สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์
333/3 ถนนวิภาวดีรังสิต แขวงจอมพล
เขตจตุจักร กรุงเทพมหานคร 10900

www.sec.or.th
โทร : 0-2033-9999
แฟกซ์ : 0-2033-9660

20 ธันวาคม 2566

เรียน ผู้จัดการ

บริษัทหลักทรัพย์ทุกแห่ง

ผู้ประกอบธุรกิจสัญญาซื้อขายล่วงหน้าทุกแห่ง

นายกสมาคมบริษัทหลักทรัพย์ไทย

ที่ กลต.กธ.(ว) 59/2566 เรื่อง คู่มือการบริหารและจัดการความเสี่ยงสำหรับบริษัทหลักทรัพย์และผู้ประกอบธุรกิจสัญญาซื้อขายล่วงหน้า

สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ (“สำนักงาน ก.ล.ต.”) ได้จัดทำคู่มือการบริหารและจัดการความเสี่ยงสำหรับบริษัทหลักทรัพย์และผู้ประกอบธุรกิจสัญญาซื้อขายล่วงหน้า (รวมเรียกว่า “ผู้ประกอบธุรกิจ”) เพื่อให้ผู้ประกอบธุรกิจนำไปใช้เป็นแนวทางในการจัดให้มีระบบงาน การกำกับดูแล การบริหารความเสี่ยง และการควบคุมอย่างเป็นระบบ และเหมาะสมกับรูปแบบและกิจกรรมสำคัญของผู้ประกอบธุรกิจ เพื่อสร้างความเชื่อมั่นว่าผู้ประกอบธุรกิจจะสามารถให้บริการเพื่อรักษาประโยชน์ที่ดีที่สุดของลูกค้า มีการดำเนินงานที่เป็นธรรม มีประสิทธิภาพต่อเนื่องและรักษาความเป็นระเบียบเรียบร้อยของตลาดทุน รวมทั้งรับผิดชอบต่อการพัฒนาอย่างยั่งยืนของตลาดทุนและสังคมโดยรวมภายใต้สถานการณ์และความเสี่ยงในมิติต่าง ๆ และมีการนำไปใช้ตลอดทั้งองค์กร

คู่มือนี้จัดทำขึ้นโดยได้ศึกษาแนวทางของหน่วยงานกำกับดูแลทั้งในประเทศและต่างประเทศตลอดจนนำข้อคิดเห็นและข้อเสนอแนะของผู้แทนผู้ประกอบธุรกิจและสมาคมบริษัทหลักทรัพย์ไทยมาใช้ประกอบการพิจารณากำหนดแนวปฏิบัติที่สอดคล้องกับวัตถุประสงค์และแนวทางที่สำนักงาน ก.ล.ต. ใช้ในการกำกับดูแลผู้ประกอบธุรกิจตามระดับความเสี่ยง (Risk-Based Approach: RBA) ทั้งนี้ สำนักงาน ก.ล.ต. มีนโยบายที่จะกำกับดูแล หรือบังคับใช้กฎหมายกับผู้ประกอบธุรกิจ โดยเลือกเครื่องมือที่สมเหตุสมผล ได้สัดส่วน (proportionate) กับลักษณะการกระทำที่เป็นความเสี่ยงภัย (harm) ต่อผู้ลงทุนหรือตลาดทุนโดยรวม และพฤติกรรมในการกระทำผิดของผู้ประกอบธุรกิจ

สำนักงาน ก.ล.ต. ขอนำส่งคู่มือนี้ และคาดหวังให้ผู้ประกอบธุรกิจนำไปทบทวนนโยบายและแนวทางปฏิบัติในการบริหารความเสี่ยงให้เป็นไปตามคู่มือดังกล่าว และรายงานผลการทบทวนต่อสำนักงาน ก.ล.ต. เป็นส่วนหนึ่งของรายงาน Compliance Report ประจำปี 2567 ทั้งนี้ หากผู้ประกอบธุรกิจมิได้นำหลักการใดไปปรับใช้ หรือยังปรับใช้ไม่แล้วเสร็จ ให้อธิบาย (apply or explain) โดยมีมติของคณะกรรมการบริษัท หรือคณะกรรมการตรวจสอบประกอบด้วย

สำนักงาน ก.ล.ต. เชื่อว่า การปฏิบัติตามคู่มือนี้ นอกจากจะช่วยให้ผู้ประกอบธุรกิจดำเนินงานให้เป็นไปตามวัตถุประสงค์เพื่อรักษาประโยชน์ของลูกค้า เสริมสร้างความน่าเชื่อถือของผู้ประกอบธุรกิจ และรักษาความเป็นธรรมในตลาดทุนโดยรวมแล้ว ยังเป็น self-discipline ที่ช่วยลดโอกาสที่จะมีการกระทำฝ่าฝืนกฎหมายหรือกฎเกณฑ์ที่เกี่ยวข้อง และหากยังพบการกระทำผิด ขอให้ผู้ประกอบธุรกิจรายงานต่อสำนักงาน ก.ล.ต. โดยการรายงานและการแสดงว่ามีระบบในการควบคุมบริหารความเสี่ยงดังกล่าวอย่างเพียงพอแล้ว จะได้รับการพิจารณาในทางที่เป็นคุณแก่ผู้ประกอบธุรกิจในการเลือกเครื่องมือกำกับดูแลและบังคับใช้กฎหมายที่เหมาะสม

จึงเรียนมาเพื่อโปรดทราบและถือปฏิบัติ

ขอแสดงความนับถือ

(นางพรอนงค์ บุษราตระกูล)
เลขาธิการ

สิ่งที่ส่งมาด้วย คู่มือการบริหารและจัดการความเสี่ยงสำหรับบริษัทหลักทรัพย์และผู้ประกอบธุรกิจสัญญาซื้อขายล่วงหน้า

ฝ่ายกำกับธุรกิจตัวกลาง
โทรศัพท์/โทรสาร 0-2033-9768, 0-2033-9551

คู่มือการบริหารและจัดการความเสี่ยง
สำหรับบริษัทหลักทรัพย์และผู้ประกอบธุรกิจสัญญาซื้อขายล่วงหน้า

สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์

มกราคม 2567

คำนำ

สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ (“สำนักงาน ก.ล.ต.”) ได้จัดทำคู่มือการบริหารและจัดการความเสี่ยงฉบับนี้ขึ้น เพื่อให้บริษัทหลักทรัพย์และผู้ประกอบธุรกิจสัญญาซื้อขายล่วงหน้า (รวมเรียกว่า “ผู้ประกอบธุรกิจ”) นำไปใช้เป็นแนวทางในการจัดให้มีระบบงาน การกำกับดูแล การบริหารความเสี่ยง และการควบคุมอย่างเป็นระบบ และเหมาะสมกับรูปแบบและกิจกรรมที่เกี่ยวข้องกับการประกอบธุรกิจ เพื่อสร้างความเชื่อมั่นว่า ผู้ประกอบธุรกิจสามารถให้บริการเพื่อรักษาประโยชน์ที่ดีที่สุดของลูกค้า มีการดำเนินงานที่เป็นธรรม มีประสิทธิภาพ ต่อเนื่อง และรักษาความเป็นระเบียบเรียบร้อยของตลาดทุน รวมทั้งรับผิดชอบต่อการพัฒนาอย่างยั่งยืนของตลาดทุนและสังคมโดยรวม ภายใต้สถานการณ์ และความเปลี่ยนแปลงต่าง ๆ

สำนักงาน ก.ล.ต. ขอขอบคุณผู้แทนผู้ประกอบธุรกิจที่ได้ร่วมให้ความเห็นและข้อเสนอแนะประกอบการจัดทำคู่มือฉบับนี้ และขอรับข้อเสนอแนะเพื่อพัฒนาปรับปรุงคู่มือนี้ให้เป็นประโยชน์และเหมาะสมยิ่งขึ้นต่อไป ผ่านฝ่ายกำกับธุรกิจตัวกลาง อีเมล seccom@sec.or.th

รายนามผู้แทนผู้ประกอบธุรกิจและสมาคมบริษัทหลักทรัพย์ไทยเพื่อการให้ความเห็น (Reading Committee)

คุณอารีย์ เติมวัฒนาภักดี	บริษัทหลักทรัพย์ กรุงไทย เอ็กซ์สปริง จำกัด
คุณนิติพร แสงจันทร์	บริษัทหลักทรัพย์ กรุงไทย เอ็กซ์สปริง จำกัด
คุณณากร ลัมภเวส	บริษัทหลักทรัพย์ ซีจีเอส-ซีไอเอ็มบี (ประเทศไทย) จำกัด
คุณอภิชาติ จงสงวนประดับ	ธนาคารเกียรตินาคินภัทร จำกัด (มหาชน)
คุณเบญวรรณ แวนไดน์	บริษัทหลักทรัพย์ แมคควอรี (ประเทศไทย) จำกัด
คุณสุรเชษฐ์ อำนวยวิทยากุล	บริษัทหลักทรัพย์ เคจีไอ (ประเทศไทย) จำกัด (มหาชน)
คุณกัญญภัทร รังกุพันธุ์	บริษัทหลักทรัพย์ กสิกรไทย จำกัด (มหาชน)
คุณณัชณิชา บุญสุทานันท์	บริษัทหลักทรัพย์ ทิสโก้ จำกัด
คุณนธี สุทธิพันธ์พงศ์	บริษัทหลักทรัพย์ ทิสโก้ จำกัด
คุณณรงค์ โรจน์คุณารักษ์	สมาคมบริษัทหลักทรัพย์ไทย
คุณศรีวิไล สิทธิสงวนไทย	สมาคมบริษัทหลักทรัพย์ไทย

