



หลักเกณฑ์ แนวปฏิบัติ  
และคู่มือปฏิบัติเกี่ยวกับ  
การบริหารความเสี่ยง  
และการควบคุมภายใน  
สำหรับรัฐวิสาหกิจ  
ปี 2568



สำนักงานคณะกรรมการนโยบายรัฐวิสาหกิจ  
กระทรวงการคลัง



[www.sepo.go.th](http://www.sepo.go.th)



**หลักเกณฑ์ แนวปฏิบัติ และคู่มือปฏิบัติ**  
**เกี่ยวกับการบริหารความเสี่ยง**  
**และการควบคุมภายใน**  
**สำหรับรัฐวิสาหกิจ ปี 2568**



# บทนำ

ปัจจุบันรัฐวิสาหกิจดำเนินงานท่ามกลางบริบทที่เปลี่ยนแปลงอย่างรวดเร็วและมีความไม่แน่นอนสูง ภายใต้ภาวะเศรษฐกิจที่ผันผวน ความก้าวหน้าทางเทคโนโลยีสารสนเทศ และความคาดหวังที่เพิ่มขึ้นจากผู้มีส่วนได้เสีย ตลอดจนบทบาทด้านความรับผิดชอบต่อสังคมและสิ่งแวดล้อมที่มีความสำคัญมากยิ่งขึ้น ดังนั้น เพื่อให้องค์กรสามารถปรับตัวได้อย่างเหมาะสมและดำเนินงานได้อย่างมีประสิทธิภาพภายใต้บริบทที่เปลี่ยนแปลงดังกล่าว รัฐวิสาหกิจจึงจำเป็นต้องให้ความสำคัญกับระบบการบริหารความเสี่ยง และการควบคุมภายในอย่างรัดกุมและเป็นระบบ อันจะส่งผลให้รัฐวิสาหกิจสามารถขับเคลื่อนภารกิจได้อย่างมีประสิทธิภาพ โปร่งใส และยั่งยืน ซึ่งที่ผ่านมา สำนักงานคณะกรรมการนโยบายรัฐวิสาหกิจ (สคร.) ได้จัดทำหลักเกณฑ์/แนวทางปฏิบัติ และคู่มือปฏิบัติเกี่ยวกับการบริหารความเสี่ยงและการควบคุมภายใน ปี 2555 (หลักเกณฑ์/แนวทางปฏิบัติ และคู่มือปฏิบัติ ปี 2555) สำหรับรัฐวิสาหกิจใช้ปฏิบัติงาน อย่างไรก็ตาม ปัจจุบันกฎหมาย หลักเกณฑ์/แนวทางปฏิบัติ และมาตรฐานด้านการบริหารความเสี่ยงและการควบคุมภายในทั้งภายในประเทศและต่างประเทศมีการปรับปรุงและพัฒนาอย่างต่อเนื่อง ประกอบกับพระราชบัญญัติวินัยการเงินการคลังของรัฐ พ.ศ. 2561 มาตรา 79 กำหนดให้หน่วยงานของรัฐจัดให้มีการตรวจสอบภายใน การควบคุมภายใน และการบริหารจัดการความเสี่ยง โดยให้ถือปฏิบัติตามมาตรฐานและหลักเกณฑ์ที่กระทรวงการคลังกำหนด ได้แก่ หลักเกณฑ์กระทรวงการคลังว่าด้วยมาตรฐานและหลักเกณฑ์ปฏิบัติการควบคุมภายในสำหรับหน่วยงานของรัฐ พ.ศ. 2561 และหลักเกณฑ์กระทรวงการคลังว่าด้วยมาตรฐานและหลักเกณฑ์ปฏิบัติการบริหารจัดการความเสี่ยงสำหรับหน่วยงานของรัฐ พ.ศ. 2562 โดยให้รัฐวิสาหกิจถือปฏิบัติตามหลักเกณฑ์หรือแนวปฏิบัติเกี่ยวกับการบริหารความเสี่ยงและการควบคุมภายใน และคู่มือปฏิบัติเกี่ยวกับการบริหารความเสี่ยงและการควบคุมภายในตามที่ สคร. กำหนด

ด้วยเหตุนี้ สคร. จึงได้จัดทำหลักเกณฑ์/แนวทางปฏิบัติ และคู่มือปฏิบัติเกี่ยวกับการบริหารความเสี่ยง และการควบคุมภายในสำหรับรัฐวิสาหกิจ ปี 2568 โดยได้นำมาตรฐานและหลักเกณฑ์ปฏิบัติการบริหารจัดการความเสี่ยงและการควบคุมภายในที่กระทรวงการคลังกำหนด แนวทางการกำกับดูแลกิจการที่ดี ในรัฐวิสาหกิจ เรื่องการบริหารความเสี่ยงและการควบคุมภายในอย่างเพียงพอและเหมาะสม ตามพระราชบัญญัติการพัฒนากำกับดูแลและบริหารรัฐวิสาหกิจ พ.ศ. 2562 มาตรฐานสากลด้านการบริหารความเสี่ยงและการควบคุมภายใน รวมถึงหลักเกณฑ์/แนวทางปฏิบัติ และคู่มือปฏิบัติ ปี 2555 มาประกอบการดำเนินการ โดยมุ่งหวังให้รัฐวิสาหกิจมีแนวปฏิบัติที่ดีในการบริหารความเสี่ยง และการควบคุมภายในที่สอดคล้องกับแนวปฏิบัติสากล ซึ่งจะเพิ่มประสิทธิภาพในการดำเนินงานของรัฐวิสาหกิจ และสร้างประโยชน์ให้แก่ผู้มีส่วนเกี่ยวข้องกับรัฐวิสาหกิจทุกฝ่าย รวมถึงประเทศชาติโดยรวม

สคร. หวังเป็นอย่างยิ่งว่าหลักเกณฑ์ แนวปฏิบัติ และคู่มือปฏิบัติเกี่ยวกับการบริหารความเสี่ยง และการควบคุมภายในสำหรับรัฐวิสาหกิจ ปี 2568 ฉบับนี้ จะเป็นประโยชน์แก่รัฐวิสาหกิจในการปฏิบัติ ให้เป็นไปตามมาตรฐานและหลักเกณฑ์ปฏิบัติการบริหารจัดการความเสี่ยงและการควบคุมภายใน ที่กระทรวงการคลังกำหนด ตลอดจนมาตรฐานสากล และแนวปฏิบัติที่ดี รวมถึงส่งเสริมให้รัฐวิสาหกิจ สามารถพัฒนาระบบการบริหารความเสี่ยงและการควบคุมภายในให้มีประสิทธิภาพยิ่งขึ้นต่อไป

# สารบัญ

หน้า

หลักการของหลักเกณฑ์ แนวปฏิบัติ และคู่มือปฏิบัติเกี่ยวกับการบริหารความเสี่ยงและการควบคุมภายในสำหรับรัฐวิสาหกิจ	1
1. ความเชื่อมโยงของการบริหารความเสี่ยงและการควบคุมภายใน	3
2. ปัจจัยสำคัญต่อความสำเร็จในการบริหารความเสี่ยงและการควบคุมภายใน	5
3. หลักเกณฑ์ แนวปฏิบัติ และคู่มือปฏิบัติเกี่ยวกับการบริหารความเสี่ยงสำหรับรัฐวิสาหกิจ	9
1) คำจำกัดความ	10
2) หลักการพื้นฐานการบริหารความเสี่ยง	10
3) การปฏิบัติตามหลักเกณฑ์	11
4) ลำดับชั้นของการปฏิบัติ	12
5) นิยามของคำสำคัญ	12
6) ภาพรวมหลักเกณฑ์ แนวปฏิบัติ และคู่มือปฏิบัติ	15
7) หลักเกณฑ์ แนวปฏิบัติ และคู่มือปฏิบัติ	18
• องค์ประกอบที่ 1 การกำกับดูแลและวัฒนธรรม (Governance and Culture)	18
หลักเกณฑ์	18
แนวปฏิบัติที่ 1 การกำหนดหน้าที่และคุณสมบัติของคณะกรรมการ	18
แนวปฏิบัติที่ 2 การกำหนดโครงสร้างองค์กรที่สนับสนุนให้เกิดการบริหารความเสี่ยงที่มีประสิทธิภาพ	20
แนวปฏิบัติที่ 3 การกำหนดคุณค่าหลักและพฤติกรรมที่พึงประสงค์	32
แนวปฏิบัติที่ 4 การปลูกฝังการบริหารความเสี่ยงจนเป็นวัฒนธรรมองค์กร	42
แนวปฏิบัติที่ 5 การเพิ่มขีดความสามารถของบุคลากรและการจัดสรรทรัพยากรให้เพียงพอในการบริหารความเสี่ยง	45
• องค์ประกอบที่ 2 กลยุทธ์และการกำหนดวัตถุประสงค์ (Strategy and Objective Setting)	49
หลักเกณฑ์	49
แนวปฏิบัติที่ 1 การระบุเหตุการณ์ที่อาจเกิดขึ้นและส่งผลกระทบต่อการดำเนินงานขององค์กร	49
แนวปฏิบัติที่ 2 การกำหนดระดับความเสี่ยงที่องค์กรยอมรับได้ และช่วงเบี่ยงเบนของระดับความเสี่ยงที่องค์กรยอมรับได้	50
แนวปฏิบัติที่ 3 การเลือกกลยุทธ์ขององค์กร	56
แนวปฏิบัติที่ 4 การกำหนดวัตถุประสงค์ในการประกอบกิจการ	57

• องค์ประกอบที่ 3 ผลการปฏิบัติงาน (Performance)	65
หลักเกณฑ์	65
แนวปฏิบัติที่ 1 การระบุความเสี่ยงที่ชัดเจนและครอบคลุมการดำเนินงานขององค์กร และการจัดทำทะเบียนความเสี่ยง	65
แนวปฏิบัติที่ 2 การกำหนดเกณฑ์การประเมินความเสี่ยงและการประเมินความเสี่ยง	75
แนวปฏิบัติที่ 3 การจัดลำดับความสำคัญของความเสี่ยง	86
แนวปฏิบัติที่ 4 การเลือกแนวทางการตอบสนองต่อความเสี่ยง	88
แนวปฏิบัติที่ 5 การจัดทำภาพรวมความเสี่ยง	98
• องค์ประกอบที่ 4 การสอบทานและการแก้ไขปรับปรุง (Review and Revision)	101
หลักเกณฑ์	101
แนวปฏิบัติที่ 1 การวิเคราะห์การเปลี่ยนแปลงจากปัจจัยภายในและปัจจัยภายนอก ที่อาจส่งผลให้มีการทบทวนแผนการบริหารจัดการความเสี่ยง	101
แนวปฏิบัติที่ 2 การทบทวนแผนการบริหารจัดการความเสี่ยง	104
แนวปฏิบัติที่ 3 การปรับปรุงกระบวนการบริหารความเสี่ยงขององค์กรอย่างต่อเนื่อง	105
• องค์ประกอบที่ 5 สารสนเทศ การสื่อสาร และการรายงาน (Information Communication and Reporting)	109
หลักเกณฑ์	109
แนวปฏิบัติที่ 1 การบริหารสารสนเทศด้านความเสี่ยงเพื่อการจัดการที่ดี	109
แนวปฏิบัติที่ 2 การกำหนดช่องทางสื่อสารข้อมูลและสารสนเทศด้านความเสี่ยง	113
แนวปฏิบัติที่ 3 การรายงานความเสี่ยงต่อคณะกรรมการ	117
<b>4. หลักเกณฑ์ แนวปฏิบัติ และคู่มือปฏิบัติเกี่ยวกับการควบคุมภายในสำหรับรัฐวิสาหกิจ</b>	<b>121</b>
1) คำจำกัดความ	122
2) หลักการพื้นฐานการควบคุมภายใน	122
3) การปฏิบัติตามหลักเกณฑ์	124
4) ลำดับขั้นของการปฏิบัติ	124
5) นิยามของคำสำคัญ	125
6) ภาพรวมหลักเกณฑ์ แนวปฏิบัติ และคู่มือปฏิบัติ	126
7) หลักเกณฑ์ แนวปฏิบัติ และคู่มือปฏิบัติ	129
• องค์ประกอบที่ 1 สภาพแวดล้อมการควบคุม (Control Environment)	129
หลักเกณฑ์	129
แนวปฏิบัติที่ 1 การกำหนดจรรยาบรรณในการประกอบกิจการ	129
แนวปฏิบัติที่ 2 การกำกับดูแลและสนับสนุนให้มีการควบคุมภายในโดยคณะกรรมการ	130

แนวปฏิบัติที่ 3 การกำหนดโครงสร้างองค์กรและสายการบังคับบัญชา	131
แนวปฏิบัติที่ 4 การออกแบบนโยบายและแนวปฏิบัติด้านทรัพยากรบุคคล ซึ่งครอบคลุมการจูงใจ พัฒนา รักษาไว้	137
แนวปฏิบัติที่ 5 การกำหนดอำนาจหน้าที่และความรับผิดชอบต่อผลการปฏิบัติงาน	139
• องค์ประกอบที่ 2 การประเมินความเสี่ยง (Risk Assessment)	142
หลักเกณฑ์	142
แนวปฏิบัติที่ 1 การกำหนดวัตถุประสงค์ระดับองค์กรและหน่วยงานที่เกี่ยวข้อง กับการควบคุมภายใน	142
แนวปฏิบัติที่ 2 การระบุเหตุการณ์ความเสี่ยงที่อาจมีผลกระทบต่อการทำงาน	143
แนวปฏิบัติที่ 3 การประเมินความเป็นไปได้ที่จะเกิดความเสี่ยงด้านการทุจริต	147
แนวปฏิบัติที่ 4 การระบุและประเมินการเปลี่ยนแปลงของสภาพแวดล้อมที่อาจมีผลกระทบ อย่างมีนัยสำคัญต่อระบบการควบคุมภายใน	148
• องค์ประกอบที่ 3 กิจกรรมการควบคุม (Control Activities)	149
หลักเกณฑ์	149
แนวปฏิบัติที่ 1 การเลือกและพัฒนากิจกรรมการควบคุม	149
แนวปฏิบัติที่ 2 การนำเทคโนโลยีสารสนเทศมาใช้ เพื่อสนับสนุนให้บรรลุวัตถุประสงค์ ของการควบคุมภายใน	153
แนวปฏิบัติที่ 3 การกำหนดและสื่อสารนโยบายที่เกี่ยวข้องกับการควบคุมภายใน	155
• องค์ประกอบที่ 4 สารสนเทศและการสื่อสาร (Information and Communication)	156
หลักเกณฑ์	156
แนวปฏิบัติที่ 1 การดำเนินงานด้านข้อมูลสารสนเทศและระบบจัดการฐานข้อมูล	156
แนวปฏิบัติที่ 2 การจัดให้มีการสื่อสารภายในองค์กร	158
แนวปฏิบัติที่ 3 การจัดให้มีการสื่อสารกับหน่วยงานภายนอก และมีช่องทางเพื่อเปิดรับข้อมูล จากผู้มีส่วนได้เสียภายนอก	160
• องค์ประกอบที่ 5 กิจกรรมติดตามผล (Monitoring)	161
หลักเกณฑ์	161
แนวปฏิบัติที่ 1 การกำหนดให้มีการพัฒนาและประเมินผลการควบคุมภายใน อย่างต่อเนื่องและสม่ำเสมอ	161
แนวปฏิบัติที่ 2 การสื่อสารข้อบกพร่องที่ได้จากการประเมินการควบคุมภายใน	166

<b>5. ภาคผนวก</b>	167
ตัวอย่างชื่อความเสี่ยงและคำอธิบายความเสี่ยง	169
คำถาม – คำตอบที่น่ารู้เกี่ยวกับการบริหาร ความเสี่ยงและการควบคุมภายใน	175
สรุปสาระสำคัญเกี่ยวกับการบริหารความเสี่ยงและการควบคุมภายใน (Infographics)	183
• สรุปการปรับปรุงที่สำคัญ	
• ปัจจัยสำคัญต่อความสำเร็จในการบริหารความเสี่ยงและการควบคุมภายใน	
• สรุปหลักเกณฑ์ แนวปฏิบัติ และคู่มือปฏิบัติเกี่ยวกับการบริหารความเสี่ยงและการควบคุมภายใน	
◦ การบริหารความเสี่ยง	
◦ การควบคุมภายใน	
• คำถาม – คำตอบที่น่ารู้เกี่ยวกับการบริหารความเสี่ยงและการควบคุมภายใน	
<b>6. บรรณานุกรม</b>	201

# หลักการของหลักเกณฑ์ แนวปฏิบัติ และคู่มือปฏิบัติเกี่ยวกับ การบริหารความเสี่ยงและการควบคุมภายในสำหรับรัฐวิสาหกิจ

หลักเกณฑ์ แนวปฏิบัติ และคู่มือปฏิบัติเกี่ยวกับการบริหารความเสี่ยงและการควบคุมภายในสำหรับรัฐวิสาหกิจ ปี 2568 มีวัตถุประสงค์เพื่อให้รัฐวิสาหกิจนำไปใช้เป็นแนวทางการดำเนินงานเกี่ยวกับการบริหารความเสี่ยงและการควบคุมภายในได้อย่างเหมาะสมและเป็นไปตามกฎหมาย หลักเกณฑ์ แนวปฏิบัติ และมาตรฐานทั้งภายในประเทศและต่างประเทศ ประกอบด้วยรายละเอียด ดังนี้

1. หลักเกณฑ์การบริหารความเสี่ยงและการควบคุมภายใน เป็นกรอบแนวทางการปฏิบัติที่ดี เพื่อให้เห็นภาพรวมของระบบการบริหารความเสี่ยงและการควบคุมภายในของแต่ละองค์กรประกอบ

2. แนวปฏิบัติเกี่ยวกับการบริหารความเสี่ยงและการควบคุมภายใน เป็นคำอธิบายแนวทางการดำเนินงานตามหลักเกณฑ์การบริหารความเสี่ยงและการควบคุมภายใน

3. คู่มือปฏิบัติเกี่ยวกับการบริหารความเสี่ยงและการควบคุมภายใน ประกอบด้วยวิธีการปฏิบัติที่สอดคล้องกับหลักเกณฑ์และแนวปฏิบัติเกี่ยวกับการบริหารความเสี่ยงและการควบคุมภายใน พร้อมด้วย การขยายความเนื้อหาที่สำคัญ ตัวอย่างข้อความ รูปแบบเอกสาร รูปแบบการรายงานที่รัฐวิสาหกิจสามารถนำไปใช้ปฏิบัติ เพื่อสนับสนุนให้เกิดการบริหารความเสี่ยงและการควบคุมภายในขององค์กรอย่างมีประสิทธิภาพ และประสิทธิผล

ทั้งนี้ รัฐวิสาหกิจสามารถนำหลักเกณฑ์ แนวปฏิบัติ และคู่มือปฏิบัติเกี่ยวกับการบริหารความเสี่ยงและการควบคุมภายในที่กำหนดไปประยุกต์ใช้ตามบริบทและความเหมาะสมของแต่ละองค์กรได้



1

ความเชื่อมโยงของการบริหารความเสี่ยง  
และการควบคุมภายใน

# ความเชื่อมโยงของการบริหารความเสี่ยงและการควบคุมภายใน

การบริหารความเสี่ยงและการควบคุมภายใน มักเป็นเรื่องที่ได้รับการกล่าวถึงควบคู่กันอยู่เสมอ การควบคุมภายในเป็นกระบวนการและมาตรการต่างๆ ที่องค์กรได้กำหนดขึ้น เพื่อสร้างความมั่นใจอย่างสมเหตุสมผล ในด้านการดำเนินงาน การรายงาน และการปฏิบัติตามกฎหมาย ระเบียบ และข้อบังคับ จากคำจำกัดความดังกล่าว อาจเกิดคำถามขึ้นว่า เหตุใดต้องทำให้เกิดความมั่นใจ ทั้งนี้ เนื่องจากทุกองค์กร ไม่ว่าจะองค์กรขนาดเล็ก ขนาดใหญ่ และไม่ว่าจะอยู่ในธุรกิจประเภทใดย่อมเผชิญกับความไม่แน่นอนในรูปแบบต่างๆ ความไม่แน่นอนนี้ หากเป็นเหตุการณ์ที่เกิดขึ้นแล้วจะส่งผลกระทบต่อการทำงานขององค์กร หรือเป็นอุปสรรคในการบรรลุวัตถุประสงค์หรือเป้าหมาย เราเรียกว่าเป็น “ความเสี่ยง” สาเหตุของความเสี่ยง อาจมีได้ทั้งจากปัจจัยภายใน เช่น ความสามารถของบุคลากร ระบบสารสนเทศ และจากปัจจัยภายนอก เช่น สภาพเศรษฐกิจ การเมือง ภัยธรรมชาติ เป็นต้น หากรัฐวิสาหกิจมิได้ตระหนักถึงความเสี่ยงต่างๆ รัฐวิสาหกิจจะมีความมั่นใจได้อย่างไรว่าการดำเนินงานจะบรรลุตามเป้าหมายที่กำหนดไว้

การบริหารความเสี่ยง เป็นกระบวนการบริหารจัดการเหตุการณ์ที่อาจเกิดขึ้นและส่งผลกระทบต่อองค์กร เพื่อให้สามารถดำเนินงานให้บรรลุวัตถุประสงค์ในการประกอบกิจการ รวมถึงเพื่อเพิ่มศักยภาพ และขีดความสามารถให้องค์กร จากคำจำกัดความนี้จะเห็นได้ว่า รัฐวิสาหกิจจำเป็นต้องทราบว่าองค์กรมีความเสี่ยงอะไรบ้าง และในระดับที่มากหรือน้อยเพียงใด เพื่อที่จะได้กำหนดวิธีการจัดการ และนำมาตราการต่างๆ มาปฏิบัติ เพื่อให้เกิดความมั่นใจว่าความเสียหายหรือความผิดพลาดจะไม่เกิดขึ้น หรือหากเกิดขึ้น จะยังอยู่ในระดับที่ยอมรับได้ ซึ่งการควบคุมภายในถือเป็นมาตรการที่กำหนดขึ้นเพื่อบริหารจัดการความเสี่ยงให้อยู่ในระดับที่เหมาะสม

ในการพิจารณาว่าการควบคุมภายในที่ปฏิบัติอยู่นั้นมีประสิทธิภาพและประสิทธิผลเพียงพอหรือไม่ หรือต้องกำหนดมาตรการในการจัดการความเสี่ยงเพิ่มเติมเพียงใด รัฐวิสาหกิจต้องพิจารณาร่วมกับระดับความเสี่ยงที่องค์กรยอมรับได้ (Risk Appetite: RA) กล่าวคือ มาตรการในการควบคุมดังกล่าว เมื่อนำไปปฏิบัติแล้วควรจะลดความเสี่ยงลงมาให้อยู่ในระดับความเสี่ยงที่องค์กรยอมรับได้ (RA)

องค์กรที่มีการบริหารความเสี่ยงและการควบคุมภายในที่มีประสิทธิภาพและประสิทธิผล จะช่วยส่งเสริมให้องค์กรมีระบบธรรมาภิบาลที่ดี และช่วยสนับสนุนให้การดำเนินงานบรรลุเป้าหมายที่กำหนดไว้ ตลอดจนสามารถตอบสนองความต้องการของผู้มีส่วนได้เสียได้อย่างเหมาะสม

# 2

ปัจจัยสำคัญต่อความสำเร็จในการบริหาร  
ความเสี่ยงและการควบคุมภายใน

# ปัจจัยสำคัญต่อความสำเร็จในการบริหารความเสี่ยง และการควบคุมภายใน

ปัจจัยสำคัญ 7 ประการ เพื่อช่วยให้การปฏิบัติตามกรอบการบริหารความเสี่ยงและการควบคุมภายในของรวิวิสาหกิจประสบความสำเร็จ มีดังนี้

**ปัจจัยที่ 1 การสนับสนุนจากคณะกรรมการและผู้บริหารระดับสูงของรวิวิสาหกิจ (Board of Directors and Senior Management Commitment)** การปฏิบัติตามกรอบการบริหารความเสี่ยงและการควบคุมภายในของรวิวิสาหกิจ จะประสบความสำเร็จเพียงใดขึ้นอยู่กับเจตนาธรรมณ์ การสนับสนุน การมีส่วนร่วม และความเป็นผู้นำของคณะกรรมการและผู้บริหารระดับสูงของรวิวิสาหกิจ โดยจะต้องให้ความสำคัญและสนับสนุนให้ทุกคนในองค์กรเข้าใจความสำคัญและคุณค่าของการบริหารความเสี่ยงและการควบคุมภายใน อีกทั้งจะต้องปลูกฝังจิตสำนึกให้ผู้ได้บังคับบัญชาทุกระดับตระหนักถึงความสำคัญของการบริหารความเสี่ยงและการควบคุมภายใน อย่างไรก็ตาม หากนำการควบคุมภายในมาปฏิบัติอย่างไม่เหมาะสม เช่น เข้มงวดหรือเคร่งครัดเกินสมควรอาจทำให้การปฏิบัติงานเป็นไปอย่างล่าช้า ไม่คล่องตัวได้ ดังนั้น จึงเป็นหน้าที่อีกประการหนึ่งของคณะกรรมการและผู้บริหารระดับสูงของรวิวิสาหกิจที่จะต้องทำให้เกิดความสมดุลระหว่างความคล่องตัวในการปฏิบัติงานกับระดับการควบคุมภายในที่มีประสิทธิผลเพียงพอ เพราะหากไม่มีการควบคุมภายในที่เพียงพอ หรือมีการควบคุมภายในแต่มีข้อบกพร่องที่สำคัญ อาจทำให้องค์กรมีความเสี่ยงที่จะเกิดความเสียหาย หรือแม้กระทั่งอาจเกิดการทุจริตของพนักงานหรือผู้บริหารได้

**ปัจจัยที่ 2 การใช้คำให้เกิดความเข้าใจแบบเดียวกัน (Common Language)** รวิวิสาหกิจที่ได้จัดทำกรอบนโยบายการบริหารความเสี่ยงและนโยบายที่เกี่ยวข้องกับการควบคุมภายในที่มีคำอธิบายองค์ประกอบอย่างชัดเจน จะทำให้ผู้บริหารและพนักงานทุกคนเข้าใจและปฏิบัติงานไปในแนวทางเดียวกัน และมีจุดหมายร่วมกันในการบริหารความเสี่ยงและการควบคุมภายใน

**ปัจจัยที่ 3 การปฏิบัติตามกระบวนการบริหารความเสี่ยงและการควบคุมภายในอย่างต่อเนื่อง (Ongoing Risk Management and Internal Control Process)** รวิวิสาหกิจสามารถนำกระบวนการบริหารความเสี่ยงและการควบคุมภายในมาปฏิบัติอย่างทั่วถึงทั้งองค์กร และกระทำอย่างต่อเนื่องสม่ำเสมอ

**ปัจจัยที่ 4 การสื่อสารอย่างมีประสิทธิภาพ (Effective Communication)** โดยมีวัตถุประสงค์เพื่อให้มั่นใจว่าผู้บริหารได้รับข้อมูลเกี่ยวกับความเสี่ยงและการควบคุมภายในอย่างถูกต้องและทันเวลา สามารถจัดการกับความเสี่ยงตามลำดับความสำคัญหรือตามการเปลี่ยนแปลงหรือความเสี่ยงที่เกิดขึ้นใหม่ และมีการติดตามแผนการจัดการความเสี่ยง รวมถึงมาตรการควบคุมอย่างต่อเนื่อง เพื่อนำมาใช้ปรับปรุงการบริหารรวิวิสาหกิจและจัดการความเสี่ยงและการควบคุมภายใน เพื่อให้รวิวิสาหกิจมีโอกาสในการบรรลุวัตถุประสงค์ได้มากที่สุด

**ปัจจัยที่ 5 การวัดผลการบริหารความเสี่ยงและการควบคุมภายใน (Measurement)** ประกอบด้วยรูปแบบ ดังนี้

- การวัดความเสี่ยงในรูปแบบของผลกระทบและโอกาสที่อาจเกิดขึ้น การบริหารความเสี่ยงและการควบคุมภายในที่ประสบความสำเร็จ จะช่วยให้ความเสี่ยงเหลืออยู่ในระดับที่รัฐวิสาหกิจยอมรับได้
- การวัดความสำเร็จของการบริหารความเสี่ยงและการควบคุมภายใน โดยอาศัยดัชนีชี้วัดผลการดำเนินงาน (Key Performance Indicator: KPI) ซึ่งอาจกำหนดเป็นระดับองค์กร ฝ่ายงาน หรือของแต่ละบุคคล การใช้ดัชนีชี้วัดผลการดำเนินงาน (KPI) นี้ อาจปฏิบัติร่วมกับกระบวนการด้านทรัพยากรบุคคล

**ปัจจัยที่ 6 การฝึกอบรมและกลไกด้านทรัพยากรบุคคล (Reinforcement Through Training and HR Mechanism)**

กรรมการ ผู้บริหาร และพนักงานทุกคนในรัฐวิสาหกิจควรได้รับการฝึกอบรมเพื่อให้เข้าใจกรอบการบริหารความเสี่ยงและนโยบายที่เกี่ยวข้องกับการควบคุมภายใน และความรับผิดชอบของแต่ละบุคคลในการจัดการความเสี่ยงและการควบคุมภายใน รวมทั้งได้รับการสื่อสารข้อมูลเกี่ยวกับความเสี่ยงและการควบคุมภายในอย่างทันเวลา นอกจากนี้ รัฐวิสาหกิจควรมีการประเมินผลการดำเนินงานส่วนที่เกี่ยวกับการบริหารความเสี่ยงและการควบคุมภายในด้วย

**ปัจจัยที่ 7 การติดตามและพัฒนาระบวนการบริหารความเสี่ยงและการควบคุมภายใน (Monitoring and Enhancing Risk Management and Internal Control Process)**

มีการกำหนดวิธีที่เหมาะสมในการติดตามและพัฒนาระบวนการบริหารความเสี่ยงและการควบคุมภายในให้สอดคล้องกับบริบทขององค์กรและสภาพแวดล้อมที่เปลี่ยนแปลงไป โดยควรพิจารณาประเด็นต่อไปนี้

- การรายงานและการสอบทานชั้นตอนตามกระบวนการบริหารความเสี่ยงและการควบคุมภายใน
- ความชัดเจนและสม่ำเสมอของการมีส่วนร่วมและความมุ่งมั่นของผู้บริหารระดับสูง
- บทบาทของผู้นำในการสนับสนุนและติดตามการบริหารความเสี่ยงและการควบคุมภายใน
- การประยุกต์ใช้เกณฑ์การประเมินผลการดำเนินงานที่เกี่ยวกับการบริหารความเสี่ยงและการควบคุมภายใน โดยกรณีที่มีการเปลี่ยนแปลงกระบวนการต้องมีการชี้แจงให้ผู้บริหารและพนักงานทุกคนรับทราบถึงการเปลี่ยนแปลงและผลที่รัฐวิสาหกิจและแต่ละบุคคลจะได้รับจากการเปลี่ยนแปลงนั้น



# 3

## หลักเกณฑ์ แนวปฏิบัติ และคู่มือปฏิบัติ เกี่ยวกับการบริหารความเสี่ยง สำหรับรัฐวิสาหกิจ

	หน้า
คำจำกัดความ	10
หลักการพื้นฐานการบริหารความเสี่ยง	10
การปฏิบัติตามหลักเกณฑ์	11
ลำดับชั้นของการปฏิบัติ	12
นิยามของคำสำคัญ	12
ภาพรวมหลักเกณฑ์ แนวปฏิบัติ และคู่มือปฏิบัติ	15
หลักเกณฑ์ แนวปฏิบัติ และคู่มือปฏิบัติ	18
• องค์ประกอบที่ 1 การกำกับดูแลและวัฒนธรรม (Governance and Culture)	18
• องค์ประกอบที่ 2 กลยุทธ์และการกำหนดวัตถุประสงค์ (Strategy and Objective Setting)	49
• องค์ประกอบที่ 3 ผลการปฏิบัติงาน (Performance)	65
• องค์ประกอบที่ 4 การสอบทานและการแก้ไขปรับปรุง (Review and Revision)	101
• องค์ประกอบที่ 5 สารสนเทศ การสื่อสาร และการรายงาน (Information Communication and Reporting)	109

# หลักเกณฑ์ แนวปฏิบัติ และคู่มือปฏิบัติเกี่ยวกับ การบริหารความเสี่ยงสำหรับรัฐวิสาหกิจ

## 1. คำจำกัดความ

การบริหารความเสี่ยง คือ กระบวนการบริหารจัดการเหตุการณ์ที่อาจเกิดขึ้นและส่งผลกระทบต่อรัฐวิสาหกิจ เพื่อให้รัฐวิสาหกิจสามารถดำเนินงานให้บรรลุวัตถุประสงค์ขององค์กร รวมถึงเพื่อเพิ่มศักยภาพและขีดความสามารถให้รัฐวิสาหกิจ

## 2. หลักการพื้นฐานการบริหารความเสี่ยง

รัฐวิสาหกิจควรพัฒนากระบวนการบริหารความเสี่ยง โดยมีหลักการพื้นฐาน (Principles) อ้างอิงตาม ISO 31000 : 2018 Risk Management – Principles and Guidelines ดังนี้

หลักการ	คำอธิบาย
1. เป็นส่วนหนึ่งของกระบวนการในองค์กร (Integrated)	การบูรณาการการบริหารความเสี่ยงเข้าเป็นส่วนหนึ่งของทุกกิจกรรมในองค์กร
2. ดำเนินการอย่างเป็นระบบ มีรูปแบบที่ชัดเจนและครอบคลุม (Structured and Comprehensive)	การบริหารความเสี่ยงควรปฏิบัติอย่างเป็นระบบในหน่วยงานต่างๆ เพื่อให้การดำเนินการมีประสิทธิภาพมีความสอดคล้องกัน และมีความน่าเชื่อถือ
3. ดำเนินการบนพื้นฐานของข้อมูลที่ดีที่สุดที่มีอยู่ (Best Available Information)	การบริหารความเสี่ยงควรดำเนินการโดยพิจารณาข้อมูลจากแหล่งต่างๆ เช่น จากประสบการณ์ ข้อมูลย้อนกลับ การสังเกตการณ์ การพยากรณ์และมุมมองจากผู้เชี่ยวชาญ อย่างไรก็ตาม ผู้ทำหน้าที่ตัดสินใจความเสี่ยงจากข้อมูลนั้น ต้องคำนึงถึงข้อจำกัดของข้อมูล แบบจำลอง การตัดสินใจ รวมถึงความแตกต่างที่อาจเกิดขึ้นจากมุมมองของผู้เชี่ยวชาญต่างๆ ด้วย
4. ปรับให้เหมาะสมกับองค์กร (Customized)	การบริหารความเสี่ยงต้องสอดคล้องไปในทิศทางเดียวกันกับสภาพแวดล้อมทั้งภายในและภายนอกขององค์กร และวัตถุประสงค์ขององค์กร

หลักการ	คำอธิบาย
5. คำนึงถึงปัจจัยด้านบุคลากร และวัฒนธรรม (Human and Cultural Factors)	การบริหารความเสี่ยงควรได้รับการปฏิบัติโดยคำนึงถึงความสามารถ การยอมรับในความสำคัญ ความตั้งใจของบุคลากร และวัฒนธรรมองค์กรด้วย
6. ได้รับการมีส่วนร่วมจากผู้มีส่วนได้เสียอย่างทันเวลา (Inclusive)	การบริหารความเสี่ยงต้องการความร่วมมืออย่างเหมาะสมของผู้มีส่วนได้เสีย รวมถึงผู้ทำหน้าที่ตัดสินใจในทุกๆ ระดับขององค์กร รวมถึงการให้ผู้มีส่วนได้เสียได้รับข้อมูลอย่างเหมาะสม และการนำมุมมองและความคิดเห็นต่างๆ มาพิจารณาในการกำหนดเกณฑ์ความเสี่ยง
7. เป็นพลวัต (Dynamic)	การบริหารความเสี่ยงช่วยให้องค์กรตอบสนองต่อการเปลี่ยนแปลงต่างๆ ได้อย่างต่อเนื่อง เมื่อมีการเปลี่ยนแปลงสภาพแวดล้อมหรือเหตุการณ์ต่างๆ ทั้งภายในและภายนอกองค์กร
8. ได้รับการพัฒนาปรับปรุงอย่างต่อเนื่อง (Continual Improvement)	องค์กรจะต้องพัฒนา และมีกลยุทธ์ในการปรับปรุงการบริหารความเสี่ยงในทุกๆ ด้านอย่างต่อเนื่อง

### 3. การปฏิบัติตามหลักเกณฑ์

- 3.1 หลักเกณฑ์ แนวปฏิบัติ และคู่มือปฏิบัติเกี่ยวกับการบริหารความเสี่ยงนี้ จะไม่มีประโยชน์อันใด หากไม่มีการนำไปปฏิบัติ
- 3.2 หลักเกณฑ์ แนวปฏิบัติ และคู่มือปฏิบัติเกี่ยวกับการบริหารความเสี่ยง จัดทำขึ้นสำหรับใช้เป็นแนวปฏิบัติของรัฐบาลศึกษา โดยหวังว่าจะทำให้เกิดความคิดเบื้องต้น ซึ่งผู้เกี่ยวข้องสามารถนำไปปรับปรุงแก้ไขในการปฏิบัติให้มีความเหมาะสมกับการดำเนินงาน
- 3.3 ผู้มีส่วนได้เสียของรัฐบาลศึกษาต้องการความมั่นใจจากรัฐบาลศึกษา ด้วยการมีระบบการบริหารความเสี่ยงที่ดี ทั้งนี้ คณะกรรมการรัฐบาลศึกษา (คณะกรรมการ) และผู้บริหารต้องร่วมกันกำหนดนโยบายและกระบวนการบริหารความเสี่ยงตามบริบทของแต่ละองค์กร
- 3.4 ให้รัฐบาลศึกษาดำเนินการตามส่วนที่เป็นหลักเกณฑ์ โดยแนวปฏิบัติและคู่มือปฏิบัติเป็นส่วนที่ให้รายละเอียดหรือวิธีการดำเนินการเพิ่มเติม เพื่อให้รัฐบาลศึกษาสามารถปฏิบัติตามหลักเกณฑ์ได้ สำหรับรัฐบาลศึกษาที่เป็นบริษัทจดทะเบียนในตลาดหลักทรัพย์แห่งประเทศไทยให้ถือปฏิบัติตามหลักการบริหารความเสี่ยงของตลาดหลักทรัพย์แห่งประเทศไทยควบคู่ไปด้วย

## 4. ลำดับชั้นของการปฏิบัติ

- 4.1 ให้รัฐวิสาหกิจจัดให้มีระบบการบริหารความเสี่ยงตามหลักเกณฑ์ แนวปฏิบัติ และคู่มือปฏิบัติ และให้รัฐวิสาหกิจมีถ้อยแถลง (Statement) ไว้ในรายงานประจำปีของรัฐวิสาหกิจ ซึ่งอธิบายถึงนโยบายและกระบวนการที่คณะกรรมการได้เลือกใช้ปฏิบัติ โดยข้อมูลนี้จะใช้เป็นส่วนหนึ่งของการประเมินการบริหารความเสี่ยงในรัฐวิสาหกิจ
- 4.2 หลักเกณฑ์ แนวปฏิบัติ และคู่มือปฏิบัติจะช่วยให้รัฐวิสาหกิจสามารถยกระดับการบริหารความเสี่ยงให้ทัดเทียมกับสากลได้ รัฐวิสาหกิจควรนำหลักเกณฑ์ แนวปฏิบัติ และคู่มือปฏิบัติไปปฏิบัติให้ได้มากที่สุด โดยอาจปรับใช้ให้เหมาะสมกับบริบทของแต่ละองค์กร ทั้งนี้ สคร. อาจกำหนดให้มีการประเมินระบบการบริหารความเสี่ยงของรัฐวิสาหกิจควบคู่ไปด้วย รวมถึงการรายงานผลการบริหารความเสี่ยง

## 5. นิยามของคำสำคัญ

คำสำคัญ	ความหมาย
บริบทขององค์กร (Business Context)	เหตุการณ์ ความสัมพันธ์ รวมทั้งปัจจัยอื่นๆ ที่อาจมีอิทธิพลให้ความกระจ่าง หรือเปลี่ยนแปลงกลยุทธ์และวัตถุประสงค์ในการประกอบกิจการในปัจจุบันและในอนาคต
วัตถุประสงค์ในการประกอบกิจการ (Business Objectives)	ขั้นตอนที่องค์กรสามารถใช้วัดความสำเร็จตามกลยุทธ์
วิสัยทัศน์ (Vision)	ความมุ่งหวังขององค์กรที่จะบรรลุสถานะที่ต้องการในอนาคต หรือสิ่งที่องค์กรตั้งเป้าหมายที่จะบรรลุในอนาคต
คุณค่าหลัก (Core Values)	ความเชื่อและอุดมการณ์ขององค์กรเกี่ยวกับสิ่งที่พึงประสงค์และไม่พึงประสงค์ สิ่งที่ยอมรับได้หรือยอมรับไม่ได้ ซึ่งมีอิทธิพลต่อพฤติกรรมขององค์กร
วัฒนธรรม (Culture)	ทัศนคติ พฤติกรรม และความเข้าใจเกี่ยวกับความเสี่ยง ทั้งในแง่บวกและลบ ซึ่งมีอิทธิพลต่อการตัดสินใจของผู้บริหารและบุคลากร และสะท้อนให้เห็นถึงพันธกิจ วิสัยทัศน์และคุณค่าหลักขององค์กร
การบริหารความเสี่ยง (Enterprise Risk Management)	กระบวนการบริหารจัดการเหตุการณ์ที่อาจเกิดขึ้นและส่งผลกระทบต่อองค์กร เพื่อให้องค์กรสามารถดำเนินงานให้บรรลุวัตถุประสงค์ในการประกอบกิจการ รวมถึงเพื่อเพิ่มศักยภาพและขีดความสามารถให้องค์กร

คำสำคัญ	ความหมาย
การปฏิบัติตามกฎระเบียบ (Compliance)	เรื่องที่เกี่ยวข้องกับการปฏิบัติตามกฎหมาย กฎ ระเบียบและข้อบังคับที่เกี่ยวข้องกับองค์กร
การให้ความเชื่อมั่นอย่างสมเหตุสมผล (Reasonable Assurance)	แนวคิดที่ว่าไม่ว่าการบริหารความเสี่ยงขององค์กรจะได้รับการออกแบบมาดี หรือนำมาใช้ได้ดีเพียงใดก็ไม่สามารถรับประกันการบรรลุวัตถุประสงค์ขององค์กรได้ทั้งหมด ทั้งนี้ เนื่องจากข้อจำกัดต่างๆ ที่มีอยู่ตามธรรมชาติของการบริหารความเสี่ยงขององค์กร
ความเสี่ยง (Risk)	ความเป็นไปได้ของเหตุการณ์ที่อาจเกิดขึ้น และเป็นอุปสรรคต่อการบรรลุวัตถุประสงค์ขององค์กร
ระดับความเสี่ยงที่องค์กรยอมรับได้ (RA)	ประเภทความเสี่ยงและค่าความเสี่ยงที่กำหนดในภาพกว้าง ซึ่งองค์กรเต็มใจยอมรับสำหรับการสร้างคุณค่า
ช่วงเบี่ยงเบนของระดับความเสี่ยงที่องค์กรยอมรับได้ (Risk Tolerance : RT)	ขอบเขตความเบี่ยงเบนในผลการปฏิบัติงานที่ยอมรับได้ที่สัมพันธ์กับการบรรลุวัตถุประสงค์ใดวัตถุประสงค์หนึ่ง
ความเสี่ยงก่อนมาตรการควบคุม (Inherent Risk)	ความเสี่ยงที่มีต่อองค์กรโดยที่ฝ่ายจัดการยังไม่ได้กระทำการใดๆ เพื่อที่จะเปลี่ยนแปลงโอกาสที่จะเกิดหรือผลกระทบของความเสี่ยงนั้นๆ
ความเสี่ยงที่เหลืออยู่ (Residual Risk)	ความเสี่ยงที่เหลืออยู่หลังจากที่ฝ่ายจัดการได้ดำเนินการที่จะเปลี่ยนแปลงระดับของโอกาสที่จะเกิดหรือผลกระทบของความเสี่ยง
ความไม่แน่นอน (Uncertainty)	สถานะของการไม่ทราบว่าจะเกิดเหตุการณ์ที่อาจเกิดขึ้นนั้นจะเกิดขึ้นจริงหรือไม่ หรือเหตุการณ์ดังกล่าวจะเกิดขึ้นอย่างไร
ภาพรวมความเสี่ยง (Portfolio View)	การวิเคราะห์ความเสี่ยงที่องค์กรเผชิญอยู่ ซึ่งทำให้ผู้บริหารและคณะกรรมการสามารถพิจารณาความรุนแรง และความเกี่ยวข้องกันของความเสี่ยงกับปัจจัยต่างๆ ที่อาจมีผลกระทบต่อผลการปฏิบัติงาน กลยุทธ์และวัตถุประสงค์ในการประกอบกิจการ
ผลกระทบ (Impact)	ผลที่ตามมาหรือผลของความเสี่ยง โดยความเสี่ยงหนึ่งอาจมีผลกระทบที่เป็นไปได้หลากหลาย ผลกระทบของความเสี่ยงอาจเป็นผลในเชิงบวกหรือเชิงลบต่อกลยุทธ์หรือวัตถุประสงค์ในการประกอบกิจการ

คำสำคัญ	ความหมาย
โอกาสที่จะเกิดหรือ ความเป็นไปได้ (Likelihood)	โอกาสที่เหตุการณ์หนึ่งเหตุการณ์ใดจะเกิดขึ้น ซึ่งอาจนำเสนอ ในรูปของความน่าจะเป็นหรือความถี่ของการเกิด
หน่วยงานแนวป้องกันด่านที่ 1 (First Line of Defense)	ผู้บริหารและบุคลากรที่อยู่หน้างานเป็นด่านป้องกันด่านแรกในกิจกรรม ประจำวัน เป็นผู้รับผิดชอบในการบริหารความเสี่ยงและดูแลรักษา ประสิทธิผลของการควบคุมภายในประจำวัน
หน่วยงานแนวป้องกันด่านที่ 2 (Second Line of Defense)	หน่วยงานที่มีหน้าที่ให้คำแนะนำและแนวทางเกี่ยวกับการบริหารความเสี่ยง การควบคุมภายใน และการปฏิบัติตามมาตรฐานที่องค์กรกำหนดไว้
หน่วยงานแนวป้องกันด่านที่ 3 (Third Line of Defense)	ผู้ตรวจสอบภายในทำหน้าที่ตรวจสอบและประเมินประสิทธิภาพ ของการบริหารความเสี่ยงและการควบคุมภายใน รวมทั้งให้คำแนะนำ แก่ผู้บริหารในการปรับปรุงกระบวนการบริหารความเสี่ยงและการควบคุม ภายใน

## 6. ภาพรวมหลักเกณฑ์ แนวปฏิบัติ และคู่มือปฏิบัติ

หลักเกณฑ์ แนวปฏิบัติ และคู่มือปฏิบัติเกี่ยวกับการบริหารความเสี่ยง ประกอบด้วย 5 องค์ประกอบ ดังนี้

องค์ประกอบที่ 1 การกำกับดูแลและวัฒนธรรม (Governance and Culture)		
<b>หลักเกณฑ์</b>		
<p>รัฐวิสาหกิจควรกำหนดสภาพแวดล้อมภายในองค์กรให้สนับสนุนการบริหารความเสี่ยงทั่วทั้งองค์กร โดยสภาพแวดล้อมภายในองค์กรควรมีความเหมาะสมกับลักษณะขององค์กรนั้น ทั้งในด้านการกำกับดูแล การบริหารความเสี่ยงโดยคณะกรรมการที่เป็นผู้มีคุณสมบัติและประสบการณ์ที่เหมาะสม ด้านการกำหนด โครงสร้างองค์กร (Organization Chart) สายการรายงาน อำนาจและความรับผิดชอบที่เหมาะสม รวมถึง ด้านการสร้างวัฒนธรรมและพฤติกรรมที่องค์กรพึงประสงค์ที่สะท้อนคุณค่าหลักขององค์กร ความมุ่งมั่น ต่อการเพิ่มขีดความสามารถของบุคลากร มาตรฐานด้านบุคลากร สภาพแวดล้อมภายในองค์กรถือเป็น พื้นฐานขององค์ประกอบอื่นของการบริหารความเสี่ยง</p>		
แนวปฏิบัติ		จำนวนคู่มือปฏิบัติ
แนวปฏิบัติที่ 1	การกำหนดหน้าที่และคุณสมบัติของคณะกรรมการ	3
แนวปฏิบัติที่ 2	การกำหนดโครงสร้างองค์กรที่สนับสนุนให้เกิดการบริหาร ความเสี่ยงที่มีประสิทธิภาพ	4
แนวปฏิบัติที่ 3	การกำหนดคุณค่าหลักและพฤติกรรมที่พึงประสงค์	2
แนวปฏิบัติที่ 4	การปลูกฝังการบริหารความเสี่ยงจนเป็นวัฒนธรรมองค์กร	1
แนวปฏิบัติที่ 5	การเพิ่มขีดความสามารถของบุคลากรและการจัดสรรทรัพยากร ให้เพียงพอในการบริหารความเสี่ยง	3
รวม		13

**องค์ประกอบที่ 2 กลยุทธ์และการกำหนดวัตถุประสงค์ (Strategy and Objective Setting)**

**หลักเกณฑ์**  
 รัฐวิสาหกิจควรระบุเหตุการณ์ที่อาจเกิดขึ้นและส่งผลกระทบต่อองค์กรทั้งด้านที่เป็นโอกาสและความเสี่ยง และจะต้องมีความเข้าใจถึงปัจจัยต่างๆ ทั้งภายในและภายนอกองค์กร ทั้งเหตุการณ์ที่เคยเกิดขึ้นมาแล้วในอดีต และการคาดการณ์ในอนาคต เพื่อนำไปกำหนดวัตถุประสงค์ขององค์กรที่ชัดเจนและสอดคล้องกัน ทั้งวัตถุประสงค์ด้านกลยุทธ์และวัตถุประสงค์ด้านการดำเนินงานขององค์กร และจะต้องเป็นไปในแนวทางเดียวกันกับระดับความเสี่ยงที่องค์กรยอมรับได้ (RA)

แนวปฏิบัติ		จำนวนคู่มือปฏิบัติ
แนวปฏิบัติที่ 1	การระบุเหตุการณ์ที่อาจเกิดขึ้นและส่งผลกระทบต่อการทำงานขององค์กร	1
แนวปฏิบัติที่ 2	การกำหนดระดับความเสี่ยงที่องค์กรยอมรับได้ และช่วงเปี่ยงเบนของระดับความเสี่ยงที่องค์กรยอมรับได้	2
แนวปฏิบัติที่ 3	การเลือกกลยุทธ์ขององค์กร	1
แนวปฏิบัติที่ 4	การกำหนดวัตถุประสงค์ในการประกอบกิจการ	2
รวม		6

**องค์ประกอบที่ 3 ผลการปฏิบัติงาน (Performance)**

**หลักเกณฑ์**  
 รัฐวิสาหกิจควรมีการระบุและประเมินความเสี่ยงที่ชัดเจนและเป็นระบบ โดยการประเมินความเสี่ยงจะมีการพิจารณาทั้งด้านโอกาสที่ความเสี่ยงจะเกิดขึ้น และผลกระทบหากความเสี่ยงเกิดขึ้นจริง ช่วงระยะเวลาที่ใช้ในการประเมินความเสี่ยงควรสอดคล้องกับกลยุทธ์และวัตถุประสงค์ในการประกอบกิจการและสามารถทำการประเมินได้ตั้งแต่ระดับองค์กรไปจนถึงระดับหน่วยงาน ภายหลังจากประเมินความเสี่ยง รัฐวิสาหกิจควรมีการจัดลำดับความสำคัญของความเสี่ยงตามระดับความรุนแรงของความเสี่ยง และช่วงความเปี่ยงเบนของระดับความเสี่ยงที่องค์กรยอมรับได้ (RA) เพื่อให้สามารถจัดสรรทรัพยากรในการตอบสนองต่อความเสี่ยงได้อย่างเหมาะสม

แนวปฏิบัติ		จำนวนคู่มือปฏิบัติ
แนวปฏิบัติที่ 1	การระบุความเสี่ยงที่ชัดเจนและครอบคลุมการดำเนินงานขององค์กรและการจัดทำทะเบียนความเสี่ยง	4
แนวปฏิบัติที่ 2	การกำหนดเกณฑ์การประเมินความเสี่ยงและการประเมินความเสี่ยง	4
แนวปฏิบัติที่ 3	การจัดลำดับความสำคัญของความเสี่ยง	1
แนวปฏิบัติที่ 4	การเลือกแนวทางการตอบสนองต่อความเสี่ยง	2
แนวปฏิบัติที่ 5	การจัดทำภาพรวมความเสี่ยง	1
รวม		12

#### องค์ประกอบที่ 4 การสอบทานและการแก้ไขปรับปรุง (Review and Revision)

##### หลักเกณฑ์

รัฐวิสาหกิจควรมีการติดตามและทบทวนความรู้ความสามารถและแนวปฏิบัติในการบริหารความเสี่ยงขององค์กรอย่างสม่ำเสมอ เพื่อให้มั่นใจว่าองค์กรดำเนินการตามแนวปฏิบัติอย่างมีประสิทธิภาพตามที่ตั้งใจไว้ รวมถึงช่วยให้องค์กรสามารถระบุแนวทางการปรับปรุงการบริหารความเสี่ยง และนำไปพัฒนาประสิทธิภาพของการบริหารความเสี่ยงขององค์กรในทุกระดับ เพื่อให้สามารถปรับเปลี่ยนการบริหารความเสี่ยงหรือประยุกต์ใช้ให้เหมาะสมกับการเปลี่ยนแปลงต่างๆ ได้อย่างทันเวลา

แนวปฏิบัติ		จำนวนคู่มือปฏิบัติ
แนวปฏิบัติที่ 1	การวิเคราะห์การเปลี่ยนแปลงจากปัจจัยภายในและปัจจัยภายนอกที่อาจส่งผลให้มีการทบทวนแผนการบริหารจัดการความเสี่ยง	2
แนวปฏิบัติที่ 2	การทบทวนแผนการบริหารจัดการความเสี่ยง	1
แนวปฏิบัติที่ 3	การปรับปรุงกระบวนการบริหารความเสี่ยงขององค์กรอย่างต่อเนื่อง	1
รวม		4

#### องค์ประกอบที่ 5 สารสนเทศ การสื่อสาร และการรายงาน (Information Communication and Reporting)

##### หลักเกณฑ์

รัฐวิสาหกิจควรกำหนดให้มีสารสนเทศและการสื่อสารที่สนับสนุนการบริหารความเสี่ยง ข้อมูลสารสนเทศที่เกี่ยวข้องกับองค์กรทั้งจากแหล่งข้อมูลภายในและภายนอกองค์กรควรได้รับการบันทึกและสื่อสารอย่างเหมาะสมและทันเวลา โดยเฉพาะข้อมูลสนับสนุนที่มีความสำคัญเกี่ยวกับการระบุ การประเมิน และการตอบสนองต่อความเสี่ยง เพื่อให้องค์กรสามารถตอบสนองต่อความเสี่ยงได้อย่างรวดเร็วและมีประสิทธิภาพ รัฐวิสาหกิจควรมีการสื่อสารให้บุคลากรมีความตระหนักและเข้าใจการบริหารความเสี่ยง

แนวปฏิบัติ		จำนวนคู่มือปฏิบัติ
แนวปฏิบัติที่ 1	การบริหารสารสนเทศด้านความเสี่ยงเพื่อการจัดการที่ดี	2
แนวปฏิบัติที่ 2	การกำหนดช่องทางสื่อสารข้อมูลและสารสนเทศด้านความเสี่ยง	2
แนวปฏิบัติที่ 3	การรายงานความเสี่ยงต่อคณะกรรมการ	1
รวม		5

## 7. หลักเกณฑ์ แนวปฏิบัติ และคู่มือปฏิบัติ

### องค์ประกอบที่ 1 การกำกับดูแลและวัฒนธรรม (Governance and Culture)

#### หลักเกณฑ์

รัฐวิสาหกิจควรกำหนดสภาพแวดล้อมภายในองค์กรให้สนับสนุนการบริหารความเสี่ยงทั่วทั้งองค์กร โดยสภาพแวดล้อมภายในองค์กรควรมีความเหมาะสมกับลักษณะขององค์กรนั้น ทั้งในด้านการกำกับดูแลการบริหารความเสี่ยงโดยคณะกรรมการที่เป็นผู้มีคุณสมบัติและประสบการณ์ที่เหมาะสม ด้านการกำหนดโครงสร้างองค์กร (Organization Chart) สายการรายงาน อำนาจและความรับผิดชอบที่เหมาะสม รวมถึงด้านการสร้างวัฒนธรรมและพฤติกรรมที่องค์กรพึงประสงค์ที่สะท้อนคุณค่าหลักขององค์กร ความมุ่งมั่นต่อการเพิ่มขีดความสามารถของบุคลากร มาตรฐานด้านบุคลากร สภาพแวดล้อมภายในองค์กรถือเป็นพื้นฐานขององค์ประกอบอื่นของการบริหารความเสี่ยง

#### แนวปฏิบัติที่ 1

คณะกรรมการควรมีบทบาทในการควบคุมดูแลกลยุทธ์และกำกับดูแลการบริหารความเสี่ยงขององค์กร เพื่อสนับสนุนผู้บริหารในการดำเนินการเพื่อบรรลุกลยุทธ์และวัตถุประสงค์ในการประกอบกิจการ โดยคณะกรรมการควรมีทักษะ ความรู้ ความเชี่ยวชาญ ประสบการณ์ และความสามารถ รวมทั้งควรกำหนดให้มีการทบทวนคุณสมบัติดังกล่าวอย่างสม่ำเสมอ เพื่อให้มั่นใจว่าคณะกรรมการสามารถควบคุมดูแลความเสี่ยงขององค์กรได้อย่างมีประสิทธิภาพ รวมถึงคณะกรรมการควรมีความเป็นอิสระเพื่อทำหน้าที่ในการตรวจสอบ ถ่วงดุลการปฏิบัติงานของผู้บริหาร และเพื่อให้มั่นใจว่ารัฐวิสาหกิจบริหารงานโดยยึดผลประโยชน์สูงสุดของผู้มีส่วนได้เสียทุกฝ่าย

#### คู่มือปฏิบัติ

1. รัฐวิสาหกิจควรกำหนดบทบาทหน้าที่ของคณะกรรมการในการควบคุมดูแลกลยุทธ์และกำกับการบริหารความเสี่ยงขององค์กร และคุณสมบัติของคณะกรรมการเป็นลายลักษณ์อักษร โดยจัดทำกฎบัตรคณะกรรมการเพื่อระบุบทบาทหน้าที่ด้านการบริหารความเสี่ยงของคณะกรรมการดังต่อไปนี้
  - อนุมัตินโยบายการบริหารความเสี่ยง โดยพิจารณานำมาตรฐานการบริหารจัดการความเสี่ยงสำหรับหน่วยงานของรัฐที่กระทรวงการคลังกำหนด มาเป็นแนวทางในการบริหารจัดการความเสี่ยง และอาจพิจารณานำมาตรฐานสากลอื่นมาปฏิบัติร่วมด้วย โดยนโยบายการบริหารความเสี่ยงควรกำหนดแนวทางการบริหารความเสี่ยงให้สอดคล้องกับวัตถุประสงค์ในการประกอบกิจการเป้าหมายหลัก กลยุทธ์ และระดับความเสี่ยงที่องค์กรยอมรับได้ (RA) รวมถึงการทบทวนนโยบายการบริหารความเสี่ยงเป็นประจำอย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงอย่างมีนัยสำคัญ

- อนุมัติระดับความเสี่ยงที่องค์กรยอมรับได้ (RA) และช่วงความเบี่ยงเบนของระดับความเสี่ยงที่องค์กรยอมรับได้ (RT) โดยเชื่อมโยงกับวิสัยทัศน์ ค่านิยมหลัก และกลยุทธ์ขององค์กร รวมถึงมีการทบทวนเป็นประจำเพื่อให้มั่นใจว่าระดับความเสี่ยงที่องค์กรยอมรับได้ (RA) และช่วงความเบี่ยงเบนของระดับความเสี่ยงที่องค์กรยอมรับได้ (RT) ที่ใช้บังคับยังมีประสิทธิภาพ และเหมาะสมกับรัฐวิสาหกิจ
  - กำกับดูแลให้ผู้บริหารจัดการให้มีโครงสร้างการบริหารความเสี่ยงให้สอดคล้องกับกลยุทธ์ และวัตถุประสงค์ในการประกอบกิจการ โดยการมอบหมายอำนาจหน้าที่และการรายงานให้ชัดเจน ทั้งระดับคณะกรรมการ ฝ่ายจัดการ และระดับต่างๆ พร้อมจัดสรรบุคลากร ทรัพยากร และงบประมาณอย่างเพียงพอสำหรับการปฏิบัติงาน
  - พิจารณาให้ความเห็นชอบแผนการบริหารจัดการความเสี่ยงประจำปี และติดตามแผนดังกล่าว อย่างน้อยทุกไตรมาส พร้อมให้ข้อสังเกตและข้อเสนอแนะ โดยนำผลประเมินความเสี่ยงที่ผ่านมา เป็นข้อมูลพื้นฐานประกอบการพิจารณาเพื่อนำไปพัฒนาแผนการบริหารจัดการความเสี่ยง รวมถึงพิจารณาเรื่องความยั่งยืนเป็นส่วนหนึ่งของแผนการบริหารจัดการความเสี่ยง โดยแผนการบริหารจัดการความเสี่ยง อาจประกอบด้วยหัวข้อดังต่อไปนี้เป็นอย่างน้อย
    - วิธีการจัดการความเสี่ยง
    - ผู้รับผิดชอบในการบริหารความเสี่ยง
    - ดัชนีชี้วัดความเสี่ยงที่สำคัญ
    - วิธีการติดตามและการรายงานผล
    - ความถี่ในการรายงานผลการบริหารความเสี่ยง
  - ส่งเสริมวัฒนธรรมการบริหารความเสี่ยงโดยกำหนดแนวทางที่ชัดเจน พร้อมทั้งสร้างความตระหนัก และความรับผิดชอบให้กับพนักงานทุกระดับ ซึ่งสามารถดำเนินการได้โดยเชื่อมโยงการบริหาร ความเสี่ยงเข้ากับการประเมินผลการปฏิบัติงาน ตลอดจนกำหนดระบบรางวัลหรือแรงจูงใจที่พิจารณา จากประสิทธิภาพในการจัดการความเสี่ยง
  - กำกับและติดตามในองค์กรมีการบริหารงานแบบบูรณาการกันทั้งในด้านการกำกับดูแลกิจการ การบริหารความเสี่ยง และการปฏิบัติตามกฎระเบียบ (Governance Risk and Compliance: GRC) พร้อมมอบข้อสังเกตและข้อเสนอแนะ เพื่อนำไปเพิ่มประสิทธิภาพของการบูรณาการ ในเรื่องการกำกับดูแลกิจการ การบริหารความเสี่ยง และการปฏิบัติตามกฎระเบียบ (GRC)
2. คณะกรรมการควรมีความรู้ความเข้าใจบริบทขององค์กร มีประสบการณ์ทางธุรกิจ และเข้าใจ ความเสี่ยงที่เกี่ยวข้องเป็นอย่างดี และรัฐวิสาหกิจควรจัดให้มีการระบุความรู้ความสามารถ ด้านการบริหารความเสี่ยงเป็นสมรรถนะหลัก (Skill Matrix) ของคณะกรรมการ เพื่อใช้ประเมิน

ทักษะ ความรู้ ความเชี่ยวชาญ ประสบการณ์ ความสามารถ ระบุช่องว่างทางทักษะ (Skill Gaps) และนำมาจัดทำแผนการพัฒนาคณะกรรมการรายบุคคลประจำปี

3. คณะกรรมการควรประกอบด้วยกรรมการที่มีความเป็นอิสระในสัดส่วนที่เหมาะสม เพื่อส่งเสริมให้กรรมการสามารถแสดงความเห็นและตัดสินใจเกี่ยวกับการบริหารความเสี่ยงของมหาวิทยาลัยได้อย่างอิสระและมีความเป็นธรรม โดยยึดผลประโยชน์สูงสุดของผู้มีส่วนได้เสียทุกฝ่าย ทั้งนี้ สำหรับจำนวนและคุณสมบัติของกรรมการอิสระอย่างน้อยมหาวิทยาลัยต้องถือปฏิบัติให้เป็นไปตามแนวทางการกำกับดูแลกิจการที่ดีในมหาวิทยาลัย ตามพระราชบัญญัติการพัฒนากำกับดูแลและบริหารมหาวิทยาลัย พ.ศ. 2562 รวมถึงหลักเกณฑ์อื่นที่มหาวิทยาลัยต้องถือปฏิบัติให้เป็นไปตามกฎหมายที่เกี่ยวข้อง

## แนวปฏิบัติที่ 2

มหาวิทยาลัยควรกำหนดโครงสร้างองค์กร (Organization Chart) และออกแบบสายการรายงาน การมอบอำนาจและความรับผิดชอบที่สนับสนุนให้เกิดการบริหารความเสี่ยงที่มีประสิทธิภาพ พร้อมทั้งจัดให้มีการบูรณาการการกำกับดูแลกิจการ การบริหารความเสี่ยง และการปฏิบัติตามกฎระเบียบ เพื่อให้บรรลุกลยุทธ์และวัตถุประสงค์ในการประกอบกิจการ นอกจากนี้ ควรมีการกำหนดผู้รับผิดชอบหลักในการพัฒนาวางระบบและติดตามการบริหารความเสี่ยงขององค์กร รวมถึงกำหนดเจ้าของความเสี่ยง (Risk Owner) ที่จะต้องรับผิดชอบในการบริหารความเสี่ยงนั้นๆ

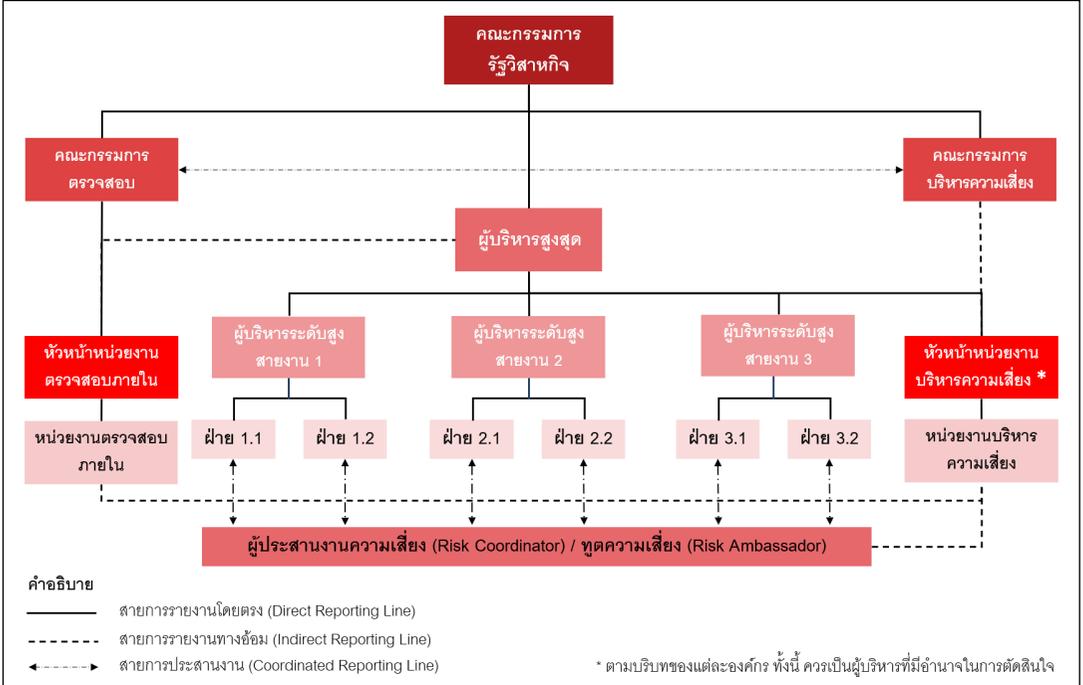
### คู่มือปฏิบัติ

1. โครงสร้างองค์กร (Organization Chart) ส่งผลกระทบต่อแนวทางการบริหารความเสี่ยงขององค์กร โดยโครงสร้างการบริหารความเสี่ยงที่ดีจะช่วยสนับสนุนให้เกิดความชัดเจนและความราบรื่นในการนำการบริหารความเสี่ยงไปปฏิบัติ ซึ่งคณะกรรมการอาจพิจารณาแต่งตั้งคณะกรรมการชุดย่อย เช่น คณะกรรมการบริหารความเสี่ยง คณะกรรมการตรวจสอบ เพื่อทำหน้าที่พิจารณาประเด็นด้านความเสี่ยง กลั่นกรองข้อมูลและให้ข้อเสนอแนะเกี่ยวกับแผนการบริหารจัดการความเสี่ยง ก่อนเสนอให้คณะกรรมการพิจารณาให้ความเห็นชอบ

คณะกรรมการบริหารความเสี่ยงและหน่วยงานบริหารความเสี่ยง เป็นกลไกสำคัญในการผลักดันการบริหารความเสี่ยง การกำหนดสายการรายงาน บทบาทหน้าที่ และความรับผิดชอบของกรรมการผู้บริหารและพนักงานทุกคน ซึ่งโครงสร้างองค์กรที่ดีและการกำหนดบทบาทหน้าที่ที่ชัดเจน จะช่วยให้ทุกส่วนงานสามารถปฏิบัติหน้าที่ตามที่ได้รับมอบหมายได้ และช่วยให้การระบุ ประเมิน จัดการ และติดตามความเสี่ยงเป็นไปอย่างมีประสิทธิภาพและทันเวลา

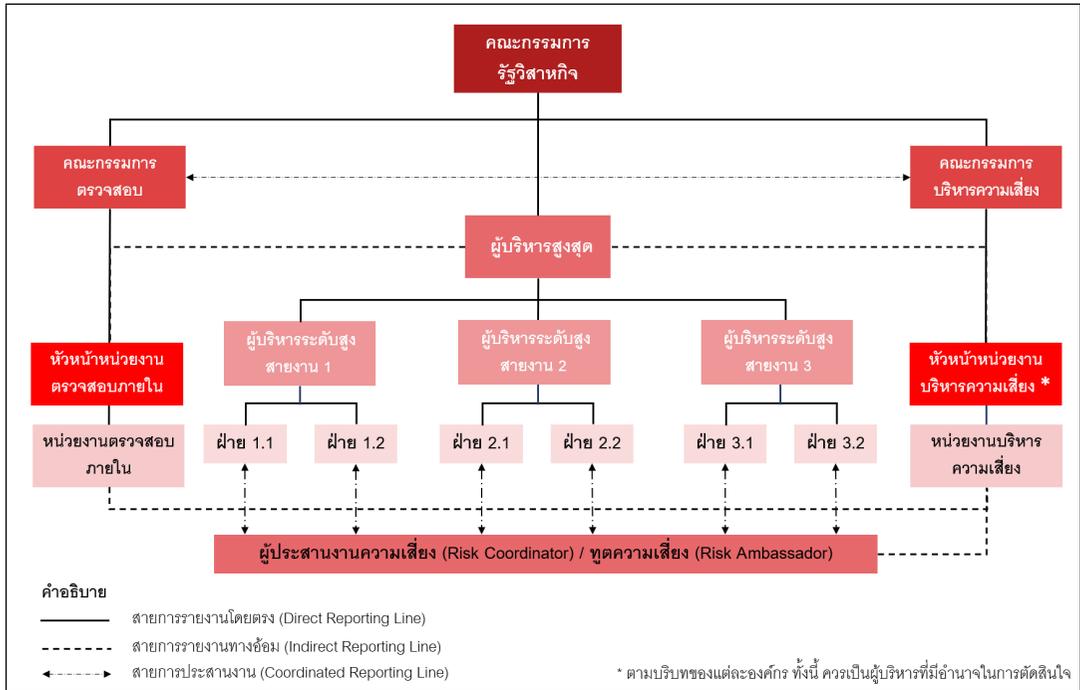
รัฐวิสาหกิจควรพิจารณากำหนดผู้รับผิดชอบในการบริหารความเสี่ยงตามความเหมาะสมของแต่ละองค์กร โดยอาจเป็นคณะบุคคลหรือหน่วยงานที่ได้รับมอบหมายให้ทำหน้าที่เกี่ยวกับการบริหารจัดการความเสี่ยงของรัฐวิสาหกิจที่อยู่ภายใต้การบริหารจัดการของผู้บริหารสูงสุด ซึ่งต้องประกอบด้วย ฝ่ายบริหารและบุคลากรที่มีความรู้ความเข้าใจเกี่ยวกับการจัดทำยุทธศาสตร์ และการบริหารจัดการความเสี่ยงของรัฐวิสาหกิจ โดยไม่ควรเป็นผู้ตรวจสอบภายในของรัฐวิสาหกิจ นอกจากนี้ รัฐวิสาหกิจควรให้ความสำคัญกับการกำหนดเจ้าของความเสี่ยง (Risk Owner) โดยเจ้าของความเสี่ยงเป็นผู้รับผิดชอบในการบริหารความเสี่ยงที่ตนเป็นเจ้าของและเป็นผู้ติดตาม เพื่อให้มั่นใจว่าแผนจัดการความเสี่ยงได้รับการนำไปปฏิบัติอย่างเหมาะสม โดยหลังจากจัดการความเสี่ยงแล้ว ควรทบทวนผลการประเมินความเสี่ยงว่าความเสี่ยงดังกล่าวอยู่ในระดับที่ยอมรับได้แล้วหรือไม่ ทั้งนี้ รัฐวิสาหกิจควรจัดทำคำพรรณาลักษณะงาน (Job Description: JD) และกำหนดโครงสร้างความรับผิดชอบในคำพรรณาลักษณะงาน (JD) รวมถึงระบุโครงสร้างความรับผิดชอบ และสายการรายงานไว้ในโครงสร้างองค์กร (Organization Chart) อย่างชัดเจน

ตัวอย่างโครงสร้างการบริหารความเสี่ยงสำหรับรัฐวิสาหกิจ  
แบบที่ 1 : โครงสร้างแบบอิสระระดับปานกลาง (Medium Level)



โครงสร้างและสายการรายงานแบบที่ 1 แสดงให้เห็นถึงโครงสร้างการบริหารความเสี่ยงที่มีความเป็นอิสระในระดับปานกลาง โดยหน่วยงานบริหารความเสี่ยงจะมีการรายงานโดยตรงต่อผู้บริหารสูงสุด

## แบบที่ 2 : โครงสร้างแบบอิสระระดับสูง (High Level)



โครงสร้างและสายการรายงานแบบที่ 2 แสดงให้เห็นถึงโครงสร้างการบริหารความเสี่ยงที่มีความเป็นอิสระในระดับสูง โดยหน่วยงานบริหารความเสี่ยงจะมีการรายงานโดยตรงต่อคณะกรรมการบริหารความเสี่ยง

ทั้งนี้ การพิจารณาโครงสร้างองค์กร (Organization Chart) และสายการรายงานขึ้นอยู่กับขนาดและความซับซ้อนขององค์กร โดยโครงสร้างและสายการรายงานแบบที่ 2 เหมาะสำหรับองค์กรที่อยู่ในสถานะที่ต้องเผชิญกับความเสี่ยงระดับสูงหลายประการ เช่น เป็นรัฐวิสาหกิจที่อยู่ระหว่างแก้ไขปัญหาองค์กร หรือรัฐวิสาหกิจที่ต้องการส่งเสริมความน่าเชื่อถือและความโปร่งใสอย่างเร่งด่วน หรือองค์กรที่ประกอบธุรกิจปกติที่มีความเสี่ยงในระดับสูงและควรต้องเน้นการบริหารความเสี่ยงเป็นพิเศษ เป็นต้น

2. รัฐวิสาหกิจควรกำหนดบทบาทและความรับผิดชอบในการบริหารความเสี่ยงขององค์กรอย่างชัดเจน และเป็นลายลักษณ์อักษร โดยพิจารณาระบุในกฎบัตร นโยบายการบริหารความเสี่ยง หรือคำพรรณนาลักษณะงาน (JD) ดังตัวอย่างต่อไปนี้

### 1) คณะกรรมการ

- คณะกรรมการมีหน้าที่กำกับดูแลการบริหารความเสี่ยงที่ฝ่ายจัดการได้ดำเนินการ โดยมุ่งเน้นให้การบริหารความเสี่ยงต้องช่วยผลักดัน ส่งเสริมให้กลยุทธ์ขององค์กรประสบความสำเร็จ ตามที่ผู้มีส่วนได้เสียคาดหวัง และช่วยให้องค์กรมีความเสี่ยงไม่สูงเกินกว่าระดับความเสี่ยง

ที่องค์กรยอมรับได้ (RA) โดยอ้างอิงรายละเอียดบทบาทและความรับผิดชอบของคณะกรรมการ  
ด้านการบริหารความเสี่ยงในองค์ประกอบที่ 1 แนวปฏิบัติที่ 1

## 2) คณะกรรมการตรวจสอบ

- สอบทานประสิทธิภาพและประสิทธิผลของกระบวนการควบคุมภายใน กระบวนการบริหารจัดการ  
ความเสี่ยง และกระบวนการกำกับดูแลที่ดี รวมถึงระบบบริหารจัดการความเสี่ยงด้านการทุจริต  
ของรัฐวิสาหกิจ และระบบการรับแจ้งเบาะแส
- กำกับดูแลและติดตามการบริหารความเสี่ยงอย่างเป็นอิสระ
- ติดตามประสิทธิภาพการทำงานของหน่วยงานตรวจสอบภายใน
- รายงานต่อคณะกรรมการและผู้ถือหุ้นเกี่ยวกับประสิทธิภาพและประสิทธิผลของการควบคุม  
ภายใน
- สื่อสารกับคณะกรรมการบริหารความเสี่ยง เพื่อให้เข้าใจความเสี่ยงที่สำคัญและเชื่อมโยง  
กับระบบการควบคุมภายใน

## 3) คณะกรรมการบริหารความเสี่ยง

- ดำเนินการตามหน้าที่ที่ได้รับมอบหมายจากคณะกรรมการ ซึ่งครอบคลุมถึง
  - การพิจารณานโยบายและกรอบการบริหารความเสี่ยง
  - การติดตามการพัฒนากรอบการบริหารความเสี่ยง
  - การติดตามกระบวนการระบุและประเมินความเสี่ยง
  - การประเมินและอนุมัติแผนการบริหารจัดการความเสี่ยง
- รายงานต่อคณะกรรมการเกี่ยวกับความเสี่ยงและการจัดการความเสี่ยง
- สื่อสารกับคณะกรรมการตรวจสอบเกี่ยวกับความเสี่ยงที่สำคัญ

## 4) ผู้บริหารสูงสุด

- สอบทานและให้ความเห็นต่อนโยบายการบริหารความเสี่ยง กรอบการบริหารความเสี่ยง  
แนวปฏิบัติการบริหารความเสี่ยง และกระบวนการบริหารความเสี่ยง เพื่อให้มั่นใจว่าสอดคล้อง  
กับกลยุทธ์และวัตถุประสงค์ในการประกอบกิจการ
- ติดตามความเสี่ยงที่สำคัญทั้งองค์กร และทำให้มั่นใจว่ามีแผนการจัดการที่เหมาะสม
- ส่งเสริมนโยบายการบริหารความเสี่ยง และทำให้มั่นใจว่ากระบวนการบริหารความเสี่ยง  
ได้รับการปฏิบัติทั่วทั้งองค์กร
- ส่งเสริมวัฒนธรรมการบริหารความเสี่ยง และทำให้มั่นใจว่าบุคลากรในแต่ละระดับ  
ให้ความสำคัญกับการบริหารความเสี่ยงตามบทบาทหน้าที่ของตน

