



คู่มือบริหารความเสี่ยง
ปรับปรุงครั้งที่ 1 (กุมภาพันธ์ 2566)



สารบัญ

| หัวข้อ | หน้า |
|---|------|
| บทที่ 1 : ขอบเขตทั่วไป | 1 |
| 1.1 วัตถุประสงค์ของคู่มือบริหารความเสี่ยง | 1 |
| 1.2 ความหมายและคำจำกัดความของการบริหารความเสี่ยง | 1 |
| 1.3 ประโยชน์ของการบริหารความเสี่ยง | 4 |
| บทที่ 2 : การบริหารความเสี่ยงตามแนวทาง COSO ERM | |
| 2.1 หลักการสำคัญในการบริหารความเสี่ยงตามแนวทาง COSO ERM | 5 |
| 2.2 การบริหารความเสี่ยงตามแนวทาง COSO ERM | 5 |
| บทที่ 3 : การบริหารความเสี่ยงของบริษัท ทีซีเอ็ม คอร์ปอเรชั่น จำกัด (มหาชน) | |
| 3.1 โครงสร้างการบริหารความเสี่ยงของบริษัท ทีซีเอ็ม คอร์ปอเรชั่น จำกัด (มหาชน) | 8 |
| 3.2 ขั้นตอนการจัดทำระบบบริหารความเสี่ยง | 9 |
| - ขั้นตอนที่ 1 การกำหนดเกณฑ์การประเมินมาตรฐาน | |
| - ขั้นตอนที่ 2 การกำหนดวัตถุประสงค์ (Objective Setting) | |
| - ขั้นตอนที่ 3 การระบุความเสี่ยง / เหตุการณ์ความเสี่ยง (Identify Risks) | |
| - ขั้นตอนที่ 4 การประเมินความเสี่ยง | |
| - ขั้นตอนที่ 5 การวิเคราะห์ความเสี่ยงและจัดลำดับ | |
| - ขั้นตอนที่ 6 การจัดทำทะเบียนความเสี่ยง | |
| 3.3 การจัดการและจัดทำแผนบริหารความเสี่ยง | 12 |
| 3.4 การรายงานและติดตามผล | 13 |
| 3.5 ปัจจัยที่ทำให้การบริหารความเสี่ยงประสบผลสำเร็จ | 14 |
| 3.6 ปัจจัยที่ทำให้การบริหารความเสี่ยงล้มเหลว | 14 |
| บทที่ 4 : เบ็ดเตล็ด | 15 |

บทที่ 1 ขอบเขตทั่วไป

การบริหารความเสี่ยง นับเป็นเครื่องมือสำคัญและมีประโยชน์ในการบริหารจัดการองค์กรให้สามารถบรรลุเป้าหมายและวัตถุประสงค์ตามที่กำหนดไว้ได้อย่างมีประสิทธิภาพประสิทธิผล ช่วยสร้างคุณค่า รักษาคุณค่า และทำให้เกิดคุณค่าที่แท้จริงขององค์กร ด้วยการบริหารปัจจัยและควบคุมกิจกรรมทั้งกระบวนการดำเนินงานต่าง ๆ โดยลดมูลเหตุของแต่ละโอกาสที่ก่อให้เกิดผลกระทบ ทั้งนี้ เพื่อให้ระดับและขนาดของผลกระทบที่จะเกิดขึ้นกับองค์กรในอนาคตอยู่ในระดับที่ยอมรับได้ หรือควบคุมได้อย่างเป็นระบบทั่วทั้งองค์กร

1.1 วัตถุประสงค์ของคู่มือการบริหารความเสี่ยง

- (1) เพื่อให้ผู้บริหารและพนักงานมีความรู้ ความเข้าใจในกระบวนการบริหารความเสี่ยงขององค์กรเพื่อสนับสนุนการดำเนินงานขององค์กรให้เป็นไปตามเป้าหมายที่กำหนดไว้ในแผนดำเนินงาน และแผนกลยุทธ์
- (2) เพื่อเป็นเครื่องมือให้ผู้บริหารและพนักงานปฏิบัติหน้าที่ตามกระบวนการบริหารความเสี่ยงอย่างเป็นระบบและต่อเนื่อง สอดคล้องกับวิสัยทัศน์ พันธกิจ และคุณค่าหลักขององค์กร
- (3) เพื่อให้องค์กรมีกรอบการดำเนินงานเพื่อตอบสนองต่อเหตุการณ์ที่อาจส่งผลให้เกิดความเสี่ยงทุกด้านได้อย่างเป็นระบบ รวมทั้งมีการดำเนินการเพื่อสร้างพื้นฐานในการป้องกันและจัดการกับความเสี่ยงที่อาจเกิดขึ้นในอนาคต
- (4) เพื่อเป็นเครื่องมือช่วยในการปลูกฝังวัฒนธรรมองค์กรที่มุ่งเน้นการสร้างองค์ความรู้ด้านการบริหารความเสี่ยงไปยังผู้บริหาร และบุคลากรทุกระดับ เพื่อเป็นกลไกในการพัฒนาองค์ความรู้ด้านการบริหารความเสี่ยงและสนับสนุนให้การบริหารความเสี่ยงเป็นวัฒนธรรมองค์กรได้อย่างยั่งยืน

1.2 ความหมายและคำจำกัดความของการบริหารความเสี่ยง

เพื่อให้เข้าใจความหมายและคำจำกัดความของการบริหารความเสี่ยง จึงควรทำความเข้าใจกับความหมายของคำที่เกี่ยวข้อง ต่อไปนี้

- (1) **ความเสี่ยง (Risk)** หมายถึง ความเป็นไปได้ที่เหตุการณ์จะเกิดขึ้นและส่งผลกระทบต่อการบรรลุกลยุทธ์และวัตถุประสงค์ทางธุรกิจ โดยเหตุการณ์นั้นอาจส่งผลกระทบได้ทั้งทางบวกและทางลบ เพื่อให้ครอบคลุมการดำเนินงานขององค์กรจึงแบ่งประเภทของความเสี่ยงออกเป็น 5 ด้าน ดังนี้
 - (ก) ความเสี่ยงด้านกลยุทธ์ (Strategic Risk) คือ ความเสี่ยงที่เกิดจากการกำหนดแผนกลยุทธ์ แผนดำเนินงานที่นำไปปฏิบัติไม่เหมาะสมหรือไม่สอดคล้องกับปัจจัยภายในและภายนอก อันส่งผลกระทบต่อการบรรลุวัตถุประสงค์ วิสัยทัศน์ พันธกิจ หรือคุณค่าหลักขององค์กร
 - (ข) ความเสี่ยงด้านการดำเนินงาน (Operational Risk) คือ ความเสี่ยงที่เกิดจากการปฏิบัติงานทุก ๆ ขั้นตอนโดยครอบคลุมถึงปัจจัยที่เกี่ยวกับกระบวนการ อุปกรณ์ บุคลากร ระบบสารสนเทศในการปฏิบัติงาน เป็นต้น
 - (ค) ความเสี่ยงด้านการเงิน (Financial Risk) คือ ความเสี่ยงทางการเงินในภาพรวม ทั้งในด้านการวางแผนทางการเงิน การบริหารจัดการด้านการเงิน ซึ่งต้องไปในทิศทางเดียวกับกลยุทธ์ขององค์กร
 - (ง) ความเสี่ยงด้านกฎระเบียบ หรือกฎหมายที่เกี่ยวข้อง (Compliance Risk) คือ ความเสี่ยงที่เกิดจากการไม่สามารถปฏิบัติตามกฎระเบียบ ข้อบังคับ หรือกฎหมายของหน่วยงานหรือองค์กรที่เกี่ยวข้องและมีผลกระทบต่อการทำงานของบริษัทได้ รวมถึงความเสี่ยงจากการเปลี่ยนแปลงกฎระเบียบ ข้อบังคับ หรือกฎหมายข้างต้น