สารบัญ

หลักการ และสรุปสาระสำคัญ

1. วัตถุประสงค์

สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ (“สำนักงาน ก.ล.ต.”) คาดหวังให้ผู้ประกอบธุรกิจมีระบบงาน การกำกับดูแล การบริหารความเสี่ยง และการควบคุมอย่างเป็นระบบตามความเสี่ยงที่เกี่ยวข้องกับการประกอบธุรกิจ เพื่อสร้างความเชื่อมั่นว่า ผู้ประกอบธุรกิจมีความพร้อม และความสามารถที่จะรองรับสถานการณ์ความเปลี่ยนแปลงต่างๆ เพื่อให้การประกอบธุรกิจเป็นไปตามวัตุประสงค์ ดังนี้

(1) ให้บริการเพื่อตอบสนองความต้องการและประโยชน์ที่ดีที่สุดของลูกค้า

(2) มีฐานะการเงิน การดำเนินงาน และระบบรองรับการประกอบธุรกิจที่มีประสิทธิภาพ น่าเชื่อถือ

(3) คำนึงถึงผลกระทบต่อความเป็นระเบียบเรียบร้อยของระบบตลาดทุน (systemic risk) และรับผิดชอบต่อการพัฒนาอย่างยั่งยืนของตลาดทุน เศรษฐกิจ สังคม สิ่งแวดล้อม

2. ขอบเขตความครอบคลุม

ประกาศคณะกรรมการกำกับตลาดทุน ที่ ทธ. 35/2556 เรื่อง มาตรฐานการประกอบธุรกิจ โครงสร้างการบริหารงาน ระบบงาน และการให้บริการของผู้ประกอบธุรกิจหลักทรัพย์ และผู้ประกอบธุรกิจสัญญาซื้อขายล่วงหน้า ลงวันที่ 6 กันยายน พ.ศ. 2556 กำหนดให้ผู้ประกอบธุรกิจมีระบบการบริหารและจัดการความเสี่ยงที่อาจเกิดขึ้นในทุกด้านอย่างรัดกุม โดยต้องมีมาตรการอย่างเพียงพอที่จะป้องกันและจัดการความเสี่ยงอย่างมีประสิทธิภาพ คู่มือนี้จึงได้วางแนวปฏิบัติเพิ่มเติม โดยคาดหวังให้ผู้ประกอบธุรกิจ มีวินัยในตนเอง (self-discipline) ในการจัดให้มีระบบการบริหารความเสี่ยงที่มีลักษณะ ดังนี้

- สอดคล้องกับลักษณะธุรกิจ (business model) และลักษณะธุรกรรม (significant activity) ของบริษัท
- มีโครงสร้าง และมีการกำหนดบทบาทหน้าที่ผู้รับผิดชอบที่ชัดเจน ตั้งแต่ระดับคณะกรรมการ ผู้บริหาร และผู้ปฏิบัติงาน โดยมีการตรวจสอบถ่วงดุลในลักษณะ 3 ประสาน (3-lines of defense)
- กำหนดความเสี่ยงโดยมองไปข้างหน้า (forward looking) และครอบคลุมมิติรอบด้านที่อาจกระทบต่อการดำเนินงานให้เป็นไปตามวัตถุประสงค์ตามข้อ 1 โดยอย่างน้อยให้ครอบคลุมความเสี่ยงด้านกลยุทธ์ ด้านการเปลี่ยนแปลงสภาพตลาด (market risk) ด้านเครดิต ด้านการดูแลลูกค้า (customer conduct risk) ด้านการดำเนินงานและเทคโนโลยี (Operation risk) รวมทั้งด้านฐานะการเงิน
- มีการกำกับดูแล (governance) การบริหารความเสี่ยง และการควบคุมที่ดี อย่างเพียงพอ เพื่อลดโอกาสและผลกระทบ ที่ความเสี่ยงเหล่านั้นจะต่อการดำเนินงานให้เป็นไปตามวัตถุประสงค์

- ครอบคลุมกระบวนการบริหารความเสี่ยงทั้งระบบ ตั้งแต่การกำหนดนโยบาย การวางแผน การติดตาม ปรับเปลี่ยนให้เหมาะสมกับสภาวการณ์ที่เปลี่ยนไป รวมทั้งมีการวางแผนสำรองหากเกิดเหตุการณ์วิกฤติหรือเสี่ยงสูง โดยมีการทดสอบความเพียงพอของระบบ และมีการฝึกซ้อมด้วย

3. แนวทางในการกำกับดูแลของสำนักงาน ก.ล.ต.

3.1 วัตถุประสงค์และแนวทางบริหารความเสี่ยงตามคู่มือนี้ สอดคล้องกับวัตถุประสงค์และแนวทางที่สำนักงาน ก.ล.ต. ใช้ในการกำกับดูแลผู้ประกอบธุรกิจตามระดับความเสี่ยง (Risk-Based Approach: RBA) โดยแนวทางปัจจุบัน ส่วนมากยังเป็นหลักการหรือแนวคิด และจะพัฒนาให้มีข้อมูลตัวชี้วัด (data driven) หรือการให้คะแนน (scoring) ในแต่ละมิติเพิ่มขึ้น โดยจะดำเนินการควบคู่ไปกับการปรับปรุงการนำส่งข้อมูล หรือรายงานของผู้ประกอบธุรกิจต่อสำนักงาน ก.ล.ต. ด้วย เพื่อให้สามารถติดตามความเสี่ยงของผู้ประกอบธุรกิจ และกำกับดูแลได้อย่างมีประสิทธิภาพยิ่งขึ้นต่อไป

3.2 เมื่อพบความเสี่ยงต่อการบรรลุวัตถุประสงค์ที่กล่าวตามข้อ 1 หรือพบการกระทำผิดกฎหมาย กฎเกณฑ์ที่เกี่ยวข้อง **สำนักงาน ก.ล.ต. มีนโยบายที่จะกำกับดูแล หรือบังคับใช้กฎหมายกับผู้ประกอบธุรกิจโดยเลือกเครื่องมือที่สมเหตุสมผล ได้สัดส่วน (proportionate) กับลักษณะการกระทำที่เป็นความเสี่ยง หรือความผิด และพฤติกรรมของผู้ประกอบธุรกิจในแต่ละกรณี** เพื่อป้องปรามไม่ให้เกิดการกระทำที่เป็นความเสี่ยงภัย (harm) ต่อผู้ลงทุน และตลาดทุนโดยรวม หรือการกระทำผิดกฎหมาย เช่น

(1) ความร้ายแรงของพฤติกรรม โดยพิจารณาจาก

- การมีระบบกำกับดูแล บริหารความเสี่ยง ก่อนเกิดการกระทำผิด
- แรงจูงใจ และพฤติกรรมในการกระทำผิด
- ผลกระทบต่อลูกค้า ความน่าเชื่อถือของบริษัท และตลาดทุน
- พฤติกรรมภายหลังการกระทำผิด เช่น การรายงานการกระทำผิด การหาสาเหตุ เพื่อแก้ไขปรับปรุงที่ต้นเหตุ การชดใช้เยียวยาลูกค้าที่เสียหายจากการกระทำผิด การดำเนินการกับบุคลากรที่เป็นเหตุให้กระทำผิด เป็นต้น

(2) มาตรการที่ใช้ในการกำกับดูแล และบังคับใช้กฎหมาย ซึ่งรวมถึงการดำเนินการอย่างใดอย่างหนึ่งหรือหลายอย่าง ตามความจำเป็นและสมควรแก่กรณี เช่น

- การให้ชี้แจง แก้ไข เปิดเผยข้อมูล จัดทำรายงานต่อผู้ที่เกี่ยวข้อง
- การเข้าตรวจสอบการดำเนินงาน
- การตักเตือน คาดโทษ เปิดเผยการตักเตือน คาดโทษต่อสาธารณชน

- การดำเนินการเปรียบเทียบปรับบริษัท และผู้บริหารที่เกี่ยวข้อง หรือกล่าวโทษเพื่อดำเนินคดีอาญาในชั้นศาล
- การกำหนดลักษณะต้องห้ามของผู้บริหาร การจำกัดการประกอบธุรกิจ
- การเสนอพัก เพิกถอนใบอนุญาต

4. ประโยชน์ในการปฏิบัติตามคู่มือนี้

สำนักงาน ก.ล.ต. คาดหวังให้ผู้ประกอบธุรกิจมี self-discipline ในการบริหารความเสี่ยงตามคู่มือนี้ ซึ่งนอกจากจะช่วยให้ผู้ประกอบธุรกิจดำเนินงานให้เป็นไปตามวัตถุประสงค์แล้ว ยังช่วยลดโอกาสที่จะมีการกระทำผิดฝ่าฝืนกฎหมายหรือกฎเกณฑ์ที่เกี่ยวข้อง และหากยังพบการกระทำผิด ขอให้ผู้ประกอบธุรกิจรายงานต่อสำนักงาน ก.ล.ต. โดยการรายงาน และการแสดงว่ามีการระบบในการควบคุม บริหารความเสี่ยงดังกล่าวอย่างเพียงพอแล้ว จะได้รับการพิจารณาในทางที่เป็นคุณแก่ผู้ประกอบธุรกิจ