## 5) หัวหน้าหน่วยงานบริหารความเสี่ยง

- ให้คำปรึกษาในฐานะผู้เชี่ยวชาญด้านความเสี่ยงและประสานงานเกี่ยวกับประเด็นด้านความเสี่ยง

- สอบทานนโยบายการบริหารความเสี่ยง กรอบการบริหารความเสี่ยง แนวปฏิบัติการบริหารความเสี่ยง และกระบวนการบริหารความเสี่ยง เพื่อนำเสนอต่อผู้บริหารสูงสุดและคณะกรรมการบริหารความเสี่ยงพิจารณาให้ความเห็นชอบ ก่อนนำเสนอต่อคณะกรรมการเพื่อพิจารณาอนุมัติ รวมถึงควบคุมดูแลให้มีการปฏิบัติตาม เพื่อให้บรรลุกลยุทธ์และวัตถุประสงค์ในการประกอบกิจการ
- กำกับดูแลให้มีเจ้าของความเสี่ยง (Risk Owner) ในแต่ละความเสี่ยงอย่างครบถ้วน เพื่อให้มีผู้รับผิดชอบโดยตรงต่อผลการดำเนินงานในแต่ละสายงาน
- รายงานประเด็นความเสี่ยงต่อคณะกรรมการ คณะกรรมการบริหารความเสี่ยง และผู้บริหารสูงสุด และอาจรวมถึงการอภิปรายเกี่ยวกับความเสี่ยงที่ร้ายแรงหรือความเสี่ยงใหม่ที่ยังไม่สามารถประเมินผลกระทบได้
- จัดให้มีการพัฒนาการบริหารความเสี่ยงองค์กร โดยประเมินระดับวุฒิภาวะ (Maturity) เพื่อเพิ่มประสิทธิภาพของกระบวนการบริหารความเสี่ยง

#### 6) หน่วยงานบริหารความเสี่ยง<sup>1</sup>

- จัดทำนโยบายการบริหารความเสี่ยง กรอบการบริหารความเสี่ยง แนวปฏิบัติการบริหารความเสี่ยง และกระบวนการให้กับหน่วยงาน และเสนอหัวหน้าหน่วยงานบริหารความเสี่ยงเพื่อสอบทานความเหมาะสม
- จัดทำแผนการบริหารจัดการความเสี่ยง เพื่อให้บรรลุกลยุทธ์และวัตถุประสงค์ในการประกอบกิจการ
- ติดตามประเมินผลการบริหารความเสี่ยง
- จัดทำรายงานผลตามแผนการบริหารจัดการความเสี่ยง
- พิจารณาทบทวนแผนการบริหารจัดการความเสี่ยง
- ให้การสนับสนุนและแนะนำกระบวนการบริหารความเสี่ยงแก่หน่วยงานต่างๆ ภายในองค์กร ตามที่มีการร้องขอ
- จัดให้มีการประชุมด้านความเสี่ยงเป็นประจำ อย่างน้อยทุกไตรมาส
- ศึกษาและติดตามความก้าวหน้าของแนวปฏิบัติที่ดีในการบริหารความเสี่ยง เพื่อนำมาพัฒนาและปรับปรุงนโยบายการบริหารความเสี่ยง กรอบการบริหารความเสี่ยง และแนวปฏิบัติการบริหารความเสี่ยงขององค์กรตามความเหมาะสม

<sup>1</sup> หน่วยงานบริหารความเสี่ยง หมายถึง ผู้รับผิดชอบในการบริหารความเสี่ยง อาจรวมถึงคณะบุคคลหรือหน่วยงานที่ได้รับมอบหมายให้ทำหน้าที่เกี่ยวกับการบริหารจัดการความเสี่ยงของหน่วยงานของรัฐที่อยู่ภายใต้การบริหารจัดการของหัวหน้าหน่วยงานของรัฐ อ้างอิงนิยามตามหลักเกณฑ์กระทรวงการคลังว่าด้วยมาตรฐานและหลักเกณฑ์ปฏิบัติการบริหารจัดการความเสี่ยงสำหรับหน่วยงานของรัฐ พ.ศ. 2562

- จัดให้มีช่องทางการสื่อสารเรื่องข้อมูลความเสี่ยงและระบบการบริหารความเสี่ยงที่ชัดเจน มีประสิทธิภาพ และทันเวลา รวมทั้งดำเนินการสื่อสาร ให้คำแนะนำ จัดฝึกอบรมเรื่องระบบการบริหารความเสี่ยงให้กับทุกหน่วยงาน และโครงการภายในองค์กร เพื่อสร้างวัฒนธรรมการบริหารความเสี่ยงในองค์กร
  - พัฒนา ติดตาม ปรับปรุงข้อมูลความเสี่ยงขององค์กร และรายงานข้อมูลความเสี่ยงและความคืบหน้าของการบริหารความเสี่ยงต่อคณะกรรมการบริหารความเสี่ยง
  - ประสานงานกับหน่วยงานตรวจสอบภายในเพื่อแลกเปลี่ยนความรู้และข้อมูลเกี่ยวกับความเสี่ยงที่อาจมีผลกระทบต่อรัฐวิสาหกิจ
- 7) เจ้าของความเสี่ยง (Risk Owner)
- ระบุและรายงานความเสี่ยงที่เกี่ยวข้องกับการปฏิบัติงานต่อหัวหน้าหน่วยงานและเข้าร่วมในการจัดทำแผนจัดการความเสี่ยง
  - นำส่งข้อมูลด้านความเสี่ยงให้กับหน่วยงานบริหารความเสี่ยง
  - นำแผนไปปฏิบัติและติดตามความเสี่ยงที่เกิดขึ้นในการปฏิบัติงานประจำวัน (Daily Operation) เพื่อให้เป็นไปตามแนวทางที่กำหนด
- 8) ผู้ประสานงานความเสี่ยง (Risk Coordinator) / ทูตความเสี่ยง (Risk Ambassador)
- ประสานงานระหว่างหน่วยงานและผู้บริหารระดับสูงในประเด็นความเสี่ยงและให้คำปรึกษาเกี่ยวกับแนวปฏิบัติในการบริหารความเสี่ยงให้แก่เจ้าของความเสี่ยง
  - สนับสนุนให้มีการฝึกอบรม การสื่อสาร และรับข้อมูลตอบกลับเกี่ยวกับการเปลี่ยนแปลงทางวัฒนธรรมด้านความเสี่ยง
  - รายงานประเด็นความเสี่ยงต่อหน่วยงานบริหารความเสี่ยง รวมถึงรายงานความเห็นจากเจ้าของความเสี่ยง (Risk Owner) เพื่อนำไปพัฒนาและปรับปรุงกระบวนการบริหารความเสี่ยง
- 9) ผู้ตรวจสอบภายใน
- กำหนดเป้าหมาย ทิศทาง ภารกิจงานตรวจสอบภายใน เพื่อสนับสนุนการบริหารงาน และการดำเนินงานด้านต่างๆ ของรัฐวิสาหกิจ ให้สอดคล้องกับนโยบายของรัฐวิสาหกิจ คณะกรรมการ และคณะกรรมการตรวจสอบ โดยคำนึงถึงการกำกับดูแลที่ดี ความมีประสิทธิภาพของกิจกรรมการบริหารความเสี่ยงและความเพียงพอของการควบคุมภายในของรัฐวิสาหกิจด้วย
  - สื่อสารกับหน่วยงานบริหารความเสี่ยงเพื่อทำความเข้าใจเกี่ยวกับความเสี่ยงและดำเนินการตรวจสอบภายในตามแนวความเสี่ยง (Risk Based Auditing)
  - รายงานผลการตรวจสอบต่อผู้บริหารสูงสุดและคณะกรรมการตรวจสอบ อย่างน้อยปีละ 1 ครั้ง โดยครอบคลุมเรื่องการบริหารความเสี่ยงและการควบคุมภายในดังต่อไปนี้
    - ความเสี่ยงที่สำคัญเกี่ยวกับการดำเนินงานของรัฐวิสาหกิจ

- ความเห็นเกี่ยวกับประสิทธิผลของการบริหารจัดการความเสี่ยง และการบริหารจัดการความเสี่ยงด้านการทุจริต รวมถึงระบบการร้องเรียน (Whistleblowing) ของรัฐวิสาหกิจ
- ความเห็นเกี่ยวกับความเพียงพอและเหมาะสมของการควบคุมภายในด้านการเงิน และกระบวนการอื่นที่พิจารณาว่ามีความเสี่ยงสูงต่อการเกิดการทุจริต

นอกจากนี้ คณะกรรมการอาจมีการแต่งตั้งคณะกรรมการชุดย่อยอื่น เช่น คณะกรรมการบริหารความยั่งยืน รวมถึงคณะกรรมการชุดย่อยที่เกี่ยวข้องกับความเสี่ยงควรมีการสื่อสารกับคณะกรรมการบริหารความเสี่ยงถึงความเสี่ยงที่สำคัญ เพื่อให้มีข้อมูลเพียงพอในการกำกับดูแลการบริหารความเสี่ยง และครอบคลุมความเสี่ยงทุกด้าน

3. รัฐวิสาหกิจควรทบทวนโครงสร้างองค์กร (Organization Chart) สายการรายงาน และบทบาทหน้าที่ในการบริหารความเสี่ยงองค์กร อย่างน้อยปีละ 1 ครั้ง เพื่อให้มั่นใจว่าโครงสร้างองค์กรสนับสนุนให้บรรลุกลยุทธ์และวัตถุประสงค์ในการประกอบกิจการ และสอดคล้องกับสถานการณ์การเปลี่ยนแปลงในปัจจุบัน เช่น การเปลี่ยนแปลงด้านเทคโนโลยีสารสนเทศที่มีการพัฒนาตลอดเวลา ในกรณีที่พบว่าการดำเนินงานไม่เป็นไปตามแผนการปฏิบัติงานหรือดัชนีชี้วัดของหน่วยงาน โดยสาเหตุเกิดจากโครงสร้างองค์กรและบทบาทหน้าที่ที่ไม่เหมาะสม ทำให้การตัดสินใจในการบริหารความเสี่ยงล่าช้า ซึ่งรัฐวิสาหกิจควรนำข้อมูลดังกล่าวไปประกอบการพิจารณาปรับปรุงโครงสร้างองค์กร (Organization Chart) และบทบาทหน้าที่ หรือพิจารณาปรับปรุงกระบวนการกำหนดโครงสร้างองค์กร (Organization Chart) และบทบาทหน้าที่ในลำดับถัดไป
4. รัฐวิสาหกิจควรจัดให้มีการบูรณาการในเรื่องการกำกับดูแลกิจการ การบริหารความเสี่ยงและการปฏิบัติตามกฎระเบียบ (GRC) ซึ่งสามารถทำให้เกิดขึ้นได้โดยการสร้างความเข้าใจในสิ่งที่กรรมการ ผู้บริหาร และพนักงานแต่ละคนต้องปฏิบัติ ผ่านการจัดทำเป็นนโยบายและสื่อสารไปยังบุคลากรและหน่วยงานที่เกี่ยวข้อง เพื่อให้ทุกคนเข้าใจและสามารถปฏิบัติเป็นส่วนหนึ่งของการดำเนินงานตามความรับผิดชอบของตน โดยนโยบายการบูรณาการในเรื่องการกำกับดูแลกิจการ การบริหารความเสี่ยง และการปฏิบัติตามกฎระเบียบ (GRC) ควรสอดคล้องกับนโยบายอื่นที่เกี่ยวข้อง เช่น นโยบายการบริหารความเสี่ยง ทั้งนี้ ควรกำหนดให้มีการทบทวนนโยบายดังกล่าวอย่างสม่ำเสมอ อย่างน้อยปีละ 1 ครั้ง

#### **ความหมายของการบูรณาการในเรื่องการกำกับดูแลกิจการ การบริหารความเสี่ยง และการปฏิบัติตามกฎระเบียบ (GRC)**

การบูรณาการในเรื่องการกำกับดูแลกิจการ การบริหารความเสี่ยง และการปฏิบัติตามกฎระเบียบ (GRC) คือ การจัดให้มีบุคลากรที่มีความรู้และคุณสมบัติเหมาะสม (People) ขั้นตอนการทำงานที่โปร่งใส และมีการควบคุมภายในที่ดี (Process) การบริหารจัดการข้อมูลให้ถูกต้อง เหมาะสม ทันเวลา (Information) และการใช้เทคโนโลยีอย่างมีประสิทธิภาพ (Technology) เพื่อช่วยให้องค์กรมีการกำกับ

ดูแลกิจการที่ดี มีการบริหารความเสี่ยงอย่างเป็นระบบ และสามารถปฏิบัติตามกฎระเบียบที่เกี่ยวข้องได้อย่างครบถ้วน ทั้งนี้ เพื่อช่วยเพิ่มความมั่นใจว่าองค์กรจะสามารถบรรลุวัตถุประสงค์หรือเป้าหมายที่ตั้งไว้ได้อย่างสมเหตุสมผล

**การบูรณาการในเรื่องการกำกับดูแลกิจการ การบริหารความเสี่ยง และการปฏิบัติตามกฎระเบียบ (GRC) ให้เป็นส่วนหนึ่งของการดำเนินงาน (Integrated GRC) ประกอบด้วย**

- การมีวิสัยทัศน์ที่ถูกต้องในเรื่องการกำกับดูแลกิจการ (Governance: G) ซึ่งหมายถึง การมอบหมายอำนาจหน้าที่และความรับผิดชอบระหว่างคณะกรรมการ และผู้บริหาร รวมถึงการออกแบบกระบวนการปฏิบัติงานและการกำหนดโครงสร้างองค์กร (Organization Chart) ที่เหมาะสมเพื่อให้คณะกรรมการ และผู้บริหาร สามารถสั่งการ บริหารจัดการองค์กร และตัดสินใจในเรื่องสำคัญต่างๆ เพื่อให้มั่นใจว่าองค์กรมีผลการดำเนินงานตามเป้าหมายที่กำหนด เพิ่มคุณค่าต่อผู้ถือหุ้น และเป็นไปตามความคาดหวังของผู้มีส่วนได้เสียทุกกลุ่ม
- การบริหารความเสี่ยงถูกรวมเข้าเป็นส่วนหนึ่งของการดำเนินงานขององค์กร (Risk: R) มีการคำนึงถึงการบริหารความเสี่ยงประกอบการตัดสินใจ และการวางแผนกลยุทธ์
- การให้ความสำคัญต่อเรื่องการปฏิบัติตามกฎระเบียบ (Compliance: C) กล่าวคือ องค์กรมีความตระหนักว่าการปฏิบัติตามกฎระเบียบเป็นผลลัพธ์ที่ต้องการให้เกิดขึ้น มิได้เป็นเพียงหน้าที่ของหน่วยงานใดหน่วยงานหนึ่งเท่านั้น ซึ่งกฎระเบียบดังกล่าวอาจอยู่ในรูปของนโยบาย ขั้นตอนการทำงานที่กำหนดขึ้นภายในองค์กร และกฎหมายหรือระเบียบที่กำหนดขึ้นโดยหน่วยงานภายนอก และต้องมีความสอดคล้องกับความคาดหวังของผู้มีส่วนได้เสียด้วย

ทั้งนี้ การบูรณาการในเรื่องการกำกับดูแลกิจการ การบริหารความเสี่ยง และการปฏิบัติตามกฎระเบียบ (GRC) ครอบคลุมถึงการบูรณาการกับด้านอื่นๆ ทั้งการกำหนดกลยุทธ์ (Strategy & Performance) การรักษาความปลอดภัยและการบริหารความต่อเนื่อง (Security & Continuity) และการตรวจสอบภายใน (Audit & Assurance) เพื่อให้รัฐวิสาหกิจบรรลุวัตถุประสงค์หรือเป้าหมายที่ตั้งไว้ รัฐวิสาหกิจควรกำหนดกลยุทธ์ โดยคำนึงถึงระดับความเสี่ยงที่องค์กรยอมรับได้ (RA) และช่วงเบี่ยงเบนของระดับความเสี่ยงที่องค์กรยอมรับได้ (RT) มีการมอบหมายอำนาจหน้าที่และความรับผิดชอบให้แก่ผู้บริหารและพนักงานในระดับต่างๆ อย่างเหมาะสม กำหนดนโยบาย และมาตรฐานในการปฏิบัติงาน (Policies & Standards) ที่มีความชัดเจน รัดกุม และสอดคล้องกับกลยุทธ์ของรัฐวิสาหกิจ โดยมีการประเมินความเสี่ยงและการควบคุมภายในอย่างเพียงพอ หากความเสี่ยงใดสูงกว่าระดับที่ยอมรับได้ ก็จัดให้มีการบริหารจัดการ หากการควบคุมใดมีจุดอ่อนก็จัดให้มีการปรับปรุงการควบคุมนั้น นอกจากนี้ ยังต้องมีการติดตามประเมินผลเพื่อให้มั่นใจว่าความเสี่ยงได้รับการจัดการตามแผนที่กำหนด และมีการปรับปรุงการควบคุมให้มีประสิทธิภาพและประสิทธิผล โดยจัดให้มีการสอบทานอย่างสม่ำเสมอ ทั้งจากหน่วยงานแนวป้องกันด้านที่ 2 และหน่วยงานแนวป้องกันด้านที่ 3 (Second

and Third Line of Defense) และให้หน่วยงานที่ดูแลรับผิดชอบเกี่ยวกับการกำกับดูแลกิจการ การบริหารความเสี่ยง และการปฏิบัติตามกฎระเบียบ (GRC) รายงานประเด็นที่สำคัญ ให้คณะกรรมการและผู้บริหารระดับสูงได้รับทราบ และจัดให้มีการสื่อสารและให้ความรู้แก่พนักงาน ทุกระดับ กิจกรรมที่กล่าวมาข้างต้นนี้ จะช่วยส่งเสริมการบูรณาการในเรื่องการกำกับดูแลกิจการ การบริหารความเสี่ยง และการปฏิบัติตามกฎระเบียบ (GRC) ภายในรัฐวิสาหกิจ โดยสามารถ ดำเนินการผ่านองค์ประกอบ 4 ด้าน ได้แก่ การบริหารจัดการบุคลากร (People) การจัดให้มีกระบวนการ ปฏิบัติงานที่เหมาะสม (Process) การบริหารจัดการข้อมูล (Information) และการนำเทคโนโลยีมาใช้ (Technology)

### **ประโยชน์ของการบูรณาการในเรื่องการกำกับดูแลกิจการ การบริหารความเสี่ยง และการปฏิบัติตามกฎระเบียบ (GRC)**

- กำหนดวัตถุประสงค์ในการประกอบกิจการเพื่อให้สอดคล้องกับมูลค่าและความเสี่ยงที่เกี่ยวข้องได้อย่างมีประสิทธิภาพยิ่งขึ้น รวมถึงช่วยให้บรรลุวัตถุประสงค์ในการประกอบกิจการตามที่กำหนด และสามารถเพิ่มประสิทธิภาพในการเฝ้าระวังความเสี่ยง และปกป้องคุณค่าขององค์กร (Value)
- รักษาชื่อเสียงขององค์กรและคุณค่าของตราสินค้า (Reputation and Brand Value)
- สอดคล้องกับความคาดหวังที่เพิ่มขึ้นของผู้มีส่วนได้เสีย ได้แก่ ผู้ถือหุ้น หน่วยงานกำกับดูแล ลูกค้า/ผู้บริโภคน คู่ค้า พนักงาน และประชาชนทั่วไป เป็นต้น
- สร้างคุณค่าแก่องค์กรด้วยการดำเนินงานตามหลักจรรยาบรรณและการกำกับดูแลกิจการที่ดี
- กำหนดแนวทางและการควบคุมเพื่อป้องกัน ตรวจสอบ ปรับปรุงและลดผลกระทบเชิงลบ จากเหตุการณ์ต่างๆ ได้อย่างมีประสิทธิภาพมากยิ่งขึ้น
- ส่งเสริมให้เกิดความร่วมมือในองค์กร โดยหน่วยงานต่างๆ มีการแบ่งปันความรู้และข้อมูลที่เกี่ยวข้องกับการกำกับดูแลกิจการ การบริหารความเสี่ยง และการปฏิบัติตามกฎระเบียบ (GRC) ระหว่างกัน เพื่อช่วยลดความซ้ำซ้อนของงาน
- ช่วยให้องค์กรมีการตัดสินใจที่มีประสิทธิภาพและแม่นยำขึ้น อันเนื่องมาจากข้อมูลด้านการกำกับดูแลกิจการ การบริหารความเสี่ยง และการปฏิบัติตามกฎระเบียบ (GRC) ถูกบูรณาการร่วมกัน องค์กรจึงสามารถบริหารความเสี่ยงและตัดสินใจได้ผ่านการวิเคราะห์ข้อมูลด้านดังกล่าวในเชิงลึก
- ช่วยเตรียมความพร้อมในการดำเนินงานภายใต้ภาวะวิกฤติ โดยรวมถึงการบริหารจัดการในกรณีที่ถูกฟ้องร้องดำเนินคดี การเรียกร้องค่าปรับหรือค่าเสียหาย การถูกลงโทษและการดำเนินงานหยุดชะงัก
- ส่งเสริมการวัดผลของกระบวนการดำเนินงานอย่างมีประสิทธิภาพ

## แนวปฏิบัติเพื่อส่งเสริมให้รัฐวิสาหกิจมีการบูรณาการในเรื่องการกำกับดูแลกิจการ การบริหารความเสี่ยง และการปฏิบัติตามกฎระเบียบ (GRC)

### 1) บุคลากร (People)

- กำหนดบทบาทหน้าที่ของคณะกรรมการและหน่วยงานที่เกี่ยวข้องกับการบูรณาการในเรื่องการกำกับดูแลกิจการ การบริหารความเสี่ยง และการปฏิบัติตามกฎระเบียบ (GRC) อย่างชัดเจน และจัดให้มีการรายงานต่อคณะกรรมการถึงการดำเนินงานของรัฐวิสาหกิจว่าเป็นไปตามหลักการของการบูรณาการในเรื่องการกำกับดูแลกิจการ การบริหารความเสี่ยง และการปฏิบัติตามกฎระเบียบ (GRC) หรือไม่ อย่างสม่ำเสมอ
- จัดให้มีการสื่อสารเรื่องความสำคัญของการบูรณาการในเรื่องการกำกับดูแลกิจการ การบริหารความเสี่ยง และการปฏิบัติตามกฎระเบียบ (GRC) จากกรรมการและผู้บริหารระดับสูงถึงพนักงานทุกระดับอย่างทั่วถึง
- จัดให้มีการเผยแพร่ความรู้ความเข้าใจหรือฝึกอบรมเกี่ยวกับการบูรณาการในเรื่องการกำกับดูแลกิจการ การบริหารความเสี่ยง และการปฏิบัติตามกฎระเบียบ (GRC) ให้แก่กรรมการ ผู้บริหาร และพนักงานทุกระดับ เพื่อให้มั่นใจว่าบุคลากรมีความเข้าใจเกี่ยวกับการบูรณาการในเรื่องการกำกับดูแลกิจการ การบริหารความเสี่ยง และการปฏิบัติตามกฎระเบียบ (GRC) เป็นอย่างดี และสามารถนำแนวปฏิบัติดังกล่าวไปปรับใช้กับการดำเนินงานของตนเองได้อย่างมีประสิทธิภาพ
- สร้างจิตสำนึกในการปฏิบัติตามหลักจรรยาบรรณและจัดให้มีการติดตามการปฏิบัติตามหลักจรรยาบรรณอย่างสม่ำเสมอ เพื่อสร้างวัฒนธรรมด้านการบูรณาการในเรื่องการกำกับดูแลกิจการ การบริหารความเสี่ยง และการปฏิบัติตามกฎระเบียบ (GRC) และความรู้ดีกมีส่วนร่วมในการปฏิบัติตามแนวทางการบูรณาการในเรื่องการกำกับดูแลกิจการ การบริหารความเสี่ยง และการปฏิบัติตามกฎระเบียบ (GRC) ให้เกิดขึ้นภายในรัฐวิสาหกิจ

### 2) การจัดให้มีกระบวนการปฏิบัติงานที่เหมาะสม (Process)

- กำหนดนโยบายและวิธีการปฏิบัติงาน (Policies & Procedures) เกี่ยวกับการบูรณาการในเรื่องการกำกับดูแลกิจการ การบริหารความเสี่ยง และการปฏิบัติตามกฎระเบียบ (GRC) ที่ชัดเจน โดยคำนึงถึงประสิทธิภาพในการทำงานที่มีความครอบคลุมและมีการบูรณาการอย่างเหมาะสม โดยไม่มีกระบวนการทำงานที่ซ้ำซ้อนกัน ควบคู่กับการจัดให้มีการควบคุมภายในที่ตีความระดับความเสี่ยงที่องค์กรยอมรับได้ (RA) ของงานนั้นๆ

### 3) การบริหารจัดการข้อมูล (Information)

- กำหนดคำนิยาม (Taxonomy) และใช้ชุดข้อมูลเดียวกัน เพื่อทำให้มั่นใจว่าข้อมูลที่นำมาใช้นั้น มีความครบถ้วน ถูกต้อง และทันเวลา

- ข้อมูลเกี่ยวกับการบูรณาการในเรื่องการกำกับดูแลกิจการ การบริหารความเสี่ยง และการปฏิบัติตามกฎระเบียบ (GRC) มีการบันทึกและสื่อสารอย่างเหมาะสม เช่น รายงานเหตุการณ์ ความสูญเสีย ข้อมูลสนับสนุนสำหรับประเมินความเสี่ยงและการควบคุมภายใน การบันทึกเหตุการณ์การทุจริต การบันทึกเหตุการณ์การละเมิดกฎระเบียบ รวมถึงการจัดให้มีช่องทางในการสื่อสารข้อมูลเกี่ยวกับการบูรณาการในเรื่องการกำกับดูแลกิจการ การบริหารความเสี่ยง และการปฏิบัติตามกฎระเบียบ (GRC) ภายในองค์กร และกำหนดระดับในการเข้าถึงข้อมูลต่างๆ อย่างเหมาะสม
- กำหนดรูปแบบของการรายงานและข้อมูลที่นำมาใช้ในการรายงานให้มีความเหมาะสมกับความต้องการของผู้ใช้ เช่น ข้อมูลสำหรับผู้บริหารระดับสูงมีความกระชับ สรุปลงเฉพาะประเด็นที่สำคัญที่ต้องใช้ในการตัดสินใจ อาจมีแผนภาพประกอบที่ช่วยให้เข้าใจได้ง่ายหรือจัดทำในรูปแบบแผนแสดงหน้าจอดีชบอร์ด (Dashboard) ในขณะที่ข้อมูลสำหรับหน่วยงานที่มีหน้าที่ในการวิเคราะห์อาจอยู่ในรูปแบบของข้อมูลดิบที่มีความละเอียดมากกว่า เพื่อให้สามารถนำไปวิเคราะห์ในมุมมองต่างๆ ได้ตามความต้องการ

#### 4) การนำเทคโนโลยีมาใช้ (Technology)

โดยทั่วไป รัฐวิสาหกิจที่ต้องใช้ข้อมูลในการบริหารจัดการองค์กรเป็นจำนวนมากได้นำเทคโนโลยีมาใช้เป็นเครื่องมือสนับสนุนการดำเนินงานของรัฐวิสาหกิจ ดังนั้น การบูรณาการในเรื่องการกำกับดูแลกิจการ การบริหารความเสี่ยง และการปฏิบัติตามกฎระเบียบ (GRC) ก็เช่นเดียวกัน รัฐวิสาหกิจควรพิจารณาว่าระบบข้อมูลสารสนเทศและเทคโนโลยีต่างๆ ที่สามารถนำมาสนับสนุนงานด้านการบูรณาการในเรื่องการกำกับดูแลกิจการ การบริหารความเสี่ยง และการปฏิบัติตามกฎระเบียบ (GRC) ได้อย่างเหมาะสมเพียงใด และต้องมีการปรับปรุงระบบเดิมหรือจัดหาระบบใหม่หรือไม่ โดยพิจารณาในประเด็นดังต่อไปนี้

- (1) การนำเทคโนโลยีมาใช้เพื่อช่วยในการจัดทำรายงานสำหรับกรรมการและผู้บริหาร รวมถึงหน่วยงานต่างๆ ทั้งภายในและภายนอกวิสาหกิจ เพื่อส่งเสริมการกำกับดูแลกิจการที่ดี
- (2) การนำเทคโนโลยีมาใช้เพื่อช่วยในการระบุ ประเมิน จัดการ และติดตามความเสี่ยงได้อย่างครอบคลุมและทันเวลา รวมถึงการออกแบบระบบเตือนภัยล่วงหน้า (Early Warning) เช่น กำหนดให้มีระบบแจ้งเตือนไปยังเจ้าของความเสี่ยง (Risk Owner) และหน่วยงานบริหารความเสี่ยง เมื่อมีความเสี่ยงสูงเกินกว่าช่วงเบี่ยงเบนของระดับความเสี่ยงที่องค์กรยอมรับได้ (RT)
- (3) การนำเทคโนโลยีมาใช้เพื่อช่วยให้การปฏิบัติงานเป็นไปตามนโยบายและวิธีการปฏิบัติงาน (Policies & Procedures) ที่กำหนด รวมถึงช่วยให้การปฏิบัติงานเป็นไปตามกฎระเบียบทั้งภายในและภายนอกองค์กร

- (4) การนำเทคโนโลยีมาใช้เพื่อช่วยออกแบบการควบคุมภายในให้มีประสิทธิภาพและประสิทธิผลมากขึ้น เช่น การแบ่งแยกหน้าที่ การอนุมัติรายการ การเข้าถึงฐานข้อมูล การกระหนาบยอด
- (5) การนำเทคโนโลยีมาใช้เพื่อช่วยในการติดตามประเมินผลการดำเนินงานของรัฐวิสาหกิจเปรียบเทียบกับเป้าหมายที่ตั้งไว้
- (6) การนำเทคโนโลยีมาใช้เพื่อช่วยให้ข้อมูลมีความครบถ้วน ถูกต้อง และทันเวลา มากยิ่งขึ้น

### การบูรณาการการบริหารความเสี่ยงกับองค์ประกอบอื่น ๆ

#### ตัวอย่างการบูรณาการการบริหารความเสี่ยงกับองค์ประกอบอื่น ๆ ได้แก่

- **การกำกับดูแลกิจการ**

- กำหนดโครงสร้างที่ครอบคลุมและเหมาะสมในการกำกับดูแลและติดตามการบริหารความเสี่ยง
- ในการพิจารณากำหนดกลยุทธ์ หรือนโยบายต่างๆ ควรมีการพิจารณาประเด็นความเสี่ยงขององค์กรร่วมด้วย
- กรณีที่พบข้อบกพร่องที่เกิดจากการกำกับดูแล ควรมีการแจ้งหน่วยงานที่เกี่ยวข้องเพื่อทำการทบทวนโครงสร้างองค์กร (Organization Chart) หรือแนวปฏิบัติอย่างทันเวลา

- **การปฏิบัติตามกฎระเบียบ**

- ใช้เกณฑ์การวัดระดับความเสี่ยงชุดเดียวกัน
- เชื่อมโยงกฎหมาย กฎระเบียบที่เกี่ยวข้องกับความเสี่ยงในทะเบียนความเสี่ยง เพื่อใช้ในการติดตามได้อย่างทันเวลา
- ในการประเมินผลกระทบของกฎหมายใหม่หรือกฎหมายที่มีการเปลี่ยนแปลงควรมีการใช้เกณฑ์การวัดผลกระทบและความเป็นไปได้ชุดเดียวกัน และหน่วยงานบริหารความเสี่ยงควรได้รับผลการประเมินเพื่อนำไปพิจารณาความเสี่ยงระดับองค์กรในลำดับถัดไป

- **การควบคุมภายใน**

- ใช้เกณฑ์การวัดระดับความเสี่ยงชุดเดียวกัน
- สื่อสารผลการประเมินความเสี่ยง และผลการประเมินประสิทธิภาพของการควบคุมภายในร่วมกันเพื่อใช้ในการพิจารณาความเสี่ยงขององค์กร
- เชื่อมโยงกิจกรรมการควบคุมภายในกับความเสี่ยงในทะเบียนความเสี่ยง เพื่อใช้ในการติดตามได้อย่างทันเวลา

- **การรักษาความปลอดภัยและการบริหารความต่อเนื่อง**

- สื่อสารผลการประเมินความเสี่ยงให้หน่วยงานหรือคณะทำงานที่รับผิดชอบด้านการรักษาความปลอดภัยและการบริหารความต่อเนื่องรับทราบ เพื่อใช้ในการพิจารณาการจัดทำและซักซ้อมแผนบริหารความต่อเนื่อง

- การตรวจสอบภายใน

- สื่อสารผลการประเมินความเสี่ยงและผลการตรวจสอบภายในร่วมกัน เพื่อใช้ในการพิจารณาความเสี่ยงขององค์กร โดยหน่วยงานตรวจสอบภายในสามารถนำข้อมูลไปใช้ในการพิจารณาวางแผนการตรวจสอบ
- ใช้ Risk Universe และเกณฑ์การวัดระดับความเสี่ยงชุดเดียวกัน

### การวัดความสำเร็จของการบูรณาการในเรื่องการกำกับดูแลกิจการ การบริหารความเสี่ยง และการปฏิบัติตามกฎระเบียบ (GRC)

ตัวอย่างดัชนีชี้วัดความสำเร็จของการบูรณาการในเรื่องการกำกับดูแลกิจการ การบริหารความเสี่ยง และการปฏิบัติตามกฎระเบียบ (GRC) ได้แก่

- ค่าใช้จ่ายที่ประหยัดได้จากการลดกิจกรรมเกี่ยวกับการปฏิบัติตามกฎระเบียบที่ซ้ำซ้อนกัน หรือที่มีมากเกินไปจนความจำเป็น
- จำนวนครั้งของการละเมิดข้อกำหนดในนโยบายและขั้นตอนการปฏิบัติงานต่างๆ
- ระยะเวลาที่คณะกรรมการได้อุทิสให้กับการกำกับดูแลเรื่องการบริหารความเสี่ยงและการปฏิบัติตามกฎระเบียบ
- อัตราการเข้าร่วมกิจกรรมที่เกี่ยวข้องกับการบูรณาการในเรื่องการกำกับดูแลกิจการ การบริหารความเสี่ยง และการปฏิบัติตามกฎระเบียบ (GRC)
- ผลการประเมินความเข้าใจของบุคลากรในด้านการบูรณาการในเรื่องการกำกับดูแลกิจการ การบริหารความเสี่ยง และการปฏิบัติตามกฎระเบียบ (GRC)

## แนวปฏิบัติที่ 3

รัฐวิสาหกิจควรกำหนดคุณค่าหลัก (Core Value) และพฤติกรรมที่พึงประสงค์ (Desired Behavior) รวมถึงแสดงให้เห็นถึงการยึดมั่นต่อคุณค่าหลักขององค์กร อันเป็นพื้นฐานสำคัญของการบริหารความเสี่ยง โดยผู้บริหารปฏิบัติเป็นแบบอย่าง นอกจากนี้ รัฐวิสาหกิจควรกำหนดนโยบายการบริหารความเสี่ยง (Risk Management Policy) ที่เป็นลายลักษณ์อักษร เพื่อแสดงถึงความมุ่งมั่นในการให้ความสำคัญกับการบริหารความเสี่ยงในองค์กร

### คู่มือปฏิบัติ

1. รัฐวิสาหกิจควรกำหนดคุณค่าหลัก (Core Value) อันแสดงถึงความเชื่อและอุดมการณ์เกี่ยวกับการบริหารความเสี่ยงที่บุคลากรทุกคนในองค์กรต้องมีร่วมกันอย่างเป็นลายลักษณ์อักษร จากนั้นผู้บริหารระดับสูงสื่อสารคุณค่าหลักขององค์กรไปยังพนักงาน เพื่อนำไปปฏิบัติจนสะท้อนผ่านการกระทำ

และการตัดสินใจในการปฏิบัติงานประจำวันที่เป็นไปในทิศทางเดียวกันทั่วทั้งองค์กรหรือที่เรียกว่า พฤติกรรมที่พึงประสงค์ (Desired Behavior) จนเกิดเป็นวัฒนธรรมองค์กร

นอกจากการนำการบริหารความเสี่ยงไปปฏิบัติตามคุณค่าหลัก (Core Value) และวัฒนธรรมองค์กร รัฐวิสาหกิจควรให้ความสำคัญกับความซื่อสัตย์ จริยธรรม และจรรยาบรรณในการประกอบกิจการ (Code of Conduct) ขององค์กร โดยเฉพาะอย่างยิ่ง จรรยาบรรณในระดับผู้บริหาร เนื่องจาก เป็นผู้กำหนดแนวปฏิบัติ และมีอำนาจในการตัดสินใจในส่วนอื่นๆ

การส่งเสริมวัฒนธรรมองค์กรที่ให้ความสำคัญกับความซื่อสัตย์ จริยธรรม และจรรยาบรรณ สามารถทำได้ด้วยการสื่อสาร เช่น การจัดทำหลักการ การแถลงการณ์ว่าองค์กรได้ให้ความสำคัญกับเรื่องจริยธรรมและจรรยาบรรณ การจัดทำ “จรรยาบรรณในการประกอบกิจการ (Code of Conduct)” อย่างเป็นลายลักษณ์อักษร โดยการจัดทำจรรยาบรรณนี้ควรแสดงถึงความเชื่อมโยงระหว่างพันธกิจ วิสัยทัศน์องค์กรกับนโยบายและขั้นตอนการปฏิบัติงาน

ตัวอย่างหัวข้อที่ควรมีในจรรยาบรรณในการประกอบกิจการ (Code of Conduct) อ้างอิงหัวข้อตามแนวปฏิบัติด้านการกำกับดูแลกิจการที่ดี เรื่อง การจัดทำจรรยาบรรณธุรกิจ (Code of Conduct) ของตลาดหลักทรัพย์แห่งประเทศไทย

- 1) สาระจากประธานกรรมการ
  - สาระจากประธานกรรมการที่สื่อให้พนักงานทุกระดับตระหนักว่า ผู้นำองค์กรให้ความสำคัญและจริงจังกับการปฏิบัติหน้าที่อย่างมีจรรยาบรรณ และคาดหวังให้พนักงานมีส่วนร่วมในการปฏิบัติตามจรรยาบรรณที่กำหนด
- 2) วิสัยทัศน์ พันธกิจ และค่านิยมขององค์กร
  - คณะกรรมการควรให้ทิศทางที่ชัดเจนว่าจรรยาบรรณที่กำหนดขึ้นสอดคล้องกับวิสัยทัศน์ พันธกิจ และค่านิยมขององค์กร เพื่อให้พนักงานใช้เป็นหลักในการพิจารณาความเหมาะสมของการปฏิบัติที่อาจเสี่ยงต่อการขัดหรือผิดต่อจรรยาบรรณองค์กร ซึ่งบางครั้งอาจไม่ได้กำหนดไว้เป็นการเฉพาะ
- 3) ข้อพึงปฏิบัติ
  - กำหนดหัวข้อตามการจัดการองค์กร เช่น
    - การต่อต้านการทุจริตคอร์รัปชัน
    - การป้องกันความขัดแย้งทางผลประโยชน์และการใช้ข้อมูลภายใน
    - การเปิดเผยข้อมูล
    - การรักษาความปลอดภัยของข้อมูลสารสนเทศ
    - การรักษาความลับทางธุรกิจและปกป้องทรัพย์สินทางปัญญา

- การรับแจ้งเบาะแสและข้อร้องเรียน
- การกำกับดูแลบริษัทย่อยและบริษัทร่วม
- ประเด็นสำคัญด้านความยั่งยืนของธุรกิจ เช่น นวัตกรรม สิทธิมนุษยชน การดูแลรักษาสิ่งแวดล้อม
- ความรับผิดชอบต่อผู้มีส่วนได้เสีย (Stakeholders) เช่น
  - การปฏิบัติและความรับผิดชอบต่อผู้ถือหุ้น
  - การปฏิบัติและความรับผิดชอบต่อภาครัฐ
  - การปฏิบัติและความรับผิดชอบต่อพนักงาน
  - การปฏิบัติและความรับผิดชอบต่อลูกค้า
  - การปฏิบัติและความรับผิดชอบต่อลูกค้า
  - การปฏิบัติและความรับผิดชอบต่อเจ้าหน้าที่
  - การปฏิบัติและความรับผิดชอบต่อคู่แข่ง
  - การปฏิบัติและความรับผิดชอบต่อสังคม ชุมชน และสิ่งแวดล้อม

#### 4) การติดตามดูแลให้มีการปฏิบัติ

- กำหนดเป็นหน้าที่และความรับผิดชอบของกรรมการ ผู้บริหารและพนักงานทุกคนที่ต้องรับทราบและทำความเข้าใจ รวมถึงปฏิบัติตามจรรยาบรรณโดยเคร่งครัด
- กำหนดแนวทางยกย่องและลงโทษ เช่น การให้รางวัลแก่ผู้ปฏิบัติดี การลงโทษตามวินัยแก่ผู้กระทำผิดจรรยาบรรณ เพื่อให้มีการปฏิบัติอย่างจริงจัง
- กำหนดให้มีวิธีการถามข้อสงสัยและการรายงานในกรณีที่สงสัยว่าจะมีการฝ่าฝืนจรรยาบรรณหรือการรับข้อร้องเรียน ซึ่งอาจมีทางเลือกได้หลายช่องทาง เช่น ผู้บังคับบัญชาตามลำดับชั้น กรรมการตรวจสอบ ไปรษณีย์อิเล็กทรอนิกส์ (Email) หรือผ่านช่องทางเว็บไซต์ภายในองค์กร
- กำหนดสายการรายงานการติดตามดูแลให้มีการปฏิบัติ เช่น หน่วยงานที่ดูแลรับข้อร้องเรียน รายงานตรงต่อคณะกรรมการตรวจสอบ หรือคณะกรรมการวินัยและจรรยาบรรณ ซึ่งอาจประกอบด้วยคณะผู้บริหารระดับสูง นำโดยผู้บริหารระดับสูงที่ดูแลด้านกฎหมาย และรายงานต่อคณะกรรมการตรวจสอบอีกชั้นหนึ่ง
- กำหนดรอบระยะเวลาที่จะให้มีการทบทวนจรรยาบรรณ เช่น ทุกปี เพื่อให้มีความเหมาะสมกับสภาพการณ์ หรือสภาพแวดล้อมทางธุรกิจที่อาจเปลี่ยนแปลงไป

ภายหลังจากการจัดทำจรรยาบรรณในการประกอบกิจการ (Code of Conduct) รัฐวิสาหกิจควรสื่อสารให้ผู้บริหารและพนักงานทุกฝ่ายในองค์กร และบุคคลทั่วไปได้รับทราบ โดยวิธีการสื่อสารอาจทำได้โดยเผยแพร่บนเว็บไซต์ขององค์กร การตีพิมพ์ประกาศ การจัดทำแผ่นพับ หรือจัดทำคู่มือฉบับพกพา (Booklet) การจัดฝึกอบรม เป็นต้น

ทั้งนี้ ควรกำหนดให้มีหลักฐานการลงนามเพื่อรับทราบและถือปฏิบัติ (Acknowledgement) เพื่อให้มั่นใจว่าพนักงานทุกคนเข้าใจและปฏิบัติตามแนวทางจรรยาบรรณในการประกอบกิจการ (Code of Conduct) ขององค์กรอย่างเคร่งครัด โดยอาจพิจารณาให้ลงนามเมื่อเข้าทำงานใหม่ เมื่อมีการปรับปรุงหรือเปลี่ยนแปลงจรรยาบรรณในการประกอบกิจการ (Code of Conduct)

นอกจากนี้ ควรกำหนดให้มีการทบทวนจรรยาบรรณในการประกอบกิจการ (Code of Conduct) อย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงอย่างมีนัยสำคัญ เพื่อความเหมาะสมกับการดำเนินธุรกิจขององค์กร

### ตัวอย่างจรรยาบรรณในการประกอบกิจการ (Code of Conduct)

#### สารจากประธานกรรมการ

[ระบุชื่อรัฐวิสาหกิจ] จะยึดมั่นในแนวทางการกำกับดูแลกิจการที่ดี ตั้งอยู่บนพื้นฐานของความรับผิดชอบต่อความโปร่งใส ตรวจสอบได้ เป็นธรรม มีจรรยาบรรณและคำนึงถึงผู้มีส่วนได้เสียทุกฝ่าย โดยคณะกรรมการผู้บริหาร และพนักงาน [ระบุชื่อรัฐวิสาหกิจ] จะยึดถือเป็นแนวทางในการปฏิบัติงาน

#### วิสัยทัศน์

[ระบุวิสัยทัศน์ของรัฐวิสาหกิจ]

#### พันธกิจ

[ระบุพันธกิจของรัฐวิสาหกิจ]

#### ค่านิยม

[ระบุค่านิยมของรัฐวิสาหกิจ]

#### ข้อพึงปฏิบัติ

##### 1. การจัดการองค์กร

###### 1.1 ความขัดแย้งทางผลประโยชน์

คณะกรรมการ ผู้บริหาร และพนักงานพึงหลีกเลี่ยงการกระทำใดๆ อันเป็นการขัดต่อผลประโยชน์ขององค์กร ไม่ว่าจะเกิดจากการติดต่อกับผู้เกี่ยวข้องทางการค้า เช่น คู่ค้า ลูกค้า คู่แข่งขัน หรือจากการใช้โอกาสหรือข้อมูลที่ได้จากการเป็นคณะกรรมการ ผู้บริหาร และพนักงาน ในการหาประโยชน์ส่วนตน

###### 1.2 การรักษาและการใช้ทรัพย์สินขององค์กร

คณะกรรมการ ผู้บริหาร และพนักงานมีหน้าที่และความรับผิดชอบในการดูแลทรัพย์สินขององค์กรมิให้เสื่อมเสีย สูญหาย และใช้ทรัพย์สินอย่างมีประสิทธิภาพให้เกิดประโยชน์ต่อองค์กรอย่างเต็มที่ และไม่นำทรัพย์สินขององค์กรไปใช้เพื่อประโยชน์ของตนเองหรือผู้อื่น

## 2. การปฏิบัติต่อตนเอง

- 2.1 ดำรงตนตั้งมั่นอยู่ในความซื่อสัตย์ สุจริต เทียงธรรม และมีจริยธรรมในการดำเนินงาน
- 2.2 ปฏิบัติหน้าที่ด้วยความรับผิดชอบ รอบคอบ พุ่มเทำกำลังกายและกำลังความคิดในการทำงาน โดยถือประโยชน์ขององค์กรเป็นสำคัญ
- 2.3 ปฏิบัติหน้าที่ด้วยความขยันหมั่นเพียร รวมทั้งแสวงหาแนวทางในการพัฒนาและปรับปรุงงานให้มีประสิทธิภาพอยู่เสมอ
- 2.4 รักษาเกียรติของตนให้เป็นที่ยอมรับในสังคม
- 2.5 เป็นผู้มีความวินัยและประพฤติปฏิบัติตามกฎระเบียบขององค์กร ค่านิยมขององค์กรและประเพณีอันดีงามไม่ว่าจะระบุไว้เป็นลายลักษณ์อักษรหรือไม่ก็ตาม
- 2.6 หลีกเลี่ยงการกระทำใดๆ อันอาจกระทบต่อชื่อเสียงและภาพลักษณ์ขององค์กรหรือเป็นปัญหาแก่องค์กรในภายหลังได้
- 2.7 ไม่ใช้เวลาปฏิบัติงานขององค์กรไปทำงานอื่น หรือใช้เพื่อประโยชน์ส่วนตนที่ส่งผลให้ไม่สามารถปฏิบัติงานได้อย่างเต็มที่
- 2.8 เสริมสร้างการทำงานเป็นทีมโดยให้ความร่วมมือช่วยเหลือเกื้อกูลซึ่งกันและกันเพื่อประโยชน์ต่องานขององค์กรโดยส่วนรวม
- 2.9 ไม่ใช้ข้อมูลที่ได้รับจากการปฏิบัติหน้าที่เพื่อแสวงหาผลประโยชน์ให้แก่ตนเองหรือผู้อื่นโดยมิชอบ
- 2.10 ห้ามรับสิ่งของหรือผลประโยชน์อื่นใดจากบุคคลอื่นที่มีหน้าที่หรือธุรกรรมเกี่ยวข้องกับองค์กร เว้นแต่ในโอกาสหรือเทศกาลอันเป็นประเพณีนิยมที่คนทั่วไปพึงปฏิบัติต่อกัน
- 2.11 การรับสิ่งของหรือประโยชน์อื่นใดที่ให้แก่กัน ในกิจกรรมต่างๆ ระหว่างองค์กรหรือเป็นการเชื่อมสัมพันธ์ไมตรีระหว่างองค์กร ให้ผู้รับรายงานผู้บังคับบัญชาของตนทราบและส่งมอบให้หน่วยงานที่เกี่ยวข้องเพื่อใช้ในกิจการขององค์กรภายใน 7 วัน

## 3. การปฏิบัติต่อผู้มีส่วนได้เสีย

- 3.1 การปฏิบัติต่อภาครัฐ
  - 3.1.1 ปฏิบัติตามกฎหมาย และระเบียบข้อบังคับต่างๆ ที่ภาครัฐกำหนดอย่างเคร่งครัด
  - 3.1.2 ให้ความสำคัญในการมีส่วนร่วมในกิจกรรมของภาครัฐ เพื่อร่วมเสริมสร้างความมั่นคงและความเจริญเติบโตทางเศรษฐกิจ รวมถึงสร้างความสัมพันธ์อันดีในขอบเขตที่เหมาะสม
  - 3.1.3 ปฏิบัติงานด้วยความโปร่งใสและตรงไปตรงมาในการติดต่อหรือทำธุรกรรมกับภาครัฐ
- 3.2 การปฏิบัติต่อพนักงาน
  - 3.2.1 ปฏิบัติตามกฎหมาย และระเบียบข้อบังคับต่างๆ ที่เกี่ยวข้องกับพนักงานอย่างเคร่งครัด

3.2.2 การแต่งตั้ง และการโยกย้าย รวมทั้งการให้รางวัลและการลงโทษพนักงานต้องกระทำด้วยความเสมอภาค สุจริตใจ และตั้งอยู่บนพื้นฐานของความรู้ ความสามารถ และความเหมาะสม รวมทั้งการกระทำ หรือการปฏิบัติของพนักงานนั้นๆ

3.2.3 รับฟังข้อคิดเห็น และข้อเสนอแนะจากพนักงานทุกระดับอย่างเท่าเทียมและเสมอภาค

3.3 การปฏิบัติต่อลูกค้า

3.3.1 อำนวยความสะดวกและปฏิบัติต่อผู้มาติดต่อด้วยความสุภาพเรียบร้อยอย่างเต็มใจ และเต็มความสามารถ โดยไม่ชักช้า

3.3.2 ให้ความสำคัญในการรักษาข้อมูลที่เป็นความลับของลูกค้าอย่างจริงจังและสม่ำเสมอ และไม่นำข้อมูลดังกล่าวมาใช้เพื่อผลประโยชน์ของตนเองและผู้เกี่ยวข้อง

3.3.3 ไม่เรียก ไม่รับ หรือไม่ให้ผลประโยชน์ใดๆ ที่ไม่สุจริตกับลูกค้า

3.4 การปฏิบัติต่อสังคม ชุมชน และสิ่งแวดล้อม

3.4.1 ให้ความร่วมมือ และควบคุมให้มีการปฏิบัติตามอย่างเคร่งครัดตามเจตนารมณ์ของกฎหมาย และกฎระเบียบที่เกี่ยวข้อง

3.4.2 ปลูกฝังจิตสำนึกความรับผิดชอบต่อสังคม และสิ่งแวดล้อมให้เกิดขึ้นในพนักงานทุกระดับอย่างต่อเนื่อง

3.4.3 ให้ความสำคัญในการมีส่วนร่วม และสร้างความสัมพันธ์อันดีให้เกิดขึ้นระหว่างองค์กร และสังคมบนพื้นฐานของความถูกต้อง โปร่งใส เป็นธรรม เพื่อร่วมสร้างองค์ความรู้ และนำไปสู่การพัฒนาสังคมอย่างยั่งยืน

4. การติดตามดูแลให้มีการปฏิบัติ

จรรยาบรรณในการประกอบกิจการ (Code of Conduct) ฉบับนี้ เป็นการประมวลแนวปฏิบัติที่ดี เพื่อกำหนดขอบเขตการประพฤติปฏิบัติที่ได้มาตรฐานภายใต้กรอบของจริยธรรมและคุณธรรม ใช้บังคับกับคณะกรรมการ ผู้บริหาร และพนักงานทุกระดับขององค์กร โดยถือเป็นข้อบังคับที่ต้องปฏิบัติตามอย่างเคร่งครัด ไม่ใช้การปฏิบัติตามความสมัครใจ และไม่สามารถอ้างความไม่รู้ เป็นข้อยกเว้นได้ ไม่ว่าบุคคลดังกล่าวจะได้ลงนามรับทราบหรือไม่ก็ตาม โดยหากพบกรณีไม่ปฏิบัติตามจะพิจารณาบทลงโทษตามกฎหมาย ระเบียบ และข้อบังคับขององค์กร

ทั้งนี้ จรรยาบรรณในการประกอบกิจการ (Code of Conduct) นี้ ถือเป็นส่วนเพิ่มเติมจากระเบียบข้อบังคับ ประกาศหรือคำสั่งอื่นๆ ขององค์กร และในกรณีที่มีความขัดแย้ง ให้ยึดข้อความในจรรยาบรรณนี้เป็นหลัก องค์กรได้ดำเนินการเผยแพร่จรรยาบรรณในการประกอบกิจการ (Code of Conduct) แก่คณะกรรมการ ผู้บริหาร และพนักงานใหม่ในวันปฐมนิเทศ รวมถึงเผยแพร่ในระบบ Intranet และเว็บไซต์ขององค์กร เพื่อให้สามารถเข้าถึงและศึกษาได้โดยสะดวก

คณะกรรมการและผู้บริหารมีหน้าที่สอดส่อง ดูแล และให้คำแนะนำแก่ผู้ได้บังคับบัญชา เพื่อส่งเสริมความเข้าใจและการปฏิบัติตามจรรยาบรรณในการประกอบกิจการ (Code of Conduct) อย่างต่อเนื่อง และเคร่งครัด รวมถึงหน่วยงานที่ดูแลรับข้อร้องเรียนมีหน้าที่ในการติดตามให้มีการปฏิบัติและรายงานตรงต่อคณะกรรมการตรวจสอบ

จรรยาบรรณในการประกอบกิจการ (Code of Conduct) จะถูกทบทวนทุก 1 ปี หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญเกิดขึ้น หากบุคลากรเกิดความสงสัย สามารถติดต่อสอบถามได้ที่ช่องทางที่องค์กรกำหนดหรือติดต่อผู้บังคับบัญชาหน่วยงานของตน

ทั้งนี้ นอกจากรัฐวิสาหกิจจะได้อำนาจจรรยาบรรณในการประกอบกิจการ (Code of Conduct) รัฐวิสาหกิจควรกำหนดข้อห้ามและบทลงโทษเป็นลายลักษณ์อักษร เช่น ข้อห้ามฝ่ายบริหารและพนักงานมิให้ปฏิบัติตนในลักษณะที่ก่อให้เกิดความขัดแย้งทางผลประโยชน์กับองค์กร หรือข้อห้ามพนักงานในลักษณะที่มีผลประโยชน์ทับซ้อน (Conflict of Interest)

**Conflict of Interest** หมายถึง การที่บุคลากรในองค์กรไม่ได้ทำหน้าที่ให้เกิดผลลัพธ์หรือผลประโยชน์ตรงตามวัตถุประสงค์ขององค์กร แต่เอื้อผลประโยชน์ให้ตนเองหรือบุคคลอื่นจนทำให้องค์กรไม่ได้รับผลประโยชน์เต็มที่หรืออาจได้รับความเสียหาย เช่น พนักงานขององค์กรที่เกี่ยวข้องในหน้าที่นั้นเข้าไปเป็นคู่สัญญาหรือมีส่วนได้เสียในสัญญา หรือเป็นหุ้นส่วนหรือผู้ถือหุ้นในห้างหุ้นส่วนหรือบริษัทที่เข้าเป็นคู่สัญญากับองค์กร ดังนั้น ฝ่ายบริหารควรกำหนดข้อห้ามเกี่ยวกับผลประโยชน์ทับซ้อนดังกล่าวไว้ในข้อกำหนดด้านจริยธรรม โดยฝ่ายบริหารและพนักงานทุกคนในองค์กรต้องหลีกเลี่ยงสถานการณ์ที่อาจก่อให้เกิดผลประโยชน์ทับซ้อนด้วย

2. คณะกรรมการควรพิจารณากำหนดให้มโนนโยบายการบริหารความเสี่ยงให้เป็นไปตามพันธกิจ วิสัยทัศน์ และคุณค่าหลัก (Core Value) ขององค์กร

การจัดทำ**นโยบายการบริหารความเสี่ยง** (Risk Management Policy) รัฐวิสาหกิจควรพิจารณาให้ครอบคลุมหัวข้อ ดังต่อไปนี้

- 1) วัตถุประสงค์ของนโยบาย
- 2) คำจำกัดความของความเสี่ยง
- 3) หลักสำคัญในการปฏิบัติ
- 4) บทบาทและความรับผิดชอบ
- 5) การทบทวนนโยบายการบริหารความเสี่ยง

## ตัวอย่างนโยบายการบริหารความเสี่ยง

## นโยบายการบริหารความเสี่ยง

## วัตถุประสงค์ของนโยบาย

เพื่อให้ [ระบุชื่อรัฐวิสาหกิจ] สามารถใช้การบริหารความเสี่ยงในการบริหารจัดการองค์กรให้บรรลุตามเป้าหมายการดำเนินงาน สร้างมูลค่าเพิ่มและความมั่นคงเพื่อประโยชน์สูงสุดของผู้มีส่วนได้เสีย และสอดคล้องตามหลักการกำกับดูแลกิจการที่ดี (Good Corporate Governance)

นโยบายนี้มีผลบังคับใช้กับกรรมการ ผู้บริหาร และพนักงานทุกคนใน [ระบุชื่อรัฐวิสาหกิจ] โดยจัดทำขึ้นจากการพิจารณาให้มีความสอดคล้องกับแผนวิสาหกิจ แผนปฏิบัติการประจำปี และแผนงานโครงการรวมทั้งกฎหมายและกฎระเบียบต่างๆ ที่เกี่ยวข้องกับการดำเนินงานขององค์กร

## คำจำกัดความของ “ความเสี่ยง”

ความเสี่ยง (Risk) คือ ความเป็นไปได้ของเหตุการณ์ที่อาจเกิดขึ้น และเป็นอุปสรรคต่อการบรรลุวัตถุประสงค์ขององค์กร

## หลักสำคัญในการปฏิบัติ

1. รักษาสมดุลระหว่างระดับความเสี่ยง (Risk) และผลตอบแทน (Return) เพื่อให้มั่นใจถึงการบรรลุตามเป้าหมายจากการดำเนินงาน ความคาดหวังของผู้มีส่วนได้เสีย และประโยชน์สูงสุดแก่ผู้ถือหุ้นภายใต้ความเสี่ยงในระดับที่องค์กรยอมรับได้ (RA)
2. กลยุทธ์การดำเนินงานต้องสอดคล้องกับระดับความเสี่ยงที่คณะกรรมการพิจารณาอนุมัติ
3. การบริหารความเสี่ยงเป็นหนึ่งในวัฒนธรรมที่สำคัญขององค์กรที่จำเป็นต้องดำเนินการอย่างมีประสิทธิภาพและประสิทธิผลโดยผู้บริหารและพนักงานทุกคน
4. คณะกรรมการบริหารความเสี่ยง ผู้บริหาร และพนักงาน ควรทบทวนความเสี่ยงเป็นประจำ รวมถึงอภิปรายและทบทวนสถานการณ์เกี่ยวกับความเสี่ยง ก่อนการตัดสินใจทางธุรกิจที่สำคัญ
5. ความเสี่ยงที่อาจส่งผลกระทบต่อการบรรลุวัตถุประสงค์และกลยุทธ์ของ [ระบุชื่อรัฐวิสาหกิจ] จะต้องได้รับการจัดการอย่างทันเวลาและต่อเนื่อง ดังนี้
  - 1) ต้องมีการระบุความเสี่ยงอย่างครอบคลุมและทันเวลา
  - 2) ต้องมีการประเมินความเสี่ยงในด้านของความเป็นไปได้ที่เหตุการณ์นั้นจะเกิดขึ้น (Likelihood) และผลกระทบ (Impact) หากความเสี่ยงนั้นเกิดขึ้น
  - 3) ต้องมีการจัดการความเสี่ยงให้อยู่ในระดับที่คณะกรรมการและผู้บริหารยอมรับได้ ทั้งนี้ ต้องมีการพิจารณาความเหมาะสมของต้นทุน และผลลัพธ์ที่จะเกิดขึ้นควบคู่กันไปด้วย
  - 4) ต้องมีการติดตามและรายงานความเสี่ยงอย่างสม่ำเสมอ เพื่อให้สามารถบริหารความเสี่ยงของ [ระบุชื่อรัฐวิสาหกิจ] ได้อย่างเหมาะสมและทันเวลา

### **บทบาทและความรับผิดชอบ**

1. คณะกรรมการเป็นผู้พิจารณาและอนุมัตินโยบายการบริหารความเสี่ยง รวมถึงกำกับดูแลและสนับสนุนการนำนโยบายการบริหารความเสี่ยงนี้ไปปฏิบัติใน [ระบุชื่อรัฐวิสาหกิจ] ผ่านทางคณะกรรมการบริหารความเสี่ยงและผู้บริหารสูงสุดของ [ระบุชื่อรัฐวิสาหกิจ]
2. คณะกรรมการบริหารความเสี่ยง เป็นผู้กำกับดูแลการนำนโยบายและกรอบการบริหารความเสี่ยงไปปฏิบัติภายในองค์กร ติดตามกระบวนการบริหารความเสี่ยง และรายงานให้คณะกรรมการทราบเป็นระยะ
3. ผู้บริหารสูงสุด เป็นผู้รับผิดชอบในการนำนโยบายการบริหารความเสี่ยงไปปฏิบัติ และติดตามการนำไปใช้อย่างต่อเนื่อง โดยได้รับการสนับสนุนจากคณะกรรมการบริหารความเสี่ยง
4. หน่วยงานบริหารความเสี่ยง เป็นผู้จัดทำนโยบายการบริหารความเสี่ยง กรอบการบริหารความเสี่ยง แนวปฏิบัติการบริหารความเสี่ยง กระบวนการบริหารความเสี่ยง และแผนการบริหารจัดการความเสี่ยง
5. ผู้ประสานงานความเสี่ยง ประสานงานระหว่างหน่วยงานและผู้บริหารระดับสูงในประเด็นความเสี่ยง
6. พนักงานทุกคนต้องรับผิดชอบในการปฏิบัติตามนโยบายและคู่มือการบริหารความเสี่ยง รวมถึงมีส่วนร่วมในการจัดทำแผนการบริหารจัดการความเสี่ยง

### **การทบทวนนโยบายการบริหารความเสี่ยง**

1. ในกรณีที่ผู้บริหารพบว่านโยบายการบริหารความเสี่ยงไม่เหมาะสมกับสภาพแวดล้อมการดำเนินงาน ต้องนำเสนอต่อคณะกรรมการ ผ่านคณะกรรมการบริหารความเสี่ยง เพื่อขออนุมัติการปรับปรุงนโยบายการบริหารความเสี่ยง
2. คณะกรรมการบริหารความเสี่ยงจะทบทวนนโยบายการบริหารความเสี่ยงทุกปี และนำเสนอต่อคณะกรรมการ ทั้งนี้ เพื่อให้มั่นใจว่านโยบายดังกล่าวยังเหมาะสมกับสภาพแวดล้อมการดำเนินงานขององค์กร

ทั้งนี้ นโยบายนี้อนุมัติโดยคณะกรรมการ และมีผลบังคับใช้กับกรรมการ ผู้บริหาร และพนักงานทุกคนตั้งแต่วันที่ ... เป็นต้นไป

อนุมัติโดย

(.....)

ประธานกรรมการ [ระบุชื่อรัฐวิสาหกิจ]

วันที่ .....

## การจัดทำคู่มือการบริหารความเสี่ยง (Risk Management Manual)

รัฐวิสาหกิจควรจัดให้มีคู่มือการบริหารความเสี่ยง เพื่อให้ทุกคนในองค์กรนำไปปฏิบัติได้และควรจัดทำเป็นลายลักษณ์อักษรและมีการเผยแพร่ให้กับพนักงานทุกระดับผ่านช่องทางที่เหมาะสม โดยรัฐวิสาหกิจจะต้องมีกระบวนการตรวจสอบความเข้าใจของผู้บริหารและพนักงานในคู่มือดังกล่าวด้วย ทั้งนี้ การจัดทำคู่มือการบริหารความเสี่ยงอาจประกอบด้วยหัวข้อต่อไปนี้

- 1) วัตถุประสงค์ของคู่มือการบริหารความเสี่ยง
- 2) นโยบายการบริหารความเสี่ยง
- 3) คำจำกัดความที่สำคัญและกรอบการบริหารความเสี่ยง
- 4) โครงสร้างและบทบาทหน้าที่ในการบริหารความเสี่ยง
  - หน่วยงานที่รับผิดชอบด้านการบริหารความเสี่ยง/การติดตามงาน/การรายงานผลการบริหารความเสี่ยง
- 5) กระบวนการบริหารความเสี่ยง
  - การระบุความเสี่ยง เป็นการพิจารณาว่ามีความเสี่ยงใดบ้างที่เกี่ยวข้องกับการดำเนินกิจการขององค์กร เช่น ความเสี่ยงทางการเงิน อาจประกอบด้วย ความเสี่ยงด้านอัตราดอกเบี้ย ความเสี่ยงด้านอัตราแลกเปลี่ยน และความเสี่ยงด้านสภาพคล่อง หรือความเสี่ยงด้านการดำเนินงาน อาจประกอบไปด้วยความเสี่ยงด้านการบริหารและการจัดการ
  - การระบุระดับความเสียหายที่อาจเกิดขึ้นได้จากความเสี่ยงแต่ละประเภท (ระดับความเสียหาย = ระดับของความรุนแรง x โอกาสของการเกิดความเสี่ยง) และมีการจัดลำดับความเสี่ยงจากผลการวิเคราะห์ความเสียหายข้างต้น
  - การกำหนด/คัดเลือกวิธีการจัดการต่อความเสี่ยง โดยพิจารณาถึงผลกระทบ (Impact) และโอกาสที่จะเกิด (Likelihood) ต้นทุนและผลประโยชน์ที่ได้รับ และระดับความเสี่ยงที่องค์กรยอมรับได้ (RA) ของความเสี่ยงที่เหลืออยู่ (Residual Risk) ขององค์กร
  - การรายงานผลตามแผนการบริหารจัดการความเสี่ยง และการติดตามประเมินผลการบริหารความเสี่ยง

## แนวปฏิบัติที่ 4

คณะกรรมการและผู้บริหารควรให้ความสำคัญกับการบริหารความเสี่ยงและส่งเสริมให้มีการปลูกฝังการบริหารความเสี่ยงให้เป็นส่วนหนึ่งของกระบวนการดำเนินการต่างๆ ตามปกติของธุรกิจ และต่อเนื่องจนเป็นวัฒนธรรมองค์กร

### คู่มือปฏิบัติ

1. เนื่องจากความตระหนักในความเสี่ยงเป็นปัจจัยสำคัญประการหนึ่งของความสำเร็จในการบริหารความเสี่ยงของธุรกิจ ผู้บริหารจึงควรกำหนดแนวทางการสร้างความตระหนักเรื่องความเสี่ยงให้กับองค์กร ครอบคลุมไปถึงการจัดให้มีบรรยากาศและวัฒนธรรมที่สนับสนุนการบริหารความเสี่ยง โดยปลูกฝังให้พนักงานทุกคนตระหนักถึงความสำคัญของการบริหารความเสี่ยงขององค์กร ซึ่งสามารถกระทำผ่านหลายวิธี เช่น
  - กำหนดคุณค่าหลัก (Core Value) และพฤติกรรมที่พึงประสงค์ พร้อมสื่อสารไปยังบุคลากรทุกระดับ
  - จัดแสดงการปฏิบัติที่ชัดเจนเกี่ยวกับนโยบายการบริหารความเสี่ยงขององค์กรและการมอบหมายอำนาจหน้าที่ที่ชัดเจน
  - สื่อสารเรื่องการบริหารความเสี่ยงไปยังบุคลากร ให้ครอบคลุมหัวข้อ ดังนี้
    - ความสำคัญและความจำเป็นของการบริหารความเสี่ยงขององค์กร
    - วัตถุประสงค์ขององค์กร
    - ระดับความเสี่ยงที่องค์กรยอมรับได้ (RA) และช่วงเบี่ยงเบนของระดับความเสี่ยงที่องค์กรยอมรับได้ (RT)
    - การใช้ภาษาเดียวกันในเรื่องการบริหารความเสี่ยง
    - บทบาทและความรับผิดชอบของบุคลากรที่จะสนับสนุนและนำองค์ประกอบต่างๆ ของการบริหารความเสี่ยงขององค์กรมาใช้ในแต่ละกระบวนการดำเนินงาน
  - สนับสนุนให้มีการหารือร่วมกัน เพื่อแบ่งปันข้อมูลการตัดสินใจที่เกี่ยวข้องกับการบริหารความเสี่ยง
  - จัดให้มีแผนการฝึกอบรมสำหรับพนักงานในองค์กร โดยให้ความสำคัญกับการฝึกอบรมผู้บริหารระดับสูง 3 ลำดับแรก โดยให้นับถัดจากผู้ว่าการ ผู้อำนวยการ กรรมการผู้จัดการใหญ่ กรรมการผู้อำนวยการใหญ่ หรือบุคคลซึ่งดำรงตำแหน่งผู้บริหารสูงสุดในรัฐวิสาหกิจนั้น และเจ้าของความเสี่ยง (Risk Owner) หรือจัดหาเครื่องมือเพื่อสนับสนุนให้บุคลากรเห็นความสำคัญและยอมรับในการบริหารความเสี่ยงขององค์กร เพื่อให้มั่นใจว่าบุคลากรมีความรู้ความสามารถในการบริหารความเสี่ยง



## แนวปฏิบัติเพื่อการต่อยอด

ปัจจัยการสร้างวัฒนธรรมด้านความเสี่ยงที่สำคัญมี 4 ด้าน ดังนี้

- 1) ผู้นำปฏิบัติเป็นแบบอย่างและสนับสนุนให้มีการบริหารความเสี่ยง (Tone at the Top and Leadership)
  - กำหนดวัฒนธรรมองค์กรที่ดี โดยส่งเสริมให้มีการหารือและแลกเปลี่ยนความคิดเห็นอย่างโปร่งใส รวมถึงจัดอบรมให้บุคลากรทุกระดับ
  - สื่อสารคุณค่าหลัก (Core Value) ขององค์กร นโยบายการบริหารความเสี่ยง กรอบการบริหารความเสี่ยง และแนวทางปฏิบัติในการบริหารความเสี่ยงเพื่อสนับสนุนให้มีพฤติกรรมที่พึงประสงค์ให้กับบุคลากรทุกระดับ
  - ปฏิบัติตนเป็นแบบอย่างที่ดี ให้สอดคล้องกับพฤติกรรมที่พึงประสงค์และส่งเสริมให้เกิดวัฒนธรรมความเสี่ยงที่ถูกต้องขององค์กร
  - กำกับดูแลการบริหารความเสี่ยง โดยเฉพาะอย่างยิ่งการติดตามประเด็นต่างๆ ที่เกี่ยวข้องกับความเสี่ยงและการควบคุมภายใน
- 2) ความรับผิดชอบต่อความเสี่ยง (Accountability for Risks)
  - กำหนดบทบาทหน้าที่ของผู้รับผิดชอบในการบริหารความเสี่ยงอย่างชัดเจน พร้อมสื่อสารไปยังบุคลากรทุกคน ให้ตระหนักถึงหน้าที่ของตนในการบริหารความเสี่ยง
  - กำหนดบทลงโทษ พร้อมสื่อสารผลกระทบ กรณีที่บุคลากรไม่ปฏิบัติตามบทบาทหน้าที่ในการบริหารความเสี่ยงของตน
- 3) การสื่อสารและการแลกเปลี่ยนความคิดเห็นให้เกิดการถ่วงดุลอย่างมีประสิทธิภาพ (Effective Communication Challenge and Diversity)
  - เปิดโอกาสให้มีการแลกเปลี่ยนความคิดเห็นประเด็นด้านการบริหารความเสี่ยง วัฒนธรรมความเสี่ยง และพฤติกรรมที่พึงประสงค์ เช่น แสดงความคิดเห็นผ่านการประชุมเกี่ยวกับการบริหารความเสี่ยงและจัดให้มีช่องทางมารับฟังความคิดเห็นจากบุคลากรในองค์กร เป็นต้น
- 4) การสร้างแรงจูงใจ และการบริหารจัดการทรัพยากรบุคคล (Incentives and HR Practices)
  - กำหนดให้มีดัชนีชี้วัดผลการดำเนินงาน (KPI) ที่สอดคล้องกับระดับความเสี่ยงที่องค์กรยอมรับได้ (RA) พร้อมกำหนดแรงจูงใจที่อาจอยู่ในรูปค่าตอบแทน การเลื่อนตำแหน่ง การให้ค่าชมเชย การดักเตือน การลงโทษ หรือรูปแบบอื่น เพื่อเป็นเครื่องมือสร้างพฤติกรรมที่มุ่งหวังหรือลดทอนพฤติกรรมที่ไม่พึงประสงค์ของพนักงาน



ทั้งนี้ รัฐวิสาหกิจควรสำรวจทัศนคติของพนักงานที่มีต่อการบริหารความเสี่ยงและการควบคุมภายในขององค์กร เพื่อนำผลการสำรวจไปจัดทำแผนปรับปรุงและพัฒนากระบวนการดังกล่าว จากนั้นรายงานผลการสำรวจทัศนคติของพนักงานต่อผู้บริหารในสายงานที่เกี่ยวข้องต่อไป ซึ่งการประเมินทัศนคติของพนักงานในเรื่องปัจจัยที่ส่งเสริมพฤติกรรมในการสร้างวัฒนธรรมองค์กร สามารถปฏิบัติได้ผ่านการจัดทำแบบสำรวจความคิดเห็นของบุคลากร โดยการตั้งคำถามให้สอดคล้องกับปัจจัยการสร้างวัฒนธรรม ทั้ง 4 ด้าน ดังตัวอย่างต่อไปนี้

**ด้านที่ 1 : ผู้นำปฏิบัติเป็นแบบอย่างและสนับสนุนให้มีการบริหารความเสี่ยง (Tone at the Top and Leadership)**

- ผู้บริหารสูงสุดและผู้บริหารระดับสูงเป็นแบบอย่างที่ดีให้กับบุคลากรในเรื่องวัฒนธรรมความเสี่ยงมากน้อยเพียงใด
- ผู้บริหารสูงสุดและผู้บริหารระดับสูงสนับสนุนให้มีการฝึกอบรมให้พนักงานตระหนักถึงการบริหารความเสี่ยงมากน้อยเพียงใด
- ผู้บริหารสูงสุดและผู้บริหารระดับสูงส่งเสริมให้มีการหารือและแลกเปลี่ยนความคิดเห็นอย่างโปร่งใสมากน้อยเพียงใด

**ด้านที่ 2 : ความรับผิดชอบต่อความเสี่ยง (Accountability for Risks)**

- บุคลากรได้รับการสื่อสารบทบาทหน้าที่ของตนเองในการบริหารความเสี่ยงอย่างชัดเจนหรือไม่เพียงใด
- บุคลากรตระหนักถึงผลกระทบจากการไม่ปฏิบัติตามพฤติกรรมที่พึงประสงค์ขององค์กรหรือไม่
- บุคลากรได้รับการอบรมอย่างเพียงพอเพื่อเพิ่มความรู้ความเข้าใจเกี่ยวกับการปฏิบัติงานที่เกี่ยวข้องกับการบริหารความเสี่ยงมากน้อยเพียงใด

**ด้านที่ 3 : การสื่อสารและการแลกเปลี่ยนความคิดเห็นให้เกิดการถ่วงดุลอย่างมีประสิทธิภาพ (Effective Communication Challenge and Diversity)**

- บุคลากรมีความมั่นใจเพียงใดในการพูดถึงการกระทำผิด การแสดงความคิดเห็นเกี่ยวกับข้อกังวล และการให้ข้อเสนอแนะที่สร้างสรรค์
- บุคลากรได้เรียนรู้จากสิ่งที่ผิดพลาดจากการบริหารความเสี่ยงที่เกิดขึ้นในองค์กร พร้อมทราบบแผนการแก้ไขข้อผิดพลาดดังกล่าวหรือไม่

**ด้านที่ 4 : การสร้างแรงจูงใจและการบริหารจัดการทรัพยากรบุคคล (Incentives and HR Practices)**

- มีการกำหนดมาตรการสร้างแรงจูงใจที่ดึงดูดให้บุคลากรมีส่วนร่วมในการบริหารความเสี่ยงมากน้อยเพียงใด
- ผู้บริหารในหน่วยงานของท่านทบทวนดัชนีชี้วัดผลการดำเนินงาน (KPI) เป็นประจำ เพื่อให้มั่นใจว่าดัชนีชี้วัดยังมีความเหมาะสม สมเหตุสมผล และสามารถยอมรับความเสี่ยงในระดับที่กำหนดไว้หรือไม่

## แนวปฏิบัติที่ 5

ผู้บริหารควรแสดงความมุ่งมั่นต่อการเพิ่มขีดความสามารถของบุคลากรให้มีความรู้ ความชำนาญที่จำเป็นต่อการปฏิบัติงานที่ได้รับมอบหมาย และจะต้องมีการจัดสรรทรัพยากรที่เหมาะสมให้เพียงพอในแต่ละขั้นตอนของกระบวนการบริหารความเสี่ยง รวมถึงกำหนดแนวปฏิบัติในการรักษาและสร้างแรงจูงใจอย่างเป็นรูปธรรม

### คู่มือปฏิบัติ

1. รัฐวิสาหกิจควรจัดให้มีกระบวนการสรรหา พัฒนา ประเมินผล และรักษาบุคลากรอย่างเป็นลายลักษณ์อักษร เพื่อให้มั่นใจว่าองค์กรมีบุคลากรที่มีความรู้ความสามารถในการบริหารความเสี่ยง โดยครอบคลุมกระบวนการ ดังนี้
    - การสรรหา : รัฐวิสาหกิจกำหนดให้มีการสำรวจความต้องการทรัพยากรบุคคลผ่านการเก็บรวบรวมข้อมูล เพื่อนำมาจัดทำแผนอัตรากำลังคน และการพิจารณารับสมัครพนักงาน โดยจัดให้มีการสัมภาษณ์หรือการทดสอบความรู้ เพื่อให้มั่นใจว่าได้ผู้สมัครที่มีคุณสมบัติที่เหมาะสมกับตำแหน่งงาน จากนั้นดำเนินการจัดทำสัญญาจ้างงาน และจัดปฐมนิเทศให้กับพนักงานใหม่
    - การฝึกอบรม : รัฐวิสาหกิจกำหนดให้มีการสำรวจความต้องการหลักสูตรการพัฒนาศักยภาพของพนักงาน เพื่อออกแบบการพัฒนาพนักงานผ่านการจัดทำแผนการฝึกอบรมประจำปี ซึ่งรวมถึงหลักสูตรการบริหารความเสี่ยง จากนั้นติดตามให้มีการฝึกอบรมตามแผนการฝึกอบรมประจำปี รวมถึงจัดให้มีกระบวนการในการขอฝึกอบรมภายนอกองค์กร
    - การประเมินผล : รัฐวิสาหกิจควรกำหนดให้มีการประเมินผลการปฏิบัติงานของพนักงานตามดัชนีชี้วัดผลการดำเนินงาน (KPI) พร้อมทั้งกำหนดรอบการประเมินและเกณฑ์ที่ใช้ในการประเมินพนักงานอย่างชัดเจน พร้อมรายงานผลการประเมินไปยังผู้บริหาร และสื่อสารให้พนักงานรับทราบผลการประเมินของตนเอง จากนั้นนำผลการประเมินดังกล่าวไปพิจารณาจัดทำแผนพัฒนาบุคลากร (Individual Development Plan: IDP)
    - การรักษาบุคลากร : รัฐวิสาหกิจควรกำหนดโครงสร้างเงินเดือน หลักเกณฑ์การสร้างแรงจูงใจ และการจ่ายค่าตอบแทนอื่นๆ อย่างเป็นลายลักษณ์อักษร โดยสามารถพิจารณากำหนดแรงจูงใจได้ 2 ประเภท ดังนี้
      - 1) แรงจูงใจที่เป็นตัวเงิน เช่น การขึ้นเงินเดือน การให้โบนัส สวัสดิการ
      - 2) แรงจูงใจที่ไม่ใช่ตัวเงิน เช่น การเลื่อนตำแหน่ง การได้รับการฝึกอบรม การมอบประกาศนียบัตร
- นอกจากนี้ รัฐวิสาหกิจควรพิจารณาทบทวนและปรับปรุงกระบวนการดังกล่าวเป็นประจำอย่างน้อยปีละ 1 ครั้ง เพื่อให้สอดคล้องกับสถานการณ์และการปฏิบัติงานที่อาจเปลี่ยนแปลงไป จากนั้นสื่อสารให้บุคลากรที่เกี่ยวข้องรับทราบและนำไปปฏิบัติ