- (จ) ความเสี่ยงด้านเทคโนโลยี (Cyber Risk) คือ ความเสี่ยงที่เกี่ยวข้องกับการบริหารจัดการประสิทธิภาพการดำเนินงาน รวมถึงความมั่นคงปลอดภัยด้านเทคโนโลยี ได้แก่ การเข้าถึงข้อมูลหรือระบบงานโดยไม่ได้รับอนุญาต, Phishing mail, Malware, Ransomware เป็นต้น
- (2) **ปัจจัยเสี่ยง (Risk Factor)** หมายถึง สาเหตุของความเสี่ยงที่ทำให้ไม่บรรลุวัตถุประสงค์ตามที่กำหนดไว้ ปัจจัยเสี่ยงอาจมีสาเหตุมาจากทั้งปัจจัยภายในและภายนอก ซึ่งองค์กรควรระบุสาเหตุที่แท้จริงเพื่อจะได้วิเคราะห์และกำหนดกลยุทธ์/มาตรการ/แนวทางในการลดความเสี่ยงได้อย่างถูกต้อง เหมาะสมกับสถานการณ์ และสอดคล้องกับบริบทขององค์กร
- (2.1) ปัจจัยภายนอก หมายถึง ปัจจัยภายนอกองค์กรที่มีอิทธิพลต่อความสำเร็จตามวัตถุประสงค์ เป็นปัจจัยที่องค์กรไม่สามารถควบคุมโอกาสที่จะเกิดได้ แต่สามารถลดผลกระทบได้ตามวิธีการการตอบสนองต่อความเสี่ยงขององค์กร เช่น การซื้อ Forward contact เพื่อลดความผันผวนจากอัตราแลกเปลี่ยน เป็นต้น ปัจจัยภายนอก มีดังนี้
- (ก) ภัยธรรมชาติและสิ่งแวดล้อม (Natural Environment) การเกิดน้ำท่วม ไฟไหม้ แผ่นดินไหว คลื่นยักษ์สึนามิ โรคระบาด ที่ทำความเสียหายต่ออาคาร ทรัพย์สิน แหล่งวัตถุดิบ แรงงาน
 - (ข) ภาวะเศรษฐกิจ (Economic) ภาวะเงินเฟ้อ เงินฝืด อัตราดอกเบี้ย อัตราแลกเปลี่ยนสกุลเงิน และเหตุการณ์ที่เกี่ยวข้องกับการเคลื่อนไหวของราคา แหล่งเงินทุน คู่แข่ง
 - (ค) ภาวะการเมือง (Political) เหตุการณ์เกี่ยวกับรัฐบาล ผู้บริหารประเทศที่องค์กรดำเนินกิจการอยู่หรือทำธุรกิจด้วย การประกาศใช้กฎหมาย ระเบียบและเหตุการณ์ที่เปิดหรือจำกัดโอกาสเข้าสู่ตลาดต่างประเทศ การเปลี่ยนแปลงอัตราภาษี
 - (ง) สังคม (Social) เหตุการณ์ที่เกี่ยวกับการเปลี่ยนแปลงของประชากร การย้ายแหล่งที่อยู่โครงสร้างครอบครัว มาตรฐานและรสนิยมของสังคม การก่อการร้าย
 - (จ) เทคโนโลยีสารสนเทศ เหตุการณ์ที่เกี่ยวกับการเปลี่ยนแปลงเทคโนโลยีคอมพิวเตอร์
- (2.2) ปัจจัยภายใน หมายถึง ปัจจัยภายในองค์กรที่มีอิทธิพลต่อความสำเร็จตามวัตถุประสงค์ เป็นปัจจัยที่ผู้บริหารสามารถจัดการควบคุมได้ ดังนี้
- (ก) โครงสร้างพื้นฐาน (Infrastructure) เหตุการณ์ที่เกี่ยวกับความต้องการเงินทุนเพื่อขยายหรือรักษาโครงสร้างพื้นฐาน การลดเวลาที่เครื่องจักรเสีย และการเพิ่มความพึงพอใจของลูกค้า
 - (ข) พนักงาน (Personnel) หมายถึง เหตุการณ์ที่เกี่ยวกับบุคลากรในองค์กร เช่น การหมดอายุสัญญาจ้างพนักงานสำคัญ, การแสวงหาบุคลากรที่มีความสามารถในการดำเนินงาน, การรักษา และการพัฒนาบุคลากรที่มีอยู่
 - (ค) กระบวนการ (Process) หมายถึง เหตุการณ์ที่เกี่ยวกับขั้นตอนการปฏิบัติงาน การเปลี่ยนแปลงวิธีการหรือขั้นตอนการทำงาน ความผิดพลาดในกระบวนการ การส่งมอบสินค้า การควบคุมที่ไม่เพียงพอที่ส่งผลต่อความไม่พอใจของลูกค้า การเสียส่วนแบ่งการตลาด และการเสียชื่อเสียง
 - (ง) เทคโนโลยี (Technology) เหตุการณ์ที่เกี่ยวกับระบบไอทีและสารสนเทศภายในองค์กร ความถูกต้องครบถ้วนของสารสนเทศ ความมั่นคงปลอดภัย การเลือกระบบที่จะใช้การพัฒนา การบำรุงรักษาระบบ การสำรองข้อมูลและการกู้คืนระบบ
- (3) **การประเมินความเสี่ยง (Risk Assessment)** หมายถึง กระบวนการระบุความเสี่ยง และการวิเคราะห์เพื่อจัดลำดับความเสี่ยงที่จะมีผลกระทบต่อการบรรลุวัตถุประสงค์ขององค์กร โดยการประเมินจากโอกาสที่จะเกิด

เหตุการณ์ (Likelihood) และผลกระทบ (Impact) จากเหตุการณ์ความเสี่ยง**หลังจากมีมาตรการควบคุมความเสี่ยงที่อยู่ในการดำเนินงานตามปกติ**ของหน่วยงานต่างๆ ในองค์กร

- (ก) โอกาสที่จะเกิดเหตุการณ์ (Likelihood) หมายถึง ความถี่หรือโอกาสที่จะเกิดเหตุการณ์ความเสี่ยง
 - (ข) ผลกระทบ (Impact) หมายถึง ปริมาณของความรุนแรงหรือความเสียหายที่จะเกิดขึ้นจากเกิดเหตุการณ์หรือความเสี่ยง
 - (ค) ระดับของความเสี่ยง (Degree of Risk) หมายถึง สถานะของความเสี่ยงที่ได้จากการประเมินโอกาสและผลกระทบของแต่ละปัจจัยเสี่ยง
- (4) **ระดับความเสี่ยงที่ยอมรับได้ (Risk Appetite)** หมายถึง ประเภทและเกณฑ์ของความเสี่ยงหรือความไม่แน่นอนโดยรวมที่องค์กรยอมรับได้โดยยังคงให้องค์กรบรรลุเป้าหมาย ซึ่งความเสี่ยงที่ยอมรับได้นั้นอาจระบุเป็นค่าเดียวหรือระบุเป็นช่วงก็ได้
- (5) **การตอบสนองความเสี่ยง (Risk Response)** หมายถึง กระบวนการที่ใช้ในการบริหารจัดการต่อความเสี่ยงที่ยังเหลืออยู่หลังจากมีมาตรการควบคุมความเสี่ยงในการดำเนินงานตามปกติ
- (6) **การบริหารความเสี่ยงทั่วทั้งองค์กร (Enterprise Risk Management)** เป็นการให้กรอบการบริหารความเสี่ยงสำหรับคณะกรรมการ ผู้บริหารและบุคลากรทุกระดับในองค์กรในการบริหารจัดการกับความเสี่ยงที่เผชิญอยู่ รวมถึงความเสี่ยงที่อาจเกิดขึ้นในอนาคต โดย

คณะกรรมการบริษัท มีบทบาทในการควบคุมดูแลซึ่งหมายความรวมถึง การกำกับดูแลและวัฒนธรรม, กลยุทธ์และการกำหนดวัตถุประสงค์, ผลการปฏิบัติงาน, สารสนเทศ การสื่อสารและการรายงาน ตลอดจนการสอบทานและการทบทวนแนวปฏิบัติเพื่อปรับปรุงผลการปฏิบัติงานของกิจการให้ดีขึ้น สนับสนุนการสร้างคุณค่าของกิจการและป้องกันไม่ให้เกิดต่ำลง รวมทั้งกำหนดระดับความเสี่ยงที่ยอมรับได้สำหรับองค์กรด้วย