1. นโยบายการบริหารความเสี่ยง

1.1 วัตถุประสงค์

บริษัทควรกำหนดนโยบายบริหารความเสี่ยง เพื่อกำหนดนโยบาย บทบาทความรับผิดชอบ และแนวทางในการบริหารความเสี่ยง โดยมีวัตถุประสงค์เพื่อปกป้อง (safeguard) ทรัพย์สินและประโยชน์ของลูกค้า ป้องกันความเสี่ยงในการดำเนินงานของบริษัท และรักษาไว้ซึ่งความน่าเชื่อถือของระบบตลาดทุนโดยรวม นโยบายบริหารความเสี่ยงที่บริษัทจัดทำ ต้องครอบคลุมวัตุประสงค์อย่างน้อย

(1) ปกป้องทรัพย์สินและประโยชน์ของลูกค้า

- ปกป้องทรัพย์สินของลูกค้า นโยบายที่จัดทำต้องครอบคลุมการรักษาความปลอดภัยของบัญชี ทรัพย์สิน ข้อมูลของลูกค้า จากการนำไปใช้โดยไม่ได้รับอนุญาต การจัดเก็บข้อมูลไม่ถูกต้อง การทุจริต การรั่วไหล การโจมตีทาง cyber
- ให้บริการอย่างเป็นธรรมโปร่งใส นโยบายที่จัดทำควรสนับสนุนให้เกิดการปฏิบัติต่อลูกค้าอย่างเป็นธรรมโปร่งใส เพื่อคุ้มครองลูกค้าจากการมีข้อมูลไม่ถูกต้อง ไม่เพียงพอประกอบการตัดสินใจลงทุน (misinformation) หรือลงทุนในราคาหรือต้นทุนที่ไม่เหมาะสม (mispricing) หรือไม่ตรงกับความต้องการ หรือความสามารถในการรับความเสี่ยงของลูกค้า
- การบริหารความเสี่ยงจากการลงทุน (risk exposure) ของลูกค้า นโยบายที่จัดทำควรสนับสนุนให้ผู้ประกอบธุรกิจให้คำแนะนำ ติดตามดูแล และมีเครื่องมือให้ลูกค้าบริหารความเสี่ยงจากการลงทุนได้อย่างเหมาะสม

(2) ป้องกันความเสี่ยงในการดำเนินงานของบริษัท

- ลดความเสี่ยงทางการเงิน นโยบายที่จัดทำควรครอบคลุมการกำหนด การบริหารความเสี่ยงในมิติต่าง ๆ ที่อาจกระทบทางการเงินต่อฐานะ สภาพคล่อง และการดำรงเงินกองทุนที่เพียงพอของบริษัท
- ดำเนินงานให้เป็นไปตามกฎหมาย และกฎเกณฑ์ที่เกี่ยวข้อง
- สนับสนุนการดำเนินงานอย่างมีประสิทธิภาพ ต่อเนื่อง รวมทั้งลดโอกาสความผิดพลาดในการดำเนินงาน

(3) รักษาความน่าเชื่อถือของระบบตลาดทุน และรับผิดชอบต่อสังคม

- เสริมสร้างความเชื่อมั่น และรักษาความน่าเชื่อถือของตลาดทุน (market integrity) นโยบายที่จัดทำต้องช่วยป้องกันไม่ให้บริษัทมีส่วนเกี่ยวข้องหรือสนับสนุนการกระทำไม่เป็นธรรม หรือผิดกฎหมาย เช่น การใช้ข้อมูลภายในซื้อขายหลักทรัพย์ การสร้างราคาหลักทรัพย์

การแพร่ข่าวเท็จ การฟอกเงิน การใช้ nominee ปกปิดหน้าที่หรือความรับผิดตามกฎหมาย เป็นต้น

- ลดความเสี่ยงต่อระบบการเงิน และระบบชำระราคาและส่งมอบหลักทรัพย์

นอกจากนี้ นโยบายที่จัดทำขึ้นควร**สนับสนุนให้เกิดการนำไปสู่การปฏิบัติโดยตลอดทั้งองค์กรอย่างเหมาะสม** โดยสนับสนุนวัฒนธรรมการบริหารความเสี่ยง และมีการพัฒนาปรับปรุงอย่างต่อเนื่องให้สะท้อนธุรกิจ และสภาพแวดล้อมที่เปลี่ยนไปด้วย

1.2 แนวทางการกำหนดนโยบายบริหารความเสี่ยง

บริษัทต้องกำหนดนโยบายการบริหารความเสี่ยงที่ครอบคลุมความเสี่ยงที่สำคัญและสอดคล้องกับแผนธุรกิจและธุรกรรมสำคัญของบริษัท (significant activity) โดยคำนึงถึงปัจจัยต่าง ๆ เช่น ลักษณะการดำเนินธุรกิจ ขนาด กลุ่มลูกค้า สภาพตลาด ความพร้อมของบุคลากร ระบบงานและทรัพยากรที่ใช้ในการปฏิบัติงาน เป็นต้น อันจะช่วยให้ผู้ลงทุนได้รับบริการที่ดี และธุรกิจเติบโตอย่างยั่งยืน โดยนโยบายบริหารความเสี่ยงอย่างน้อยควรครอบคลุมเรื่องต่อไปนี้

(1) การประเมินความเสี่ยง ได้แก่ การระบุความเสี่ยง การวิเคราะห์ความเสี่ยง และการประเมินระดับความเสี่ยง
(2) การจัดการและควบคุมความเสี่ยงของธุรกรรมสำคัญ รวมถึงความเสี่ยงที่เหลืออยู่
(3) การติดตามและทบทวนความเสี่ยง
(4) การรายงานผลการบริหารและจัดการความเสี่ยง
(5) การกำหนดผู้มีอำนาจอนุมัติในการบริหารและจัดการความเสี่ยง

การบริหารความเสี่ยงของบริษัทเป็นการบริหารความเสี่ยงองค์กรทั้งหมด จึงไม่ใช่หน้าที่ของฝ่ายบริหารความเสี่ยงเพียงฝ่ายเดียว แต่เป็นหน้าที่และความรับผิดชอบของคณะกรรมการบริษัท คณะกรรมการบริหารความเสี่ยง ผู้บริหารระดับสูง รวมถึงพนักงานทุกคนและทุกหน่วยงาน ซึ่งต้องมีความเข้าใจและร่วมมือในการบริหารและจัดการความเสี่ยง โดยมีบทบาท หน้าที่และความรับผิดชอบในการบริหารความเสี่ยง ดังนี้

1.2.1 คณะกรรมการบริษัท

(1) ให้ความสำคัญ (Tone from the top) และกำหนดทิศทางการบริหารและจัดการความเสี่ยง และอนุมัตินโยบายการบริหารความเสี่ยงของบริษัทหรือนโยบายของกลุ่มบริษัท ที่สามารถแสดงให้เห็นถึงแนวทางในการบริหารความเสี่ยงที่ครอบคลุมความเสี่ยงในธุรกรรมที่สำคัญ (significant activity) รวมถึงกำหนดและให้ความเห็นชอบระดับความเสี่ยงที่ยอมรับได้ (risk appetite) และอนุมัติกฎระเบียบ และระบบงานที่เกี่ยวข้อง รวมทั้งติดตามกำกับดูแลให้การดำเนินธุรกิจอยู่ภายในขอบเขตความเสี่ยงที่กำหนดไว้ เพื่อให้มั่นใจได้ว่า

บริษัทสามารถรู้เท่าทันความเสี่ยงที่อาจจะเกิดขึ้น และสามารถป้องกันและบริหารจัดการความเสี่ยงที่สำคัญได้อย่างทันท่วงที รวมทั้งสามารถตรวจจับปัญหาที่เกิดขึ้น และแก้ไขได้อย่างรวดเร็ว

(2) กำหนดให้มีการรายงานการติดตามผลการดูแลและบริหารความเสี่ยง ซึ่งรวมถึงการรายงานผลการตรวจสอบและติดตามการปรับปรุงแก้ไข (ถ้ามี) แก่คณะกรรมการที่เกี่ยวข้อง และคณะกรรมการบริษัทให้รับทราบเป็นประจำ โดยกำหนดเป็นวาระหลัก ตามรอบระยะเวลาที่เหมาะสม ทั้งนี้ หากมีเหตุการณ์ที่กระทบความเสี่ยงอย่างมีนัยสำคัญหรือพบการปฏิบัติที่เข้าข่ายหรืออาจเข้าข่ายไม่เป็นไปตามนโยบาย กฎระเบียบและระบบงานในการบริหารความเสี่ยงที่กำหนดอย่างมีนัยสำคัญ ให้รายงานให้คณะกรรมการที่เกี่ยวข้อง และคณะกรรมการบริษัทโดยไม่ชักช้า เพื่อให้สามารถจัดการได้ทันท่วงที

