระดับความเสี่ยง	คะแนน (I,L)	สัญลักษณ์	ความหมาย
สูงมาก	16 - 25		ความเสี่ยงระดับสูงมาก/ระดับที่ไม่สามารถยอมรับได้ จำเป็นต้องจัดทำแผนการดำเนินงานเร่งรัดจัดการความเสี่ยงเพิ่มเติมสำหรับการบริหารจัดการความเสี่ยง
สูง	10 - 15		ความเสี่ยงระดับสูง/ระดับที่ไม่สามารถยอมรับได้ ผู้บริหารควรพิจารณาจัดทำแผนการดำเนินงานเพิ่มเติม เพื่อให้ความเสี่ยงกลับมาอยู่ในระดับที่ยอมรับได้
ปานกลาง	5 - 9		ความเสี่ยงระดับปานกลาง/ระดับที่พอยอมรับได้ ผู้บริหารควรมอบหมายให้ผู้รับผิดชอบดำเนินการติดตามประสิทธิภาพการควบคุมภายในเป็นประจำ เพื่อป้องกันไม่ให้ความเสี่ยงเคลื่อนย้ายไปยังระดับที่ยอมรับไม่ได้
ต่ำ	1 - 4		ความเสี่ยงระดับต่ำ/ระดับความเสี่ยงที่ยอมรับได้ ไม่ต้องควบคุมความเสี่ยง ไม่ต้องมีการจัดการเพิ่มเติม

ตารางที่ 5 ตารางแสดงความหมายระดับความเสี่ยง (Risk Assessment Matrix)

9.2.1 ตารางประเมินโอกาสที่จะเกิดความเสี่ยง (Likelihood)

โอกาสที่จะเกิดความเสี่ยง (Likelihood)	ระดับคะแนน	ความน่าจะเป็นสำหรับโอกาสที่จะเกิด
ค่อนข้างแน่นอน	5	มีการปฏิบัติที่ฝ่าฝืนหรือไม่ปฏิบัติหรือไม่ควบคุมดูแลให้ปฏิบัติเป็นไปตามที่กฎหมาย/กฎเกณฑ์กำหนด
น่าจะเกิด	4	มีกระบวนการควบคุมแต่ยังไม่เพียงพอหรือไม่เหมาะสมเป็นเหตุให้มีการปฏิบัติที่ไม่ถูกต้องหรือไม่สม่ำเสมอ
เป็นไปได้ที่จะเกิด	3	มีกระบวนการการควบคุมแต่มีการปฏิบัติที่ล่าช้า ล่วงเลยระยะเวลาที่กฎหมายกำหนด
ไม่น่าจะเกิด	2	มีกระบวนการควบคุมเพียงพอ มีความพร้อมต่อการปฏิบัติตามที่กฎหมาย/กฎเกณฑ์กำหนดไว้
ยากที่จะเกิด	1	มีกระบวนการควบคุมเพียงพอ เหมาะสมโดยไม่จำเป็นต้องกำหนดเพิ่มเติม

ตารางที่ 6 ตารางแสดงประเมินโอกาสที่จะเกิดความเสี่ยง (Likelihood)

9.2.2 ตารางการประเมินความรุนแรงของผลกระทบ (Impact)

ระดับความรุนแรง ของผลกระทบ (Impact)	ระดับ คะแนน	ผลกระทบ
สูงมาก	5	อ.ส.ค. ถูกลดระดับเกรตริวิสาหกิจ
สูง	4	อ.ส.ค. ได้รับโทษจากหน่วยงานที่กำลังดูแล
ปานกลาง	3	อ.ส.ค. ได้รับหนังสือตักเตือน หรือต้องชี้แจงต่อหน่วยงานที่กำลังดูแล
ต่ำ	2	อ.ส.ค. อาจได้รับข้อเสนอแนะ/ข้อสังเกตจากหน่วยงานที่กำลังดูแลเพิ่มเติม (ข้อสังเกตจาก สคร.,ทริส)
ต่ำมาก	1	ไม่มีผลกระทบต่อการดำเนินงานที่สำคัญ

ตารางที่ 7 ตารางแสดงประเมินความรุนแรงของผลกระทบ (Impact)

9.3 การจัดระดับความเสี่ยง (หลังการจัดการ)

การจัดระดับความเสี่ยง หน่วยงานเจ้าของความเสี่ยงจะทำการจัดระดับความเสี่ยงโดยประเมินระดับความเสี่ยงที่ได้กับคุณภาพความเสี่ยง เพื่อระบุการจัดระดับความเสี่ยงของ อ.ส.ค. ที่บ่งชี้ถึงระดับความสำคัญที่ต้องให้ความเอาใจใส่ ติดตามและดำเนินมาตรการแก้ไข โดยมีตารางจัดระดับความเสี่ยง ดังนี้