ผู้บริหาร เป็นผู้รับผิดชอบโดยรวมในนำกระบวนการบริหารความเสี่ยงไปใช้ในกิจการ รวมถึงเพิ่มการสื่อสารกับคณะกรรมการบริษัทและผู้มีส่วนได้เสียเกี่ยวกับการนำการบริหารความเสี่ยงองค์กรมาใช้เพื่อช่วยในการกำหนดแผนงานเพื่อให้สอดคล้องกับกลยุทธ์และวัตถุประสงค์ขององค์กร

พนักงานทุกระดับ ร่วมสร้างวัฒนธรรมและตระหนักถึงความเสี่ยงในการปฏิบัติงานประจำวันและหน้าที่ที่ได้รับมอบหมาย สนับสนุนนโยบายความเสี่ยงขององค์กร

- (7) **การควบคุม (Control)** หมายถึง นโยบายและวิธีปฏิบัติที่จะช่วยให้มั่นใจว่า ได้มีการดำเนินการตามแนวทางการลดระดับความเสี่ยงหรือควบคุมให้อยู่ในระดับที่กำหนดไว้ กิจกรรมการควบคุมเกิดขึ้นในทุกระดับ ทุกหน้าที่งาน และทั่วทั้งองค์กร ประกอบด้วยกิจกรรมที่แตกต่างกันไปแบ่งได้เป็น 4 ประเภท คือ
- (ก) การควบคุมแบบป้องกัน (Preventive Control) เป็นการควบคุมเพื่อป้องกันหรือลดความเสี่ยง ความเสียหายจากความผิดพลาดที่อาจเกิดขึ้น เช่น การอนุมัติ การแบ่งแยกหน้าที่การทำงาน การควบคุมการเข้าถึงทรัพย์สิน เป็นต้น
 - (ข) การควบคุมแบบค้นพบ (Detective Control) เป็นการควบคุมเพื่อค้นพบความเสียหายหรือความผิดพลาดที่เกิดขึ้นแล้ว เช่น การสอบทาน การสอบย้อนอด การตรวจนับ เป็นต้น
 - (ค) การควบคุมแบบส่งเสริม (Directive Control) เป็นวิธีการควบคุมที่ส่งเสริมหรือกระตุ้นให้เกิดความสำเร็จตามวัตถุประสงค์ที่ต้องการ เช่น การให้รางวัลแก่ผู้มีผลงานดี
 - (ง) การควบคุมแบบแก้ไข (Corrective Control) เป็นวิธีการควบคุมที่กำหนดขึ้นเพื่อแก้ไขความผิดพลาดที่เกิดขึ้นให้ถูกต้อง ไม่ให้เกิดข้อผิดพลาดซ้ำอีกในอนาคต

1.3 ประโยชน์ของการบริหารความเสี่ยง

- (1) ขยายขอบเขตของโอกาส โดยผู้บริหารสามารถระบุถึงโอกาสสำหรับกิจการและความท้าทายที่มีลักษณะเฉพาะทั้งในปัจจุบันและอนาคต โดยพิจารณาความน่าจะเป็นที่สมเหตุสมผลของความเสี่ยงทั้งแง่บวกและแง่ลบ
- (2) ลดขนาดหรือความรุนแรงของผลกระทบจากสิ่งที่ไม่ถึงในอนาคต ในขณะที่เดียวกันอาจเพิ่มผลลัพธ์เชิงบวกสำหรับโอกาสได้
- (3) ระบุและบริหารจัดการความเสี่ยงที่มีความสำคัญได้ทันเวลา
- (4) ช่วยลดความแปรปรวนของผลการปฏิบัติงาน นำกลยุทธ์องค์กรไปใช้ในการปฏิบัติงานให้ประสบความสำเร็จ
- (5) ปรับปรุงการใช้ทรัพยากร การได้มาซึ่งสารสนเทศด้านความเสี่ยงที่เพียงพอทำให้ผู้บริหารสามารถประเมินความต้องการทรัพยากรในภาพรวมและช่วยให้จัดสรรทรัพยากรได้อย่างเหมาะสม

บทที่ 2

การบริหารความเสี่ยงตามแนวทาง COSO ERM 2017

2.1 หลักการสำคัญในการบริหารความเสี่ยงตามแนวทาง COSO ERM 2017

กรอบการบริหารความเสี่ยงขององค์กรที่ได้รับการยอมรับว่าเป็นแนวทางในการส่งเสริมการบริหารความเสี่ยงและเป็นหลักปฏิบัติที่เป็นสากล คือกรอบการบริหารความเสี่ยงสำหรับองค์กรของคณะกรรมการ COSO (Committee of Sponsoring Organization of the Treadway Commission) ที่มอบหมายให้ PricewaterhouseCoopers เป็นผู้เขียนกรอบการบริหารความเสี่ยงสำหรับองค์กร (Enterprise Risk Management Framework) ตามภาพ



รูปภาพ : กรอบการบริหารความเสี่ยงตามแนว COSO ERM 2017 (ที่มา www.coso.org)

2.2 การบริหารความเสี่ยงตามแนวทาง COSO ERM 2017

การบริหารความเสี่ยงขององค์กร – การบูรณาการร่วมกันกับกลยุทธ์และผลการปฏิบัติงาน เป็นกรอบการบริหารความเสี่ยงตามแนวทาง COSO ERM 2017 เพื่อสร้างความชัดเจนเกี่ยวกับความสำคัญของการบริหารความเสี่ยงขององค์กรในการวางแผนกลยุทธ์ และความสำคัญในการนำการบริหารความเสี่ยงขององค์กรไปใช้ร่วมกับการดำเนินงานตามปกติทั่วทั้งองค์กร (ทั้งนี้ เนื่องจากความเสี่ยงมีอิทธิพลต่อทุกแผนกและหน้าที่งาน อีกทั้งความเสี่ยงทำให้กลยุทธ์ต้องสอดคล้องกับผลการปฏิบัติงานในทุกแผนกและหน้าที่งาน)

กรอบโครงสร้างนี้เป็นชุดของหลักการที่แบ่งได้เป็น 5 องค์ประกอบ 20 หลักการที่สัมพันธ์กัน มีสาระสำคัญดังนี้

องค์ประกอบที่ 1 : การกำกับดูแลและวัฒนธรรม (Governance & Culture)

การกำกับดูแลกำหนดหน้าที่ขององค์กร เสริมสร้างความสำคัญ รวมทั้งกำหนดความรับผิดชอบในการควบคุมดูแลสำหรับการบริหารความเสี่ยงขององค์กร วัฒนธรรมที่เกี่ยวข้องกับคุณค่าทางจริยธรรม พฤติกรรมที่พึงประสงค์ และความเข้าใจในความเสี่ยงของกิจการ ประกอบด้วย 5 หลักการ คือ

- หลักการที่ 1 :** ควบคุมดูแลความเสี่ยงโดยคณะกรรมการ (Execute Board Risk Oversight) – คณะกรรมการบริษัททำหน้าที่ในการควบคุมดูแลกลยุทธ์และการกำกับดูแลเพื่อสนับสนุนผู้บริหารในการดำเนินการเพื่อบรรลุกลยุทธ์และวัตถุประสงค์ทางธุรกิจ
- หลักการที่ 2 :** จัดตั้งโครงสร้างดำเนินงาน (Establishes Operating Structures) - องค์กรจัดตั้งโครงสร้างดำเนินงาน เพื่อให้บรรลุกลยุทธ์และวัตถุประสงค์ทางธุรกิจ
- หลักการที่ 3 :** กำหนดวัฒนธรรมที่พึงประสงค์ (Defines Desired Culture) - องค์กรกำหนดพฤติกรรมที่พึงประสงค์ ซึ่งแสดงให้เห็นถึงลักษณะของวัฒนธรรมที่กิจการพึงประสงค์
- หลักการที่ 4 :** แสดงให้เห็นถึงการยึดมั่นต่อคุณค่าหลัก (Demonstrates Commitment to Core Values)
- หลักการที่ 5 :** ดึงดูด พัฒนาและรักษาบุคคลที่มีความสามารถ (Attracts, Develops, and Retains Capable Individuals) - องค์กรยึดมั่นที่จะสร้างทรัพยากรบุคคล เพื่อให้สอดคล้องกับกลยุทธ์และวัตถุประสงค์ทางธุรกิจ