(3) รับทราบผลการประเมินความเสี่ยงและทบทวนความเพียงพอของระบบบริหารความเสี่ยง และประเมินประสิทธิภาพอย่างน้อยปีละครั้ง หรือเมื่อมีการเปลี่ยนอย่างมีนัยสำคัญ ตามที่คณะกรรมการบริหารความเสี่ยงหรือคณะกรรมการที่ได้รับมอบหมายจากคณะกรรมการบริษัทได้นำเสนอเพื่อพิจารณา รวมถึงให้ความเห็น คำแนะนำในการจัดการความเสี่ยง เพื่อให้มั่นใจว่าระบบดังกล่าวยังมีประสิทธิภาพ และสามารถใช้ได้กับเหตุการณ์หรือสภาพแวดล้อมที่เปลี่ยนแปลงไป

(4) กำหนดให้มีการสื่อสารให้พนักงานทุกคนในบริษัทตระหนักถึงการปฏิบัติงานตามนโยบายและแนวทางการบริหารความเสี่ยงของบริษัทอย่างจริงจังและเคร่งครัด และดูแลให้มีการปลูกฝังวัฒนธรรมองค์กรที่คำนึงถึงความเสี่ยง โดยอาจมอบหมายให้ฝ่ายงานต่าง ๆ เช่น ฝ่ายกำกับดูแลการปฏิบัติงานหรือฝ่ายบริหารความเสี่ยง เป็นผู้ดำเนินการดังกล่าว

(5) บูรณาการการบริหารความเสี่ยงเข้ากับการตัดสินใจทางธุรกิจ การกำกับดูแลกิจการ และการควบคุมภายในของบริษัท

(6) อาจพิจารณาจัดตั้งและสนับสนุนการดำเนินงานคณะกรรมการปฏิบัติการชุดต่าง ๆ เพื่อทำหน้าที่กำกับดูแล และกำหนดเกณฑ์การบริหารความเสี่ยงเพื่อให้มีการปฏิบัติงานที่เป็นไปตามทิศทางและนโยบายที่กำหนด เช่น คณะกรรมการกำกับความเสี่ยง (Risk Oversight Committee: ROC) คณะกรรมการบริหารความเสี่ยง (Risk Management Committee: RMC) เป็นต้น ทั้งนี้ บริษัทสามารถพิจารณาตามความเหมาะสมโดยกำหนดให้สอดคล้องกับขนาดและรูปแบบการดำเนินธุรกิจ ตลอดจนความซับซ้อนและความหลากหลายของการประกอบธุรกิจ (one size does not fit all)

ทั้งนี้ เพื่อป้องกันการเกิดปัญหาความขัดแย้งทางผลประโยชน์ หากมีการประชุมวาระใดที่กรรมการบริษัทท่านใดมีผลประโยชน์เกี่ยวข้อง ไม่ว่าทางตรงหรือทางอ้อม จะต้องแจ้งให้คณะกรรมการบริษัททราบและไม่เข้าไปมีส่วนร่วมหรือไม่มีส่วนที่เกี่ยวข้องในการตัดสินใจและไม่ลงมติในการประชุมวาระนั้น

อนึ่ง กรรมการบริษัทควรดำเนินการตามความคาดหวังของสำนักงานที่ระบุไว้ในหนังสือเวียนที่ กลต.กธ.(ว) 15/2562 ลงวันที่ 31 กรกฎาคม 2562 เรื่อง แนวปฏิบัติเกี่ยวกับบทบาทและความคาดหวังในการปฏิบัติหน้าที่ของกรรมการของบริษัทหลักทรัพย์และผู้ประกอบธุรกิจสัญญาซื้อขายล่วงหน้า ซึ่งประกอบด้วยบทบาทหน้าที่สำคัญของกรรมการบริษัท จำนวน 5 เรื่อง ได้แก่ การกำหนดและส่งเสริมให้เกิดค่านิยมและวัฒนธรรมที่ดีของบริษัท การกำหนดและอนุมัติการบริหารความเสี่ยง การกำหนดการควบคุมภายใน การกำกับดูแลและติดตามผลการดำเนินงาน และการติดตามแก้ไข

1.2.2 คณะกรรมการบริหารความเสี่ยง

กรณีที่คณะกรรมการบริษัทจัดตั้งและมีการมอบหมายงานให้คณะกรรมการบริหารความเสี่ยง หรือคณะกรรมการชุดอื่น ๆ เพื่อสนับสนุนและแบ่งเบาภารกิจของคณะกรรมการบริษัท คณะกรรมการบริษัทอาจพิจารณามอบหมายภารกิจในข้อ 1.2.1 ของคณะกรรมการตามความเหมาะสม ทั้งนี้ หน้าที่ของคณะกรรมการบริหารความเสี่ยงหรือคณะกรรมการชุดอื่น ๆ ที่ได้รับมอบหมายจากคณะกรรมการบริษัทในการบริหารความเสี่ยงอาจรวมถึง

(1) กำหนดกรอบและนโยบาย กฎระเบียบ และระบบงานในการบริหารความเสี่ยงเสนอต่อคณะกรรมการบริษัท เพื่อพิจารณาอนุมัติ โดยต้องครอบคลุมความเสี่ยงของธุรกรรมที่สำคัญของบริษัทตามทิศทางที่คณะกรรมการบริษัทกำหนด

(2) กำกับดูแล ทบทวนและให้ข้อเสนอแนะต่อคณะกรรมการบริษัท บุคคลที่เกี่ยวข้อง เกี่ยวกับกรอบและนโยบายการบริหารความเสี่ยง กฎระเบียบ วิธีปฏิบัติที่เป็นมาตรฐาน กลยุทธ์และการวัดความเสี่ยงโดยรวมของบริษัท เพื่อให้มั่นใจว่ามีการนำกลยุทธ์การบริหารความเสี่ยงไปปฏิบัติอย่างเหมาะสมและสอดคล้องกับกลยุทธ์โครงสร้างองค์กรและทรัพยากรของบริษัท

(3) ติดตามสถานะและการเปลี่ยนแปลงความเสี่ยงของบริษัท ความคืบหน้าในการบริหารความเสี่ยง รวมทั้งประเมินความเพียงพอและประสิทธิภาพของระบบการบริหารความเสี่ยงและให้ข้อเสนอแนะในสิ่งที่ต้องดำเนินการปรับปรุงแก้ไข เพื่อให้สอดคล้องกับนโยบายการบริหารความเสี่ยงที่กำหนด

(4) พิจารณาการกำหนดระดับความเสี่ยงที่องค์กรยอมรับได้ (risk appetite) และพิจารณาอนุมัติการกำหนดเพดานความเสี่ยง (risk limits) และมาตรการดำเนินการกรณีไม่เป็นไปตามเพดานความเสี่ยงที่กำหนด (corrective measure)

(5) พิจารณาเห็นชอบและทบทวนนโยบายการบริหารความเสี่ยงที่เกี่ยวข้องกับธุรกิจของบริษัทโดยครอบคลุมความเสี่ยงที่มีนัยสำคัญต่อธุรกิจ

(6) พิจารณาอนุมัติการขายผลิตภัณฑ์หรือให้บริการใหม่โดยคำนึงถึงความพร้อมของบริษัท ความเสี่ยงที่สำคัญ กระบวนการควบคุมความเสี่ยง และแนวทางการป้องกันความเสียหายที่อาจเกิดขึ้นตลอดกระบวนการดำเนินธุรกิจ

(7) พิจารณากลั่นกรองความเสี่ยงที่สำคัญของกิจการ ติดตามให้มีการประเมินความเสี่ยงตามมาตรฐานสากล ตั้งแต่การระบุความเสี่ยงโดยพิจารณาปัจจัยทั้งภายนอกและภายในองค์กร การประเมินผลกระทบและโอกาสที่เกิดขึ้นของความเสี่ยง รวมถึงการกำหนดมาตรการจัดการความเสี่ยงที่เหมาะสม และมีการติดตามประเมินผลประสิทธิผลการดำเนินงานด้านการบริหารความเสี่ยงอย่างต่อเนื่อง รวมทั้งให้คำแนะนำและความเห็นชอบในกระบวนการต่าง ๆ ที่มีความสำคัญ

(8) กำกับดูแลและสนับสนุนการบริหารความเสี่ยงให้มีประสิทธิผลและประสิทธิภาพทั้งในระดับองค์กรตลอดจนระดับกลุ่มงาน/หน่วยงาน (enterprise-wide risk management)

(9) กำหนดให้มีผู้รับผิดชอบในแต่ละปัจจัยเสี่ยง เพื่อให้มั่นใจว่าจะมีผู้รับผิดชอบที่จะจัดทำมาตรการจัดการความเสี่ยง ติดตาม และประเมินผลอย่างต่อเนื่อง

(10) กำกับดูแลการพัฒนาระบบการควบคุมภายในภาพรวม

(11) มีอำนาจเชิญผู้บริหาร ฝ่ายจัดการ หรือพนักงานของบริษัทที่เกี่ยวข้องมาชี้แจง ให้ความเห็นร่วมประชุม หรือส่งเอกสารตามที่เห็นว่าเกี่ยวข้องจำเป็น

(12) มีอำนาจให้ฝ่ายงานต่าง ๆ ที่เกี่ยวข้องกับการประกอบธุรกิจของบริษัทดำเนินการหรือปฏิบัติอย่างหนึ่งอย่างใดเท่าที่จำเป็นเพื่อให้คณะอนุกรรมการบริหารความเสี่ยงสามารถปฏิบัติหน้าที่ได้ตามที่กำหนดไว้