2. การพัฒนาบุคลากรเป็นเรื่องที่ทุกองค์กรยอมรับว่ามีความสำคัญมากเป็นอันดับต้นๆ ในการบริหารจัดการองค์กร สำหรับการบริหารความเสี่ยงก็เช่นเดียวกัน บุคลากรที่มีความสามารถ มีความชำนาญ ในการปฏิบัติงาน เข้าใจในบทบาทหน้าที่ที่ได้รับมอบหมายเป็นปัจจัยที่สำคัญอย่างยิ่งในการสนับสนุนให้องค์กรมีสภาพแวดล้อมในการบริหารความเสี่ยงที่เหมาะสม กล่าวคือ บุคลากรที่เข้าใจในงานของตน จะสามารถทำการระบุ ประเมิน จัดการ และติดตามความเสี่ยง ในส่วนงานที่ตนรับผิดชอบ และในภาพรวมขององค์กรได้เป็นอย่างดี

ดังนั้น รัฐวิสาหกิจควรจัดทำแผนแม่บทการบริหารทรัพยากรบุคคล ที่สอดคล้องกับยุทธศาสตร์ขององค์กร และแผนการดำเนินงานด้านอื่นๆ ของรัฐวิสาหกิจ เพื่อเป็นแนวทางในการพัฒนา และบริหารทรัพยากรบุคคลให้ได้มาซึ่งบุคลากรที่มีคุณภาพ โดยมีกิจกรรมที่ต้องดำเนินการ ดังตัวอย่างต่อไปนี้

- 1) การสรรหา : รัฐวิสาหกิจควรพิจารณาสรรหาบุคลากรให้ทันต่อการเติบโตขององค์กร โดยการสรรหาบุคลากรควรพิจารณาผู้สมัครที่มีความรู้ความสามารถกับตำแหน่งที่เปิดรับสมัคร และเป็นผู้สมัครที่มีลักษณะสอดคล้องกับวัฒนธรรมองค์กรและสอดคล้องกับกลยุทธ์ขององค์กร โดยพิจารณา กำหนดค่าพรรณนาลักษณะงาน (JD) ทั้งนี้ การสรรหาบุคลากร อาจต้องสรรหาทั้งจากภายใน และภายนอก หาก**สรรหาจากภายใน** ควรพิจารณาว่าบุคลากรปัจจุบันนั้นมีทักษะ ความรู้ ความชำนาญที่จำเป็นต่อการปฏิบัติงานเพียงพอหรือไม่ ทำการศึกษา วิเคราะห์ ทำความเข้าใจ ในทักษะ ความรู้ความชำนาญที่ต้องการ เปรียบเทียบกับทักษะ ความรู้ความชำนาญของบุคลากร ในปัจจุบัน แล้วจัดทำแผนพัฒนาบุคลากร (IDP) เพื่อให้ได้คุณภาพตามที่ต้องการ หาก**สรรหาจากภายนอก** ควรพิจารณาจัดทำหรือปรับปรุงหลักเกณฑ์ในการสรรหาบุคลากรให้สอดคล้องกับ ความต้องการ เช่น ข้อกำหนดเรื่องคุณสมบัติ การศึกษา ประสบการณ์ พร้อมทั้งทบทวนอัตราผลตอบแทนและสวัสดิการต่างๆ ให้อยู่ในระดับที่แข่งขันได้
- 2) การฝึกอบรม : รัฐวิสาหกิจควรจัดทำแผนการฝึกอบรมประจำปีที่สอดคล้องกับกลยุทธ์ขององค์กร เช่น แผนยุทธศาสตร์ด้านทรัพยากรบุคคล (Human Resource: HR) แผนแม่บทเทคโนโลยีดิจิทัล เพื่อให้มั่นใจว่าพนักงานมีความรู้ความเข้าใจเรื่องความเสี่ยงที่เป็นปัจจุบัน ครอบคลุมถึงความเสี่ยงใหม่ (Emerging Risk) และพิจารณาเทคนิคการอบรมที่หลากหลาย เช่น บรรยายในห้องเรียน (Classroom Instruction) ศึกษาด้วยตนเอง (Self-Study) เรียนรู้ระหว่างปฏิบัติงาน (On-the-job Training) เป็นต้น และจัดให้มีการทบทวนความรู้ความเข้าใจในการบริหารความเสี่ยง ให้กับพนักงานอย่างน้อยปีละ 1 ครั้ง

### ตัวอย่างการออกแบบหลักสูตรการอบรม

หลักสูตร	ความถี่ในการจัดอบรม
หลักสูตรสำหรับกรรมการและผู้บริหาร	ประมาณ 1 ครั้งต่อปี
หลักสูตรสำหรับพนักงาน	จัดอบรมตามความเหมาะสม ของลักษณะงาน และความจำเป็น
หลักสูตรสำหรับหน่วยงานบริหารความเสี่ยง	ประมาณ 2 ครั้งต่อปี

#### ตัวอย่างหัวข้อการอบรมการบริหารความเสี่ยง

- ความสำคัญของการบริหารความเสี่ยง
- กรอบการบริหารความเสี่ยงตามหลักสากล เช่น COSO Enterprise Risk Management – Integrating with Strategy and Performance (COSO ERM 2017) ISO 31000: 2018 Risk Management
- โครงสร้างและบทบาทหน้าที่ในการบริหารความเสี่ยง
- กระบวนการบริหารความเสี่ยง
- การสร้างวัฒนธรรมการบริหารความเสี่ยงภายในองค์กร
- ความเชื่อมโยงของการบริหารความเสี่ยงและการวางแผนกลยุทธ์
- ดัชนีชี้วัดความเสี่ยงหลัก (Key Risk Indicator: KRI)

อย่างไรก็ตาม ควรมีการคัดกรองเนื้อหาต่างๆ ของการอบรมให้เหมาะสมกับหน้าที่ความรับผิดชอบของผู้เข้ารับการอบรม และมีความสอดคล้องต่อเหตุการณ์ในปัจจุบัน เพื่อให้ผู้เข้ารับการอบรมสามารถนำความรู้ที่ได้จากการอบรมไปประยุกต์ใช้ในการปฏิบัติงานได้อย่างมีประสิทธิภาพ

- 3) การประเมินผล : รัฐวิสาหกิจดำเนินการประเมินผลการปฏิบัติงานของแต่ละบุคลากรโดยกำหนดดัชนีชี้วัดผลการดำเนินงาน (KPI) ที่สอดคล้องกับกลยุทธ์ขององค์กร รวมถึงควรกำหนดการบริหารความเสี่ยงเป็นส่วนหนึ่งของดัชนีชี้วัดผลการดำเนินงาน (KPI) เพื่อให้สามารถตรวจสอบและประเมินผลการจัดการความเสี่ยงได้อย่างชัดเจนและมีประสิทธิภาพ

#### ตัวอย่างดัชนีชี้วัดด้านกระบวนการบริหารความเสี่ยง

- ความสามารถในการระบุความเสี่ยงได้อย่างครบถ้วน
- การเข้าอบรมด้านการบริหารความเสี่ยงอย่างครบถ้วน
- ความสำเร็จในการปฏิบัติตามแผนการบริหารจัดการความเสี่ยงที่กำหนด
- ระดับความสอดคล้องของการบริหารความเสี่ยงกับนโยบายองค์กร

ทั้งนี้ การกำหนดดัชนีชี้วัดผลการดำเนินงาน (KPI) จะต้องไม่กดดันบุคลากรจนเกินไป เพื่อไม่ให้เกิดพฤติกรรมที่ไม่พึงประสงค์ โดยรัฐวิสาหกิจควรพิจารณาทบทวนและปรับปรุงดัชนีชี้วัด

ผลการดำเนินงาน (KPI) เป็นประจำ อย่างน้อยปีละ 1 ครั้ง เพื่อให้สอดคล้องกับกลยุทธ์ และการปฏิบัติงานที่อาจเปลี่ยนแปลงไป

- 4) การรักษานโยบาย : รัฐวิสาหกิจควรกำหนดแรงจูงใจให้สอดคล้องกับผลการประเมิน การปฏิบัติงานด้านการบริหารความเสี่ยง เช่น การจ่ายค่าตอบแทน การมอบประกาศนียบัตร หรือจัดงาน เพื่อยกย่องและแสดงความขอบคุณต่อพนักงานที่มีความสำคัญต่อการบริหาร ความเสี่ยงขององค์กร เพื่อกระตุ้นให้บุคลากรตระหนักถึงความสำคัญของการบริหารความเสี่ยง และก่อให้เกิดระดับของผลการปฏิบัติงานและพฤติกรรมที่พึงประสงค์ ทั้งนี้ การกำหนดแรงจูงใจและผลตอบแทน ต้องสอดคล้องกับระบบแรงจูงใจตามระบบประเมินผล การดำเนินงานรัฐวิสาหกิจ

3. รัฐวิสาหกิจควรพิจารณาเตรียมความพร้อมในการสืบทอดตำแหน่ง โดยคณะกรรมการและผู้บริหาร ต้องมีการกำหนดแผนสืบทอดตำแหน่งสำหรับตำแหน่งที่สำคัญต่อการบริหารความเสี่ยงขององค์กร โดยผู้ที่เป็นผู้สืบทอดตำแหน่งควรได้รับการอบรม การแนะนำแนวทางสำหรับตำแหน่งนั้นๆ เพื่อเป็นการเตรียมความพร้อมกรณีฉุกเฉินสำหรับการมอบหมายความรับผิดชอบที่มีความสำคัญ ต่อการบริหารความเสี่ยง

## องค์ประกอบที่ 2 กลยุทธ์และการกำหนดวัตถุประสงค์ (Strategy and Objective Setting)

### หลักเกณฑ์

รัฐวิสาหกิจควรระบุเหตุการณ์ที่อาจเกิดขึ้นและส่งผลกระทบต่อองค์กรทั้งด้านที่เป็นโอกาสและความเสี่ยง และจะต้องมีความเข้าใจถึงปัจจัยต่างๆ ทั้งภายในและภายนอกองค์กร ทั้งเหตุการณ์ที่เคยเกิดขึ้นมาแล้วในอดีต และการคาดการณ์ในอนาคต เพื่อนำไปกำหนดวัตถุประสงค์ขององค์กรที่ชัดเจนและสอดคล้องกัน ทั้งวัตถุประสงค์ด้านกลยุทธ์และวัตถุประสงค์ด้านการดำเนินงานขององค์กร และจะต้องเป็นไปในแนวทางเดียวกันกับระดับความเสี่ยงที่องค์กรยอมรับได้ (RA)

### แนวปฏิบัติที่ 1

รัฐวิสาหกิจควรระบุเหตุการณ์ที่อาจเกิดขึ้นและส่งผลกระทบต่อการทำงานขององค์กร โดยประเมินปัจจัยที่มีอิทธิพลต่อองค์กร ทั้งจากสภาพแวดล้อมภายในและภายนอก รวมถึงการพิจารณาข้อมูลจากเหตุการณ์ในอดีตควบคู่กับการคาดการณ์แนวโน้มในอนาคต

### คู่มือปฏิบัติ

1. รัฐวิสาหกิจควรทำความเข้าใจบริบทขององค์กร สภาพแวดล้อมในการดำเนินงาน สภาพแวดล้อมในการแข่งขันขององค์กร และปัจจัยอื่นๆ ที่มีอิทธิพลต่อความสามารถขององค์กรในการบรรลุกลยุทธ์และวัตถุประสงค์ในการประกอบกิจการ โดยควรกำหนดกระบวนการในการรวบรวมข้อมูล (Input) ซึ่งรวมถึงแหล่งที่มาของข้อมูล ผู้รับผิดชอบในการจัดเก็บข้อมูล และฐานข้อมูลที่ใช้ในการจัดเก็บ ทั้งนี้ อาจเป็นข้อมูลจากอดีตและการคาดการณ์สถานการณ์ที่อาจเป็นความเสี่ยงหรือภัยคุกคามที่จะเกิดขึ้นในอนาคต เพื่อนำมาวิเคราะห์และกำหนดวัตถุประสงค์และกลยุทธ์ขององค์กร รวมถึงนำมาประกอบการจัดทำแผนวิสาหกิจ/แผนยุทธศาสตร์ (แผนระยะยาว)

#### ตัวอย่างสภาพแวดล้อมภายในและภายนอกองค์กร

##### 1) สภาพแวดล้อมภายใน เช่น

- ทุน เช่น สินทรัพย์ ซึ่งรวมถึงเงินสด อุปกรณ์ อสังหาริมทรัพย์ สิทธิบัตร
- ทรัพยากรบุคคล เช่น ความรู้ ความชำนาญ ทักษะ ทักษะคนดี ความสัมพันธ์ คุณค่าและวัฒนธรรม
- กระบวนการ เช่น กิจกรรม งาน นโยบาย วิธีปฏิบัติ การเปลี่ยนแปลงในกระบวนการบริหาร กระบวนการดำเนินงาน และกระบวนการสนับสนุนต่างๆ
- เทคโนโลยีที่ใช้ ซึ่งรวมไปถึงเทคโนโลยีใหม่หรือเทคโนโลยีที่ได้รับการปรับปรุง

## 2) สภาพแวดล้อมภายนอก เช่น

- ผู้ที่ได้รับผลกระทบจากองค์กร เช่น ลูกค้า ผู้ขาย คู่แข่ง
- ผู้ที่มีอิทธิพลต่อสภาพแวดล้อมทางธุรกิจขององค์กร เช่น รัฐบาล หน่วยงานที่มีอำนาจในการกำกับดูแล
- ผู้ที่มีอิทธิพลต่อชื่อเสียง หรือภาพลักษณ์ขององค์กร เช่น ชุมชน กลุ่มผลประโยชน์
- กฎหมาย ระเบียบ
- ภัยธรรมชาติ

โดยรัฐวิสาหกิจอาจพิจารณานำการวิเคราะห์ PESTEL มาเป็นเครื่องมือในการวิเคราะห์เพื่อช่วยระบุปัจจัยภายนอกที่อาจส่งผลกระทบต่อองค์กร ผ่านการวิเคราะห์ปัจจัยต่างๆ ได้แก่ ปัจจัยทางการเมือง (Political Factor) ปัจจัยทางเศรษฐกิจ (Economic Factor) ปัจจัยทางสังคม (Social Factor) ปัจจัยทางเทคโนโลยี (Technological Factor) ปัจจัยทางสิ่งแวดล้อม (Environmental Factor) และปัจจัยทางด้านกฎหมาย (Legal Factor) รวมถึงอาจพิจารณานำการวิเคราะห์ SWOT มาช่วยในการวิเคราะห์และประเมินสภาพแวดล้อมภายในและภายนอกองค์กร รวมถึงประเมินจุดแข็ง (Strength: S) จุดอ่อน (Weakness: W) โอกาส (Opportunity: O) และอุปสรรค (Threat: T)

การนำข้อมูลที่ได้จากการวิเคราะห์มาใช้ในการกำหนดกลยุทธ์ ต้องมีความสอดคล้องกับข้อมูลที่ปรากฏอยู่ในแผนแม่บทที่เกี่ยวข้อง รวมถึงกำหนดให้มีกระบวนการทบทวนการระบุและรวบรวมข้อมูลในการวิเคราะห์ เพื่อให้มั่นใจว่ากระบวนการดังกล่าวมีประสิทธิภาพ นำมาซึ่งความเป็นปัจจุบันและความถูกต้องของข้อมูล

## แนวปฏิบัติที่ 2

คณะกรรมการและผู้บริหารควรกำหนดให้รัฐวิสาหกิจมีระดับความเสี่ยงที่องค์กรยอมรับได้ (RA) และช่วงเบี่ยงเบนของระดับความเสี่ยงที่องค์กรยอมรับได้ (RT) ที่มีความสอดคล้องกับการกำหนดกลยุทธ์ และวัตถุประสงค์ในการประกอบกิจการ

### คู่มือปฏิบัติ

1. **ระดับความเสี่ยงที่องค์กรยอมรับได้ (RA)** หมายถึง ประเภทความเสี่ยงและค่าความเสี่ยงที่กำหนดในภาพกว้าง ซึ่งองค์กรเต็มใจยอมรับสำหรับการสร้างคุณค่า คณะกรรมการและผู้บริหารควรพิจารณา กำหนดระดับความเสี่ยงที่องค์กรยอมรับได้ (RA) เพื่อนำมาใช้ในการบริหารความเสี่ยง โดยสามารถระบุได้ตามประเภทความเสี่ยง Strategic Risk Operational Risk Financial Risk และ Compliance Risk (S-O-F-C) หรือประเภทความเสี่ยงอื่นๆ ตามที่กำหนด

โดยทั่วไป การดำเนินงานให้ได้ผลตอบแทนนั้น รัฐวิสาหกิจอาจจำเป็นต้องยอมรับความเสี่ยงบ้าง การกำหนดระดับความเสี่ยงที่องค์กรยอมรับได้ (RA) จะช่วยให้รัฐวิสาหกิจทราบว่าคุณภาพความเสี่ยงประเภทใด ลักษณะใด ตลอดจนระดับความเสี่ยงที่สูงเพียงใดที่รัฐวิสาหกิจสามารถยอมรับได้เพื่อให้สามารถดำเนินงานได้ตามเป้าหมายที่กำหนด นอกจากนี้ ระดับความเสี่ยงที่องค์กรยอมรับได้ (RA) ยังสามารถนำมาใช้เป็นกรอบในการดำเนินงานและการตัดสินใจต่างๆ ของรัฐวิสาหกิจได้

**ตัวอย่าง:** ในการดำเนินโครงการใหม่ รัฐวิสาหกิจควรพิจารณาว่ามีปัจจัยใดบ้างที่อาจทำให้ต้องเผชิญกับความเสี่ยงที่สูงเกินกว่าระดับความเสี่ยงที่องค์กรยอมรับได้ (RA) เช่น สถานที่ตั้งอยู่ใกล้ชุมชนมากเกินไปจนอาจก่อให้เกิดข้อร้องเรียนหรือกรณีพิพาทหรือไม่ ผลกระทบต่อสิ่งแวดล้อมอยู่ในระดับที่สูงเกินกว่าค่าที่กฎหมายกำหนดหรือไม่ ซึ่งระดับความเสี่ยงที่องค์กรยอมรับได้ (RA) ที่รัฐวิสาหกิจได้กำหนดไว้จะทำหน้าที่เป็นกรอบในการตัดสินใจว่าจะอนุมัติการดำเนินโครงการนี้หรือไม่ หรือหากจะดำเนินโครงการนี้ รัฐวิสาหกิจได้จัดให้มีมาตรการในการบริหารจัดการความเสี่ยงอย่างเหมาะสมเพียงใด และมาตรการดังกล่าวสามารถช่วยลดความเสี่ยงให้ลงมาอยู่ในระดับที่องค์กรยอมรับได้ (RA) หรือไม่

**การกำหนดระดับความเสี่ยงที่องค์กรยอมรับได้ (RA) มีดังนี้**

- ผู้บริหารควรเป็นผู้กำหนดระดับความเสี่ยงที่องค์กรยอมรับได้ (RA) และเสนอคณะกรรมการเพื่อพิจารณาอนุมัติ
- ปัจจัยที่ควรคำนึงถึงในการกำหนดระดับความเสี่ยงที่องค์กรยอมรับได้ (RA) ได้แก่
  - ความต้องการของผู้มีส่วนได้เสีย
  - วัตถุประสงค์ เป้าหมาย วิสัยทัศน์ พันธกิจ ของรัฐวิสาหกิจ
  - ความเสี่ยงในการประกอบกิจการของรัฐวิสาหกิจ
  - ปัจจัยภายในองค์กร รัฐวิสาหกิจมีมุมมองต่อความเสี่ยงอย่างไร รับความเสี่ยงได้ หรือไม่ยอมรับความเสี่ยง (Risk Taker vs Risk Averse)
  - ปัจจัยภายนอกองค์กร สภาพแวดล้อมต่างๆ ในการดำเนินงานของรัฐวิสาหกิจมีความเสี่ยงหรือความไม่แน่นอนมากเพียงใด
  - ระดับความเสี่ยงที่องค์กรยอมรับได้ (RA) สามารถกำหนดได้ทั้งแบบเชิงปริมาณและแบบเชิงคุณภาพ ทั้งนี้ อาจขึ้นอยู่กับความสมบูรณ์ของข้อมูลที่มีอยู่ในองค์กร

**ตัวอย่างคำถามที่จะช่วยรัฐวิสาหกิจในการกำหนดระดับความเสี่ยงที่องค์กรยอมรับได้ (RA) มีดังนี้**

- ความเสี่ยงอะไรบ้างที่รัฐวิสาหกิจสามารถยอมรับได้และไม่สามารถยอมรับได้
- รัฐวิสาหกิจจะยอมรับความเสี่ยงที่เพิ่มขึ้นจากที่มีอยู่ได้หรือไม่ ด้วยระดับผลตอบแทนที่ต้องการเท่าใด
- ระดับความเสี่ยงที่องค์กรยอมรับได้ (RA) ของรัฐวิสาหกิจเทียบกับรัฐวิสาหกิจอื่นในประเภทธุรกิจเดียวกันมีความเหมือนหรือต่างกันอย่างไร
- มีความเสี่ยงเรื่องใดเรื่องหนึ่งโดยเฉพาะที่องค์กรไม่สามารถยอมรับได้หรือไม่ เช่น ความเสี่ยงที่อาจทำให้องค์กรไม่สามารถปฏิบัติตามกฎหมาย
- รัฐวิสาหกิจมีการกำหนดกลยุทธ์ในการบริหารความเสี่ยงหรือไม่ อย่างไร
- พิจารณาดูตัวอย่างและผลของการบริหารความเสี่ยงในอดีตที่รัฐวิสาหกิจยอมรับความเสี่ยงมากหรือน้อยเกินควร เพื่อเปรียบเทียบกับกลยุทธ์ วัตถุประสงค์ และเป้าหมาย

**ขั้นตอนการกำหนดระดับความเสี่ยงที่องค์กรยอมรับได้ (RA) ประกอบด้วย 4 ขั้นตอนหลักดังต่อไปนี้**

- 1) การวิเคราะห์ความคาดหวังของผู้มีส่วนได้เสียทั้งจากภายในและภายนอกรัฐวิสาหกิจเกี่ยวกับระดับความเสี่ยงที่องค์กรยอมรับได้ (RA)
  - 2) การกำหนดระดับความเสี่ยงที่องค์กรยอมรับได้ (RA) จากระดับบนลงสู่ระดับล่าง (Top-down) โดยเชื่อมโยงเข้ากับกลยุทธ์และวัตถุประสงค์ในการประกอบกิจการของรัฐวิสาหกิจ
  - 3) การกำหนดระดับความเสี่ยงที่องค์กรยอมรับได้ (RA) จากระดับล่างขึ้นสู่ระดับบน (Bottom-up) จากการวิเคราะห์ข้อมูลความเสี่ยงของรัฐวิสาหกิจในแต่ละด้าน
  - 4) การกำหนดระดับความเสี่ยงที่องค์กรยอมรับได้ (RA) โดยพิจารณาจากผลที่ได้จากขั้นตอนที่ 1) – 3)
- ระดับความเสี่ยงที่องค์กรยอมรับได้ (RA) ของรัฐวิสาหกิจสามารถแสดงอยู่ในรูปแบบต่างๆ ได้หลายรูปแบบ ดังตัวอย่างต่อไปนี้

**ตัวอย่างที่ 1 การกำหนดระดับความเสี่ยงที่องค์กรยอมรับได้ (RA) เชิงคุณภาพ (Qualitative)**

ประเภทของความเสี่ยง	ระดับที่องค์กรยอมรับได้	คำอธิบาย / แนวปฏิบัติ
กลยุทธ์ (Strategic)	ปานกลาง	• ยอมรับความเสี่ยงจากผลขาดทุนที่เกิดจากโครงการใหม่ๆ เพื่อการวิจัยและพัฒนาได้ในระดับปานกลาง
การเงิน (Financial)	ต่ำ	• ยอมรับความเสี่ยงได้ต่ำสำหรับเรื่องสภาพคล่องทางการเงิน

ประเภทของความเสี่ยง	ระดับที่องค์กรยอมรับได้	คำอธิบาย / แนวปฏิบัติ
ปฏิบัติการ (Operational)	ต่ำ	<ul style="list-style-type: none"> <li>ยอมรับความเสี่ยงได้ต่ำสำหรับเรื่องความปลอดภัยและอาชีวอนามัย</li> <li>ยอมรับความเสี่ยงได้ต่ำสำหรับเรื่องเกี่ยวกับการปฏิบัติการในกระบวนการทำงานที่ทำอยู่แล้วเป็นประจำ</li> </ul>
การปฏิบัติตามกฎระเบียบ (Compliance)	ไม่ยอมรับเลย	<ul style="list-style-type: none"> <li>ไม่ยอมรับความเสี่ยงในการละเมิดกฎหมายหรือกฎระเบียบ</li> <li>ไม่ยอมให้มีการละเมิดหลักจรรยาบรรณพนักงาน โดยจะติดตามดูแลอย่างเข้มงวด</li> </ul>
ตลาด (Market)	ต่ำ	<ul style="list-style-type: none"> <li>ยอมรับความเสี่ยงได้ต่ำสำหรับผลขาดทุนจากการบริหารเงิน (Treasury Operations)</li> <li>การทำธุรกรรมเพื่อการเก็งกำไร (Speculative) สามารถทำได้ตามความจำเป็นเท่านั้น</li> </ul>

**ตัวอย่างที่ 2** การกำหนดระดับความเสี่ยงที่องค์กรยอมรับได้ (RA) เชิงปริมาณ (Quantitative)

ประเภทของความเสี่ยง	ข้อความแสดงระดับความเสี่ยงที่องค์กรยอมรับได้ (RA)
การขยายการดำเนินงาน	<ul style="list-style-type: none"> <li>รัฐวิสาหกิจจะไม่ขยายการดำเนินงานไปในธุรกิจที่ไม่ใช่ธุรกิจหลักในระยะเวลา 5 ปีข้างหน้า</li> </ul>
คุณภาพของการบริการ	<ul style="list-style-type: none"> <li>รัฐวิสาหกิจมีความมุ่งมั่นในการให้บริการที่ดีที่สุดแก่ประชาชนผู้รับบริการ โดยรักษาระดับความพึงพอใจของลูกค้าไม่น้อยกว่าร้อยละ 90</li> </ul>
การเงิน	<ul style="list-style-type: none"> <li>รัฐวิสาหกิจไม่ต้องการให้อัตราส่วนหนี้สินต่อทุน (Debt to Equity Ratio) มากกว่าหรือเท่ากับ 2 ต่อ 1</li> </ul>
การพัฒนาบุคลากร	<ul style="list-style-type: none"> <li>การฝึกอบรมการบริหารความเสี่ยงต้องมีพนักงานเข้ารับการฝึกอบรมไม่ต่ำกว่าร้อยละ 90</li> </ul>

**ตัวอย่างที่ 3** การกำหนดระดับความเสี่ยงที่องค์กรยอมรับได้ (RA) ในแผนภาพความเสี่ยง  
(Heat Map/Risk Map)

โอกาสที่จะเกิด ผลกระทบ	ต่ำมาก	ต่ำ	ปานกลาง	สูง	สูงมาก	โอกาสที่จะเกิด ผลกระทบ	ต่ำมาก	ต่ำ	ปานกลาง	สูง	สูงมาก
	(1)	(2)	(3)	(4)	(5)		(1)	(2)	(3)	(4)	(5)
สูงมาก (5)	ปานกลาง	สูง	สูงมาก	สูงมาก	สูงมาก	สูงมาก (5)	สูง	สูง	สูง	สูง	สูง
สูง (4)	ปานกลาง	ปานกลาง	สูง	สูงมาก	สูงมาก	สูง (4)	ปานกลาง	สูง	สูง	สูง	สูง
ปานกลาง (3)	ต่ำ	ปานกลาง	ปานกลาง	สูง	สูงมาก	ปานกลาง (3)	ต่ำ	ปานกลาง	สูง	สูง	สูง
ต่ำ (2)	ต่ำ	ต่ำ	ปานกลาง	ปานกลาง	สูง	ต่ำ (2)	ต่ำ	ต่ำ	ปานกลาง	สูง	สูง
ต่ำมาก (1)	ต่ำมาก	ต่ำ	ต่ำ	ปานกลาง	ปานกลาง	ต่ำมาก (1)	ต่ำมาก	ต่ำ	ต่ำ	ปานกลาง	สูง

แผนภาพความเสี่ยงนี้ ใช้ในการแสดงผลของการประเมินความเสี่ยงว่ามีโอกาสที่จะเกิดและผลกระทบอยู่ในระดับใด โดยวิธีวิสาห์กิจอาจกำหนดให้ระดับความเสี่ยง “สูงมาก” มีจำนวนตามภาพด้านซ้ายหรือกำหนดให้ระดับความเสี่ยง “สูงมาก” ครอบคลุมจำนวนช่องที่มากขึ้นดังแสดงในภาพด้านขวา กล่าวคือ หากองค์กรใดกำหนดให้ระดับความเสี่ยง “สูงมาก” มีจำนวนช่องที่มากกว่า แสดงว่าองค์กรนั้นยอมรับความเสี่ยงได้น้อยกว่า นอกจากนี้ การกำหนดเกณฑ์การประเมินความเสี่ยง ว่าระดับผลกระทบเท่ากับ 5 หมายถึงอะไร ระดับ 4 หมายถึงอะไรนั้น ก็เป็นรูปแบบหนึ่งที่สามารถสะท้อนให้เห็นถึงระดับความเสี่ยงที่องค์กรยอมรับได้ (RA) เช่นกัน

ทั้งนี้ รายละเอียดเกี่ยวกับการประเมินความเสี่ยงและการกำหนดเกณฑ์การประเมินความเสี่ยงได้อธิบายไว้ในองค์ประกอบที่ 3 แนวปฏิบัติที่ 2

**ช่วงเบี่ยงเบนของระดับความเสี่ยงที่องค์กรยอมรับได้ (RT)** หมายถึง ขอบเขตความเบี่ยงเบนในผลการปฏิบัติงานที่ยอมรับได้ที่เกี่ยวข้องกับการบรรลุวัตถุประสงค์ และสอดคล้องกับระดับความเสี่ยงที่องค์กรยอมรับได้ (RA)

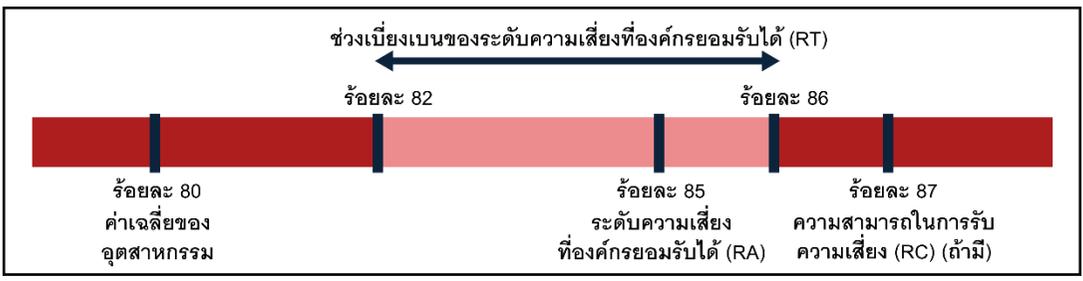
**ตัวอย่าง:** องค์กรแห่งหนึ่งมีเป้าหมายในการให้บริการที่ลูกค้ามีความพึงพอใจ ซึ่งในการพิจารณาช่วงเบี่ยงเบนของระดับความเสี่ยงที่องค์กรยอมรับได้ (RT) นั้น ผู้บริหารได้ระบุว่า

- ค่าเป้าหมายของระดับความพึงพอใจของลูกค้า เท่ากับร้อยละ 85 มาเป็นเวลานานหลายปี ซึ่งองค์กรก็สามารถดำเนินงานได้ตามค่าเป้าหมายนี้มาโดยตลอด
- ค่าเฉลี่ยของอุตสาหกรรม เท่ากับร้อยละ 80 และมีแนวโน้มคงที่
- หากความพึงพอใจของลูกค้าลดลงเป็นการชั่วคราว และยังคงอยู่ในระดับที่สูงกว่าค่าเฉลี่ยของอุตสาหกรรมพบว่าผลกระทบน้อยมากต่อการตัดสินใจใช้บริการของลูกค้า

- หากจะทำให้ความพึงพอใจของลูกค้าเพิ่มขึ้นสูงกว่าร้อยละ 87 ต้องใช้ทรัพยากรเพิ่มขึ้นอย่างมาก และไม่คุ้มค่ากับผลที่ได้รับ
- องค์กรกำลังถูกจับตามองจากสาธารณชนและมีการวิพากษ์วิจารณ์ถึงการที่องค์กรไม่สามารถลดต้นทุนได้

จากตัวอย่างดังกล่าว ผู้บริหารจึงกำหนดว่าควรคงค่าเป้าหมายของระดับความพึงพอใจของลูกค้า หรือระดับความเสี่ยงที่องค์กรยอมรับได้ (RA) ที่ร้อยละ 85 และมีช่วงความเบี่ยงเบนของระดับความเสี่ยงที่องค์กรยอมรับได้ (RT) อยู่ระหว่างร้อยละ 82 - 86

ภาพแสดงตัวอย่างการกำหนดช่วงเบี่ยงเบนของระดับความเสี่ยงที่องค์กรยอมรับได้ (RT)



**แนวปฏิบัติเพื่อการต่อยอด**

รัฐวิสาหกิจอาจพิจารณากำหนดความสามารถในการรับความเสี่ยง (Risk Capacity: RC) เพื่อใช้ประกอบการพิจารณาความเหมาะสมของการกำหนดระดับความเสี่ยงที่องค์กรยอมรับได้ (RA) และช่วงเบี่ยงเบนของระดับความเสี่ยงที่องค์กรยอมรับได้ (RT)

**ความสามารถในการรับความเสี่ยง (RC)** หมายถึง ค่าความเสี่ยงสูงสุดที่องค์กรสามารถรับได้ เพื่อให้บรรลุกลยุทธ์และวัตถุประสงค์ในการประกอบกิจการ โดยความสามารถในการรับความเสี่ยง (RC) มักถูกพิจารณาเมื่อมีการกำหนดระดับความเสี่ยงที่องค์กรยอมรับได้ (RA) เนื่องจากโดยทั่วไปองค์กรพยายามที่จะรักษาให้ระดับความเสี่ยงที่องค์กรยอมรับได้ (RA) อยู่ภายใต้ความสามารถในการรับความเสี่ยง (RC)

กรณีที่ระดับความเสี่ยงที่องค์กรยอมรับได้ (RA) สูงมากเกินกว่าความสามารถในการรับความเสี่ยง (RC) องค์กรอาจประสบความล้มเหลวได้ ในทางกลับกัน หากความสามารถในการรับความเสี่ยง (RC) มีมากเกินกว่าระดับความเสี่ยงที่องค์กรยอมรับได้ (RA) อย่างมีนัยสำคัญ หมายความว่า องค์กรอาจสูญเสียโอกาสในการเพิ่มมูลค่าขององค์กรให้กับผู้มีส่วนได้เสีย

2. รัฐวิสาหกิจควรกำหนดให้มีการสื่อสารระดับความเสี่ยงที่องค์กรยอมรับได้ (RA) และช่วงเบี่ยงเบนของระดับความเสี่ยงที่องค์กรยอมรับได้ (RT) ต่อผู้มีส่วนได้เสียที่เกี่ยวข้อง รวมถึงกำหนดให้มีการทบทวนอย่างสม่ำเสมอหรือเมื่อมีการเปลี่ยนแปลงที่สำคัญ

### แนวปฏิบัติที่ 3

รัฐวิสาหกิจพิจารณาเลือกกลยุทธ์ที่ดีที่สุดที่อยู่ในระดับความเสี่ยงที่องค์กรยอมรับได้ (RA) และสนับสนุนพันธกิจและวิสัยทัศน์ โดยพิจารณาโอกาสและความเสี่ยงของแต่ละกลยุทธ์ เพื่อให้ผู้บริหารและคณะกรรมการใช้ประกอบการตัดสินใจเลือกกลยุทธ์ที่ดีที่สุด

#### คู่มือปฏิบัติ

1. รัฐวิสาหกิจพิจารณาเลือกกลยุทธ์ที่เป็นทางเลือก โดยกลยุทธ์นั้นต้องสนับสนุนพันธกิจและวิสัยทัศน์ และสอดคล้องกับคุณค่าหลัก (Core Value) รวมถึงต้องทำให้องค์กรอยู่ภายใต้ระดับความเสี่ยงที่องค์กรยอมรับได้ (RA) รัฐวิสาหกิจต้องพิจารณาข้อสมมติฐานที่เกี่ยวกับบริบทขององค์กร ทรัพยากร และความรู้ความสามารถ ซึ่งเป็นข้อมูลจากองค์ประกอบที่ 2 แนวปฏิบัติที่ 1 นำมาประกอบการพิจารณาประเมินกลยุทธ์ที่เป็นทางเลือก โดยสามารถประเมินได้หลายวิธี ดังตัวอย่างต่อไปนี้

- การวิเคราะห์ SWOT

เป็นการวิเคราะห์และประเมินสภาพแวดล้อมภายในและภายนอกองค์กร รวมถึงประเมินจุดแข็ง (Strength: S) จุดอ่อน (Weakness: W) โอกาส (Opportunity: O) และอุปสรรค (Threat: T) โดยองค์กรควรพิจารณาใช้ฐานข้อมูลการวิเคราะห์ศักยภาพขององค์กร และข้อมูลเทียบกับคู่แข่งในอุตสาหกรรมเดียวกัน

- การวิเคราะห์สถานการณ์สมมติ (Scenario Analysis)

เป็นการวิเคราะห์เหตุการณ์ในอนาคตที่อาจเกิดขึ้น โดยพิจารณาถึงผลกระทบที่เป็นไปได้จากเหตุการณ์นั้นๆ โดยส่วนใหญ่จะแบ่งการคาดการณ์เป็น 3 ด้าน คือ 1) สถานการณ์สมมติที่เป็นปกติตามที่คาดการณ์ (Base Case หรือ Normal Case) 2) สถานการณ์สมมติที่ดีกว่าที่คาดการณ์ (Best Case) และ 3) สถานการณ์สมมติที่แย่กว่าที่คาดการณ์ (Worst Case)

ในการพิจารณาเลือกกลยุทธ์ รัฐวิสาหกิจควรคำนึงถึงความเสี่ยงและโอกาสที่เป็นไปได้สำหรับกลยุทธ์ในแต่ละทางเลือก เพื่อให้ผู้บริหารสามารถพิจารณาตัดสินใจเลือกกลยุทธ์ที่ดีที่สุดโดยยังอยู่ในระดับความเสี่ยงที่องค์กรยอมรับได้ (RA)

นอกจากนี้ รัฐวิสาหกิจควรมีการติดตามผลการดำเนินงานตามกลยุทธ์ที่เลือก ในกรณีที่รัฐวิสาหกิจพบว่ากลยุทธ์ปัจจุบันนั้นไม่สามารถสร้างคุณค่า รักษาคุณค่า และทำให้คุณค่าเกิดขึ้นจริง หรือเมื่อมีการเปลี่ยนแปลงในบริบทขององค์กร จนทำให้ความเสี่ยงขององค์กรเข้าใกล้ระดับความเสี่ยงที่องค์กรยอมรับได้ (RA) มากเกินไป อาจพิจารณาเปลี่ยนแปลงกลยุทธ์ได้

## แนวปฏิบัติที่ 4

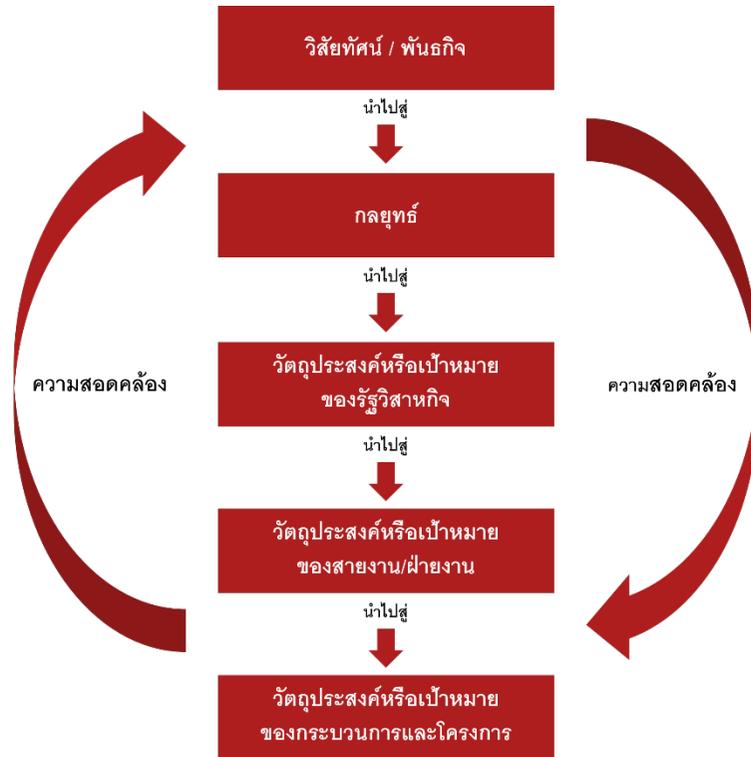
รัฐวิสาหกิจพิจารณาความเสี่ยงในขณะที่กำหนดวัตถุประสงค์ในการประกอบกิจการในระดับต่างๆ ที่สอดคล้องกัน ทั้งวัตถุประสงค์ด้านกลยุทธ์และวัตถุประสงค์ด้านการดำเนินงานขององค์กรและจะต้องเป็นไปในแนวทางเดียวกันกับระดับความเสี่ยงที่องค์กรยอมรับได้ (RA)

### คู่มือปฏิบัติ

1. วัตถุประสงค์ในการประกอบกิจการ (Business Objectives) หมายถึง ขั้นตอนที่องค์กรสามารถใช้วัดความสำเร็จตามกลยุทธ์ โดยรัฐวิสาหกิจควรพิจารณากำหนดวัตถุประสงค์ในการประกอบกิจการที่สามารถวัดได้ สอดคล้องและสนับสนุนให้บรรลุกลยุทธ์ โดยยังคงอยู่ภายใต้ระดับความเสี่ยงที่องค์กรยอมรับได้ (RA) เพื่อให้มั่นใจว่าองค์กรไม่ได้รับความเสี่ยงมากหรือน้อยเกินไป โดยวัตถุประสงค์จะได้รับการสื่อสารจากบนลงล่าง และมีหลายระดับ ตั้งแต่ระดับที่เป็นภาพรวมขององค์กรคือ วิสัยทัศน์ พันธกิจ ซึ่งจะนำไปสู่วัตถุประสงค์หรือเป้าหมายของรัฐวิสาหกิจ ระดับรองลงมาคือ วัตถุประสงค์หรือเป้าหมายของสายงานหรือฝ่ายงานต่างๆ และยังมีระดับที่ย่อยลงไปจนถึงวัตถุประสงค์หรือเป้าหมายของกระบวนการและโครงการ

ทั้งนี้ วัตถุประสงค์ทั้งในระดับเดียวกันและในระดับที่สูงขึ้นไป ตลอดจนกลยุทธ์และระดับความเสี่ยงที่องค์กรยอมรับได้ (RA) ของรัฐวิสาหกิจจะต้องสอดคล้องกัน เพื่อให้เกิดความมั่นใจว่า กิจกรรมต่างๆ ที่สายงาน/ฝ่ายงาน ผู้บริหารและพนักงานได้ดำเนินการจะช่วยสนับสนุนต่อการบรรลุซึ่งวัตถุประสงค์ของรัฐวิสาหกิจภาพรวม

ภาพแสดงความสอดคล้องของวัตถุประสงค์ในระดับต่างๆ



เมื่อดำเนินการกำหนดวัตถุประสงค์ในระดับองค์กร (Entity-Level Objectives) แล้วเสร็จผู้บริหารควรจัดให้มีการกำหนดวัตถุประสงค์ในระดับกิจกรรม (Activity-Level Objectives) ที่สนับสนุนและสอดคล้องกับวัตถุประสงค์ในระดับองค์กร

การกำหนดวัตถุประสงค์ที่ดีควรเป็นไปตามหลักการที่เรียกว่า SMART โดยวัตถุประสงค์ที่ดีควรมีความชัดเจน (Specific) สามารถวัดผลได้ (Measurable) สามารถบรรลุได้ (Achievable) มีความเกี่ยวข้องสอดคล้องกัน (Relevant) และมีการกำหนดระยะเวลา (Time Bound) ดังรายละเอียดต่อไปนี้

หลักการ	คำอธิบาย
ความชัดเจน (Specific)	วัตถุประสงค์ควรมีความชัดเจนเพื่อให้เกิดความเข้าใจตรงกันในผลตอบแทนหรือผลลัพธ์ที่ต้องการ
สามารถวัดผลได้ (Measurable)	วัตถุประสงค์ควรสามารถวัดผลได้และควรมีการระบุหลักเกณฑ์และข้อมูลที่ต้องการใช้ในการวัดผล ในกรณีที่ไม่สามารถวัดผลได้ ผู้บริหารควรเพิ่มความระมัดระวังในการพิจารณากิจกรรมต่างๆ ที่เกี่ยวข้องกับวัตถุประสงค์ รวมถึงขนาดของการลงทุนในกิจกรรมนั้นๆ ด้วย

หลักการ	คำอธิบาย
สามารถบรรลุได้ (Achievable)	วัตถุประสงค์หรือเป้าหมายต้องมีความสมเหตุสมผลและสามารถบรรลุได้จริง โดยพิจารณาปัจจัยต่างๆ เช่น สภาพตลาด ช่วงเวลา การจัดสรรทรัพยากร
ความเกี่ยวข้อง สอดคล้องกัน (Relevant)	วัตถุประสงค์ที่กำหนดขึ้นต้องสอดคล้องและสนับสนุนต่อการบรรลุวัตถุประสงค์ ทั้งในระดับเดียวกันและวัตถุประสงค์ที่สูงกว่า
การกำหนดระยะเวลา (Time bound)	ควรกำหนดเวลาในการบรรลุวัตถุประสงค์ให้ชัดเจน

สิ่งที่สำคัญ คือ วัตถุประสงค์ ทั้งในระดับองค์กรและระดับกิจกรรม ตลอดจนพันธกิจ กลยุทธ์ แผนการดำเนินงาน และระดับความเสี่ยงที่องค์กรยอมรับได้ (RA) จะต้องสอดคล้องกัน เพื่อให้การถ่ายทอดจากระดับองค์กรลงไปสู่วัตถุประสงค์ย่อย และกิจกรรมการดำเนินงานทุกอย่าง ทั้งทั้งองค์กรมีความเชื่อมโยง ผสมผสาน และเป็นไปในแนวทางเดียวกัน

**ตัวอย่างวัตถุประสงค์ที่เป็นไปตามหลักการ SMART**

- เพิ่มระดับการบริการของศูนย์บริการลูกค้า (Call Center) ให้ลูกค้ามีความพึงพอใจที่มากกว่าปีที่ผ่านมาอย่างน้อยร้อยละ 5 ภายในธันวาคม 25XX
- ขยายการดำเนินงานด้านสินเชื่อรถยนต์ให้ครอบคลุมทุกจังหวัดในภาคตะวันออกเฉียงเหนือ โดยให้วงเงินเพิ่มขึ้นเป็นสองเท่าของปีที่ผ่านมา ภายใน 3 ปีข้างหน้า
- พัฒนานุคลากรในหน่วยงานตรวจสอบภายใน ให้ได้เป็นผู้ตรวจสอบภายในวิชาชีพ อย่างน้อย 5 คน ภายในธันวาคม 25XX
- ลดปริมาณขยะพลาสติกที่ไม่สามารถรีไซเคิลได้ลงร้อยละ 30 ภายในธันวาคม 25XX ผ่านมาตรการลด เลิกใช้พลาสติกแบบใช้ครั้งเดียว (Single-use Plastic)

**ตัวอย่างวัตถุประสงค์ที่ไม่เป็นไปตามหลักการ SMART**

- เพิ่มระดับการบริการให้ลูกค้ามีความพึงพอใจมากที่สุด (ไม่ชัดเจนว่ามากที่สุดคือเท่าใด ไม่ระบุว่าวัดผลอย่างไร และไม่กำหนดระยะเวลา)
- ขยายการดำเนินงานให้ครอบคลุมภูมิภาคใหม่ๆ ภายในไตรมาสแรกของปี (ไม่ชัดเจนว่าจะขยายการดำเนินงานส่วนงานใด ภูมิภาคใด และไม่ระบุว่าวัดผลอย่างไร จึงเป็นไปได้ยากที่จะบรรลุได้ภายในเวลาที่กำหนด)
- พัฒนานุคลากร (ไม่ชัดเจนว่าผลที่ต้องการคืออะไร ไม่ระบุว่าวัดผลอย่างไร และไม่กำหนดระยะเวลา)
- ปรับปรุงคุณภาพน้ำให้ดีขึ้น (ไม่ชัดเจนว่าต้องปรับปรุงคุณภาพน้ำให้ดีขึ้นอย่างไร ไม่ระบุว่าวัดผลอย่างไร และไม่กำหนดระยะเวลา)

- รัฐวิสาหกิจควรกำหนดให้มีการจัดทำการบริหารความเสี่ยงเพื่อสร้างสรรคมูลค่าขององค์กร (Value Creation) และการบริหารความเสี่ยงเพื่อเพิ่มมูลค่าขององค์กร ( Value Enhancement) โดยเชื่อมโยงการบริหารความเสี่ยงกับวิสัยทัศน์ พันธกิจ แผนยุทธศาสตร์ แผนวิสาหกิจ หรือแผนการดำเนินงานที่องค์กรกำหนด เพื่อสร้างคุณค่าให้กับองค์กร

### การบริหารความเสี่ยงเพื่อสร้างสรรคมูลค่าขององค์กร (Value Creation)

“มูลค่า” ของรัฐวิสาหกิจ แสดงอยู่ในรูปของวิสัยทัศน์ พันธกิจ แผนยุทธศาสตร์ หรือแผนวิสาหกิจ ซึ่งถือได้ว่าเป็นเป้าหมายหรือวัตถุประสงค์ขององค์กร

ดังนั้น การบริหารความเสี่ยงเพื่อสร้างสรรคมูลค่าขององค์กร (Value Creation) คือ การที่องค์กรสามารถระบุเหตุการณ์ที่เป็นโอกาสและความเสี่ยงเมื่อมีการพิจารณากำหนดหรือทบทวนกลยุทธ์ขององค์กร เพื่อช่วยสร้างมูลค่าขององค์กรได้ ทั้งนี้ โอกาส หมายถึง ความเป็นไปได้ที่เหตุการณ์ใดเหตุการณ์หนึ่งจะเกิดขึ้นและส่งผลดีต่อการบรรลุวัตถุประสงค์

### ประโยชน์ของการบริหารความเสี่ยงเพื่อสร้างสรรคมูลค่าขององค์กร (Value Creation)

ประโยชน์ของการบริหารความเสี่ยงเพื่อสร้างสรรคมูลค่าขององค์กร (Value Creation) ได้แก่ ประโยชน์ที่องค์กรได้รับจากเหตุการณ์ที่เป็นโอกาส (Opportunity) กล่าวคือ องค์กรมองเห็นช่องทาง กิจกรรมหรือโครงการใหม่ๆ ที่สามารถดำเนินการได้เพื่อสร้างมูลค่าขององค์กร เมื่อมีโอกาสเกิดขึ้น ผู้บริหารควรนำโอกาสนั้นไปพิจารณาในกระบวนการกำหนดกลยุทธ์ขององค์กรเพื่อวางแผนดำเนินกิจกรรมต่างๆ ในอันที่จะคว้าโอกาสนั้นไว้ ดังนั้น ประโยชน์ที่องค์กรได้รับก็คือ กลยุทธ์ที่ได้รับการปรับปรุงให้มีความสร้างสรรค์ต่อมูลค่าขององค์กรมากขึ้นนั่นเอง

### แนวทางดำเนินงาน

- รวบรวมข้อมูล que แสดงถึงมูลค่า (Value) ของรัฐวิสาหกิจ ได้แก่ วิสัยทัศน์ พันธกิจ กลยุทธ์ วัตถุประสงค์ แผนยุทธศาสตร์ แผนวิสาหกิจ หรือแผนการดำเนินงานขององค์กร เป็นต้น โดยองค์กรควรทำความเข้าใจบริบทขององค์กรผ่านการตั้งคำถาม เพื่อนำผลลัพธ์มาพิจารณาความเสี่ยงเมื่อมีการกำหนดกลยุทธ์ จนเกิดเป็นการสร้างมูลค่าให้กับองค์กร ดังนี้

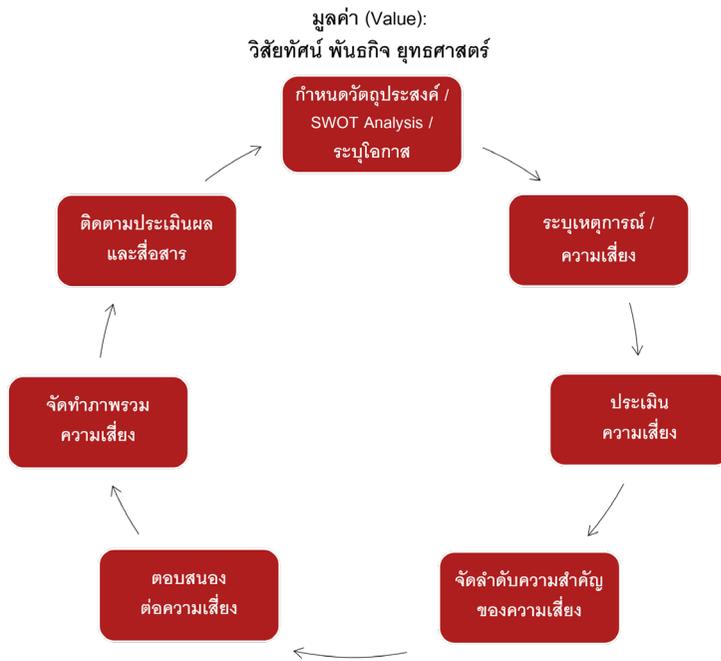
องค์ประกอบของกระบวนการสร้างคุณค่า	คำถามเพื่อพิจารณา
ภาพรวมขององค์กร และสภาพแวดล้อมจากปัจจัยภายนอก	<ul style="list-style-type: none"> <li>สภาพแวดล้อมภายนอกของบริบททางกฎหมาย การค้า สังคม สิ่งแวดล้อมและการเมืองในแง่มุมใดบ้างที่ส่งผลต่อความสามารถขององค์กรในการสร้างคุณค่าในระยะสั้น ระยะกลาง และระยะยาว</li> <li>พันธกิจและวิสัยทัศน์ขององค์กรมีจุดมุ่งหมายอย่างไร</li> </ul>

องค์ประกอบของกระบวนการสร้างคุณค่า	คำถามเพื่อพิจารณา
	<ul style="list-style-type: none"> <li>• บริบทขององค์กรเชื่อมโยงกับการสร้างคุณค่าให้กับองค์กรในวงกว้างได้อย่างไร</li> <li>• แนวโน้มเมกะเทรนด์ที่จะส่งผลกระทบต่อกิจการมีอะไรบ้าง โดยเฉพาะประเด็นด้านสังคมในเรื่องใด เช่น การเปลี่ยนแปลงทางประชากร สุขภาพ ความยากจน หรือความท้าทายด้านสิ่งแวดล้อมในเรื่องใด เช่น การเปลี่ยนแปลงสภาพภูมิอากาศ การขาดแคลนทรัพยากร ข้อจำกัดความปลอดภัยของโลกที่ส่งผลกระทบต่อองค์กร</li> <li>• การเปลี่ยนแปลงใดในสภาพแวดล้อมด้านกฎหมายหรือกฎระเบียบข้อบังคับที่ส่งผลกระทบต่อองค์กร</li> </ul>
ปัจจัยนำเข้า (Inputs)	<ul style="list-style-type: none"> <li>• องค์กรนำเงินทุนประเภทใดบ้างจาก 6 ประเภท ได้แก่ ทุนทางการเงิน ทุนทางการผลิต ทุนมนุษย์ ทุนทางสังคม ทุนทางธรรมชาติ และทุนทางปัญญา</li> </ul>
กิจกรรมทางธุรกิจ	<ul style="list-style-type: none"> <li>• ห่วงโซ่คุณค่าของกิจการคืออะไร</li> <li>• องค์กรสร้างความแตกต่างในตลาดอย่างไร</li> <li>• รูปแบบการสร้างรายได้คืออะไร</li> <li>• องค์กรสร้างนวัตกรรมอย่างไร</li> <li>• องค์กรปรับตัวเข้ากับการเปลี่ยนแปลงได้ดีเพียงใด</li> </ul>
ผลที่ได้รับ (Outputs)	<ul style="list-style-type: none"> <li>• ผลกระทบที่เกิดขึ้นแล้วหรือผลกระทบที่อาจเกิดขึ้นของผลิตภัณฑ์หรือของเสียตลอดห่วงโซ่คุณค่ามีอะไรบ้าง</li> </ul>
ผลลัพธ์ (Outcomes)	<ul style="list-style-type: none"> <li>• ผลลัพธ์ที่จะได้จากผลกระทบหรือกิจกรรมทางธุรกิจสร้างคุณค่าหรือเสียคุณค่ามีอะไรบ้าง</li> </ul>
กลยุทธ์และการจัดสรรทรัพยากร	<ul style="list-style-type: none"> <li>• องค์กรกำหนดกลยุทธ์ระยะสั้น ระยะกลาง และระยะยาวอย่างไร</li> <li>• วัตถุประสงค์เชิงกลยุทธ์ระยะสั้น ระยะกลาง และระยะยาวขององค์กรคืออะไร</li> <li>• ผลกระทบในการบรรลุวัตถุประสงค์ในการประกอบกิจการมีอะไรบ้าง โดยเฉพาะอย่างยิ่งความเสี่ยงระยะกลางถึงระยะยาวที่จะส่งผลกระทบต่อกลยุทธ์ เช่น การเปลี่ยนแปลงสภาพภูมิอากาศ</li> <li>• มีการพิจารณาด้านสิ่งแวดล้อมและสังคมในกลยุทธ์ เพื่อให้มีความได้เปรียบในการแข่งขันมากน้อยเพียงใด</li> </ul>

องค์ประกอบของกระบวนการ สร้างคุณค่า	คำถามเพื่อพิจารณา
	<ul style="list-style-type: none"> <li>• ความเสี่ยงใดบ้างที่สะท้อนให้เห็นในกลยุทธ์</li> <li>• ต้องใช้ทรัพยากรและการจัดสรรทุนในการดำเนินการตามกลยุทธ์อย่างไรบ้าง</li> <li>• ผลประโยชน์ของผู้มีส่วนได้เสียรวมอยู่ในการพัฒนากลยุทธ์อย่างไร</li> </ul>

- 2) หรือร่วมกับผู้บริหารระดับสูง เพื่อระดมสมองและทำการวิเคราะห์ SWOT เพื่อพิจารณากำหนด Value ขององค์กร พร้อมดำเนินการบริหารความเสี่ยงเพื่อให้สามารถสร้าง Value ตามที่คาดหวังได้ โดยการดำเนินการตามกระบวนการบริหารความเสี่ยงขององค์กร ได้แก่ ระบุโอกาส/ความเสี่ยง ประเมินโอกาสที่จะเกิดและผลกระทบ จัดลำดับความเสี่ยง ตอบสนองต่อความเสี่ยง โดยการหารือนี้อาจจัดทำโดยใช้วิธีการประชุมเชิงปฏิบัติการ (Workshop) ซึ่งประกอบด้วยหัวข้อดังต่อไปนี้
  - ทำการวิเคราะห์ SWOT จากผลลัพธ์ของการทำความเข้าใจบริบทขององค์กร เพื่อระบุ Value ขององค์กร กล่าวคือ วิสัยทัศน์ พันธกิจ แผนยุทธศาสตร์ หรือแผนวิสาหกิจ
  - ระบุเหตุการณ์ที่เป็นโอกาส (Opportunity) หรือระบุความเสี่ยงที่รัฐวิสาหกิจจะสูญเสียโอกาสในการดำเนินการตามแผนงานที่กำหนด
  - ประเมินโอกาสที่จะเกิดและผลกระทบที่รัฐวิสาหกิจจะสูญเสียโอกาสดังกล่าวไป โดยใช้เกณฑ์การประเมินความเสี่ยงของรัฐวิสาหกิจ
  - จัดลำดับความสำคัญของความเสี่ยงเพื่อช่วยในการตัดสินใจเลือกแนวทางการตอบสนองต่อความเสี่ยง
  - ตอบสนองต่อความเสี่ยง โดยรัฐวิสาหกิจพิจารณาเลือกแนวทางการตอบสนองต่อความเสี่ยง พร้อมทั้งระบุผู้รับผิดชอบ กำหนดแผนจัดการ ซึ่งเป็นกิจกรรมใหม่ ภารกิจใหม่ หรือโครงการใหม่ และกำหนดเวลาที่คาดว่าจะแล้วเสร็จ
  - จัดทำแบบจำลองเพื่อใช้ในการบริหารความเสี่ยง (Portfolio View of Risk)
- 3) สรุปผลที่ได้จากการหารือ/ประชุมเชิงปฏิบัติการ โดยจัดทำเป็นแผนการบริหารจัดการความเสี่ยง เพื่อสร้างสรรค้มูลค่าขององค์กร
- 4) สื่อสารความคืบหน้าของการบริหารความเสี่ยงทั้งภายในและภายนอกองค์กรอย่างสม่ำเสมอ การสื่อสารภายใน ได้แก่ การรายงานต่อผู้บริหารระดับสูง คณะกรรมการบริหารความเสี่ยง คณะกรรมการตรวจสอบ และคณะกรรมการทุกไตรมาส ทั้งนี้ เพื่อนำข้อมูลความเสี่ยงมาใช้ประกอบการตัดสินใจที่สำคัญของรัฐวิสาหกิจ ส่วนการสื่อสารภายนอก ได้แก่ การรายงานต่อผู้มีส่วนได้เสีย อย่างไรก็ตาม รัฐวิสาหกิจควรคำนึงถึงความเหมาะสมของระดับการเปิดเผยข้อมูล

ต่อบุคคลภายนอกด้วย เช่น รายงานเรื่องปัจจัยเสี่ยงที่เปิดเผยในรายงานประจำปีอาจไม่จำเป็นต้องมีรายละเอียดมากเท่ากับรายงานความเสี่ยงที่ใช้ภายในองค์กรที่นำเสนอต่อผู้บริหาร



**ตัวอย่าง:** รัฐวิสาหกิจมีทรัพย์สิน เช่น ที่ดิน ซึ่งเดิมไม่ได้นำมาใช้ประโยชน์ และสามารถระบุเหตุการณ์ที่เป็นโอกาสที่จะได้ใช้ประโยชน์จากทรัพย์สินนั้น เพื่อเพิ่มรายได้ให้แก่รัฐวิสาหกิจหรืออาจคิดเป็นโครงการหรือกิจกรรมใหม่ๆ ขึ้นมา ที่สามารถก่อให้เกิดประโยชน์ต่อรัฐวิสาหกิจได้ ซึ่งในที่สุดแล้วจะมีผลให้มูลค่าขององค์กรเพิ่มขึ้น

### การบริหารความเสี่ยงเพื่อเพิ่มมูลค่าขององค์กร (Value Enhancement)

การบริหารความเสี่ยงเพื่อเพิ่มมูลค่าขององค์กร (Value Enhancement) คือ การที่รัฐวิสาหกิจมีการระบุ ประเมิน และจัดการความเสี่ยงที่อาจเกิดขึ้นเพื่อลดโอกาสที่จะเกิด และ/หรือผลกระทบต่อการบรรลุเป้าหมายหรือวัตถุประสงค์ เพื่อช่วยเพิ่มความมั่นใจอย่างสมเหตุสมผล (Reasonable Assurance) ว่ารัฐวิสาหกิจจะสามารถดำเนินงานให้บรรลุเป้าหมายหรือวัตถุประสงค์ที่ดีกว่าที่คาดไว้ซึ่งจะมีผลต่อการเพิ่มมูลค่าขององค์กรนั่นเอง

### ประโยชน์ของการบริหารความเสี่ยงเพื่อเพิ่มมูลค่าขององค์กร (Value Enhancement)

การบริหารความเสี่ยงที่มีประสิทธิผล นอกจากจะช่วยลดความสูญเสียที่อาจเกิดขึ้นจากเหตุการณ์ต่างๆ แล้วยังช่วยส่งเสริมให้เกิดวัฒนธรรมองค์กรที่มีความตระหนักถึงความเสี่ยง การเห็นความสำคัญของการปฏิบัติตามมาตรการป้องกันและบรรเทาความเสี่ยง ซึ่งจะทำให้การทำงานเป็นไปด้วยความรัดกุม

และรอบคอบ และในที่สุดจะช่วยให้รัฐวิสาหกิจมีความมั่นใจอย่างสมเหตุสมผลว่าจะสามารถบรรลุ เป้าหมายหรือวัตถุประสงค์ที่ตั้งไว้ นอกจากนี้ การบริหารความเสี่ยงยังช่วยสนับสนุนการเป็นองค์กร แห่งการเรียนรู้ (Learning Organization) ซึ่งจะส่งเสริมพัฒนาทักษะ ความสามารถ ความคิด สร้างสรรค์ของบุคลากร รวมถึงส่งเสริมและสร้างบรรยากาศเพื่อก่อให้เกิดนวัตกรรมและการสร้างสรรค์ ขององค์กรด้วย

**ตัวอย่าง:** รัฐวิสาหกิจมีทรัพย์สิน เช่น ที่ดิน ซึ่งกำหนดเป้าหมายขององค์กรไว้ว่าต้องการรายได้ จากการปล่อยเช่าเพิ่มขึ้นร้อยละ 20 ภายในสิ้นปีบัญชี จึงจัดให้มีการบริหารความเสี่ยงของการบริหารจัดการทรัพย์สินดังกล่าว โดยคำนึงถึงเหตุการณ์ต่างๆ ที่อาจเกิดขึ้นแล้วจะทำให้รัฐวิสาหกิจมีรายได้ ต่ำกว่าเป้าหมายที่กำหนด และดำเนินการตามแผนการบริหารจัดการความเสี่ยง เพื่อลดโอกาส ที่จะเกิด และ/หรือผลกระทบของเหตุการณ์ต่างๆ เหล่านั้น ผลที่ได้จากการปฏิบัติตามแผนการบริหาร จัดการความเสี่ยงนี้ อาจทำให้รัฐวิสาหกิจมีรายได้เพิ่มขึ้นมากกว่าร้อยละ 20 หมายความว่า รัฐวิสาหกิจสามารถเพิ่มมูลค่าขององค์กรได้จากการบริหารความเสี่ยง ทั้งนี้ มูลค่าขององค์กรอาจอยู่ใน รูปแบบที่เป็นตัวเงิน เช่น รายได้ที่เพิ่มขึ้น ค่าใช้จ่ายที่ลดลง หรืออยู่ในรูปแบบที่ไม่ใช่ตัวเงิน เช่น ความพึงพอใจของผู้เช่า

## องค์ประกอบที่ 3 ผลการปฏิบัติงาน (Performance)

### หลักเกณฑ์

รัฐวิสาหกิจควรมีการระบุและประเมินความเสี่ยงที่ชัดเจนและเป็นระบบ โดยการประเมินความเสี่ยงจะมีการพิจารณาทั้งด้านโอกาสที่ความเสี่ยงจะเกิดขึ้น และผลกระทบหากความเสี่ยงเกิดขึ้นจริง ช่วงระยะเวลาที่ใช้ในการประเมินความเสี่ยงควรสอดคล้องกับกลยุทธ์และวัตถุประสงค์ในการประกอบกิจการ และสามารถทำการประเมินได้ตั้งแต่ระดับองค์กรไปจนถึงระดับหน่วยงาน ภายหลังจากการประเมินความเสี่ยง รัฐวิสาหกิจควรมีการจัดลำดับความสำคัญของความเสี่ยงตามระดับความรุนแรงของความเสี่ยง และช่วงความเบี่ยงเบนของระดับความเสี่ยงที่องค์กรยอมรับได้ (RA) เพื่อให้สามารถจัดสรรทรัพยากรในการตอบสนองต่อความเสี่ยงได้อย่างเหมาะสม

### แนวปฏิบัติที่ 1

รัฐวิสาหกิจควรกำหนดให้มีการระบุความเสี่ยงที่ชัดเจน ครอบคลุมทุกการดำเนินงานขององค์กร เช่น ความเสี่ยงด้านกลยุทธ์ (Strategic Risk) ความเสี่ยงด้านการปฏิบัติการ (Operational Risk) ความเสี่ยงด้านการเงิน (Financial Risk) ความเสี่ยงด้านกฎระเบียบ/ข้อบังคับ (Compliance Risk) รวมถึงความเสี่ยงใหม่ๆ (Emerging Risk) ที่อาจส่งผลกระทบต่อผลการปฏิบัติงานตามกลยุทธ์และวัตถุประสงค์ในการประกอบกิจการ จากนั้นรัฐวิสาหกิจควรจัดทำทะเบียนความเสี่ยงเพื่อรวบรวมรายการข้อมูลความเสี่ยงที่องค์กรเผชิญอยู่

### คู่มือปฏิบัติ

1. รัฐวิสาหกิจควรระบุปัจจัยเสี่ยง (Risk Factor) ที่อาจเกิดขึ้นและส่งผลกระทบต่อกลยุทธ์และการดำเนินงานขององค์กร ทั้งนี้ ปัจจัยเสี่ยงที่ระบุนั้นต้องสามารถเชื่อมโยงกับวัตถุประสงค์ในการประกอบกิจการและดัชนีชี้วัดขององค์กรได้ การระบุความเสี่ยงมีขั้นตอนการปฏิบัติดังต่อไปนี้
  - 1) ศึกษาและพิจารณาเหตุการณ์ที่อาจเกิดขึ้นที่จะทำให้องค์กรไม่บรรลุวัตถุประสงค์ต่างๆ ตามที่กำหนดเบื้องต้น รวมถึงองค์กรควรระบุโอกาสที่เกิดขึ้นจากความเสี่ยง เช่น ความก้าวหน้าทางเทคโนโลยีปัญญาประดิษฐ์ (Artificial Intelligence: AI) จะช่วยให้องค์กรประหยัดเวลาในการวิเคราะห์ข้อมูลจำนวนมาก อย่างไรก็ตาม ปัญญาประดิษฐ์ (AI) อาจก่อให้เกิดความเสี่ยงในด้านความปลอดภัยของข้อมูล ซึ่งอาจทำให้เกิดการรั่วไหลของข้อมูลได้
  - 2) สรุปประเด็นความเสี่ยงที่อาจเกิดขึ้นซึ่งมีผลกระทบต่อการบรรลุวัตถุประสงค์ และสาเหตุของความเสี่ยงดังกล่าวให้เป็นลายลักษณ์อักษร เพื่อหารือร่วมกันระหว่างผู้บริหารระดับสูง โดยเหตุการณ์ที่มีผลกระทบในเชิงลบผู้บริหารต้องประเมินและจัดการความเสี่ยงนั้น ทั้งนี้ ในกรณี

ที่รัฐวิสาหกิจมีบริษัทย่อยหรือบริษัทร่วม ควรระบุความเสี่ยงของบริษัทย่อยและบริษัทร่วมด้วย เพื่อให้มั่นใจว่าการบริหารความเสี่ยงเป็นไปอย่างมีประสิทธิภาพและครอบคลุมทั้งรัฐวิสาหกิจ บริษัทย่อย และบริษัทร่วม

### สาเหตุของความเสียหาย

การวิเคราะห์เหตุการณ์ที่เป็นสาเหตุของความเสียหายเป็นส่วนหนึ่งของกระบวนการระบุความเสี่ยง ผู้วิเคราะห์ควรให้ความสำคัญต่อการระบุและบันทึกสาเหตุของความเสียหาย รวมถึงผลกระทบที่เกิดขึ้น เพื่อให้การกำหนดแผนจัดการความเสี่ยงสามารถแก้ไขได้ตรงกับสาเหตุและสามารถลดความเสี่ยงได้อย่างมีประสิทธิภาพและประสิทธิผลมากขึ้น เนื่องจากมีความเป็นไปได้ว่าความเสี่ยงข้อหนึ่งๆ อาจมีสาเหตุมากกว่าหนึ่งข้อหรือความเสี่ยงหลายข้ออาจมีสาเหตุร่วมกัน หรือความเสี่ยงข้อหนึ่งๆ อาจมีผลกระทบหลายอย่าง หรือความเสี่ยงหลายข้ออาจมีผลกระทบที่เหมือนกัน เป็นต้น

**ตัวอย่าง:** หากวัตถุประสงค์ขององค์กร คือ “การดำเนินธุรกิจให้มั่นคงและมีคุณภาพ” เหตุการณ์ที่อาจเกิดขึ้นและทำให้องค์กรไม่บรรลุวัตถุประสงค์ เช่น

- การที่อุปสงค์ของสินค้าและ/หรือบริการที่องค์กรดำเนินงานอยู่ลดลง
- การขาดความต่อเนื่องในการดำเนินงาน
- การที่คุณภาพสินค้าและ/หรือบริการลดต่ำลง เป็นต้น

รายการเหตุการณ์/ความเสี่ยงดังกล่าว อาจมาจากสาเหตุเดียวกัน คือ เหตุการณ์วิกฤติน้ำท่วม เนื่องจากน้ำท่วมส่งผลกระทบต่อสภาพเศรษฐกิจของประเทศ และความสามารถในการใช้จ่ายของประชาชนส่งผลกระทบต่ออุปสงค์ลดลง นอกจากนี้ น้ำท่วมยังทำให้การผลิตหยุดชะงักหรือช่องทางจำหน่ายต้องหยุดการให้บริการ และน้ำท่วมยังทำให้คุณภาพในการให้บริการลดลง

ในขณะเดียวกัน การขาดความต่อเนื่องในการดำเนินงานอาจเกิดจากสาเหตุอื่นได้ เช่น การเกิดเหตุการณ์ความไม่สงบทางการเมือง การเกิดความเสียหายด้านระบบเทคโนโลยีสารสนเทศ ในการบริหารจัดการธุรกิจ การที่ผู้ส่งวัตถุดิบงดการส่งสินค้าให้กับกระบวนการผลิตในองค์กร เป็นต้น



#### Tip:

ในการระบุความเสี่ยง จะต้องระบุสาเหตุของความเสียหายด้วยทุกครั้ง และควรระบุให้ครบทุกสาเหตุที่ทำให้เกิดความเสี่ยงดังกล่าว เพื่อให้ผู้บริหารสามารถกำหนดแผนการบริหารจัดการความเสี่ยงให้สามารถบริหารจัดการความเสี่ยงได้ตรงกับสาเหตุที่ทำให้เกิดความเสี่ยง และสามารถลดความเสี่ยงได้อย่างมีประสิทธิภาพและประสิทธิผล

## ตารางอธิบายความเสี่ยงและสาเหตุความเสี่ยง

เลขที่ความเสี่ยง	ความเสี่ยง	เลขที่สาเหตุ	สาเหตุความเสี่ยง
R1	การที่อุปสงค์ของสินค้าและ/หรือบริการที่องค์กรดำเนินงานอยู่ลดลง	C1 	<b>เหตุการณ์วิกฤติน้ำท่วม</b> เนื่องจากน้ำท่วมส่งผลกระทบต่อสภาพเศรษฐกิจของประเทศและความสามารถในการใช้จ่ายของประชาชนส่งผลกระทบต่ออุปสงค์ลดลง
R2	การขาดความต่อเนื่องในการดำเนินงาน	C1 	<b>เหตุการณ์วิกฤติน้ำท่วม</b> เนื่องจากน้ำท่วมส่งผลให้การผลิตหยุดชะงักหรือช่องทางจำหน่ายต้องหยุดการให้บริการ
		C2	การเกิดเหตุการณ์ความไม่สงบทางการเมือง
		C3	การเกิดความเสียหายด้านระบบเทคโนโลยีสารสนเทศในการบริหารจัดการธุรกิจ
		C4	การที่ผู้ส่งวัตถุดิบงดการส่งสินค้าให้กับกระบวนการผลิตในองค์กร
R3	การที่คุณภาพสินค้าและ/หรือบริการลดต่ำลง	C1 	<b>เหตุการณ์วิกฤติน้ำท่วม</b> เนื่องจากน้ำท่วมส่งผลให้คุณภาพในการให้บริการลดลง

**หมายเหตุ:**  หมายถึง สาเหตุเดียวกันที่ทำให้เกิดความเสี่ยงมากกว่าหนึ่งความเสี่ยง

### เทคนิคการระบุความเสี่ยง

การระบุความเสี่ยงสามารถจัดทำโดยบุคคลหรือกลุ่มบุคคล เช่น คณะผู้บริหาร พนักงานที่เกี่ยวข้อง เป็นต้น โดยอาศัยเทคนิคและเครื่องมือต่างๆ เช่น การประชุมเชิงปฏิบัติการ การสัมภาษณ์ หรือการสำรวจความคิดเห็น รายการเหตุการณ์ที่อาจเกิดขึ้น การเปรียบเทียบกับองค์กรอื่น การรายงานเหตุการณ์สูญเสีย และการวิเคราะห์แผนภาพขั้นตอนการปฏิบัติงาน เป็นต้น โดยมีคำอธิบายเทคนิคต่างๆ ดังนี้

#### 1) ผู้ปฏิบัติงานเป็นผู้ระบุความเสี่ยง

ผู้ปฏิบัติงานเป็นผู้ที่มีข้อมูล ความรู้ และความเข้าใจในการปฏิบัติงานของตน และสามารถระบุความเสี่ยงที่อาจเกิดขึ้นจากการปฏิบัติงานได้ เช่น องค์กรที่มีการดำเนินธุรกิจหลักที่เกี่ยวข้องกับการปฏิบัติงานในโรงงาน พนักงานในสวนปฏิบัติงานในโรงงานจะสามารถระบุความเสี่ยงที่อาจทำให้เครื่องจักรหยุดการปฏิบัติงานได้อย่างชัดเจน