องค์ประกอบที่ 2 : กลยุทธ์และการกำหนดวัตถุประสงค์ (Strategy & Objective-Setting)

กระบวนการวางแผนกลยุทธ์เป็นการทำงานร่วมกันของการบริหารความเสี่ยงขององค์กร กลยุทธ์และการกำหนดวัตถุประสงค์ องค์กรกำหนดระดับความเสี่ยงที่ยอมรับได้ให้สอดคล้องกับกลยุทธ์ วัตถุประสงค์ทางธุรกิจทำให้เกิดการดำเนินการตามกลยุทธ์ ในขณะที่เดียวกันก็ใช้เป็นเกณฑ์ในการระบุ ประเมิน และตอบสนองความเสี่ยง ประกอบด้วย 4 หลักการ ได้แก่

- หลักการที่ 6 :** วิเคราะห์บริบททางธุรกิจ (Analyzes Business Context) – องค์กรพิจารณาผลกระทบที่อาจเป็นไปได้ของบริบททางธุรกิจต่อภาพความเสี่ยง
- หลักการที่ 7 :** กำหนดระดับความเสี่ยงที่ยอมรับได้ (Defines Risk Appetite) - องค์กรกำหนดระดับความเสี่ยงที่ยอมรับได้ในบริบทของการสร้างคุณค่า การรักษาคุณค่า และการทำให้คุณค่าเกิดขึ้นจริง
- หลักการที่ 8 :** ประเมินกลยุทธ์ทางเลือก (Evaluates Alternative Strategies) – องค์กรประเมินกลยุทธ์ที่เป็นทางเลือกและผลกระทบที่อาจเกิดขึ้นต่อภาพความเสี่ยง
- หลักการที่ 9 :** กำหนดวัตถุประสงค์ทางธุรกิจ (Formulates Business Objectives) – องค์กรพิจารณาความเสี่ยงในขณะกำหนดวัตถุประสงค์ทางธุรกิจในระดับต่างๆ ที่สอดคล้องและสนับสนุนกับกลยุทธ์

องค์ประกอบที่ 3 : ผลการปฏิบัติงาน (Performance)

ความเสี่ยงที่อาจมีผลกระทบต่อความสำเร็จของกลยุทธ์และวัตถุประสงค์ทางธุรกิจจำเป็นต้องถูกระบุและประเมินความเสี่ยงจะต้องถูกจัดลำดับความสำคัญตามความรุนแรงในบริบทของระดับความเสี่ยงที่ยอมรับได้ ต่อจากนั้น องค์กรจึงคัดเลือกวิธีการตอบสนองความเสี่ยงและพิจารณาภาพรวมของค่าความเสี่ยงที่องค์กรรับไว้ ผลของกระบวนการข้างต้นนี้จะรายงานต่อผู้มีส่วนได้เสียสำคัญของความเสี่ยง

- หลักการที่ 10 :** ระบุความเสี่ยง (Identifies Risk) – องค์กรระบุความเสี่ยงที่อาจส่งผลกระทบต่อผลการปฏิบัติงานตามกลยุทธ์และวัตถุประสงค์ทางธุรกิจ
- หลักการที่ 11 :** ประเมินความรุนแรงของความเสี่ยง (Assesses Severity of Risk)
- หลักการที่ 12 :** จัดลำดับความสำคัญของความเสี่ยง (Prioritizes Risks) - องค์กรจัดลำดับความสำคัญของความเสี่ยง (เพื่อใช้เป็นเกณฑ์ในการเลือกวิธีการตอบสนองความเสี่ยง)
- หลักการที่ 13 :** นำวิธีการตอบสนองความเสี่ยงไปปฏิบัติ (Implements Risk Responses) - องค์กรระบุและเลือกวิธีการตอบสนองความเสี่ยง

หลักการที่ 14 : พัฒนาภาพรวมความเสี่ยง (Develops Portfolio View) – องค์กรพัฒนาและประเมินภาพรวม
ของความเสี่ยง

องค์ประกอบที่ 4 : การสอบทานและแก้ไขปรับปรุง (Review & Revision)

ทำได้โดยการสอบทานผลการปฏิบัติงานของกิจการ องค์กรจะสามารถพิจารณาได้ว่าองค์ประกอบของการบริหาร
ความเสี่ยงขององค์กรทำหน้าที่ได้ดีเพียงใดในช่วงที่ผ่านมาและเมื่อเกิดการเปลี่ยนแปลงที่สำคัญ รวมทั้งมีสิ่งใดที่
จำเป็นต้องมีการแก้ไขปรับปรุง

หลักการที่ 15 : ประเมินการเปลี่ยนแปลงที่สำคัญ (Assess Substantial Change) – องค์กรระบุและประเมินการ
เปลี่ยนแปลงที่อาจส่งผลกระทบต่อกลยุทธ์และวัตถุประสงค์ทางธุรกิจ

หลักการที่ 16 : สอบทานความเสี่ยงและผลการปฏิบัติงาน (Reviews Risk and Performance)

หลักการที่ 17 : พยายามปรับปรุงการบริหารความเสี่ยงขององค์กรอย่างต่อเนื่อง (Pursues Improvement in
Enterprise Risk Management) – องค์กรพยายามปรับปรุงการบริหารความเสี่ยงขององค์กร
อย่างต่อเนื่อง

องค์ประกอบที่ 5 : สารสนเทศ การสื่อสารและการรายงาน (Information, Communication, & Reporting

การบริหารความเสี่ยงขององค์กรจำเป็นต้องมีกระบวนการที่ต่อเนื่องเพื่อการได้มาและการใช้สารสนเทศที่จำเป็น
ร่วมกัน ทั้งสารสนเทศจากแหล่งภายในและภายนอกซึ่งไหลเวียนอยู่ทั่วทั้งองค์กร ประกอบด้วย 3 หลักการ ได้แก่

หลักการที่ 18 : ใช้ประโยชน์จากสารสนเทศและเทคโนโลยี (Leverages Information and Technology) –

องค์กรใช้ประโยชน์จากระบบสารสนเทศและเทคโนโลยีของกิจการเพื่อสนับสนุนการบริหารความ
เสี่ยงขององค์กร

หลักการที่ 19 : สื่อสารสารสนเทศด้านความเสี่ยง (Communication Risk Information) - องค์กรใช้ช่องทางการ
สื่อสารต่างๆ เพื่อสนับสนุนการบริหารความเสี่ยงขององค์กร

หลักการที่ 20 : รายงานความเสี่ยง วัฒนธรรมและผลการปฏิบัติงาน (Reports on Risk, Culture, and
Performance) - องค์กรรายงานความเสี่ยง วัฒนธรรม และผลการปฏิบัติงานในระดับต่างๆ
ครอบคลุมทั้งองค์กร

บทที่ 3

การบริหารความเสี่ยงของ บริษัท ทีซีเอ็ม คอร์ปอเรชั่น จำกัด (มหาชน)

3.1 โครงสร้างการบริหารความเสี่ยงของ บริษัท ทีซีเอ็ม คอร์ปอเรชั่น จำกัด (มหาชน)

โครงสร้างการบริหารความเสี่ยงของบริษัท ประกอบด้วย คณะกรรมการบริษัท คณะกรรมการบริหารความเสี่ยง และ คณะทำงานบริหารความเสี่ยง มีหน้าที่ในการบริหารจัดการความเสี่ยงในทุกระดับของบริษัท รวมทั้งจัดการบริหารเหตุการณ์ ความเสี่ยงที่จะเกิดขึ้นจากทั้งปัจจัยภายในและภายนอก

คณะกรรมการบริษัท

คือคณะกรรมการของ บริษัท ทีซีเอ็ม คอร์ปอเรชั่น จำกัด (มหาชน) มีหน้าที่ให้ข้อเสนอแนะ และพิจารณาแต่งตั้งคณะกรรมการบริหารความเสี่ยง ตลอดจนให้ความเห็นชอบนโยบายการบริหารความเสี่ยง

คณะกรรมการบริหารความเสี่ยง

คณะกรรมการบริหารความเสี่ยงของ บริษัท ทีซีเอ็ม คอร์ปอเรชั่น จำกัด (มหาชน) ประกอบไปด้วย