(13) ปรึกษาผู้เชี่ยวชาญทั้งภายในและภายนอกบริษัทในกรณีที่จำเป็น

(14) รายงานผลการปฏิบัติงานให้คณะกรรมการบริษัททราบเป็นประจำ โดยเป็นวาระหลัก ตามรอบระยะเวลาที่เหมาะสม

(15) จัดให้มีการประชุมเป็นประจำอย่างน้อยไตรมาสละหนึ่งครั้ง เพื่อติดตามสถานะความเสี่ยงและการเปลี่ยนแปลงความเสี่ยงของบริษัท รวมถึงติดตามความคืบหน้าในการบริหารความเสี่ยง และให้ข้อเสนอแนะในสิ่งที่ต้องดำเนินการปรับปรุงแก้ไข เพื่อให้สอดคล้องกับกรอบการบริหารความเสี่ยง และนโยบายการบริหารความเสี่ยงที่กำหนด

(16) จัดเตรียมแผนบรรเทาความเสี่ยงเพื่อรับมือกับความเสี่ยงกรณีฉุกเฉิน โดยควรมีการทบทวนแผนอย่างสม่ำเสมอและมีการรายงานให้คณะกรรมการบริษัทรับทราบ

(17) ปฏิบัติการอื่นใดเกี่ยวกับการบริหารความเสี่ยงที่คณะกรรมการบริษัทมอบหมาย

ทั้งนี้ เพื่อป้องกันการเกิดปัญหาความขัดแย้งทางผลประโยชน์ หากมีการประชุมวาระใดที่กรรมการท่านใดมีผลประโยชน์เกี่ยวข้อง ไม่ว่าทางตรงหรือทางอ้อม จะต้องแจ้งให้คณะกรรมการบริหารความเสี่ยงทราบและไม่เข้าไปมีส่วนร่วมหรือไม่มีส่วนที่เกี่ยวข้องในการตัดสินใจหรือไม่ลงมติในการประชุมวาระนั้น

1.2.3 ผู้บริหารระดับสูง (Top management)

ในการบริหารและจัดการความเสี่ยงอย่างรัดกุมและมีประสิทธิภาพนั้น ผู้บริหารระดับสูงต้องมีความเข้าใจในความเสี่ยงที่สำคัญในการประกอบธุรกิจ เพื่อใช้ประกอบการพิจารณากำหนดกลยุทธ์ นโยบาย หลักเกณฑ์ และระบบงาน เสนอคณะกรรมการเพื่อพิจารณาให้ความเห็นชอบและนำทิศทาง กลยุทธ์ นโยบาย และหลักเกณฑ์ มาจัดทำระบบงานสื่อสารเพื่อนำไปสู่การปฏิบัติงานที่เหมาะสมและครอบคลุมความเสี่ยงสำคัญที่อาจเกิดขึ้น รวมทั้งควบคุมดูแลการปฏิบัติงานให้เป็นไปตามกฎหมาย กฎระเบียบที่กำหนด

1.2.4 ฝ่ายควบคุมและบริหารความเสี่ยง

มีหน้าที่รับผิดชอบดังนี้

(1) ทำหน้าที่สนับสนุนการดำเนินงานที่เกี่ยวกับการประชุมคณะกรรมการบริหารความเสี่ยง จัดทำรายงานการประชุมอย่างครบถ้วนและถูกต้อง รวมทั้งติดตาม แจ้งคำสั่งหรือมติดังกล่าวให้ผู้ที่เกี่ยวข้องทราบและดำเนินการ

(2) รายงานประเด็นความเสี่ยงระดับองค์กร และความเสี่ยงระดับปฏิบัติการที่มีนัยสำคัญ พร้อมทั้งแนวทางบริหารความเสี่ยง และความคืบหน้าของการดำเนินงานเพื่อลดความเสี่ยงอย่างสม่ำเสมอและทันท่วงที

(3) รายงานประเด็นความเสี่ยงที่สำคัญต่อคณะกรรมการบริหารความเสี่ยง เพื่อประกอบการกลั่นกรอง

(4) ปฏิบัติการอื่นใดอันเกี่ยวเนื่องกับการบริหารความเสี่ยงของบริษัทตามที่คณะกรรมการบริหารความเสี่ยงมอบหมาย

1.2.5 หน่วยธุรกิจ

หน่วยธุรกิจหรือหน่วยงานเจ้าของความเสี่ยง (risk owner) มีหน้าที่รับผิดชอบในการระบุ ประเมิน ติดตาม ควบคุมและรายงานความเสี่ยงที่เกี่ยวข้องกับผลิตภัณฑ์และบริการของหน่วยงานตนเองให้อยู่ภายใต้ระดับความเสี่ยงที่ยอมรับได้ และสอดคล้องกับนโยบาย และกระบวนการบริหารความเสี่ยงที่บริษัทกำหนด

2. โครงสร้างการกำกับดูแลบริหารความเสี่ยง

2.1 โมเดลสามประสาน[1]

การกำกับดูแลบริหารความเสี่ยงทั้งองค์กร เป็นกุญแจสำคัญในการทำให้บริษัทเข้มแข็ง โมเดลสามประสานเป็นแนวทางในการจัดโครงสร้าง ออกแบบกระบวนการ และกำหนดความรับผิดชอบในองค์กร ผ่านการประสานงานร่วมกันในสามด่าน โดยทุกระดับชั้นควรร่วมกันในการกำหนดความเสี่ยงที่สำคัญเพื่อให้มีเป้าหมายในการทำงานที่สอดคล้องกัน เพื่อช่วยให้บรรลุวัตถุประสงค์ และสร้างการกำกับดูแลบริหารความเสี่ยงที่เข้มแข็ง ซึ่งสรุปได้ดังนี้

(1) ด่านที่ 1: หน่วยงานหรือผู้ที่ก่อให้เกิดความเสี่ยงในชั้นแรก (business unit) ซึ่งเป็นเจ้าของความเสี่ยง รับผิดชอบในการระบุความเสี่ยง ประเมินความเสี่ยง กำหนดมาตรการบริหารความเสี่ยง ควบคุมความเสี่ยง ปฏิบัติตามมาตรการและสอบทานการปฏิบัติงานประจำวันให้เป็นไปตามมาตรการที่กำหนด

(2) ด่านที่ 2: หน่วยงานบริหารความเสี่ยง (risk management) รับผิดชอบงานที่เกี่ยวกับการกำกับดูแลการบริหารความเสี่ยงในลักษณะ oversight function ให้มีการปฏิบัติงานเป็นไปตามที่กำหนดหรือไม่ และ

[1] สมาคมผู้ตรวจสอบภายในสากล (Institute of Internal Auditors: IIA) ได้ออกโมเดลสามประสาน (The Three Lines Model) ฉบับปรับปรุง 2563 เพื่อช่วยตอบคำถามให้แก่องค์กรที่ต้องการเพิ่มการกำกับดูแลกิจการให้แข็งแกร่ง ทั้งนี้ รู้จักกันในชื่อเดิมว่า แนวป้องกัน 3 ด่าน (Three Lines of Defense)

หน่วยงานกำกับดูแลการปฏิบัติงาน (compliance) รับผิดชอบงานที่เกี่ยวกับการติดตามและตรวจสอบความเสี่ยงด้านการปฏิบัติตามกฎหมายและกฎเกณฑ์ว่า มีการปฏิบัติที่ไม่เป็นไปตามกฎหมายหรือกฎเกณฑ์ที่เกี่ยวข้องหรือไม่

(3) ด่านที่ 3: งานตรวจสอบภายใน (internal audit) ซึ่งเป็นหน่วยงานที่เป็นอิสระจากฝ่ายบริหารจัดการ ทำหน้าที่ตรวจสอบเพื่อประเมินความเพียงพอของมาตรการ และตรวจสอบการปฏิบัติงานของด่านที่ 1 และ 2 ทั้งนี้ หน่วยงานในด่านที่ 3 อาจเป็นหน่วยงานภายในของบริษัท หรือเป็นหน่วยงานภายนอกบริษัทก็ได้ โดย outsource งานตรวจสอบภายในไปยังหน่วยงานตรวจสอบของบริษัทแม่ หรือว่าจ้างผู้เชี่ยวชาญ เช่น บริษัทสอบบัญชี (audit firm) เป็นต้น

ทั้งนี้ บริษัทควรกำหนดให้ระบบการกำกับดูแลมีความสอดคล้องกับลักษณะการประกอบธุรกิจและขนาดของบริษัท (one size not fit all) อย่างมีประสิทธิภาพ เหมาะสม และเพียงพอสำหรับธุรกิจของบริษัท

- หากธุรกิจมีขนาดใหญ่ หรือมีการดำเนินธุรกิจที่มีความซับซ้อน ควรมีหน่วยงานกำกับดูแลการปฏิบัติงาน (compliance) และหน่วยงานตรวจสอบภายในที่แยกออกจากกัน
- หากธุรกิจมีการดำเนินธุรกิจที่ไม่ซับซ้อนหรือมีขนาดเล็ก/ปริมาณธุรกรรมค่อนข้างน้อย อาจจัดให้หน่วยงานกำกับดูแลการปฏิบัติงาน (compliance) และหน่วยงานตรวจสอบภายในอยู่ในหน่วยงานเดียวกันได้ แต่ควรพิจารณาจัดให้มีความอิสระในการปฏิบัติงาน เช่น แยกบุคลากรที่ทำหน้าที่ด้านการกำกับดูแลการปฏิบัติงานและการตรวจสอบภายในออกจากกัน หรือการมอบหมายให้บุคคลอื่น (outsource) เช่น บริษัทแม่ ให้ดำเนินการตรวจสอบการทำงานของหน่วยงานกำกับดูแลการปฏิบัติงาน (compliance) เป็นต้น เพื่อให้การตรวจสอบมีความเป็นอิสระและให้มีการตรวจสอบการดำเนินงานของหน่วยงานกำกับดูแลการปฏิบัติงาน (compliance) อีกชั้นหนึ่งด้วย โดยให้รายงานผลการตรวจสอบต่อคณะกรรมการบริษัทหรือคณะกรรมการตรวจสอบ