2) **การสัมภาษณ์หรือการสำรวจความคิดเห็นด้านความเสี่ยง เพื่อรับฟังความคิดเห็นของผู้อื่น**  
ในการระบุความเสี่ยงบางครั้งผู้ปฏิบัติงานอาจมองไม่เห็นความเสี่ยงของตนเอง ดังนั้น การรับฟังความคิดเห็นของผู้อื่นในการระบุความเสี่ยง จึงเป็นอีกแนวทางหนึ่งที่จะช่วยให้สามารถระบุความเสี่ยงที่ครอบคลุมมากยิ่งขึ้น การสัมภาษณ์และการสำรวจความคิดเห็นผ่านแบบสอบถามสามารถใช้เป็นเทคนิคที่เป็นประโยชน์สำหรับการรวบรวมข้อมูลความเสี่ยง โดยข้อมูลที่รวบรวมได้จากการสัมภาษณ์หรือการสำรวจความคิดเห็นสามารถใช้เป็นจุดเริ่มต้นสำหรับการหาหรือในการประชุมเชิงปฏิบัติการความเสี่ยงได้เป็นอย่างดี

3) **การวิเคราะห์แผนภาพขั้นตอนการปฏิบัติงาน**

เป็นการจัดทำแผนภาพขั้นตอนการปฏิบัติงาน อาจอยู่ในรูปแบบแผนภาพกระบวนการ (Process Map) หรือคำอธิบาย หรือทั้งสองอย่างรวมกัน เพื่อแสดงความสัมพันธ์ระหว่างกันของข้อมูลนำเข้า งาน ผลลัพธ์และความรับผิดชอบ เพื่อช่วยในการทำความเข้าใจการดำเนินงานปัจจุบันหรือกระบวนการตามแนวปฏิบัติที่ดี (Best Practice) และสามารถระบุปัจจัยความเสี่ยงในระดับกระบวนการได้

4) **การประชุมเชิงปฏิบัติการ (Workshops)**

เป็นวิธีที่ใช้โดยทั่วไปในการระบุความเสี่ยง การประชุมเชิงปฏิบัติการควรดำเนินการโดยผู้ประสานงาน (Facilitator) ที่มีความเชี่ยวชาญเพื่อให้แน่ใจว่าสามารถบรรลุวัตถุประสงค์ภายใต้กระบวนการและเวลาที่กำหนด และสามารถเกิดองค์ความรู้ร่วมกันและพัฒนารายการความเสี่ยงต่างๆ ที่เกี่ยวข้องกับกลยุทธ์และวัตถุประสงค์ในการประกอบกิจการ สิ่งที่ต้องระมัดระวังคือ การคัดเลือกผู้เข้าร่วมการประชุมเชิงปฏิบัติการให้เหมาะสม โดยผู้เข้าร่วมประชุมจะต้องเป็นผู้ที่เกี่ยวข้องกับวัตถุประสงค์ หรือมีความรู้ในประเด็นหรือกระบวนการที่จะหาหรือในการประชุมเชิงปฏิบัติการและสามารถมีส่วนร่วมในการหาหรือดังกล่าว

5) **การเปรียบเทียบกับองค์กรอื่น**

เป็นการศึกษาค้นคว้าและเปรียบเทียบกับองค์กรอื่นทั้งในและต่างประเทศ ซึ่งจะช่วยให้รัฐวิสาหกิจสามารถระบุความเสี่ยงในอุตสาหกรรมหรือในหน่วยงานได้ครอบคลุมมากขึ้น เทคนิคการค้นคว้าและเปรียบเทียบนี้ ทำได้โดยการศึกษาวารสารวิชาการที่เกี่ยวข้อง การเข้าร่วมสัมมนาที่เกี่ยวข้องกับการดำเนินงานขององค์กร การสอบถามองค์กรที่เกี่ยวข้องในประเทศและต่างประเทศ การค้นหาข้อมูลทางอินเทอร์เน็ต การสอบถามความคิดเห็น การหาหรืออย่างเป็นทางการและไม่เป็นทางการกับตัวแทนจากองค์กรอื่นๆ

**ตัวอย่าง:** องค์กรอยู่ในธุรกิจด้านสาธารณูปโภค และมีทิศทางที่จะขยายการดำเนินงานไปในธุรกิจอื่นที่เกี่ยวข้องเนื่อง เช่น ธุรกิจพลังงานแสงอาทิตย์ หากองค์กรมีข้อมูลด้านความเสี่ยงในธุรกิจดังกล่าวไม่เพียงพอ องค์กรอาจเทียบเคียงข้อมูลกับองค์กรอื่นๆ ที่ดำเนินธุรกิจพลังงาน

แสงอาทิตย์ในประเทศ หรือต่างประเทศ เพื่อช่วยให้สามารถวิเคราะห์และระบุเหตุการณ์ความเสี่ยงได้อย่างเหมาะสม

**6) การแสวงหาข้อมูลเพื่อช่วยในการระบุความเสี่ยง**

เป็นการสืบค้นข้อมูลจากแหล่งข้อมูลภายในและภายนอกจากหน่วยงานหรือแหล่งข้อมูลที่น่าเชื่อถือ เพื่อช่วยในการคาดการณ์เหตุการณ์ที่อาจเกิดขึ้นในอนาคต

- **แหล่งข้อมูลภายใน**

เช่น รายงานการตรวจสอบภายใน หรือกับหน่วยงานบริหารความเสี่ยง ประเด็นความเสี่ยงของปีก่อนหน้า

- **แหล่งข้อมูลภายนอก**

เช่น บทความทางธุรกิจ ข้อเสนอจากผู้เชี่ยวชาญภายนอก องค์กรกำกับดูแล รายงานการวิเคราะห์ของภาคอุตสาหกรรมที่รัฐวิสาหกิจนั้นดำเนินกิจการอยู่

**7) การพิจารณาโดยผู้เชี่ยวชาญภายนอก**

เป็นการจัดให้มีผู้เชี่ยวชาญภายนอกที่มีความรู้ที่เกี่ยวข้องในความเสี่ยงนั้นๆ เข้ามามีส่วนร่วมในการระบุเหตุการณ์ความเสี่ยงด้วย โดยอาจมีการจัดทำรายงานเป็นการเฉพาะเรื่อง จากนั้นองค์กรอาจนำข้อมูลดังกล่าวมาพิจารณาประกอบกับสภาพแวดล้อมขององค์กร เพื่อให้เชื่อมโยงกับความเสี่ยงขององค์กรยิ่งขึ้น และสอดคล้องกับวิธีการบริหารความเสี่ยงที่ใช้อยู่โดยทั่วไปในองค์กร

**8) ระบบคอมพิวเตอร์เสมือนมนุษย์ (Cognitive Computing)**

เป็นเครื่องมือที่ช่วยให้องค์กรสามารถรวบรวมและวิเคราะห์ข้อมูลขนาดใหญ่ (Big Data) ทั้งจากภายในและภายนอกองค์กร เพื่อระบุแนวโน้มในอนาคตและข้อมูลเชิงลึกที่มีประโยชน์ในการทำความเข้าใจเกี่ยวกับความเสี่ยงใหม่และการเปลี่ยนแปลงของความเสี่ยงที่มีอยู่ในปัจจุบันได้อย่างมีประสิทธิภาพ

**9) การติดตามข้อมูล (Data Tracking)**

เป็นการติดตามข้อมูลจากเหตุการณ์ในอดีตเพื่อช่วยคาดการณ์เหตุการณ์ที่อาจเกิดขึ้นในอนาคตพร้อมระดับความรุนแรง ข้อมูลดังกล่าวสามารถนำมาใช้เพื่อทำความเข้าใจความสัมพันธ์ระหว่างข้อมูลต่างๆ และพัฒนาแบบจำลองที่ใช้ในการคาดการณ์และวิเคราะห์สาเหตุ

ทั้งนี้ หากข้อมูลที่ได้จากการระบุความเสี่ยงเป็นข้อมูลเชิงปริมาณที่มีส่วนสำคัญในการวิเคราะห์ความเสี่ยง ผู้บริหารควรมีการสอบถามข้อมูลให้ชัดเจนว่า ข้อมูลดังกล่าวสะท้อนถึงความเสี่ยงหรือเป็นส่วนหนึ่งในการใช้วิเคราะห์ความเสี่ยงได้อย่างถูกต้อง เหมาะสมกับช่วงระยะเวลาที่ใช้ในการวิเคราะห์ และแสดงถึงกิจกรรมการปฏิบัติงานที่เกี่ยวข้องในองค์กร นอกจากนี้ ผู้บริหารควรให้ความมั่นใจว่าข้อมูลที่ใช้มีการปรับปรุงให้เป็นปัจจุบันอย่างสม่ำเสมอ



Tip:

ในการระบุความเสี่ยง ผู้วิเคราะห์ควรพิจารณาทั้งเหตุการณ์ที่เคยเกิดขึ้นในอดีตและเหตุการณ์ที่อาจเกิดขึ้นในอนาคต



Tip:

การระบุความเสี่ยง ต้องเป็นการระบุเหตุการณ์ที่เมื่อเกิดขึ้นแล้ว จะส่งผลกระทบต่อการบรรลุวัตถุประสงค์ขององค์กร ไม่ใช่ประโยคปฏิเสธของวัตถุประสงค์ และคำอธิบายความเสี่ยงควรใช้โครงสร้างประโยคที่เป็นมาตรฐานเดียวกัน เช่น

- ความเป็นไปได้ของ [อธิบายเหตุการณ์หรือสถานการณ์ที่อาจเกิดขึ้น] และผลกระทบที่เกี่ยวข้อง [อธิบายวัตถุประสงค์ในการประกอบกิจการที่เฉพาะเจาะจงขององค์กร]  
เช่น ความเป็นไปได้ของการเปลี่ยนแปลงในอัตราแลกเปลี่ยนเงินตราต่างประเทศและผลกระทบที่เกี่ยวข้องกับรายได้
- ความเสี่ยงต่อ [อธิบายประเภทความเสี่ยงที่กำหนดโดยองค์กร] ที่เกี่ยวข้องกับ [อธิบายเหตุการณ์หรือสถานการณ์ที่เป็นไปได้] และ [อธิบายผลกระทบที่เกี่ยวข้อง]



Tip:

เมื่อระบุความเสี่ยงเป็นที่เรียบร้อยแล้ว ก่อนการดำเนินการในขั้นตอนต่อไป ผู้วิเคราะห์ควรทบทวนรายการความเสี่ยงทั้งหมด เพื่อพิจารณาความสัมพันธ์ของความเสี่ยงทั้งหมด ซึ่งบางความเสี่ยง อาจจะเป็นสาเหตุที่ทำให้เกิดอีกความเสี่ยงหนึ่ง ดังนั้น ผู้วิเคราะห์ควรพิจารณาให้ถี่ถ้วน เพื่อให้การประเมินความเสี่ยงเป็นไปอย่างมีประสิทธิภาพและประสิทธิผลมากยิ่งขึ้น

2. ผู้บริหารควรมีการจัดกลุ่มความเสี่ยงที่ชัดเจน เพื่อให้มีความสะดวก คล่องตัวในการปฏิบัติงาน และมีความเข้าใจในความเสี่ยง ชนิดความเสี่ยง ได้อย่างเป็นระเบียบและเป็นไปในแนวทางเดียวกัน โดยอาจแบ่งประเภทของความเสี่ยงเป็น 4 ประเภท ดังต่อไปนี้

- 1) **ความเสี่ยงด้านกลยุทธ์ (Strategic Risk)** คือ ความเสี่ยงที่อาจก่อให้เกิดการสูญเสียทางการเงินหรือศักยภาพในการแข่งขัน อันเนื่องมาจากกระบวนการตัดสินใจเชิงกลยุทธ์ที่ไม่เหมาะสม ตัวอย่างความเสี่ยงด้านกลยุทธ์ เช่น
  - การเปลี่ยนแปลงทางการเมือง
  - การไม่สามารถเพิ่มรายได้และลดค่าใช้จ่ายได้ตามเป้าหมายที่กำหนด
  - การเปลี่ยนแปลงความต้องการของลูกค้าไปสู่ผลิตภัณฑ์ซึ่งผลิตโดยผู้ผลิตที่มุ่งเน้นส่งเสริมด้านสิ่งแวดล้อม สังคมและการกำกับดูแล (Environmental Social and Governance: ESG)
  - การเพิ่มความสนใจของนักลงทุนในประเด็นด้านสิ่งแวดล้อม สังคม และการกำกับดูแล (ESG) เช่น ประเด็นความหลากหลายของคณะกรรมการ การตัดไม้ทำลายป่า และสิทธิมนุษยชน
  - การวิเคราะห์การควมรวมและซื้อกิจการอย่างผิดพลาด
- 2) **ความเสี่ยงด้านการปฏิบัติการ (Operational Risk)** คือ ความเสี่ยงที่อาจส่งผลกระทบต่อการทำงานขององค์กร อันเนื่องมาจากความผิดพลาดที่เกิดจากการปฏิบัติงานของบุคลากร ระบบหรือกระบวนการต่างๆ ตัวอย่างความเสี่ยงด้านการปฏิบัติการ เช่น
  - การขาดบุคลากรที่มีคุณภาพ
  - การก่อการร้าย
  - การใช้งานระบบเทคโนโลยีสารสนเทศได้ไม่เต็มประสิทธิภาพ
  - การเปลี่ยนแปลงสภาพภูมิอากาศและการเพิ่มขึ้นของภัยธรรมชาติ เช่น อุทกภัย อัคคีภัย ภัยพิบัติภัย ซึ่งส่งผลกระทบต่อการทำงานและความต่อเนื่องทางธุรกิจ
- 3) **ความเสี่ยงด้านการเงิน (Financial Risk)** คือ ความเสี่ยงที่เกิดจากความผันผวนของตัวแปรทางการเงิน เช่น อัตราแลกเปลี่ยน อัตราดอกเบี้ย สภาพคล่องทางการเงิน และราคาสินค้าโภคภัณฑ์ (Commodity) เป็นต้น ซึ่งก่อให้เกิดการสูญเสียทางการเงิน ตัวอย่างความเสี่ยงด้านการเงิน เช่น
  - ความเสี่ยงด้านเครดิต
  - ความเสี่ยงด้านสภาพคล่อง
  - การขาดทุนจากอัตราแลกเปลี่ยน
  - ความผันผวนของราคาวัตถุดิบ
  - การเพิ่มภาษีจากกฎหมายภาษีคาร์บอน
- 4) **ความเสี่ยงด้านกฎระเบียบ/ข้อบังคับ (Compliance Risk)** คือ ความเสี่ยงที่เกิดจากการละเมิดหรือไม่ปฏิบัติตามนโยบาย กระบวนการ หรือการควบคุมต่างๆ ที่กำหนดขึ้น เพื่อให้สอดคล้องกับกฎระเบียบ ข้อบังคับ ข้อสัญญา และข้อกำหนดที่เกี่ยวข้องกับการดำเนินงานขององค์กร ตัวอย่างความเสี่ยงด้านกฎระเบียบ/ข้อบังคับ เช่น

- การทุจริต
- การถูกฟ้องร้อง ร้องเรียนจากผู้มีส่วนได้เสีย
- การไม่ปฏิบัติตามกฎ ระเบียบ ที่เกี่ยวข้องกับรัฐวิสาหกิจแต่ละแห่ง
- การเปิดเผยข้อมูลการปล่อยมลพิษที่เป็นเท็จหรือมีการทุจริต ทำให้เสียค่าปรับและถูกลงโทษ รวมไปถึงการสูญเสียความไว้วางใจจากผู้บริโภค

**ตัวอย่าง:** หากองค์กรมีรายการความเสี่ยงด้านอัตราดอกเบี้ย ความเสี่ยงด้านอัตราแลกเปลี่ยน และความเสี่ยงด้านสภาพคล่อง ผู้บริหารควรจัดรวมความเสี่ยงดังกล่าวให้อยู่ในกลุ่มความเสี่ยงทางการเงิน (F) และทำการประเมินความเสี่ยง โดยการประเมินควรมีการพิจารณาด้วยว่าความเสี่ยงแต่ละเรื่องดังกล่าวควรจะมีการรายงานต่อผู้บริหารหรือผู้รับผิดชอบคนใด และความถี่เท่าใด เพื่อให้การประเมินความเสี่ยงในด้านต่างๆ นั้นสะท้อนภาพการดำเนินงานและความเสี่ยงโดยรวมขององค์กรที่ถูกต้องและมีประสิทธิภาพ

ทั้งนี้ อาจพิจารณากำหนดประเภทของความเสี่ยงเป็นประการอื่นก็ได้

3. รัฐวิสาหกิจควรมีการวิเคราะห์ความเสี่ยงที่เกิดขึ้นใหม่ (Emerging Risk) ซึ่งเป็นความเสี่ยงที่มีโอกาสที่จะเกิดต่ำ แต่ผลกระทบรุนแรงมากต่อองค์กรและควรจัดหาแนวทางการบริหารความเสี่ยงดังกล่าวอย่างเหมาะสม

**ความเสี่ยงที่เกิดขึ้นใหม่ (Emerging Risk)** คือ ลักษณะความเสี่ยงที่ไม่สามารถคาดการณ์ได้ และไม่สามารถจัดการใดๆ โดยองค์กรหนึ่งองค์กรใดได้ ลักษณะความเสี่ยงอาจปรากฏทั้งในรูปแบบทางด้านเศรษฐกิจ สังคม สิ่งแวดล้อม ประชากร

**ตัวอย่างของความเสี่ยงที่เกิดขึ้นใหม่ (Emerging Risk)**

- วิกฤติเศรษฐกิจโลกอย่างรุนแรง
- การใช้ข้อมูลที่ไม่ถูกต้องหรือให้ข้อมูลที่เป็นเท็จ (Misinformation and Disinformation)
- สภาพอากาศที่รุนแรง (Extreme Weather Events)
- ความขัดแย้งระหว่างรัฐ (State-based Armed Conflict)
- การแบ่งแยกทางสังคม (Societal Polarization)
- การจารกรรมและสงครามทางไซเบอร์ (Cyber Espionage and Warfare)
- การสูญเสียความหลากหลายทางชีวภาพและการล่มสลายของระบบนิเวศ (Biodiversity Loss and Ecosystem Collapse)
- การระบาดของโรคติดต่อหรือโรคระบาด (Infection Diseases)

การบริหารจัดการ Emerging Risk แตกต่างจากการบริหารความเสี่ยงทั่วไป (Traditional Risk Management) กล่าวคือ การบริหารจัดการ Emerging Risk จะมุ่งเน้นในประเด็นต่อไปนี้

- การทำความเข้าใจในเหตุการณ์ต่างๆ ที่อาจเกิดขึ้นพร้อมๆ กัน

- ความพร้อมที่จะตอบสนองต่อเหตุการณ์ในอนาคตที่อาจเกิดขึ้นในลักษณะที่แตกต่างไปจากที่คาดการณ์ไว้เดิม
- การทำความเข้าใจว่าความเสี่ยงใดที่จะกระทบต่อวัตถุประสงค์ขององค์กรมากที่สุด
- ความเสี่ยงที่เกิดขึ้นใหม่ (Emerging Risk) ควรพิจารณาโอกาสเกิดในระยะยาวมากกว่าความเสี่ยงทั่วไป และพิจารณาผลกระทบที่มีต่อเป้าหมายทั้งระยะสั้นและระยะยาว
- รัฐวิสาหกิจสามารถประเมินและจัดลำดับความสำคัญความเสี่ยงดังกล่าว โดยขึ้นอยู่กับความเข้าใจเรื่องความสัมพันธ์ของความเสี่ยงต่างๆ ทั้งภายในรัฐวิสาหกิจและปฏิสัมพันธ์ที่มีกับสภาพแวดล้อมภายนอก
- รัฐวิสาหกิจอาจริเริ่มการวางแผนการบริหารจัดการความเสี่ยงหลายๆ แบบในเวลาเดียวกัน

สิ่งสำคัญที่รัฐวิสาหกิจพึงปฏิบัติ คือ การปรับตัวให้เข้ากับสภาวะการณ์ต่างๆ และสามารถที่จะติดต่อสื่อสารภายในและภายนอกองค์กรถึงเรื่องความเสี่ยงดังกล่าวกับผู้มีส่วนได้เสียทุกกลุ่ม

4. รัฐวิสาหกิจควรกำหนดให้มีการจัดทำทะเบียนความเสี่ยง (Risk Register) อันเป็นรายการข้อมูลความเสี่ยงที่องค์กรเผชิญอยู่ โดยจัดแบ่งประเภทความเสี่ยงเป็นกลุ่มต่างๆ และกำหนดนิยามความเสี่ยงแต่ละประเภท เพื่อให้การปฏิบัติตามกระบวนการบริหารความเสี่ยงเป็นไปในแนวทางเดียวกัน รัฐวิสาหกิจสามารถนำรูปแบบทะเบียนความเสี่ยงดังกล่าวมาปรับใช้เพื่อบันทึกข้อมูลความเสี่ยง นอกจากนี้ ทะเบียนความเสี่ยง (Risk Register) ยังสามารถนำมาใช้เป็นเครื่องมือในการติดตามความเสี่ยงได้อีกด้วย รวมถึงรัฐวิสาหกิจควรปรับปรุงทะเบียนความเสี่ยง (Risk Register) ให้เป็นปัจจุบันอยู่เสมอ เพื่อสะท้อนการเปลี่ยนแปลงที่เกิดขึ้น

ทะเบียนความเสี่ยง (Risk Register)													
วัตถุประสงค์ เพื่อพัฒนาทรัพยากรบุคคลให้มีศักยภาพสอดคล้องกับกลยุทธ์ขององค์กร และมีความรู้ความสามารถในการสนับสนุนการบรรลุเป้าหมายขององค์กรอย่างยั่งยืน													
1	2	3	4			5	6			7	8	9	10
ชื่อ	ความเสี่ยง	รายละเอียดความเสี่ยง	ผลการประเมินความเสี่ยงก่อนมาตรการควบคุม (Inherent risk)			มาตรการจัดการความเสี่ยงที่ดำเนินการอยู่แล้วในปัจจุบัน	ผลการประเมินความเสี่ยงที่เหลืออยู่ (Residual risk)			ประเภทการตอบสนองต่อความเสี่ยง	แผนจัดการความเสี่ยง	เจ้าของความเสี่ยง	กำหนดการแล้วเสร็จ
			ผลกระทบ	โอกาสเกิด	ระดับความเสี่ยง		ผลกระทบ	โอกาสเกิด	ระดับความเสี่ยง				
1	Human Resource Risk	การไม่มีบุคลากรที่มีความรู้ความสามารถเนื่องจากการพัฒนาบุคลากรไม่ทันกับการเติบโตขององค์กร และการเปลี่ยนแปลงของสภาพแวดล้อม	4	4	สูงมาก	จัดให้มีการอบรมทั้งภายในและภายนอกองค์กรเป็นประจำทุกปี	3	2	ปานกลาง	ลดความเสี่ยง (Reduction)	1. ปรับปรุง HR Strategy ให้สอดคล้องกับกลยุทธ์ภาพรวมขององค์กร 2. จัดทำ Competency Gap Analysis และนำมาปรับปรุงเป็นแผนพัฒนาทรัพยากรบุคคล (IDP)	ผู้อำนวยการฝ่ายทรัพยากรบุคคล	ธันวาคม 25XX

## คำอธิบายหัวข้อในทะเบียนความเสี่ยง

- 1) วัตถุประสงค์ อาจแบ่งออกได้เป็น 3 ระดับ ดังนี้
  - (1) วัตถุประสงค์ระดับองค์กร พิจารณาเป้าหมายที่มีผลกระทบหรือสอดคล้องกับแผนยุทธศาสตร์ของรัฐวิสาหกิจ
  - (2) วัตถุประสงค์ระดับฝ่ายงาน พิจารณาเป้าหมายที่มีผลกระทบหรือสอดคล้องกับแผนปฏิบัติงานประจำปีของแต่ละฝ่ายงาน
  - (3) วัตถุประสงค์ระดับกระบวนการ พิจารณาเป้าหมายที่มีผลกระทบหรือสอดคล้องกับกระบวนการปฏิบัติงานนั้นๆทั้งนี้ รัฐวิสาหกิจอาจพิจารณาใช้วัตถุประสงค์ในด้านอื่นๆ ตามความเหมาะสม เช่น วัตถุประสงค์ของโครงการ เนื่องจากการระบุความเสี่ยงสามารถทำได้ในทุกระดับ ขึ้นอยู่กับว่ารัฐวิสาหกิจจะใช้วัตถุประสงค์ในระดับใดเป็นตัวตั้งต้น
- 2) ความเสี่ยง หมายถึง ความเป็นไปได้ของเหตุการณ์ที่อาจเกิดขึ้น และเป็นอุปสรรคต่อการบรรลุวัตถุประสงค์ในการประกอบกิจการ
- 3) รายละเอียดความเสี่ยง หมายถึง คำอธิบายอย่างละเอียด ซึ่งครอบคลุมถึงสาเหตุของความเสี่ยง ผลกระทบที่เกิดขึ้นหรืออาจเกิดขึ้นจากความเสี่ยงนั้นและข้อมูลอื่นๆ ที่เกี่ยวข้อง
- 4) ผลการประเมินความเสี่ยงก่อนมาตรการควบคุม (Inherent Risk) หมายถึง การประเมินความเสี่ยง ทั้งโอกาสที่จะเกิด (Likelihood) และผลกระทบ (Impact) โดยผู้บริหารยังไม่ได้ดำเนินการใดๆ เพื่อที่จะลดความรุนแรงของความเสี่ยงนั้น ทั้งนี้ การประเมินความเสี่ยงเป็นไปตามเกณฑ์ที่รัฐวิสาหกิจกำหนด
- 5) มาตรการจัดการความเสี่ยงที่ดำเนินการอยู่แล้วในปัจจุบัน หมายถึง การควบคุมกิจกรรมหรือมาตรการที่ดำเนินการอยู่ในปัจจุบัน เพื่อจัดการกับความเสี่ยงนั้นๆ
- 6) ผลการประเมินความเสี่ยงที่เหลืออยู่ (Residual Risk) หมายถึง การประเมินความเสี่ยง ทั้งโอกาสที่จะเกิด (Likelihood) และผลกระทบ (Impact) โดยคำนึงถึงการควบคุมหรือมาตรการจัดการความเสี่ยงที่ดำเนินการอยู่ในปัจจุบัน ทั้งนี้ การประเมินความเสี่ยงเป็นไปตามเกณฑ์ที่รัฐวิสาหกิจกำหนด
- 7) ประเภทการตอบสนองต่อความเสี่ยง ได้แก่ การยอมรับความเสี่ยง (Acceptance) การลดความเสี่ยง (Reduction) การหาผู้ร่วมรับความเสี่ยง (Sharing) การหลีกเลี่ยงความเสี่ยง (Avoidance) และการดำเนินการต่อ (Pursuing)
- 8) แผนจัดการความเสี่ยง หมายถึง แผนจัดการความเสี่ยงที่ต้องทำเพิ่มเติมซึ่งกำหนดโดยเจ้าของความเสี่ยง (Risk Owner)

- 9) เจ้าของความเสี่ยง (Risk Owner) หมายถึง ผู้รับผิดชอบหลักในการกำหนดแผนจัดการความเสี่ยง และกำหนดเวลาที่คาดว่าจะ การปฏิบัติตามแผนจัดการความเสี่ยงจะแล้วเสร็จ และติดตามความคืบหน้าของการนำแผนจัดการความเสี่ยงไปปฏิบัติและรายงานต่อหน่วยงานบริหารความเสี่ยง และคณะกรรมการบริหารความเสี่ยง (ถ้ามี)
- ผู้ที่ควรเป็นเจ้าของความเสี่ยง ได้แก่ ผู้ที่ได้รับผลกระทบมากที่สุดหากเหตุการณ์ความเสี่ยงนั้นเกิดขึ้น หรือผู้ที่มีความเกี่ยวข้องกับเหตุการณ์ความเสี่ยงนั้นโดยตรง ทั้งนี้ เจ้าของความเสี่ยง อาจมิใช่ผู้ที่ก่อให้เกิดความเสี่ยง แต่เป็นผู้ที่สามารถบริหารจัดการความเสี่ยงนั้นได้ดีที่สุด
- 10) กำหนดการแล้วเสร็จ หมายถึง กำหนดเวลาในการดำเนินงานตามแผนจัดการความเสี่ยงที่คาดว่าจะแล้วเสร็จ (วัน เดือน ปี) หากเป็นกิจกรรมที่ต้องดำเนินการอย่างต่อเนื่องควรระบุกำหนดเวลาที่จะเริ่มดำเนินการ และความถี่ เช่น เดือนละครั้ง หรือไตรมาสละครั้ง ให้ชัดเจนด้วย

## แนวปฏิบัติที่ 2

รัฐวิสาหกิจควรกำหนดเกณฑ์การประเมินความเสี่ยงและดำเนินการประเมินความเสี่ยงตามเกณฑ์ โดยจะต้องวิเคราะห์ที่มาของความเสี่ยงนั้นๆ โอกาสที่จะเกิดความเสี่ยงดังกล่าว และผลกระทบหากความเสี่ยงเกิดขึ้นจริง ทั้งนี้ การประเมินความเสี่ยงจะต้องประเมินทั้งความเสี่ยงก่อนมาตรการควบคุม (Inherent Risk) และความเสี่ยงที่เหลืออยู่ (Residual Risk)

### คู่มือปฏิบัติ

1. จากรายการความเสี่ยงที่มีภาระระบุไว้ในทะเบียนความเสี่ยง (Risk Register) รัฐวิสาหกิจควรประเมินว่าผลกระทบของความเสี่ยงเหล่านั้นเป็นไปในเชิงบวกหรือเชิงลบต่อการบรรลุวัตถุประสงค์ ตั้งแต่ระดับองค์กรไปจนถึงระดับหน่วยงาน ผู้บริหารควรระบุระดับความเสียหายที่อาจเกิดขึ้น โดยพิจารณาถึงโอกาสที่จะเกิด (Likelihood) และผลกระทบ (Impact) หากความเสี่ยงเกิดขึ้นจริง

**โอกาสที่จะเกิดหรือความเป็นไปได้ (Likelihood)** หมายถึง โอกาสที่เหตุการณ์หนึ่งเหตุการณ์ใดจะเกิดขึ้น ซึ่งอาจนำเสนอในรูปของความน่าจะเป็นหรือความถี่ของการเกิด

**ผลกระทบ (Impact)** หมายถึง ผลที่ตามมาหรือผลของความเสี่ยง โดยความเสี่ยงหนึ่งอาจมีผลกระทบที่เป็นไปได้หลากหลาย ผลกระทบของความเสี่ยงอาจเป็นผลในเชิงบวกหรือเชิงลบต่อกลยุทธ์หรือวัตถุประสงค์ในการประกอบกิจการ

โดยรัฐวิสาหกิจสามารถนำโอกาสที่จะเกิด (Likelihood) และผลกระทบ (Impact) มาแสดง อยู่ในรูปของผังจัดระดับความเสี่ยง

**ตัวอย่างผังจัดระดับความเสี่ยง**

โอกาสที่จะเกิด / ผลกระทบ	ต่ำมาก (1)	ต่ำ (2)	ปานกลาง (3)	สูง (4)	สูงมาก (5)
สูงมาก (5)	สูง	สูง	สูงมาก	สูงมาก	สูงมาก
สูง (4)	ปานกลาง	สูง	สูง	สูงมาก	สูงมาก
ปานกลาง (3)	ต่ำ	ปานกลาง	สูง	สูง	สูงมาก
ต่ำ (2)	ต่ำ	ต่ำ	ปานกลาง	สูง	สูง
ต่ำมาก (1)	ต่ำมาก	ต่ำ	ต่ำ	ปานกลาง	สูง

ตัวอย่างดังที่แสดงนี้ เป็นผังจัดระดับความเสี่ยงแบบ 5x5 กล่าวคือ มีโอกาสเกิด 5 ระดับ และมีผลกระทบ 5 ระดับ โดยในทางปฏิบัติ รัฐวิสาหกิจสามารถพิจารณาผังจัดระดับความเสี่ยง ในแบบอื่นๆ ได้เช่นกัน เช่น 3x3 หรือ 4x4 ตามการพิจารณาของผู้บริหาร และความเหมาะสม ของแต่ละองค์กร

ทั้งนี้ รัฐวิสาหกิจสามารถพิจารณากำหนดสีตารางได้ตามระดับความเสี่ยงที่องค์กรยอมรับได้ (RA)

**ตัวอย่าง:** บางองค์กรอาจกำหนดให้มีความเสี่ยงสูงมาก (พื้นที่สีแดง) มากกว่าความเสี่ยงระดับอื่นๆ เพื่อแสดงถึงระดับความเสี่ยงที่องค์กรยอมรับได้ (RA) ที่ต่ำกว่า (อ้างถึงคำอธิบายเรื่อง ระดับความเสี่ยง ที่องค์กรยอมรับได้ (RA) ในองค์ประกอบที่ 2 แนวปฏิบัติที่ 2)

นอกจากนี้ เพื่อให้การประเมินความเสี่ยงมีแนวทางที่สอดคล้องกันทั่วทั้งองค์กร และทุกคนในองค์กร มีความเข้าใจที่ตรงกันถึงระดับความรุนแรงของความเสี่ยงแต่ละข้อ กล่าวคือ ระดับสูงมาก สูง ปานกลาง ต่ำ และต่ำมากว่าต้องดำเนินการอย่างไร รัฐวิสาหกิจควรกำหนดคำอธิบายระดับความเสี่ยง และจัดทำเกณฑ์การประเมินความเสี่ยง (Risk Rating Scale) ด้านโอกาสที่จะเกิด (Likelihood) และผลกระทบ (Impact) โดยอาจพิจารณาจากฐานข้อมูลในอดีตหรือการคาดการณ์ในอนาคต ดังตัวอย่างที่แสดงต่อไปนี้

### ตัวอย่างคำอธิบายระดับความเสี่ยงที่ปรากฏบนผังจัดระดับความเสี่ยง

ระดับความเสี่ยง	สี	คำอธิบาย
สูงมาก	สีแดง	ความเสี่ยงที่มีความสำคัญสูงมาก จะต้องได้รับการจัดการทันที
สูง	สีส้ม	ความเสี่ยงที่มีความสำคัญสูง จะต้องได้รับการจัดการในลำดับถัดมา
ปานกลาง	สีส้มอ่อน	ความเสี่ยงที่มีความสำคัญ และต้องติดตามการปฏิบัติตามมาตรการจัดการความเสี่ยงที่ดำเนินการอยู่ในปัจจุบันอย่างเคร่งครัด
ต่ำ	สีเหลือง	ความเสี่ยงที่มีความสำคัญน้อย อยู่ในระดับที่ผู้บริหารยอมรับได้ แต่ต้องติดตามอย่างสม่ำเสมอ
ต่ำมาก	สีเหลืองอ่อน	ความเสี่ยงที่มีความสำคัญน้อยมาก อยู่ในระดับที่ผู้บริหารยอมรับได้ แต่ต้องติดตามอย่างสม่ำเสมอ

### ตัวอย่างเกณฑ์การประเมินความเสี่ยง - ด้านโอกาสที่จะเกิด (Likelihood)

ระดับ	โอกาสที่จะเกิด	คำอธิบาย
สูงมาก (5)	มากกว่าร้อยละ 75	<ul style="list-style-type: none"> <li>เคยเกิดขึ้นในองค์กรมากกว่า 1 ครั้ง ภายใน 6 เดือน หรือ</li> <li>คาดว่าจะเกิดขึ้นอย่างน้อย 2 ครั้งต่อปี</li> </ul>
สูง (4)	ร้อยละ 50 - 75	<ul style="list-style-type: none"> <li>เคยเกิดขึ้นในองค์กรมากกว่า 1 ครั้ง ภายใน 1 ปี หรือ</li> <li>คาดว่าจะเกิดขึ้นอย่างน้อย 1 ครั้งต่อปี</li> </ul>
ปานกลาง (3)	ร้อยละ 25 - 50	<ul style="list-style-type: none"> <li>เคยเกิดขึ้นในองค์กรมากกว่า 1 ครั้ง ภายใน 5 ปี หรือ</li> <li>คาดว่าจะเกิดขึ้นมากกว่า 1 ครั้งในช่วง 5 ปีข้างหน้า</li> </ul>
ต่ำ (2)	ร้อยละ 10 - 25	<ul style="list-style-type: none"> <li>เคยเกิดขึ้นในองค์กร 1 ครั้ง ภายใน 5 ปี หรือ</li> <li>คาดว่าจะเกิดขึ้นได้ 1 ครั้งในช่วง 5 ปีข้างหน้า</li> </ul>
ต่ำมาก (1)	น้อยกว่าร้อยละ 10	<ul style="list-style-type: none"> <li>ไม่เคยเกิดขึ้นในองค์กรมาก่อน หรือ</li> <li>มีโอกาสเกิดขึ้นน้อยมากแต่เป็นไปได้ทางทฤษฎี</li> </ul>

ตัวอย่างเกณฑ์การประเมินความเสี่ยง - ด้านผลกระทบ (Impact)

เกณฑ์	ต่ำมาก (1)	ต่ำ (2)	ปานกลาง (3)	สูง (4)	สูงมาก (5)
<b>ผลกระทบเชิงปริมาณ</b>					
<b>ด้านการเงิน</b>	ผลกำไรสุทธิ ไม่ต่ำกว่า ค่าเป้าหมาย	ผลกำไรสุทธิ ต่ำกว่า ค่าเป้าหมาย ร้อยละ 1 - 10	ผลกำไรสุทธิ ต่ำกว่า ค่าเป้าหมาย ร้อยละ 10 - 20	ผลกำไรสุทธิ ต่ำกว่า ค่าเป้าหมาย ร้อยละ 20 - 30	ผลกำไรสุทธิ ต่ำกว่า ค่าเป้าหมาย เกินกว่า ร้อยละ 30
<b>ด้านรายได้</b>	รายได้ลดลง น้อยกว่าร้อยละ 1 จากค่าเป้าหมาย	รายได้ลดลง ร้อยละ 1 - 2 จากค่าเป้าหมาย	รายได้ลดลง ร้อยละ 2 - 5 จากค่าเป้าหมาย	รายได้ลดลง ร้อยละ 5 - 10 จากค่าเป้าหมาย	รายได้ลดลง เกินกว่า ร้อยละ 10 จากค่าเป้าหมาย
<b>ผลกระทบเชิงคุณภาพ</b>					
<b>ด้านชื่อเสียง</b>	มีการเสนอ ประเด็นใน วงจำกัด เฉพาะกลุ่ม แต่ไม่มี ผลกระทบ ในทางลบ ต่อชื่อเสียง	มีการเสนอ ประเด็นผ่าน ชุมชนกลุ่มต่างๆ เช่น มีการแสดง ความคิดเห็น เชิงลบจำนวนมาก บนช่องทาง ออนไลน์ส่วนตัว	มีการเสนอข่าว เชิงลบผ่านสื่อ ภายในประเทศ และโซเชียลมีเดีย	มีการเสนอข่าว เชิงลบผ่านสื่อ ภายในประเทศ ภายนอกประเทศ และโซเชียลมีเดีย	มีการเสนอข่าว เชิงลบผ่านสื่อ ภายในประเทศ ภายนอกประเทศ และโซเชียลมีเดีย และมีการร้องเรียน เป็นลายลักษณ์ อักษรถึง หน่วยงานของรัฐ
<b>ด้านการบริการ</b>	การให้บริการ ลูกค้าหยุดชะงัก ไม่เกิน 1 ชั่วโมง	การให้บริการ ลูกค้าหยุดชะงัก 1 - 4 ชั่วโมง	การให้บริการ ลูกค้าหยุดชะงัก 4 - 24 ชั่วโมง	การให้บริการ ลูกค้าหยุดชะงัก 24 - 36 ชั่วโมง	การให้บริการ ลูกค้าหยุดชะงัก เกินกว่า 36 ชั่วโมง
<b>ด้านความปลอดภัย</b>	มีการบาดเจ็บ เล็กน้อย สามารถรักษาได้ โดยการปฐม พยาบาล	มีการบาดเจ็บ ที่ต้องได้รับ การรักษา ทางการแพทย์/ พนักงานหยุดงาน ไม่เกิน 10 วัน	มีการบาดเจ็บ ที่ต้องได้รับ การรักษา ทางการแพทย์ อย่างต่อเนื่อง/ พนักงานหยุดงาน	มีการบาดเจ็บ ที่ต้องได้รับ การรักษา ทางการแพทย์ อย่างต่อเนื่อง/ พนักงานหยุดงาน	มีพนักงาน ทุพพลภาพ หรือเสียชีวิต และไม่สามารถ กลับมาทำงานได้

เกณฑ์	ต่ำมาก (1)	ต่ำ (2)	ปานกลาง (3)	สูง (4)	สูงมาก (5)
			10 - 30 วัน	เกินกว่า 30 วัน แล้วสามารถ กลับมาทำงานได้	
<b>ด้าน กฎหมาย/ ระเบียบ ข้อบังคับ</b>	ไม่ปฏิบัติตาม กฎระเบียบ หรือข้อบังคับ ขององค์กร	ไม่ปฏิบัติตาม กฎหมาย ระเบียบ ข้อบังคับ และได้รับ การตักเตือน จากบุคคล หรือหน่วยงาน ภายนอก แต่สามารถ แก้ไขได้	ไม่ปฏิบัติตาม กฎหมาย และ เสียค่าปรับ จากการไม่ ปฏิบัติตาม กฎหมาย	ไม่ปฏิบัติตาม กฎหมาย และ เสียค่าปรับ จากการไม่ ปฏิบัติตาม กฎหมาย รวมถึง ถูกสั่งให้ระงับ การดำเนินงาน ชั่วคราว	ไม่ปฏิบัติตาม กฎหมาย และ เสียค่าปรับ จากการไม่ ปฏิบัติตาม กฎหมาย รวมถึง ถูกสั่งให้ระงับ การดำเนินงาน และถูกเพิกถอน ใบอนุญาต
<b>ด้าน บุคลากร</b>	ไม่มีผลกระทบ ต่อขวัญและ กำลังใจ ของพนักงาน	มีผลกระทบ ต่อขวัญและ กำลังใจ ของพนักงาน ในระดับต่ำ	พนักงานเกิด ความไม่พึงพอใจ ปานกลาง เช่น เสียขวัญ และกำลังใจ ในการทำงาน อย่างกว้างขวาง	พนักงานเกิด ความไม่พึงพอใจ สูง เช่น พนักงานบางกลุ่ม มีการประท้วง (หยุดการ ดำเนินงาน บางส่วน)	พนักงานเกิด ความไม่พึงพอใจ อย่างรุนแรง เช่น มีการประท้วง (หยุดการ ดำเนินงาน ทั้งหมด)
<b>ด้าน การดำเนิน กิจการ อย่าง ต่อเนื่อง</b>	กระบวนการ และการดำเนิน กิจการ ไม่หยุดชะงัก	กระบวนการ และการดำเนิน กิจการได้รับ ผลกระทบ น้อยกว่า 1 ชั่วโมง	กระบวนการ และการดำเนิน กิจการได้รับ ผลกระทบ อย่างรุนแรง เป็นเวลา 1 - 3 ชั่วโมง	กระบวนการ และการดำเนิน กิจการได้รับ ผลกระทบ อย่างรุนแรง เป็นเวลา 3 - 12 ชั่วโมง	กระบวนการ และการดำเนิน กิจการได้รับ ผลกระทบ อย่างรุนแรง เป็นเวลา มากกว่า 12 ชั่วโมง

เกณฑ์	ต่ำมาก (1)	ต่ำ (2)	ปานกลาง (3)	สูง (4)	สูงมาก (5)
<b>ด้านข้อมูลส่วนบุคคล</b>	กรณีเกิดการรั่วไหลหรือการละเมิดข้อมูลส่วนบุคคลที่ไม่สามารถระบุเจ้าของข้อมูลส่วนบุคคลได้โดยตรงโดยข้อมูลดังกล่าวไม่มีข้อมูลส่วนบุคคลประเภทอ่อนไหว (Sensitive Data)	กรณีเกิดการรั่วไหลหรือการละเมิดข้อมูลส่วนบุคคลที่สามารถระบุเจ้าของข้อมูลส่วนบุคคลได้โดยตรงและอาจส่งผลกระทบต่อเจ้าของข้อมูลเพียงเล็กน้อยโดยข้อมูลดังกล่าวไม่มีข้อมูลส่วนบุคคลประเภทอ่อนไหว (Sensitive Data)	กรณีเกิดการรั่วไหลหรือการละเมิดข้อมูลส่วนบุคคลที่อาจส่งผลกระทบต่อเจ้าของข้อมูลส่วนบุคคลอย่างมีนัยสำคัญโดยข้อมูลดังกล่าวไม่มีข้อมูลส่วนบุคคลประเภทอ่อนไหว (Sensitive Data)	กรณีเกิดการรั่วไหลหรือการละเมิดข้อมูลส่วนบุคคลที่อาจส่งผลกระทบต่อสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคลอย่างมีนัยสำคัญเนื่องจากเป็นกิจกรรมที่มีข้อมูลส่วนบุคคลประเภทอ่อนไหว (Sensitive Data)	กรณีเกิดการรั่วไหลหรือการละเมิดข้อมูลส่วนบุคคลที่อาจส่งผลกระทบต่อสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคลอย่างร้ายแรงเนื่องจากเป็นกิจกรรมที่มีข้อมูลส่วนบุคคลประเภทอ่อนไหว (Sensitive Data)



**Tip:**

ในการกำหนดเกณฑ์การประเมินผลกระทบด้านการเงินนั้น รัฐวิสาหกิจสามารถดำเนินการโดยพิจารณาจากงบการเงินของรัฐวิสาหกิจ และรายงานเหตุการณ์สูญเสีย เพื่อพิจารณาจำนวนเงินที่รัฐวิสาหกิจเคยสูญเสียเมื่อเกิดเหตุการณ์ใดๆ โดยจะต้องพิจารณาประกอบกับระดับความเสี่ยงที่องค์กรยอมรับได้ (RA) ด้วย

จากตัวอย่างเกณฑ์การประเมินความเสี่ยงด้านผลกระทบข้างต้น หากองค์กรกำหนดให้ระดับความเสี่ยงที่องค์กรยอมรับได้ (RA) อยู่ในระดับปานกลาง ซึ่งระดับผลกระทบด้านการเงินที่ระดับปานกลาง มีผลกำไรสุทธิต่ำกว่าค่าเป้าหมายร้อยละ 10 - 20 โดยหากระดับความเสี่ยงที่ยอมรับได้ของรัฐบาลกิจลดลง คือ ยอมรับได้ หากผลกำไรสุทธิต่ำกว่าค่าเป้าหมายได้ไม่เกินร้อยละ 15 ดังนั้น ระดับผลกระทบด้านการเงินที่ระดับปานกลางนี้จะต้องมีการปรับปรุงเป็นมีผลกำไรสุทธิต่ำกว่าค่าเป้าหมายร้อยละ 10 - 15 ในขณะที่ระดับผลกระทบที่ระดับต่ำมาก ต่ำ สูง และสูงมาก ก็จะต้องมีการปรับเปลี่ยนเพื่อให้สอดคล้องกับระดับความเสี่ยงที่องค์กรยอมรับได้ (RA) เช่นกัน

นอกจากนี้ รัฐบาลกิจควรสื่อสารเกณฑ์การประเมินระดับความรุนแรงของแต่ละปัจจัยเสี่ยงต่อเจ้าของความเสี่ยง (Risk Owner) และกำหนดให้มีการทบทวนเกณฑ์การประเมินความเสี่ยงทั้งด้านผลกระทบและโอกาสที่จะเกิดเป็นประจำอย่างสม่ำเสมอ เมื่อสภาพแวดล้อมของรัฐบาลกิจมีการเปลี่ยนแปลงไป

2. ผู้บริหารควรประเมินระดับความเสี่ยงทั้งระดับความเสี่ยงก่อนมาตรการควบคุม (Inherent Risk) ความเพียงพอของมาตรการการควบคุมที่มีอยู่ในปัจจุบัน รวมถึงพิจารณาระดับความเสี่ยงที่เหลืออยู่ (Residual Risk) ว่าอยู่ในระดับความเสี่ยงที่องค์กรยอมรับได้ (RA) หรือไม่

**คำอธิบายระดับความเสี่ยงก่อนมาตรการควบคุม (Inherent Risk) และระดับความเสี่ยงที่เหลืออยู่ (Residual Risk)**

**ระดับความเสี่ยงก่อนมาตรการควบคุม (Inherent Risk)** คือ ระดับความเสี่ยงที่เกิดขึ้นจากการดำเนินกิจกรรมต่างๆ ขององค์กร โดยที่ผู้บริหารยังไม่ได้ดำเนินการใดๆ เพื่อลดผลกระทบหรือโอกาสที่จะเกิดของความเสี่ยงนั้น การประเมินระดับความเสี่ยงก่อนมาตรการควบคุมจะทำให้ผู้บริหารสามารถประมาณการทรัพยากรที่ต้องใช้ และระดับการควบคุมที่ต้องมีในการจัดการความเสี่ยง

**ระดับความเสี่ยงที่เหลืออยู่ (Residual Risk)** คือ ระดับความเสี่ยงคงเหลือหลังจากที่ได้พิจารณาถึงมาตรการควบคุมต่างๆ ที่ผู้บริหารกำหนดให้มีในปัจจุบัน การประเมินระดับความเสี่ยงที่เหลืออยู่ (Residual Risk) ทำให้ผู้บริหารสามารถพิจารณาได้ว่ามาตรการจัดการความเสี่ยงที่มีอยู่ในปัจจุบันมีประสิทธิภาพเพียงพอหรือไม่ หรือมีมาตรการควบคุมเกินความจำเป็น หากระดับความเสี่ยงที่เหลืออยู่ (Residual Risk) อยู่ในระดับที่สูงเกินกว่าระดับความเสี่ยงที่องค์กรยอมรับได้ (RA) ผู้บริหารจะต้องกำหนดแผนจัดการความเสี่ยงและดำเนินการตามแผนดังกล่าว

ตัวอย่างแผนภาพแสดงระดับความเสี่ยงก่อนมาตรการควบคุม (Inherent Risk)  
และระดับความเสี่ยงที่เหลืออยู่ (Residual Risk)



จากแผนภาพข้างต้น จะเห็นได้ว่าความเสี่ยงก่อนมาตรการควบคุม (Inherent Risk) จะอยู่ที่ระดับสูงกว่า ความเสี่ยงที่เหลืออยู่ (Residual Risk) เมื่อองค์กรได้มีการจัดการความเสี่ยงตามมาตรการ ควบคุมที่มีอยู่ในปัจจุบัน นอกจากนี้ หากรัฐวิสาหกิจมีการพิจารณาต่อไปว่ามาตรการจัดการ ความเสี่ยงที่มีอยู่ในปัจจุบันมีประสิทธิภาพเพียงพอหรือไม่ จากนั้นมีการกำหนดแผนจัดการความเสี่ยง และดำเนินการตามแผนดังกล่าวเพิ่มเติม และหากการดำเนินการมีประสิทธิภาพ องค์กรจะสามารถ ลดระดับความเสี่ยงลงจนไปถึงระดับความเสี่ยงที่องค์กรยอมรับได้ (RA)

การพิจารณาความเพียงพอและประสิทธิภาพของการควบคุมที่มีอยู่ในปัจจุบัน สามารถทำได้ ดังต่อไปนี้

- พิจารณาการออกแบบการควบคุม (Design Effectiveness) เปรียบเทียบกับแนวปฏิบัติที่ดี (Best Practice) ของการควบคุมภายใน โดยมีเป้าหมายสูงสุดที่จะพิจารณาว่าการควบคุมนั้น ก่อให้เกิดความเชื่อมั่นอย่างสมเหตุสมผลในวัตถุประสงค์ที่ได้กำหนดไว้หรือไม่

**ตัวอย่าง:** การกำหนดให้ผู้มาติดต่อทุกคนต้องแลกบัตรประชาชนกับพนักงานรักษาความปลอดภัย และลงชื่อในสมุดลงทะเบียนก่อนเข้ามาในบริเวณสำนักงาน

- พิจารณาว่าการควบคุมที่ได้ออกแบบไว้นั้น ได้รับการนำไปปฏิบัติอย่างเหมาะสมหรือไม่ (Operating Effectiveness)

**ตัวอย่าง:** การติดตามและประเมินผลเพื่อให้มั่นใจว่า ผู้เกี่ยวข้องทุกคนได้ปฏิบัติตามการควบคุมที่ได้ออกแบบไว้ นั่น กล่าวคือ ผู้มาติดต่อได้แลกบัตรประชาชนกับพนักงานรักษาความปลอดภัย และลงชื่อในสมุดลงทะเบียนก่อนเข้ามาในบริเวณสำนักงานทุกครั้งหรือไม่ พนักงานรักษาความปลอดภัยได้บังคับใช้ระเบียบดังกล่าวอย่างเข้มงวดเพียงใด

- การควบคุมเกินความจำเป็น คือ การกำหนดขั้นตอน หรือมาตรการต่างๆ เพื่อการควบคุมในแต่ละกิจกรรมมากเกินไปเมื่อเปรียบเทียบกับระดับความเสี่ยง ซึ่งอาจต้องใช้ทรัพยากร เช่น บุคลากร เทคโนโลยีเพื่อการบริหารจัดการมากเกินไป

**ตัวอย่าง:** การจ้างพนักงานเงินเดือน 150,000 บาท เพื่อดูแลและควบคุมการจ่ายเงินสดจำนวน 10,000 บาท

ภายหลังจากการพิจารณามาตรการจัดการความเสี่ยงที่มีอยู่ในปัจจุบันแล้ว หากพบว่ายังไม่มีประสิทธิภาพและประสิทธิผลเพียงพอ ผู้บริหารควรจะต้องจัดทำแผนจัดการความเสี่ยงเพิ่มเติม และติดตามการปฏิบัติตามแผนจัดการความเสี่ยงนั้น เพื่อให้ความเสี่ยงอยู่ในระดับความเสี่ยงที่องค์กรยอมรับได้ (RA)

3. ภายหลังจากการกำหนดเกณฑ์การประเมินความเสี่ยง ผู้บริหารควรมีการประเมินความเสี่ยงโดยสามารถพิจารณานำผลจากการวิเคราะห์เชิงลึกถึงสาเหตุและที่มาของความเสี่ยงนั้นๆ มาเป็นส่วนหนึ่งในการประเมินความเสี่ยง

### เครื่องมือหรือเทคนิคที่ใช้ในการประเมินความเสี่ยง

ปัจจัยหลักในการพิจารณาเครื่องมือที่จะเลือกใช้ในการประเมินความเสี่ยงขึ้นอยู่กับความรุนแรงของความเสี่ยงนั้นๆ ความซับซ้อนของความเสี่ยง ความเพียงพอของข้อมูลที่จะใช้ในการประเมินความสามารถหรือความต้องการขององค์กรในการใช้แนวทางหรือเครื่องมือในการประเมินนั้นๆ และต้นทุนที่ใช้ในการประเมินความเสี่ยง

การประเมินความเสี่ยงสามารถทำได้โดยใช้เครื่องมือเชิงคุณภาพ เชิงปริมาณหรืออาจพิจารณาใช้ทั้งสองเครื่องมือร่วมกัน ดังนี้

- 1) เครื่องมือการประเมินความเสี่ยงเชิงคุณภาพ มักนำมาใช้เมื่อการหาข้อมูลเชิงปริมาณไม่สามารถทำได้หรือมีต้นทุนสูงกว่าประโยชน์ที่คาดว่าจะได้รับจากแนวทางการประเมินดังกล่าว เช่น
  - การสัมภาษณ์
  - การประชุมเชิงปฏิบัติการ (Workshop)
  - การสำรวจ
  - การหาตัววัดเปรียบเทียบ (Benchmarking)
  - Bow-Tie Analysis

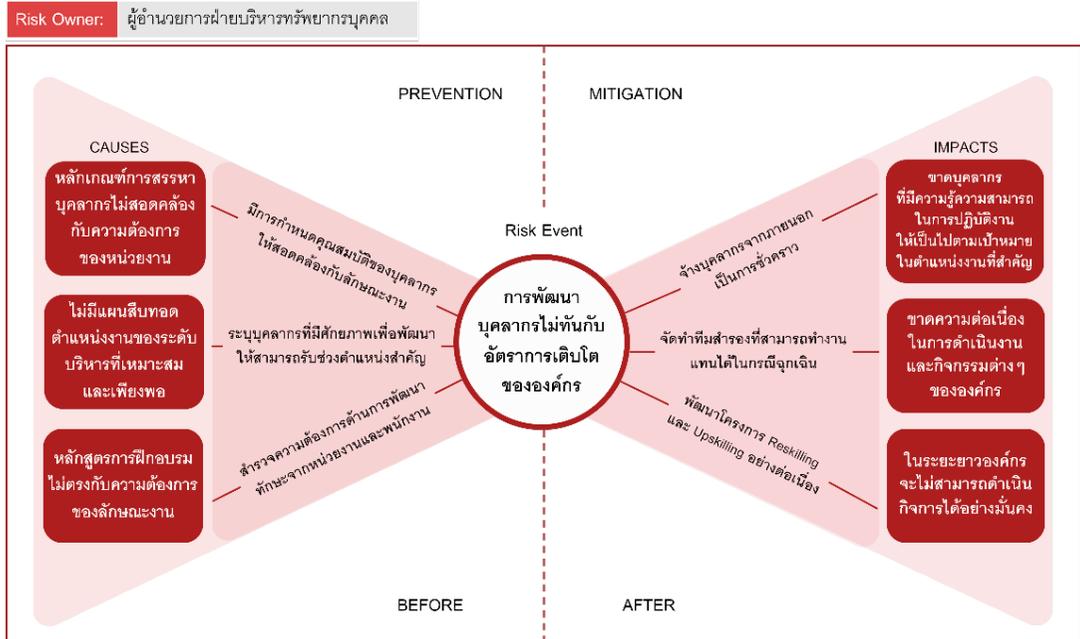
2) เครื่องมือการประเมินความเสี่ยงเชิงปริมาณเป็นแนวทางที่จะช่วยเพิ่มความละเอียดและแม่นยำ และสนับสนุนการวิเคราะห์ผลประโยชน์ที่จะได้รับกับต้นทุนที่เกิดขึ้น ดังนั้น แนวทางเชิงปริมาณ จึงมักใช้กับกิจกรรมที่ซับซ้อนและช่วยเสริมเทคนิคเชิงคุณภาพ เช่น

- แผนภูมิต้นไม้ (Decision Trees)
- แบบจำลอง Monte Carlo
- แบบจำลองความน่าจะเป็น เช่น มูลค่าที่ได้รับผลกระทบจากความเสียหาย (Value at Risk) กระแสเงินสดที่ได้รับผลกระทบจากความเสียหาย (Cash Flow at Risk) การกระจายของค่าความสูญเสียด้านการดำเนินงาน (Operational Loss Distribution)
- แบบจำลองที่ไม่ใช้ความน่าจะเป็น เช่น การวิเคราะห์ความอ่อนไหว (Sensitivity Analysis) การวิเคราะห์สถานการณ์สมมติ (Scenario Analysis)

ทั้งนี้ เครื่องมือหรือเทคนิคที่ใช้ในการประเมินความเสี่ยงที่นิยมใช้กันมากและเป็นวิธีที่ง่าย ได้แก่ Bow-Tie Analysis ซึ่งการประเมินความเสี่ยงโดยอาศัยเครื่องมือดังกล่าวจะเน้นไปที่การระบุสาเหตุของความเสี่ยง และผลกระทบเมื่อเกิดเหตุการณ์ความเสี่ยงนั้นๆ โดยชื่อวิธีการ Bow-Tie Analysis มาจากลักษณะแผนภาพที่มีการแสดงถึงสาเหตุและผลกระทบของเหตุการณ์ความเสี่ยง โดยทั่วไปแล้วจะใช้วิธีนี้ร่วมกับการสัมมนากลุ่ม หรือการประชุมเชิงปฏิบัติการ (Workshop) เพื่อหารือและแลกเปลี่ยนความคิดเห็นต่างๆ (Brainstorming) ในเรื่องความเสี่ยง

ประโยชน์ของ Bow-Tie Analysis คือ การช่วยให้การวิเคราะห์ความเสี่ยงครอบคลุมไปถึงสาเหตุต่างๆ อย่างรอบด้าน เพื่อให้ผู้บริหารประเมินต่อไปได้ว่า สาเหตุในเรื่องใดที่มีความสำคัญมากที่สุด และควรกำหนดแผนจัดการความเสี่ยงอย่างไร เพื่อให้สอดคล้องกับสาเหตุของความเสี่ยงนั้น และควรจัดสรรทรัพยากรในการจัดการความเสี่ยงอย่างไร นอกจากนี้ การแสดงผลกระทบในหลายๆ ด้าน จะช่วยให้ผู้บริหารทราบว่า ควรนำเกณฑ์การประเมินความเสี่ยงด้านใดมาใช้ เช่น ผลกระทบด้านที่เป็นตัวเงิน หรือด้านชื่อเสียง

## ตัวอย่างการวิเคราะห์ความเสี่ยงตามวิธี Bow-Tie Analysis



กรณีความเสี่ยงที่อาจมีผลกระทบรุนแรงมาก ผู้บริหารอาจเลือกใช้การวิเคราะห์สถานการณ์สมมติ (Scenario Analysis) แต่เมื่อต้องประเมินผลกระทบของหลายเหตุการณ์ ผู้บริหารอาจพิจารณานำการสร้างสถานการณ์จำลอง (Simulations) มาใช้ซึ่งอาจมีประโยชน์มากกว่า เช่น การทดสอบภาวะวิกฤติ (Stress Testing) ที่ใช้ในการประเมินความสามารถในการรับมือกับสถานการณ์ที่ไม่ปกติหรือสถานการณ์ที่มีความเสี่ยงสูง

ในทางกลับกัน ในกรณีที่ความเสี่ยงมีโอกาสที่จะเกิดขึ้นสูงแต่ผลกระทบต่ำ ผู้บริหารอาจเลือกใช้วิธีติดตามข้อมูล (Data Tracking) และระบบคอมพิวเตอร์เสมือนมนุษย์ (Cognitive Computing) ในการหาข้อสรุปเกี่ยวกับความรุนแรงของความเสี่ยง ทั้งนี้ องค์กรอาจใช้แนวทางเดียวกันกับที่เคยใช้ในขั้นตอนการระบุความเสี่ยงก็ได้

4. ภายหลังจากการประเมินความรุนแรงของความเสี่ยงแล้ว รัฐวิสาหกิจควรพิจารณาแสดงผลการประเมินดังกล่าวผ่าน “แผนภาพความเสี่ยง” (Heat Map/Risk Map) หรือแผนภาพชนิดอื่นๆ เพื่อแสดงความรุนแรงของความเสี่ยงแต่ละความเสี่ยงต่อการบรรลุกลยุทธ์และวัตถุประสงค์ในการประกอบกิจการ ความเสี่ยงที่แสดงในแผนภาพความเสี่ยง (Heat Map/Risk Map) ใช้สมมติฐานของผลการปฏิบัติงานเพื่อบรรลุกลยุทธ์และวัตถุประสงค์ในการประกอบกิจการในระดับหนึ่งๆ โดยสีในแผนภาพแสดงความรุนแรงของความเสี่ยงในระดับต่างๆ เป็นผลมาจากการพิจารณาความเป็นไปได้ที่จะเกิดร่วมกับผลกระทบ ณ ระดับความเสี่ยงที่ยอมรับได้หนึ่งๆ

## ตัวอย่างแผนภาพความเสี่ยงที่แสดงความรุนแรงของความเสี่ยงต่อการบรรลุวัตถุประสงค์ ในการประกอบกิจการ

โอกาสที่จะเกิด ผลกระทบ	ต่ำมาก (1)	ต่ำ (2)	ปานกลาง (3)	สูง (4)	สูงมาก (5)
สูงมาก (5)	ปานกลาง	สูง	สูงมาก	สูงมาก	สูงมาก
สูง (4)	ปานกลาง	ปานกลาง	สูง	● ความเสี่ยง 1	สูงมาก
ปานกลาง (3)	● ความเสี่ยง 4	ปานกลาง	ปานกลาง	สูง	สูงมาก
ต่ำ (2)	ต่ำ	ต่ำ	● ความเสี่ยง 3	● ความเสี่ยง 2	สูง
ต่ำมาก (1)	ต่ำมาก	ต่ำ	ต่ำ	ปานกลาง	ปานกลาง

จากรูปข้างต้นแสดงให้เห็นว่าองค์กรมีระดับความรุนแรงทั้งหมด 5 ระดับ จากสีแดงถึงสีเขียวอ่อน สีแต่ละสีแสดงถึงความรุนแรงในระดับต่างๆ รวมถึงระดับความเสี่ยงที่องค์กรยอมรับได้ (RA) ขององค์กร ที่หลีกเลี่ยงความเสี่ยง (Risk Averse) จะมีพื้นที่สีแดงมากกว่าเมื่อเปรียบเทียบกับองค์กรที่รับความเสี่ยงได้สูง (Risk Aggressive)

### แนวปฏิบัติที่ 3

รัฐวิสาหกิจควรจัดลำดับความสำคัญของความเสี่ยงและเลือกแนวทางการตอบสนองต่อความเสี่ยงที่เหมาะสม

#### คู่มือปฏิบัติ

1. การจัดลำดับความสำคัญของความเสี่ยงและช่วยให้รัฐวิสาหกิจตัดสินใจเลือกวิธีการตอบสนองต่อความเสี่ยง และจัดสรรทรัพยากรได้อย่างเหมาะสม ผู้บริหารควรนำระดับความเสี่ยงที่องค์กรยอมรับได้ (RA) มาพิจารณาประกอบการจัดลำดับความสำคัญของความเสี่ยงด้วย กล่าวคือ ความเสี่ยงจะมีลำดับความสำคัญสูงหากเข้าใกล้ระดับความเสี่ยงที่องค์กรยอมรับได้ (RA) ซึ่งมีการจัดลำดับความสำคัญของความเสี่ยงสามารถพิจารณาจากเกณฑ์ ดังตัวอย่างต่อไปนี้

- **ความสามารถในการปรับตัว (Adaptability)**

เป็นความสามารถขององค์กรในการปรับตัวและตอบสนองต่อความเสี่ยง

**ตัวอย่าง:** เมื่อเกิดการระบาดของโรคติดต่อ ทำให้พนักงานไม่สามารถมาทำงานที่สำนักงานได้ องค์กรจึงต้องปรับตัวโดยนำระบบการทำงานแบบออนไลน์มาใช้ รวมถึงจัดอบรมให้พนักงานมีทักษะในการใช้เทคโนโลยี เพื่อให้การทำงานยังคงดำเนินไปได้อย่างมีประสิทธิภาพ ทั้งนี้ หากสถานการณ์โรคติดต่อทุเลาลง องค์กรก็อาจพิจารณาแนวทางปฏิบัติในการทำงานอีกครั้ง เช่น การทำงานแบบผสมผสาน (Hybrid Working)

- **ความซับซ้อน (Complexity)**

ลักษณะของความเสี่ยงและความสัมพันธ์ระหว่างความเสี่ยงมีความซับซ้อน

**ตัวอย่าง:** องค์กรอยู่ระหว่างการพัฒนาแพลตฟอร์มกลางสำหรับให้บริการประชาชน โดยต้องมีการยืนยันตัวตนหรือทำธุรกรรมอื่นๆ ผ่านทางแพลตฟอร์มดังกล่าว องค์กรจึงควรพิจารณาความเสี่ยงด้านความมั่นคงทางไซเบอร์ เนื่องจากในการพัฒนาแพลตฟอร์ม ต้องใช้ข้อมูลและเชื่อมโยงจากหลายระบบ หลายฐานข้อมูล และหลายหน่วยงาน ซึ่งหากข้อมูลส่วนใดส่วนโหลก็มีแนวโน้มที่จะกระทบต่อความเสี่ยงอื่น อาทิ ข้อมูลส่วนบุคคลรั่วไหลก็จะส่งผลกระทบต่อความเสี่ยงด้านกฎหมายและการปฏิบัติตามข้อกำหนด เช่น กฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล

- **ความรวดเร็ว (Velocity)**

ระยะเวลาที่ความเสี่ยงเกิดขึ้นและส่งผลกระทบต่อองค์กร ความรวดเร็วในการส่งผลกระทบต่อองค์กรอาจทำให้องค์กรไม่สามารถรักษาระดับในความเป็นเบงในผลการปฏิบัติงานที่ยอมรับได้ กล่าวคือ หากความเสี่ยงมีความเร็วสูง จะส่งผลกระทบต่อองค์กรทันที ส่งผลให้องค์กรมีเวลารับมือหรือแก้ไขน้อย

**ตัวอย่าง:** ความเสี่ยงจากการหยุดชะงักการดำเนินงาน เนื่องจากการหยุดงานประท้วง เป็นความเสี่ยงที่มีความเร็วสูง เนื่องจากองค์กรได้รับผลกระทบทันที ซึ่งมีผลต่อประสิทธิภาพของการบริหารจัดการห่วงโซ่อุปทาน

- **ระยะเวลาที่คงอยู่ (Persistence)**

ระยะเวลาที่ความเสี่ยงส่งผลกระทบต่อองค์กร กรณีที่ความเสี่ยงนั้นส่งผลกระทบต่อองค์กรเป็นระยะเวลานาน หรือเกิดขึ้นบ่อยครั้ง ควรให้ความสำคัญกับความเสียดังกล่าว

**ตัวอย่าง:** ในทุกฤดูร้อนมักเกิดภัยแล้ง ซึ่งมักเกิดขึ้นต่อเนื่องเป็นเวลาหลายสัปดาห์และส่งผลกระทบต่อเกษตรกรและระบบสาธารณสุข ภาค หน่วยงานที่เกี่ยวข้องจึงจัดทำแผนรับมือภัยแล้งสำหรับการสำรองการจ่ายน้ำประปา

### • การฟื้นตัว (Recovery)

ความสามารถขององค์กรในการปรับตัวเข้าสู่ช่วงที่ยอมรับได้ เช่น องค์กรกลับมาดำเนินงานอีกครั้ง หลังจากประสบภัยแผ่นดินไหวหรือภัยธรรมชาติอื่นๆ

ทั้งนี้ การจัดลำดับความสำคัญของความเสี่ยง ความเสี่ยงที่มีความรุนแรงใกล้เคียงกันอาจได้รับการจัดลำดับความสำคัญที่แตกต่างกันได้

**ตัวอย่าง:** ความเสี่ยงสองเรื่องอาจมีความรุนแรง “ปานกลาง” เหมือนกัน แต่ความเสี่ยงที่หนึ่งได้รับการจัดลำดับว่ามีความสำคัญมากกว่า เนื่องจากมีความเร็วมากกว่าและมีระยะเวลาที่คงอยู่นานกว่าหรือเนื่องจากวิธีการตอบสนองต่อความเสี่ยงสำหรับความเสี่ยงที่หนึ่งให้ผลตอบแทนที่ปรับด้วยความเสี่ยง (Risk-adjust Return) หรือปรับลดระดับความเสี่ยงลงได้มากกว่าความเสี่ยงที่สอง

## แนวปฏิบัติที่ 4

รัฐวิสาหกิจควรเลือกแนวทางการตอบสนองต่อความเสี่ยง 5 แนวทาง คือ 1) การหลีกเลี่ยงความเสี่ยง (Avoidance) 2) การลดความเสี่ยง (Reduction) 3) การหาผู้ร่วมรับความเสี่ยง (Sharing) 4) การยอมรับความเสี่ยง (Acceptance) และ 5) การดำเนินการต่อโดยการยอมรับความเสี่ยงที่สูงขึ้น (Pursuing) และเลือกใช้วิธีในการตอบสนองต่อความเสี่ยงให้สอดคล้องกับระดับความรุนแรงของความเสี่ยง และช่วงความเบี่ยงเบนของระดับความเสี่ยงที่องค์กรยอมรับได้ (RT) และระดับความเสี่ยงที่เหลืออยู่ (Residual Risk) นอกจากนี้ ควรพิจารณาถึงผลกระทบและโอกาสที่จะเกิด ความสมดุลของต้นทุนที่ต้องใช้ในการตอบสนองต่อความเสี่ยงและผลที่ได้จากการตอบสนองต่อความเสี่ยงนั้น รวมถึงความเสี่ยงใหม่ที่อาจเกิดเพิ่มขึ้น ซึ่งเป็นผลจากการตอบสนองต่อความเสี่ยงเดิม

### คู่มือปฏิบัติ

1. เมื่อการจัดลำดับความสำคัญของความเสี่ยงแล้วเสร็จ ผู้บริหารควรพิจารณากำหนดแนวทางการตอบสนองต่อความเสี่ยง และจัดทำแผนจัดการความเสี่ยง ดังต่อไปนี้
  - 1) ศึกษาและวิเคราะห์ความเสี่ยงแต่ละข้อ ระดับความเสี่ยง สาเหตุและที่มาของความเสี่ยงนั้น เพื่อทำความเข้าใจในแต่ละองค์ประกอบและความสัมพันธ์ของแต่ละความเสี่ยง และเหตุการณ์ที่เกี่ยวข้องต่างๆ โดยในการวิเคราะห์ให้เน้นไปที่อะไรคือสาเหตุที่แท้จริงของความเสี่ยง ผ่านการจัดทำแผนภาพแสดงความเชื่อมโยงของความเสี่ยง (Risk Correlation Map) เพื่อวิเคราะห์และแสดงให้เห็นถึงความสัมพันธ์ระหว่างความเสี่ยงต่างๆ อย่างเป็นระบบ เพื่อช่วยในการประเมินผลกระทบทำได้ครอบคลุมยิ่งขึ้นและสนับสนุนการตัดสินใจเชิงกลยุทธ์ของคณะกรรมการและผู้บริหารได้อย่างมีประสิทธิภาพ โดยมีขั้นตอนดังต่อไปนี้

- (1) การกำหนดปัจจัยเสี่ยงและสาเหตุของความเสี่ยงในทุกปัจจัยเสี่ยง รวมถึงกำหนดระดับความรุนแรงของแต่ละสาเหตุในทุกปัจจัยเสี่ยง อีกทั้งกำหนดน้ำหนักของแต่ละสาเหตุที่กระทบต่อปัจจัยเสี่ยงนั้นๆ ให้ครบร้อยละ 100 โดยกระบวนการวิเคราะห์นี้จะดำเนินการร่วมกันระหว่างเจ้าของความเสี่ยง (Risk Owner) และหน่วยงานบริหารความเสี่ยง
- (2) การวิเคราะห์ความสัมพันธ์ระหว่างทุกปัจจัยเสี่ยงในระดับองค์กรและสาเหตุของความเสียหายทั้งหมดโดยจะมีการเชื่อมโยงความสัมพันธ์ระหว่างปัจจัยเสี่ยงและสาเหตุแต่ละรายการผ่านการกำหนดเส้นโยง เพื่อแสดงถึงความสัมพันธ์อย่างชัดเจน จนเกิดเป็นแผนภาพแสดงความเชื่อมโยงของความเสี่ยง (Risk Correlation Map) โดยกระบวนการวิเคราะห์นี้จะดำเนินการร่วมกันระหว่างเจ้าของความเสี่ยง (Risk Owner) และหน่วยงานบริหารความเสี่ยง
- (3) การสรุปสาเหตุของความเสียหายในทุกปัจจัยเสี่ยงและผลกระทบ โดยมีการวิเคราะห์ผลกระทบทั้งเชิงพรรณนาและเชิงปริมาณโดยกระบวนการวิเคราะห์นี้ ซึ่งจะดำเนินการร่วมกันระหว่างเจ้าของความเสี่ยง (Risk Owner) และหน่วยงานบริหารความเสี่ยง โดยอาจพิจารณาระบุตามตารางดังตัวอย่างต่อไปนี้

ความสัมพันธ์	สาเหตุ	ผลกระทบ	การวิเคราะห์ผลกระทบเชิงพรรณนา	การวิเคราะห์ผลกระทบเชิงปริมาณ
คู่ที่ 1 ความเสี่ยงด้านรายได้และความพึงพอใจของผู้รับบริการ	การให้บริการที่ไม่ได้คุณภาพ	<ul style="list-style-type: none"> <li>• รายได้ไม่เป็นไปตามเป้าหมาย</li> <li>• ระดับความพึงพอใจของผู้รับบริการไม่เป็นไปตามเป้าหมาย</li> </ul>	สาเหตุหนึ่งที่ทำให้รายได้ไม่เป็นไปตามเป้าหมาย คือ การให้บริการที่ไม่ได้คุณภาพ ทำให้ระดับความพึงพอใจของผู้รับบริการลดลง และผู้รับบริการเปลี่ยนไปเลือกใช้บริการจากคู่แข่ง	คะแนนความพึงพอใจของผู้รับบริการ ลดลง 0.5 คะแนน ทำให้ผู้รับบริการเปลี่ยนไปเลือกใช้บริการจากคู่แข่ง และทำให้รายได้ลดลงร้อยละ 2 จากเป้าหมายที่กำหนด

- (4) การนำแผนภาพแสดงความเชื่อมโยงของความเสี่ยง (Risk Correlation Map) ไปใช้ในการร่วมพิจารณากำหนดแผนการบริหารจัดการความเสี่ยงที่จะระบุในขั้นถัดไป โดยมีการบริหาร

ถึงปัจจัยเสี่ยงที่เป็นสาเหตุหลัก และมีการกล่าวถึงปัจจัยเสี่ยงที่มีระดับความรุนแรงสูง และส่งผลกระทบต่อปัจจัยเสี่ยงดังกล่าว รวมถึงมีการประเมินความสำเร็จของเป้าหมายในการบริหารความเสี่ยงของปัจจัยเสี่ยงหลักกว่าเป็นผลมาจากการบริหารปัจจัยเสี่ยงที่เป็นสาเหตุ หรือการบริหารปัจจัยเสี่ยงที่มีผลกระทบสูง

- (5) การสร้างความเข้าใจในเรื่องแผนภาพแสดงความเชื่อมโยงของความเสี่ยง (Risk Correlation Map) ให้กับบุคลากรในองค์กร โดยเจ้าของความเสี่ยง (Risk Owner) มีส่วนร่วมในการจัดทำแผนภาพแสดงความเชื่อมโยงของความเสี่ยง (Risk Correlation Map) และยอมรับในการร่วมกันจัดทำแผนการบริหารจัดการความเสี่ยงในกลุ่มความเสี่ยงที่มีความสัมพันธ์กัน รวมถึงบุคลากรในองค์กรรับรู้และเข้าใจเรื่องแผนภาพความเสี่ยง (Heat Map/Risk Map)
- 2) วางแผนและปรึกษาร่วมกัน ระหว่างผู้บริหารและพนักงานที่เกี่ยวข้อง ถึงประเด็นต่อไปนี้
  - (1) แนวทางการตอบสนองต่อความเสี่ยงทั้ง 5 แนวทาง ดังตารางแสดงกลยุทธ์การตอบสนองต่อความเสี่ยง/การจัดการความเสี่ยง และหาข้อสรุปแนวทางการตอบสนองต่อความเสี่ยงที่องค์กรจะเลือกดำเนินการต่อไป เพื่อลดผลกระทบและ/หรือโอกาสที่จะเกิดของความเสี่ยงให้ลดลงถึงระดับความเสี่ยงที่องค์กรยอมรับได้ (RA)

#### กลยุทธ์การตอบสนองต่อความเสี่ยง/การจัดการความเสี่ยง

กลยุทธ์/แนวทาง/วิธี	ความหมายของกลยุทธ์และการปฏิบัติ
การยอมรับความเสี่ยง (Acceptance)	<p>ยอมรับความเสี่ยง โดยไม่มีการดำเนินการใดๆ เพิ่มเติม เพื่อลดโอกาสที่จะเกิดหรือผลกระทบของความเสี่ยง เนื่องจากความเสี่ยงอยู่ในระดับความเสี่ยงที่องค์กรยอมรับได้ (RA) หรือค่าใช้จ่ายของการจัดการความเสี่ยงนั้นไม่คุ้มค่ากับผลที่องค์กรจะได้รับ</p> <ul style="list-style-type: none"> <li>ตัวอย่างการตอบสนองต่อความเสี่ยงโดยใช้กลยุทธ์นี้: การติดตามความเสี่ยงว่ายังคงอยู่ในระดับความเสี่ยงที่องค์กรยอมรับได้ (RA) หรือไม่ และการติดตามการเปลี่ยนแปลงในสภาพแวดล้อมทางธุรกิจ เพื่อติดตามสถานการณ์และรับมือได้อย่างทันท่วงที หากมีการเปลี่ยนแปลงใหม่ๆ ที่สำคัญ</li> </ul>
การลดความเสี่ยง (Reduction)	<p>ไม่สามารถยอมรับความเสี่ยงได้ ต้องดำเนินการเพื่อลดโอกาสที่จะเกิดหรือลดผลกระทบของความเสี่ยงให้อยู่ในระดับที่องค์กรยอมรับได้ (RA) หรือทั้งสองอย่าง โดยจัดทำแผนจัดการความเสี่ยงเพื่อเพิ่มประสิทธิภาพและประสิทธิผลในการลดความเสี่ยง การตอบสนองต่อความเสี่ยงลักษณะนี้โดยทั่วไปจะเกี่ยวข้องกับการตัดสินใจทางธุรกิจในทุกๆ วัน</p>