- ประธานคณะกรรมการบริหารความเสี่ยง 1 คน
- กรรมการบริหารความเสี่ยง (อย่างน้อย) 4 คน
- เลขานุการคณะกรรมการ 1 คน (อาจเป็นคณะกรรมการด้วยก็ได้)

คณะกรรมการบริหารความเสี่ยงมีหน้าที่และความรับผิดชอบดังนี้

- (1) นำเสนอนโยบายด้านการบริหารความเสี่ยงต่อคณะกรรมการบริษัท เพื่อให้ความเห็นชอบและข้อเสนอแนะ
- (2) กำหนดแนวทางการบริหารความเสี่ยงให้ครอบคลุมทั้งองค์กร
- (3) ติดตามกระบวนการ ระบุและประเมินความเสี่ยงที่คณะกรรมการบริหารความเสี่ยงนำเสนอ
- (4) ประเมินและอนุมัติแผนการจัดการความเสี่ยง ที่คณะกรรมการบริหารความเสี่ยงได้เสนอ
- (5) นำเสนอรายงานการบริหารความเสี่ยงต่อคณะกรรมการบริษัท
- (6) กำกับดูแลประสิทธิภาพของการบริหารความเสี่ยง
- (7) ปฏิบัติงานอื่นๆ ในส่วนที่เกี่ยวข้องกับการบริหารความเสี่ยงภายในองค์กร

คณะทำงานบริหารความเสี่ยง

คณะทำงานบริหารความเสี่ยงของ บริษัท ทีซีเอ็ม คอร์ปอเรชั่น จำกัด (มหาชน) ประกอบไปด้วย

- ผู้จัดการฝ่ายทุกหน่วยงานในบริษัท

โดยคณะทำงานบริหารความเสี่ยงมีหน้าที่และความรับผิดชอบดังนี้

- (1) บริหารความเสี่ยงตามกรอบที่ระบุไว้ในคู่มือบริหารความเสี่ยง
- (2) ประเมินความเสี่ยงที่มีผลกระทบต่อบริษัท โดยระบุปัจจัยทั้งภายในและภายนอก
- (3) จัดลำดับความเสี่ยง พร้อมทั้งจัดทำแผนการเพื่อป้องกัน หรือลดความเสี่ยงของบริษัท
- (4) นำเสนอรายงานการบริหารความเสี่ยงต่อคณะกรรมการบริหารความเสี่ยง
- (5) จัดวางระบบการบริหารความเสี่ยง โดยการนำระบบเทคโนโลยีสารสนเทศมาเชื่อมโยงด้วย
- (6) ปฏิบัติงานอื่นๆ ตามที่คณะกรรมการบริหารความเสี่ยงมอบหมาย

เลขานุการคณะกรรมการบริหารความเสี่ยง

เลขานุการคณะกรรมการบริหารความเสี่ยง มีหน้าที่รวบรวมความเสี่ยงและการบริหารความเสี่ยงแต่ละหน่วยงานเสนอต่อคณะกรรมการบริหารความเสี่ยง ประสานงานเพื่อให้มีการวิเคราะห์ ประเมินและจัดการความเสี่ยงตามแนวทางที่กำหนด

จัดทำรายงานการบริหารและนำเสนอรายงานต่อคณะกรรมการบริหารความเสี่ยง จัดทำและปรับปรุงคู่มือการบริหารความเสี่ยง และให้ความรู้แก่หน่วยงานต่างๆ ในองค์กรในเรื่องการบริหารความเสี่ยง

3.2 ขั้นตอนการจัดทำระบบบริหารความเสี่ยง

เป็นการวิเคราะห์ และจัดลำดับความเสี่ยง โดยพิจารณาจากการประเมินโอกาสที่จะเกิดความเสี่ยง (Likelihood) และ ความรุนแรงของผลกระทบ (Impact) จากเหตุการณ์ความเสี่ยงมีผลกระทบต่อการบรรลุวัตถุประสงค์ของหน่วยงานหรือของ องค์กร โดยอาศัยเกณฑ์มาตรฐานที่ได้กำหนดไว้ ประกอบด้วย 4 ขั้นตอน คือ

(1) การกำหนดเกณฑ์การประเมินมาตรฐาน

เป็นการกำหนดเกณฑ์ที่จะใช้ในการประเมิน ระดับโอกาสที่จะเกิดความเสี่ยง (Likelihood) ระดับความ รุนแรงของผลกระทบ (Impact) และระดับของความเสี่ยง (Degree of Risk) สำหรับการประเมินความเสี่ยงในการ ทำงานประจำวัน แต่ละหน่วยงานอาจกำหนดเกณฑ์ที่ใช้ในการประเมินของหน่วยงานขึ้น โดยเกณฑ์ดังกล่าวอาจ เป็นได้ทั้งเชิงปริมาณและเชิงคุณภาพ ทั้งนี้ขึ้นอยู่กับข้อมูลสภาพแวดล้อมในหน่วยงานและดุลยพินิจการตัดสินใจ ของฝ่ายบริหารของหน่วยงาน

สำหรับการประเมินความเสี่ยงของบริษัทให้ใช้หลักเกณฑ์ดังต่อไปนี้

- (ก) โอกาสในการเกิดเหตุการณ์ต่างๆ ว่ามีมากน้อยเพียงใด โดยแบ่งเป็น 5 ระดับ คือ สูงมาก สูง ปานกลาง ต่ำ และต่ำมาก แทนด้วยตัวเลข 5,4,3,2,1 ตามลำดับ
- (ข) ความรุนแรงของผลกระทบที่เกิดจากเหตุการณ์ต่างๆ ว่ามีมากน้อยเพียงใด โดยจัดระดับความรุนแรงออกเป็น 5 ระดับ คือ สูงมาก สูง ปานกลาง ต่ำ และต่ำมาก แทนด้วยตัวเลข 5,4,3,2,1 ตามลำดับ
- (ค) บริษัทไม่ยอมรับความเสี่ยงใดๆ ที่จะส่งผลกระทบต่อชื่อเสียง ภาพลักษณ์ของตราสินค้าหรือบริษัท

โอกาส / ความถี่ที่น่าจะเกิดขึ้น

| ระดับ | โอกาส | จำนวนครั้งที่เกิด | ความถี่ |
|-------|---------|--|--------------------------------------|
| 1 | น้อยมาก | ไม่เคยเกิดเลยในรอบ 1- 3 ปีที่ผ่านมา | มากกว่า 3 ปี ต่อครั้ง หรือไม่เคยเกิด |
| 2 | น้อย | เคยเกิด 1 ครั้งในรอบปีที่ผ่านมา | 1-3 ปี ต่อครั้ง |
| 3 | ปานกลาง | เคยเกิด 2-3 ครั้งในรอบปีที่ผ่านมา | 6 - 12 เดือน ต่อครั้ง |
| 4 | สูง | เคยเกิด 4-5 ครั้งในรอบปีที่ผ่านมา | 3 - 6 เดือน ต่อครั้ง |
| 5 | สูงมาก | เคยเกิดมากกว่า 5 ครั้งในรอบปีที่ผ่านมา | น้อยกว่า 3 เดือน ต่อครั้ง |

ระดับผลกระทบต่อครั้ง (ด้านกลยุทธ์)

| ระดับ | ผลกระทบ | เปรียบเทียบกับเป้าหมาย |
|-------|---------|--|
| 1 | ต่ำมาก | เบี่ยงเบนจากเป้าหมาย / แผนงาน / งบประมาณ $\leq 10\%$ |
| 2 | ต่ำ | เบี่ยงเบนจากเป้าหมาย / แผนงาน / งบประมาณ $> 10 - 15\%$ |
| 3 | ปานกลาง | เบี่ยงเบนจากเป้าหมาย / แผนงาน / งบประมาณ $> 15 - 20\%$ |
| 4 | สูง | เบี่ยงเบนจากเป้าหมาย / แผนงาน / งบประมาณ $> 20 - 25\%$ |
| 5 | สูงมาก | เบี่ยงเบนจากเป้าหมาย / แผนงาน / งบประมาณ $> 25\%$ |