2.2 บทบาทหน้าที่ของด่านที่ 1

2.2.1 การประเมิน และการบริหารจัดการความเสี่ยงในชั้นแรก

(1) มีการระบุ วิเคราะห์ปัจจัยความเสี่ยง และประเมินความเสี่ยงที่เกี่ยวข้องกับผลิตภัณฑ์และบริการของบริษัท เพื่อนำมากำหนดเป็นมาตรการบริหารความเสี่ยงและมาตรการควบคุมความเสี่ยงในชั้นแรก รวมทั้งกำหนดระดับความเสี่ยงที่ยอมรับได้

(2) มีการจัดวางระบบงาน และจัดทำมาตรการบริหารความเสี่ยงที่เหมาะสมกับระดับความเสี่ยงของแต่ละธุรกรรมของบริษัท เพื่อให้มั่นใจได้ว่า บริษัทมีมาตรการรองรับที่ครอบคลุมทุกความเสี่ยงที่สำคัญของบริษัท

(3) บริหารจัดการความเสี่ยงตามมาตรการที่กำหนดได้อย่างทันท่วงที และมีประสิทธิภาพ โดยสามารถควบคุมให้ความเสี่ยงอยู่ในระดับที่ยอมรับได้ เมื่อเกิดเหตุการณ์ที่กระทบกับความเสี่ยงของบริษัท

(4) มีกระบวนการที่มีประสิทธิภาพในการติดตาม วิเคราะห์สาเหตุของความเสี่ยงที่เกิดขึ้น ทบทวนความเสี่ยงของบริษัท และปรับปรุงให้มีประสิทธิภาพมากขึ้น (ถ้าจำเป็น) อย่างเป็นประจำตามรอบระยะเวลาที่เหมาะสม รวมทั้งมีกระบวนการสอบทานการปฏิบัติงานประจำวัน

(5) มีการรายงานผลการบริหารความเสี่ยงของบริษัท ซึ่งรวมถึงสาเหตุที่ทำให้เกิดความเสี่ยงดังกล่าว แนวโน้มความเสี่ยงที่อาจจะเกิดขึ้น และแนวทางป้องกันต่อคณะกรรมการบริษัท หรือคณะกรรมการที่ได้รับมอบหมายตามรอบระยะเวลาที่เหมาะสมหรือหากเป็นเรื่องที่มีนัยสำคัญให้รายงานโดยไม่ชักช้า

2.2.2 การจัดบุคลากรอย่างเหมาะสม เพียงพอ และสามารถปฏิบัติหน้าที่ได้อย่างมีประสิทธิภาพ

(1) บุคลากรที่ปฏิบัติงานในหน่วยธุรกิจมีความรู้ความเข้าใจในผลิตภัณฑ์และบริการของหน่วยงานตนตลอดจนความเสี่ยงที่เกี่ยวข้องเป็นอย่างดี และมีจำนวนเพียงพอต่อการปฏิบัติงาน

(2) บุคลากรได้รับการอบรมความรู้อย่างสม่ำเสมอทั้งด้านผลิตภัณฑ์และบริการของบริษัท และความเสี่ยงที่เกี่ยวข้อง ตลอดจนกระบวนการปฏิบัติตามระบบงานและมาตรการบริหารความเสี่ยง ทำให้ตระหนักถึงความสำคัญของความเสี่ยง และสามารถบริหารจัดการความเสี่ยงในชั้นต้นได้อย่างมีประสิทธิภาพ อันช่วยลดผลกระทบทางด้านความเสี่ยงของบริษัทได้

2.3 บทบาทหน้าที่ของด่านที่ 2

บริษัทพิจารณาจัดตั้งหน่วยงานที่ทำหน้าที่ในด่านที่ 2 ตามความเหมาะสมและความสอดคล้องกับรูปแบบการดำเนินธุรกิจ โดยอาจกำหนดให้มีหน่วยงานหนึ่งทำหน้าที่ทั้งบริหารความเสี่ยงและกำกับดูแลการปฏิบัติงาน หรือกำหนดหน่วยงานบริหารความเสี่ยง และหน่วยงานกำกับดูแลการปฏิบัติงานแยกออกจากกัน หรือ outsource ไปยังหน่วยงานของบริษัทในกลุ่มได้ โดยมีบทบาทหน้าที่ครอบคลุมอย่างน้อย ดังนี้

2.3.1 หน่วยงานบริหารความเสี่ยง

(1) การบริหารความเสี่ยง

- มีการระบุ วิเคราะห์ ประเมินความเสี่ยงที่สำคัญของบริษัท และผลกระทบต่อการปฏิบัติงานและการดำเนินธุรกิจ เพื่อหาแนวทางในการจัดการความเสี่ยงที่เหมาะสม รวมทั้งกำหนดระดับความเสี่ยงที่ยอมรับได้
- มีการจัดทำแนวทางในการจัดการ ควบคุม และป้องกันความเสี่ยงที่เหมาะสมสอดคล้องกับผลการประเมินความเสี่ยง เพื่อให้มั่นใจได้ว่าระดับความเสี่ยงอยู่ในระดับที่ยอมรับได้

- มีกระบวนการที่มีประสิทธิภาพในการติดตามและทบทวนความเสี่ยงที่สำคัญของบริษัทอย่างเป็นประจำตามรอบระยะเวลาที่เหมาะสม
- มีการรายงานผลการบริหารความเสี่ยงของบริษัท และแนวโน้มความเสี่ยงที่อาจจะเกิดขึ้นต่อคณะกรรมการบริษัท หรือคณะกรรมการที่ได้รับมอบหมายในระยะเวลาที่เหมาะสม

ทั้งนี้ บริษัทต้องจัดให้มีการทบทวนระเบียบวิธีปฏิบัติและกระบวนการบริหารความเสี่ยงอย่างน้อยปีละ 1 ครั้ง และทุกครั้งที่มีการเปลี่ยนแปลงอย่างมีนัยสำคัญ

(2) การจัดบุคลากรอย่างเหมาะสม เพียงพอ และสามารถปฏิบัติหน้าที่อย่างเป็นอิสระ

- บุคลากรที่ปฏิบัติงานในหน่วยงานบริหารความเสี่ยงมีความรู้ความสามารถ ประสบการณ์และมีจำนวนเพียงพอต่อการปฏิบัติงานและลักษณะความเสี่ยงของบริษัท
- บุคลากรได้รับการอบรมความรู้อย่างสม่ำเสมอทั้งด้านการบริหารความเสี่ยงด้านเทคโนโลยีและด้านธุรกิจ เพื่อให้มีความเข้าใจในผลิตภัณฑ์และบริการ รวมทั้งความเสี่ยงที่เกี่ยวข้อง ทำให้สามารถบริหารจัดการความเสี่ยงได้ครอบคลุมทุกด้านและทันท่วงที

2.3.2 หน่วยงานกำกับดูแลการปฏิบัติงาน

(1) การกำกับดูแลการปฏิบัติงาน

- มีการกำกับดูแลและจัดทำแผนการกำกับดูแลมีประสิทธิภาพ ครอบคลุมธุรกรรมที่สำคัญและดำเนินการในระยะเวลาที่เหมาะสม โดยแผนการกำกับดูแลต้องผ่านการพิจารณาจากคณะกรรมการบริษัทหรือคณะกรรมการที่ได้รับมอบหมาย และกำหนดให้มีการทบทวนอย่างน้อยปีละ 1 ครั้งและเมื่อมีการเปลี่ยนแปลงอย่างมีนัยสำคัญ
- มีการระบุและประเมินความเสี่ยงที่สำคัญของบริษัทก่อนจัดทำแผนการกำกับดูแลเพื่อให้แผนการกำกับดูแลของบริษัทมีความสอดคล้องกับความเสี่ยง ธุรกรรมที่สำคัญ และธุรกรรมใหม่ที่เริ่มดำเนินการ
- มีการกำกับดูแลการปฏิบัติตามกฎระเบียบของบริษัท กฎหมายและหลักเกณฑ์ที่เกี่ยวข้องของทางการ เพื่อป้องกันการไม่ปฏิบัติตามกฎระเบียบของบริษัท กฎหมายและหลักเกณฑ์ของทางการ
- มีการรายงานการตรวจสอบและประเด็นที่ตรวจพบให้คณะกรรมการบริษัทหรือคณะกรรมการที่ได้รับมอบหมาย รับทราบตามเวลาที่กำหนด และทันต่อเหตุการณ์
- มีการติดตามการแก้ไขในประเด็นที่ตรวจพบในระยะเวลาที่เหมาะสม กรณีพบเหตุหรือการกระทำที่เป็นการฝ่าฝืนกฎเกณฑ์ หรือมีข้อสังเกตจากการตรวจสอบจากหน่วยงานทางการ โดยให้มีการวิเคราะห์สาเหตุ แนวทางแก้ไข และวิธีป้องกันเพื่อไม่ให้เกิดเหตุดังกล่าวซ้ำ