กลยุทธ์/แนวทาง/วิธี	ความหมายของกลยุทธ์และการปฏิบัติ
	<ul style="list-style-type: none"> <li>ตัวอย่างการตอบสนองต่อความเสี่ยงโดยใช้กลยุทธ์นี้: การปรับปรุงและพัฒนานโยบายและกระบวนการ การลงทุนในระบบสารสนเทศ/Software/อุปกรณ์ การแก้ไขกระบวนการทางธุรกิจใหม่</li> </ul>
การหาผู้ร่วมรับความเสี่ยง (Sharing)	<p>การถ่ายโอนหรือแบ่งความเสี่ยงบางส่วนไปยังบุคคลหรือองค์กรอื่นเพื่อลดโอกาสที่จะเกิดความเสี่ยงหรือลดผลกระทบ เช่น การซื้อประกัน การซื้ออนุพันธ์ทางการเงิน เพื่อป้องกันความเสี่ยง (Hedging) การใช้ผู้รับเหมาหรือผู้รับจ้าง อย่างไรก็ตาม การถ่ายโอนความเสี่ยงไปยังบุคคลหรือองค์กรอื่น อาจก่อให้เกิดความเสี่ยงใหม่ เนื่องจากบุคคลหรือองค์กรอื่นนั้น อาจไม่มีวิธีการจัดการความเสี่ยงที่มีประสิทธิภาพ หรือไม่รับรู้ถึงหน้าที่ในการจัดการความเสี่ยงดังกล่าว</p> <ul style="list-style-type: none"> <li>ตัวอย่างการตอบสนองต่อความเสี่ยงโดยใช้กลยุทธ์นี้: การทำประกันภัยโรงงาน การทำ Hedging การร่วมทุนกับบริษัทอื่น</li> </ul>
การหลีกเลี่ยงความเสี่ยง (Avoidance)	<p>ยกเลิกหรือหลีกเลี่ยงกิจกรรมที่ก่อให้เกิดความเสี่ยง การหลีกเลี่ยงความเสี่ยง อาจเกี่ยวกับการหยุดสายการผลิต การยกเลิกการขายตลาดในภูมิภาค หรือการขายหน่วยงาน (Spin-off)</p> <ul style="list-style-type: none"> <li>ตัวอย่างการตอบสนองต่อความเสี่ยงโดยใช้กลยุทธ์นี้: การหยุดและเลิกการดำเนินงาน การปรับปรุงวัตถุประสงค์ เริ่มแรกของกิจการหรือแผนกลยุทธ์</li> </ul>
การดำเนินการต่อ (Pursuing)	<p>ดำเนินการกิจกรรมนั้นต่อ โดยยอมรับความเสี่ยงที่สูงขึ้นเพื่อให้บรรลุผลการปฏิบัติงานที่ต้องการ ในขณะที่ต้องระวังไม่ให้ความเสี่ยงสูงเกินกว่าช่วงเบี่ยงเบนของระดับความเสี่ยงที่องค์กรยอมรับได้ (RT)</p> <ul style="list-style-type: none"> <li>ตัวอย่างการตอบสนองต่อความเสี่ยงโดยใช้กลยุทธ์นี้: แม้ว่าการผลิตก่อให้เกิดของเสียจำนวนมาก อย่างไรก็ตาม องค์กรเลือกที่จะดำเนินการผลิตต่อ เพราะคาดว่าของเสียจากการผลิตจะสามารถนำไปขายต่อเพื่อก่อให้เกิดรายได้ได้</li> </ul>

ทั้งนี้ ในการเลือกวิธีการตอบสนองต่อความเสี่ยงประเภทต่างๆ ตามตารางข้างต้น ควรคำนึงถึง การบริหารความเสี่ยงในบริบทขององค์กร วัตถุประสงค์ในการประกอบกิจการ เป้าหมายของผลการปฏิบัติงาน และระดับความเสี่ยงที่องค์กรยอมรับได้ (RA) ด้วย นอกจากนี้ บางกรณีผู้บริหารอาจจำเป็นต้องพิจารณาการดำเนินการอื่นๆ ร่วมด้วย เช่น

- การทบทวนวัตถุประสงค์ในการประกอบกิจการ : ความรุนแรงของความเสี่ยง และช่วงเบี่ยงเบนของระดับความเสี่ยงที่องค์กรยอมรับได้ (RT) ที่กำหนดขึ้น อาจทำให้องค์กรตัดสินใจทบทวนและปรับปรุงแก้ไขวัตถุประสงค์ในการประกอบกิจการ

กรณีนี้อาจเกิดขึ้นเมื่อวิธีการตอบสนองต่อความเสี่ยงประเภทอื่นๆ ไม่สอดคล้องกับความต้องการขององค์กร

- การทบทวนกลยุทธ์ : ความรุนแรงของความเสี่ยงและระดับความเสี่ยงที่องค์กรยอมรับได้ (RA) ที่กำหนดขึ้น อาจทำให้องค์กรตัดสินใจทบทวนและปรับปรุงแก้ไขกลยุทธ์ กรณีนี้อาจเกิดขึ้นเมื่อวิธีการตอบสนองต่อความเสี่ยงประเภทอื่นๆ ไม่สอดคล้องกับความต้องการขององค์กร เช่นเดียวกับการทบทวนวัตถุประสงค์ในการประกอบกิจการ

องค์กรอาจเลือกที่จะกระทำการที่มีความเสี่ยงสูงเกินกว่าระดับความเสี่ยงที่องค์กรยอมรับได้ (RA) หากพิจารณาแล้วพบว่า ผลกระทบจากการอยู่ภายใต้ระดับความเสี่ยงที่องค์กรยอมรับได้ (RA) ก่อให้เกิดความเสียหายมากกว่า ทั้งนี้ ต้องขออนุมัติจากผู้มีอำนาจในการเลือกวิธีดังกล่าว



#### แนวปฏิบัติเพื่อการต่อยอด

กรณีที่รัฐวิสาหกิจกำหนดความสามารถในการรับความเสี่ยง (RC) และพบว่าความเสี่ยงที่องค์กรเผชิญเกินกว่าความสามารถในการรับความเสี่ยง (RC) จะถือเป็นสถานการณ์ที่อาจก่อให้เกิดอันตรายอย่างมีนัยสำคัญต่อเสถียรภาพและความต่อเนื่องในการดำเนินงานขององค์กร ดังนั้น องค์กรควรเร่งดำเนินการตรวจสอบ รายงาน และจัดการกับความเสี่ยงที่เกินขอบเขตโดยทันที อาจรวมถึงการจัดทำแผนการบริหารจัดการความเสี่ยงเฉพาะกิจหรือการทบทวนกลยุทธ์ขององค์กรใหม่ เพื่อควบคุมและลดระดับความเสี่ยง

การเลือกวิธีการตอบสนองต่อความเสี่ยง ควรพิจารณาถึงผลกระทบ (Impact) และโอกาสที่จะเกิด (Likelihood) ดังนี้

**ตัวอย่างแผนภาพแสดงแนวทางในการกำหนดกลยุทธ์เพื่อตอบสนอง/จัดการความเสี่ยง**

โอกาสที่จะเกิด / ผลกระทบ	ต่ำมาก (1)	ต่ำ (2)	ปานกลาง (3)	สูง (4)	สูงมาก (5)				
สูงมาก (5)	<div style="border: 1px solid black; padding: 5px;"> <p><b>โอกาสที่จะเกิดสูง ผลกระทบสูง</b> รายงานและบริหารความเสี่ยงทันที เช่น</p> <ul style="list-style-type: none"> <li>• จัดตั้งคณะทำงาน</li> <li>• รายงานความคืบหน้าและระดับความเสี่ยงต่อผู้บริหารระดับสูงอย่างสม่ำเสมอ</li> <li>• รายงานความคืบหน้าต่อคณะกรรมการ</li> </ul> </div>								
สูง (4)						<div style="border: 1px solid black; padding: 5px;"> <p><b>โอกาสที่จะเกิดต่ำ ผลกระทบสูง</b> ลดผลกระทบที่อาจเกิดขึ้น เช่น</p> <ul style="list-style-type: none"> <li>• กำหนดแผนการดำเนินงานอย่างต่อเนื่อง</li> <li>• จัดทำประกันภัยต่างๆ</li> </ul> </div>			
ปานกลาง (3)						<div style="border: 1px solid black; padding: 5px;"> <p><b>โอกาสที่จะเกิดปานกลาง ผลกระทบปานกลาง</b> บริหารและติดตามผลเพื่อไม่ให้เกิดผลเสียหายขึ้น เช่น</p> <ul style="list-style-type: none"> <li>• จัดทำแผนปฏิบัติการเพื่อลดความเสี่ยง</li> <li>• ติดตามการดำเนินการตามแผน</li> </ul> </div>			
ต่ำ (2)						<div style="border: 1px solid black; padding: 5px;"> <p><b>โอกาสที่จะเกิดต่ำ ผลกระทบต่ำ</b> ไม่ต้องให้ความสนใจในการจัดการความเสี่ยงมากนัก เช่น</p> <ul style="list-style-type: none"> <li>• ติดตามการควบคุมและกระบวนการปฏิบัติงานตามปกติและต่อเนื่อง</li> <li>• พิจารณาความเสี่ยงตามวาระปกติ</li> </ul> </div>			
ต่ำมาก (1)						<div style="border: 1px solid black; padding: 5px;"> <p><b>โอกาสที่จะเกิดสูง ผลกระทบต่ำ</b> อาจไม่ต้องจัดการความเสี่ยงทันที แต่หากจัดการความเสี่ยงจะสามารถทำให้ผลการดำเนินงานโดยรวมดีขึ้น เช่น</p> <ul style="list-style-type: none"> <li>• ทำให้กระบวนการต่างๆ เป็นอัตโนมัติเพื่อลดความผิดพลาดที่เกิดซ้ำๆ</li> <li>• พัฒนาการฝึกอบรม</li> <li>• กำหนดกิจกรรมการควบคุม</li> </ul> </div>			

นอกจากนี้ ผู้บริหารควรมีการประมาณการต้นทุนและผลประโยชน์ที่ได้รับของวิธีการตอบสนองต่อความเสี่ยงในแต่ละทางเลือก โดยอาจพิจารณาทั้งต้นทุนทางตรง ต้นทุนทางอ้อม ต้นทุนค่าเสียโอกาสในการใช้ทรัพยากร รวมถึงต้นทุนทางสังคมและต้นทุนด้านสิ่งแวดล้อม เช่นเดียวกันกับทางด้านผลประโยชน์ที่ผู้บริหารควรพิจารณาประมาณการทั้งผลประโยชน์ทางตรงและผลประโยชน์ทางอ้อม รวมถึงผลประโยชน์ทางสังคม

และผลประโยชน์ด้านสิ่งแวดล้อม ตามตัวอย่างแบบฟอร์มที่ช่วยในการพิจารณาทางเลือกที่เหมาะสมในการจัดการความเสี่ยง ดังนี้

**ตัวอย่างแบบฟอร์มที่ช่วยในการพิจารณาทางเลือกที่เหมาะสมในการจัดการความเสี่ยง**

ความเสี่ยง	กลยุทธ์การจัดการความเสี่ยง	คำอธิบายวิธีการจัดการความเสี่ยง	ต้นทุน	ผลประโยชน์
	การยอมรับความเสี่ยง (Acceptance)			
	การลดความเสี่ยง (Reduction)			
	การหาผู้ร่วมรับความเสี่ยง (Sharing)			
	การหลีกเลี่ยงความเสี่ยง (Avoidance)			
	การดำเนินการต่อ (Pursuing)			
	อื่นๆ .....			
<b>สรุปทางเลือกที่เหมาะสมในการจัดการความเสี่ยง</b>				

**คำอธิบาย**

- **ต้นทุนทางตรง** คือ ต้นทุนที่รัฐวิสาหกิจใช้ในการก่อให้เกิดกิจกรรมนั้นๆ โดยตรง
- **ต้นทุนทางอ้อม** คือ ต้นทุนที่รัฐวิสาหกิจไม่อาจคิดเข้าโดยตรงเพราะมีการใช้ร่วมกัน จึงจำเป็นต้องมีเกณฑ์ในการปันส่วน
- **ต้นทุนค่าเสียโอกาส** คือ มูลค่าของผลตอบแทนจากกิจกรรมที่สูญเสียโอกาสไปในการเลือกทำกิจกรรมอย่างหนึ่ง ซึ่งเป็นต้นทุนที่ต้องคำนึงถึงเสมอในทางเศรษฐศาสตร์
- **ต้นทุนทางสังคม** คือ ค่าใช้จ่ายหรือผลกระทบเชิงลบที่เกิดขึ้นกับสังคมจากกิจกรรมทางเศรษฐกิจหรือโครงการต่างๆ เช่น การตักงาน ต้นทุนการดูแลสุขภาพ การเพิ่มขึ้นของโรคอุบัติใหม่

- **ต้นทุนด้านสิ่งแวดล้อม** คือ ต้นทุนที่เกิดจากผลกระทบเชิงลบต่อสิ่งแวดล้อม อันเนื่องมาจากกิจกรรมทางเศรษฐกิจหรือการพัฒนา เช่น มลพิษ การสูญเสียธาตุอาหารในดิน การขาดแคลนน้ำ การปล่อยก๊าซเรือนกระจก
- **ผลประโยชน์ทางตรง** คือ ผลประโยชน์ที่รัฐวิสาหกิจได้รับจากกิจกรรมนั้นๆ โดยตรง
- **ผลประโยชน์ทางอ้อม** คือ ผลประโยชน์ที่รัฐวิสาหกิจได้รับจากกิจกรรมที่ไม่ได้ดำเนินการ ซึ่งอาจเป็นผลประโยชน์ที่ได้จากการดำเนินการของกิจกรรมอื่นๆ นอกหน่วยงาน แต่ได้ส่งผลประโยชน์มาสู่หน่วยงาน
- **ผลประโยชน์ทางสังคม** คือ ผลประโยชน์ที่เกิดขึ้นกับสังคมจากกิจกรรมหรือโครงการที่มีเป้าหมายเพื่อพัฒนาคุณภาพชีวิตของประชาชน เช่น เพิ่มเวลาว่างจากการทำงานที่อยู่อาศัยราคาไม่แพง ความรู้สึกมั่นคงปลอดภัย อัตราป่วยการป่วยที่ลดลง
- **ผลประโยชน์ด้านสิ่งแวดล้อม** คือ ผลประโยชน์ที่เกิดขึ้นกับสิ่งแวดล้อมจากกิจกรรมหรือโครงการที่ช่วยลดผลกระทบทางลบหรือฟื้นฟูทรัพยากรธรรมชาติ เช่น คุณค่าของผลประโยชน์จากลุ่มน้ำ การปรับปรุงคุณภาพอากาศและน้ำ ความหลากหลายทางชีวภาพ

นอกจากการพิจารณาด้านทุนและผลประโยชน์ของแต่ละความเสี่ยงแล้ว ผู้บริหารควรพิจารณาเพิ่มเติมต่อเนื่องไปอีกว่าควรเลือกวิธีการตอบสนองต่อความเสี่ยงวิธีใดวิธีหนึ่งหรือใช้หลายๆ วิธีร่วมกัน เพื่อให้โอกาสที่จะเกิดและผลกระทบของความเสี่ยงลดลงมาอยู่ในระดับที่ยอมรับได้ รวมถึงความเป็นไปได้ในการตอบสนองต่อความเสี่ยงหลายๆ ข้อด้วยวิธีการจัดการแบบเดียวกัน

**ตัวอย่าง:** การจัดฝึกอบรมพนักงานเพื่อพัฒนาศักยภาพในการปฏิบัติงาน จัดเป็นการตอบสนองต่อความเสี่ยงได้หลายความเสี่ยงผ่านการดำเนินการด้วยวิธีเดียวกัน กล่าวคือ การจัดฝึกอบรมพนักงานสามารถลดความเสี่ยงจากการปฏิบัติงานผิดพลาด ในขณะเดียวกัน สามารถลดความเสี่ยงจากคุณภาพของสินค้าหรือบริการที่ลดลงได้ด้วย

แนวทางการตอบสนองต่อความเสี่ยงมีหลากหลาย และบางครั้งการตอบสนองต่อความเสี่ยงจากหนึ่งกิจกรรมยังอาจช่วยลดความเสี่ยงได้มากกว่าหนึ่งความเสี่ยง ดังนั้น กระบวนการพิจารณาแนวทางการเลือกสรร รวมทั้งการจัดลำดับความสำคัญควรดำเนินการอย่างเป็นระบบเพื่อให้หน่วยงานต่างๆ มีความเข้าใจที่ตรงกัน

โดยทั่วไปแล้ว แนวทางการตอบสนองต่อความเสี่ยงที่ได้เลือกแล้ว อาจไม่เพียงพอหรือไม่เหมาะสมเมื่อสถานการณ์บางอย่างเปลี่ยนแปลงไป รัฐวิสาหกิจจึงควรพิจารณาปรับเปลี่ยนแนวทางการเลือกสรรและการตอบสนองต่อความเสี่ยงตามความเหมาะสมของสถานการณ์

**ตัวอย่าง:** หากรัฐวิสาหกิจมีทิศทางการขยายการดำเนินงานไปสู่ธุรกิจใหม่ๆ ที่เกี่ยวเนื่องกับธุรกิจหลักดั้งเดิมของรัฐวิสาหกิจ และเคยมีการระบุถึงความเสี่ยงและการตอบสนองต่อความเสี่ยงที่เกี่ยวข้องนั้นๆ แล้ว แต่เมื่อทิศทางในการดำเนินงานเปลี่ยนแปลงไป ผู้บริหารอาจพิจารณาปรับเปลี่ยนการตอบสนองต่อความเสี่ยงนั้น โดยการ “ยอมรับความเสี่ยง” เพื่อที่จะติดตามโอกาสใหม่ๆ ในการพัฒนาธุรกิจนั้นๆ ได้เช่นกัน หรืออีกตัวอย่างหนึ่ง เช่น เมื่อเวลาผ่านไป ผลการประเมินความเสี่ยงในรูปของผลกระทบ และ/หรือโอกาสที่จะเกิด อาจเปลี่ยนแปลงไป รัฐวิสาหกิจอาจจำเป็นต้องทบทวนวิธีการจัดการความเสี่ยงที่ได้เลือกแล้ว ไปใช้วิธีการอื่นๆ ที่มีความเหมาะสมมากกว่า

- (2) กำหนดเวลาในการดำเนินงานที่คาดว่าจะแล้วเสร็จ (วัน เดือน ปี) ของแผนจัดการความเสี่ยงให้ชัดเจน
- (3) กำหนดเจ้าของความเสี่ยง (Risk Owner) ซึ่งหมายถึง ผู้รับผิดชอบในการกำหนดรายละเอียดของแผนจัดการความเสี่ยงหรือกิจกรรมการควบคุมที่จำเป็น รวมถึงงบประมาณที่จำเป็นในการดำเนินการ เพื่อให้มั่นใจว่ามาตรการในการจัดการความเสี่ยงนั้น สามารถจัดการกับความเสี่ยงได้อย่างมีประสิทธิภาพและมีประสิทธิผล และสามารถสัมฤทธิ์ผลได้ตามเวลาที่กำหนด
- (4) ในขั้นตอนการกำหนดแผนจัดการความเสี่ยงควรกำหนดให้สอดคล้องกับสาเหตุของความเสี่ยง โดยอาจพิจารณามาตรการที่มีอยู่แล้วในปัจจุบันและวิเคราะห์หาแนวทางหรือมาตรการที่ควรจัดให้มีเพิ่มขึ้นเพื่อลดความเสี่ยงให้อยู่ในระดับที่องค์กรยอมรับได้ (RA) แผนจัดการความเสี่ยงไม่ควรเป็นกิจกรรมที่ทำอยู่แล้วในปัจจุบัน แต่ควรเป็นกิจกรรมที่ต้องจัดให้มีเพิ่มเติม รวมถึงควรพิจารณาว่าสำหรับความเสี่ยงแต่ละข้อ มีการกำหนดแผนจัดการความเสี่ยงที่ลด “โอกาสที่จะเกิด/ความเป็นไปได้”(Likelihood) หรือ “ผลกระทบ” (Impact) อย่างเหมาะสม เช่น การอบรมเป็นการจัดการความเสี่ยงที่ช่วยลดโอกาสที่จะเกิดความผิดพลาดในการปฏิบัติงาน ในขณะที่การจัดหากรรมธรรม์ประกันภัยเป็นการจัดการความเสี่ยงที่ช่วยลดผลกระทบที่เป็นความเสียหายทางการเงิน



**Tip:**

หากรัฐวิสาหกิจสามารถกำหนดการตอบสนองต่อความเสี่ยงหลายความเสี่ยงด้วยวิธีการจัดการแบบเดียวกันจะช่วยลดต้นทุนในการบริหารความเสี่ยงได้



**Tip:**

การกำหนดแผนจัดการความเสี่ยงที่มีประสิทธิภาพ จะต้องกำหนดให้ครอบคลุมทุกๆ สาเหตุความเสี่ยง

- 3) นำเสนอต่อผู้มีอำนาจเพื่อพิจารณานุมัติตามลำดับชั้น จากนั้นจึงถ่ายทอดให้ผู้ที่เกี่ยวข้องทราบ และนำไปปฏิบัติ รวมถึงจัดให้มีการติดตามความคืบหน้าของการนำแผนจัดการความเสี่ยงไปปฏิบัติด้วย (รายละเอียดของการติดตามจะอธิบายในองค์ประกอบที่ 4 แนวปฏิบัติที่ 1)
  - 4) การตอบสนองต่อความเสี่ยงควรทำอย่างต่อเนื่องและมีการทบทวนอย่างสม่ำเสมอ เพื่อให้การตอบสนองต่อความเสี่ยงนั้นเป็นไปอย่างมีประสิทธิภาพและทันต่อเหตุการณ์
2. รัฐวิสาหกิจควรจัดให้มีการเตรียมความพร้อมเพื่อรองรับเหตุการณ์ไม่คาดคิดที่อาจส่งผลกระทบต่อ การดำเนินงานอย่างต่อเนื่อง โดยเฉพาะในกระบวนการที่สำคัญและมีความเกี่ยวข้องกับการให้บริการหลักขององค์กร โดยพิจารณาจัดทำกระบวนการบริหารความต่อเนื่องทางธุรกิจ (Business Continuity Management: BCM) ของงานหลักๆ ทุกด้าน เพื่อให้องค์กรสามารถดำเนินการได้อย่างต่อเนื่อง รวมถึงควรมีการวิเคราะห์ผลกระทบต่อการดำเนินงาน (Business Impact Analysis: BIA) เพื่อให้มั่นใจว่ามีการเตรียมความพร้อมอย่างเหมาะสมเมื่อเกิดสถานการณ์ฉุกเฉิน โดยรัฐวิสาหกิจควรกำหนดกระบวนการบริหารจัดการความต่อเนื่องทางธุรกิจ (BCM) และแนวปฏิบัติอย่างครบถ้วนและเป็นระบบ ซึ่งประกอบด้วย
- 1) การประเมินความเสี่ยง (Risk Analysis)
  - 2) การวิเคราะห์ผลกระทบต่อการดำเนินงาน (BIA) ที่ครอบคลุมระบบงานที่สำคัญและทิศทางของยุทธศาสตร์องค์กรอย่างครบถ้วน
  - 3) การจัดลำดับความสำคัญของระบบงาน
  - 4) การกำหนดกลยุทธ์แผนบริหารความต่อเนื่องทางธุรกิจ (Business Continuity Plan: BCP)
  - 5) การจัดทำแผนบริหารความต่อเนื่องทางธุรกิจ (BCP)
  - 6) การสื่อสารและฝึกอบรมแผนบริหารความต่อเนื่องทางธุรกิจ (BCP)
  - 7) การทดสอบ ปรับปรุง และการสอบทานแผนบริหารความต่อเนื่องทางธุรกิจ (BCP)
- นอกจากนี้ รัฐวิสาหกิจควรทบทวนกระบวนการบริหารความต่อเนื่องทางธุรกิจ (BCM) เพื่อนำผลไปใช้ในการปรับปรุงกระบวนการ โดยอาจพิจารณาทบทวนเป็นประจำอย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงอย่างมีนัยสำคัญ

## แนวปฏิบัติที่ 5

รัฐวิสาหกิจควรจัดทำภาพรวมความเสี่ยง เพื่อช่วยให้คณะกรรมการและผู้บริหารสามารถพิจารณาความเสี่ยงจากมุมมองความเสี่ยงในภาพรวม เพื่อใช้ในการสื่อสารและนำเสนอข้อมูลความเสี่ยงต่อผู้ที่เกี่ยวข้องในระดับต่างๆ อย่างเป็นระบบ

### คู่มือปฏิบัติ

1. รัฐวิสาหกิจควรพิจารณาจัดทำแบบจำลองเพื่อใช้ในการบริหารความเสี่ยง (Portfolio View of Risk) ซึ่งถือเป็นเทคนิคชนิดหนึ่งในการวิเคราะห์และประเมินความเสี่ยง โดยนำข้อมูลที่เกี่ยวข้องกับความเสี่ยงที่ต้องการพิจารณามาใช้กับแบบจำลอง (Model) เพื่อประเมินผลกระทบของความเสี่ยงออกมาในรูปของตัวเลขหรือจำนวนเงิน (Risk Quantification) และนำผลดังกล่าวมาพิจารณาถึงทางเลือกที่เหมาะสมในการบริหารจัดการความเสี่ยงให้อยู่ในระดับที่องค์กรยอมรับได้ (RA) โดยมีวิธีการจัดทำแบบจำลองเพื่อใช้ในการบริหารความเสี่ยง (Portfolio View of Risk) ประกอบด้วยขั้นตอนอย่างน้อย ดังนี้
  - 1) คัดเลือกความเสี่ยงจากทะเบียนความเสี่ยงที่รัฐวิสาหกิจระบุไว้ เพื่อนำมาทำการวิเคราะห์ความเสี่ยงเชิงปริมาณ โดยความเสี่ยงที่จะนำมาใช้นั้นควรพิจารณาตามความต้องการในการวิเคราะห์ข้อมูล เช่น เป็นความเสี่ยงที่สำคัญ มีผลการประเมินความเสี่ยงอยู่ในระดับสูง โดยความเสี่ยงดังกล่าวต้องมีข้อมูลสนับสนุนที่เพียงพอ เพื่อนำมาจัดทำ Portfolio View of Risk ได้อย่างมีประสิทธิภาพ
  - 2) กำหนดผลลัพธ์ (Output) ที่รัฐวิสาหกิจต้องการทราบ โดยผลลัพธ์ของความเสี่ยงดังกล่าวอาจอยู่ในรูปแบบของรายได้ กำไรสุทธิ สินทรัพย์ เป็นต้น
  - 3) เตรียมข้อมูลประมาณการทางการเงินที่เกี่ยวข้อง (Financial Forecast) เช่น งบกำไรขาดทุน งบแสดงฐานะการเงิน เป็นต้น เพื่อใช้เป็นข้อมูลประกอบการจัดทำแบบจำลอง
  - 4) เลือกเทคนิคการประเมินและวิเคราะห์ภาพรวมความเสี่ยง ซึ่งมีหลากหลายวิธี ดังตัวอย่างต่อไปนี้
    - (1) ประเมินจากข้อมูลในอดีตโดยใช้ข้อมูลทั้งภายนอกและภายในรัฐวิสาหกิจ (Past History – Internal and External Data)
    - (2) ประเมินโดยผู้เชี่ยวชาญ
    - (3) การวิเคราะห์ความไว (Sensitivity Analysis)
    - (4) การวิเคราะห์สถานการณ์สมมติ (Scenario Analysis)
    - (5) การวิเคราะห์ตามแผนภูมิต้นไม้ (Decision Tree Analysis)
    - (6) การวิเคราะห์โดยใช้เทคนิคการจำลองสถานการณ์ (Simulations) เช่น แบบจำลอง Monte Carlo การทดสอบภาวะวิกฤติ (Stress Testing)

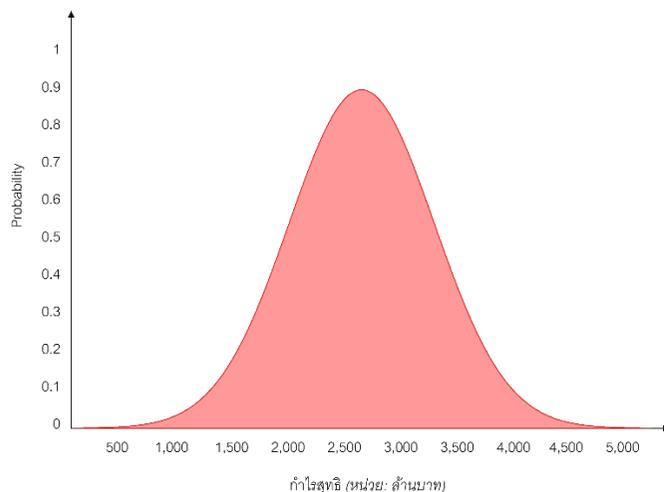
- 5) ระบุและรวบรวมตัวแปรที่เกี่ยวข้องกับความเสี่ยงที่คัดเลือกไว้ในข้อ 1) ทั้งหมด เช่น อัตราแลกเปลี่ยน อัตราดอกเบี้ย ราคาน้ำมัน อัตราการเติบโตของตลาด ส่วนแบ่งตลาด เป็นต้น ทั้งนี้ หากไม่มีข้อมูลที่ต้องการ สามารถใช้การตั้งสมมติฐาน โดยอาศัยข้อมูลจากผู้เชี่ยวชาญหรือผู้บริหารที่เกี่ยวข้อง เพื่อให้สมมติฐานดังกล่าวมีความเหมาะสมกับรัฐวิสาหกิจ
- 6) สร้างแบบจำลอง (Model) โดยใช้ข้อมูลประกอบตามที่ได้เตรียมไว้ในข้อ 3)
- 7) พิจารณาความเชื่อมโยงของข้อมูลของตัวแปรที่เกี่ยวข้องในข้อ 5) กับข้อมูลประมาณการของงบการเงินที่ได้จัดเตรียมไว้ในข้อ 3) เพื่อนำข้อมูลตัวแปรไปผูกกับแบบจำลองดังกล่าวและดำเนินการตามเทคนิคการประเมินและวิเคราะห์ความเสี่ยงที่เลือกไว้ (Run Model)
- 8) วิเคราะห์ผลลัพธ์ที่มีต่อ Output ที่กำหนดไว้ตามข้อ 2)
- 9) สอบทานความถูกต้องของแบบจำลอง (Sanity Check) เพื่อค้นหาข้อผิดพลาดของแบบจำลองในกรณีผลลัพธ์ที่ได้มีความผิดปกติหรือไม่ถูกต้อง
- 10) นำผลที่ได้มาใช้ในการกำหนดแผนจัดการความเสี่ยงต่อไป

ทั้งนี้ องค์การอาจพิจารณาแสดงภาพรวมความเสี่ยงในรูปแบบต่างๆ เช่น กราฟการกระจายความน่าจะเป็น (Probability Distribution/Bell Curve) แผนภาพความเสี่ยง (Heat Map/Risk Map) ตารางการทดสอบภาวะวิกฤติ (Stress Testing) โดยการเลือกใช้ขึ้นอยู่กับวัตถุประสงค์ในการวิเคราะห์และความซับซ้อนของข้อมูล รวมถึงควรคำนึงถึงการสื่อสารภาพรวมความเสี่ยงไปยังผู้บริหารหรือผู้ตัดสินใจอื่นๆ ให้อยู่ในรูปแบบที่เข้าใจง่าย

### ตัวอย่างกราฟการกระจายความน่าจะเป็น

#### สมมติฐาน

- ความเสี่ยงที่สำคัญ ได้แก่ ความเสี่ยงด้านรายได้ และความเสี่ยงด้านความพึงพอใจของผู้รับบริการ
- ความเสี่ยงทั้ง 2 ข้อ อาจทำให้กำไรสุทธิที่ประมาณการไว้ลดลง



## ประโยชน์ที่ได้จากการจัดทำแบบจำลองเพื่อใช้ในการบริหารความเสี่ยง (Portfolio View of Risk)

- 1) ทำให้มีความเข้าใจความเสี่ยงขององค์กรเพิ่มมากขึ้น รวมถึงสร้างความเข้าใจความสัมพันธ์ระหว่างความเสี่ยงต่างๆ ในภาพรวมความเสี่ยง และการเปลี่ยนแปลงของความเสี่ยงภายใต้วิกฤติต่างๆ
- 2) ทำให้ทราบถึงความเหมาะสมของสมมติฐานที่ใช้ในการประเมินความรุนแรงของความเสี่ยง
- 3) ทำให้ทราบประสิทธิผลของวิธีการตอบสนองต่อความเสี่ยงในปัจจุบัน
- 4) เป็นข้อได้เปรียบในการแข่งขันเนื่องจากการจัดการความเสี่ยงที่ดีขึ้น
- 5) เป็นข้อมูลในการตัดสินใจที่เห็นเป็นรูปธรรม ทำให้สามารถตัดสินใจบริหารความเสี่ยงได้ดีขึ้น
- 6) ทำให้สามารถประมาณการต้นทุนและผลประโยชน์ที่จะได้รับในการจัดการความเสี่ยงได้
- 7) สามารถคำนวณประมาณการความสูญเสียที่เกิดจากความเสี่ยงได้
- 8) สอบทานและจัดการความคาดหวังและมุมมองที่เกี่ยวกับความเสี่ยงได้
- 9) ช่วยกำหนดระดับการดำรงเงินทุนตามระดับความเสี่ยง (Risk-based Capital)



### Tip:

- 1) การคัดเลือกความเสี่ยงที่จะนำมาจัดทำแบบจำลองเพื่อใช้ในการบริหารความเสี่ยง (Portfolio View of Risk) อาจใช้หลักการของพาเรโต (80-20 Rule) ได้ เช่น ในจำนวนความเสี่ยงทั้งหมด 10 ข้อ อาจมีความเสี่ยงที่สำคัญมากที่สุดเพียง 2 ข้อ ที่มีผลกระทบต่อองค์กรถึงร้อยละ 80 ดังนั้น จึงควรเลือกความเสี่ยง 2 ข้อดังกล่าวมาทำการวิเคราะห์
- 2) สำหรับข้อมูลที่นำมาใช้ ในบางกรณี การตั้งสมมติฐานโดยผู้เชี่ยวชาญอาจให้ผลลัพธ์ที่ดีกว่าการใช้ข้อมูลในอดีต
- 3) ผลที่ได้จากการทำแบบจำลองเพื่อใช้ในการบริหารความเสี่ยง (Portfolio View of Risk) สามารถนำมาใช้เป็นข้อมูลสนับสนุนในการทบทวนผลการประเมินความเสี่ยงเชิงคุณภาพได้ รวมถึงสามารถนำมาใช้เป็นข้อมูลสนับสนุนในการประเมินประสิทธิภาพของการจัดการความเสี่ยงได้ เช่น เมื่อจัดการความเสี่ยงแล้ว ระดับความเสี่ยงลดลงมาอยู่ในระดับที่ยอมรับได้แล้วใช่หรือไม่

## องค์ประกอบที่ 4 การสอบทานและการแก้ไขปรับปรุง (Review and Revision)

### หลักเกณฑ์

รัฐวิสาหกิจควรมีการติดตามและทบทวนความรู้ความสามารถและแนวปฏิบัติในการบริหารความเสี่ยงขององค์กรอย่างสม่ำเสมอ เพื่อให้มั่นใจว่าองค์กรดำเนินการตามแนวปฏิบัติอย่างมีประสิทธิภาพตามที่ตั้งใจไว้ รวมถึงช่วยให้องค์กรสามารถระบุแนวทางการปรับปรุงการบริหารความเสี่ยง และนำไปพัฒนาประสิทธิภาพของการบริหารความเสี่ยงขององค์กรในทุกระดับ เพื่อให้สามารถปรับเปลี่ยนการบริหารความเสี่ยงหรือประยุกต์ใช้ให้เหมาะสมกับการเปลี่ยนแปลงต่างๆ ได้อย่างทันเวลา

### แนวปฏิบัติที่ 1

รัฐวิสาหกิจควรจัดทำการวิเคราะห์ถึงการเปลี่ยนแปลงต่างๆ ทั้งจากปัจจัยภายในและปัจจัยภายนอกที่ส่งผลต่อการเปลี่ยนแปลงในเกณฑ์การประเมินความเสี่ยง และประเด็นความเสี่ยง ซึ่งอาจส่งผลให้รัฐวิสาหกิจต้องมีการทบทวนแผนการบริหารจัดการความเสี่ยง โดยกำหนดให้มีคณะทำงานหรือผู้รับผิดชอบเพื่อดำเนินการติดตามความเสี่ยงผ่านความคืบหน้าของแผนจัดการความเสี่ยงหรือใช้ดัชนีชี้วัดและรายงานผลการบริหารความเสี่ยงให้กับผู้บริหารสูงสุดหรือผู้กำกับดูแล

### คู่มือปฏิบัติ

1. รัฐวิสาหกิจควรกำหนดให้มีการติดตามความเสี่ยงอย่างต่อเนื่อง โดยมอบหมายให้หน่วยงานบริหารความเสี่ยงเป็นผู้รับผิดชอบหลักในการติดตามการบริหารความเสี่ยง และหน่วยงานบริหารความเสี่ยงสามารถกำหนดให้เจ้าของความเสี่ยง (Risk Owner) เป็นผู้ติดตามได้ รวมถึงผู้บริหารต้องทำการวิเคราะห์เพื่อติดตามแผนการบริหารจัดการความเสี่ยง โดยตัวอย่างของวิธีการติดตามความเสี่ยงมีดังต่อไปนี้
  - 1) ผู้บริหารติดตามผลและดูแลกิจกรรมการบริหารความเสี่ยงผ่านการประชุมตามปกติหรือการประชุมเฉพาะกิจ
  - 2) การบันทึกและการวัดประสิทธิภาพการปฏิบัติงานของกิจกรรมการจัดการความเสี่ยง โดยอาจวัดจากระยะเวลาหรือความก้าวหน้าของกิจกรรม
  - 3) การวัดประสิทธิภาพการปฏิบัติงานโดยอาศัยดัชนีชี้วัด เช่น การพิจารณาจากดัชนีชี้วัดผลการดำเนินงาน (KPI) หรือดัชนีชี้วัดความเสี่ยงหลัก (KRI) หรือ Scorecard หรือ Milestone
  - 4) การพิจารณาและวิเคราะห์จากรายงานเหตุการณ์ร้ายแรงหรือเหตุการณ์ไม่คาดคิด
  - 5) การสำรวจผลการดำเนินงานหรือการเปรียบเทียบกับมาตรฐานต่างๆ (Benchmarking)
  - 6) การประเมินการควบคุมด้วยตนเอง (Control Self - Assessment: CSA)
  - 7) การประเมินผลการดำเนินงานของเจ้าของความเสี่ยง (Risk Owner)

- 8) การสำรวจความเห็นของผู้ร่วมดำเนินกิจกรรมหรือผู้ที่ได้รับผลกระทบจากการจัดการความเสี่ยง
- 9) การสอบทานการปฏิบัติตามนโยบาย กระบวนการ หรือขั้นตอนที่กำหนดขึ้นเพื่อจัดการความเสี่ยง
- 10) การติดตามผลจากความผิดพลาดที่เกิดขึ้น

ทั้งนี้ วิธีที่มักนำมาใช้ในติดตามความเสี่ยง คือ การใช้ดัชนีชี้วัดตามที่ระบุในข้อ 3) โดยรัฐวิสาหกิจสามารถพิจารณาติดตามความเสี่ยงได้ 2 รูปแบบ ได้แก่

1) การติดตามความเสี่ยงโดยใช้ความคืบหน้าของแผนจัดการความเสี่ยง (Milestone)

เจ้าของความเสี่ยง (Risk Owner) เป็นผู้ทำการติดตามว่าการนำแผนจัดการความเสี่ยงไปปฏิบัตินั้น ได้ดำเนินการตามแผนงานและกรอบระยะเวลาที่กำหนดไว้หรือไม่ แล้วบันทึกสถานะของการติดตามว่า ดำเนินการแล้ว อยู่ระหว่างดำเนินการ ดำเนินการล่าช้ากว่ากำหนด หรือยังไม่เริ่มดำเนินการ และเมื่อมีการดำเนินการตามแผนงานดังกล่าวแล้ว เจ้าของความเสี่ยง (Risk Owner) จะต้องประเมินโอกาสที่จะเกิดและผลกระทบของความเสี่ยงอีกครั้งหนึ่ง เพื่อให้มั่นใจว่าระดับความเสี่ยงลดลงมาอยู่ในระดับที่องค์กรยอมรับได้ (RA) แล้วใช่หรือไม่ ในกรณีที่ระดับความเสี่ยงยังสูงเกินกว่าระดับที่องค์กรยอมรับได้ (RA) เจ้าของความเสี่ยง (Risk Owner) จะต้องจัดให้มีมาตรการเพิ่มเติมเพื่อจัดการความเสี่ยงดังกล่าว ทั้งนี้ หน่วยงานบริหารความเสี่ยงสามารถพิจารณากำหนดให้เจ้าของความเสี่ยงเป็นผู้ติดตามและรวบรวมข้อมูลเพื่อรายงานความคืบหน้าของแผนจัดการความเสี่ยง ต่อหน่วยงานบริหารความเสี่ยงเป็นระยะ

2) การติดตามความเสี่ยงโดยใช้ดัชนีชี้วัด

• ดัชนีชี้วัดผลการดำเนินงาน (KPI)

ดัชนีชี้วัดผลการดำเนินงาน (KPI) มักใช้พิจารณาร่วมกับการติดตามความคืบหน้าของแผนจัดการความเสี่ยง โดยจะช่วยให้องค์กรเห็นภาพทั้งระดับการดำเนินงานและผลลัพธ์ที่เกิดขึ้นจริง ได้อย่างชัดเจน ทั้งนี้ องค์กรควรกำหนดดัชนีชี้วัดผลการดำเนินงาน (KPI) ให้เชื่อมโยงกับกลยุทธ์องค์กร เช่น องค์กรที่ให้ความสำคัญกับการให้บริการประชาชน ควรกำหนดให้มีดัชนีชี้วัดผลการดำเนินงาน (KPI) เรื่องการให้บริการประชาชนด้วย รวมถึงควรพิจารณานำหลักการ SMART ที่อธิบายในองค์ประกอบที่ 2 แนวปฏิบัติที่ 4 มาเป็นเครื่องมือช่วยกำหนดดัชนีชี้วัดผลการดำเนินงาน (KPI)

• ดัชนีชี้วัดความเสี่ยงหลัก (KRI)

โดยทั่วไปดัชนีชี้วัดความเสี่ยงหลัก (KRI) มีลักษณะเป็นดัชนีชี้วัดที่สามารถกำหนดค่าได้ (Target/Trigger/Threshold) ซึ่งจะช่วยให้เจ้าของความเสี่ยง (Risk Owner) สามารถเปรียบเทียบค่าจริงกับค่าเป้าหมายของดัชนีชี้วัดความเสี่ยงหลัก (KRI) เพื่อที่จะพิจารณานำแผนจัดการความเสี่ยงมาปฏิบัติ รวมถึงดัชนีชี้วัดความเสี่ยงหลัก (KRI) ยังสามารถทำหน้าที่เตือนภัยล่วงหน้าก่อนที่ความเสี่ยงนั้นจะเกิดขึ้นได้ (Early Warning) อย่างไรก็ตาม การนำดัชนีชี้วัด

ความเสี่ยงหลัก (KRI) มาใช้ มีข้อควรคำนึงถึง กล่าวคือ ความยาก – ยากในการเข้าถึงข้อมูลที่ต้องนำมาใช้ในการคำนวณดัชนีชี้วัดความเสี่ยงหลัก (KRI) รวมถึงการเปรียบเทียบต้นทุนและผลประโยชน์ที่ได้รับจากการจัดทำดัชนีชี้วัดความเสี่ยงหลัก (KRI) ทั้งนี้ การนำดัชนีชี้วัดความเสี่ยงหลัก (KRI) มาใช้ในการติดตามความคืบหน้าของแผนจัดการความเสี่ยง จะช่วยในการประเมินว่าแผนจัดการความเสี่ยงที่กำหนดไว้นั้นเพียงพอหรือไม่ ซึ่งหากค่าที่วัดได้จริงยังคงมีค่าสูงเท่ากับหรือมากกว่าดัชนีชี้วัดความเสี่ยงหลัก (KRI) องค์กรควรพิจารณาปรับปรุงแผนจัดการความเสี่ยง

### ตัวอย่างดัชนีชี้วัดผลการดำเนินงาน (KPI) และดัชนีชี้วัดความเสี่ยงหลัก (KRI)

ด้าน	ดัชนีชี้วัดผลการดำเนินงาน (KPI)	ดัชนีชี้วัดความเสี่ยงหลัก (KRI)
การเงิน	กำไรสุทธิรายไตรมาสเพิ่มขึ้น ร้อยละ 10	อัตราการผิดนัดชำระหนี้เกิน 30 วัน สูงกว่าร้อยละ 5
การบัญชี	ระยะเวลาการปิดบัญชี ไม่เกิน 20 วันนับแต่วันสิ้นเดือน	จำนวนครั้งในการปิดบัญชีไม่ทัน ตามที่กำหนด เกิน 3 ครั้งต่อปี
การให้บริการ ลูกค้า	คะแนนความพึงพอใจ เกินกว่าร้อยละ 75	จำนวนข้อร้องเรียนจากลูกค้า เกินกว่าร้อยละ 10 จากจำนวน การให้บริการทั้งหมด
เทคโนโลยี	ความพร้อมใช้งานของระบบ มากกว่าร้อยละ 99	จำนวนเหตุการณ์ระบบล่ม เกิน 2 ครั้ง ต่อเดือน

2. รัฐวิสาหกิจควรติดตามการเปลี่ยนแปลงที่สามารถส่งผลกระทบต่อการบริหารความเสี่ยงขององค์กร รวมถึงส่งผลกระทบต่อบรรลุลยุทธ์และวัตถุประสงค์ในการประกอบกิจการ ผ่านการระบุการเปลี่ยนแปลงของสภาพแวดล้อมทั้งภายในและภายนอกที่เกี่ยวข้องกับบริบทขององค์กร และการเปลี่ยนแปลงวัฒนธรรมองค์กร

### ตัวอย่างการเปลี่ยนแปลงปัจจัยภายในและปัจจัยภายนอก

ปัจจัยภายใน	ปัจจัยภายนอก
<ul style="list-style-type: none"> <li>• ทรัพยากรบุคคล</li> <li>• ระบบเทคโนโลยีสารสนเทศ</li> <li>• ระบบงานสนับสนุนต่างๆ</li> </ul>	<ul style="list-style-type: none"> <li>• กฎหมาย ระเบียบ หรือข้อบังคับใหม่ หรือที่อยู่ระหว่างดำเนินการ</li> <li>• เทคโนโลยีที่พัฒนาอย่างรวดเร็ว</li> </ul>

ปัจจัยภายใน	ปัจจัยภายนอก
<ul style="list-style-type: none"> <li>• การเปลี่ยนแปลงกลยุทธ์หรือวัตถุประสงค์ในการประกอบกิจการ</li> <li>• การเติบโตอย่างรวดเร็วขององค์กร</li> <li>• การเปลี่ยนแปลงองค์กร และการเปลี่ยนผู้นำขององค์กร</li> <li>• การควบรวมและการซื้อกิจการ</li> <li>• นวัตกรรมขององค์กร</li> </ul>	<ul style="list-style-type: none"> <li>• สภาพตลาด</li> <li>• ภัยธรรมชาติ</li> <li>• ความไม่สงบทางการเมือง</li> <li>• การเปลี่ยนแปลงความคาดหวังของผู้มีส่วนได้เสีย</li> <li>• ภาวะอากาศแปรปรวนที่เกิดขึ้นบ่อยครั้ง</li> <li>• การเปลี่ยนแปลงของเมกะเทรนด์ระดับโลก</li> </ul>

ทั้งนี้ รัฐวิสาหกิจควรติดตามการเปลี่ยนแปลงเหล่านี้อย่างสม่ำเสมอ และเมื่อพบว่ามีเปลี่ยนแปลงที่อาจส่งผลกระทบต่อการบริหารความเสี่ยง รัฐวิสาหกิจควรทบทวนแผนการบริหารจัดการความเสี่ยงให้สอดคล้องกับสถานการณ์ใหม่ เพื่อให้สามารถจัดการความเสี่ยงได้อย่างมีประสิทธิภาพและเท่าทันต่อการเปลี่ยนแปลง

## แนวปฏิบัติที่ 2

รัฐวิสาหกิจควรจัดให้มีการทบทวนแผนการบริหารจัดการความเสี่ยงอย่างสม่ำเสมอและต่อเนื่อง เพื่อให้มั่นใจว่าองค์กรมีการบริหารความเสี่ยงอย่างมีประสิทธิภาพและสนับสนุนให้บรรลุวัตถุประสงค์ในการประกอบกิจการได้

### คู่มือปฏิบัติ

1. การบริหารจัดการความเสี่ยงอาจไม่สามารถบรรลุผลได้อย่างยั่งยืน หากปราศจากการติดตามประเมินผล และทบทวนอย่างสม่ำเสมอ ดังนั้น ผู้บริหารควรสนับสนุนให้มีการจัดโครงสร้างระบบในการทบทวน เรื่องความเสี่ยงทั้งในกรณีปกติและกรณีเกิดเหตุการณ์พิเศษ โดยดำเนินการดังต่อไปนี้

#### 1) กรณีปกติ

รัฐวิสาหกิจควรดำเนินการทบทวนความเสี่ยงตามรอบระยะเวลาที่กำหนด เช่น รายไตรมาส หรือรายปี ผ่านการสอบทานผลการปฏิบัติงาน โดยพิจารณาว่าผลของการบริหารความเสี่ยงเป็นไปตามที่คาดหวัง สามารถช่วยลดความเสี่ยงและทำให้บรรลุเป้าหมายขององค์กรที่ตั้งไว้หรือไม่ รวมถึงพิจารณาถึงความเสี่ยงใหม่ที่กำลังเกิดขึ้นและอาจส่งผลกระทบต่อผลการปฏิบัติงานด้วย

#### 2) กรณีเกิดเหตุการณ์พิเศษ

รัฐวิสาหกิจควรดำเนินการทบทวนความเสี่ยงเฉพาะกิจ เมื่อเกิดเหตุการณ์ที่อาจส่งผลกระทบต่อการบริหารความเสี่ยงหรือส่งผลกระทบต่อบรรลุกลยุทธ์และวัตถุประสงค์ในการประกอบกิจการ

ตามที่ระบุในองค์ประกอบที่ 4 แนวปฏิบัติที่ 1 เช่น ดัชนีชี้วัดความเสี่ยงหลัก (KRI) มีค่าสูง เนื่องจากการเปลี่ยนแปลงสภาพแวดล้อมภายในและภายนอกที่สำคัญ เป็นต้น ทั้งนี้ รัฐวิสาหกิจควรกำหนดให้เจ้าของความเสี่ยง (Risk Owner) พิจารณาทบทวนความเสี่ยง โดยหากพบว่าผลจากการทบทวนความเสี่ยงทั้งในกรณีปกติและกรณีเกิดเหตุการณ์พิเศษ มีความเบี่ยงเบนจากที่คาดการณ์ไว้ ควรแจ้งหน่วยงานบริหารความเสี่ยง รวมถึงพิจารณาปรับปรุง แผนการบริหารจัดการความเสี่ยงและติดตามผลอย่างใกล้ชิด เพื่อให้สามารถรับมือกับสถานการณ์ ปัจจุบันได้อย่างมีประสิทธิภาพ จากนั้นควรรายงานผลต่อคณะกรรมการบริหารความเสี่ยง และผู้บริหาร

### แนวปฏิบัติที่ 3

รัฐวิสาหกิจควรจัดให้มีการปรับปรุงกระบวนการบริหารความเสี่ยงขององค์กรอย่างต่อเนื่อง เพื่อให้สามารถปรับเปลี่ยนการบริหารความเสี่ยงหรือประยุกต์ใช้ให้เหมาะสมกับการเปลี่ยนแปลงต่างๆ ได้อย่างทันเวลา

#### คู่มือปฏิบัติ

1. รัฐวิสาหกิจควรส่งเสริมให้มีการทบทวนและปรับปรุงกระบวนการบริหารความเสี่ยงอย่างต่อเนื่อง ทั้งทั้งองค์กร ตั้งแต่กระบวนการให้ความเห็นชอบและติดตามแผนการบริหารจัดการความเสี่ยง การวางแผนเชิงกลยุทธ์ การบริหารความเสี่ยงเพื่อสร้างเสริมมูลค่าขององค์กร (Value Creation) และการบริหารความเสี่ยงเพื่อเพิ่มมูลค่าขององค์กร (Value Enhancement) การกำหนดผลตอบแทน/แรงจูงใจ การกำหนดเกณฑ์ประเมินระดับความรุนแรง การตอบสนองต่อความเสี่ยงองค์กร การวิเคราะห์แผนภาพแสดงความเชื่อมโยงของความเสี่ยง (Risk Correlation Map) และภาพรวมของความเสี่ยง (Portfolio View of Risk) ขององค์กร รวมทั้งมีการทบทวนและปรับปรุงผลการบริหารความเสี่ยงเพื่อเพิ่มประสิทธิภาพและประสิทธิผลของการบริหารความเสี่ยงขององค์กรในทุกระดับ และนำผลการประเมินกระบวนการดังกล่าวไปสร้างแผนพัฒนากระบวนการ จากนั้นพิจารณาจัดทำรายงานผลการประเมินและแผนพัฒนากระบวนการเสนอต่อคณะกรรมการ ผู้บริหารหรือผู้บังคับบัญชาต่อไป โดยมีปัจจัยที่มักทำให้เกิดการทบทวนและปรับปรุงประสิทธิภาพด้านการบริหารความเสี่ยง ดังต่อไปนี้
  - 1) เทคโนโลยีใหม่

องค์กรที่ต้องจัดการข้อมูลลูกค้าจำนวนมากสามารถเพิ่มประสิทธิภาพในการประมวลผลได้ โดยการนำเทคโนโลยีใหม่ๆ มาใช้

**ตัวอย่าง:** องค์กรอาจพิจารณาทำเหมืองข้อมูล (Data Mining) ซึ่งช่วยให้สามารถวิเคราะห์ข้อมูล และคาดการณ์ความเสี่ยงล่วงหน้าได้อย่างแม่นยำและครอบคลุมมากยิ่งขึ้น ส่งผลให้การตัดสินใจขององค์กรมีประสิทธิภาพมากขึ้น และสามารถลดข้อผิดพลาดที่เคยเกิดขึ้นในอดีตได้อย่างเป็นระบบ

## 2) ข้อบกพร่องในอดีต

การสอบทานผลการดำเนินงานที่ผ่านมาเป็นเครื่องมือสำคัญที่ช่วยให้องค์กรสามารถระบุข้อบกพร่องหรือจุดอ่อนที่เคยเกิดขึ้นแล้วในอดีต รวมถึงสาเหตุของความล้มเหลวต่างๆ ที่ส่งผลกระทบต่อประสิทธิภาพของการบริหารความเสี่ยง ทั้งนี้ แม้ว่าองค์กรอาจมีการดำเนินการบางอย่างเพื่อขจัดข้อยกพร่องเหล่านั้นแล้ว แต่หากข้อผิดพลาดยังคงเกิดขึ้น ผู้บริหารควรพิจารณาทบทวนแนวทางการประเมินความเสี่ยงให้รัดกุมยิ่งขึ้น

**ตัวอย่าง:** หากองค์กรพบว่าในอดีตมีข้อบกพร่องด้านการประเมินความเสี่ยง แม้ว่าจะดำเนินการอย่างอื่นเพื่อขจัดข้อยกพร่องดังกล่าวแล้ว แต่หากข้อผิดพลาดยังคงเกิดขึ้น ดังนั้น องค์กรจึงตัดสินใจปรับปรุงแนวปฏิบัติใหม่ในการประเมินความเสี่ยงเพื่อลดจำนวนข้อบกพร่องและปรับปรุงการบริหารความเสี่ยงองค์กรให้ดีขึ้น

นอกจากนี้ องค์กรอาจพิจารณากำหนดให้มีการประเมินผลอย่างอิสระเพื่อตรวจสอบประสิทธิภาพของระบบการบริหารความเสี่ยง เช่น การตรวจสอบโดยหน่วยงานตรวจสอบภายในขององค์กร หรือการให้หน่วยงานภายนอกเป็นผู้ดำเนินการ เพื่อให้มั่นใจว่าได้รับการประเมินที่เป็นกลางและไม่ถูกรบกวนจากอิทธิพลภายในองค์กร

## 3) การเปลี่ยนแปลงขององค์กร

หากองค์กรมีการเปลี่ยนแปลงอย่างมีนัยสำคัญ องค์กรควรพิจารณาปรับปรุงการบริหารความเสี่ยงให้สอดคล้องกับการเปลี่ยนแปลงดังกล่าว เช่น การเปลี่ยนแปลงโครงสร้างการกำกับดูแล

**ตัวอย่าง:** โดยปกติหน่วยงานที่มีหน้าที่บริหารความเสี่ยงขององค์กรจะรายงานตรงต่อผู้บริหารระดับสูงด้านการเงิน แต่เมื่อองค์กรมีการปรับโครงสร้างกลุ่มงานใหม่ จึงตัดสินใจย้ายหน้าที่ความรับผิดชอบในการบริหารความเสี่ยงไปยังกลุ่มงานที่เกี่ยวข้องกับกลยุทธ์แทน เพื่อให้สอดคล้องกับทิศทางและเป้าหมายใหม่ขององค์กร

## 4) ระดับความเสี่ยงที่องค์กรยอมรับได้ (RA)

การสอบทานผลการปฏิบัติงานช่วยให้องค์กรมองเห็นชัดเจนมากขึ้นว่ามีปัจจัยใดบ้างที่ส่งผลกระทบต่อระดับความเสี่ยงที่องค์กรยอมรับได้ (RA) นอกจากนี้ ยังเป็นการเปิดโอกาสสำหรับผู้บริหารในการพิจารณาปรับเปลี่ยนระดับความเสี่ยงให้เหมาะสมกับสถานการณ์

**ตัวอย่าง:** หากผู้บริหารติดตามผลการดำเนินงานของผลิตภัณฑ์ใหม่ตลอดระยะเวลาหนึ่งปี และพบว่าสถานการณ์ตลาดกำลังเป็นไปด้วยดีและมีความผันผวนน้อยกว่าที่คาดไว้ องค์กรก็อาจพิจารณาเพิ่มระดับความเสี่ยงที่องค์กรยอมรับได้ (RA) สำหรับผลิตภัณฑ์ใหม่ในอนาคต เพื่อเปิดโอกาสให้ธุรกิจเติบโตมากขึ้นภายใต้ความเสี่ยงที่ยังอยู่ในขอบเขตที่ควบคุมได้

5) ประเภทความเสี่ยง

องค์กรที่มุ่งมั่นพัฒนาและปรับปรุงตนเองอย่างต่อเนื่องมักสามารถระบุแนวโน้มของการเปลี่ยนแปลงในธุรกิจได้อย่างทันท่วงที ซึ่งอาจนำไปสู่การทบทวนและปรับปรุงการจัดประเภทของความเสี่ยงให้เหมาะสมยิ่งขึ้น

**ตัวอย่าง:** ในระยะแรก องค์กรไม่ได้จัดให้ความเสี่ยงด้านไซเบอร์อยู่ในประเภทความเสี่ยงหลักขององค์กร แต่เมื่อมีการตัดสินใจนำเสนอสินค้าและบริการผ่านช่องทางออนไลน์ องค์กรจึงได้ปรับปรุงประเภทความเสี่ยงใหม่ โดยเพิ่มความเสี่ยงด้านไซเบอร์เข้าไปด้วย เพื่อให้สามารถกำหนดกลยุทธ์ได้อย่างเหมาะสมกับความเสี่ยงมากยิ่งขึ้น

6) การสื่อสาร

การสอบถามผลการปฏิบัติงานสามารถช่วยให้องค์กรสามารถระบุความเสี่ยงด้านการสื่อสารที่อาจส่งผลกระทบต่อประสิทธิภาพการดำเนินงานได้ รวมถึงช่วยให้ระบุได้ว่ากระบวนการสื่อสารใดที่ล้มล้ม หรือไม่สามารถถ่ายทอดข้อมูลได้อย่างมีประสิทธิภาพ

**ตัวอย่าง:** องค์กรพบว่า การสื่อสารผ่านไปรษณีย์อิเล็กทรอนิกส์ (Email) ไม่สามารถถ่ายทอดข้อมูลสำคัญเกี่ยวกับการบริหารความเสี่ยงไปยังพนักงานได้อย่างมีประสิทธิภาพ ซึ่งอาจนำไปสู่ความล่าช้าหรือความคลาดเคลื่อนในการปฏิบัติงาน ดังนั้น เพื่อบริหารจัดการความเสี่ยงดังกล่าว องค์กรจึงปรับกลยุทธ์การสื่อสารใหม่ โดยใช้ช่องทางที่เหมาะสมยิ่งขึ้น เช่น ระบบส่งข้อความทันที (Instant Messaging) เพื่อเพิ่มการเข้าถึงและการมีส่วนร่วมของพนักงานในกระบวนการสื่อสาร

7) การเปรียบเทียบกับองค์กรอื่น

การเปรียบเทียบผลการดำเนินงานกับองค์กรอื่นในอุตสาหกรรมเดียวกัน เป็นหนึ่งในแนวทางการบริหารความเสี่ยงที่ช่วยให้องค์กรสามารถประเมินสถานะของตนเองเมื่อเทียบกับคู่แข่งรวมทั้งระบุความเสี่ยงที่อาจส่งผลกระทบต่อความสามารถในการแข่งขันในอนาคต

**ตัวอย่าง:** องค์กรดำเนินการเปรียบเทียบ (Benchmarking) ประสิทธิภาพการดำเนินงานด้านการบริหารความเสี่ยงกับคู่แข่งในอุตสาหกรรมเดียวกัน และพบว่า การดำเนินงานขององค์กรมีประสิทธิภาพต่ำกว่าคู่แข่งหลักอย่างมีนัยสำคัญ ซึ่งองค์กรได้ประเมินต้นทุนและผลประโยชน์ที่ได้รับ จึงวางแผนเพื่อปรับปรุงกระบวนการบริหารความเสี่ยง โดยอาจนำระบบปฏิบัติการด้านการบริหารความเสี่ยงเข้ามาใช้เพื่อเพิ่มขีดความสามารถในการปฏิบัติงาน

8) อัตราการเปลี่ยนแปลง

ในการบริหารความเสี่ยง ผู้บริหารควรพิจารณาอัตราการเปลี่ยนแปลงในบริบทขององค์กรที่สำคัญที่องค์กรกำลังเผชิญ

**ตัวอย่าง:** การเปลี่ยนแปลงทางเทคโนโลยีอย่างรวดเร็ว หรือการเปลี่ยนแปลงภายในองค์กรอย่างต่อเนื่อง อาจส่งผลให้องค์กรเผชิญความเสี่ยงใหม่ๆ มากขึ้น จึงจำเป็นต้องมีการปรับปรุงกระบวนการบริหารความเสี่ยงและเพิ่มความคล่องตัวในการตอบสนองต่อความเสี่ยงเหล่านั้น

หากองค์กรพบกับปัจจัยตามที่กล่าวมาแล้วข้างต้น องค์กรควรพิจารณาปรับปรุงกระบวนการบริหารความเสี่ยงอย่างต่อเนื่อง เพื่อให้สามารถปรับกลยุทธ์และการดำเนินงานให้สอดคล้องกับสถานการณ์ที่เปลี่ยนแปลงไปได้อย่างมีประสิทธิภาพ

นอกจากนี้ เพื่อให้การบริหารความเสี่ยงของรัฐวิสาหกิจเป็นไปอย่างมีประสิทธิภาพและสามารถรองรับการเปลี่ยนแปลงหรือความไม่แน่นอนได้อย่างเหมาะสม รัฐวิสาหกิจอาจทำการประเมินระดับวุฒิภาวะ (Maturity Level) ด้านการบริหารความเสี่ยงขององค์กร โดยการประเมินดังกล่าวอาจดำเนินการโดยหน่วยงานอิสระภายนอก เพื่อให้มั่นใจว่าได้ข้อมูลที่เป็นกลาง ปราศจากอคติและข้อมูลมีความน่าเชื่อถือ เพื่อวัดว่าปัจจุบันองค์กรได้จัดให้มีมาตรการควบคุมและการจัดการความเสี่ยงอยู่ในระดับใด และสามารถนำผลการประเมินมาใช้ในการวางแผนและปรับปรุงกระบวนการบริหารความเสี่ยงอย่างต่อเนื่อง

ทั้งนี้ หากผลการประเมินระดับวุฒิภาวะ (Maturity Level) อยู่ในระดับที่ต่ำกว่าที่องค์กรคาดหวัง องค์กรควรใช้ผลลัพธ์ดังกล่าวเป็นจุดริเริ่มในการกำหนดแนวทางปรับปรุงกระบวนการบริหารความเสี่ยง เพื่อพัฒนาความสามารถในการบริหารความเสี่ยงให้มีประสิทธิภาพมากยิ่งขึ้น ทั้งนี้ ควรพิจารณาถึงต้นทุนและผลประโยชน์ที่จะได้รับจากการปรับปรุงกระบวนการร่วมด้วย

## องค์ประกอบที่ 5 สารสนเทศ การสื่อสาร และการรายงาน (Information Communication and Reporting)

### หลักเกณฑ์

รัฐวิสาหกิจควรกำหนดให้มีสารสนเทศและการสื่อสารที่สนับสนุนการบริหารความเสี่ยง ข้อมูลสารสนเทศที่เกี่ยวข้องกับองค์กรทั้งจากแหล่งข้อมูลภายในและภายนอกองค์กรควรได้รับการบันทึกและสื่อสารอย่างเหมาะสมและทันเวลา โดยเฉพาะข้อมูลสนับสนุนที่มีความสำคัญเกี่ยวกับการระบุ การประเมิน และการตอบสนองต่อความเสี่ยง เพื่อให้องค์กรสามารถตอบสนองต่อความเสี่ยงได้อย่างรวดเร็วและมีประสิทธิภาพ รัฐวิสาหกิจควรมีการสื่อสารให้บุคลากรมีความตระหนักและเข้าใจการบริหารความเสี่ยง

### แนวปฏิบัติที่ 1

รัฐวิสาหกิจควรกำหนดให้มีการบริหารสารสนเทศเพื่อการจัดการที่ดี โดยควรจัดให้มีข้อมูลสารสนเทศด้านความเสี่ยงที่เกี่ยวข้องกับองค์กรทั้งจากแหล่งข้อมูลภายในและภายนอกองค์กร และควรได้รับการบันทึกและสื่อสารอย่างเหมาะสมและทันเวลา รวมถึงควรมีคณะทำงานหรือผู้รับผิดชอบด้านการบริหารงานสารสนเทศ เพื่อเพิ่มประสิทธิภาพในการดำเนินงานขององค์กร โดยรัฐวิสาหกิจจะต้องพิจารณาถึงความสมดุลระหว่างผลตอบแทนจากการลงทุน ต้นทุนจากการลงทุน การจัดการด้านเทคโนโลยีและความเสี่ยงที่อาจเกิดขึ้น

### คู่มือปฏิบัติ

1. เพื่อให้การบริหารความเสี่ยงในองค์กรได้เห็นผลในทางปฏิบัติทั่วทั้งองค์กร ผู้บริหารควรพิจารณา กำหนดให้มีระบบสารสนเทศเพื่อการจัดการที่ดี ที่สามารถสนับสนุนการบริหารความเสี่ยงขององค์กรได้ โดยจัดให้มีการปฏิบัติดังต่อไปนี้
  - 1) รวบรวมและศึกษารายการความเสี่ยง ระดับความเสี่ยง และแผนจัดการความเสี่ยง รวมทั้งรายละเอียดที่เกี่ยวข้องจากการประชุมร่วมกันระหว่างผู้มีส่วนเกี่ยวข้องในการบริหารความเสี่ยง และหน่วยงานที่เกี่ยวข้องอื่นๆ ทั้งจากภายในและภายนอกองค์กร
  - 2) พิจารณาถึงความต้องการข้อมูลสำคัญต่างๆ เพื่อให้ประกอบการวิเคราะห์เรื่องความเสี่ยง และการบริหารจัดการความเสี่ยง ผู้บริหารอาจมีการจัดตั้งคณะทำงานกลุ่มย่อยๆ ในแต่ละส่วนงาน เพื่อวิเคราะห์ในรายละเอียดถึงความต้องการด้านข้อมูล ทั้งในเชิงปริมาณและเชิงคุณภาพ รวมทั้งวิเคราะห์และหาแนวทางเพื่อให้มั่นใจว่าข้อมูลมีความเพียงพอ ถูกต้องและทันเวลา

3) นอกจากนี้ในระดับองค์กร รัฐวิสาหกิจควรจัดให้มีการจัดการที่ดีในเรื่องกลยุทธ์ด้าน IT ขององค์กร เช่น การจัดตั้งคณะกรรมการกำหนดกลยุทธ์ด้าน IT (IT Strategy Committee) โดยอย่างน้อยควรมีผู้บริหารระดับสูงเป็นประธานอนุกรรมการ และกำหนดหน้าที่ความรับผิดชอบในการดำเนินงาน รวมถึงดำเนินการประชุมทุกเดือน หรือมีการประชุมเมื่อมีการเปลี่ยนแปลงที่เป็นสาระสำคัญของระบบสารสนเทศขององค์กร โดยระหว่างขั้นตอนการพิจารณาเรื่องข้อมูล คณะทำงานกลุ่มย่อย หรือผู้มีส่วนเกี่ยวข้องควรมีการสื่อสารที่ชัดเจนถึงวัตถุประสงค์ในการดำเนินการ และสรุปสิ่งที่ได้จากการสัมภาษณ์หรือประชุมกับผู้ที่เกี่ยวข้องในการให้ข้อมูลประกอบต่างๆ ดังนี้

- ความเสี่ยง
- ลักษณะข้อมูลต่างๆ ที่ต้องการใช้
- ลักษณะความถี่ของข้อมูลที่มีการนำเสนอ
- รูปแบบของข้อมูล

โดยทั่วไปแล้วข้อมูลสำคัญที่องค์กรต้องนำมาใช้ในการวิเคราะห์เรื่องความเสี่ยง เป็นข้อมูลที่มีอยู่แล้ว แต่อาจกระจัดกระจายไปตามส่วนงานต่างๆ และอยู่ในรูปแบบต่างๆ เช่น ในรูป Spreadsheet ในบางเรื่องของฝ่ายนั้นๆ หรือในรูปเอกสารการประชุม เป็นต้น

4) ในขั้นตอนการวิเคราะห์เรื่องระบบสารสนเทศนี้ ในบางกรณี บทสรุปการวิเคราะห์ชี้ให้เห็นว่าองค์กรควรมีการลงทุนเพิ่มเติมในด้านระบบสารสนเทศใหม่ๆ เช่น การลงทุนซื้อ Software Hardware หรือ Application ใหม่ๆ คณะทำงานควรมีการจัดทำการวิเคราะห์และประเมินเรื่องต้นทุนและผลตอบแทนจากการลงทุนด้วย นอกจากนี้ หากกระบวนการพิจารณาอนุมัติจากฝ่ายบริหารดำเนินการแล้วเสร็จ ผู้บริหารควรมีการวางแผนแนวทางในการประเมิน ควบคุมและติดตามต่อไป เพื่อให้กระบวนการลงทุนและติดตั้งระบบสารสนเทศนั้นสำเร็จได้ตามระยะเวลาที่กำหนด และสามารถให้ประโยชน์ หรือผลตอบแทนตามที่ประมาณการไว้

5) รัฐวิสาหกิจควรจัดให้มีการประเมินและทบทวนศักยภาพของ IT และการจัดการดังกล่าวอย่างสม่ำเสมอ ทั้งในด้านการเงินและมีใช้การเงิน เช่น อัตราการเพิ่มของผลตอบแทนที่ได้จากการลงทุนด้าน IT และระยะเวลาของการเปลี่ยนแปลงกระบวนการและระบบการทำงาน เป็นต้น หากการประเมินพบว่าผลการดำเนินงานด้าน IT ดังกล่าวต่ำกว่าเป้าหมายเกินกว่าระดับความเสี่ยงที่องค์กรยอมรับได้ (RA) รัฐวิสาหกิจควรจัดทำแผนรองรับที่ชัดเจน

ทั้งนี้ ในการนำระบบสารสนเทศมาใช้ รัฐวิสาหกิจควรจัดให้มีมาตรการในการบริหารจัดการข้อมูลอย่างมีประสิทธิภาพ เพื่อให้ได้สารสนเทศที่ถูกต้องและเหมาะสมในการสนับสนุนการตัดสินใจที่ตระหนักถึงความเสี่ยง โดยพิจารณา 3 ปัจจัย ดังนี้

1) การกำกับดูแลข้อมูลและสารสนเทศ

รัฐวิสาหกิจควรกำกับดูแลให้มีข้อมูลเกี่ยวกับการบริหารความเสี่ยงที่มีมาตรฐานและคุณภาพสามารถนำมาใช้ได้ทันต่อเวลา ตรวจสอบได้ และปลอดภัย โดยกำหนดให้มีผู้อนุมัติความถูกต้องของการนำเข้าข้อมูล

2) กระบวนการและการควบคุม

รัฐวิสาหกิจควรกำหนดกระบวนการควบคุมข้อมูลเพื่อช่วยป้องกันและลดความเสี่ยงในการเข้าถึงข้อมูลที่สำคัญ โดยการกำหนดสิทธิการเข้าถึงข้อมูลที่เกี่ยวข้องกับการบริหารความเสี่ยงอย่างเคร่งครัด เพื่อให้มั่นใจว่าเฉพาะผู้ที่มีสิทธิและความรับผิดชอบเท่านั้นที่สามารถบันทึกหรือปรับปรุงข้อมูลได้ การแยกหน้าที่และการควบคุมการเข้าถึงจะช่วยป้องกันการเกิดความเสี่ยงจากการใช้ข้อมูลไม่ถูกต้อง หรือการจัดการข้อมูลที่ไม่เหมาะสม

3) สถาปัตยกรรมการจัดการข้อมูล

รัฐวิสาหกิจควรจัดให้มีการออกแบบชั้นพื้นฐานของเทคโนโลยี ซึ่งประกอบด้วย แบบจำลองนโยบาย กฎระเบียบ หรือมาตรฐานที่ใช้กำหนดว่าข้อมูลใดควรถูกเก็บรวบรวมมาใช้พิจารณาในการบริหารความเสี่ยง และมีวิธีการเก็บรักษา จัดการ และนำไปใช้ในระบบและในองค์กรอย่างไร เพื่อให้สามารถบริหารจัดการข้อมูลและบริหารความเสี่ยงได้อย่างมีคุณภาพ

ทั้งนี้ การพิจารณานำสารสนเทศมาสนับสนุนแนวปฏิบัติในการบริหารความเสี่ยงขององค์กรในแต่ละองค์ประกอบ รัฐวิสาหกิจสามารถพิจารณาได้ดังตัวอย่างต่อไปนี้

- แนวปฏิบัติสำหรับองค์ประกอบที่ 1 การกำกับดูแลและวัฒนธรรมองค์กร  
องค์กรอาจต้องการสารสนเทศเกี่ยวกับมาตรฐานที่พึงปฏิบัติและผลการปฏิบัติงานรายบุคคลที่เกี่ยวกับมาตรฐานดังกล่าว

**ตัวอย่าง:** จัดให้มีระบบในการติดตามการฝึกอบรมด้านการบริหารความเสี่ยงของพนักงาน เพื่อให้มั่นใจว่าพนักงานทุกคนได้รับการฝึกอบรมอย่างครบถ้วน รวมถึงจัดให้มีระบบจัดเก็บผลการทดสอบหลังจากการอบรม เพื่อใช้ในการวิเคราะห์ความรู้ความเข้าใจด้านการบริหารความเสี่ยงของพนักงาน

- แนวปฏิบัติสำหรับองค์ประกอบที่ 2 กลยุทธ์และการกำหนดวัตถุประสงค์  
องค์กรอาจต้องการสารสนเทศในเรื่องความคาดหวังของผู้มีส่วนได้เสียเกี่ยวกับระดับความเสี่ยงที่องค์กรยอมรับได้ (RA)

**ตัวอย่าง:** องค์กรจัดเก็บข้อมูลระดับความเสี่ยงที่ยอมรับได้ (RA) จากผู้บริหารระดับสูง โดยให้ทำแบบสอบถามผ่านระบบและนำข้อมูลดังกล่าวมาวิเคราะห์ และพิจารณากำหนดระดับความเสี่ยงที่องค์กรยอมรับได้ (RA)

- แนวปฏิบัติสำหรับองค์กรประกอบที่ 3 ผลการปฏิบัติงาน

องค์กรอาจต้องการสารสนเทศเกี่ยวกับคู่แข่งเพื่อประกอบการประเมินความเสี่ยง

**ตัวอย่าง:** องค์กรที่ให้บริการขนส่งสาธารณะอาจต้องประเมินความเสี่ยงจากการสูญเสียผู้รับบริการไปยังผู้ให้บริการเอกชนรายใหม่ที่มีการให้บริการผ่าน Application และมีโครงสร้างค่าโดยสารที่ยืดหยุ่นหรือมีโปรโมชั่นจูงใจลูกค้า องค์กรจึงควรจัดเก็บสารสนเทศที่เกี่ยวข้อง เช่น รูปแบบการคิดค่าบริการของคู่แข่ง แผนการทำการตลาดผ่านช่องทางดิจิทัล และแนวโน้มพฤติกรรมผู้บริโภค เพื่อนำมาประกอบการพิจารณาทบทวนแผนการดำเนินงาน รวมถึงกลยุทธ์การให้บริการขององค์กร เพื่อรักษาความสามารถในการแข่งขันและบรรลุเป้าหมายการให้บริการตามภารกิจที่ได้รับมอบหมาย

- แนวปฏิบัติสำหรับองค์กรประกอบที่ 4 การสอบทานและการแก้ไขปรับปรุง

องค์กรอาจต้องการสารสนเทศเกี่ยวกับแนวโน้มที่กำลังจะเกิดขึ้นในการบริหารความเสี่ยงขององค์กร โดยสามารถรวบรวมสารสนเทศดังกล่าวจากการเข้าร่วมสัมมนาเกี่ยวกับการบริหารความเสี่ยงขององค์กรและติดตามข่าวสารของอุตสาหกรรมที่องค์กรดำเนินกิจการอยู่

**ตัวอย่าง:** องค์กรติดตามแนวโน้มเกี่ยวกับการโจมตีทางไซเบอร์รูปแบบใหม่ จากบทความและข่าวสารขององค์กรในด้านความปลอดภัยไซเบอร์ หากพบว่ามีกรณีเพิ่มขึ้นของภัยคุกคามแบบ Phishing Email ภายในองค์กร ควรนำข้อมูลนี้มาทบทวนแผนการบริหารจัดการความเสี่ยงเดิม และจัดอบรมบุคลากรเกี่ยวกับวิธีระงับภัยไซเบอร์ที่เป็นปัจจุบัน เพื่อให้มั่นใจว่าบุคลากรจะสามารถรับมือได้อย่างเหมาะสมและทันเวลาที่