ระดับผลกระทบต่อครั้ง (ด้านการเงิน)

| ระดับ | ผลกระทบ | ตัวเงิน (บาท) |
|-------|---------|--|
| 1 | ต่ำมาก | มีมูลค่าน้อยกว่าหรือเท่ากับ 10 ล้านบาท |

| | | |
|---|---------|---|
| 2 | ต่ำ | มีมูลค่ามากกว่า 10 ล้านบาทถึง 35 ล้านบาท |
| 3 | ปานกลาง | มีมูลค่ามากกว่า 35 ล้านบาทถึง 75 ล้านบาท |
| 4 | สูง | มีมูลค่ามากกว่า 75 ล้านบาทถึง 100 ล้านบาท |
| 5 | สูงมาก | มีมูลค่ามากกว่า 100 ล้านบาท |

ระดับผลกระทบต่อครั้ง (ด้านสิ่งแวดล้อม / สุขภาพ)

| ระดับ | ผลกระทบ | ด้านสิ่งแวดล้อม | ด้านความปลอดภัย |
|-------|---------|--|---|
| 1 | ต่ำมาก | สามารถแก้ไขหรือควบคุมได้ทันที | บาดเจ็บเล็กน้อย ไม่ต้องหยุดงาน |
| 2 | ต่ำ | ใช้เวลาแก้ไขไม่เกิน 1 สัปดาห์ | มีอาการบาดเจ็บ หยุดงานตั้งแต่ 1 – 3 วัน |
| 3 | ปานกลาง | ใช้เวลาแก้ไขนานกว่า 1 สัปดาห์ถึง 1 เดือน | มีอาการบาดเจ็บ หยุดงานตั้งแต่ 4 – 7 วัน |
| 4 | สูง | ใช้เวลาแก้ไขนานกว่า 1 เดือนถึง 6 เดือน | บาดเจ็บสาหัส ต้องพักรักษาตัวในโรงพยาบาล |
| 5 | สูงมาก | ใช้เวลาแก้ไขนานกว่า 6 เดือน | ทุพพลภาพหรือเสียชีวิต |

ระดับผลกระทบต่อครั้ง (ด้านภาพลักษณ์ / ชื่อเสียง)

| ระดับ | ผลกระทบ | ด้านกฎระเบียบ / กฎหมาย |
|-------|---------|--|
| 1 | ต่ำมาก | ไม่ได้รับผลกระทบ หรือแก้ไขให้ถูกต้องไม่เกิน 1 วัน |
| 2 | ต่ำ | ถูกปรับไม่เกิน 500,000 บาท หรือใช้เวลาแก้ไขไม่เกิน 3 วัน |
| 3 | ปานกลาง | ถูกปรับมากกว่า 500,000 – 1,000,000 บาท หรือใช้เวลาแก้ไขไม่เกิน 7 วัน |
| 4 | สูง | ถูกปรับมากกว่า 1,000,000 -3,000,000 บาท หรือถูกขึ้นเครื่องหมาย (ตลาดหลักทรัพย์ฯ) |
| 5 | สูงมาก | ถูกปรับมากกว่า 3,000,000 บาท หรือมีโทษทางอาญา หรือ ถูกขึ้นเครื่องหมาย SP |

(ง) ระดับความเสี่ยง (Degree of Risk) คือ ตัวชี้วัดที่ใช้กำหนดความสำคัญของความเสี่ยง ค่าระดับความเสี่ยงได้จากการนำโอกาสที่จะเกิดและผลกระทบของความเสี่ยงมาพิจารณาร่วมกัน ดังนี้

$$\text{ความเสี่ยง} = \text{ระดับโอกาสที่จะเกิดความเสี่ยง} \times \text{ระดับผลกระทบที่เกิดขึ้น}$$

(2) การกำหนดวัตถุประสงค์ (Objective Setting)

การกำหนดวัตถุประสงค์เพื่อให้ทราบขอบเขตการดำเนินงานในแต่ละระดับและสามารถวิเคราะห์ความเสี่ยงที่จะเกิดขึ้นได้ครบถ้วน การกำหนดวัตถุประสงค์ของบริษัทควรมีความสอดคล้องกับเป้าหมายเชิงกลยุทธ์และความเสี่ยงที่บริษัทยอมรับได้ สำหรับในระดับฝ่าย การกำหนดวัตถุประสงค์จะต้องสอดคล้องหรือเป็นไปในทิศทางเดียวกับวัตถุประสงค์ของบริษัทฯ เพื่อให้วัตถุประสงค์ในภาพรวมบรรลุเป้าหมาย โดยการกำหนดวัตถุประสงค์จะต้องคำนึงถึงหลัก SMART ด้วย

(3) การระบุความเสี่ยง / เหตุการณ์ความเสี่ยง (Identify Risks)

ในการระบุความเสี่ยง เป็นการพิจารณาว่ามีสิ่งใดหรือเหตุการณ์ใดที่อาจจะเป็นอุปสรรคและทำให้การดำเนินงานไม่ประสบความสำเร็จตามวัตถุประสงค์หรือเป้าหมายทั้งในระดับองค์กรและระดับกิจกรรม โดยควรเน้นค้นหาความเสี่ยงจากงาน/โครงการ/ กิจกรรม/ กระบวนการที่มีความสำคัญและเป็นงานหลักขององค์กร

เหตุการณ์ความเสี่ยงอาจหาได้จากกระบวนการความคิดเห็นของบุคลากรในฝ่ายต่าง ๆ ของหน่วยงาน / คณะกรรมการบริหารความเสี่ยง หรือการสัมภาษณ์บุคลากรหรือผู้เชี่ยวชาญในสายงาน หรือจากการวิเคราะห์ ขั้นตอนการปฏิบัติงานในแต่ละขั้นตอนที่สำคัญ เป็นต้น ทั้งนี้สาเหตุของความเสี่ยงที่ระบุควรเป็นสาเหตุที่แท้จริง เพื่อนำมาวิเคราะห์และกำหนดมาตรการลดความเสี่ยงในภายหลังได้อย่างถูกต้อง

(4) การประเมินความเสี่ยง

เป็นการนำความเสี่ยงและปัจจัยเสี่ยงแต่ละปัจจัยที่ระบุไว้มาประเมินระดับของโอกาสที่จะเกิดเหตุการณ์ความเสี่ยง (Likelihood) และประเมินระดับความรุนแรงหรือมูลค่าความเสียหาย (Impact) จากความเสี่ยง โดยผู้ประเมินควรเป็นผู้มีความรู้ ความชำนาญในด้านนั้นๆ หรืออาจใช้คะแนนเสี่ยงข้างมากจากที่ประชุม หรือให้ผู้เข้าประชุมเป็นผู้ให้คะแนนแล้วนำคะแนนนั้นมาหาค่าเฉลี่ยก็ทำได้

(5) การวิเคราะห์ความเสี่ยงและการจัดลำดับ

เมื่อหน่วยงานพิจารณาระดับของโอกาส / ความถี่ที่จะเกิดเหตุการณ์ (Likelihood) และความรุนแรงของผลกระทบ (Impact) ของแต่ละปัจจัยเสี่ยงแล้ว ให้นำผลที่ได้มาคำนวณเพื่อพิจารณาว่าความเสี่ยงนั้นอยู่ในระดับใดในตารางระดับความเสี่ยง ซึ่งจะช่วยให้องค์กรทราบว่ามีความเสี่ยงใดเป็นความเสี่ยงสูงสามารถจัดลำดับความเสี่ยงที่จะต้องบริหารจัดการก่อน สามารถกำหนดการควบคุมความเสี่ยงได้อย่างเหมาะสม ช่วยให้องค์กรสามารถวางแผนและจัดสรรทรัพยากรได้อย่างถูกต้องภายใต้งบประมาณ กำลังคน หรือเวลาที่มีจำกัด

| สี | ความหมาย | ระดับความเสี่ยง |
|----------|-------------------|---|
| สีแดง | ความเสี่ยงสูงมาก | ตั้งแต่ 16 – 25 |
| สีส้ม | ความเสี่ยงสูง | ตั้งแต่ 12 – 15 |
| สีเหลือง | ความเสี่ยงปานกลาง | ตั้งแต่ 8 – 10 หรือ Impact หรือ Likelihood (อย่างใดอย่างหนึ่ง) มีระดับ 4 ขึ้นไป |
| สีเขียว | ความเสี่ยงต่ำ | ตั้งแต่ 4 – 6 |
| สีขาว | ความเสี่ยงต่ำมาก | ตั้งแต่ 1 - 3 |