การจัดระดับความเสี่ยง		ระดับความเสี่ยง		
		ต่ำ	ปานกลาง	สูงมาก
คุณภาพการ	อ่อน	ปานกลาง	ค่อนข้างสูง	สูง
	พอใช้	ค่อนข้างต่ำ	ปานกลาง	ค่อนข้างสูง
	ดี	ต่ำ	ค่อนข้างต่ำ	ปานกลาง

ตารางที่ 8 ตารางแสดงการจัดระดับความเสี่ยง (หลังการจัดการ)

โดยการคำนวณระดับความเสี่ยง = โอกาสในการเกิดเหตุการณ์ต่างๆ x ความรุนแรงของเหตุการณ์นั้น ซึ่งระดับความเสี่ยงที่ได้รับนี้จะแสดงถึงระดับความสำคัญในการบริหารความเสี่ยง โดยพิจารณาระดับของความเสี่ยงตามเกณฑ์ที่กำหนดตามร่าง คือ

ลำดับ	ระดับความเสี่ยง	ช่วงคะแนน
1	ความเสี่ยงระดับต่ำ (Low Risk : L)	1 - 4 คะแนน
2	ความเสี่ยงระดับปานกลาง (Moderate Risk : M)	5 - 9 คะแนน
3	ความเสี่ยงระดับสูง (High Risk : H)	10 - 15 คะแนน
4	ความเสี่ยงระดับสูงมาก (Extreme Risk : E)	16 - 25 คะแนน

ตารางที่ 9 ตารางแสดงการคำนวณระดับความเสี่ยง

9.4 (ตัวอย่าง) การกรอกแบบฟอร์มประเมินความเสี่ยงสำหรับบูรณาการ GRC (Integrated GRC)

กฎหมาย/ข้อบังคับ : ABC หน่วยงานที่นำไปปฏิบัติ/บังคับใช้ : /ฝ่ายทรัพยากรมนุษย์

ลำดับ	ประเด็นความเสี่ยง	ก่อนการจัดการความเสี่ยง			แนวทางการจัดการ(กรณีความเสี่ยงสูง/สูงมาก)	หลังการจัดการความเสี่ยง		
		โอกาสเกิดความเสี่ยง (Likelihood)	ระดับผลกระทบ (Impact)	ระดับความเสี่ยงก่อนการจัดการ		ระดับความเสี่ยง	การจัดการความเสี่ยง/การควบคุมภายใน	ระดับความเสี่ยงหลังการจัดการ
1	ความเสี่ยงจากพนักงานไม่ปฏิบัติตามกฎระเบียบข้อบังคับ	3	4	สูง (ต้องมีแนวทางการจัดการเพิ่มเติมเพื่อลดระดับความเสี่ยง)	ทบทวนปรับปรุงแผนการดำเนินการให้อยู่ภายใต้กฎหมาย/ข้อบังคับ	สูง	พอใช้	ค่อนข้างสูง

Risk Assessment Matrix		ความน่าจะเป็น				
		ยากที่จะเกิด	ไม่แน่ใจว่าจะเกิด	เป็นไปได้ที่จะเกิด	น่าจะเกิด	ค่อนข้างแน่นอน
		1	2	3	4	5
ผลกระทบ	สูงมาก	5 (5x1)	10 (5x2)	15 (5x3)	20 (5x4)	25 (5x5)
	สูง	4 (4x1)	8 (4x2)	12 (4x3)	16 (4x4)	20 (4x5)
	ปานกลาง	3 (3x1)	6 (3x2)	9 (3x3)	12 (3x4)	15 (3x5)
	ต่ำ	2 (2x1)	4 (2x2)	6 (2x3)	8 (2x4)	10 (2x5)
	ต่ำมาก	1 (1x1)	2 (1x2)	3 (1x3)	4 (1x4)	5 (1x5)
ระดับของความเสี่ยง						

การจัดระดับความเสี่ยง		ระดับความเสี่ยง		
		ต่ำ	ปานกลาง	สูงมาก
คุณภาพการจัดการ	อ่อน	ปานกลาง	ค่อนข้างสูง	สูง
	พอใช้	ค่อนข้างต่ำ	ปานกลาง	ค่อนข้างสูง
	ดี	ต่ำ	ค่อนข้างต่ำ	ปานกลาง
		ต่ำ	ปานกลาง	สูงมาก