## ประโยชน์จากการนำระบบสารสนเทศมาใช้ในการรวบรวมและรายงานสารสนเทศที่เกี่ยวข้องกับความเสี่ยง

- การติดตามและการสื่อสารได้อย่างต่อเนื่องและทันเวลาที่
- การตัดสินใจบนพื้นฐานข้อมูลที่ครบถ้วนและน่าเชื่อถือ
- การมองภาพความเสี่ยงได้ครอบคลุมทั่วทั้งองค์กร
- การทำงานร่วมกันเป็นทีมและข้ามหน่วยงาน

2. รัฐวิสาหกิจควรจัดให้มีข้อมูลสารสนเทศที่เกี่ยวข้องกับองค์กร ทั้งจากแหล่งข้อมูลภายในและภายนอกองค์กร และควรได้รับการบันทึกและสื่อสารอย่างเป็นระบบและทันเวลา

สิ่งที่ท้าทายในเรื่องระบบสารสนเทศและการจัดการความเสี่ยง คือ การประมวลผลและการกลั่นกรองข้อมูลที่มีอยู่จำนวนมากให้กลายเป็นสารสนเทศที่ใช้งานได้ และสามารถเป็นส่วนประกอบในการตัดสินใจต่างๆของผู้บริหารในเรื่องกลยุทธ์และการดำเนินงาน ระบบสารสนเทศดังกล่าวนี้ อาจมาจาก

- 1) แหล่งข้อมูลภายในองค์กร เช่น รายงานการประชุมประจำเดือน รายงานทิศทางการธุรกิจขององค์กร รายงานการตรวจสอบภายใน รายงานสภาพคล่อง รายงานความเสี่ยง
- 2) แหล่งข้อมูลภายนอกองค์กร เช่น ข้อมูลทางเศรษฐกิจ ข้อมูลทางการตลาด บทความทางธุรกิจ บทความที่เกี่ยวข้องกับอุตสาหกรรมหรือธุรกิจที่องค์กรดำเนินกิจการอยู่

ระบบสารสนเทศที่เกี่ยวข้องในเรื่องการบริหารความเสี่ยงนี้ควรมีการบันทึกอย่างเป็นระบบตามความเหมาะสมของข้อมูลนั้นๆ เช่น อาจมีการบันทึกในรูปแบบรายงานที่เป็นลายลักษณ์อักษร หรืออาจมีการบันทึกในรูปแบบตัวเลขข้อมูลในระบบคอมพิวเตอร์

นอกจากนี้ ข้อมูลสารสนเทศควรมีการสื่อสารให้เป็นที่เข้าใจในแนวทางเดียวกันอย่างเหมาะสม เช่น หากเป็นข้อมูลเกี่ยวกับความเสี่ยงในระดับองค์กร ควรมีการจัดทำข้อมูลสรุปเป็นภาพรวมเพื่อนำเสนอให้ผู้บริหารใช้ประกอบการพิจารณาเชิงนโยบาย แต่หากเป็นข้อมูลที่เกี่ยวข้องกับความเสี่ยงเฉพาะของแต่ละหน่วยงาน ควรมีการวิเคราะห์และสรุปในระดับหน่วยงาน เพื่อให้พนักงานสามารถเข้าใจและบริหารจัดการความเสี่ยงของตนเองได้อย่างตรงจุด

ระบบสารสนเทศกับการสื่อสารที่เหมาะสมอย่างทันเวลา จะขึ้นอยู่กับลักษณะความเสี่ยงที่พิจารณา เช่น ความเสี่ยงระดับองค์กร คือ การพิจารณาความเสี่ยงในภาพรวมซึ่งโดยทั่วไปจะพิจารณาเป็นรายไตรมาสหรือรายปี หรือเมื่อมีเหตุการณ์สำคัญที่อาจส่งผลกระทบต่อภาพรวมขององค์กร ผู้บริหารต้องการข้อมูลสารสนเทศเพื่อประกอบการพิจารณาในเรื่องดังกล่าวร่วมกับการวางแผนกลยุทธ์ ในขณะที่การพิจารณาระบบสารสนเทศสำหรับการบริหารความเสี่ยงด้านตลาด เช่น อัตราแลกเปลี่ยน อัตราดอกเบี้ย ราคาน้ำมัน เป็นต้น ควรดำเนินการเป็นรายวัน เพื่อให้ได้รับข้อมูลประกอบการตัดสินใจอย่างเหมาะสมและทันเวลา

## แนวปฏิบัติที่ 2

รัฐวิสาหกิจควรกำหนดช่องทางที่จะสื่อสารข้อมูลและสารสนเทศด้านความเสี่ยงต่อผู้มีส่วนได้เสียภายในและภายนอก อีกทั้งอาจพิจารณากำหนดให้มีช่องทางการสื่อสารอื่นๆ ที่อยู่นอกเหนือจากช่องทางการสื่อสารปกติขององค์กร เช่น สายด่วนแจ้งเบาะแสและข้อร้องเรียน (Whistle- Blower Hotline) เพื่อให้ผู้ร้องเรียนสามารถรายงานเพิ่มเติมได้โดยไม่ส่งผลกระทบต่อผู้ร้องเรียน

### คู่มือปฏิบัติ

1. ผู้บริหารควรจัดให้มีช่องทางการสื่อสารข้อมูลและสารสนเทศด้านความเสี่ยงต่อผู้มีส่วนได้เสียทั้งภายในและภายนอก เพื่อให้ผู้บริหารสามารถสื่อสารกลยุทธ์ วัตถุประสงค์ในการประกอบกิจการ และสร้างความรู้ความเข้าใจในการตระหนักรู้และทัศนคติต่อการบริหารความเสี่ยงของพนักงาน

ได้ทั่วทั้งองค์กร เพื่อให้มั่นใจว่าบุคลากรที่เกี่ยวข้องเข้าใจบทบาทหน้าที่ของตนเองต่อการบริหารความเสี่ยง และกำหนดช่องทางเปิดรับสารสนเทศจากผู้มีส่วนได้เสียภายนอก เช่น ไปรษณีย์ อิเล็กทรอนิกส์ (Email) การอภิปรายสาธารณะ เว็บไซต์ สายด่วน หรือช่องทางอื่นๆ เพื่อช่วยให้สามารถระบุความเสี่ยงที่อาจเกิดขึ้นต่อองค์กรได้ รวมถึงกำหนดให้มีการทบทวนความเหมาะสมของช่องทาง การสื่อสารและปรับปรุงให้สอดคล้องกับความก้าวหน้าของเทคโนโลยีในสถานการณ์ปัจจุบัน

### ตัวอย่างสารสนเทศที่จำเป็นและวิธีการสื่อสารกับผู้มีส่วนได้เสียทั้งภายในและภายนอก

ผู้มีส่วนได้เสีย	สารสนเทศที่จำเป็น	วิธีการสื่อสาร
<b>1. กลุ่มผู้มีส่วนได้เสียภายใน</b>		
คณะกรรมการ	<ul style="list-style-type: none"> <li>การเปลี่ยนแปลงที่สำคัญของสภาพแวดล้อมทางธุรกิจ ทั้งภายในและภายนอก และการตอบสนองขององค์กร ต่อการเปลี่ยนแปลงดังกล่าว</li> <li>ความเสี่ยงที่สูงเกินกว่าระดับความเสี่ยงที่องค์กรยอมรับได้ (RA) หรือช่วงเบี่ยงเบนของระดับความเสี่ยงที่องค์กรยอมรับได้ (RT)</li> <li>ประสิทธิผลโดยรวมของการตอบสนองต่อความเสี่ยง</li> </ul>	<ul style="list-style-type: none"> <li>เอกสารประกอบการประชุม ที่ส่งให้คณะกรรมการล่วงหน้าและการนำเสนอ</li> </ul>
ผู้บริหาร	<ul style="list-style-type: none"> <li>การเปลี่ยนแปลงที่สำคัญของสภาพแวดล้อม ทั้งภายในและภายนอกที่กระทบต่อกลยุทธ์ และระดับความเสี่ยงที่องค์กรยอมรับได้ (RA)</li> <li>การเปลี่ยนแปลงที่สำคัญของความเสี่ยง หรือแบบจำลองเพื่อใช้ในการบริหารความเสี่ยง (Portfolio View of Risk)</li> <li>สถานะและประสิทธิผลของการตอบสนองต่อความเสี่ยง</li> </ul>	<ul style="list-style-type: none"> <li>เอกสารภายในที่เป็นลายลักษณ์อักษร เช่น รายงานสรุป รายงานแผนแสดงหน้าจอข้อมูลชี้วัด (Dashboard) การประเมินผลการปฏิบัติงาน การนำเสนอ แบบสอบถาม และแบบสำรวจ นโยบาย และแนวปฏิบัติ คำถามที่พบบ่อย (FAQs)</li> <li>การสื่อสารด้วยวาจา หรือไม่เป็นทางการ เช่น การสนทนาแบบตัวต่อตัว การประชุม</li> </ul>

ผู้มีส่วนได้เสีย	สารสนเทศที่จำเป็น	วิธีการสื่อสาร
พนักงาน	<ul style="list-style-type: none"> <li>ลักษณะของการตอบสนองต่อความเสี่ยงและผลกระทบต่อหน้าที่และความรับผิดชอบ</li> <li>ความสำคัญของกิจกรรมการตอบสนองต่อความเสี่ยงสำหรับองค์กร</li> </ul>	<ul style="list-style-type: none"> <li>การฝึกอบรม สัมมนา การฝึกอบรมเชิงปฏิบัติการ การเผยแพร่ผ่าน อินเทอร์เน็ต (Webcast) หรือวิดีโออื่นๆ</li> <li>เอกสารการประชุม หรือการมีปฏิสัมพันธ์กัน</li> <li>ข้อความอิเล็กทรอนิกส์ เช่น ไปรษณีย์อิเล็กทรอนิกส์ (Email) โซเชียลมีเดีย การส่งข้อความ ระบบส่งข้อความทันที (Instant Messaging)</li> <li>งานกิจกรรมสาธารณะ เช่น การจัดงานตามสถานที่ต่างๆ (Road Shows) การจัดประชุมใหญ่ (Town Hall) การสัมมนาของกลุ่มอุตสาหกรรม หรือวิชาชีพเฉพาะทาง</li> </ul>
<b>2. กลุ่มผู้มีส่วนได้เสียภายนอก</b>		
หน่วยงานกำกับดูแล	<ul style="list-style-type: none"> <li>รายงานแผนการบริหารจัดการความเสี่ยง</li> <li>รายงานผลตามแผนการบริหารจัดการความเสี่ยง</li> </ul>	<ul style="list-style-type: none"> <li>หนังสือราชการ</li> </ul>
นักลงทุน	<ul style="list-style-type: none"> <li>ความเสี่ยงและแนวทางการบริหารความเสี่ยงขององค์กร</li> </ul>	<ul style="list-style-type: none"> <li>การประชุมสามัญผู้ถือหุ้นประจำปี</li> <li>รายงานประจำปี</li> <li>รายงานผลการบริหารความเสี่ยง</li> <li>รายงานการพัฒนาความยั่งยืน</li> <li>การแต่งตั้งตัวแทน (Proxy)</li> </ul>

ผู้มีส่วนได้เสีย	สารสนเทศที่จำเป็น	วิธีการสื่อสาร
ผู้ชาย	<ul style="list-style-type: none"> <li>มาตรฐานสำหรับผู้ชาย เช่น จริยธรรม ความซื่อตรง มาตรฐานตามกฎหมาย การปฏิบัติตามกฎระเบียบ ข้อกำหนดด้านอาชีพอนามัย ความปลอดภัย และสิ่งแวดล้อม</li> <li>ผลการปฏิบัติงานของผู้ชายเทียบกับมาตรฐานที่เกี่ยวกับความเสี่ยงขององค์กร</li> </ul>	<ul style="list-style-type: none"> <li>จรรยาบรรณสำหรับผู้ชาย</li> <li>ใบรายงาน เช่น คุณภาพ การส่งมอบ จำนวนที่ส่งมอบ ผลการปฏิบัติงานในอดีต รายงานเหตุการณ์ และความคิดเห็น</li> <li>การประชุมผู้บริหาร</li> </ul>
ลูกค้า	<ul style="list-style-type: none"> <li>ข้อมูล รายละเอียดของการให้บริการ</li> <li>ข้อมูลวิธีใช้ผลิตภัณฑ์ และผลกระทบต่อสุขภาพ และความปลอดภัยของผู้ใช้ (ถ้ามี) เช่น ผลข้างเคียงของยา</li> </ul>	<ul style="list-style-type: none"> <li>การสื่อสารทางการตลาด</li> <li>ฉลากผลิตภัณฑ์และข้อมูลประกอบ เช่น ข้อมูลโภชนาการ</li> <li>การแสดงใบอนุญาต หรือการรับรองจากผู้เชี่ยวชาญ เช่น เกสัชกร</li> <li>การแสดงความเห็นกลุ่มย่อย (Focus Group)</li> </ul>

2. ผู้บริหารควรพิจารณาจัดให้มีช่องทางการสื่อสารอื่นๆ ที่แยกออกจากการรายงานตามสายงาน การบังคับบัญชาแบบปกติ เพื่อเป็นกลไกป้องกันความผิดพลาดในกรณีช่องทางปกติไม่ทำงาน ไม่โปร่งใสหรือทำให้ผู้ที่ต้องการรายงานเกิดความไม่มั่นใจในความปลอดภัยในหน้าที่ความรับผิดชอบของตนเอง รัฐวิสาหกิจอาจพิจารณาจัดให้มีช่องทางการสื่อสารโดยตรงถึงหัวหน้าหน่วยงานตรวจสอบภายในหรือฝ่ายกฎหมาย หรือผู้บริหารระดับสูงอื่นๆ ที่สามารถเข้าถึงคณะกรรมการได้

รัฐวิสาหกิจสามารถกำหนดนโยบายการรายงานเบาะแส หรือนโยบายการร้องเรียน (Whistle Blowing Policy) ซึ่งนโยบายนี้จะช่วยให้รัฐวิสาหกิจทราบถึงความผิดปกติที่อาจเกิดขึ้นภายในรัฐวิสาหกิจ รวมถึงการกระทำที่ผิดกฎหมายหรือการไม่ปฏิบัติตามระเบียบ ข้อบังคับ และจรรยาบรรณ ในการประกอบกิจการ (Code of Conduct) โดยจะมีการกำหนดช่องทางสำหรับพนักงาน ในการรายงานการกระทำผิดกฎหมายการทุจริตคอร์รัปชัน การกระทำที่ไม่ถูกต้อง ไม่เหมาะสม หรือผิดศีลธรรม จริยธรรม เช่น กล่องรับข้อร้องเรียน เบอร์โทรศัพท์ที่พนักงานสามารถโทรเข้ามา เพื่อรายงาน (สายด่วนเพื่อรายงาน) ไปรษณีย์อิเล็กทรอนิกส์ (Email) หรือเว็บไซต์ของรัฐวิสาหกิจ เป็นต้น

ทั้งนี้ รัฐวิสาหกิจจะต้องกำหนดหน่วยงานผู้รับผิดชอบ และกำหนดแนวปฏิบัติของนโยบายและขั้นตอนอย่างชัดเจน ตัวอย่างของแนวปฏิบัติ เช่น

- ดำเนินการกับเรื่องที่ได้รับการรายงานอย่างเป็นทางการเป็นความลับ ตั้งแต่การรับเรื่อง การสอบสวน ตลอดจนการจัดการที่เหมาะสม เช่น เสนอแนวทางแก้ไขและบทลงโทษแก่ผู้บังคับบัญชาภายในระยะเวลาที่กำหนด
- กำหนดให้มีมาตรการเพื่อคุ้มครองผู้แจ้งเบาะแสหรือผู้ร้องเรียน โดยกำหนดให้ข้อมูลเกี่ยวกับการแจ้งเบาะแสหรือข้อร้องเรียนและข้อมูลส่วนบุคคลของผู้ที่เกี่ยวข้องจะถูกเก็บรักษาเป็นความลับ ไม่เปิดเผยต่อบุคคลที่ไม่เกี่ยวข้อง โดยจำกัดการเข้าถึงข้อมูลเฉพาะผู้รับผิดชอบในการตรวจสอบเรื่องที่ร้องเรียนเท่านั้น นอกจากนี้ กรณีที่ผู้แจ้งเบาะแสหรือผู้ร้องเรียนและผู้ที่มีความร่วมมือในการตรวจสอบข้อเท็จจริงเห็นว่าตนเองอาจเดือดร้อนหรือเสียหาย สามารถร้องขอให้องค์กรคุ้มครองตามมาตรการที่องค์กรกำหนด
- กำหนดให้มีการรายงานให้กับผู้บริหารระดับสูง หรือคณะกรรมการได้รับทราบ

**ตัวอย่างหัวข้อของนโยบายการรายงานเบาะแส หรือนโยบายการร้องเรียน (Whistle Blowing Policy)**

- บทนำ
- ขอบเขตของนโยบาย
- การคุ้มครองผู้ร้องเรียน
- การรักษาความลับ
- การเปิดเผยชื่อผู้ร้องเรียน
- ขั้นตอนและช่องทางการร้องเรียน
- ขั้นตอนการสอบสวน

**แนวปฏิบัติที่ 3**

รัฐวิสาหกิจควรมีการกำหนดกระบวนการและผู้รับผิดชอบในการรายงานความเสี่ยงต่อคณะกรรมการรายงานเกี่ยวกับวัฒนธรรมการบริหารความเสี่ยงในองค์กร รูปแบบของรายงาน ความถี่ในการรายงาน และผู้ใช้รายงาน เพื่อให้มั่นใจว่าองค์กรมีการรายงานข้อมูลความเสี่ยงที่ถูกต้องและเหมาะสมต่อผู้ใช้รายงานและทันเวลา

**คู่มือปฏิบัติ**

1. รัฐวิสาหกิจควรจัดให้มีการรายงานด้านการบริหารความเสี่ยงอย่างสม่ำเสมอและต่อเนื่อง โดยกำหนดให้มีคณะทำงานหรือผู้รับผิดชอบในการรายงานผลการบริหารความเสี่ยงให้กับคณะกรรมการคณะกรรมการบริหารความเสี่ยง ผู้บริหารสูงสุด และผู้ที่เกี่ยวข้อง โดยดำเนินการ ดังนี้

- 1) มอบหมายให้ มีผู้รับผิดชอบในการรายงานความเสี่ยง เช่น หน่วยงานบริหารความเสี่ยง เจ้าของความเสี่ยง (Risk Owner)
- 2) หน่วยงานบริหารความเสี่ยงควรคัดกรองและวิเคราะห์ข้อมูลอย่างสม่ำเสมอ ตามความเหมาะสมของระดับความรุนแรงและข้อมูล เช่น อาจมีการรวบรวมและวิเคราะห์คัดกรองเป็นรายเดือนหรือรายไตรมาส เพื่อนำเสนอต่อคณะกรรมการบริหารความเสี่ยงและผู้บริหารสูงสุด
- 3) หน่วยงานบริหารความเสี่ยงรายงานประเด็นด้านการบริหารความเสี่ยงต่อคณะกรรมการบริหารความเสี่ยงและผู้บริหารสูงสุด โดยในการรายงานความเสี่ยงควรครอบคลุมหัวข้อดังต่อไปนี้
  - รายการความเสี่ยง ผลการประเมินความเสี่ยง และแผนการบริหารจัดการความเสี่ยงประจำปี
  - ระดับความรุนแรงของแต่ละปัจจัยเสี่ยงรายไตรมาส เทียบกับเป้าหมายที่คาดหวัง พร้อมวิเคราะห์ปัญหา อุปสรรค และแนวทางที่จะบรรลุเป้าหมายเป็นรายไตรมาส
  - ความคืบหน้าและผลของการดำเนินการตามแผนจัดการความเสี่ยง ปัญหา และอุปสรรค (ถ้ามี) รวมถึงกิจกรรมการควบคุม (Existing Control)
  - ผลการติดตามสภาพแวดล้อมในการดำเนินงานของรัฐวิสาหกิจและการระบุความเสี่ยงเพิ่มเติม (ถ้ามี)
  - ข้อสังเกตและข้อเสนอแนะในการบริหารความเสี่ยง
  - การวิเคราะห์ความเสี่ยงใหม่และสาเหตุที่แท้จริง รวมถึงแนวโน้มการเปลี่ยนแปลงในภาพรวมความเสี่ยง ภาพความเสี่ยง และผลการปฏิบัติงานขององค์กร
  - เกณฑ์และดัชนีชี้วัดผลการปฏิบัติงานที่สำคัญ (KPI)
  - เกณฑ์และดัชนีชี้วัดความเสี่ยงหลัก (KRI)

นอกจากนี้ รัฐวิสาหกิจอาจพิจารณารายงานหัวข้อดังต่อไปนี้เพิ่มเติมตามความเหมาะสม

- รายงานการเปิดเผยข้อมูลเกี่ยวกับเหตุการณ์ไม่พึงประสงค์ การฝ่าฝืน หรือความเสียหาย
  - การวิเคราะห์ความอ่อนไหวของการเปลี่ยนแปลงในสมมติฐานหลักที่อยู่ในกลยุทธ์ และผลกระทบที่อาจเกิดต่อกลยุทธ์และวัตถุประสงค์ในการประกอบกิจการ
  - รายงานเกี่ยวกับวัฒนธรรมการบริหารความเสี่ยงในองค์กร เช่น การวิเคราะห์แนวโน้มทางวัฒนธรรม การหาตัววัดเปรียบเทียบกับองค์กรหรือมาตรฐานอื่น รูปแบบผลตอบแทน และสิ่งที่อาจเกิดขึ้น ซึ่งมีอิทธิพลต่อการตัดสินใจ การวิเคราะห์การถอดบทเรียน การสอบทานแนวโน้มทางพฤติกรรมหรือการสอบทานทัศนคติต่อความเสี่ยงและการตระหนักต่อความเสี่ยง
- ทั้งนี้ การรายงานความเสี่ยงควรถูกเสริมโดยความเห็นและการวิเคราะห์ของผู้เชี่ยวชาญในสาขานั้นๆ เช่น ผู้เชี่ยวชาญด้านการปฏิบัติตามกฎระเบียบข้อบังคับ ด้านข้อกำหนดและด้านเทคโนโลยี จะให้ความเห็นและการวิเคราะห์เกี่ยวกับความรุนแรงของความเสี่ยง ความมีประสิทธิผลของวิธีการตอบสนองต่อความเสี่ยง สิ่งที่ผลักดันให้เกิดการเปลี่ยนแปลงซึ่งพบจากการวิเคราะห์แนวโน้ม รวมทั้งพัฒนาการในอุตสาหกรรม และโอกาสที่เปิดให้กับองค์กร

- 4) คณะกรรมการบริหารความเสี่ยงพิจารณาอนุมัติหรือให้ข้อคิดเห็น/คำแนะนำในการจัดการความเสี่ยงเพิ่มเติม แล้วให้หน่วยงานบริหารความเสี่ยงนำสิ่งที่ได้จากมติที่ประชุมคณะกรรมการบริหารความเสี่ยงไปปฏิบัติ จากนั้นสื่อสารไปยังผู้ที่มีหน้าที่รับผิดชอบในเรื่องต่างๆ ต่อไป เช่น เจ้าของความเสี่ยง (Risk Owner) โดยการจัดการประชุมคณะกรรมการบริหารความเสี่ยง ควรจัดอย่างสม่ำเสมอตามความเหมาะสมของแต่ละองค์กร โดยทั่วไปแล้ว อาจมีการประชุมทุกเดือน หรืออย่างน้อยทุกไตรมาส เพื่อติดตามและประเมินผลการบริหารความเสี่ยงได้อย่างมีประสิทธิภาพ และสามารถแก้ไขหรือควบคุมความเสี่ยงได้อย่างทันท่วงที
- 5) เมื่อคณะกรรมการตรวจสอบได้รับการสื่อสารเกี่ยวกับการบริหารความเสี่ยงในประเด็นที่สำคัญแล้ว จากนั้นให้ดำเนินการให้ความเห็นในเรื่องความเพียงพอของการบริหารความเสี่ยง โดยอาจพิจารณาประเมินความเพียงพอ อย่างน้อยปีละ 1 ครั้ง เพื่อให้มั่นใจว่ากระบวนการบริหารความเสี่ยงมีประสิทธิภาพหรือเพื่อให้สามารถแก้ไขได้ทันเวลา
- 6) คณะกรรมการได้รับการรายงานจากคณะกรรมการบริหารความเสี่ยงและผู้บริหารผ่านการประชุม โดยสิ่งสำคัญ คือ เนื้อหาการรายงานควรมุ่งเน้นที่การเชื่อมโยงระหว่างกลยุทธ์และวัตถุประสงค์ ในการประกอบกิจการ ความเสี่ยง และผลการดำเนินงาน โดยการรายงานในระดับคณะกรรมการ นั้นถือเป็นระดับสูงสุด จึงควรสะท้อนภาพรวมของความเสี่ยงที่องค์กรเผชิญอย่างชัดเจน



# 4

## หลักเกณฑ์ แนวปฏิบัติ และคู่มือปฏิบัติ เกี่ยวกับการควบคุมภายใน สำหรับรัฐวิสาหกิจ

	หน้า
คำจำกัดความ	122
หลักการพื้นฐานการควบคุมภายใน	122
การปฏิบัติตามหลักเกณฑ์	124
ลำดับขั้นของการปฏิบัติ	124
นิยามของคำสำคัญ	125
ภาพรวมหลักเกณฑ์ แนวปฏิบัติ และคู่มือปฏิบัติ	126
หลักเกณฑ์ แนวปฏิบัติ และคู่มือปฏิบัติ	129
• องค์ประกอบที่ 1 สภาพแวดล้อมการควบคุม (Control Environment)	129
• องค์ประกอบที่ 2 การประเมินความเสี่ยง (Risk Assessment)	142
• องค์ประกอบที่ 3 กิจกรรมการควบคุม (Control Activities)	149
• องค์ประกอบที่ 4 สารสนเทศและการสื่อสาร (Information and Communication)	156
• องค์ประกอบที่ 5 กิจกรรมติดตามผล (Monitoring)	161

# หลักเกณฑ์ แนวปฏิบัติ และคู่มือปฏิบัติเกี่ยวกับ การควบคุมภายในสำหรับรัฐวิสาหกิจ

## 1. คำจำกัดความ

การควบคุมภายใน คือ กระบวนการปฏิบัติงานที่ผู้กำกับดูแล ผู้บริหารสูงสุด ฝ่ายบริหาร และบุคลากรของรัฐวิสาหกิจจัดให้มีขึ้น เพื่อสร้างความมั่นใจอย่างสมเหตุสมผลว่าการดำเนินงานของรัฐวิสาหกิจจะบรรลุวัตถุประสงค์ด้านการดำเนินงาน ด้านการรายงาน และด้านการปฏิบัติตามกฎหมาย ระเบียบ และข้อบังคับ

## 2. หลักการพื้นฐานการควบคุมภายใน

รัฐวิสาหกิจควรพัฒนากระบวนการควบคุมภายใน โดยอ้างอิงมาตรฐานการควบคุมภายในสำหรับหน่วยงานของรัฐ ตามหลักเกณฑ์กระทรวงการคลังว่าด้วยมาตรฐานและหลักเกณฑ์ปฏิบัติการควบคุมภายในสำหรับหน่วยงานของรัฐ พ.ศ. 2561 ดังนี้

หลักการพื้นฐาน	คำอธิบาย
1. สภาพแวดล้อมการควบคุม	<ul style="list-style-type: none"><li>รัฐวิสาหกิจแสดงให้เห็นถึงการยึดมั่นในคุณค่าของความซื่อตรงและจริยธรรม</li><li>ผู้กำกับดูแลของรัฐวิสาหกิจ แสดงให้เห็นถึงความเป็นอิสระจากฝ่ายบริหารและมีหน้าที่กำกับดูแลให้มีการพัฒนาหรือปรับปรุงการควบคุมภายใน รวมถึงการดำเนินการเกี่ยวกับการควบคุมภายใน</li><li>ผู้บริหารสูงสุดจัดให้มีโครงสร้างองค์กร (Organization Chart) สายการบังคับบัญชา อำนาจหน้าที่ และความรับผิดชอบที่เหมาะสมในการบรรลุวัตถุประสงค์ขององค์กรภายใต้การกำกับดูแลของผู้กำกับดูแล</li><li>รัฐวิสาหกิจแสดงให้เห็นถึงความมุ่งมั่นในการสร้างแรงจูงใจ พัฒนาและรักษาบุคลากรที่มีความรู้ความสามารถที่สอดคล้องกับวัตถุประสงค์ขององค์กร</li><li>รัฐวิสาหกิจกำหนดให้บุคลากรมีหน้าที่และความรับผิดชอบต่อผลการปฏิบัติงานตามระบบการควบคุมภายใน เพื่อให้บรรลุวัตถุประสงค์ขององค์กร</li></ul>

หลักการพื้นฐาน	คำอธิบาย
2. การประเมินความเสี่ยง	<ul style="list-style-type: none"> <li>• รัฐวิสาหกิจจะระบุวัตถุประสงค์การควบคุมภายในของการปฏิบัติงานให้สอดคล้องกับวัตถุประสงค์ขององค์กรไว้อย่างชัดเจน และเพียงพอที่จะสามารถระบุและประเมินความเสี่ยงที่เกี่ยวข้องกับวัตถุประสงค์</li> <li>• รัฐวิสาหกิจจะระบุความเสี่ยงที่มีผลต่อการบรรลุวัตถุประสงค์ การควบคุมภายในอย่างครอบคลุมทั้งรัฐวิสาหกิจ และวิเคราะห์ความเสี่ยงเพื่อกำหนดวิธีการจัดการความเสี่ยงนั้น</li> <li>• รัฐวิสาหกิจพิจารณาโอกาสที่อาจเกิดททุจริต เพื่อประกอบการประเมินความเสี่ยงที่มีผลต่อการบรรลุวัตถุประสงค์</li> <li>• รัฐวิสาหกิจจะระบุและประเมินการเปลี่ยนแปลงที่อาจมีผลกระทบต่ออย่างมีนัยสำคัญต่อระบบการควบคุมภายใน</li> </ul>
3. กิจกรรมการควบคุม	<ul style="list-style-type: none"> <li>• รัฐวิสาหกิจจะระบุและพัฒนากิจกรรมการควบคุมเพื่อลดความเสี่ยงในการบรรลุวัตถุประสงค์ให้อยู่ในระดับที่องค์กรยอมรับได้ (RA)</li> <li>• รัฐวิสาหกิจจะระบุและพัฒนากิจกรรมการควบคุมทั่วไปด้านเทคโนโลยีเพื่อสนับสนุนการบรรลุวัตถุประสงค์</li> <li>• รัฐวิสาหกิจจัดให้มีกิจกรรมการควบคุม โดยกำหนดไว้ในนโยบาย ประกอบด้วยผลสำเร็จที่คาดหวังและขั้นตอนการปฏิบัติงาน เพื่อนำนโยบายไปสู่การปฏิบัติจริง</li> </ul>
4. สารสนเทศและการสื่อสาร	<ul style="list-style-type: none"> <li>• รัฐวิสาหกิจจัดทำหรือจัดหาและใช้สารสนเทศที่เกี่ยวข้องและมีคุณภาพ เพื่อสนับสนุนให้มีการปฏิบัติตามการควบคุมภายในที่กำหนด</li> <li>• รัฐวิสาหกิจมีการสื่อสารภายในเกี่ยวกับสารสนเทศ รวมถึงวัตถุประสงค์และความรับผิดชอบที่มีต่อการควบคุมภายในซึ่งมีความจำเป็นในการสนับสนุนให้มีการปฏิบัติตามการควบคุมภายในที่กำหนด</li> <li>• รัฐวิสาหกิจมีการสื่อสารกับบุคคลภายนอกเกี่ยวกับเรื่องที่มีผลกระทบต่อปฏิบัติตามการควบคุมภายในที่กำหนด</li> </ul>
5. กิจกรรมการติดตามผล	<ul style="list-style-type: none"> <li>• รัฐวิสาหกิจจะระบุ พัฒนา และดำเนินการประเมินผลระหว่าง การปฏิบัติงาน และหรือการประเมินผลเป็นรายครั้งตามที่กำหนด</li> </ul>

หลักการพื้นฐาน	คำอธิบาย
	<p>เพื่อให้เกิดความมั่นใจว่าได้มีการปฏิบัติตามองค์ประกอบของการควบคุมภายใน</p> <ul style="list-style-type: none"> <li>• รัฐวิสาหกิจประเมินผลและสื่อสารข้อบกพร่องหรือจุดอ่อนของการควบคุมภายในอย่างทันเวลาต่อฝ่ายบริหารและผู้กำกับดูแล เพื่อให้ผู้รับผิดชอบสามารถสั่งการแก้ไขได้อย่างเหมาะสม</li> </ul>

### 3. การปฏิบัติตามหลักเกณฑ์

- 3.1 หลักเกณฑ์ แนวปฏิบัติ และคู่มือปฏิบัติเกี่ยวกับการควบคุมภายใน จะไม่มีประโยชน์อันใด หากไม่มีการนำไปปฏิบัติ
- 3.2 หลักเกณฑ์ แนวปฏิบัติ และคู่มือปฏิบัติเกี่ยวกับการควบคุมภายใน จัดทำขึ้นสำหรับใช้เป็นแนวปฏิบัติของรัฐวิสาหกิจ โดยหวังว่าจะทำให้เกิดความคิดเบื้องต้น ซึ่งผู้เกี่ยวข้องสามารถนำไปปรับปรุงแก้ไขในการปฏิบัติให้มีความเหมาะสมกับการดำเนินงาน
- 3.3 ผู้มีส่วนได้เสียของรัฐวิสาหกิจต้องการความมั่นใจจากรัฐวิสาหกิจ ด้วยการมีระบบการควบคุมภายในที่ดี ทั้งนี้ คณะกรรมการและผู้บริหารต้องร่วมกันกำหนดนโยบายและกระบวนการควบคุมภายในขององค์กรตามบริบทของแต่ละองค์กร
- 3.4 ให้รัฐวิสาหกิจดำเนินการตามส่วนที่เป็นหลักเกณฑ์ โดยแนวปฏิบัติและคู่มือปฏิบัติเป็นส่วนที่ให้รายละเอียดหรือวิธีการดำเนินการเพิ่มเติม เพื่อให้รัฐวิสาหกิจสามารถปฏิบัติตามหลักเกณฑ์ได้ สำหรับรัฐวิสาหกิจที่เป็นบริษัทจดทะเบียนในตลาดหลักทรัพย์แห่งประเทศไทยให้ถือปฏิบัติตามแนวปฏิบัติของตลาดหลักทรัพย์แห่งประเทศไทยควบคู่ไปด้วย

### 4. ลำดับขั้นของการปฏิบัติ

- 4.1 ให้รัฐวิสาหกิจจัดให้มีระบบการควบคุมภายในตามหลักเกณฑ์ แนวปฏิบัติ และคู่มือปฏิบัติ และให้รัฐวิสาหกิจมีถ้อยแถลง (Statement) ไว้ในรายงานประจำปีของรัฐวิสาหกิจ ซึ่งอธิบายถึงนโยบายและกระบวนการที่คณะกรรมการได้เลือกใช้ปฏิบัติ โดยข้อมูลนี้จะใช้เป็นส่วนหนึ่งของการประเมินการควบคุมภายในของรัฐวิสาหกิจ
- 4.2 หลักเกณฑ์ แนวปฏิบัติ และคู่มือปฏิบัติจะช่วยให้รัฐวิสาหกิจสามารถยกระดับการควบคุมภายในให้ทัดเทียมกับสากลได้ รัฐวิสาหกิจควรนำหลักเกณฑ์ แนวปฏิบัติ และคู่มือปฏิบัติไปปฏิบัติให้ได้มากที่สุด โดยอาจปรับใช้ให้เหมาะสมกับบริบทของแต่ละองค์กร ทั้งนี้ สคร. อาจกำหนดให้มีการประเมินระบบการควบคุมภายในของรัฐวิสาหกิจควบคู่ไปด้วย รวมถึงการรายงานผลการควบคุมภายใน

## 5. นิยามของคำสำคัญ

คำสำคัญ	ความหมาย
วัตถุประสงค์ด้านการดำเนินงาน (Operations Objectives)	วัตถุประสงค์เกี่ยวกับความมีประสิทธิภาพและประสิทธิผลของการดำเนินงาน รวมถึงการบรรลุเป้าหมายด้านการดำเนินงาน ด้านการเงิน ตลอดจน การใช้ทรัพยากร การดูแลรักษาทรัพย์สิน การป้องกันหรือลดความผิดพลาดของรัฐบาลศึกษา ตลอดจนความเสียหาย การรั่วไหล การสิ้นเปลือง หรือการทุจริตในรัฐบาลศึกษา
วัตถุประสงค์ด้านการรายงานทางการเงิน (Reporting Objectives)	วัตถุประสงค์เกี่ยวกับการรายงานทางการเงินและไม่ใช่ทางการเงิน ที่ใช้ภายในและภายนอกรัฐบาลศึกษา รวมถึงการรายงานที่เชื่อถือได้ทันเวลา โปร่งใส หรือข้อกำหนดอื่นของทางราชการ
วัตถุประสงค์ด้านการปฏิบัติตามกฎหมาย ระเบียบ และข้อบังคับ (Compliance Objectives)	วัตถุประสงค์เกี่ยวกับการปฏิบัติตามกฎหมาย ระเบียบ ข้อบังคับ หรือมติคณะรัฐมนตรีที่เกี่ยวข้องกับการดำเนินงาน รวมทั้งข้อกำหนดอื่นของทางราชการ
ความซื่อตรง (Integrity)	คุณภาพหรือสภาพของการดำรงชีวิตด้วยหลักความซื่อสัตย์ ได้แก่ ความซื่อตรง ความซื่อสัตย์ และความจริงใจ รวมทั้งความปรารถนาที่จะกระทำการที่ถูกต้อง เช่น ประกอบอาชีพและดำรงชีพ ให้อยู่ในกรอบของคุณค่าและความคาดหวังต่างๆ
นโยบาย (Policy)	คำแถลงของผู้บริหารหรือคณะกรรมการถึงสิ่งสมควรกระทำเพื่อเป็นพื้นฐานการปฏิบัติงานและทำให้การควบคุมเป็นผล โดยคำแถลงเหล่านี้อาจจัดทำเป็นลายลักษณ์อักษร เพื่อให้สามารถกล่าวอ้างถึงอย่างชัดเจนในระหว่างการสื่อสาร หรืออาจแสดงเป็นนัยผ่านการกระทำและการตัดสินใจต่างๆ
ผู้มีส่วนได้เสีย (Stakeholders)	กลุ่มคนที่ได้รับผลกระทบจากองค์กร เช่น ผู้กำกับดูแล ผู้ถือหุ้น ชุมชนที่ซึ่งองค์กรดำเนินงานอยู่ พนักงาน ลูกค้า และผู้ขาย

## 6. ภาพรวมหลักเกณฑ์ แนวปฏิบัติ และคู่มือปฏิบัติ

หลักเกณฑ์ แนวปฏิบัติ และคู่มือปฏิบัติเกี่ยวกับการควบคุมภายใน ประกอบด้วย 5 องค์ประกอบ ดังนี้

องค์ประกอบที่ 1 สภาพแวดล้อมการควบคุม (Control Environment)		
<b>หลักเกณฑ์</b>		
รัฐวิสาหกิจควรกำหนดให้มีสภาพแวดล้อมการควบคุมภายใน ประกอบด้วย มาตรฐาน กระบวนการ และโครงสร้างขององค์กร เพื่อใช้เป็นแนวทางให้บุคลากรทุกระดับสามารถปฏิบัติและตัดสินใจในสิ่งที่ตนรับผิดชอบเกี่ยวกับการควบคุมภายใน		
แนวปฏิบัติ		จำนวนคู่มือปฏิบัติ
แนวปฏิบัติที่ 1	การกำหนดจรรยาบรรณในการประกอบกิจการ	2
แนวปฏิบัติที่ 2	การกำกับดูแลและสนับสนุนให้มีการควบคุมภายใน โดยคณะกรรมการ	2
แนวปฏิบัติที่ 3	การกำหนดโครงสร้างองค์กรและสายการบังคับบัญชา	3
แนวปฏิบัติที่ 4	การออกแบบนโยบายและแนวปฏิบัติด้านทรัพยากรบุคคล ซึ่งครอบคลุมการจูงใจ พัฒนา รักษาไว้	1
แนวปฏิบัติที่ 5	การกำหนดอำนาจหน้าที่และความรับผิดชอบต่อผลการปฏิบัติงาน	2
รวม		10

## องค์ประกอบที่ 2 การประเมินความเสี่ยง (Risk Assessment)

### หลักเกณฑ์

รัฐวิสาหกิจควรประเมินความเสี่ยงเพื่อให้ทราบว่าองค์กรมีความเสี่ยงอย่างไร มีระดับความเสี่ยงและโอกาสที่จะเกิดมากน้อยเพียงใด เนื่องจากองค์กรต้องเผชิญกับความเสี่ยงที่เกิดจากปัจจัยภายในและปัจจัยภายนอกที่หลีกเลี่ยงไม่ได้ ซึ่งส่งผลกระทบต่อผลสำเร็จตามวัตถุประสงค์ขององค์กร ดังนั้น ผู้บริหารต้องพิจารณาว่าองค์กรควรมีมาตรการหรือบริหารจัดการอย่างไร เพื่อจัดการกับความเสี่ยงดังกล่าวให้อยู่ในระดับความเสี่ยงที่องค์กรยอมรับได้ (RA)

แนวปฏิบัติ		จำนวนคู่มือปฏิบัติ
แนวปฏิบัติที่ 1	การกำหนดวัตถุประสงค์ระดับองค์กรและหน่วยงานที่เกี่ยวข้องกับการควบคุมภายใน	2
แนวปฏิบัติที่ 2	การระบุเหตุการณ์ความเสี่ยงที่อาจมีผลกระทบต่อการทำงาน	5
แนวปฏิบัติที่ 3	การประเมินความเป็นไปได้ที่จะเกิดความเสี่ยงด้านการทุจริต	2
แนวปฏิบัติที่ 4	การระบุและประเมินการเปลี่ยนแปลงของสภาพแวดล้อมที่อาจมีผลกระทบต่ออย่างมีนัยสำคัญต่อระบบการควบคุมภายใน	1
รวม		10

## องค์ประกอบที่ 3 กิจกรรมการควบคุม (Control Activities)

### หลักเกณฑ์

รัฐวิสาหกิจควรจัดให้มีกิจกรรมการควบคุม โดยการกำหนดให้มีมาตรการหรือขั้นตอนในการปฏิบัติงานตามนโยบาย เพื่อให้สามารถจัดการความเสี่ยงได้อย่างมีประสิทธิภาพและประสิทธิผล

แนวปฏิบัติ		จำนวนคู่มือปฏิบัติ
แนวปฏิบัติที่ 1	การเลือกและพัฒนากิจกรรมการควบคุม	3
แนวปฏิบัติที่ 2	การนำเทคโนโลยีสารสนเทศมาใช้ เพื่อสนับสนุนให้บรรลุวัตถุประสงค์ของการควบคุมภายใน	1
แนวปฏิบัติที่ 3	การกำหนดและสื่อสารนโยบายที่เกี่ยวข้องกับการควบคุมภายใน	3
รวม		7

#### องค์ประกอบที่ 4 สารสนเทศและการสื่อสาร (Information and Communication)

##### หลักเกณฑ์

รัฐวิสาหกิจต้องจัดให้มีสารสนเทศอย่างเพียงพอ เหมาะสม เชื่อถือได้ ซึ่งประกอบด้วยข้อมูลสารสนเทศที่เกี่ยวกับการดำเนินงานทั้งที่เป็นข้อมูลสารสนเทศจากแหล่งภายในและแหล่งภายนอก เพื่อสนับสนุนประสิทธิภาพและประสิทธิผลในการกำหนดกลยุทธ์ ประเมินความเสี่ยง และกิจกรรมการควบคุม

แนวปฏิบัติ		จำนวนคู่มือปฏิบัติ
แนวปฏิบัติที่ 1	การดำเนินงานด้านข้อมูลสารสนเทศและระบบจัดการฐานข้อมูล	3
แนวปฏิบัติที่ 2	การจัดให้มีการสื่อสารภายในองค์กร	2
แนวปฏิบัติที่ 3	การจัดให้มีการสื่อสารกับหน่วยงานภายนอก และมีช่องทางเพื่อเปิดรับข้อมูลจากผู้มีส่วนได้เสียภายนอก	1
รวม		6

#### องค์ประกอบที่ 5 กิจกรรมติดตามผล (Monitoring)

##### หลักเกณฑ์

รัฐวิสาหกิจควรกำหนดให้มีการติดตามและประเมินผลการควบคุมภายใน โดยมีขึ้นในระหว่างการปฏิบัติงาน และการประเมินผลเป็นรายครั้งอย่างต่อเนื่องและสม่ำเสมอ เพื่อให้คณะกรรมการและผู้บริหารระดับสูงมีความมั่นใจได้อย่างสมเหตุสมผลต่อประสิทธิภาพและประสิทธิผลของการควบคุมภายใน

แนวปฏิบัติ		จำนวนคู่มือปฏิบัติ
แนวปฏิบัติที่ 1	การกำหนดให้มีการพัฒนาและประเมินผลการควบคุมภายในอย่างต่อเนื่องและสม่ำเสมอ	1
แนวปฏิบัติที่ 2	การสื่อสารข้อบกพร่องที่ได้จากการประเมินการควบคุมภายใน	1
รวม		2

## 7. หลักเกณฑ์ แนวปฏิบัติ และคู่มือปฏิบัติ

### องค์ประกอบที่ 1 สภาพแวดล้อมการควบคุม (Control Environment)

#### หลักเกณฑ์

รัฐวิสาหกิจควรกำหนดให้มีสภาพแวดล้อมการควบคุมภายใน ประกอบด้วย มาตรฐาน กระบวนการ และโครงสร้างขององค์กร เพื่อใช้เป็นแนวทางให้บุคลากรทุกระดับสามารถปฏิบัติและตัดสินใจในสิ่งที่ตนรับผิดชอบเกี่ยวกับการควบคุมภายใน

#### แนวปฏิบัติที่ 1

รัฐวิสาหกิจควรสร้างมาตรฐานทางพฤติกรรม กรอบทางกฎหมาย และขนบธรรมเนียม เพื่อนำเป็นแนวทางในการดำเนินงานในองค์กร โดยกำหนดจรรยาบรรณในการประกอบกิจการ (Code of Conduct) ซึ่งเป็นกฎเกณฑ์มาตรฐานของพฤติกรรมและความประพฤติ พร้อมทั้งกำหนดบทลงโทษเป็นลายลักษณ์อักษร และส่งเสริมและสนับสนุนวัฒนธรรมองค์กรที่มุ่งเน้นความสำคัญของความซื่อตรงและจริยธรรม จัดให้มีการฝึกอบรมให้พนักงานทราบและเข้าใจลักษณะของพฤติกรรมที่พึงปฏิบัติ

#### คู่มือปฏิบัติ

1. รัฐวิสาหกิจควรจัดทำจรรยาบรรณในการประกอบกิจการ (Code of Conduct) จากนั้นสื่อสารไปยังผู้บริหารและพนักงานทุกระดับอย่างทั่วถึง รวมทั้งกำหนดให้มีการทบทวนอย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงอย่างมีนัยสำคัญ โดยสามารถอ้างอิงรายละเอียดจรรยาบรรณในการประกอบกิจการ (Code of Conduct) เพิ่มเติมในบทที่ 3 หลักเกณฑ์ แนวปฏิบัติ และคู่มือปฏิบัติ เกี่ยวกับการบริหารความเสี่ยงสำหรับรัฐวิสาหกิจ องค์ประกอบที่ 1 แนวปฏิบัติที่ 3
2. รัฐวิสาหกิจควรกำหนดให้มีการติดตามและประเมินผลการปฏิบัติตามจรรยาบรรณในการประกอบกิจการ (Code of Conduct) อย่างต่อเนื่อง ซึ่งสามารถปฏิบัติได้หลายวิธี เช่น การทำแบบทดสอบการตรวจสอบโดยหน่วยงานตรวจสอบภายใน การกำหนดดัชนีชี้วัดผลการดำเนินงาน (KPI) พร้อมทั้งกำหนดบทลงโทษอย่างเป็นลายลักษณ์อักษรสำหรับกรณีที่มีการไม่ปฏิบัติตามระเบียบ ข้อบังคับ หรือจรรยาบรรณในการประกอบกิจการ (Code of Conduct) นอกจากนี้ ควรจัดให้มีช่องทางสำหรับการแจ้งเบาะแสหรือร้องเรียนเกี่ยวกับการกระทำที่ผิดกฎหมาย หรือการไม่ปฏิบัติตามจรรยาบรรณในการประกอบกิจการ (Code of Conduct) โดยจัดทำนโยบายการรายงานเบาะแส หรือนโยบายการร้องเรียน (Whistle Blowing Policy) อย่างเป็นระบบ ซึ่งครอบคลุมแนวปฏิบัติเมื่อได้รับแจ้งเหตุและมาตรการคุ้มครองผู้แจ้งเบาะแสหรือผู้ร้องเรียนอย่างชัดเจน โดยสามารถอ้างอิง

รายละเอียดนโยบายการรายงานเบาะแส หรือนโยบายการร้องเรียน (Whistle Blowing Policy) เพิ่มเติมในบทที่ 3 หลักเกณฑ์ แนวปฏิบัติ และคู่มือปฏิบัติเกี่ยวกับการบริหารความเสี่ยงสำหรับ รัฐวิสาหกิจ องค์ประกอบที่ 5 แนวปฏิบัติที่ 2

## แนวปฏิบัติที่ 2

คณะกรรมการควรมีบทบาทหน้าที่ในการกำกับดูแลและสนับสนุนให้มีการควบคุมภายในที่เพียงพอ และเหมาะสมต่อการดำเนินกิจการ

### คู่มือปฏิบัติ

1. รัฐวิสาหกิจควรกำหนดบทบาทหน้าที่ของคณะกรรมการแยกจากฝ่ายบริหาร โดยเชื้อต่อการใช้ดุลพินิจในการตัดสินใจอย่างมีอิสระ และได้สงวนสิทธิ์อำนาจเฉพาะของคณะกรรมการไว้อย่างชัดเจน ผ่านการจัดทำกฎบัตรและสื่อสารให้คณะกรรมการ และคณะกรรมการชุดย่อยรับทราบถึงกฎบัตรคณะกรรมการและคณะกรรมการชุดย่อย ซึ่งอาจประกอบด้วยคณะกรรมการบริหาร คณะกรรมการตรวจสอบ คณะกรรมการบริหารความเสี่ยง
2. คณะกรรมการควรมีบทบาทหน้าที่ด้านการควบคุมภายใน ดังต่อไปนี้
  - กำกับดูแลให้มีระบบการควบคุมภายในที่เพียงพอและเหมาะสมต่อการดำเนินกิจการ
  - กำกับดูแลให้มีการแต่งตั้งคณะกรรมการควบคุมภายใน เพื่อรับผิดชอบในการปฏิบัติหน้าที่
  - ส่งเสริมให้ผู้บริหารมีทัศนคติ และรูปแบบการทำงานที่สนับสนุนให้องค์กรมีการควบคุมภายในที่ดี มีประสิทธิภาพ และสามารถปฏิบัติงานได้อย่างมีประสิทธิภาพ เนื่องจากผู้บริหารมีส่วนสำคัญอย่างยิ่งในการสร้างสภาพแวดล้อมการควบคุมที่ดีขององค์กร ทัศนคติต่อประสิทธิภาพของการควบคุมภายในจะรับรู้ได้ทั่วทั้งองค์กร ซึ่งหากผู้บริหารให้ความสนใจในการจัดสภาพแวดล้อมการควบคุมภายในให้ดีย่อมทำให้องค์กรนั้นๆ มีสภาพแวดล้อมการควบคุมที่มีเสถียรภาพ เป็นรากฐานให้องค์ประกอบการควบคุมภายในอื่นๆ มีประสิทธิภาพ ก่อให้เกิดวัฒนธรรมองค์กรที่ดีในระยะยาว เช่น จัดให้มีการประชุม หรือสัมมนา เพื่อชี้แจงถึงผลดีที่จะเกิดขึ้นจากการมีการควบคุมภายในที่ดีและการปฏิบัติตามการควบคุมภายในที่กำหนดไว้และผลเสียหากไม่ปฏิบัติ

## แนวปฏิบัติที่ 3

รัฐวิสาหกิจควรกำหนดโครงสร้างองค์กร (Organization Chart) และสายการบังคับบัญชา ความสัมพันธ์ระหว่างหน่วยงาน หน้าที่และความรับผิดชอบที่สำคัญให้ชัดเจน

### คู่มือปฏิบัติ

1. โครงสร้างองค์กร (Organization Chart) ที่ได้รับการจัดไว้เป็นอย่างดีและเป็นพื้นฐานสำคัญที่จะทำให้ผู้บริหารสามารถวางแผน สั่งการ และควบคุมการปฏิบัติงานได้อย่างถูกต้อง รวดเร็ว และมีประสิทธิภาพ รวมทั้งจะเป็นสิ่งที่บ่งบอกให้เห็นถึงกรอบการทำงานของแต่ละกิจกรรมที่ทำให้การดำเนินงานบรรลุตามวัตถุประสงค์ที่ตั้งไว้ ดังนั้น รัฐวิสาหกิจจึงควรกำหนดโครงสร้างองค์กร (Organization Chart) โดยให้มีการแบ่งแยกหน้าที่ความรับผิดชอบงานทั้ง 3 ด้าน ออกจากกัน ดังนี้

- การอนุมัติหรือให้ความเห็นชอบ
- การบันทึกข้อมูล
- การดูแลรักษาทรัพย์สินขององค์กร

เพื่อการปฏิบัติงานที่มีความโปร่งใสตามหลักการถ่วงดุลอำนาจและแบ่งหน้าที่อย่างชัดเจน โดยจะต้องไม่ให้หน่วยงานเดียว หรือคนเพียงคนเดียวทำหลายหน้าที่ เพราะจะทำให้ขาดระบบการสอบย้อนความถูกต้องระหว่างกัน และถือเป็นจุดอ่อนอย่างหนึ่งของระบบการควบคุมภายใน

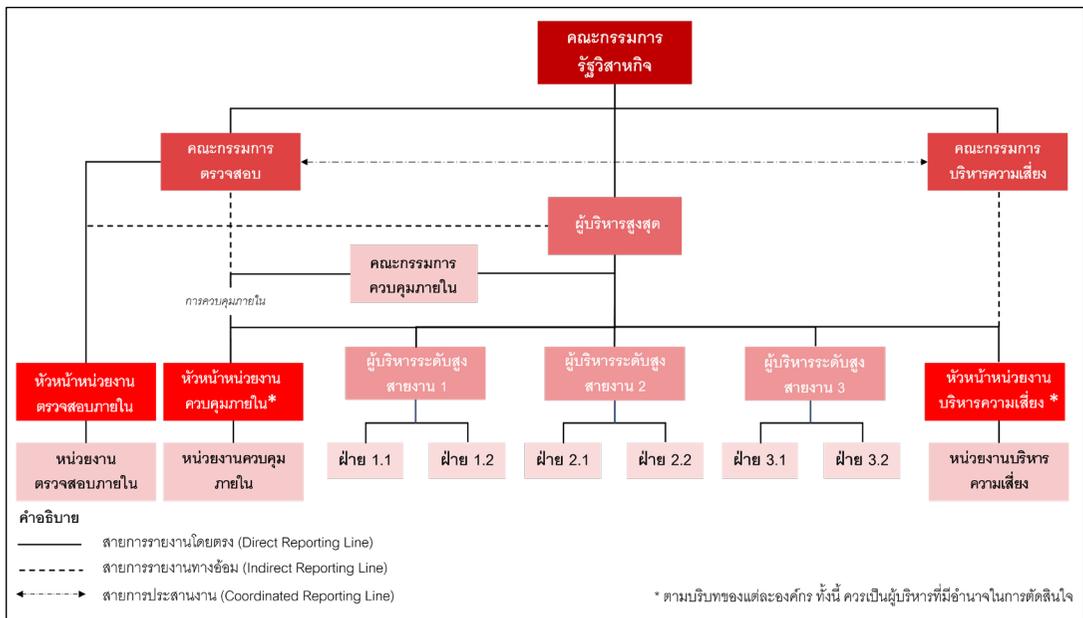
ตัวอย่างของการกำหนดโครงสร้างองค์กร (Organization Chart) ตามหลักการข้างต้น ได้แก่ การกำหนดโครงสร้างองค์กรให้ผู้บริหารในระดับสูงกว่าหน่วยปฏิบัติเป็นผู้มีอำนาจตัดสินใจจัดซื้อหรืออนุมัติการจ่ายเงิน แล้วจัดให้ฝ่ายบัญชีรับผิดชอบในส่วนที่เป็นงานจัดบันทึกรายการทางบัญชีทั้งหมด ซึ่งรวมถึงการรวบรวมตัวเลขสถิติต่างๆ และการคิดคำนวณราคาต้นทุนผลิตภัณฑ์และบริการ ส่วนฝ่ายการเงินจะถูกจัดให้รับผิดชอบในการติดต่อธนาคาร ดูแลรักษาบัญชีเงินฝากที่เก็บไว้กับธนาคาร ดูแลรักษาทรัพย์สิน สภาพคล่องอื่นๆ รับผิดชอบในการรับและจ่ายเงินสดและเงินฝากธนาคาร รวมถึงการนำเงินส่วนที่เหลือเก็บไปลงทุนให้เกิดประโยชน์นอกวง เป็นต้น

การกำหนดโครงสร้างองค์กรที่ดีควรชัดเจน การมีสายบังคับบัญชา และความสัมพันธ์ระหว่างหน่วยงานภายในองค์กรที่เหมาะสม ชัดเจน และสอดคล้องกับขนาดและการดำเนินงานขององค์กร

นอกจากนี้ เพื่อให้เกิดความชัดเจนในการแบ่งแยกหน้าที่และความรับผิดชอบภายในองค์กร คณะกรรมการอาจพิจารณาหลักการ “หน่วยงานแนวป้องกันสามด้าน” (Three Lines of Defense) มาใช้เป็นแนวทางในการกำหนดบทบาทหน้าที่ของแต่ละระดับงานให้เหมาะสมและเป็นระบบ ดังนี้

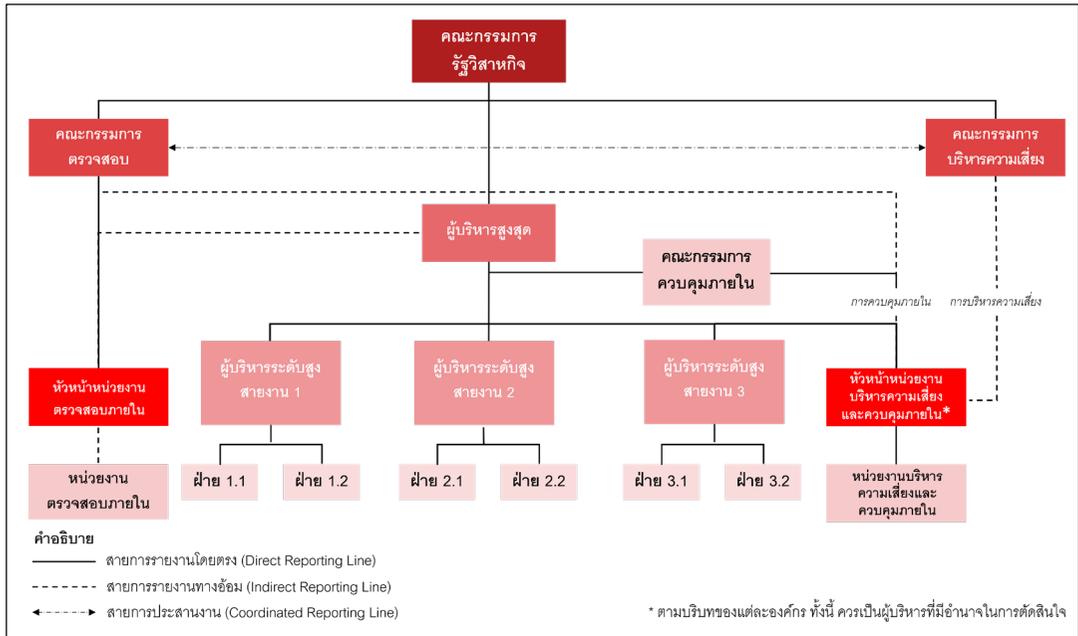
- หน่วยงานแนวป้องกันด่านที่ 1 (First Line of Defense) คือ ผู้บริหารและบุคลากรที่อยู่หน้างาน เป็นด่านป้องกันด่านแรกในกิจกรรมประจำวันเป็นผู้รับผิดชอบในการบริหารความเสี่ยงและดูแลรักษาประสิทธิภาพของการควบคุมภายในประจำวัน
- หน่วยงานแนวป้องกันด่านที่ 2 (Second Line of Defense) คือ หน่วยงานที่มีหน้าที่ให้คำแนะนำและแนวทางเกี่ยวกับการบริหารความเสี่ยง การควบคุมภายใน และการปฏิบัติตามมาตรฐานที่องค์กรกำหนดไว้
- หน่วยงานแนวป้องกันด่านที่ 3 (Third Line of Defense) คือ ผู้ตรวจสอบภายในทำหน้าที่ตรวจสอบและประเมินประสิทธิภาพของการบริหารความเสี่ยงและการควบคุมภายใน รวมทั้งให้คำแนะนำแก่ผู้บริหารในการปรับปรุงกระบวนการบริหารความเสี่ยงและการควบคุมภายใน

ตัวอย่างโครงสร้างการควบคุมภายในสำหรับรัฐวิสาหกิจ  
แบบที่ 1 : โครงสร้างสำหรับองค์กรที่มีหน่วยงานดูแลด้านการควบคุมภายในโดยเฉพาะ



โครงสร้างและสายการรายงานแบบที่ 1 แสดงให้เห็นถึงโครงสร้างการควบคุมภายในที่มีการแยกระหว่างหน่วยงานบริหารความเสี่ยงและหน่วยงานควบคุมภายในออกจากกัน โดยหัวหน้าหน่วยงานควบคุมภายในจะรายงานเกี่ยวกับการควบคุมภายในต่อคณะกรรมการควบคุมภายในเพื่อพิจารณาก่อนรายงานต่อผู้บริหารสูงสุด

## แบบที่ 2 : โครงสร้างสำหรับองค์กรที่รวมหน่วยงานดูแลด้านการบริหารความเสี่ยง และการควบคุมภายในไว้ด้วยกัน



โครงสร้างและสายการรายงานแบบที่ 2 แสดงให้เห็นถึงโครงสร้างการควบคุมภายในที่มีการรวมหน่วยงานบริหารความเสี่ยงและหน่วยงานควบคุมภายในไว้ด้วยกัน โดยหัวหน้าหน่วยงานบริหารความเสี่ยงและควบคุมภายในจะรายงานเกี่ยวกับการควบคุมภายในต่อคณะกรรมการควบคุมภายในเพื่อพิจารณา ก่อนรายงานต่อผู้บริหารสูงสุด

รัฐวิสาหกิจอาจพิจารณากำหนดโครงสร้างองค์กร (Organization Chart) ได้ตามความเหมาะสมกับบริบทขององค์กร ตลอดจนความเพียงพอและความเหมาะสมของทรัพยากรบุคคลขององค์กร โดยมีการกำหนดสายการรายงานอย่างเป็นลายลักษณ์อักษร และมีการรายงานตามสายบังคับบัญชาตามโครงสร้างองค์กร จากนั้นสื่อสารโครงสร้างองค์กร (Organization Chart) และกำหนดให้มีการทบทวนความเหมาะสมของโครงสร้างองค์กร (Organization Chart) อย่างน้อยปีละ 1 ครั้ง และเมื่อมีการเปลี่ยนแปลงอย่างมีนัยสำคัญ เพื่อให้สอดคล้องกับการดำเนินกิจการ

ตัวอย่างบทบาทและความรับผิดชอบในการควบคุมภายในขององค์กร

### 1) ผู้บริหารสูงสุด

- แต่งตั้งคณะกรรมการควบคุมภายในเพื่อปฏิบัติงานด้านการควบคุมภายใน
- ส่งเสริมและแนะแนวทางในการนำระบบการควบคุมภายในมาใช้ภายในองค์กรอย่างมีประสิทธิภาพ
- สอบทานและให้ความเห็นรายงานการประเมินผลการควบคุมภายในระดับองค์กร

## 2) คณะกรรมการควบคุมภายใน

- อำนวยการในการประเมินผลการควบคุมภายใน
- กำหนดแนวทางการประเมินผลการควบคุมภายในในภาพรวมขององค์กร
- รวบรวม พิจารณากลับกรอง และสรุปผลการประเมินการควบคุมภายในในภาพรวมขององค์กร
- ประสานงานการประเมินผลการควบคุมภายในกับหน่วยงานในสังกัดที่เกี่ยวข้อง
- จัดทำรายงานการประเมินผลการควบคุมภายในระดับองค์กร
- องค์กรประกอบและคุณสมบัติของคณะกรรมการควบคุมภายในเป็นไปตามที่องค์กรกำหนด โดยอาจเป็นคณะทำงาน ซึ่งอาจประกอบด้วยผู้บริหาร

## 3) หัวหน้าหน่วยงานควบคุมภายใน

- ให้คำปรึกษาในฐานะผู้เชี่ยวชาญด้านการควบคุมภายในและประสานงานเกี่ยวกับประเด็นด้านการควบคุมภายใน
- ให้ความเห็นชอบนโยบายการควบคุมภายใน กรอบการควบคุมภายใน และแนวทางการประเมินการควบคุมภายใน และนำเสนอคณะกรรมการควบคุมภายในและผู้บริหารสูงสุดต่อไป รวมถึงควบคุมดูแลให้มีการปฏิบัติตาม เพื่อให้บรรลุกลยุทธ์และวัตถุประสงค์ขององค์กร
- รายงานประเด็นด้านการควบคุมภายในต่อคณะกรรมการควบคุมภายใน ผู้บริหารสูงสุด และคณะกรรมการ

## 4) หน่วยงานควบคุมภายใน

- จัดทำและสื่อสารนโยบายการควบคุมภายใน กรอบการควบคุมภายใน และแนวทางการประเมินการควบคุมภายใน
- ให้คำแนะนำต่อผู้บริหารระดับสูงของแต่ละสายงานหรือเจ้าของกระบวนการในการกำหนดมาตรการควบคุมภายในอย่างเพียงพอและมีประสิทธิภาพ รวมถึงให้ข้อเสนอแนะในการปรับปรุงและพัฒนาระบบการควบคุมภายในอย่างต่อเนื่อง
- สนับสนุนให้มีการประเมินความเสี่ยงพอและประสิทธิภาพของกระบวนการควบคุมภายใน และรวบรวมผลการประเมินนำเสนอต่อหัวหน้าหน่วยงานควบคุมภายใน

## 5) ผู้บริหารระดับสูงของแต่ละสายงาน หรือเจ้าของกระบวนการ

- กำหนดมาตรการการควบคุมภายในและดูแลระบบการควบคุมภายในของหน่วยงานของตน เพื่อบริหารความเสี่ยงให้อยู่ในระดับที่ยอมรับได้
- สื่อสารไปยังพนักงานในหน่วยงานเกี่ยวกับการปฏิบัติตามระบบการควบคุมภายใน รวมถึงให้คำแนะนำเกี่ยวกับบทบาทและความรับผิดชอบด้านการควบคุมภายในแก่พนักงานในหน่วยงาน

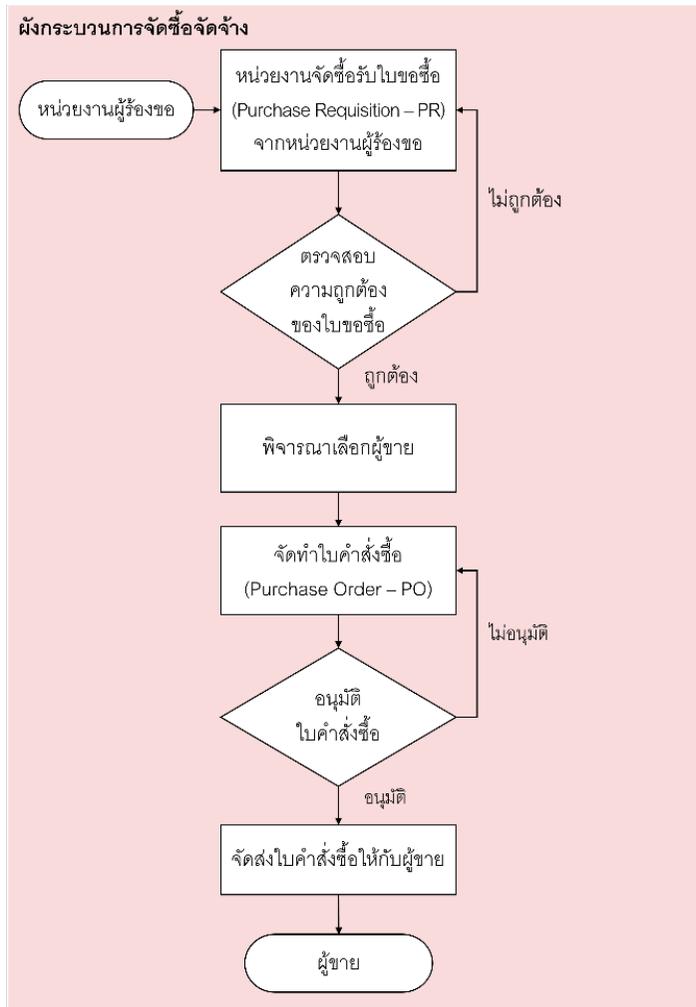
- ประเมินความเพียงพอและประสิทธิภาพของกระบวนการควบคุมภายใน โดยเลือกใช้วิธีการประเมินอย่างต่อเนื่องระหว่างการทำงาน (Ongoing Monitoring) และ/หรือการประเมินเป็นครั้งคราวแบบแยกต่างหาก (Separate Evaluations) ตามความเหมาะสม

ทั้งนี้ สำหรับหน้าที่ของคณะกรรมการตรวจสอบ คณะกรรมการบริหารความเสี่ยง และผู้ตรวจสอบภายในสามารถอ้างอิงรายละเอียดเพิ่มเติมในบทที่ 3 หลักเกณฑ์ แนวปฏิบัติ และคู่มือปฏิบัติเกี่ยวกับการบริหารความเสี่ยงสำหรับรัฐวิสาหกิจ องค์ประกอบที่ 1 แนวปฏิบัติที่ 2 และสำหรับหน้าที่ของคณะกรรมการ อ้างอิงรายละเอียดดังกล่าวเพิ่มเติมในบทที่ 4 หลักเกณฑ์ แนวปฏิบัติ และคู่มือปฏิบัติเกี่ยวกับการควบคุมภายในสำหรับรัฐวิสาหกิจ องค์ประกอบที่ 1 แนวปฏิบัติที่ 2

2. รัฐวิสาหกิจควรพิจารณากำหนดบทบาท หน้าที่ ความรับผิดชอบในแต่ละกระบวนการทำงาน โดยจัดทำคู่มือระบบงาน (Manual Documentation) ในทุกกระบวนการทำงาน ทั้งนี้ การจัดทำ การเก็บรักษา เอกสาร และการสอบทานคู่มือให้เป็นปัจจุบันอยู่เสมอจะช่วยให้การทำงานเป็นไปได้อย่างต่อเนื่อง ไม่มีความเสี่ยงที่พนักงานที่เหลืออยู่จะไม่สามารถปฏิบัติงานได้ หากผู้รับผิดชอบเดิมไม่สามารถปฏิบัติงานได้

ทั้งนี้ ในการจัดทำคู่มือระบบงาน ควรมีการกำหนดผู้รับผิดชอบในการจัดทำ การสอบทาน และการอนุมัติ รวมถึงมีการปรับปรุงคู่มือระบบงานให้เป็นปัจจุบัน สอดคล้องกับวัตถุประสงค์ และเป้าหมายขององค์กร อย่างสม่ำเสมอ รวมทั้งสื่อสารคู่มือระบบงานดังกล่าวให้พนักงานได้รับทราบ เพื่อให้เกิดความเข้าใจตรงกัน

## ตัวอย่างผังกระบวนการ (Flowchart)



### คำอธิบาย

หน่วยงานจัดซื้อรับเอกสารใบขอซื้อ (Purchase Requisition: PR) จากหน่วยงานผู้ร้องขอ จากนั้นทำการตรวจเอกสารใบขอซื้อว่ามีข้อมูลครบถ้วน ถูกต้อง และได้รับการอนุมัติอย่างถูกต้องหรือไม่ หากไม่ถูกต้องเจ้าหน้าที่หน่วยงานจัดซื้อส่งใบขอซื้อให้กับหน่วยงานผู้ร้องขอเพื่อทำการแก้ไข ในกรณีที่ข้อมูลในเอกสารใบขอซื้อ มีข้อมูลครบถ้วน ถูกต้อง และได้รับการอนุมัติเรียบร้อยแล้ว หน่วยงานจัดซื้อส่งเอกสารใบขอซื้อให้กับเจ้าหน้าที่จัดซื้ออาวุโส เพื่อพิจารณาเลือกผู้ขายจากฐานข้อมูลในระบบ และจัดทำเอกสารใบคำสั่งซื้อ (Purchase Order: PO) จากนั้นส่งให้หัวหน้าหน่วยงานจัดซื้อตรวจสอบและพิจารณาอนุมัติ เมื่อเอกสารใบคำสั่งซื้อได้รับการอนุมัติเรียบร้อยแล้ว หน่วยงานจัดซื้อส่งใบคำสั่งซื้อต้นฉบับให้กับผู้ขายและเก็บสำเนาใบสั่งซื้อเข้าแฟ้ม

3. รัฐวิสาหกิจควรกำหนดขอบเขตระดับของอำนาจอนุมัติให้ชัดเจนเป็นลายลักษณ์อักษรและสื่อสารให้พนักงานภายในองค์กรทราบ รวมทั้งมีระบบการติดตามงานระหว่างผู้บริหารระดับสูงและพนักงาน

## แนวปฏิบัติที่ 4

รัฐวิสาหกิจควรออกแบบนโยบายและแนวปฏิบัติด้านทรัพยากรบุคคล ซึ่งครอบคลุมการจูงใจ พัฒนา รักษาไว้ และนำไปปฏิบัติ เพื่อให้เกิดการควบคุมภายในที่มีประสิทธิผล รวมถึงเพื่อให้มั่นใจว่าองค์กรมีบุคลากรที่มีความชำนาญและประสบการณ์ที่จำเป็น

### คู่มือปฏิบัติ

1. รัฐวิสาหกิจควรกำหนดวิธีบริหารด้านทรัพยากรบุคคลอย่างเป็นลายลักษณ์อักษร โดยกำหนดให้มีนโยบายและแนวทางการปฏิบัติงานเกี่ยวกับการบริหารทรัพยากรบุคคล ตั้งแต่การกำหนดอัตรากำลังคน การสรรหาบุคลากร การประเมินผลการทดลองงาน การประเมินผลการปฏิบัติงาน การพัฒนาบุคลากร การรักษาบุคลากร การเลื่อนขั้นเงินเดือน การเลื่อนตำแหน่ง การโอนย้ายบุคลากร การลาออกหรือพ้นสภาพ และการอบรมพนักงานใหม่อย่างชัดเจน รวมถึงเผยแพร่แนวทางหรือหลักเกณฑ์ด้านทรัพยากรบุคคลให้พนักงานรับทราบโดยละเอียด โดยการจัดทำนโยบายและวิธีบริหารบุคลากรควรมุ่งเน้นเรื่องที่เกี่ยวข้องกับการควบคุมภายในโดยตรง ดังตัวอย่างต่อไปนี้
  - 1) ด้านการบริหาร
    - กำหนดขอบเขตหน้าที่และความรับผิดชอบของแต่ละหน่วยงานและพนักงานให้ชัดเจนเหมาะสม ไม่ซ้ำซ้อนกัน พร้อมทั้งมีการแบ่งแยกหน้าที่เพื่อให้สามารถตรวจสอบและถ่วงดุลกันได้อย่างมีประสิทธิภาพ
    - การดำเนินงานด้านการบริหารงานบุคคลควรจัดทำในรูปคณะกรรมการ ซึ่งประกอบด้วยตัวแทนจากหน่วยงานต่างๆ
    - มีการมอบอำนาจในการดำเนินงานให้เหมาะสม เพื่อให้หน่วยงานมีความคล่องตัวในการปฏิบัติงาน รวมทั้งดูแลปรับปรุงให้สอดคล้องกับการขยายหรือลดขอบเขตในการปฏิบัติงาน
  - 2) อัตรากำลังคน
    - จัดทำแผนและงบประมาณกำลังคน พร้อมทั้งปรับปรุงอยู่เสมอ
    - กำหนดนโยบาย แผน และแนวปฏิบัติการใช้กำลังคน
    - การอนุมัตินโยบาย แผน และแนวปฏิบัติการใช้กำลังคน ผ่านความเห็นชอบจากคณะกรรมการที่เกี่ยวข้อง

### 3) การสรรหาบุคลากร

- คัดเลือกผู้สมัครงานและตัดสินใจรับเข้าทำงานโดยคณะกรรมการที่เกี่ยวข้อง
- กำหนดอัตราค่าจ้างเริ่มต้นตามวุฒิการศึกษา และประสบการณ์
- กำหนดหลักเกณฑ์ในการคำนวณค่าประสบการณ์
- มีหนังสือเงื่อนไขการทดลองงานและสัญญาว่าจ้างที่เป็นมาตรฐาน

### 4) การประเมินผลการปฏิบัติงาน

- กำหนดหลักเกณฑ์และแนวปฏิบัติในการประเมินผลการปฏิบัติงานและศักยภาพพนักงาน แต่ละคนให้ครอบคลุมเรื่องการควบคุมภายใน
- จัดทำแบบฟอร์มประเมินผลการปฏิบัติงานไว้เป็นมาตรฐาน และกำหนดระยะเวลาในการประเมิน
- มีการประเมินจุดอ่อนหรือจุดแข็งของพนักงาน เพื่อประโยชน์ในการดูแลและพัฒนาพนักงาน ให้ปฏิบัติงานอย่างมีประสิทธิภาพและประสิทธิผลสูงสุด
- จัดให้มีระบบการให้คำปรึกษาหรือแก่พนักงาน ประกอบการประเมินผลการปฏิบัติงาน

### 5) การบริหารค่าจ้าง

- มีนโยบาย หลักเกณฑ์ แนวปฏิบัติในการบริหารค่าจ้าง
- กำหนดให้มีคณะกรรมการบุคคลเพื่อพิจารณาการเปลี่ยนแปลงค่าจ้าง ในกรณีต่างๆ ให้ลูกจ้าง
- การจ่ายค่าจ้าง การเปลี่ยนแปลงค่าจ้าง และการหักค่าจ้างต้องเป็นไปตามหลักเกณฑ์ของกฎหมายแรงงานรัฐวิสาหกิจสัมพันธ์
- การกำหนดงบประมาณขึ้นค่าจ้างประจำปีให้ผ่านการพิจารณาของคณะกรรมการบุคคล หรือผู้มีอำนาจ
- การกำหนดแรงจูงใจต้องสอดคล้องตามที่หน่วยงานกำกับดูแลกำหนด เช่น ระบบโบนัส ระบบการประกาศจัดอันดับผลงานของรัฐวิสาหกิจประจำปีตามระบบประเมินผลการดำเนินงานรัฐวิสาหกิจ

### 6) การพัฒนาบุคลากร

- กำหนดนโยบายด้านการพัฒนาบุคลากร
- กำหนดแผนการพัฒนาและเป้าหมายการฝึกอบรมประจำปี
- มีการสำรวจความจำเป็นในการอบรม ดำเนินการจัดอบรม และระบบติดตามผลการอบรมของบุคลากรที่ผ่านการอบรม
- จัดทำประวัติการฝึกอบรมพนักงานไว้เป็นรายบุคคล
- แสวงหาและริเริ่มแนวความคิดใหม่ๆ ในการพัฒนาบุคลากรมาประยุกต์ใช้ในองค์กร
- กำหนดแนวทางการพัฒนาบุคลากร และคุณสมบัติของแต่ละตำแหน่งในเส้นทางความก้าวหน้าในอาชีพ (Career Path)