ตารางระดับความเสี่ยง

หลังจากจัดลำดับความเสี่ยงที่ต้องบริหารจัดการก่อนได้แล้ว คณะทำงานอาจสรุปภาพรวมของความเสี่ยงทั้งหมดในรูปของแผนภาพ Heat Map เพื่อนำเสนอผู้บริหารระดับสูงได้เห็นถึงภาพรวมความเสี่ยงในองค์กร

| | | | | | | |
|-----------------------|---|----------------------------------|---|---|---|---|
| ระดับผลกระทบ (Impact) | 5 | | | | | |
| | 4 | | | | | |
| | 3 | | | | | |
| | 2 | | | | | |
| | 1 | | | | | |
| | | 1 | 2 | 3 | 4 | 5 |
| | | ระดับโอกาสที่จะเกิด (Likelihood) | | | | |

แผนผังความเสี่ยงในรูปของ Heat Map

(6) การจัดทำทะเบียนความเสี่ยง (Risk Profile)

เมื่อได้ระดับความเสี่ยงทั้งหมดมาแล้ว คณะทำงานควรจัดทำทะเบียนความเสี่ยง (Risk Profile) เพื่อใช้เป็นแหล่งอ้างอิงสำหรับการบริหารจัดการความเสี่ยงในองค์กรโดยใช้ Template ตามรูปด้านล่าง สำหรับวิธีการระบุความเสี่ยงควรระบุสิ่งที่เป็เหตุการณที่มี หรืออาจมีผลกระทบต่อองค์กรไม่ว่าจะเป็นเหตุการณ์ที่ทำให้เกิดผลในทางบวกหรือทางลบ นอกจากนี้ คณะทำงานจึงควรระบุสาเหตุที่แท้จริง ที่ทำให้เกิดหรืออาจเกิดเหตุการณ์นั้นๆ เพื่อให้คณะทำงานระบุมাত্রการหรือการควบคุมที่สอดคล้องได้อย่างถูกต้อง

TCM Corporation Risk Profile (updated February 2023)

| ลำดับ | ความเสี่ยง | ปัจจัยเสี่ยง (Risk Factor) | การควบคุมปัจจุบัน | คะแนนหลังการควบคุม | | | ผู้รับผิดชอบ |
|-------|------------------------------|-----------------------------------|---|--------------------|---------|--------|--------------|
| | | | | โอกาส | ผลกระทบ | คะแนน | |
| 2 | ความผันผวนของอัตราแลกเปลี่ยน | ภาระการจ่ายชำระเงินสกุลต่างประเทศ | - กลุ่ม Flooring ลดความผันผวนจากอัตราแลกเปลี่ยนด้วยการจอง Forward ทุกครั้งที่มีการเกิดขึ้นเพื่อลดความผันผวนของค่าเงิน - สำหรับกลุ่ม Living ได้ทำ fix forward วงเงินล่วงหน้า รวมถึงการทำสัญญาซื้อ-ขายกับผู้ผลิตในระยะยาวขึ้น * สำหรับ TCML มีทั้งดอกเบี้ยรับและดอกเบี้ยจ่าย ซึ่งเป็นสกุลเงินเดียวกัน จึงไม่มีผลกระทบต่ออัตราแลกเปลี่ยน | 4 5 | 2 1 | 8 5 | ฝ่ายบริหาร |

Template สำหรับจัดทำ Risk Profile

3.3 การจัดการและจัดทำแผนบริหารความเสี่ยง (Risk Responses)

หลังจากประเมินความเสี่ยงและจัดลำดับความสำคัญของความเสี่ยงแล้วจะมีการกำหนดมาตรการตอบสนองความเสี่ยงหรือแผนการจัดการความเสี่ยง คือการหาวิธีที่เหมาะสมสำหรับจัดการแต่ละความเสี่ยงที่ยังหลงเหลืออยู่ กลยุทธ์สำหรับจัดการความเสี่ยงมี 4 แบบรวมเรียกว่า 4T'S STRATEGIES

(1) **Take** – การยอมรับความเสี่ยง (Risk Acceptance) เป็นการยอมรับความเสี่ยงที่ยังเหลืออยู่เนื่องจากค่าใช้จ่ายในการจัดการหรือสร้างระบบควบคุมอาจมีมูลค่าสูงกว่าผลลัพธ์ที่ได้ แต่ก็ควรมีมาตรการติดตามและดูแล เช่น การกำหนดระดับของผลกระทบที่ยอมรับได้ เตรียมแผนการตั้งรับ/จัดการความเสี่ยง เป็นต้น

(2) **Treat** – การลด/ควบคุมความเสี่ยง (Risk Reduction/Control) เป็นการออกแบบระบบควบคุมเพิ่มเติม หรือแก้ไขปรับปรุงระบบควบคุมเพื่อลดความรุนแรงของความเสี่ยงที่ยังเหลืออยู่ โดยอาจลดผลกระทบหรือโอกาสเกิดเหตุการณ์นั้น เช่น ติดตั้งอุปกรณ์ความปลอดภัย ฝึกอบรมเพื่อพัฒนาทักษะวางมาตรการเชิงรุก เป็นต้น

(3) **Terminate** – การหลีกเลี่ยงความเสี่ยง (Risk Avoidance) เป็นการหยุดหรือเปลี่ยนแปลงกิจกรรมที่เป็นสาเหตุของความเสี่ยงนั้น เช่น งดทำขั้นตอนที่ไม่จำเป็นและจะนำมาซึ่งความเสี่ยง ปรับเปลี่ยนรูปแบบการทำงาน ลดการลงทุน เป็นต้น

(4) **Transfer** – การกระจาย/โอนความเสี่ยง (Risk Sharing/Spreading) เป็นการกระจายทรัพย์สินหรือกระบวนการต่าง ๆ เพื่อลดความเสี่ยงจากการสูญเสีย เช่น การประกันทรัพย์สินเพื่อโอนความเสี่ยงไปยังบริษัทประกัน การจ้างบริษัทภายนอกให้ทำงานบางส่วนแทน การทำสำเนาเอกสารหลายๆ ชุด การกระจายที่เก็บทรัพย์สินมีค่า เป็นต้น

จากนั้นทำการคิดแผนการจัดการที่สาเหตุของความเสี่ยงเหล่านั้น โดยดูว่ามาตรการควบคุมที่มีอยู่สามารถจัดการกับสาเหตุนั้นได้อย่างเพียงพอหรือไม่ หรือต้องมีมาตรการควบคุมเพิ่มเติมเพื่อจัดการกับความเสี่ยงที่ยังเหลืออยู่ โดยที่แผนการจัดการเพียงแผนเดียวอาจช่วยแก้ไขปัญหาคือหลายสาเหตุหรือช่วยจัดการความเสี่ยงอื่นก็ได้ และในขณะเดียวกัน สาเหตุใดสาเหตุหนึ่งก็อาจมีแผนจัดการมากกว่า 1 แผน ได้เช่นกัน

อย่างไรก็ตามไม่มีกฎตายตัวว่า ควรจะทำแผนใดบ้าง เพราะขึ้นกับความเหมาะสมและความพร้อมขององค์กรเป็นหลัก การเลือกแผนมาใช้ควรคำนึงถึงหลักต่าง ๆ ดังนี้

- (ก) แผนการจัดการความเสี่ยงที่ดีควรกระทำได้เร็ว ใช้งบประมาณน้อยและมีประสิทธิภาพในการลด ควบคุม หรือป้องกันความเสี่ยงได้อย่างเห็นผล
- (ข) พึงระวังว่าแผนจัดการความเสี่ยงต้องไม่ก่อให้เกิดความเสียหายอื่นตามมา หรือทำให้งานหยุดชะงัก

3.4 การรายงานและติดตามผล

เป็นการติดตามผลภายหลังจากได้ดำเนินการตามแผนการบริหารความเสี่ยงแล้ว เพื่อให้มั่นใจว่าแผนการบริหารความเสี่ยงนั้นมีประสิทธิภาพ การรายงานและการติดตามผลมีความจำเป็นและมีประโยชน์ต่อการบริหารความเสี่ยงเพราะจะทำให้ทราบว่า