- มีการกำหนดกระบวนการให้หน่วยงานกำกับดูแลการปฏิบัติงานได้รับแจ้งให้ทราบอย่างทันท่วงทีหากมีการเปลี่ยนแปลงที่สำคัญต่อกลยุทธ์ นโยบาย หรือกระบวนการบริหารความเสี่ยงของบริษัท

(2) การจัดบุคลากรอย่างเหมาะสม เพียงพอ และสามารถปฏิบัติหน้าที่อย่างเป็นอิสระ

- บุคลากรที่ปฏิบัติงานในหน่วยงานกำกับดูแลการปฏิบัติงานมีความรู้ความสามารถและมีจำนวนที่เพียงพอต่อการปฏิบัติงานและลักษณะของธุรกิจของบริษัท
- บุคลากรได้รับการอบรมความรู้อย่างสม่ำเสมอทั้งด้านกฎเกณฑ์ และด้านธุรกิจ เพื่อให้มีความเข้าใจในผลิตภัณฑ์และบริการ ทำให้สามารถปฏิบัติงานโดยเข้าใจในวัตถุประสงค์และวิธีการตรวจสอบในธุรกรรมนั้น ๆ

2.4 บทบาทหน้าที่ของด่านที่ 3

2.4.1 การตรวจสอบการปฏิบัติงาน

(1) มีการจัดทำแผนงาน และขอบเขตการตรวจสอบการปฏิบัติงานที่ครอบคลุมความเสี่ยงที่สำคัญของบริษัทและสอดคล้องกับนโยบายการบริหารความเสี่ยงของบริษัท โดยแผนงานและขอบเขตการตรวจสอบดังกล่าวต้องได้รับความเห็นชอบจากคณะกรรมการบริษัท หรือคณะกรรมการตรวจสอบ และกำหนดให้มีการทบทวนอย่างน้อยปีละ 1 ครั้งและเมื่อมีการเปลี่ยนแปลงอย่างมีนัยสำคัญ

(2) มีการระบุและประเมินความเสี่ยงที่สำคัญของบริษัทก่อนจัดทำแผนการกำกับดูแลเพื่อให้แผนการกำกับดูแลของบริษัทมีความสอดคล้องกับความเสี่ยง ธุรกรรมที่สำคัญ และธุรกรรมใหม่ที่เริ่มดำเนินการ

(3) ตรวจสอบการปฏิบัติงานของหน่วยงานด่านที่ 1 และด่านที่ 2 ตามความเสี่ยงของบริษัท (Risk Based Approach) ในขอบเขตที่กำหนดตามข้อ 2.4.1 (1) และเมื่อมีเหตุการณ์ผิดปกติที่มีนัยสำคัญ เช่น ประเด็นข้อสังเกตจากหน่วยงานทางการ ข่าว หรือข้อร้องเรียน เป็นต้น

(4) จัดทำรายงานผลการตรวจสอบ และเสนอต่อคณะกรรมการบริษัท หรือคณะกรรมการที่ได้รับมอบหมาย ตลอดจนจัดเก็บรายงานผลการตรวจสอบดังกล่าวไว้ที่บริษัทในลักษณะที่พร้อมเรียกดูหรือจัดให้หน่วยงานกำกับดูแล (regulator) และหน่วยงานทางการตรวจสอบได้เมื่อได้รับการร้องขอ

(5) ติดตามความคืบหน้าของการแก้ไขจากประเด็นที่พบจากการตรวจสอบ และรายงานให้คณะกรรมการบริษัท หรือคณะกรรมการตรวจสอบ

2.4.2 การจัดบุคลากรอย่างเหมาะสม เพียงพอ และสามารถปฏิบัติหน้าที่อย่างเป็นอิสระ

(1) บุคลากรที่ปฏิบัติงานในหน่วยงานตรวจสอบมีความรู้ ประสบการณ์ และความเชี่ยวชาญเกี่ยวกับการตรวจสอบ และมีจำนวนที่เพียงพอต่อการปฏิบัติงาน ลักษณะความเสี่ยงของบริษัท และลักษณะของธุรกิจ (business model) ของบริษัท

(2) บุคลากรได้รับการอบรมความรู้อย่างสม่ำเสมอทั้งด้านการบริหารความเสี่ยง เทคโนโลยี กฎเกณฑ์ และด้านธุรกิจ เพื่อให้มีความเข้าใจในผลิตภัณฑ์และบริการ รวมทั้งความเสี่ยงและกฎเกณฑ์ที่เกี่ยวข้อง ทำให้สามารถตรวจสอบการปฏิบัติงาน โดยเข้าใจถึงวัตถุประสงค์ และการดำเนินการในการบริหารความเสี่ยง และตรวจสอบในธุรกรรมต่าง ๆ ของหน่วยงานที่เกี่ยวข้องได้

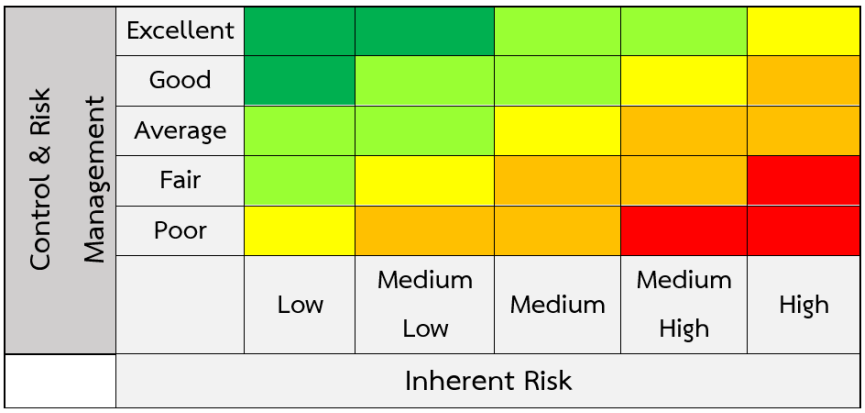
3. การประเมินความเสี่ยง

บริษัทควรกำหนดกระบวนการระบุความเสี่ยงที่อาจเกิดขึ้นในการดำเนินธุรกิจ โดยพิจารณาตามธุรกรรมที่สำคัญของบริษัท (significant activity) ทั้งจากปัจจัยภายในและปัจจัยภายนอก โดยให้มีการพิจารณาความเสี่ยงที่เกิดขึ้นในปัจจุบันและที่อาจเกิดขึ้นในอนาคต ครอบคลุมธุรกรรมสำคัญของบริษัทและวิเคราะห์ความเสี่ยงดังกล่าว โดยคาดการณ์ถึงโอกาสที่จะเกิดผลกระทบหรือความเสียหายที่คาดว่าจะเกิดขึ้น และความรุนแรงของผลกระทบการเกิดเหตุการณ์ขึ้น พร้อมทั้งกำหนดมาตรการที่ช่วยลดผลกระทบจากความเสี่ยง ตัวอย่างเช่น

- วิเคราะห์ว่าเหตุการณ์ในกระบวนการทำงานใดที่จะทำให้ปัจจัยที่เป็นความเสี่ยงเกิดขึ้นโดยพิจารณาปัจจัยต่าง ๆ เช่น ความซับซ้อนของผลิตภัณฑ์ กลุ่มลูกค้าเป้าหมาย กลุ่มผู้ขาย รวมถึงผลกระทบหากเกิดเหตุการณ์ความเสี่ยงเพื่อประเมินระดับความเสี่ยง
- จัดให้มีระบบงานและกำหนดมาตรการติดตามเหตุการณ์ที่เป็นสาเหตุของปัจจัยความเสี่ยง รวมทั้งมาตรการในการลดความเสี่ยงเหล่านั้น
- แจ้งพนักงานทุกคนที่เกี่ยวข้องรับทราบและปฏิบัติตามมาตรการบริหารความเสี่ยงที่กำหนด
- ติดตามว่าหน่วยงานต่าง ๆ ได้ปฏิบัติตามแผนการบริหารความเสี่ยงที่กำหนดไว้
- ทบทวนเหตุการณ์ที่จะก่อให้เกิดความเสี่ยง และปัจจัยที่เป็นความเสี่ยงอย่างสม่ำเสมอ เพื่อให้บริษัทสามารถปรับตัวรองรับสภาพแวดล้อมที่เปลี่ยนแปลงได้อย่างทันท่วงที
- มีการประเมินความเสี่ยงก่อนออกผลิตภัณฑ์หรือการให้บริการใหม่

ทั้งนี้ บริษัทควรมีเครื่องมือสำหรับช่วยประเมินความเสี่ยงให้เหมาะกับขนาดและความซับซ้อนของการประกอบธุรกิจ เช่น risk matrix ซึ่งจะช่วยในการวิเคราะห์ระดับความเสี่ยงและมาตรการกำกับดูแลของบริษัท รวมทั้งควรมีการดำเนินการประเมินความเสี่ยงอย่างต่อเนื่อง และทบทวนความเหมาะสมเป็นระยะ