- จัดทำแผนสืบทอดตำแหน่ง (Succession Plan) สำหรับบุคลากรในตำแหน่งสำคัญ และมีความเสี่ยงสูงต่อการดำเนินงานขององค์กร (Critical Position)

รวมถึงรัฐวิสาหกิจควรจัดทำข้อบังคับเกี่ยวกับการทำงาน โดยครอบคลุมเรื่องสำคัญดังต่อไปนี้

- การบรรจุและแต่งตั้ง
- อัตราเงินเดือน และการเลื่อนเงินเดือน
- วันทำงาน เวลาทำงานปกติ และเวลาพัก
- วันหยุดและหลักเกณฑ์การหยุด
- วันลาและหลักเกณฑ์การลา
- หลักเกณฑ์การทำงานล่วงเวลาและการทำงานในวันหยุด
- วันและสถานที่จ่ายค่าจ้าง ค่าล่วงเวลา ค่าทำงานในวันหยุด และค่าล่วงเวลาในวันหยุด
- การพัฒนาบุคลากร
- การเลิกจ้าง ค่าชดเชย และค่าชดเชยพิเศษ
- วินัยและโทษทางวินัย
- การร้องทุกข์

## แนวปฏิบัติที่ 5

รัฐวิสาหกิจควรกำหนดให้ผู้บริหารและพนักงานได้รับมอบอำนาจหน้าที่และความรับผิดชอบต่อผลการปฏิบัติงานในระดับที่เหมาะสม เพื่อให้มั่นใจว่ามีการควบคุมภายในที่มีประสิทธิภาพ

### คู่มือปฏิบัติ

1. รัฐวิสาหกิจควรกำหนดให้มีการจัดทำคำพรรณนาลักษณะงาน (JD) ของผู้บริหารและพนักงาน ในทุกระดับ เพื่อใช้ในการกำหนดอำนาจหน้าที่และความรับผิดชอบให้มีการปฏิบัติตามกิจกรรมการควบคุมตามที่องค์กรกำหนดและเพื่อใช้ในการยึดถือและปฏิบัติหน้าที่ของแต่ละตำแหน่งงาน อีกทั้งยังสามารถใช้เป็นเกณฑ์ในการพิจารณาบรรจุแต่งตั้งบุคลากรให้เหมาะสมกับหน้าที่และความรับผิดชอบ เพื่อให้การดำเนินงานบรรลุผลสำเร็จตามวัตถุประสงค์ที่ตั้งไว้ รวมถึงกำหนดให้มีการทบทวนเป็นประจำอย่างน้อย ปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงอย่างมีนัยสำคัญ ทั้งนี้ ในการจัดทำคำพรรณนาลักษณะงาน (JD) ควรมีการกำหนดผู้รับผิดชอบในการจัดทำ การสอบถาม และการอนุมัติ รวมถึงมีการปรับปรุงคำพรรณนาลักษณะงาน (JD) ให้เป็นปัจจุบัน สอดคล้องกับวัตถุประสงค์และเป้าหมายขององค์กรอย่างสม่ำเสมอ รวมทั้งสื่อสารคำพรรณนาลักษณะงาน (JD) ดังกล่าวผ่านช่องทางภายในขององค์กร เพื่อให้พนักงานได้รับทราบและมีความเข้าใจตรงกัน

ตัวอย่างคำพจนานัลักษณะงาน (JD)

ตำแหน่ง สถานที่ปฏิบัติงาน ฝ่าย รายงานต่อ/ผู้บังคับบัญชา ค่าล่วงเวลา	ผู้อำนวยการฝ่ายบริหารทรัพยากรบุคคล สำนักงานใหญ่ บริหารทรัพยากรบุคคล รองกรรมการผู้จัดการ สายงานทรัพยากรบุคคล ไม่มีค่าล่วงเวลา
ลักษณะงาน	<ul style="list-style-type: none"> <li>• ความรับผิดชอบหลัก คือ การวางแผนนโยบายและกำหนดแผนงาน เพื่อบริหารบุคลากรในองค์กรให้สามารถปฏิบัติงานได้อย่างมีประสิทธิภาพ สอดคล้องกับวัตถุประสงค์ขององค์กร</li> </ul>
ความรับผิดชอบ	<ul style="list-style-type: none"> <li>• ให้คำปรึกษาเชิงกลยุทธ์และคำแนะนำต่างๆ ที่เกี่ยวข้องกับการบริหารงาน ด้านทรัพยากรบุคคล</li> <li>• กำหนดกลยุทธ์ในการพัฒนาทรัพยากรบุคคล</li> <li>• บริหารจัดการทรัพยากรบุคคลในระดับปฏิบัติงานและสร้างความมั่นใจว่า นโยบายต่างๆ แผนงานและโครงการต่างๆ ดำเนินไปอย่างมีประสิทธิภาพ</li> <li>• จัดทำแผนอัตรากำลังคน และกำกับดูแลให้มีการทบทวนปรับปรุงให้เป็นปัจจุบันอย่างสม่ำเสมอ</li> <li>• จัดทำระเบียบและแนวปฏิบัติในเรื่องการบริหารทรัพยากรบุคคลที่ชัดเจน และปรับปรุงให้สอดคล้องกับสถานการณ์อยู่เสมอ</li> <li>• จัดทำอัตราเงินเดือนและกำกับดูแลให้อัตรากำลังเดือนอยู่ในระดับที่สามารถแข่งขันกับองค์กรอื่นในอุตสาหกรรมเดียวกัน</li> <li>• กำกับดูแลให้ผู้ใต้บังคับบัญชาปฏิบัติงานตามหน้าที่ที่ได้รับมอบหมาย อย่างเคร่งครัด และปฏิบัติงานโดยยึดถือจรรยาบรรณในการประกอบ กิจการ (Code of Conduct) หากพบผู้ไม่ปฏิบัติตามให้พิจารณา บทลงโทษตามข้อบังคับขององค์กร</li> </ul>
พนักงานใต้บังคับบัญชา	<ul style="list-style-type: none"> <li>• ผู้จัดการ ฝ่ายบริหารทรัพยากรบุคคล</li> <li>• เจ้าหน้าที่อาวุโส ฝ่ายบริหารทรัพยากรบุคคล</li> <li>• เจ้าหน้าที่ ฝ่ายบริหารทรัพยากรบุคคล</li> </ul>
ความรู้	<ul style="list-style-type: none"> <li>• ความรู้ความเข้าใจด้านการพัฒนาและบริหารทรัพยากรบุคคล</li> <li>• ความรู้ความเข้าใจเกี่ยวกับกฎหมาย และกฎระเบียบต่างๆ ที่เกี่ยวข้องกับการบริหารทรัพยากรบุคคลและการดำเนินงานของรัฐวิสาหกิจ</li> </ul>

ความสามารถ และทักษะต่างๆ	<ul style="list-style-type: none"> <li>• ความเป็นผู้นำ</li> <li>• ทักษะในการคิด วิเคราะห์</li> <li>• การใช้ภาษาไทยและภาษาอังกฤษ ในการอ่าน และเขียนรายงาน</li> <li>• ความสามารถในการใช้คอมพิวเตอร์ในการจัดทำเอกสารและนำเสนองาน</li> </ul>
การศึกษา	<ul style="list-style-type: none"> <li>•ปริญญาตรีด้านการพัฒนาหรือบริหารทรัพยากรบุคคล หรือสาขาที่เกี่ยวข้อง</li> <li>•ปริญญาโทด้านการบริหาร</li> </ul>
ประสบการณ์ทำงาน	<ul style="list-style-type: none"> <li>• ประสบการณ์ทำงานในด้านการพัฒนา และ/หรือ บริหารทรัพยากรบุคคล 5 ปีขึ้นไป</li> <li>• ประสบการณ์ทำงานในตำแหน่งบริหาร 3 ปีขึ้นไป</li> </ul>

2. รัฐวิสาหกิจควรกำหนดเป้าหมายในการดำเนินงานที่ท้าทาย เพื่อเป็นการจูงใจให้สามารถดำเนินการได้ตามวัตถุประสงค์และเป้าหมายขององค์กร ในขณะเดียวกันเป้าหมายดังกล่าวควรได้รับการยอมรับจากผู้ที่เกี่ยวข้อง เช่น พนักงานผู้ปฏิบัติงาน ดังนั้น ควรมีการปรึกษาหารือร่วมกันระหว่างผู้บริหารและพนักงานในการกำหนดเป้าหมายข้างต้น เพื่อให้มีความเข้าใจตรงกัน และได้รับการยอมรับจากผู้ที่เกี่ยวข้อง จากนั้นควรจัดให้มีการประเมินผลการปฏิบัติงานประจำปี โดยใช้แบบประเมินดัชนีชี้วัดผลการดำเนินงาน (KPI) สำหรับประเมินบุคลากรที่กำหนดให้ครอบคลุมเป้าหมาย บทบาทหน้าที่ของพนักงานตามคำพรรณนาลักษณะงาน (JD) และการปฏิบัติตามจรรยาบรรณในการประกอบกิจการ (Code of Conduct) ทั้งนี้ ดัชนีชี้วัดดังกล่าวควรได้รับการพิจารณาและปรับปรุงตามความเหมาะสมโดยฝ่ายบริหาร และอนุมัติโดยผู้บริหาร เพื่อให้มั่นใจว่าดัชนีชี้วัดผลการดำเนินงาน (KPI) ไม่ได้สร้างแรงกดดันที่มากเกินไปในการปฏิบัติงานของพนักงาน รวมถึงใช้เป็นส่วนหนึ่งในการพิจารณาให้ผลตอบแทนเพื่อสร้างแรงจูงใจทั้งที่เป็นตัวเงินและไม่เป็นตัวเงินให้กับพนักงาน เช่น การเลื่อนเงินเดือน การให้โบนัส การเลื่อนตำแหน่ง ภายหลังจากการประเมินผลการปฏิบัติงานของพนักงาน ทั้งนี้ รัฐวิสาหกิจควรกำหนดให้มีการสื่อสารผลการประเมินให้พนักงานรับทราบด้วย

## องค์ประกอบที่ 2 การประเมินความเสี่ยง (Risk Assessment)

### หลักเกณฑ์

รัฐวิสาหกิจควรประเมินความเสี่ยงเพื่อให้ทราบว่าองค์กรมีความเสี่ยงอย่างไร มีระดับความเสี่ยงและโอกาสที่จะเกิดมากน้อยเพียงใด เนื่องจากองค์กรต้องเผชิญกับความเสี่ยงที่เกิดจากปัจจัยภายในและปัจจัยภายนอกที่หลีกเลี่ยงไม่ได้ ซึ่งส่งผลกระทบต่อผลสำเร็จตามวัตถุประสงค์ขององค์กร ดังนั้น ผู้บริหารต้องพิจารณาว่าองค์กรควรมีมาตรการหรือบริหารจัดการอย่างไร เพื่อจัดการกับความเสี่ยงดังกล่าวให้อยู่ในระดับความเสี่ยงที่องค์กรยอมรับได้ (RA)

### แนวปฏิบัติที่ 1

รัฐวิสาหกิจควรกำหนดวัตถุประสงค์ระดับองค์กรและระดับหน่วยงานที่เกี่ยวข้องกับการควบคุมภายในให้ชัดเจน พร้อมระบุหลักเกณฑ์ เพื่อให้สามารถระบุและประเมินความเสี่ยงที่อาจส่งผลกระทบต่อองค์กรไม่บรรลุวัตถุประสงค์ที่กำหนดไว้

### คู่มือปฏิบัติ

1. รัฐวิสาหกิจควรกำหนดวัตถุประสงค์ที่เกี่ยวข้องกับการควบคุมภายในดังต่อไปนี้
  - 1) กำหนดวัตถุประสงค์ระดับองค์กรที่เกี่ยวข้องกับการควบคุมภายใน เช่น เป็นรัฐวิสาหกิจที่ดำเนินการเพื่อประโยชน์ต่อสังคม โดยมีการกำกับดูแลกิจการที่ดี (Good Governance) และดำเนินการด้วยความเป็นธรรม ปราศจากการทุจริต
  - 2) กำหนดวัตถุประสงค์ระดับหน่วยงานที่เกี่ยวข้องกับการควบคุมภายใน เช่น
    - การแบ่งแยกหน้าที่ที่ชัดเจน
    - การกำหนดให้มีการสอบทาน และอนุมัติในขั้นตอนการทำงานที่สำคัญ หรือมีผลกระทบอย่างเป็นทางการต่อการดำเนินงานของรัฐวิสาหกิจ

ทั้งนี้ การดำเนินกิจการขององค์กรมักจะกำหนดวัตถุประสงค์หรือเป้าหมายขององค์กรไว้ทั้งในระยะสั้นและระยะยาว วัตถุประสงค์ระดับองค์กร (Entity-Wide Objective) มักแสดงอยู่ในแถลงการณ์ภารกิจ (Mission Statement) ซึ่งวัตถุประสงค์ระดับองค์กรเหล่านี้มักจะถูกเชื่อมโยงและประสานกับวัตถุประสงค์ย่อย ที่กำหนดไว้เฉพาะเจาะจงในแต่ละกิจกรรม ซึ่งเรียกว่า วัตถุประสงค์ระดับกิจกรรม (Activity-Level Objective) โดยวัตถุประสงค์ทั้งสองชนิดนี้ต้องสอดคล้องกัน

การที่จะช่วยให้ผู้บริหารดำเนินงานให้บรรลุวัตถุประสงค์ได้ คือ การสร้างระบบการควบคุมภายในที่ดี ซึ่งวัตถุประสงค์ของการควบคุมภายใน มี 3 ประการ ดังนี้

- 1) วัตถุประสงค์ด้านการดำเนินงาน (Operations Objectives) เป็นวัตถุประสงค์เกี่ยวกับความมีประสิทธิภาพและประสิทธิผลของการดำเนินงาน รวมถึงการบรรลุเป้าหมายด้านการดำเนินงานด้านการเงิน ตลอดจนการใช้ทรัพยากร การดูแลรักษาทรัพย์สิน การป้องกันหรือลดความผิดพลาดของรัฐวิสาหกิจ ตลอดจนความเสียหาย การรั่วไหล การสิ้นเปลืองหรือการทุจริตในรัฐวิสาหกิจ
  - 2) วัตถุประสงค์ด้านการรายงานทางการเงิน (Reporting Objectives) เป็นวัตถุประสงค์เกี่ยวกับการรายงานทางการเงินและไม่ใช่ทางการเงิน ที่ใช้ภายในและภายนอกรัฐวิสาหกิจ รวมถึงการรายงานที่เชื่อถือได้ ทันเวลา โปร่งใส หรือข้อกำหนดอื่นของทางราชการ
  - 3) วัตถุประสงค์ด้านการปฏิบัติตามกฎหมาย ระเบียบและข้อบังคับ (Compliance Objectives) เป็นวัตถุประสงค์เกี่ยวกับการปฏิบัติตามกฎหมาย ระเบียบ ข้อบังคับหรือมติคณะรัฐมนตรีที่เกี่ยวข้องกับการดำเนินงาน รวมทั้งข้อกำหนดอื่นของทางราชการ
2. รัฐวิสาหกิจควรกำหนดให้รายงานทางการเงินและระดับสาระสำคัญของรายงานทางการเงินเป็นไปตามมาตรฐานการบัญชีที่รับรองทั่วไป ทั้งนี้ องค์กรต้องมั่นใจว่ารายงานทางการเงินสะท้อนถึงกิจกรรมการดำเนินงานอย่างแท้จริง และกำหนดสาระสำคัญของรายงานทางการเงินโดยคำนึงถึงปัจจัยที่สำคัญ เช่น ผู้ใช้รายงานทางการเงิน ขนาดของรายการ แนวโน้มของธุรกิจ

## แนวปฏิบัติที่ 2

รัฐวิสาหกิจควรระบุเหตุการณ์ความเสี่ยงทั้งปัจจัยภายนอกและภายใน ซึ่งอาจมีผลกระทบต่อการทำงานอย่างมีนัยสำคัญ และกำหนดเกณฑ์ในการพิจารณาระดับความสำคัญของความเสี่ยง จากนั้นจัดลำดับความสำคัญของความเสี่ยง และกำหนดมาตรการและวิธีการควบคุมภายในเพื่อให้มั่นใจว่าการควบคุมภายในสามารถควบคุมจุดที่มีความเสี่ยงให้อยู่ในระดับความเสี่ยงที่องค์กรยอมรับได้ (RA) รวมถึงควรติดตามความเสี่ยง เพื่อให้องค์กรทราบความคืบหน้าของการจัดการความเสี่ยงนั้นๆ

### คู่มือปฏิบัติ

1. รัฐวิสาหกิจควรระบุเหตุการณ์ความเสี่ยง โดยระบุเหตุการณ์ความเสี่ยงทั้งปัจจัยภายนอกและภายใน ซึ่งอาจมีผลกระทบต่อการทำงานอย่างมีนัยสำคัญ โดยมีขั้นตอน ดังนี้
  - 1) ทำความเข้าใจเกี่ยวกับธุรกิจ และการรวบรวมข้อมูล โดยผู้ประเมินต้องมีความเข้าใจเกี่ยวกับธุรกิจขององค์กรในแต่ละระดับ ดังต่อไปนี้

- ระดับองค์กร (Entity-Wide Level) ได้แก่ ประเภทธุรกิจหลักของกิจการ โครงสร้างองค์กร (Organization Chart) และโครงสร้างบริหารงาน ลักษณะของอุตสาหกรรม สภาพทางเศรษฐกิจ และแนวโน้มทางธุรกิจ นโยบายการบริหารงาน และนโยบายการบัญชี และการเงิน เป็นต้น
- ระดับกิจกรรม (Activity Level) ได้แก่ ลักษณะของรายการค้า ตลอดจนช่องทางการจัดจำหน่าย หน่วยงานต่างๆ ในองค์กร ลักษณะความซับซ้อนของรายการทางธุรกิจ ความมีสาระสำคัญของจำนวนเงิน หรือยอดคงเหลือในงบการเงิน รายการค้ากับกิจการที่เกี่ยวข้องกัน ลักษณะของระบบข้อมูล และการบัญชี เช่น ระบบการประมวลผลข้อมูล มีการพัฒนาโดยองค์กรเอง หรือว่าจ้างบุคคลภายนอก ขอบเขตและความซับซ้อนของระบบคอมพิวเตอร์ โดยการทำความเข้าใจเกี่ยวกับธุรกิจ สามารถทำได้โดย
  - ใช้ข้อมูลในปีก่อนๆ ได้แก่ รายงานประจำปี รายงานการประชุมในส่วนที่เกี่ยวกับการตัดสินใจในเรื่องสำคัญๆ ของการดำเนินงาน ตัวเลขสถิติที่สำคัญ เป็นต้น ซึ่งสามารถนำมาใช้เป็นแนวทางและเป็นข้อมูลเบื้องต้นได้ โดยข้อมูลเหล่านี้ต้องมีการแก้ไขให้เป็นปัจจุบัน
  - สอบถามจากเจ้าหน้าที่ขององค์กร ได้แก่ การสอบถามผู้บริหาร และพนักงานโดยควรมีการคิดคำถามไว้ล่วงหน้า เช่น จัดทำเป็นแบบสอบถาม เพื่อให้สามารถแน่ใจว่าจะได้ข้อมูลที่ต้องการอย่างครบถ้วน
  - ศึกษาจากคู่มือปฏิบัติงาน และเอกสารเกี่ยวกับระบบงานต่างๆ ได้แก่ คู่มือบัญชี โครงสร้างองค์กร (Organization Chart) และคู่มือนโยบายขององค์กร
  - ตรวจสอบเอกสารและสมุดบันทึก เพื่อให้เข้าใจว่าเอกสารต่างๆ มีลักษณะอย่างไร เอกสารจัดทำขึ้นอย่างไร ส่งผ่านเอกสารอย่างไร และบันทึกเอกสารเพื่อการควบคุมอย่างไร
  - สังเกตการณ์การปฏิบัติงานของเจ้าหน้าที่ ซึ่งจะช่วยให้เกิดความเข้าใจ และเห็นได้ว่านโยบายการควบคุม และขั้นตอนการปฏิบัติงานได้มีการปฏิบัติตามจริง

2) ระบุปัจจัยเสี่ยง โดยฝ่ายบริหารจำเป็นต้องตั้งคำถามว่ามีเหตุการณ์ใดหรือกิจกรรมใดของกระบวนการปฏิบัติงาน ที่อาจเกิดความผิดพลาด เสียหาย ไม่บรรลุวัตถุประสงค์ในระดับองค์กรและระดับกิจกรรมที่กำหนด รวมทั้งมีทรัพย์สินใดที่จำเป็นต้องได้รับการดูแลป้องกันรักษา เช่น ความเสี่ยงจากการจัดซื้อจัดจ้างในราคาแพง ความเสี่ยงจากการซื้อพัสดุที่มีคุณภาพต่ำกว่าที่กำหนด

2. รัฐวิสาหกิจควรกำหนดเกณฑ์ในการพิจารณาระดับความสำคัญของความเสี่ยง และทำการวิเคราะห์โดยประมาณการโอกาสที่จะเกิดหรือความเป็นไปได้ (Likelihood) ว่ามีมากน้อยเพียงใด และพิจารณาผลกระทบจากความเสี่ยง (Impact)

3. รัฐวิสาหกิจควรจัดลำดับความสำคัญของความเสี่ยงที่มีผลต่อองค์กร โดยการใช้วิธีการให้คะแนน ซึ่งสามารถอ้างอิงรายละเอียดการจัดลำดับความเสี่ยงเพิ่มเติมในบทที่ 3 หลักเกณฑ์ แนวปฏิบัติ และคู่มือปฏิบัติเกี่ยวกับการบริหารความเสี่ยงสำหรับรัฐวิสาหกิจ องค์กรประกอบที่ 3 แนวปฏิบัติที่ 3
4. รัฐวิสาหกิจควรพิจารณาวิธีการจัดการกับความเสี่ยง ซึ่งเป็นขั้นตอนการลดความเสี่ยงโดยจะต้องวิเคราะห์สาเหตุที่ทำให้เกิดความเสี่ยงและพิจารณาว่าจะจัดการกับความเสี่ยงนั้นอย่างไร โดยมีวิธีการตอบสนองต่อความเสี่ยง ดังนี้
- การยอมรับความเสี่ยง (Acceptance)
  - การลดความเสี่ยง (Reduction)
  - การหาผู้ร่วมรับความเสี่ยง (Sharing)
  - การหลีกเลี่ยงความเสี่ยง (Avoidance)
  - การดำเนินการต่อ (Pursuing)

ทั้งนี้ ในการพิจารณาเลือกการตอบสนองต่อความเสี่ยง ผู้บริหารต้องพิจารณาถึงปัจจัย ดังนี้

- ระดับผลกระทบที่อาจเกิดขึ้นของความเสี่ยง และช่วงเปี่ยงเบนของระดับความเสี่ยงที่องค์กรยอมรับได้ (RT)
- การแบ่งแยกหน้าที่ที่ดี เพื่อให้มั่นใจว่าองค์กรดำเนินการตอบสนองต่อความเสี่ยงได้อย่างมีประสิทธิภาพ
- ค่าใช้จ่ายหรือต้นทุนในการจัดการความเสี่ยง เปรียบเทียบกับผลประโยชน์ที่จะได้รับ

โดยสามารถอ้างอิงรายละเอียดการตอบสนองต่อความเสี่ยงเพิ่มเติมในบทที่ 3 หลักเกณฑ์ แนวปฏิบัติ และคู่มือปฏิบัติเกี่ยวกับการบริหารความเสี่ยงสำหรับรัฐวิสาหกิจ องค์กรประกอบที่ 3 แนวปฏิบัติที่ 4

สำหรับความเสี่ยงจากปัจจัยภายในและภายนอกซึ่งอยู่ภายใต้การควบคุมของรัฐวิสาหกิจ การป้องกันหรือลดความเสี่ยงทำได้โดยการจัดให้มีวิธีการควบคุมอย่างเพียงพอและเหมาะสม

#### ตัวอย่างของการกำหนดวิธีการควบคุม เพื่อจัดการความเสี่ยงจากปัจจัยภายในและภายนอก

ความเสี่ยง	วิธีการควบคุม
<b>1. ความเสี่ยงจากปัจจัยภายใน</b>	
การจัดซื้อพัสดุราคาแพงแต่คุณภาพต่ำ	<ul style="list-style-type: none"> <li>• การกำหนดนโยบายการคัดเลือกผู้ขายที่ดีที่สุด ทั้งในเรื่องคุณภาพและราคา</li> <li>• การกำหนดวงเงินการอนุมัติจัดซื้อให้เหมาะสม</li> </ul>

ความเสี่ยง	วิธีการควบคุม
ทรัพย์สินขององค์กรสูญหาย	<ul style="list-style-type: none"> <li>• มีการทำทะเบียนคุมทรัพย์สิน ซึ่งแสดงรายละเอียดราคาทุน วันที่ได้มา ค่าเสื่อมราคา และสถานที่ตั้งของทรัพย์สินแต่ละรายการ</li> <li>• มีการให้รหัสทรัพย์สิน และติดป้ายรหัสไว้ที่ทรัพย์สินทุกชิ้น เพื่อสะดวกในการตรวจนับ</li> <li>• ตรวจนับทรัพย์สินที่มีอยู่จริงเทียบกับที่มีในทะเบียนคุม</li> <li>• มีการทำประกันภัยสำหรับทรัพย์สินที่มีมูลค่าสูง หรือเสี่ยงต่อการสูญหายหรือถูกทำลาย</li> </ul>
<b>2. ความเสี่ยงจากปัจจัยภายนอก</b>	
การซื้อสินค้าผูกขาดโดยผู้ผลิตน้อยราย	<ul style="list-style-type: none"> <li>• พยายามหาแหล่งผู้ผลิตรายอื่นเพื่อเป็นทางเลือก</li> <li>• พยายามหาสินค้าอื่นทดแทนสินค้าที่ถูกผูกขาด</li> </ul>
ความผันผวนของอัตราแลกเปลี่ยนเงินตราต่างประเทศ ส่งผลกระทบต่อเจ้าหน้าที่การค้าต่างประเทศ	<ul style="list-style-type: none"> <li>• ประกันความเสี่ยงของอัตราแลกเปลี่ยนเงินตราต่างประเทศ โดยการจัดทำสัญญาซื้อขายเงินตราต่างประเทศล่วงหน้า</li> <li>• พิจารณาหาแหล่งผู้ผลิตในประเทศเป็นทางเลือก เพื่อให้มีเจ้าหน้าที่การค้าเป็นเงินบาท</li> </ul>
การดำเนินงานหยุดชะงักอันเนื่องมาจากภัยธรรมชาติต่างๆ	<ul style="list-style-type: none"> <li>• จัดให้มีการจัดทำแผนการรองรับการหยุดชะงักของระบบงาน รวมทั้งกำหนดผู้รับผิดชอบในการวางแผนการรองรับการหยุดชะงักของระบบงานดังกล่าว</li> <li>• จัดให้มีการทดสอบแผนงาน</li> <li>• ปรับปรุงแผนงานให้เป็นปัจจุบันอยู่เสมอ</li> </ul>

5. รัฐวิสาหกิจควรกำหนดให้มีการติดตามความเสี่ยงผ่านความคืบหน้าของแผนจัดการความเสี่ยง หรือใช้ดัชนีชี้วัดอย่างสม่ำเสมอ โดยสามารถอ้างอิงรายละเอียดการติดตามความเสี่ยงเพิ่มเติมในบทที่ 3 หลักเกณฑ์ แนวปฏิบัติ และคู่มือปฏิบัติเกี่ยวกับการบริหารความเสี่ยงสำหรับรัฐวิสาหกิจ องค์ประกอบที่ 4 แนวปฏิบัติที่ 1

## แนวปฏิบัติที่ 3

รัฐวิสาหกิจควรประเมินความเป็นไปได้ที่จะเกิดความเสี่ยงด้านการทุจริต เพื่อประกอบการประเมินความเสี่ยงที่ส่งผลกระทบต่อบรรลุดัตถุประสงค์ขององค์กร รวมถึงคณะกรรมการควรกำกับดูแลให้มีการจัดทำนโยบายและแนวปฏิบัติด้านการต่อต้านการทุจริตคอร์รัปชันที่ชัดเจนและดำเนินการสื่อสารทั่วทั้งภายในและภายนอกองค์กร

### คู่มือปฏิบัติ

1. รัฐวิสาหกิจควรประเมินความเสี่ยงให้ครอบคลุมถึงความเสี่ยงด้านการทุจริต (Fraud Risk) ซึ่งในการประเมินความเสี่ยงดังกล่าว รัฐวิสาหกิจต้องพิจารณาปัจจัยดังต่อไปนี้
  - 1) โอกาสที่จะกระทำการทุจริตในแบบต่างๆ เช่น การจัดทำรายงานทางการเงินเป็นเท็จ การทำให้สูญเสียชีวิตทรัพย์สิน การคอร์รัปชัน การที่ผู้บริหารสามารถฝ่าฝืนระบบการควบคุมภายใน การเปลี่ยนแปลงข้อมูลในรายงานที่สำคัญ การได้มาหรือใช้ไปซึ่งทรัพย์สินโดยไม่ถูกต้อง
  - 2) ทักษะคิดและการหาเหตุผลเข้าข้างตนเองของบุคลากรที่มีส่วนร่วมหรือสนับสนุนการกระทำที่ไม่เหมาะสม
  - 3) แรงจูงใจและความกดดันในการบรรลุเป้าหมาย เช่น กำหนดเป้าหมายหรือแรงกดดันที่มากเกินไป อาจผลักดันให้พนักงานใช้วิธีการที่ไม่เหมาะสมหรือเกิดการทุจริตได้
2. รัฐวิสาหกิจควรกำหนดให้มีการจัดทำนโยบายและแนวปฏิบัติด้านการต่อต้านการทุจริตคอร์รัปชันอย่างเป็นลายลักษณ์อักษร โดยมีรายละเอียดที่ให้ความสำคัญกับการต่อต้านการทุจริตคอร์รัปชันภายใต้กรอบการกำกับดูแลกิจการที่ดี โดยยึดหลักธรรมาภิบาล มุ่งดำเนินธุรกิจอย่างมีจรรยาบรรณ โปร่งใส เป็นธรรม และสามารถตรวจสอบได้ รวมทั้งปฏิบัติตามกฎหมาย กฎระเบียบ และข้อบังคับอย่างเคร่งครัดเพื่อให้มั่นใจว่าองค์กรและบุคลากรไม่ยอมรับการทุจริตคอร์รัปชันทุกรูปแบบทั้งทางตรงและทางอ้อม รวมถึงสื่อสารนโยบายและแนวปฏิบัติเกี่ยวกับการต่อต้านการทุจริตคอร์รัปชันไปยังผู้มีส่วนได้เสียทั้งภายในและภายนอกองค์กร เพื่อให้เกิดความเข้าใจและตระหนักถึงความสำคัญอย่างทั่วถึง

## แนวปฏิบัติที่ 4

รัฐวิสาหกิจระบุและประเมินการเปลี่ยนแปลงของสภาพแวดล้อมภายในและภายนอกองค์กรที่อาจมีผลกระทบต่ออย่างมีนัยสำคัญต่อระบบการควบคุมภายใน

### คู่มือปฏิบัติ

1. รัฐวิสาหกิจควรกำหนดกระบวนการเพื่อระบุการเปลี่ยนแปลงต่างๆ ของสภาพแวดล้อมภายในและภายนอกองค์กรที่มีผลกระทบต่ออย่างมีนัยสำคัญกับความสามารถในการบรรลุวัตถุประสงค์ขององค์กร จากนั้นนำมาประเมินผลกระทบจากการเปลี่ยนแปลงที่อาจเกิดขึ้นและอาจส่งผลกระทบต่อการควบคุมภายใน เพื่อนำไปกำหนดแนวทางในการตอบสนองต่อการเปลี่ยนแปลงต่อไป โดยต้องประเมินให้ครอบคลุมการเปลี่ยนแปลงที่สำคัญ ดังนี้
  - การเปลี่ยนแปลงปัจจัยภายในและปัจจัยภายนอกองค์กร
  - การเปลี่ยนแปลงรูปแบบการประกอบกิจการ
  - การเปลี่ยนแปลงผู้นำหรือผู้ปฏิบัติหน้าที่สำคัญในองค์กร

โดยสามารถอ้างอิงตัวอย่างการเปลี่ยนแปลงปัจจัยภายในและปัจจัยภายนอกองค์กร เพิ่มเติมในบทที่ 3 หลักเกณฑ์ แนวปฏิบัติ และคู่มือปฏิบัติเกี่ยวกับการบริหารความเสี่ยงสำหรับรัฐวิสาหกิจ องค์กรประกอบที่ 4 แนวปฏิบัติที่ 1

## องค์ประกอบที่ 3 กิจกรรมการควบคุม (Control Activities)

### หลักเกณฑ์

รัฐวิสาหกิจควรจัดให้มีกิจกรรมการควบคุม โดยการกำหนดให้มีมาตรการหรือขั้นตอนในการปฏิบัติงานตามนโยบาย เพื่อให้สามารถจัดการความเสี่ยงได้อย่างมีประสิทธิภาพและประสิทธิผล

### แนวปฏิบัติที่ 1

การควบคุมภายในควรบูรณาการร่วมกับการประเมินความเสี่ยง รัฐวิสาหกิจควรเลือกและพัฒนากิจกรรมการควบคุม โดยพิจารณาจากความคุ้มค่าและความเป็นไปได้ของกิจกรรมการควบคุมที่มีประสิทธิผล เพื่อลดความเสี่ยงต่อการบรรลุวัตถุประสงค์ของการควบคุมภายในให้อยู่ในระดับความเสี่ยงที่องค์กรยอมรับได้ (RA)

### คู่มือปฏิบัติ

1. กิจกรรมการควบคุมมีอยู่ในทุกหน้าที่และทุกระดับของการปฏิบัติงาน ผู้บริหารจะต้องพิจารณาว่ากระบวนการใดที่ต้องการให้มีกิจกรรมการควบคุม และควรจัดให้มีกิจกรรมการควบคุมอย่างเหมาะสม และเพียงพอกับระดับความเสี่ยงที่จะก่อให้เกิดความเสียหาย

**ประเภทของการควบคุม** สามารถจัดกลุ่มได้หลายประเภท ดังนี้

- การควบคุมแบบป้องกัน (Preventive Control) เป็นการควบคุมเพื่อป้องกันหรือลดความเสี่ยงจากความผิดพลาด ความเสียหาย เช่น การแบ่งแยกหน้าที่การทำงาน การควบคุมการเข้าถึงทรัพย์สิน
- การควบคุมแบบค้นหา (Detective Control) เป็นการควบคุมเพื่อค้นพบความเสียหายหรือความผิดพลาดที่เกิดขึ้นแล้ว เช่น การสอบทานงาน การสอบการยกยอก การตรวจนับพัสดุ
- การควบคุมแบบแก้ไข (Corrective Control) เป็นวิธีการควบคุมที่กำหนดขึ้นเพื่อแก้ไขข้อผิดพลาดที่เกิดขึ้นให้ถูกต้อง หรือเพื่อหาวิธีแก้ไขไม่ให้เกิดข้อผิดพลาดซ้ำอีกในอนาคต เช่น การมีแผนรองรับเหตุสุดวิสัย (Disaster Recovery Plan) การมีสถานที่ประมวลผลและระบบคอมพิวเตอร์สำรอง
- การควบคุมแบบส่งเสริม (Directive Control) เป็นวิธีการควบคุมที่ส่งเสริมหรือกระตุ้นให้เกิดความสำเร็จตามวัตถุประสงค์ที่ต้องการ เช่น การให้รางวัลแก่ผู้มีผลงานดี

อย่างไรก็ตาม การควบคุมในทุกประเภทข้างต้นก็เพื่อวัตถุประสงค์เดียวกัน คือ เพื่อให้การดำเนินงานมีประสิทธิภาพ สามารถบรรลุวัตถุประสงค์ขององค์กรได้

กิจกรรมการควบคุมภายในเบื้องต้นจะต้องแบ่งแยกหน้าที่งานอย่างเหมาะสม ไม่มอบหมายให้บุคคลใดบุคคลหนึ่งมีหน้าที่เป็นผู้รับผิดชอบปฏิบัติงานที่สำคัญหรืองานที่เสี่ยงต่อความเสียหายตั้งแต่ต้นจนจบ

แต่ถ้ามีความจำเป็น ให้กำหนดกิจกรรมการควบคุมอื่นที่เหมาะสมทดแทน เช่น จัดให้มีการสอบทานงาน และ/หรืออนุมัติโดยหัวหน้างาน

ทั้งนี้ รัฐวิสาหกิจสามารถพิจารณาเลือกและพัฒนากิจกรรมการควบคุมภายในโดยพิจารณา จากตัวอย่างของกิจกรรมการควบคุมภายใน ดังนี้

### 1) การแบ่งแยกหน้าที่

การแบ่งแยกหน้าที่ เป็นขั้นตอนการแบ่งงานระหว่างบุคคลหรือหน่วยงานต่างๆ แทนที่จะให้บุคคล เดียวดำเนินการทั้งหมด เพื่อช่วยตรวจสอบและถ่วงดุลกัน ลดโอกาสผิดพลาดหรือทุจริต ตัวอย่าง ลักษณะงานที่จำเป็นต้องแบ่งแยกกันทำ ได้แก่

- การอนุมัติรายงาน การจัดบันทึกรายการ และการรับ จ่าย เก็บรักษาทรัพย์สินที่อนุมัติและบันทึก
- การรับ จ่าย เก็บรักษาเงิน การลงบัญชีเงินสด และการติดต่อธนาคาร

### 2) การอนุมัติและการให้ความเห็นชอบ

การอนุมัติคือการกำหนดขอบเขตระดับของอำนาจในการอนุมัติให้ชัดเจนเป็นลายลักษณ์อักษร ของพนักงานทุกระดับและมีการสื่อสารให้พนักงานภายในองค์กรรับทราบ ผู้ที่ได้รับมอบหมาย อำนาจหน้าที่ให้เป็นผู้อนุมัติควรสอบถามความเพียงพอของเอกสารประกอบการขออนุมัติ ว่าถูกต้อง เหมาะสมและเป็นไปตามกฎ ระเบียบ นโยบาย และแนวทางการปฏิบัติงานที่เกี่ยวข้อง และมีวงเงินที่อนุมัติอยู่ภายใต้ขอบเขตอำนาจที่ตนสามารถอนุมัติได้ รวมทั้งควรสอบถามรายการ ผิดปกติจากผู้ที่เกี่ยวข้องก่อนลงนามอนุมัติ และไม่ควรลงนามอนุมัติในแบบฟอร์มเปล่า หรือแบบฟอร์มที่ไม่มีข้อมูลรายการที่ขออนุมัติอย่างเพียงพอ เช่น การอนุมัติรายการก่อนที่จะบันทึก รายการนั้นลงในบัญชี ทะเบียน หรือแฟ้มหลักฐานอื่นใดขององค์กร การสอบยันความถูกต้อง ของข้อมูลก่อนการบันทึก การใช้เทคโนโลยีที่เหมาะสมช่วยในการประมวลผลข้อมูล รวมถึงการใช้ บุคลากรที่มีความรู้ประสบการณ์ทางวิชาชีพที่เกี่ยวข้องกับการประมวลผลข้อมูล

### 3) การสอบทานความถูกต้อง

- การสอบทานโดยผู้บริหารสูงสุด หมายถึง กิจกรรมการควบคุมที่ผู้บริหารสูงสุดเป็นผู้ใช้ การสอบทานในที่นี้ หมายถึง การใช้วิธีวิเคราะห์เปรียบเทียบระหว่างผลการปฏิบัติงานจริง กับแผนงาน งบประมาณ หรือประมาณการ ซึ่งได้จัดทำหรือกำหนดขึ้นไว้เป็นการล่วงหน้า ผลการสอบทานจะทำให้ผู้บริหารสูงสุดเห็นภาพรวมว่าการดำเนินงานมีปัญหาใหญ่ๆ ด้านใดบ้าง ช่วยให้สามารถวิเคราะห์หาสาเหตุซึ่งนำไปสู่การพิจารณาแนวทางแก้ไขปัญหานั้น ที่จำเป็น
- การสอบทานโดยผู้บริหารระดับกลาง หมายถึง ผู้บริหารที่มีหน้าที่รับผิดชอบงานด้านใด ด้านหนึ่งภายในองค์กร เช่น การจัดหา การเงิน การบัญชี เป็นต้น ผู้บริหารระดับกลาง ควรสอบทาน รายงานผลการปฏิบัติงานของเจ้าหน้าที่ผู้ปฏิบัติงานด้านต่างๆ ในหน่วยงาน

ที่ตนรับผิดชอบ การสอบทานอาจจะทำกับข้อมูลเป้าหมายที่จัดทำขึ้นตามแผนงาน หรือนโยบายของรัฐวิสาหกิจ นอกจากนี้ ผู้บริหารระดับกลางยังจำเป็นต้องสอบทานวิธีการปฏิบัติจริงกับระเบียบปฏิบัติ ตัวเลขสถิติผลการปฏิบัติงานในอดีต และเป้าหมายของหน่วยงานอีกด้วย

- การสอบทานงาน การสอบทานรายงานทางการเงินและรายงานผลการดำเนินงานที่มีใช้การเงินและการสอบทานกิจกรรมการปฏิบัติงาน ได้แก่ การสอบทานการกระทำที่เป็นไปตามกฎระเบียบ ข้อบังคับขององค์กร รวมถึงกรณีความขัดแย้งทางผลประโยชน์ โดยเป็นการสอบทานจากผู้บริหารแต่ละระดับขององค์กร การสอบทานเป็นกิจกรรมการควบคุมที่สำคัญที่ควรกระทำอย่างต่อเนื่องและสม่ำเสมอ และควรบันทึกผลการสอบทานที่ผู้บริหารจำเป็นต้องแก้ไข ติดตามเป็นลายลักษณ์อักษร

4) การควบคุมทางกายภาพ

การดูแลป้องกันทรัพย์สิน พิจารณาจากการที่องค์กรดูแล รักษา ป้องกันทรัพย์สินที่มีความเสี่ยงสูง เช่น เงินสด ทรัพย์สินที่มีค่า เอกสารหลักฐานและระบบงานที่สำคัญ และข้อมูลสารสนเทศขององค์กร โดยจำกัดการเข้าถึงทรัพย์สินที่มีความเสี่ยงสูง การดูแลรักษาทรัพย์สินอย่างรัดกุม และเพียงพอ การจัดเวรยามรักษาการณ์ การประกันภัย เป็นต้น รวมทั้งพิจารณาการระงับยอดจากการเปรียบเทียบรายการบัญชีทรัพย์สินกับทรัพย์สินที่มีอยู่จริง การเปรียบเทียบรายการในบัญชีกับทะเบียนคุม เป็นต้น

5) การควบคุมข้อมูลหลัก

เป็นการทำให้ข้อมูลสำคัญขององค์กรเป็นปัจจุบัน มีความถูกต้องและครบถ้วน เช่น เมื่อถึงรอบการเลื่อนเงินเดือนประจำปี ภายหลังจากการอนุมัติการเลื่อนเงินเดือนโดยผู้มีอำนาจฝ่ายทรัพยากรบุคคลต้องดำเนินการปรับข้อมูลเงินเดือนใหม่ในระบบให้ทันเวลา เพื่อให้มั่นใจว่าข้อมูลเงินเดือนของพนักงานเป็นปัจจุบันและถูกต้องก่อนที่จะมีการจ่ายเงินเดือนในรอบถัดไป

6) การระงับยอด

การเปรียบเทียบระหว่างข้อมูล 2 ข้อมูลหรือมากกว่า และกรณีที่พบความแตกต่างจะต้องดำเนินการปรับปรุงให้ข้อมูลตรงกัน เพื่อให้มั่นใจเรื่องความครบถ้วนและถูกต้องของรายการ เช่น การระงับยอดรายการเงินสดประจำวันกับยอดสุทธิที่รายงานจากระบบ

7) การกำหนดดัชนีชี้วัดผลการดำเนินงาน (KPI)

ดัชนีชี้วัดผลการดำเนินงาน (KPI) ที่นิยมใช้เป็นเครื่องมือวัดผลการดำเนินงานมักอยู่ในรูปแบบอัตราส่วนต่างๆ ที่แสดงความสัมพันธ์ระหว่างข้อมูลทางการเงิน หรือการดำเนินงานอย่างหนึ่ง กับข้อมูลอีกอย่างหนึ่ง การติดตามวิเคราะห์ความเคลื่อนไหวของอัตราส่วน หรือแนวโน้มของความเปลี่ยนแปลงค่าอัตราส่วนที่คำนวณขึ้น โดยอัตราส่วนที่ผิดปกติ หรือแนวโน้มที่น่าสังเกต

เป็นดัชนีบ่งชี้ให้ต้องติดตามหรือให้ความสนใจในเรื่องใดเรื่องหนึ่งเป็นพิเศษเพื่อตัดสินใจสั่งการแก้ไข ปัญหาทั้งด้านการดำเนินงานและด้านการจัดทำรายงานทางการเงิน

8) การจัดทำเอกสารอ้างอิง

การทำเอกสารอ้างอิงควรมีการจัดทำหลักฐานเป็นเอกสารหรือหนังสือ สำหรับระบบงานที่มีความสำคัญ เพื่อให้บุคลากรที่มีหน้าที่เกี่ยวข้องได้ทราบ เข้าใจและสามารถค้นคว้า อ้างอิงได้ รวมทั้งสามารถใช้ในการตรวจสอบ สอบทานความถูกต้อง พิจารณานอมนุมัติอย่างชัดเจน เช่น ระเบียบ คำสั่ง คู่มือการปฏิบัติงาน ผังกระบวนการ (Flowchart)

9) กิจกรรมการควบคุมภายในแบบอัตโนมัติ (Automated Control)

เป็นการนำเทคโนโลยีมาใช้ในการปฏิบัติงานเพื่อให้กิจกรรมการควบคุมดำเนินเป็นไปโดยอัตโนมัติ เช่น ระบบสามารถสอบทานมูลค่าการสั่งซื้อกับงบประมาณที่ได้รับอนุมัติที่บันทึกไว้ในระบบได้อย่างอัตโนมัติ กรณีมีการบันทึกใบสั่งซื้อที่มีมูลค่ารวมเกินกว่างบประมาณ ระบบจะไม่อนุญาตให้ทำการการดังกล่าว

10) การสอบทานกิจกรรมการควบคุม

เป็นการประเมินว่ากิจกรรมการควบคุมรายการอื่นๆ ตามที่กล่าวมาได้ถูกนำไปปฏิบัติโดยสมบูรณ์อย่างถูกต้องและสอดคล้องตามนโยบายและวิธีปฏิบัติที่กำหนด เช่น ผู้บังคับบัญชาดำเนินการสอบทานว่าพนักงานได้ทำการกระทบยอดบัญชี (Account Reconciliation) เมื่อถึงรอบปิดบัญชีตามที่กำหนดนโยบายแล้วจริงหรือไม่

2. รัฐวิสาหกิจควรกำหนดความถี่ในการปฏิบัติตามกิจกรรมการควบคุม ซึ่งความถี่ในการปฏิบัติขึ้นกับระดับความเสี่ยงที่ประเมินได้ เช่น หากความเสี่ยงที่ประเมินได้อยู่ในระดับสูง การกำหนดความถี่ในการปฏิบัติตามกิจกรรมการควบคุมอาจกำหนดให้เป็นเดือนละ 1 ครั้ง ในขณะที่ หากความเสี่ยงที่ประเมินได้อยู่ในระดับต่ำ ความถี่ในการปฏิบัติตามกิจกรรมการควบคุมอาจกำหนดให้มีเพียงปีละ 1 ครั้งเท่านั้น
3. รัฐวิสาหกิจควรทบทวน และปรับปรุงกิจกรรมการควบคุมให้เป็นปัจจุบัน สอดคล้องกับวัตถุประสงค์และเป้าหมายขององค์กรอย่างสม่ำเสมอ

## แนวปฏิบัติที่ 2

รัฐวิสาหกิจควรกำหนดให้เทคโนโลยีสารสนเทศได้รับการออกแบบและนำไปใช้เพื่อสนับสนุนให้บรรลุวัตถุประสงค์ของการควบคุมภายใน

### คู่มือปฏิบัติ

1. รัฐวิสาหกิจควรออกแบบและนำเทคโนโลยีสารสนเทศไปใช้ โดยคำนึงถึงการควบคุมทั่วไป และการควบคุมเฉพาะระบบงาน เพื่อให้ข้อมูลที่ผ่านการประมวลผลทั้งในรูปของสารสนเทศ หรือรายงานมีความถูกต้อง ครบถ้วน ทันเวลา และมีเนื้อหาที่เป็นประโยชน์ต่อการตัดสินใจ

- 1) การควบคุมทั่วไป (General Control) หมายถึง การควบคุมในส่วนที่เกี่ยวข้องกับสภาพแวดล้อม การควบคุม นโยบายและวิธีการในการควบคุมระบบสารสนเทศ การควบคุมความปลอดภัย การควบคุมการพัฒนาและปรับปรุง และการป้องกัน/ลดความเสียหายของระบบ เป็นการควบคุมภายในสำหรับองค์การในภาพรวมหรือควรมีในทุกๆ ส่วนของระบบสารสนเทศ

#### ตัวอย่างของการควบคุมทั่วไป

- การกำหนดนโยบายในการใช้งานสารสนเทศ โดยอ้างอิงตัวอย่างนโยบายการควบคุมการใช้งานสารสนเทศ ในองค์ประกอบที่ 4 แนวปฏิบัติที่ 1 ซึ่งรัฐวิสาหกิจควรจัดให้มีการจัดทำนโยบายการควบคุมการใช้งานสารสนเทศ และจะต้องได้รับการอนุมัติจากผู้บริหารระดับสูง และมีการเผยแพร่ให้ทุกคนในองค์กรรับทราบ นอกจากนี้ ควรมีการกำหนดบทลงโทษในกรณีที่ไม่ปฏิบัติตามหรือเพิกเฉยต่อการปฏิบัติ
- การแบ่งแยกหน้าที่งานในระบบสารสนเทศ ควรแบ่งแยกการทำงานในหน้าที่ต่อไปนี้ออกจากกันอย่างชัดเจน ได้แก่ การบริหารงานทั่วไป การควบคุมความปลอดภัยของระบบคอมพิวเตอร์ การพัฒนาและเปลี่ยนแปลงระบบงาน/โปรแกรม การปฏิบัติการและการบริหารระบบสื่อสาร และเครือข่าย
- การควบคุมโครงการพัฒนาระบบสารสนเทศ
- การควบคุมการเปลี่ยนแปลงแก้ไขระบบ
- การควบคุมการปฏิบัติงานในศูนย์คอมพิวเตอร์
- การควบคุมการเข้าถึงอุปกรณ์คอมพิวเตอร์
- การควบคุมการเข้าถึงข้อมูล ระบบปฏิบัติการ (ซอฟต์แวร์ของระบบ) เครือข่าย และระบบงาน (Application)

2) การควบคุมเฉพาะระบบงาน (Application Control) เป็นการควบคุมที่กำหนดขึ้น เพื่อให้มั่นใจว่าข้อมูลที่น่าเข้าสู่การประมวลผลของระบบงาน การประมวลผลข้อมูล และผลลัพธ์ที่ได้จากการประมวลผลมีความครบถ้วน สมบูรณ์ ถูกต้อง ได้รับการอนุมัติ และเกิดขึ้นอย่างถูกต้อง ตามกฎหมาย ระเบียบและนโยบายที่กำหนด

#### ตัวอย่างของการควบคุมเฉพาะระบบงาน

- การควบคุมการเข้าถึงฟังก์ชันภายในระบบงาน โดยในการออกแบบหรือการนำโปรแกรมสำเร็จรูปมาใช้ งาน สิ่งที่ต้องคำนึงถึง คือ ระบบต้องสามารถแบ่งแยกการทำงานโดยการกำหนดฟังก์ชันให้ผู้ใช้งานแต่ละคนได้ และหลักเกณฑ์ในการจัดฟังก์ชันควรจัดตามความจำเป็นในการใช้งาน
- การควบคุมด้าน Input เพื่อลดความเป็นไปได้ที่จะเกิดข้อผิดพลาดในการนำข้อมูลเข้าสู่ระบบสารสนเทศ ซึ่งการตรวจสอบและควบคุมความถูกต้องของ Input ที่ทำโดยโปรแกรมคอมพิวเตอร์ เช่น Double Entry/Format Control และ Duplication Controls
- การควบคุมการรับส่งข้อมูล เช่น วิธีแปลงรหัส (Encrypted and Decrypted)
- การควบคุมการประมวลผล เช่น Balance Controls ซึ่งสามารถควบคุมความถูกต้องทั้งของ Master Files และระบบฐานข้อมูล โดยในการควบคุมความถูกต้องของ Master Files นั้น โปรแกรมคอมพิวเตอร์จะทำการเช็คจำนวน Record ของ Master File แต่ละ File ก่อนการเปลี่ยนแปลงกับจำนวน Record หลังการเปลี่ยนแปลง แล้วนำไปเทียบกับจำนวนธุรกรรมที่เกิดขึ้นระหว่างวัน สำหรับการควบคุมความถูกต้องของระบบฐานข้อมูลนั้น โปรแกรมคอมพิวเตอร์จะทำการตรวจสอบยอดคงเหลือของระบบฐานข้อมูลใน File ที่สำคัญๆ โดยใช้ยอดยกมาก่อนการปรับปรุงรวมด้วยยอดธุรกรรม แล้วนำไปเปรียบเทียบกับยอดยกไป (Ending Balance) ถ้าไม่ตรงกันแสดงว่ามีข้อผิดพลาดเกิดขึ้น
- การควบคุมด้าน Output เพื่อลดโอกาสที่บุคคลที่ไม่ได้รับอนุญาตนำ Output ไปใช้ เช่น การตั้งค่าผู้ที่ต้องได้รับไปรษณีย์อิเล็กทรอนิกส์ (Email) ในระบบ เพื่อช่วยควบคุมให้รายงานต่างๆ ถูกส่งไปยังผู้ที่เกี่ยวข้องเท่านั้น

## แนวปฏิบัติที่ 3

รัฐวิสาหกิจควรกำหนดและสื่อสารนโยบายที่เกี่ยวข้องกับการควบคุมภายใน พร้อมด้วยขั้นตอนการปฏิบัติงานที่สอดคล้องกับนโยบายให้ทั่วทั้งองค์กร เพื่อให้บุคลากรในองค์กรปฏิบัติตามการสั่งการของฝ่ายบริหาร

### คู่มือปฏิบัติ

1. รัฐวิสาหกิจกำหนดนโยบายและแนวทางการปฏิบัติให้ครอบคลุมถึงกิจกรรมการควบคุมภายในแต่ละกระบวนการทางธุรกิจ และในกิจกรรมการปฏิบัติงานประจำวันของพนักงาน เช่น นโยบายกำหนดให้มีการสอบทานก่อนดำเนินการจัดซื้อจัดจ้างโดยหัวหน้างาน และกำหนดวิธีปฏิบัติโดยให้มีการสอบทานอย่างทันเวลา โดยนโยบายการทำงานที่ดีต้องมีหัวข้อดังต่อไปนี้

- วัตถุประสงค์ของนโยบาย
- ขอบเขตการใช้นโยบาย
- ผู้รับผิดชอบ
- อำนาจอนุมัติ
- แนวทางการปฏิบัติ
- ระบบงานหรือเอกสารที่เกี่ยวข้อง

สำหรับการกำหนดผู้รับผิดชอบ รัฐวิสาหกิจต้องมั่นใจว่าได้กำหนดบุคลากรที่มีความรู้ความสามารถและมีอำนาจเพียงพอให้รับผิดชอบการดำเนินการตามกิจกรรมการควบคุม นอกจากนี้ การจัดทำนโยบายที่ดีจะช่วยให้องค์กรมั่นใจว่านโยบายสามารถนำไปปฏิบัติงานได้จริง และก่อให้เกิดความโปร่งใสในการปฏิบัติงาน โดยควรพิจารณาถึงหลักการดังต่อไปนี้

- การตรวจสอบและถ่วงดุลอำนาจ (Checks and Balances)
- การทำรายการกับบุคคลที่เกี่ยวข้อง
- ความสอดคล้องกับกฎหมาย หลักเกณฑ์ และมาตรฐานอื่นที่เกี่ยวข้อง

2. รัฐวิสาหกิจควรสื่อสารนโยบายต่างๆ ที่กำหนดไว้อย่างชัดเจนไปยังบุคลากรและหน่วยงานที่เกี่ยวข้อง เพื่อให้บุคลากรทั้งหมดเข้าใจเนื้อหาของนโยบายและสามารถปฏิบัติตามได้อย่างถูกต้อง
3. รัฐวิสาหกิจกำหนดให้มีการทบทวนนโยบายอย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงอย่างมีนัยสำคัญ เพื่อให้แน่ใจว่านโยบายยังคงมีประสิทธิภาพและสอดคล้องกับบริบทขององค์กรในสถานการณ์ปัจจุบัน

### หลักเกณฑ์

รัฐวิสาหกิจต้องจัดให้มีสารสนเทศอย่างเพียงพอ เหมาะสม เชื่อถือได้ ซึ่งประกอบด้วยข้อมูลสารสนเทศที่เกี่ยวกับการดำเนินงานทั้งที่เป็นข้อมูลสารสนเทศจากแหล่งภายในและแหล่งภายนอก เพื่อสนับสนุนประสิทธิภาพและประสิทธิผลในการกำหนดกลยุทธ์ ประเมินความเสี่ยง และกิจกรรมการควบคุม

### แนวปฏิบัติที่ 1

รัฐวิสาหกิจควรวางแผนการดำเนินการด้านข้อมูลสารสนเทศและกำหนดให้มีระบบจัดการฐานข้อมูล รวมถึงกำหนดข้อมูลสารสนเทศที่จำเป็นต่อการตัดสินใจให้อยู่ในรูปแบบที่เข้าใจง่าย มีความถูกต้อง สมบูรณ์ เป็นปัจจุบัน ทันเวลา และสะดวกในการเข้าถึง

### คู่มือปฏิบัติ

1. รัฐวิสาหกิจควรจัดให้มีกระบวนการในการระบุสารสนเทศที่จำเป็น เพื่อสนับสนุนการดำเนินงานขององค์ประกอบการควบคุมภายในอื่นๆ และส่งเสริมให้องค์กรสามารถบรรลุวัตถุประสงค์ขององค์กรได้อย่างมีประสิทธิภาพ

**สารสนเทศ** หมายถึง ข้อมูลที่ได้ผ่านการประมวลผลและถูกจัดให้อยู่ในรูปแบบที่มีความหมาย และเป็นประโยชน์ต่อการใช้งาน โดยสารสนเทศประกอบไปด้วยสารสนเทศทางการเงิน (Financial Information) และสารสนเทศที่เกี่ยวกับการดำเนินงานที่ไม่ใช่การเงิน (Non-financial Information)

ข้อมูลสารสนเทศและระบบฐานข้อมูลที่ดี ควรมีลักษณะดังต่อไปนี้

- 1) มีความเหมาะสมกับการใช้งาน หมายถึง ข้อมูลสารสนเทศที่บรรจุเนื้อหาสาระที่จำเป็น สำหรับการตัดสินใจ
- 2) ความถูกต้องสมบูรณ์ หมายถึง ข้อมูลสารสนเทศที่สะท้อนผลตามความเป็นจริง และมีรายละเอียดที่จำเป็นครบถ้วน
- 3) ความเป็นปัจจุบัน หมายถึง ข้อมูลสารสนเทศที่ให้ตัวเลข และข้อเท็จจริงล่าสุด หรือใกล้เคียงวันที่ใช้ตัดสินใจมากที่สุด
- 4) ความทันเวลา หมายถึง จัดทำอย่างรวดเร็วเพื่อให้ผู้ตัดสินใจได้รับทันวันเวลาที่ต้องการใช้ข้อมูลข่าวสารนั้น
- 5) ความสะดวกในการเข้าถึง หมายถึง ความยากง่ายในการเข้าถึง ซึ่งควรง่ายสำหรับผู้ที่มิอำนาจหน้าที่เกี่ยวข้อง และมีระบบรักษาความปลอดภัยมิให้ผู้ที่ไม่มีความเกี่ยวข้องเข้าถึงข้อมูลสารสนเทศได้

การจัดทำข้อมูลสารสนเทศที่ดี สามารถทำได้โดยจัดหาบุคลากรที่มีความรู้ความสามารถ และประสบการณ์ทางวิชาชีพ รวมถึงต้องจัดให้มีเครื่องมือเครื่องใช้ เทคโนโลยี และระบบงานที่ดี ซึ่งประกอบด้วยระบบเอกสาร ระบบบัญชี และระบบการประมวลผลข้อมูลเพื่อการบริหารอื่นๆ

#### ตัวอย่างกระบวนการระบุสารสนเทศขององค์ประกอบการควบคุมภายใน

- ผู้บริหารทำแบบสำรวจความคิดเห็นพนักงานประจำปี เพื่อรวบรวมข้อมูลเกี่ยวกับความประพฤติส่วนบุคคลที่เกี่ยวข้องกับข้อพึงปฏิบัติขององค์กร โดยการทำแบบสำรวจเป็นส่วนหนึ่งของกระบวนการ ซึ่งให้ข้อมูลในการสนับสนุนสภาพแวดล้อมการควบคุม
  - องค์กรตัดสินใจขยายช่องทางการขายทางออนไลน์ เนื่องจากความต้องการของลูกค้าเปลี่ยนแปลงไป ทำให้การใช้บัตรเครดิตเพิ่มสูงอย่างมีนัยสำคัญ ดังนั้น เพื่อเป็นการประเมินความเสี่ยงเกี่ยวกับการไม่ปฏิบัติตามกฎระเบียบ ข้อบังคับที่เกี่ยวข้องกับการรักษาความปลอดภัยและความเป็นส่วนตัวของข้อมูลในบัตรเครดิต ผู้ปฏิบัติงานจึงรวบรวมสารสนเทศที่เกี่ยวข้องกับจำนวนรายการ มูลค่าโดยรวม และลักษณะของข้อมูลที่จัดเก็บในปีที่ผ่านมา จากนั้นนำข้อมูลดังกล่าวมาประเมินความสำคัญของความเสี่ยงในกระบวนการวิเคราะห์ความเสี่ยง
2. รัฐวิสาหกิจควรจัดให้มีนโยบายการควบคุมการใช้งานสารสนเทศที่เป็นลายลักษณ์อักษร และเผยแพร่ให้ทุกคนในรัฐวิสาหกิจทราบ โดยนโยบายดังกล่าวควรได้รับการอนุมัติจากผู้บริหารระดับสูง และการอนุมัติต้องรวมถึงการทบทวนนโยบายอย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงอย่างมีนัยสำคัญ
- ทั้งนี้ นโยบายการควบคุมการใช้งานสารสนเทศควรครอบคลุมในเรื่องดังต่อไปนี้
- นโยบายด้าน User ID และ Password
  - นโยบายเกี่ยวกับ Privilege ID
  - การกำหนดความสำคัญของข้อมูล
  - การควบคุมการเข้าถึงข้อมูล
  - การกำหนดเจ้าของระบบงาน
  - การกำหนดความรับผิดชอบของแต่ละหน่วยงาน
  - การเปลี่ยนแปลงระบบงาน
  - แผนป้องกันการหยุดชะงักของระบบงาน
  - การใช้คอมพิวเตอร์ส่วนบุคคล
  - การเข้ารหัส (Encryption)
  - การควบคุมฮาร์ดแวร์ ซอฟต์แวร์ และระบบเครือข่าย
  - การจัดเก็บและสำรองข้อมูล

3. รัฐวิสาหกิจควรจัดโครงสร้างภายในฝ่ายเทคโนโลยีสารสนเทศให้มีการแบ่งแยกหน้าที่งานอย่างชัดเจนสำหรับหน้าที่หลักต่อไปนี้
  - การบริหาร
  - การพัฒนาระบบงาน
  - การปฏิบัติการ
  - การควบคุมความปลอดภัย

## แนวปฏิบัติที่ 2

รัฐวิสาหกิจควรจัดให้มีการสื่อสารภายในองค์กร เพื่อช่วยสนับสนุนให้เกิดความเข้าใจ ตลอดจนมีการดำเนินการตามวัตถุประสงค์ของการควบคุมภายใน กระบวนการ และความรับผิดชอบรายบุคคลในทุกระดับขององค์กร

### คู่มือปฏิบัติ

1. รัฐวิสาหกิจควรจัดให้มีระบบการสื่อสารภายในองค์กรที่มีประสิทธิภาพ โดยการสื่อสาร หมายถึง การสื่อสารข้อมูลที่จัดทำไว้แล้ว ส่งไปถึงผู้ที่ควรได้รับ หรือมีไว้พร้อมสำหรับผู้ที่ควรใช้ข้อมูลสารสนเทศนั้น ณ ฐานข้อมูลองค์กร โดยประสิทธิภาพของการสื่อสารในที่นี้ หมายถึง การที่ผู้ได้รับข้อมูลสารสนเทศได้ใช้ข้อมูลดังกล่าวให้เกิดประโยชน์ในการตัดสินใจด้านต่างๆ ดังนี้
  - บุคลากรที่มีภาระหน้าที่ด้านต่างๆ ในองค์กรจะต้องได้รับข้อมูลสารสนเทศที่ใช้ในการดำเนินงานหรือการปฏิบัติงานในหน้าที่ของแต่ละคนอย่างครบถ้วน
  - ทุกคนในองค์กรต้องได้รับการสื่อความที่ชัดเจนจากผู้บริหารสูงสุดว่าบุคลากรทุกคนจะต้องให้ความสำคัญกับการปฏิบัติตามมาตรฐานการควบคุมภายในทุกมาตรการที่องค์กรจัดให้มีขึ้น การละเมิดถือเป็นความบกพร่อง หรืออาจได้รับการลงโทษ

**ตัวอย่างของข้อมูลสารสนเทศที่ควรสื่อสารให้บุคลากรได้รับทราบทั่วกัน ได้แก่**

- มาตรการการควบคุมภายในต่างๆ ที่ใช้อยู่ในองค์กร เช่น นโยบาย แผนงาน งบประมาณ หรือประมาณการ กฎ ระเบียบต่างๆ
- บทบาท อำนาจ หน้าที่ และความรับผิดชอบของบุคลากรแต่ละตำแหน่งหน้าที่ มาตรฐานผลงานที่ต้องการจากการปฏิบัติ
- รายงานผลการดำเนินงานตามนโยบาย แผนงาน และโครงการที่กำหนดขึ้น
- ความสัมพันธ์ของงานในหน้าที่ของบุคคล หรือหน่วยงานหนึ่งซึ่งเกี่ยวข้องกับบุคคลหรือหน่วยงานอื่น
- ข้อมูลสารสนเทศที่เป็นสัญญาณอันตราย หรือสัญญาณเตือนภัยถึงสิ่งขาดตกบกพร่องจากการปฏิบัติงานที่เกิดขึ้น หรืออาจเป็นเหตุให้เกิดความบกพร่องนั้นในอนาคตอันใกล้
- สิทธิประโยชน์ด้านต่างๆ ที่กำหนดไว้สำหรับบุคลากรแต่ละระดับ

## ตัวอย่างวิธีการสื่อสาร

- แผนแสดงหน้าจอข้อมูลชี้วัด (Dashboard)
- การตีตประกาศที่กระดานข่าวสาร
- ข้อความทางไปรษณีย์อิเล็กทรอนิกส์ (Email)
- การอบรม
- บันทึก (Memoranda)
- การสนทนาแบบตัวต่อตัว
- นโยบายหรือวิธีปฏิบัติ
- การนำเสนอ (Presentation)
- ระบบส่งข้อความทันที (Instant Messaging)
- การประกาศทางเว็บไซต์

รัฐวิสาหกิจควรเลือกวิธีการสื่อสาร โดยคำนึงถึงผู้รับการสื่อสาร ลักษณะการสื่อสาร ความทันเวลา ต้นทุน และข้อกำหนดด้านกฎหมาย นอกจากนี้ รัฐวิสาหกิจควรกำหนดให้มีช่องทางการสื่อสาร แยกต่างหาก โดยสามารถสื่อสารได้โดยไม่ระบุตัวตนหรือเป็นความลับ เช่น สายด่วนแจ้งเบาะแส และข้อร้องเรียน (Whistle- Blower Hotline)

ทั้งนี้ ระบบการสื่อสารภายในองค์กรควรได้รับการประเมินเพื่อทราบประสิทธิภาพ และประสิทธิผล ของระบบการสื่อสารเป็นระยะๆ อย่างสม่ำเสมอ เพื่อให้การสื่อสารเป็นส่วนหนึ่งของระบบการควบคุม ภายในที่ให้ประโยชน์สูงสุดอยู่เสมอ

2. รัฐวิสาหกิจควรกำหนดให้มีการรายงานข้อมูลที่สำคัญต่อคณะกรรมการอย่างสม่ำเสมอ และคณะกรรมการสามารถเข้าถึงแหล่งข้อมูลที่เป็นต่อการทำหน้าที่กำกับดูแลการควบคุมภายใน ทั้งนี้ การรายงานต้องครอบคลุมประเด็นสำคัญที่เกี่ยวข้องกับการปฏิบัติตามระบบการควบคุมภายใน ความถี่ในการรายงาน และการสื่อสารต้องเพียงพอและทันเวลาต่อการตัดสินใจ

## แนวปฏิบัติที่ 3

รัฐวิสาหกิจควรกำหนดให้ระบบสื่อสารเชื่อมโยงกัน (Integrated) ซึ่งสามารถให้สารสนเทศส่งถึงผู้ที่ควรได้รับหรือมีไว้พร้อมอย่างทันเวลา รัฐวิสาหกิจควรจัดให้มีการสื่อสารกับหน่วยงานภายนอกถึงผลกระทบต่อการบรรลุวัตถุประสงค์ของการควบคุมภายใน และควรมีช่องทางเพื่อเปิดรับข้อมูลจากผู้มีส่วนได้เสียภายนอก

### คู่มือปฏิบัติ

1. รัฐวิสาหกิจควรจัดให้มีระบบการสื่อสารภายนอกองค์กรที่มีประสิทธิผล โดยการสื่อสาร หมายถึง การสื่อสารข้อมูลที่จัดทำไว้แล้ว ส่งไปถึงผู้ที่ควรได้รับ หรือมีไว้พร้อมสำหรับผู้ที่ใช้ข้อมูลสารสนเทศนั้น ณ สถานที่ขององค์กร โดยประสิทธิผลของการสื่อสารในที่นี้ หมายถึง การที่ผู้ได้รับข้อมูลสารสนเทศได้ใช้ข้อมูลดังกล่าว ให้เกิดประโยชน์ในการตัดสินใจด้านต่างๆ โดยการเลือกวิธีการสื่อสารรูปแบบใด รัฐวิสาหกิจควรคำนึงถึงผู้รับข่าวสาร ความทันเวลา และข้อกำหนดด้านกฎหมายหรือข้อบังคับ ทั้งนี้ การสื่อสารกับแหล่งข้อมูลภายนอก ควรทำอย่างเป็นทางการเป็นระยะและสม่ำเสมอ หรืออาจทำเมื่อมีเหตุจำเป็นเป็นครั้งคราวก็ได้

นอกจากนี้ รัฐวิสาหกิจควรกำหนดให้มีช่องทางการรับสารจากผู้มีส่วนได้เสีย โดยองค์กรจัดให้มีช่องทางสำหรับลูกค้า ผู้ขาย ผู้ให้บริการที่จัดจ้างจากภายนอก เป็นต้น เพื่อให้สามารถสื่อสารกับผู้บริหารและบุคลากรที่เกี่ยวข้องได้โดยตรง

#### ตัวอย่างวิธีการสื่อสาร

- การติดต่อทางโทรศัพท์
- การใช้จดหมายหรือแบบสอบถาม
- การจัดประชุม
- การเปิดเผยข้อมูลขององค์กรที่ลูกค้าสามารถเข้าถึงได้ ผ่านทางช่องทางสำหรับลูกค้า (Customer Portal)
- การเผยแพร่ข่าวสารบนเว็บไซต์ขององค์กร
- การให้ข่าวผ่านช่องทางนักลงทุนสัมพันธ์ (กรณีเป็นรัฐวิสาหกิจที่จดทะเบียนในตลาดหลักทรัพย์แห่งประเทศไทย)

ทั้งนี้ ระบบการสื่อสารภายนอกองค์กรควรได้รับการประเมินเพื่อทราบประสิทธิภาพ และประสิทธิผลของระบบเป็นระยะและสม่ำเสมอ เพื่อให้การสื่อสารเป็นส่วนหนึ่งของระบบการควบคุมภายในที่ให้ประโยชน์สูงสุดอยู่เสมอ

## องค์ประกอบที่ 5 กิจกรรมติดตามผล (Monitoring)

### หลักเกณฑ์

รัฐวิสาหกิจควรกำหนดให้มีการติดตามและประเมินผลการควบคุมภายใน โดยมีขึ้นในระหว่างการปฏิบัติงาน และการประเมินผลเป็นรายครั้งอย่างต่อเนื่องและสม่ำเสมอ เพื่อให้คณะกรรมการและผู้บริหารระดับสูง มีความมั่นใจได้อย่างสมเหตุสมผลต่อประสิทธิภาพและประสิทธิผลของการควบคุมภายใน

### แนวปฏิบัติที่ 1

รัฐวิสาหกิจควรกำหนดให้มีการพัฒนาและประเมินผลอย่างต่อเนื่องและสม่ำเสมอ โดยประเมินผลแบบต่อเนื่องและแบบแยกต่างหาก เพื่อให้คณะกรรมการและผู้บริหารระดับสูงมั่นใจได้ว่าการควบคุมภายในยังคงทำหน้าที่ได้อย่างต่อเนื่อง โดยรัฐวิสาหกิจควรประเมินผลความเพียงพอและประสิทธิผลของการควบคุมภายใน และประเมินการบรรลุตามวัตถุประสงค์ขององค์กร ในลักษณะการประเมินการควบคุมด้วยตนเองและ/หรือการประเมินการควบคุมอย่างเป็นอิสระ อย่างน้อยปีละ 1 ครั้ง ทั้งนี้ รัฐวิสาหกิจควรจัดให้มีการประเมินการควบคุมภายในอย่างเป็นอิสระ โดยผู้ที่ไม่มีส่วนเกี่ยวข้องกับการออกแบบมาตรการหรือวางระบบการควบคุมภายใน เพื่อให้สามารถแสดงความคิดเห็นได้อย่างชัดเจนตรงไปตรงมา และมีความเหมาะสม

### คู่มือปฏิบัติ

1. การติดตามประเมินผลเป็นองค์ประกอบหนึ่งที่สำคัญของระบบการควบคุมภายใน โดยวัตถุประสงค์ที่สำคัญของการติดตามประเมินผลการควบคุมภายใน มีดังนี้
  - การควบคุมที่เพียงพอ (Adequate Control) เกิดขึ้นเมื่อฝ่ายบริหารได้มีการวางแผนและออกแบบการควบคุมในลักษณะที่สามารถสร้างความมั่นใจอย่างสมเหตุสมผลว่า องค์กรจะประสบความสำเร็จตามวัตถุประสงค์และเป้าหมายที่กำหนดไว้ได้อย่างมีประสิทธิภาพและโดยประหยัด
  - การควบคุมที่มีประสิทธิผล (Effective Control) เกิดขึ้นเมื่อฝ่ายบริหารได้สั่งการ และติดตามกำกับดูแลให้มีการปฏิบัติ เพื่อให้ระบบการควบคุมภายในได้ทำหน้าที่อย่างที่กำหนดและสร้างความมั่นใจอย่างสมเหตุสมผลว่าองค์กรจะประสบความสำเร็จตามวัตถุประสงค์และเป้าหมายที่กำหนดไว้

รัฐวิสาหกิจควรจัดให้มีการติดตามและประเมินผลการควบคุมภายในขององค์กร ซึ่งครอบคลุมบริษัทย่อยหรือบริษัทร่วม โดยกำหนดผู้รับผิดชอบในการติดตาม ความถี่ในการติดตาม เพื่อประเมินผลการควบคุมภายในของหน่วยงาน การมอบข้อสังเกต ข้อเสนอแนะ หรือมอบนโยบายอันเป็นประโยชน์ต่อระบบการควบคุมภายในขององค์กร โดยคณะกรรมการควรดูแลให้ฝ่ายบริหารมีการติดตามผลการควบคุมภายในและมีการทบทวนระบบการควบคุมภายในให้มีความเพียงพอและเหมาะสม กล่าวคือ

คณะกรรมการตรวจสอบสอบทานประสิทธิภาพและประสิทธิผลของกระบวนการควบคุมภายใน ผ่านการสอบทานรายงานจากหน่วยงานและบุคคลที่เกี่ยวข้อง

การติดตามและประเมินผลการควบคุมภายใน แบ่งได้ 2 ประเภทหลัก คือ

1) การประเมินผลแบบต่อเนื่องหรือการประเมินผลระหว่างการปฏิบัติงาน (Ongoing Monitoring)

หมายถึง การติดตามประเมินผลที่ได้กำหนดหรือออกแบบให้มีเทคนิควิธีการติดตามประเมินผล คุณภาพของงานแทรกแฝงไว้ เป็นส่วนหนึ่งของกิจกรรมหรือกระบวนการปฏิบัติงานจริงตามปกติ ประจำวันขององค์กร กระทำโดยฝ่ายบริหาร ผู้จัดการสายงาน และ/หรือ ผู้ที่ได้รับมอบหมาย เฝ้าสังเกต หรือสอบทานผลการปฏิบัติตามระบบการควบคุมที่กำหนดในทันทีขณะที่เกิดเหตุการณ์ ขึ้นจริงและตามลำดับขั้นอย่างต่อเนื่องและสม่ำเสมอ เช่น การวิเคราะห์ข้อมูลปฏิบัติงานที่เกิดขึ้น การวิเคราะห์ผลต่างระหว่างผลงานจริงกับแผนการวิเคราะห์เปรียบเทียบข้อมูลเพื่อหาความสัมพันธ์ ที่ผิดปกติ ความไม่สม่ำเสมอ

อนึ่ง ผู้ประเมินควรสังเกตความแตกต่างระหว่างกิจกรรมการติดตามประเมินผลต่อเนื่องกับกิจกรรม การควบคุมที่กระทำตามกระบวนการ ขั้นตอน วิธีปฏิบัติ หรือตามที่คุณมือปฏิบัติงานกำหนด เช่น การอนุมัติรายการ การจัดทำงบประมาณรายจ่ายประจำปี การตรวจสอบความถูกต้องของการปรับปรุง แพ้ข้อมูลหลักให้เป็นปัจจุบัน ซึ่งเป็นการกระทำตามกระบวนการประมวลผลทางบัญชี เป็นกิจกรรมการควบคุม แต่ไม่ใช่กิจกรรมการติดตามประเมินผลต่อเนื่อง

2) การประเมินผลแบบแยกต่างหากหรือการประเมินผลแบบเฉพาะคราว (Separate Evaluations)

หมายถึง กิจกรรมที่จัดขึ้นเป็นครั้งคราวตามช่วงเวลาที่กำหนดหรือตามความเหมาะสม หรือจัดขึ้น เป็นกรณีพิเศษเพื่อตอบสนองต่อวัตถุประสงค์เฉพาะ เช่น เพื่อจัดทำรายงานอย่างเป็นทางการ เกี่ยวกับการควบคุมภายใน รวมถึงอาจจัดขึ้นเมื่อมีความเสี่ยงที่เปลี่ยนแปลงไปจากเดิม ความเสี่ยงใหม่ หรือเหตุการณ์ที่ไม่ปกติ เช่น การทุจริต