- (1) แผนจัดการความเสี่ยงถูกนำไปใช้อย่างถูกต้องและมีประสิทธิภาพเพียงใด
- (2) ทำให้ทราบถึงข้อผิดพลาดที่อาจเกิดขึ้นหลังจากใช้แผนจัดการความเสี่ยง
- (3) ทำให้สามารถปรับปรุงแก้ไขแผนจัดการความเสี่ยงให้สอดคล้องกับสถานการณ์ที่เปลี่ยนแปลงไป หรือกรณีที่แผนเดิมไม่มีประสิทธิภาพ
- (4) มีการรายงานต่อผู้บริหารที่ได้รับมอบหมายเป็นรายไตรมาส

บริษัทได้กำหนดแนวทางการประเมินผลการปฏิบัติงานใน 2 ลักษณะ คือ

(1) **การประเมินผลระหว่างการปฏิบัติงาน (Ongoing Monitoring)** โดยจะประเมินผลการปฏิบัติงานตามแผนบริหารความเสี่ยง เพื่อติดตามว่ากระบวนการต่าง ๆ ได้มีการดำเนินการตามมาตรการ/กิจกรรมควบคุมที่ได้กำหนดไว้หรือไม่ และสามารถลดความเสี่ยงที่เกิดขึ้นหรืออาจจะเกิดขึ้นได้หรือไม่ หรือมีเหตุการณ์ สถานการณ์ ความเปลี่ยนแปลงเกิดขึ้นนอกเหนือจากที่ได้คาดการณ์ไว้ แล้วจึงนำเสนอต่อคณะกรรมการบริหารความเสี่ยงและคณะทำงานบริหารความเสี่ยง เพื่อปรับแผนบริหารความเสี่ยงและดำเนินการปรับแก้ไขได้อย่างทันที่ โดยความถี่ในการติดตามประเมินผลจากกิจกรรมควบคุมดำเนินการเป็นรายครึ่งปี และในกรณีพิเศษหากพบว่าการเปลี่ยนแปลงที่มีสาระสำคัญ อาจจะทำให้มีการประชุมคณะกรรมการบริหารความเสี่ยงเป็นกรณีพิเศษก็ได้

(2) **การประเมินผลเป็นรายครั้ง (Separate Evaluation)** เป็นการประเมินผลโดยการรายงานเมื่อสิ้นสุดระยะเวลาที่ได้กำหนดไว้หรือในกรณีพิเศษ โดยส่วนงานหลักที่รับผิดชอบบริหารจัดการความเสี่ยงใด ส่วนงานนั้นจะเป็นผู้รับผิดชอบในการประเมินประสิทธิภาพการบริหารความเสี่ยงของตนเอง ขอบเขตความถี่ในการประเมินจะขึ้นอยู่กับกำหนดการที่กำหนดไว้ โดยมีการประเมินผลดังนี้

- (ก) มีการปฏิบัติตามมาตรการ/กิจกรรมควบคุมที่ได้กำหนดไว้อย่างครบถ้วนสมบูรณ์ หรือไม่
- (ข) การปฏิบัติตามกิจกรรมควบคุมนั้น สามารถลดความเสี่ยงได้อย่างมีประสิทธิภาพ และประสิทธิผลหรือไม่

(ค) มีข้อบกพร่องหรือสถานการณ์ใด ๆ ที่มีผลกระทบต่อการบริหารความเสี่ยงที่ควรได้รับความสนใจ แก้ไข หรือปรับปรุงแก้ไขให้ดีขึ้นหรือไม่

นอกจากนี้ ควรกำหนดให้มีการประเมินความเสี่ยงซ้ำอีกอย่างน้อยปีละหนึ่งครั้ง เพื่อดูว่าความเสี่ยงใดอยู่ในระดับที่ยอมรับได้แล้ว หรือมีความเสี่ยงใหม่เพิ่มขึ้นมาอีกหรือไม่ โดยอาจกำหนดเป็นแผนดำเนินการรวมทั้งมีเครื่องมือที่ใช้เพื่อการรายงาน การติดตามผล การประเมินผลการบริหารความเสี่ยง ประกอบด้วย

- การจัดทำแผนผังเมทริกซ์แสดงระดับความเสี่ยง (Risk Matrix) จะเป็นการแสดงให้เห็นถึงระดับความเสี่ยงที่เกิดขึ้นทั้งในระดับองค์กร และระดับสำนัก/กลุ่มภารกิจ เพื่อใช้ในการตรวจติดตาม และประเมินการบริหารความเสี่ยง
- การจัดทำ Risk Profile และการจัดลำดับความเสี่ยง จะเป็นการแสดงให้เห็นถึงความเสี่ยงทั้งหมดโดยเรียงลำดับตามระดับความเสี่ยง จะเปลี่ยนแปลงไปตามมาตรการการจัดการความเสี่ยงที่ได้กำหนดไว้
- การรายงานการติดตามแนวทางการจัดการความเสี่ยง สามารถติดตามโดยใช้แบบฟอร์มรายงานการติดตามแนวทางการจัดการความเสี่ยง เพื่อใช้ในการติดตามมาตรการในการจัดการความเสี่ยงที่เพิ่มเติมตามช่วงเวลาเป็นรายเดือน หรือไตรมาส หรือตามความเหมาะสมโดยทำการระบุความคืบหน้าของการจัดการความเสี่ยง

ซึ่งจะเห็นได้ว่าการจัดทำระบบบริหารความเสี่ยงนั้น จะต้องกระทำอย่างต่อเนื่องและสม่ำเสมอ มีการตรวจสอบและติดตามเป็นระยะๆ จึงจะเกิดประโยชน์อย่างแท้จริง

3.5 ปัจจัยที่ทำให้การบริหารความเสี่ยงประสบผลสำเร็จ

- (1) การปฏิบัติตามกระบวนการบริหารความเสี่ยงที่ต่อเนื่องสม่ำเสมอ
- (2) การมีกระบวนการในการบริหารการเปลี่ยนแปลง
- (3) การสื่อสารที่มีประสิทธิภาพ
- (4) การวัดผลการบริหารความเสี่ยงซึ่งรวมทั้งการวัดความเสี่ยง
- (5) การฝึกอบรมและกลไกด้านทรัพยากรบุคคลเพื่อให้พนักงานทุกคนเข้าใจในกรอบและความรับผิดชอบของการบริหารความเสี่ยง
- (6) การติดตามกระบวนการบริหารความเสี่ยงด้วยการกำหนดวิธีที่เหมาะสม

3.6 ปัจจัยที่ทำให้การบริหารความเสี่ยงล้มเหลว

- (1) ขาดการสนับสนุนจากผู้บริหารระดับกลางและระดับสูง
- (2) ขาดวิสัยทัศน์ที่ชัดเจนในการวางแผนกลยุทธ์
- (3) ขาดการสื่อสารให้พนักงานทุกคนทราบถึงวิสัยทัศน์ และสิ่งที่กำลังจะเกิดขึ้นในอนาคต
- (4) ล้มเหลวในการสร้างทีมสนับสนุนที่มีอำนาจตั้งแต่ระดับบนจนถึงระดับกลาง
- (5) มองทุกอย่างเป็นอุปสรรค หรือผู้คนในองค์กรเป็นตัวสกัดกั้นการทำงานไปสู่วิสัยทัศน์
- (6) การกำหนดกลยุทธ์ให้องค์กรประสบความสำเร็จในระยะสั้นล้มเหลวจะทำให้ระยะยาวล้มเหลว

บทที่ 4

เบ็ดเตล็ด

(1) การแก้ไข ปรับปรุง เปลี่ยนแปลงเอกสารฉบับนี้ในทุกกรณี จะกระทำต่อเมื่อได้รับอนุมัติจาก คณะกรรมการบริษัทแล้วเท่านั้น

(2) คู่มือบริหารความเสี่ยงฉบับนี้ ให้มีผลใช้บังคับนับตั้งแต่วันที่ 26 พฤศจิกายน 2558 เป็นต้นไป จนกว่าจะมีการเปลี่ยนแปลงเป็นลายลักษณ์อักษรเป็นอย่างอื่น

โดยมติคณะกรรมการบริษัทครั้งที่ 5/2558 เมื่อวันที่ 25 พฤศจิกายน 2558



(นายพิมล ศรีวิกรม์)

ประธานกรรมการบริษัท