การประเมินผลแบบเฉพาะคราว แตกต่างจากการติดตามประเมินผลแบบต่อเนื่อง เนื่องจาก การประเมินผลแบบเฉพาะคราวมีความมุ่งหมายเพื่อให้ทราบถึงประสิทธิผลของกิจกรรมใด กิจกรรมหนึ่งโดยตรงหรือประสิทธิผลของการควบคุมภายใน ณ เวลาใดเวลาหนึ่งที่กำหนด ในขณะที่การติดตามประเมินผลแบบต่อเนื่อง ครอบคลุมทุกกิจกรรมขององค์กรและต่อเนื่องตลอด ระยะเวลาของการปฏิบัติกิจกรรมนั้น

ทั้งนี้ รัฐวิสาหกิจสามารถพิจารณาเลือกประเมินการควบคุมภายในด้วยตนเองหรือจากหน่วยงาน ที่เป็นอิสระได้ดังต่อไปนี้

1) การประเมินการควบคุมภายในด้วยตนเอง (Control Self-Assessment: CSA) เป็นการประเมินผล

โดยกำหนดให้กลุ่มผู้ปฏิบัติงานของส่วนงานย่อยๆ ร่วมกันพิจารณาถึงความเพียงพอ

และมีประสิทธิผลของระบบการควบคุมภายใน และค้นหาความเสี่ยงของงานในความรับผิดชอบ เพื่อพิจารณาปรับปรุงกระบวนการและกิจกรรมการควบคุมที่มีอยู่ให้มีประสิทธิภาพ และประสิทธิผลมากยิ่งขึ้น นอกจากนี้ ควรดำเนินการพร้อมทั้งมีการบูรณาการกับการบริหาร ความเสี่ยงอย่างเป็นระบบ และมีการดำเนินงานตามข้อเสนอแนะ ความถี่ในการติดตาม และรายงานผลการดำเนินงาน และความสำเร็จในการดำเนินงานตามข้อเสนอแนะ/รายงาน แผนการปรับปรุงการควบคุมภายในทั้งในระดับองค์กรและหน่วยงานย่อย โดยมีวิธีปฏิบัติ ในการประเมินผลการควบคุมภายในด้วยตนเอง ดังนี้

- (1) ระบุผู้รับผิดชอบในการดำเนินการประเมินการควบคุมภายในด้วยตนเอง สำหรับแต่ละหน่วยงาน
- (2) กำหนดขอบเขตของการดำเนินการประเมินการควบคุมภายในด้วยตนเอง เช่น รายการของกระบวนการปฏิบัติงานที่จะทำการประเมิน
- (3) ระบุวัตถุประสงค์ของกระบวนการ ความเสี่ยงของกิจกรรมที่สำคัญ ระบุการควบคุมที่มีในปัจจุบันและที่ควรจะมีสำหรับความเสี่ยงที่สำคัญของกระบวนการ
- (4) จัดทำแบบสอบถามการควบคุมภายใน
- (5) ประเมินการควบคุมภายใน ระบุข้อบกพร่องของการควบคุมภายใน หรือความเสี่ยงที่การควบคุมยังไม่เพียงพอ และจัดทำแผนปรับปรุงการควบคุมสำหรับการควบคุมที่ยังไม่เพียงพอ
- (6) จัดการประชุมเชิงปฏิบัติการ CSA (CSA Workshop) เพื่อหาข้อสรุปผลการประเมินการควบคุมและแผนปรับปรุง โดยต้องคำนึงถึงต้นทุน และผลประโยชน์ที่ได้รับจากวิธีการแก้ไขนั้นด้วย
- (7) จัดทำรายงานผลการประเมินการควบคุมภายในตามรูปแบบที่กระทรวงการคลังกำหนด

2) การประเมินการควบคุมอย่างเป็นอิสระ (Independent Assessment) เป็นการประเมินผลที่กระทำโดยผู้ที่ไม่มีส่วนเกี่ยวข้องโดยตรงกับการปฏิบัติงานนั้นๆ เพื่อให้เกิดความมั่นใจว่า ผลการประเมินจะให้ข้อมูลสารสนเทศที่มีความถูกต้อง ครบถ้วน การประเมินผลอย่างอิสระ อาจกระทำโดยผู้ตรวจสอบภายในและผู้ตรวจสอบภายนอก โดยพิจารณาการจัดทำรายงานแล้วเสร็จตามแผนงานที่กำหนดและมีการประเมินการควบคุมอย่างเป็นอิสระครบถ้วนทั้งองค์กร และมีการติดตามข้อเสนอแนะ โดยขั้นตอนในการประเมินผลการควบคุมอย่างเป็นอิสระสามารถดำเนินการได้ ดังนี้

- (1) กำหนดวัตถุประสงค์และเป้าหมายที่ชัดเจนสำหรับการควบคุมนั้นๆ โดยฝ่ายบริหาร ซึ่งควรกำหนดให้ชัดเจนเพื่อให้ทุกคนเข้าใจหรือกำหนดเป็นระดับความเสี่ยงที่องค์กรยอมรับได้ (RA) หรือระดับความสำเร็จที่ต้องการ
- (2) เลือกเรื่องที่จะประเมิน เช่น การเลือกกว่าจะประเมินทั้งระบบ หรือจะประเมินเฉพาะวัตถุประสงค์หนึ่งของการควบคุมภายในที่เกี่ยวข้อง หรือจะประเมินเฉพาะองค์ประกอบด้านใด

ด้านหนึ่งก็ได้ ซึ่งวิธีการเลือกมาจาก 2 แหล่ง คือ เลือกตามคำสั่ง และเลือกตามความคิดริเริ่มของผู้ประเมิน ทั้งนี้ หากเป็นการเลือกตามความคิดริเริ่มของผู้ประเมินเอง วิธีการที่นิยมใช้ในการเลือก คือ การประเมินและจัดลำดับตามความเสี่ยงของเรื่อง

- (3) ศึกษาทำความเข้าใจโครงสร้างของระบบการควบคุมว่าประกอบด้วยองค์ประกอบการควบคุมภายในครบถ้วนทุกด้านหรือไม่ อย่างไร ซึ่งเทคนิคสำหรับผู้ประเมินที่ใช้ในการทำความเข้าใจโครงสร้างของระบบการควบคุม อาจจะใช้วิธีสอบถาม ประชุมปรึกษาหารือกับผู้บริหาร และการสอบทานเอกสารการควบคุมภายใน เช่น คู่มือการปฏิบัติงาน โครงสร้างองค์กร (Organization Chart) เอกสารกำหนดหน้าที่ความรับผิดชอบในงาน แผนงานงบประมาณ แผนภาพแสดงขั้นตอนการปฏิบัติงาน และเริ่มจัดทำเอกสารเกี่ยวกับการประเมินระบบการควบคุมภายใน เช่น การจัดทำแบบสอบถาม การทำแผนภาพ การทำกระดาษทำการ ประเมินผล องค์ประกอบการควบคุมภายใน เพื่อใช้เป็นหลักฐานขั้นต้นประกอบการประเมินผลต่อไป
- (4) ดำเนินการทดสอบการมีอยู่จริงและการปฏิบัติงานจริงของระบบการควบคุม ซึ่งเป็นการประเมินขั้นต้นว่าระบบการควบคุมนั้นมีอยู่จริง ใช้ปฏิบัติงานจริงหรือไม่ หากไม่มีหรือไม่ได้ใช้ปฏิบัติงานจริง องค์กรมีวิธีควบคุมอย่างอื่นชดเชยหรือไม่ โดยในขั้นตอนนี้ผู้ประเมินต้องหาหลักฐานเกี่ยวกับการปฏิบัติงานจริงในปัจจุบันว่ามีวิธีการอย่างไร ยังคงเหมือนหรือแตกต่างกับรูปแบบโครงสร้าง หรือองค์ประกอบการควบคุมที่กำหนดไว้หรือไม่ เพราะวิธีการควบคุมบางอย่างอาจจะเปลี่ยนแปลงไป เพื่อให้เหมาะสมกับสถานการณ์จริง หรือปฏิบัติตามบ้าง ไม่ปฏิบัติตามบ้าง หรือละเลยไม่ได้ปฏิบัติตามานแล้ว ซึ่งข้อมูลเหล่านี้ยังไม่ได้แก้ไขในเอกสารที่เกี่ยวข้อง และฝ่ายบริหารไม่ทราบการเปลี่ยนแปลงที่เกิดขึ้น

**การทดสอบการมีอยู่และการปฏิบัติงานจริง** ผู้ประเมินอาจใช้วิธีการ ดังต่อไปนี้

- สอบถามผู้ปฏิบัติงาน ผู้ควบคุมงาน และตรวจสอบเอกสารที่เกี่ยวข้อง
- สังเกตการณ์การปฏิบัติงานตามขั้นตอนตั้งแต่ต้นจนจบ (Walk Through)
- ออกเยี่ยมสถานที่ต่างๆ ที่มีความสำคัญต่อการดำเนินงาน เพื่อให้เห็นสภาพที่ทำงาน การจัดเก็บรักษาอุปกรณ์
- การทดสอบแบบจำกัด ซึ่งหมายถึง การสุ่มตัวอย่างแบบจำกัดจำนวน แล้วทดสอบกับปัจจัยต่างๆ ด้านที่เกี่ยวข้อง ไม่ว่าจะเป็นวัตถุประสงค์ที่ใช้ เอกสารที่เกี่ยวข้อง และผลลัพธ์ที่ได้จากการควบคุมนั้น เช่น การทดสอบแบบจำกัดเกี่ยวกับการควบคุมคลังสินค้า ซึ่งสิ่งที่ผู้ประเมินต้องการทราบ คือ จำนวนสินค้าที่รับตรงกับจำนวนใบสั่งซื้อ ใบกำกับสินค้า และใบรับสินค้าหรือไม่ ผู้ประเมินอาจหาคำตอบเบื้องต้นโดยการทดสอบแบบจำกัด ดังนี้

- ผู้ประเมินอาจใช้วิธีตรวจสอบแฟ้มเอกสารการสั่งซื้อ และรับสินค้าไว้ที่แผนกบัญชี เพื่อดูการจัดเก็บเอกสารใบสั่งซื้อแต่ละรายการว่าเรียงลำดับเลขที่ เอกสารการสั่งซื้อ แต่ละชุดมีเอกสารใบสั่งซื้อ ใบกำกับสินค้า และใบรับสินค้าแนบติดกันเป็นชุดอย่างครบถ้วนหรือไม่
- ผู้ประเมินอาจเลือกเอกสารการสั่งซื้อจำนวน 10 - 15 ชุด มาตรวจสอบความครบถ้วน ถูกต้องตรงกันของเอกสารทั้ง 3 ฉบับในแต่ละชุดนั้น

ทั้งนี้ ผู้ประเมินควรใช้วิธีการทดสอบหลายวิธีร่วมกัน เนื่องจากแต่ละวิธีมีข้อดีและข้อเสียแตกต่างกัน เช่น ผู้ประเมินได้จัดทำแบบสอบถามการควบคุมภายในแล้ว ได้รับคำตอบจากแบบสอบถามการควบคุมภายในที่ไม่แน่นอน ผู้ประเมินอาจเลือกคำถามนี้มาตรวจสอบกับเอกสารตลอดระบบ หรือไปสังเกตการณ์การปฏิบัติงานจริงเพื่อประเมินขั้นตอนการปฏิบัติงานจริงของคำถามนั้น

- (5) ประเมินประสิทธิผลของการควบคุมว่าได้ผลตามวัตถุประสงค์ที่กำหนดหรือไม่ ซึ่งเป็นการประเมินขั้นสุดท้ายโดยอาศัยหลักฐานที่รวบรวมได้จากการประเมินในขั้นต้น แล้วขยายผลการประเมิน โดยจะขยายผลการประเมินไปอย่างไรนั้น มีหลักในการพิจารณาว่าการขยายผลการประเมินนั้นจะให้ข้อมูล หรือหลักฐานที่มี 3 คุณลักษณะต่อไปนี้หรือไม่
- ตรงกับวัตถุประสงค์หรือความเสี่ยงที่จะประเมิน เช่น ความเชื่อถือได้ ความทันต่อเวลา
  - คุ่มค่า ไม่เสียเวลาและค่าใช้จ่ายในการประเมินมากเกินไป แต่จะให้ข้อมูลที่เพิ่มคุณค่า และประโยชน์ต่อองค์กร
  - ปฏิบัติได้ โดยผู้ประเมินมีความรู้ทักษะที่จะประเมิน หรือโดยอาศัยความรู้และทักษะจากผู้เชี่ยวชาญและที่ปรึกษา

ซึ่งการขยายผลการประเมิน อาจใช้วิธีดังนี้

- เพิ่มจำนวนการทดสอบการปฏิบัติตามระบบ
- การใช้วิธีสอบทานเชิงวิเคราะห์ (Data Analytics)
- การทดสอบสาระสำคัญ
- การทดสอบยอดคงเหลือ

- (6) สรุปผลการประเมินการควบคุมภายในตามรูปแบบที่กระทรวงการคลังกำหนด

แม้ว่าฝ่ายบริหารและฝ่ายตรวจสอบภายในมีหน้าที่รับผิดชอบโดยตรงในการจัดให้มีการติดตามประเมินผลการควบคุมภายในก็ตาม แต่พนักงานทุกระดับในองค์กร ควรมีหน้าที่ความรับผิดชอบร่วมกันในการจัดให้มีกิจกรรมติดตามประเมินผลการควบคุมภายในของส่วนงานที่ตนรับผิดชอบ โดยถือเป็นส่วนหนึ่งของกิจกรรมการบริหารและการปฏิบัติงานประจำวันขององค์กร เพื่อที่จะนำไปสู่การเปลี่ยนแปลงที่ดีขึ้นในองค์กร

## แนวปฏิบัติที่ 2

รัฐวิสาหกิจควรจัดให้มีการสื่อสารข้อบกพร่องที่ได้จากผลการประเมินการควบคุมภายใน ทั้งการประเมินการควบคุมด้วยตนเองและ/หรือการประเมินการควบคุมอย่างเป็นอิสระ และรายงานผลการประเมินไปยังคณะกรรมการ คณะกรรมการตรวจสอบ ผู้บริหาร ผู้กำกับดูแล กระทรวงเจ้าสังกัด หรือหน่วยงานอื่นที่เกี่ยวข้อง

### คู่มือปฏิบัติ

1. ภายหลังจากการประเมินการควบคุมภายใน รัฐวิสาหกิจควรนำส่งรายงานผลการประเมินการควบคุมภายในแก่คณะกรรมการ คณะกรรมการตรวจสอบ ผู้บริหาร ผู้กำกับดูแล กระทรวงเจ้าสังกัด หรือหน่วยงานอื่นที่เกี่ยวข้อง รวมถึงรัฐวิสาหกิจควรกำหนดให้มีการติดตามการปฏิบัติตามแผนปรับปรุงการควบคุม เพื่อตรวจสอบว่าข้อบกพร่องได้ถูกแก้ไขอย่างทันเวลาหรือไม่ และรายงานความคืบหน้าในการปรับปรุงข้อบกพร่องของการควบคุมภายในที่เป็นสาระสำคัญต่อคณะกรรมการ คณะกรรมการตรวจสอบ ผู้บริหาร ผู้กำกับดูแล กระทรวงเจ้าสังกัด หรือหน่วยงานอื่นที่เกี่ยวข้อง

นอกจากนี้ รัฐวิสาหกิจควรจัดให้มีกระบวนการติดตามและรายงานผลการประเมินการควบคุมภายในของบริษัทย่อยหรือบริษัทร่วมอย่างทันเวลาในกรณีที่เกิดเหตุการณ์ผิดปกติหรือมีข้อบ่งชี้ที่อาจเกี่ยวข้องกับการทุจริตขององค์กร โดยควรจัดให้มีการรายงานต่อคณะกรรมการและผู้บริหาร เพื่อรับทราบและพิจารณาแนวทางการแก้ไขปัญหาได้อย่างเหมาะสมและทันเวลา

# 5

## ภาคผนวก

	หน้า
ตัวอย่างชื่อความเสี่ยงและคำอธิบายความเสี่ยง	169
คำถาม – คำตอบที่นำรู้เกี่ยวกับการบริหารความเสี่ยงและการควบคุมภายใน	175
สรุปสาระสำคัญเกี่ยวกับการบริหารความเสี่ยงและการควบคุมภายใน (Infographics)	183
• สรุปการปรับปรุงที่สำคัญ	
• ปัจจัยสำคัญต่อความสำเร็จในการบริหารความเสี่ยงและการควบคุมภายใน	
• สรุปหลักเกณฑ์ แนวปฏิบัติ และคู่มือปฏิบัติเกี่ยวกับการบริหารความเสี่ยง และการควบคุมภายใน	
◦ การบริหารความเสี่ยง	
◦ การควบคุมภายใน	
• คำถาม – คำตอบที่นำรู้เกี่ยวกับการบริหารความเสี่ยงและการควบคุม ภายใน	



**ตัวอย่างชื่อความเสี่ยง  
และคำอธิบายความเสี่ยง**



## ตัวอย่างชื่อความเสี่ยงและคำอธิบายความเสี่ยง

ตารางต่อไปนี้แสดงตัวอย่างชื่อความเสี่ยงและคำอธิบายความเสี่ยง เพื่อให้ผู้บริหารและพนักงานเข้าใจไปในแนวทางเดียวกัน และช่วยลดปัญหาการตีความที่แตกต่างกัน

ลำดับ	ชื่อความเสี่ยง (Risk Category)	คำอธิบายความเสี่ยง (Definition/Description)
1	ความเสี่ยงด้านกลยุทธ์ (Strategy)	ความเสี่ยงที่เกิดจากการเปลี่ยนแปลงที่ไม่พึงประสงค์ทางด้านเศรษฐกิจมหภาค การเมือง สังคม และปัจจัยทางเทคโนโลยี รวมทั้งความไม่เหมาะสมทางด้านการวางแผนเชิงกลยุทธ์
2	ความเสี่ยงด้านทรัพยากรบุคคล (Human Resources)	ภัยคุกคามอันเกิดจากความไม่เพียงพอของพนักงานที่มีความสามารถที่เหมาะสมกับการดำเนินงานในองค์กร หรือการขาดการกระตุ้นให้พนักงานมีสำนึกในความรับผิดชอบหน้าที่ในกิจกรรมธุรกิจที่ดำเนินอยู่ ซึ่งรวมถึงเรื่องอื่นๆ ที่เกี่ยวข้อง กับองค์กร เช่น สุขภาพ ความปลอดภัย การประท้วง หรือข้อโต้แย้งต่างๆ ขององค์กร
3	ความเสี่ยงด้านจริยธรรม จรรยาบรรณ (Integrity and Ethical Values)	ความเสี่ยงที่ทำให้เกิดความสูญเสียจากเหตุการณ์ที่เกี่ยวข้องกับความซื่อสัตย์สุจริต จริยธรรม จรรยาบรรณ หรือการแบ่งแยกกันในองค์กร
4	ความเสี่ยงด้านกฎระเบียบ (Regulatory)	เหตุการณ์ที่นำไปสู่ความกีดกันทางด้านกฎระเบียบ การคว่ำบาตร หรือการโดนปรับค่าเสียหาย การเพิ่มขึ้นของกฎระเบียบ หรือความซับซ้อนของกฎระเบียบใหม่ๆ
5	ความเสี่ยงด้านตลาด (Market)	ความเสี่ยงที่ทำให้เกิดความเสียหาย อันเกิดมาจากการเปลี่ยนแปลงที่ไม่พึงประสงค์ทางด้านตลาดที่มีความเกี่ยวข้องกับอัตราดอกเบี้ย สินค้าอุปโภคบริโภค อัตราแลกเปลี่ยน หรือการลงทุนในตลาดหุ้น
6	ความเสี่ยงด้านเครดิต (Credit)	ความเสี่ยงที่เกิดจากลูกหนี้ไม่ชำระหนี้
7	ความเสี่ยงด้านสภาพคล่อง (Liquidity)	ความเสี่ยงที่เกิดจากการไม่สามารถปฏิบัติตามภาระผูกพันทางการเงินในปัจจุบัน เนื่องจากขาดการวางแผนในการเตรียมทุนสำรองทางการเงินให้เหมาะสมกับสถานการณ์

ลำดับ	ชื่อความเสี่ยง (Risk Category)	คำอธิบายความเสี่ยง (Definition/Description)
8	ความเสี่ยงด้านการรายงานทางการเงิน (Financial Reporting)	ความเสี่ยงที่เกิดจากการเปิดเผยรายงานทางการเงินที่มีความผิดพลาดอย่างมีนัยสำคัญ
9	ความเสี่ยงด้านการทุจริตจากภายในองค์กร (Internal Fraud)	ความเสี่ยงที่ทำให้เกิดความสูญเสียเงินลงทุนที่เกิดจากการตั้งใจฉ้อฉล โกง หลอกหลวงจากพนักงานภายในองค์กร โดยอาจมีหรือไม่มีผู้สมรู้ร่วมคิด ทั้งจากภายในและภายนอกองค์กร
10	ความเสี่ยงด้านการทุจริตจากภายนอกองค์กร (External Fraud and Security)	ความเสี่ยงที่ทำให้เกิดความสูญเสียเงินลงทุนที่เกิดจากการตั้งใจฉ้อฉล โกง หลอกหลวงจากบุคคลภายนอกองค์กร
11	ความเสี่ยงด้านสารสนเทศ (Information Technology)	ความเสี่ยงจากการขาดความต่อเนื่อง หรือการขัดขวางใดๆ ที่ทำให้องค์กรไม่สามารถดำเนินงานได้อย่างมีประสิทธิภาพ โดยอาจเกิดจากการขาดความเหมาะสมในการพัฒนา และลงวางระบบ รวมทั้งการสูญเสียเทคโนโลยีสารสนเทศแม้ในระยะสั้น
12	ความเสี่ยงด้านกฎหมาย (Legal)	ความสูญเสียที่เกิดจากการดำเนินการตามกฎหมาย หรือความล้มเหลวจากการบังคับใช้กฎหมายกับคู่กรณี
13	ความเสี่ยงด้านภาษี (Tax)	ความสูญเสียที่เกิดจากการเปลี่ยนแปลงที่ไม่พึงประสงค์ที่เกี่ยวข้องกับกฎหมายทางด้านภาษี หรือการนำกฎหมายทางด้านภาษีไปใช้ไม่ถูกต้อง หรือการฝ่าฝืนทางด้านกฎหมายที่เกี่ยวข้องกับภาษี
14	ความเสี่ยงด้านการทำธุรกรรม (Transaction Processing)	ความสูญเสียที่เกิดจากความผิดพลาดหรือการละเลยเพิกเฉยในการดำเนินการด้านธุรกรรม หรือเกิดจากการขาดความต่อเนื่อง
15	ความเสี่ยงด้านการขาดความต่อเนื่องในการดำเนินงาน (Business Disruption)	ความสูญเสียที่เกิดจากการขาดความต่อเนื่องในการดำเนินงาน ทำให้องค์กรไม่สามารถดำเนินงานได้ตามปกติในแต่ละกระบวนการ
16	ความเสี่ยงด้านความเสียหายของทรัพย์สิน (Damage to Physical Assets)	ความสูญเสียจากการเจตนา หรือไม่เจตนาที่ทำให้เกิดความเสียหาย ของทรัพย์สินที่นอกเหนือไปจากผลของความเสียหาย ที่เกิดจากการขาดความต่อเนื่องในการดำเนินงาน

ลำดับ	ชื่อความเสี่ยง (Risk Category)	คำอธิบายความเสี่ยง (Definition/Description)
17	ความเสี่ยงด้านลูกค้า สินค้า และการปฏิบัติทางธุรกิจ (Clients Products and Business Practices)	ความสูญเสียที่เกิดจากความไม่เหมาะสม หรือการปฏิบัติที่ผิดกฎหมายในเรื่องที่เกี่ยวข้องกับการพัฒนาและการตลาด สำหรับผลิตภัณฑ์ขององค์กร การติดต่อปฏิสัมพันธ์กับลูกค้า และการดำเนินธุรกิจโดยทั่วไป
18	ความเสี่ยงด้านสิ่งแวดล้อม สังคม และการกำกับดูแล (ESG)	ความสูญเสียที่เกิดจากปัจจัยด้านสิ่งแวดล้อม สังคม และการกำกับดูแล (ESG) ซึ่งอาจส่งผลให้เกิดความสูญเสียต่อองค์กรทั้งในด้านชื่อเสียง การเงิน กฎหมาย หรือความสามารถในการดำเนินธุรกิจระยะยาว



คำถาม – คำตอบที่นารู้เกี่ยวกับการบริหาร  
ความเสี่ยงและการควบคุมภายใน



## คำถาม – คำตอบที่นำสู่เกี่ยวกับการบริหารความเสี่ยง และการควบคุมภายใน

คำถาม	คำตอบ						
<p>1. เหตุการณ์หรือความเสี่ยงหนึ่งเรื่องสามารถมีดัชนีชี้วัดความเสี่ยงหลัก (KRI) ได้มากกว่า 1 ดัชนีหรือไม่ และเหตุการณ์หรือความเสี่ยงหลายเรื่องสามารถมี KRI ร่วมกันได้หรือไม่</p>	<p>ในการกำหนดดัชนีชี้วัดความเสี่ยงหลัก (KRI) เพื่อพิจารณาแนวโน้มของความเสี่ยงใดๆ ที่อาจจะเปลี่ยนแปลงไป สามารถกำหนดได้มากกว่า 1 ดัชนี เพื่อให้มั่นใจว่าสถานะความเสี่ยงได้เปลี่ยนแปลงไปอย่างมีนัยสำคัญ ซึ่งการกำหนดดัชนีชี้วัดความเสี่ยงหลัก (KRI) นี้ จะขึ้นอยู่กับจำนวนสาเหตุที่ทำให้เกิดความเสี่ยงนั้นๆ ดังตัวอย่างที่แสดงในตารางต่อไปนี้</p> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="background-color: #f8d7da;">เหตุการณ์ความเสี่ยง</th> <th style="background-color: #f8d7da;">ตัวอย่าง KRI</th> </tr> </thead> <tbody> <tr> <td>ความผันผวนของรายได้</td> <td> <ul style="list-style-type: none"> <li>• อัตราความพึงพอใจของลูกค้า</li> <li>• อัตราการร้องเรียนของลูกค้า</li> <li>• ความผันผวนของอัตราแลกเปลี่ยน</li> </ul> </td> </tr> <tr> <td>ขาดบุคลากรที่มีคุณภาพ</td> <td> <ul style="list-style-type: none"> <li>• อัตราการหมุนเวียนของพนักงาน</li> <li>• จำนวนชั่วโมงในการฝึกอบรม</li> <li>• จำนวนตำแหน่งว่างเฉลี่ยต่อเดือนที่ใช้เวลาเกินมาตรฐานในการสรรหา</li> </ul> </td> </tr> </tbody> </table> <p>อย่างไรก็ตาม รัฐวิสาหกิจควรคำนึงถึงต้นทุนที่จะเกิดขึ้นในการกำหนดดัชนีชี้วัดความเสี่ยงหลัก (KRI) เพื่อติดตามแนวโน้มของความเสี่ยง เนื่องจากจะต้องมีการกำหนดผู้รับผิดชอบเพื่อเก็บข้อมูลและเฝ้าติดตามแนวโน้มของความเสี่ยง โดยความถี่ในการติดตามอาจจะเริ่มจากทุกวัน ทุกสัปดาห์ หรือทุกเดือนขึ้นอยู่กับลักษณะของข้อมูลที่ต้องการ ซึ่งอาจจะทำให้ต้นทุนในการติดตามสูงเกินความจำเป็น อย่างไรก็ตาม เพื่อเป็นการประหยัดต้นทุนในการเก็บข้อมูลสำหรับเฝ้าดูแนวโน้มของความเสี่ยงหนึ่งๆ รัฐวิสาหกิจอาจกำหนดดัชนีชี้วัดความเสี่ยงหลัก 1 ดัชนี สำหรับเฝ้าระวังเหตุการณ์หรือความเสี่ยงมากกว่า 1 เรื่องได้</p>	เหตุการณ์ความเสี่ยง	ตัวอย่าง KRI	ความผันผวนของรายได้	<ul style="list-style-type: none"> <li>• อัตราความพึงพอใจของลูกค้า</li> <li>• อัตราการร้องเรียนของลูกค้า</li> <li>• ความผันผวนของอัตราแลกเปลี่ยน</li> </ul>	ขาดบุคลากรที่มีคุณภาพ	<ul style="list-style-type: none"> <li>• อัตราการหมุนเวียนของพนักงาน</li> <li>• จำนวนชั่วโมงในการฝึกอบรม</li> <li>• จำนวนตำแหน่งว่างเฉลี่ยต่อเดือนที่ใช้เวลาเกินมาตรฐานในการสรรหา</li> </ul>
เหตุการณ์ความเสี่ยง	ตัวอย่าง KRI						
ความผันผวนของรายได้	<ul style="list-style-type: none"> <li>• อัตราความพึงพอใจของลูกค้า</li> <li>• อัตราการร้องเรียนของลูกค้า</li> <li>• ความผันผวนของอัตราแลกเปลี่ยน</li> </ul>						
ขาดบุคลากรที่มีคุณภาพ	<ul style="list-style-type: none"> <li>• อัตราการหมุนเวียนของพนักงาน</li> <li>• จำนวนชั่วโมงในการฝึกอบรม</li> <li>• จำนวนตำแหน่งว่างเฉลี่ยต่อเดือนที่ใช้เวลาเกินมาตรฐานในการสรรหา</li> </ul>						
<p>2. บทบาทของผู้ตรวจสอบภายในด้านการสอบทานกระบวนการบริหารความเสี่ยงควรเป็นอย่างไร</p>	<p>บทบาทและความรับผิดชอบของผู้ตรวจสอบภายในด้านการสอบทานกระบวนการบริหารความเสี่ยง สามารถแบ่งได้เป็น 3 ลักษณะ ได้แก่</p> <ol style="list-style-type: none"> <li>1. <b>บทบาทและความรับผิดชอบหลักของหน่วยงานตรวจสอบภายใน</b> ต่อการบริหารความเสี่ยงที่ผู้ตรวจสอบภายในจะต้องทำให้เกิดความมั่นใจว่าระบบบริหารความเสี่ยงมีประสิทธิภาพและประสิทธิผล โดยมีบทบาท</li> </ol>						

คำถาม	คำตอบ
	<p>และความรับผิดชอบหลัก ดังนี้</p> <ul style="list-style-type: none"> <li>• ดำเนินการให้มั่นใจว่ากรอบการบริหารความเสี่ยงมีประสิทธิภาพทั้งในด้านการออกแบบและการนำไปใช้</li> <li>• ดำเนินการให้มั่นใจว่าการประเมินความเสี่ยงมีความน่าเชื่อถือและการบริหารความเสี่ยงเป็นไปตามกรอบและนโยบายที่กำหนดไว้</li> <li>• ดำเนินการให้มั่นใจว่าการประเมินความเสี่ยงได้บรรลุตามวัตถุประสงค์ที่กำหนดไว้อย่างมีประสิทธิภาพ</li> </ul> <p><b>2. บทบาทและความรับผิดชอบที่หน่วยงานตรวจสอบภายในสามารถดำเนินการภายใต้ข้อจำกัด</b></p> <p>บทบาท และความรับผิดชอบที่หน่วยงานตรวจสอบภายในสามารถเข้าไปร่วมดำเนินการได้มีหลายรูปแบบ อย่างไรก็ตาม ต้องมีการพิจารณาถึงความเหมาะสมและต้องเป็นไปตามกฎ ระเบียบ และข้อบังคับทั้งภายในและภายนอกองค์กร ตัวอย่างบทบาทดังกล่าว มีดังนี้</p> <ul style="list-style-type: none"> <li>• เป็นผู้อำนวยความสะดวก (Facilitator) ในการประชุมเชิงปฏิบัติการ และกำหนดแนวทางในการตอบสนองต่อความเสี่ยง</li> <li>• เป็นผู้ประสานงานในกระบวนการบริหารความเสี่ยง</li> <li>• ให้คำแนะนำแก่ผู้บริหารเกี่ยวกับวิธีการในการตอบสนองต่อความเสี่ยง</li> <li>• รวบรวมรายงานความเสี่ยง</li> </ul> <p><b>3. บทบาทและความรับผิดชอบที่ไม่ควรอยู่ภายใต้ความรับผิดชอบของหน่วยงานตรวจสอบภายใน</b></p> <p>บทบาท และความรับผิดชอบบางอย่างไม่ควรให้หน่วยงานตรวจสอบภายในเป็นผู้รับผิดชอบ โดยเฉพาะความรับผิดชอบในการบริหารความเสี่ยงโดยตรง เนื่องจากหน่วยงานตรวจสอบภายในต้องทำหน้าที่สอบทานประสิทธิภาพและประสิทธิผลของกระบวนการบริหารความเสี่ยงภายในองค์กร ตัวอย่างบทบาทที่หน่วยงานตรวจสอบภายในไม่ควรเข้าไปมีส่วนร่วม มีดังนี้</p> <ul style="list-style-type: none"> <li>• การกำหนดระดับความเสี่ยงที่องค์กรยอมรับได้ (RA)</li> <li>• การกำหนดกระบวนการบริหารความเสี่ยง</li> <li>• การตัดสินใจในการตอบสนองต่อความเสี่ยง</li> <li>• เป็นผู้ดำเนินการจัดการความเสี่ยงแทนผู้บริหาร</li> <li>• เป็นผู้รับผิดชอบในกระบวนการบริหารความเสี่ยง</li> </ul>

คำถาม	คำตอบ
<p>3. การประเมินผล การควบคุมภายใน และการตรวจสอบภายในแตกต่างกันอย่างไร</p>	<p><b>การประเมินผลการควบคุมภายใน</b> เป็นกระบวนการที่ดำเนินการ โดยหน่วยงานแนวป้องกันด้านที่ 1 หรือหน่วยงานแนวป้องกันด้านที่ 2 เพื่อทบทวนความเพียงพอและประสิทธิผลของระบบการควบคุมภายในว่ามีความเหมาะสมและสามารถจัดการความเสี่ยงได้อย่างมีประสิทธิภาพและทันต่อการเปลี่ยนแปลงหรือไม่</p> <p><b>การตรวจสอบภายใน</b> เป็นกระบวนการที่ดำเนินการโดยหน่วยงานแนวป้องกันด้านที่ 3 เพื่อให้ความเชื่อมั่นและให้คำปรึกษาอย่างเที่ยงธรรมและเป็นอิสระ ในการประเมินประสิทธิผลของกระบวนการบริหารความเสี่ยง การควบคุมภายใน และการกำกับดูแล ซึ่งขอบเขตของการตรวจสอบภายในจะกว้างกว่าการประเมินผลการควบคุมภายในที่มุ่งเน้นการประเมินประสิทธิภาพและประสิทธิผลของกิจกรรมการควบคุม</p>
<p>4. ความเสี่ยงด้านสิ่งแวดล้อม สังคม และการกำกับดูแล (ESG) เชื่อมโยงกับกระบวนการบริหารความเสี่ยงอย่างไร</p>	<p>การบริหารความเสี่ยงด้านสิ่งแวดล้อม สังคม และการกำกับดูแล (ESG) จะช่วยสร้างความยั่งยืนและเพิ่มมูลค่าให้กับรัฐวิสาหกิจ ทำให้เกิดความเชื่อมั่นจากผู้มีส่วนได้เสีย โดยรัฐวิสาหกิจสามารถใช้กรอบโครงสร้างการบริหารความเสี่ยงขององค์กร ในการบริหารความเสี่ยงดังกล่าวได้ตามปกติ</p> <p>โดยพิจารณาความเสี่ยงด้าน ESG เป็นความเสี่ยงหนึ่งขององค์กร ดังต่อไปนี้</p> <ol style="list-style-type: none"> <li>1) การกำกับดูแลและวัฒนธรรม เช่น เพิ่มความตระหนักของคณะกรรมการและผู้บริหารเกี่ยวกับความเสี่ยงด้านสิ่งแวดล้อม สังคม และการกำกับดูแล (ESG)</li> <li>2) กลยุทธ์และการกำหนดวัตถุประสงค์ เช่น การทำความเข้าใจบริบท กลยุทธ์ และวัตถุประสงค์ควรคำนึงถึงด้านสิ่งแวดล้อม สังคม และการกำกับดูแล (ESG) ด้วย</li> <li>3) ผลปฏิบัติการ เช่น นำความเสี่ยงด้านสิ่งแวดล้อม สังคม และการกำกับดูแล (ESG) มาพิจารณาในกระบวนการระบุ ประเมินความรุนแรง และตอบสนองต่อความเสี่ยง</li> <li>4) การสอบทานและการแก้ไขปรับปรุง เช่น ประเมินประสิทธิผลและปรับเปลี่ยนแนวทางการบริหารความเสี่ยงโดยคำนึงถึงด้านสิ่งแวดล้อม สังคม และการกำกับดูแล (ESG)</li> <li>5) สารสนเทศ การสื่อสาร และการรายงาน เช่น สื่อสารและรายงานสารสนเทศที่เกี่ยวข้องกับด้านสิ่งแวดล้อม สังคม และการกำกับดูแล (ESG) ไปยังหน่วยงานกำกับดูแลและผู้มีส่วนได้เสีย</li> </ol>

คำถาม	คำตอบ
<p>5. เทคโนโลยีที่นำมาใช้ในการบริหารความเสี่ยงควรมีลักษณะอย่างไรและจำเป็นต้องเป็นระบบสารสนเทศหรือไม่</p>	<p>เทคโนโลยีที่นำมาใช้ในการบริหารความเสี่ยงไม่จำเป็นต้องเป็นระบบสารสนเทศหรือซอฟต์แวร์เฉพาะทางเสมอไป แต่อย่างน้อยควรเป็นเทคโนโลยีที่สนับสนุนให้การบริหารความเสี่ยงดำเนินการอย่างเป็นระบบ และสามารถตรวจสอบได้ รวมถึงสามารถนำไปปฏิบัติจริงได้อย่างต่อเนื่อง โดยเทคโนโลยีควรมีลักษณะดังนี้</p> <ul style="list-style-type: none"> <li>• สนับสนุนการสื่อสารข้อมูลความเสี่ยงอย่างต่อเนื่องและทั่วถึงในทุกระดับขององค์กร</li> <li>• ช่วยรวบรวม วิเคราะห์ และแสดงข้อมูลความเสี่ยงได้อย่างเป็นระบบ เพื่อช่วยให้ผู้บริหารสามารถตัดสินใจบนพื้นฐานข้อมูลที่ถูกต้องได้</li> <li>• ส่งเสริมการติดตามความเสี่ยงอย่างต่อเนื่อง</li> </ul> <p>ทั้งนี้ เทคโนโลยีอาจอยู่ในรูปแบบที่เรียบง่าย เช่น ตารางติดตามความเสี่ยง (Risk Register) ใน Spreadsheet หรือแบบฟอร์มออนไลน์สำหรับพนักงานที่ต้องการแจ้งรายละเอียดเมื่อพบความเสี่ยง</p>
<p>6. บุคคลใดเป็นผู้มีหน้าที่ในการระบุความเสี่ยงใหม่ (Emerging Risk) และเป็นผู้รับผิดชอบในการบริหารจัดการความเสี่ยงนั้น</p>	<p>การบริหารความเสี่ยงเป็นหน้าที่ของทุกคนในองค์กร ดังนั้น หากมีความเสี่ยงใหม่ (Emerging Risk) เกิดขึ้น ผู้ที่มีหน้าที่ในการระบุความเสี่ยงดังกล่าว อาจเป็นหน่วยงานดังนี้</p> <ul style="list-style-type: none"> <li>• หน่วยงานแนวป้องกันด้านที่ 1 เมื่อมีการเปลี่ยนแปลงการปฏิบัติการหรือเปลี่ยนแปลงกฎหมายที่เกี่ยวข้อง ผู้ปฏิบัติงานอาจเป็นผู้ระบุความเสี่ยงใหม่ที่เกิดขึ้นจากการเปลี่ยนแปลงดังกล่าว</li> <li>• หน่วยงานแนวป้องกันด้านที่ 2 หน่วยงานบริหารความเสี่ยงใช้เครื่องมือในการพยากรณ์หรือคาดคะเนความเสี่ยงเพื่อระบุความเสี่ยงใหม่</li> </ul> <p>ทั้งนี้ เมื่อทราบถึงความเสี่ยงใหม่ที่อาจเกิดขึ้นแล้ว จะต้องมีการแจ้งไปยังหน่วยงานบริหารความเสี่ยง เพื่อดำเนินการประเมินความเสี่ยงใหม่นั้น ตามกระบวนการบริหารความเสี่ยงและระบุผู้รับผิดชอบในการบริหารจัดการความเสี่ยงนั้นต่อไป</p>
<p>7. คณะกรรมการบริหารความเสี่ยงควรมีคุณสมบัติและองค์ประกอบอย่างไร</p>	<p>คณะกรรมการมีหน้าที่ในการกำกับดูแลการบริหารความเสี่ยง ซึ่งอาจพิจารณาแต่งตั้งและมอบหมายอำนาจและหน้าที่ให้คณะกรรมการบริหารความเสี่ยงดูแลด้านการบริหารความเสี่ยงแทนได้ โดยคุณสมบัติและองค์ประกอบของคณะกรรมการบริหารความเสี่ยงอาจเป็นไปตามกฎหมาย หรือกฎระเบียบ</p>

คำถาม	คำตอบ
	<p>ที่เกี่ยวข้องกำหนด หรือเป็นไปตามที่คณะกรรมการกำหนด โดยพิจารณาความเหมาะสมตามบริบทขององค์กร</p> <p>ทั้งนี้ คุณสมบัติที่คณะกรรมการบริหารความเสี่ยงพึงมี คือ ควรเป็นผู้ที่มีความรู้เกี่ยวกับลักษณะการประกอบธุรกิจ มีวิสัยทัศน์กว้างไกล สามารถวิเคราะห์และคาดการณ์ เหตุการณ์ในอนาคตได้อย่างรอบด้านและสมเหตุสมผล มีภาวะผู้นำ และกล้าตัดสินใจ ตลอดจนมีความรู้เกี่ยวกับวิธีการจัดการความเสี่ยงนั้นๆ</p>
<p>8. คณะกรรมการควบคุมภายในควรมีคุณสมบัติและองค์ประกอบอย่างไร และหน่วยงานควบคุมภายในควรมีการกำหนดโครงสร้างอย่างไร</p>	<p><b>คณะกรรมการควบคุมภายใน</b></p> <p>องค์ประกอบและคุณสมบัติของคณะกรรมการควบคุมภายในให้เป็นไปตามที่รัฐวิสาหกิจกำหนด ซึ่งอาจเป็นคณะทำงานที่ประกอบด้วยผู้บริหารที่มีความรู้ความสามารถในการทำหน้าที่อำนวยความสะดวก การกำหนดแนวทาง รวบรวม พิจารณา กลั่นกรอง สรุปผลการประเมินการควบคุมภายใน และให้คำแนะนำด้านการควบคุมภายใน รวมถึงประสานงานและจัดทำรายงานการประเมินผลการควบคุมภายใน</p> <p><b>หน่วยงานควบคุมภายใน</b></p> <p>รัฐวิสาหกิจอาจพิจารณากำหนดหน่วยงานควบคุมภายในเป็นหน่วยงานแยกต่างหากหรือรวมกับหน่วยงานแนวป้องกันด่านที่ 2 (Second Line of Defense) ขึ้นซึ่งขึ้นอยู่กับบริบทของแต่ละองค์กร และควรประกอบด้วยบุคลากรที่มีความรู้ความเข้าใจในด้านการควบคุมภายในอย่างเพียงพอ เพื่อสามารถให้คำแนะนำในการออกแบบระบบการควบคุมภายในที่เกี่ยวข้องกับกระบวนการทำงาน</p>



สรุปลสาระสำคัญเกี่ยวกับการบริหารความเสี่ยง  
และการควบคุมภายใน (Infographics)



# หลักเกณฑ์ แนวปฏิบัติ และคู่มือปฏิบัติเกี่ยวกับการบริหารความเสี่ยง และการควบคุมภายในสำหรับรัฐวิสาหกิจ ปี 2568

## สรุปการปรับปรุงที่สำคัญ

หลักเกณฑ์ แนวปฏิบัติ และคู่มือปฏิบัติเกี่ยวกับการบริหารความเสี่ยงและการควบคุมภายในสำหรับรัฐวิสาหกิจ ปี 2568 ได้มีการปรับปรุงให้สอดคล้องกับกฎหมาย กฎ ระเบียบ และหลักเกณฑ์อื่นๆ ที่เกี่ยวกับการบริหารความเสี่ยง และการควบคุมภายใน เช่น หลักเกณฑ์กระทรวงการคลังว่าด้วยมาตรฐานและหลักเกณฑ์ปฏิบัติการควบคุมภายใน สำหรับหน่วยงานของรัฐ พ.ศ. 2561 หลักเกณฑ์กระทรวงการคลังว่าด้วยมาตรฐานและหลักเกณฑ์ปฏิบัติการบริหารจัดการความเสี่ยงสำหรับหน่วยงานของรัฐ พ.ศ. 2562 COSO IC 2013 และ COSO ERM 2017 โดยมีการปรับปรุงที่สำคัญ ดังนี้

### 1 ทบทวนและปรับปรุงองค์ประกอบ

ทบทวนและปรับปรุงองค์ประกอบของการบริหารความเสี่ยงและการควบคุมภายใน เพื่อให้สอดคล้องกับมาตรฐานและหลักเกณฑ์ของกระทรวงการคลัง และมาตรฐานสากล เช่น COSO ERM 2017



### 2 การกำกับดูแลการบริหารความเสี่ยงและการควบคุมภายในที่ชัดเจน

เพิ่มเติมบทบาทหน้าที่และคุณสมบัติของคณะกรรมการรัฐวิสาหกิจ และหน่วยงานที่เกี่ยวข้องให้ชัดเจนและสอดคล้องกับกฎหมาย หลักเกณฑ์ แนวปฏิบัติ และมาตรฐานสากล

### 3 การบูรณาการความเสี่ยง

กำหนดให้มีการบูรณาการความเสี่ยงให้เป็นส่วนหนึ่งของกระบวนการปฏิบัติงาน ตั้งแต่การกำหนดวัตถุประสงค์ กลยุทธ์ขององค์กรและกำหนดให้การบริหารความเสี่ยงเป็นหน้าที่ของพนักงานทุกระดับในองค์กร รวมถึงเพิ่มเติมแนวทางการบริหารความเสี่ยงกับการบูรณาการด้าน GRC ในองค์กร



### 4 แนวปฏิบัติและตัวอย่างที่ครอบคลุม

ปรับปรุงแนวปฏิบัติและเพิ่มเติมตัวอย่างที่เกี่ยวข้องกับการบริหารความเสี่ยงและการควบคุมภายในให้ชัดเจนและครอบคลุมมากยิ่งขึ้น เพื่อให้รัฐวิสาหกิจสามารถนำไปประยุกต์ใช้ได้เหมาะสมกับบริบทขององค์กร เช่น

- ตัวอย่างโครงสร้างการบริหารความเสี่ยงและการควบคุมภายในสำหรับรัฐวิสาหกิจ และบทบาทหน้าที่หน่วยงานหรือตำแหน่งงานที่เกี่ยวข้อง
- ตัวอย่างการบูรณาการด้าน GRC
- แนวปฏิบัติเพื่อการต่อยอด เรื่องการสำรวจทัศนคติของบุคลากรที่มีต่อการบริหารความเสี่ยงและการควบคุมภายใน รวมถึงการประเมินทัศนคติของพนักงานในเรื่องปัจจัยที่ส่งเสริมพฤติกรรมในการสร้างวัฒนธรรมองค์กร
- ตัวอย่างการพิจารณานำระบบสารสนเทศมาใช้ในการบริหารความเสี่ยง



# 7 ปัจจัยสำคัญต่อความสำเร็จในการบริหารความเสี่ยง และการควบคุมภายใน



01

## การสนับสนุนจากคณะกรรมการรัฐวิสาหกิจ และผู้บริหารระดับสูง

คณะกรรมการรัฐวิสาหกิจและผู้บริหารระดับสูง ควรสนับสนุน มีส่วนร่วมและปลูกฝังให้บุคลากร ตระหนักถึงความสำคัญและเห็นคุณค่า ของการบริหารความเสี่ยงและการควบคุมภายใน

02

## การใช้คำให้เกิดความเข้าใจแบบเดียวกัน

รัฐวิสาหกิจที่ได้จัดทำกรอบนโยบายการบริหาร ความเสี่ยงและการควบคุมภายในที่มีคำอธิบาย องค์ประกอบอย่างชัดเจน จะทำให้ผู้บริหาร และพนักงานทุกคนเข้าใจและปฏิบัติงาน ไปในแนวทางเดียวกันและมีจุดหมายร่วมกัน

03

## การปฏิบัติตามกระบวนการบริหารความเสี่ยง และการควบคุมภายในอย่างต่อเนื่อง

รัฐวิสาหกิจสามารถนำกระบวนการบริหารความเสี่ยง และการควบคุมภายในมาปฏิบัติอย่างทั่วถึง ทั้งองค์กร และกระทำอย่างต่อเนื่องสม่ำเสมอ

04

## การสื่อสารอย่างมีประสิทธิภาพ

ผู้บริหารได้รับข้อมูลเกี่ยวกับความเสี่ยง และการควบคุมภายในอย่างถูกต้องและทันเวลา เพื่อนำมาใช้ปรับปรุงการบริหารรัฐวิสาหกิจ รวมถึงจัดการความเสี่ยงและการควบคุมภายใน

05

## การวัดผลการบริหารความเสี่ยง และการควบคุมภายใน

การวัดความเสี่ยงอาจอยู่ในรูปแบบของการวัด ผลกระทบและโอกาสที่อาจเกิดขึ้น หรือการกำหนด ดัชนีชี้วัดผลการดำเนินงาน (KPI) ก็ได้ โดยการบริหาร ความเสี่ยงและการควบคุมภายในที่ประสบความสำเร็จ จะช่วยให้ความเสี่ยงเหลืออยู่ในระดับที่รัฐวิสาหกิจ ยอมรับได้

06

## การฝึกอบรมและกลไกด้านทรัพยากรบุคคล

กรรมการ ผู้บริหาร และพนักงานทุกคน ในรัฐวิสาหกิจควรได้รับการฝึกอบรม เพื่อให้เข้าใจกรอบการบริหารความเสี่ยง และการควบคุมภายใน

07

## การติดตามและพัฒนาระบบการบริหาร ความเสี่ยงและการควบคุมภายใน

รัฐวิสาหกิจควรกำหนดวิธีที่เหมาะสมในการติดตาม และพัฒนาระบบการบริหารความเสี่ยง และการควบคุมภายในให้สอดคล้องกับบริบท ขององค์กรและสภาพแวดล้อมที่เปลี่ยนแปลงไป



# การบริหารความเสี่ยงและการควบคุมภายใน (Enterprise Risk Management and Internal Control)

แนวปฏิบัติที่ดีตามหลักเกณฑ์ แนวปฏิบัติ และคู่มือปฏิบัติเกี่ยวกับการบริหารความเสี่ยงและการควบคุมภายใน สำหรับรัฐวิสาหกิจ ปี 2568 ที่รัฐวิสาหกิจควรนำไปปรับใช้ให้สอดคล้องกับบริบทขององค์กรและนำไปปฏิบัติ สรุปได้ดังนี้

การบริหารความเสี่ยง (Enterprise Risk Management)	การควบคุมภายใน (Internal Control)
 <p><b>1. การกำกับดูแลและวัฒนธรรม (Governance and Culture)</b> ควรกำหนดสภาพแวดล้อมภายในองค์กรให้สนับสนุนการบริหารความเสี่ยงทั่วทั้งองค์กร</p>	 <p><b>1. สภาพแวดล้อมการควบคุม (Control Environment)</b> ควรกำหนดสภาพแวดล้อมการควบคุมภายในที่ครอบคลุมมาตรฐานกระบวนการ และโครงสร้างองค์กร</p>
 <p><b>2. กลยุทธ์และการกำหนดวัตถุประสงค์ (Strategy and Objective Setting)</b> ควรระบุเหตุการณ์ที่อาจเกิดขึ้นและส่งผลกระทบต่อองค์กรทั้งด้านที่เป็นโอกาสและความเสี่ยง เพื่อนำไปกำหนดวัตถุประสงค์ขององค์กร</p>	 <p><b>2. การประเมินความเสี่ยง (Risk Assessment)</b> ควรประเมินความเสี่ยงขององค์กรที่จะส่งผลกระทบต่อผลสำเร็จตามวัตถุประสงค์ขององค์กร</p>
 <p><b>3. ผลการปฏิบัติงาน (Performance)</b> ควรมีการระบุและประเมินความเสี่ยงที่ชัดเจนและเป็นระบบ</p>	 <p><b>3. กิจกรรมการควบคุม (Control Activities)</b> ควรจัดให้มีกิจกรรมการควบคุมโดยการกำหนดให้มีมาตรการหรือขั้นตอนในการปฏิบัติงานตามนโยบาย</p>
 <p><b>4. การสอบทานและการแก้ไขปรับปรุง (Review and Revision)</b> ควรติดตามและทบทวนแนวปฏิบัติในการบริหารความเสี่ยงอย่างสม่ำเสมอ</p>	 <p><b>4. สารสนเทศและการสื่อสาร (Information and Communication)</b> ควรจัดให้มีสารสนเทศที่เพียงพอเหมาะสม และเชื่อถือได้จากทั้งแหล่งภายในและภายนอก</p>
 <p><b>5. สารสนเทศ การสื่อสาร และการรายงาน (Information Communication and Reporting)</b> ควรจัดให้มีสารสนเทศและการสื่อสารที่สนับสนุนการบริหารความเสี่ยง</p>	 <p><b>5. กิจกรรมติดตามผล (Monitoring)</b> ควรติดตามและประเมินผลการควบคุมภายในอย่างต่อเนื่องและสม่ำเสมอ</p>



## องค์ประกอบที่ 1 การกำกับดูแลและวัฒนธรรม (Governance and Culture)

รัฐวิสาหกิจควรกำหนดสภาพแวดล้อมภายในองค์กรให้สนับสนุนการบริหารความเสี่ยงทั่วทั้งองค์กร ให้มีความเหมาะสมกับลักษณะขององค์กรนั้น ทั้งในด้านการกำกับดูแลการบริหารความเสี่ยงโดยคณะกรรมการรัฐวิสาหกิจที่เป็นผู้มีคุณสมบัติและประสบการณ์ที่เหมาะสมด้านการกำหนดโครงสร้างองค์กร ด้านการสร้างวัฒนธรรมและพฤติกรรมที่องค์กรพึงประสงค์ ความมุ่งมั่นต่อการเพิ่มขีดความสามารถของบุคลากร สภาพแวดล้อมภายในองค์กรถือเป็นพื้นฐานขององค์ประกอบอื่นของการบริหารความเสี่ยง โดยมีแนวปฏิบัติที่ดี ดังนี้

### แนวปฏิบัติที่ 1

การกำหนดหน้าที่และคุณสมบัติของคณะกรรมการรัฐวิสาหกิจ

### แนวปฏิบัติที่ 2

การกำหนดโครงสร้างองค์กร (Organization Chart) ที่สนับสนุนให้เกิดการบริหารความเสี่ยงที่มีประสิทธิภาพ

### แนวปฏิบัติที่ 3

การกำหนดคุณค่าหลัก (Core Value) และพฤติกรรมที่พึงประสงค์ (Desired Behavior)

### แนวปฏิบัติที่ 4

การปลูกฝังการบริหารความเสี่ยงจนเป็นวัฒนธรรมองค์กร

### แนวปฏิบัติที่ 5

การเพิ่มขีดความสามารถของบุคลากรและการจัดสรรทรัพยากรให้เพียงพอในการบริหารความเสี่ยง





## องค์ประกอบที่ 2 กลยุทธ์และการกำหนดวัตถุประสงค์ (Strategy and Objective Setting)

รัฐวิสาหกิจควรระบุเหตุการณ์ที่อาจเกิดขึ้นและส่งผลกระทบต่อองค์กรทั้งด้านที่เป็นโอกาสและความเสี่ยง และจะต้องมีความเข้าใจถึงปัจจัยต่างๆ ทั้งภายในและภายนอก เพื่อนำไปกำหนดวัตถุประสงค์ขององค์กรที่ชัดเจน และสอดคล้องกัน และจะต้องเป็นในแนวทางเดียวกันกับระดับความเสี่ยงที่องค์กรยอมรับได้ โดยมีแนวปฏิบัติที่ดี ดังนี้

### แนวปฏิบัติที่ 1

การระบุเหตุการณ์ที่อาจเกิดขึ้นและส่งผลกระทบต่อการทำงานขององค์กร

### แนวปฏิบัติที่ 2

การกำหนดระดับความเสี่ยงที่องค์กรยอมรับได้ (Risk Appetite) และช่วงเบี่ยงเบนของระดับความเสี่ยงที่องค์กรยอมรับได้ (Risk Tolerance)

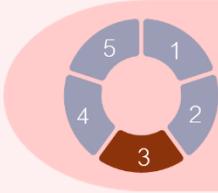
### แนวปฏิบัติที่ 3

การเลือกกลยุทธ์ขององค์กร

### แนวปฏิบัติที่ 4

การกำหนดวัตถุประสงค์ในการประกอบกิจการ





## องค์ประกอบที่ 3 ผลการปฏิบัติงาน (Performance)

รัฐวิสาหกิจควรมีการระบุและประเมินความเสี่ยงที่ชัดเจนและเป็นระบบ โดยการประเมินความเสี่ยงจะมีการพิจารณาทั้งด้านโอกาสที่ความเสี่ยงจะเกิดขึ้น และผลกระทบหากความเสี่ยงเกิดขึ้นจริง รวมถึงควรมีการจัดลำดับความสำคัญของความเสี่ยงตามระดับความรุนแรงของความเสี่ยงและช่วงความเบี่ยงเบนของระดับความเสี่ยงที่องค์กรยอมรับได้ เพื่อให้สามารถจัดสรรทรัพยากรในการตอบสนองต่อความเสี่ยงได้อย่างเหมาะสม โดยมีแนวปฏิบัติที่ดี ดังนี้

### แนวปฏิบัติที่ 1

การระบุความเสี่ยงที่ชัดเจนและครอบคลุมการดำเนินงานขององค์กร และการจัดทำทะเบียนความเสี่ยง

### แนวปฏิบัติที่ 2

การกำหนดเกณฑ์การประเมินความเสี่ยงและการประเมินความเสี่ยง

### แนวปฏิบัติที่ 3

การจัดลำดับความสำคัญของความเสี่ยง

### แนวปฏิบัติที่ 4

การเลือกแนวทางการตอบสนองต่อความเสี่ยง

### แนวปฏิบัติที่ 5

การจัดทำภาพรวมความเสี่ยง





## องค์ประกอบที่ 4 การสอบทานและการแก้ไขปรับปรุง (Review and Revision)

รัฐวิสาหกิจควรมีการติดตามและทบทวนแนวปฏิบัติในการบริหารความเสี่ยงขององค์กรอย่างสม่ำเสมอ เพื่อให้องค์กรสามารถระบุแนวทางการปรับปรุงการบริหารความเสี่ยง และนำไปพัฒนาประสิทธิภาพของการบริหารความเสี่ยงขององค์กรในทุกระดับ ตลอดจนสามารถปรับเปลี่ยนการบริหารความเสี่ยง หรือประยุกต์ใช้ให้เหมาะสมกับการเปลี่ยนแปลงต่างๆ ได้อย่างทันเวลา โดยมีแนวปฏิบัติที่ดี ดังนี้

### แนวปฏิบัติที่ 1

การวิเคราะห์การเปลี่ยนแปลงจากปัจจัยภายในและปัจจัยภายนอก ที่อาจส่งผลให้มีการทบทวนแผนการบริหารจัดการความเสี่ยง

### แนวปฏิบัติที่ 2

การทบทวนแผนการบริหารจัดการความเสี่ยง

### แนวปฏิบัติที่ 3

การปรับปรุงกระบวนการบริหารความเสี่ยงขององค์กรอย่างต่อเนื่อง





## องค์ประกอบที่ 5 สารสนเทศ การสื่อสาร และการรายงาน (Information Communication and Reporting)

รัฐวิสาหกิจควรกำหนดให้มีสารสนเทศและการสื่อสารที่สนับสนุนการบริหารความเสี่ยง ข้อมูลสารสนเทศที่เกี่ยวข้องกับองค์กรทั้งจากแหล่งข้อมูลภายในและภายนอกองค์กรควรต้องได้รับการบันทึกและสื่อสารอย่างเหมาะสมและทันเวลา โดยมีแนวปฏิบัติที่ดี ดังนี้

### แนวปฏิบัติที่ 1

การบริหารสารสนเทศด้านความเสี่ยงเพื่อการจัดการที่ดี

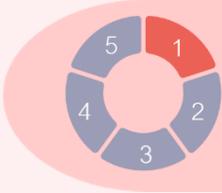
### แนวปฏิบัติที่ 2

การกำหนดช่องทางสื่อสารข้อมูลและสารสนเทศด้านความเสี่ยง

### แนวปฏิบัติที่ 3

การรายงานความเสี่ยงต่อคณะกรรมการรัฐวิสาหกิจ





## องค์ประกอบที่ 1 สภาพแวดล้อมการควบคุม (Control Environment)

รัฐวิสาหกิจควรกำหนดให้มีสภาพแวดล้อมการควบคุมภายใน ประกอบด้วย มาตรฐาน กระบวนการ และโครงสร้างขององค์กร เพื่อใช้เป็นแนวทางให้บุคลากรทุกระดับสามารถปฏิบัติและตัดสินใจในสิ่งที่ตนรับผิดชอบเกี่ยวกับการควบคุมภายใน โดยมีแนวปฏิบัติที่ดี ดังนี้

### แนวปฏิบัติที่ 1

การกำหนดจรรยาบรรณ  
ในการประกอบกิจการ

### แนวปฏิบัติที่ 2

การกำกับดูแลและสนับสนุน  
ให้มีการควบคุมภายใน  
โดยคณะกรรมการรัฐวิสาหกิจ

### แนวปฏิบัติที่ 3

การกำหนดโครงสร้างองค์กร  
(Organization Chart)  
และสายการบังคับบัญชา

### แนวปฏิบัติที่ 4

การออกแบบนโยบาย  
และแนวปฏิบัติด้านทรัพยากร  
บุคคล ซึ่งครอบคลุมการจูงใจ  
พัฒนา รักษาไว้

### แนวปฏิบัติที่ 5

การกำหนดอำนาจหน้าที่  
และความรับผิดชอบต่อผล  
การปฏิบัติงาน





## องค์ประกอบที่ 2 การประเมินความเสี่ยง (Risk Assessment)

รัฐวิสาหกิจควรประเมินความเสี่ยงเพื่อให้ทราบว่าองค์กรมีความเสี่ยงอย่างไร มีระดับความเสี่ยงและโอกาสที่จะเกิดมากน้อยเพียงใด โดยผู้บริหารต้องพิจารณาว่าองค์กรควรมีมาตรการหรือบริหารจัดการอย่างไร เพื่อจัดการความเสี่ยงให้อยู่ในระดับที่องค์กรยอมรับได้ โดยมีแนวปฏิบัติที่ดี ดังนี้

### แนวปฏิบัติที่ 1

การกำหนดวัตถุประสงค์ระดับองค์กร และหน่วยงานที่เกี่ยวข้องกับการควบคุมภายใน

### แนวปฏิบัติที่ 2

การระบุเหตุการณ์ความเสี่ยงที่อาจมีผลกระทบต่อการทำงาน

### แนวปฏิบัติที่ 3

การประเมินความเป็นไปได้ที่จะเกิดความเสี่ยงด้านการทุจริต



### แนวปฏิบัติที่ 4

การระบุและประเมินการเปลี่ยนแปลงของสภาพแวดล้อมที่อาจมีผลกระทบอย่างมีนัยสำคัญต่อระบบการควบคุมภายใน



## องค์ประกอบที่ 3 กิจกรรมการควบคุม (Control Activities)

รัฐวิสาหกิจควรจัดให้มีกิจกรรมการควบคุม โดยการกำหนดให้มีมาตรการหรือขั้นตอนในการปฏิบัติงานตามนโยบาย เพื่อให้สามารถจัดการความเสี่ยงได้อย่างมีประสิทธิภาพและประสิทธิผล โดยมีแนวปฏิบัติที่ดี ดังนี้

### แนวปฏิบัติที่ 1

การเลือกและพัฒนากิจกรรมการควบคุม

### แนวปฏิบัติที่ 2

การนำเทคโนโลยีสารสนเทศมาใช้ เพื่อสนับสนุนให้บรรลุวัตถุประสงค์ของการควบคุมภายใน

### แนวปฏิบัติที่ 3

การกำหนดและสื่อสารนโยบายที่เกี่ยวข้องกับการควบคุมภายใน





## องค์ประกอบที่ 4 สารสนเทศและการสื่อสาร (Information and Communication)

รัฐวิสาหกิจต้องจัดให้มีสารสนเทศอย่างเพียงพอ เหมาะสม เชื่อถือได้ ซึ่งประกอบด้วยข้อมูลสารสนเทศที่เกี่ยวกับการดำเนินงานทั้งจากแหล่งภายในและแหล่งภายนอกองค์กร เพื่อสนับสนุนประสิทธิภาพและประสิทธิผล ในการกำหนดกลยุทธ์ ประเมินความเสี่ยง และกิจกรรมการควบคุม โดยมีแนวปฏิบัติที่ดี ดังนี้

### แนวปฏิบัติที่ 1

การดำเนินงานด้านข้อมูล  
สารสนเทศและระบบ  
จัดการฐานข้อมูล

### แนวปฏิบัติที่ 2

การจัดให้มีการสื่อสาร  
ภายในองค์กร

### แนวปฏิบัติที่ 3

การจัดให้มีการสื่อสาร  
กับหน่วยงานภายนอก  
และมีช่องทางเพื่อเปิดรับ  
ข้อมูลจากผู้มีส่วนได้เสีย  
ภายนอกองค์กร





## องค์ประกอบที่ 5 กิจกรรมติดตามผล (Monitoring)

รัฐวิสาหกิจควรกำหนดให้มีการติดตามและประเมินผลการควบคุมภายใน โดยมีขึ้นในระหว่างการทำงาน และการประเมินผลเป็นรายครั้งอย่างต่อเนื่องและสม่ำเสมอ เพื่อให้คณะกรรมการรัฐวิสาหกิจและผู้บริหารระดับสูงมีความมั่นใจได้อย่างสมเหตุสมผลต่อประสิทธิภาพและประสิทธิผลของการควบคุมภายใน โดยมีแนวปฏิบัติที่ดี ดังนี้

### แนวปฏิบัติที่ 1

การพัฒนาและประเมินผลการควบคุมภายใน  
อย่างต่อเนื่องและสม่ำเสมอ

### แนวปฏิบัติที่ 2

การสื่อสารข้อบกพร่องที่ได้จากการประเมิน  
การควบคุมภายใน



# คำถาม-คำตอบที่น่าสนใจ

## เกี่ยวกับการบริหารความเสี่ยง และการควบคุมภายใน



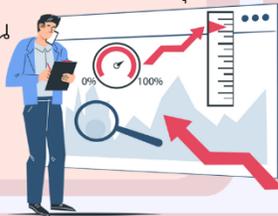
**Q:**

1

เหตุการณ์หรือความเสี่ยง 1 เรื่อง สามารถมีดัชนีชี้วัดความเสี่ยงหลัก (KRI) ได้มากกว่า 1 ดัชนีหรือไม่

**A:**

ในการกำหนด KRI เพื่อเฝ้าระวังแนวโน้มของความเสี่ยงที่อาจเปลี่ยนแปลงสามารถกำหนดได้มากกว่า 1 ดัชนี ทั้งนี้ จำนวน KRI ที่กำหนดควรพิจารณาจากจำนวนสาเหตุที่อาจก่อให้เกิดความเสี่ยงนั้น



**Q:**

2

บทบาทของผู้ตรวจสอบภายใน ในด้านการสอบทานกระบวนการบริหารความเสี่ยงควรเป็นอย่างไร

**A:**

ผู้ตรวจสอบภายในมีหน้าที่ **สอบทาน ประสิทธิภาพ และ ประสิทธิผล** ของกระบวนการบริหารความเสี่ยง เช่น

- ทำให้มั่นใจว่าระบบบริหารความเสี่ยง มีประสิทธิภาพและประสิทธิผล
- กรอบการบริหารความเสี่ยงมีประสิทธิภาพ
- การบริหารความเสี่ยงเป็นไปตามกรอบและนโยบายที่กำหนดไว้

**Q:**

3

การประเมินผลการควบคุมภายในและการตรวจสอบภายในแตกต่างกันอย่างไร

**A:**

**การประเมินผลการควบคุมภายใน**

เป็นกระบวนการที่ดำเนินการโดยหน่วยงานแนวป้องกันด้านที่ 1 หรือหน่วยงานแนวป้องกันด้านที่ 2 เพื่อดำเนินการ**ทบทวน**ความเพียงพอและประสิทธิผลของระบบการควบคุมภายใน เพื่อให้สามารถจัดการความเสี่ยงได้อย่างมีประสิทธิภาพและทันต่อการเปลี่ยนแปลง

**การตรวจสอบภายใน**

เป็นหน้าที่ของหน่วยงานแนวป้องกันด้านที่ 3 ในการประเมินอย่างอิสระและให้คำปรึกษา เพื่อให้**ความเชื่อมั่น**ต่อประสิทธิผลของการบริหารความเสี่ยง การควบคุมภายใน และการกำกับดูแล

# คำถาม-คำตอบที่น่าสนใจ

## เกี่ยวกับการบริหารความเสี่ยง และการควบคุมภายใน



**Q:**

4

ความเสี่ยงด้านสิ่งแวดล้อม สังคม และการกำกับดูแล (ESG) เชื่อมโยงกับกระบวนการบริหารความเสี่ยงอย่างไร

**A:**

การบริหารความเสี่ยงด้าน ESG ช่วยเสริมสร้างความยั่งยืน เพิ่มคุณค่าให้กับรัฐวิสาหกิจ และสร้างความเชื่อมั่นแก่ผู้มีส่วนได้เสีย โดยในการระบุหรือประเมินความเสี่ยง ให้รัฐวิสาหกิจพิจารณาถึงความเสี่ยงด้าน ESG ด้วย

**Q:**

5

เทคโนโลยีที่นำมาใช้ในการบริหารความเสี่ยงควรมีลักษณะอย่างไร และจำเป็นต้องเป็นระบบสารสนเทศหรือไม่

**A:**

เทคโนโลยีที่นำมาใช้ในการบริหารความเสี่ยงไม่จำเป็นต้องเป็นระบบสารสนเทศ หรือซอฟต์แวร์เฉพาะทางเสมอไป โดยอาจอยู่ในรูปแบบ Spreadsheet แบบฟอร์มออนไลน์ที่สามารถดำเนินการอย่างต่อเนื่อง เป็นระบบ และตรวจสอบได้

**Q:**

ใครเป็นผู้มีหน้าที่ในการระบุความเสี่ยงใหม่ (Emerging Risk) และเป็นผู้รับผิดชอบในการบริหารจัดการความเสี่ยงนั้น

**A:**

การระบุความเสี่ยงอาจเกิดขึ้นได้จากหลายบุคคล เช่น

หน่วยงานแนวป้องกันด้านที่ 1 เมื่อมีการเปลี่ยนแปลงการปฏิบัติการหรือเปลี่ยนแปลงกฎหมายที่เกี่ยวข้อง ผู้ปฏิบัติงานอาจเป็นผู้ระบุความเสี่ยงใหม่ที่เกิดขึ้นจากการเปลี่ยนแปลงดังกล่าว

หน่วยงานแนวป้องกันด้านที่ 2 หน่วยงานบริหารความเสี่ยงใช้เครื่องมือในการพยากรณ์หรือคาดการณ์ความเสี่ยงเพื่อระบุความเสี่ยงใหม่

ทั้งนี้ เมื่อทราบถึงความเสี่ยงใหม่ที่อาจเกิดขึ้นแล้ว จะต้องมีการแจ้งไปยังหน่วยงานบริหารความเสี่ยง เพื่อดำเนินการประเมินความเสี่ยงใหม่นั้นตามกระบวนการบริหารความเสี่ยงและระบุผู้รับผิดชอบในการบริหารจัดการความเสี่ยงนั้น



6

# คำถาม-คำตอบที่น่าสนใจ

## เกี่ยวกับการบริหารความเสี่ยง และการควบคุมภายใน



**Q:**

คณะกรรมการบริหารความเสี่ยงควรมีคุณสมบัติและองค์ประกอบอย่างไร

7

**A:**

คณะกรรมการรัฐวิสาหกิจมีหน้าที่ในการกำกับดูแลการบริหารความเสี่ยง ซึ่งอาจพิจารณาแต่งตั้งและมอบหมายอำนาจและหน้าที่ให้คณะกรรมการบริหารความเสี่ยงดูแลด้านการบริหารความเสี่ยงแทนได้ โดยคุณสมบัติและองค์ประกอบของคณะกรรมการบริหารความเสี่ยงอาจเป็นไปตามกฎหมาย หรือกฎระเบียบที่เกี่ยวข้องกำหนด หรือเป็นไปตามที่คณะกรรมการรัฐวิสาหกิจกำหนด โดยพิจารณาความเหมาะสมตามบริบทขององค์กร



**Q:**

คณะกรรมการควบคุมภายในควรมีคุณสมบัติและองค์ประกอบอย่างไร และหน่วยงานควบคุมภายในควรมีการกำหนดโครงสร้างอย่างไร

8

**A:**

**คณะกรรมการควบคุมภายใน**

องค์ประกอบและคุณสมบัติของคณะกรรมการควบคุมภายในให้เป็นไปตามที่รัฐวิสาหกิจกำหนด ซึ่งอาจเป็นคณะทำงานที่ประกอบด้วยผู้บริหารที่มีความรู้ความสามารถในการทำหน้าที่อำนาจการกำหนดแนวทาง รวบรวม พิจารณากลับกรอง สรุปผล และให้คำแนะนำด้านการควบคุมภายใน รวมถึงประสานงานและจัดทำรายงานการประเมินผลการควบคุมภายใน

**หน่วยงานควบคุมภายใน**

รัฐวิสาหกิจอาจพิจารณากำหนดหน่วยงานควบคุมภายในเป็นหน่วยงานแยกต่างหากหรือรวมกับหน่วยงานแนวป้องกันด่านที่ 2 (Second Line of Defense) อื่น ขึ้นอยู่กับบริบทของแต่ละองค์กร และควรประกอบด้วยบุคลากรที่มีความรู้ความเข้าใจในด้านการควบคุมภายในอย่างเพียงพอ

6

บรรณานุกรม

## บรรณานุกรม

1. กระทรวงการคลัง. (พ.ศ. 2561). หลักเกณฑ์กระทรวงการคลังว่าด้วยมาตรฐานและหลักเกณฑ์ปฏิบัติการควบคุมภายในสำหรับหน่วยงานของรัฐ พ.ศ. 2561.
2. กระทรวงการคลัง. (พ.ศ. 2562). หลักเกณฑ์กระทรวงการคลังว่าด้วยมาตรฐานและหลักเกณฑ์ปฏิบัติการบริหารจัดการความเสี่ยงสำหรับหน่วยงานของรัฐ พ.ศ. 2562.
3. กระทรวงการคลัง. (พ.ศ. 2564). แนวทางการบริหารจัดการความเสี่ยงสำหรับหน่วยงานของรัฐ เรื่อง หลักการบริหารจัดการความเสี่ยงระดับองค์กร.
4. กระทรวงการคลัง. (พ.ศ. 2566). หลักเกณฑ์กระทรวงการคลังว่าด้วยมาตรฐานและหลักเกณฑ์ปฏิบัติการตรวจสอบภายในสำหรับหน่วยงานของรัฐ พ.ศ. 2561 และที่แก้ไขเพิ่มเติม.
5. ตลาดหลักทรัพย์แห่งประเทศไทย (The Stock Exchange of Thailand). (พ.ศ. 2560). หลักการกำกับดูแลกิจการที่ดีสำหรับบริษัทจดทะเบียน ปี 2560.
6. ตลาดหลักทรัพย์แห่งประเทศไทย (The Stock Exchange of Thailand). (พ.ศ. 2564). แนวปฏิบัติด้านการกำกับดูแลกิจการที่ดี เรื่อง การจัดทำจรรยาบรรณธุรกิจ (Code of Conduct).
7. สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์. (พ.ศ. 2556). แบบประเมินความเพียงพอของระบบการควบคุมภายใน ของสำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์.
8. สำนักงานคณะกรรมการนโยบายรัฐวิสาหกิจ กระทรวงการคลัง. (พ.ศ. 2566). คู่มือการปฏิบัติงานการตรวจสอบภายใน สำหรับรัฐวิสาหกิจ ปี 2566.
9. สำนักงานคณะกรรมการนโยบายรัฐวิสาหกิจ กระทรวงการคลัง. (พ.ศ. 2566). คู่มือการปฏิบัติงานของคณะกรรมการตรวจสอบ สำหรับรัฐวิสาหกิจ ปี 2566.
10. สำนักงานคณะกรรมการนโยบายรัฐวิสาหกิจ กระทรวงการคลัง. (พ.ศ. 2567). หลักเกณฑ์การประเมินกระบวนการปฏิบัติงาน และการจัดการ Core Business Enablers ของรัฐวิสาหกิจ (ฉบับปรับปรุงปี 2567).
11. สำนักงานคณะกรรมการนโยบายรัฐวิสาหกิจ กระทรวงการคลัง. (พ.ศ. 2562). หลักการและแนวทางการกำกับดูแลกิจการที่ดีของรัฐวิสาหกิจ พ.ศ. 2562.
12. สำนักงานคณะกรรมการนโยบายรัฐวิสาหกิจ กระทรวงการคลัง. (พ.ศ. 2568). ประกาศคณะกรรมการนโยบายรัฐวิสาหกิจ เรื่อง การกำกับดูแลกิจการที่ดีในรัฐวิสาหกิจ พ.ศ. 2568.
13. International Organization for Standardization (ISO). (2018). ISO 31000:2018 Risk Management – Principles and Guidelines.
14. Open Compliance and Ethics Group (OCEG). (2024). GRC Capability Model.
15. Open Compliance and Ethics Group (OCEG). (2024). Integrated Risk Management Framework.

16. The Committee of Sponsoring Organizations of the Treadway Commission (COSO). (2009). Guidance on Monitoring Internal Control Systems.
17. The Committee of Sponsoring Organizations of the Treadway Commission (COSO). (2013). กรอบการควบคุมภายในแบบบูรณาการ (Internal Control – Integrated Framework). ฉบับภาษาไทย แปลโดย สภาวิชาชีพบัญชี ในพระบรมราชูปถัมภ์.
18. The Committee of Sponsoring Organizations of the Treadway Commission (COSO). (2017). การบริหารความเสี่ยงขององค์กร การบูรณาการร่วมกับกลยุทธ์และผลการปฏิบัติงาน (Enterprise Risk Management – Integrating with Strategy and Performance). ฉบับภาษาไทย แปลโดย สภาวิชาชีพบัญชี ในพระบรมราชูปถัมภ์.
19. The Committee of Sponsoring Organizations of the Treadway Commission (COSO). (2023). การบริหารความเสี่ยงขององค์กร การประยุกต์ใช้การบริหารความเสี่ยงขององค์กรกับความเสี่ยงที่เกี่ยวข้องกับสิ่งแวดล้อม สังคม และการกำกับดูแล (ESG) (Enterprise Risk Management – Applying enterprise risk management to environmental, social and governance – related risks). ฉบับภาษาไทย แปลโดย สภาวิชาชีพบัญชี ในพระบรมราชูปถัมภ์.
20. The Organization for Economic Cooperation and Development (OECD). (2025). OECD Review of the Corporate Governance of State – Owned Enterprises in Thailand.
21. The World Economic Forum. (2025). The Global Risks Report 2025.



ติดต่อเรา

สำนักงานคณะกรรมการนโยบายรัฐวิสาหกิจ  
กระทรวงการคลัง

อาคาร 150 ปี กระทรวงการคลัง ชั้น 12เอ-15  
ถนนพระรามที่ 6 แขวงพญาไท เขตพญาไท  
กรุงเทพมหานคร 10400

โทรศัพท์

0 2298 5880

Email

[webmaster@sepo.go.th](mailto:webmaster@sepo.go.th)