Heat Map



จากตัวอย่าง heat map ข้างต้น เป็นตัวอย่างการประเมินความเสี่ยงซึ่งประกอบด้วย 2 ส่วน ได้แก่ (1) Inherent Risk : ความเสี่ยงจากการประกอบธุรกิจ (ก่อนพิจารณามาตรการกำกับดูแล) ซึ่งมีระดับความเสี่ยงในการประเมินตั้งแต่ความเสี่ยงต่ำ (low) ไปจนถึงความเสี่ยงสูง (high) และ (2) Control and Risk Management: มาตรการกำกับดูแล ซึ่งมีระดับการกำกับดูแลจากระดับอ่อน (poor) ไปจนถึงระดับการกำกับดูแลที่ดีมาก (excellent) เช่น บริษัทประเมินความเสี่ยงของธุรกรรมหนึ่ง (significant activity) เป็น Inherent risk อยู่ในระดับปานกลาง และ Control and Risk Management ในระดับที่ดีมาก ก็จะทำให้ผลลัพธ์จากการประเมินความเสี่ยง (net risk) อยู่ในระดับดี (สีเขียวใน heat map) ซึ่งเมื่อบริษัทประเมินความเสี่ยงธุรกรรมทั้งหมดของบริษัท จะทำให้บริษัทได้เห็นภาพรวมความเสี่ยงของทั้งบริษัท (overall net risk) และความเสี่ยงในแต่ละธุรกรรม (significant activity) เพื่อจะได้ใช้ในการจัดการกับความเสี่ยงที่เหมาะสมได้ต่อไป (ตามระดับความเสี่ยง)

4. ประเภทความเสี่ยงที่ต้องคำนึงถึงและการบริหารจัดการความเสี่ยง

ในการกำหนดนโยบายการบริหารความเสี่ยงและกรอบการบริหารความเสี่ยงให้เหมาะสมและสอดรับกับความเสี่ยงในการดำเนินธุรกิจ บริษัทควรกำหนดนโยบายการบริหารความเสี่ยงและการบริหารจัดการความเสี่ยงให้ครอบคลุมความเสี่ยงสำคัญที่มีอยู่ในกิจกรรมและกระบวนการดำเนินธุรกิจอย่างน้อยในเรื่องต่อไปนี้

4.1 ความเสี่ยงด้านกลยุทธ์ (strategic risk)

(1) ความเสี่ยง

ความเสี่ยงด้านกลยุทธ์เป็นความเสี่ยงที่เกิดจากการที่บริษัทไม่สามารถดำเนินธุรกิจตามแผนหรือกลยุทธ์ที่บริษัทได้กำหนดไว้ อันจะส่งผลกระทบต่อรายได้ ฐานะการเงินหรือศักยภาพในการแข่งขัน ชื่อเสียงของบริษัท ซึ่งความเสี่ยงด้านกลยุทธ์อาจเกิดขึ้นได้จากการที่บริษัทกำหนดนโยบาย แผนกลยุทธ์ แผนการดำเนินงาน และการนำไปปฏิบัติอย่างไม่เหมาะสม หรือเกิดจากปัจจัยและสภาพแวดล้อมต่าง ๆ มีการเปลี่ยนแปลงไปจากเดิม ซึ่งส่งผลต่อแผนหรือกลยุทธ์ที่บริษัทได้กำหนดไว้ โดยความเสี่ยงด้านกลยุทธ์อาจเกิดจากเหตุการณ์ต่าง ๆ เช่น

- การเปลี่ยนแปลงผู้ถือหุ้นรายใหญ่ กรรมการ ผู้บริหาร หรือบุคลากรที่มีความสำคัญต่อการดำเนินธุรกิจ
- ความไม่พร้อมหรือไม่เพียงพอของระบบงานหรือบุคลากรในการดำเนินการตามแผนกลยุทธ์ที่วางไว้
- การเปลี่ยนแปลงกลยุทธ์การดำเนินธุรกิจของบริษัทแม่หรือกลุ่มธุรกิจ รวมถึงการเปลี่ยนแปลงนโยบายการบริหารความเสี่ยงของบริษัทแม่หรือกลุ่มธุรกิจ (Group risk)
- ความบกพร่องหรือความผิดพลาดจากการดำเนินการของบริษัทที่ไม่รองรับปริมาณและความซับซ้อนของผลิตภัณฑ์หรือบริการใหม่
- ผลิตภัณฑ์หรือบริการใหม่ของบริษัทไม่บรรลุเป้าหมายตามแผนกลยุทธ์ที่วางไว้
- การให้บริการที่ไม่มีคุณภาพหรือไม่เหมาะสมถูกต้องต่อลูกค้า

(2) การบริหารจัดการความเสี่ยง

การบริหารจัดการความเสี่ยงด้านกลยุทธ์อย่างน้อยควรครอบคลุมในเรื่องต่อไปนี้

- กำหนดนโยบายการบริหารความเสี่ยง กรอบการบริหารและจัดการความเสี่ยง รวมถึงเพดานความเสี่ยงและความเสี่ยงที่ยอมรับได้ของบริษัทให้สอดรับกับความเสี่ยงด้านกลยุทธ์ที่อาจเกิดขึ้น
- จัดให้มีการรายงานข้อมูลที่เกี่ยวข้องกับความเสี่ยงและการดำเนินการที่สำคัญของบริษัทให้คณะกรรมการบริษัท หรือคณะกรรมการที่ได้รับมอบหมาย รับทราบอย่างสม่ำเสมอ เพื่อให้มีข้อมูลประกอบการพิจารณากำหนดกลยุทธ์และทิศทางการดำเนินธุรกิจที่ครบถ้วน นอกจากนี้

คณะกรรมการบริษัทหรือคณะกรรมการที่ได้รับมอบหมายควรมีการติดตามความเสี่ยงด้านกลยุทธ์ของบริษัทอย่างสม่ำเสมอ

- ทบทวน และปรับปรุงการดำเนินงาน เพื่อรองรับการเปลี่ยนแปลงกลยุทธ์ในการดำเนินธุรกิจ เช่น การจัดสรรและพัฒนาบุคลากรให้เหมาะสมและเพียงพอกับขนาดและปริมาณของธุรกิจ การจัดให้มีระบบเทคโนโลยีสารสนเทศให้รองรับการประกอบธุรกิจอย่างมีประสิทธิภาพ
- มีการพิจารณาปัจจัยและผลกระทบจากการออกผลิตภัณฑ์ใหม่และการเปลี่ยนแปลงกลุ่มลูกค้าอย่างละเอียดรอบคอบ เช่น ความเสี่ยงที่ยอมรับได้ ผลกระทบและความพร้อมของระบบงาน ทรัพยากร และฐานะการเงินของบริษัท ความเหมาะสมกับกลุ่มและสภาพตลาด เป็นต้น
- มีการอบรมให้ความรู้แก่ผู้บริหารและพนักงาน เพื่อให้มีความพร้อมต่อผลิตภัณฑ์หรือบริการใหม่ของบริษัท และสามารถปฏิบัติงานได้ตามนโยบายและกลยุทธ์ของบริษัท

4.2 ความเสี่ยงด้านตลาด (market risk)

(1) ความเสี่ยง

ความเสี่ยงด้านตลาดเป็นความเสี่ยงที่เกิดจากการเปลี่ยนแปลงมูลค่าของหลักทรัพย์หรือสัญญาซื้อขายล่วงหน้า (“สัญญาฯ”) โดยความเสี่ยงด้านตลาดอาจเกิดจากปัจจัยต่าง ๆ เช่น

- ภาวะเศรษฐกิจและตลาดมีความผันผวน
- การกระจุกตัว (concentration) ในหลักทรัพย์หรือตราสารหนี้มากเกินไป
- การเปลี่ยนแปลงของอัตราดอกเบี้ย/อัตราแลกเปลี่ยน
- การด้อยค่าของตราสารหนี้หรือการไม่ชำระหนี้อันเกิดจากการเปลี่ยนแปลงของสถานะเครดิตของบริษัท/ผู้ออกตราสารหนี้ ซึ่งส่งผลกระทบต่อเงินลงทุนของบริษัท (portfolio)/ลูกค้า

โดยความเสี่ยงด้านตลาดสามารถเกิดขึ้นได้ต่อทั้งบริษัทและลูกค้า ดังนี้

(1.1) บริษัท

- บริษัทอาจได้รับความเสียหายจากการเปลี่ยนแปลงมูลค่าของหลักทรัพย์หรือสัญญาฯ ซึ่งส่งผลกระทบต่อรายได้ เงินกองทุนของบริษัท และสภาพคล่องของบริษัท
- ความเสี่ยงด้านตลาดที่เกิดขึ้นกับบริษัท เกิดขึ้นได้จากธุรกรรมต่าง ๆ เช่น
  - การลงทุนเพื่อบริษัท (proprietary trade) การลงทุนเพื่อป้องกันความเสี่ยง

- การเป็นนายหน้าซื้อขายหลักทรัพย์/ตัวแทนสัญญาซื้อขายล่วงหน้า (เช่น กรณีคำสั่งซื้อขายผิดพลาดที่ต้องรับรายการดังกล่าวเข้าบัญชีบริษัท (error port) และการทำธุรกรรมการซื้อขายรายใหญ่ (block trade) เป็นต้น
- การทำธุรกิจวาณิชธนกิจ ในการจัดจำหน่ายและรับประกันการจำหน่ายหลักทรัพย์

(1.2) ลูกค้า

- การเปลี่ยนแปลงมูลค่าของหลักทรัพย์หรือสัญญาฯ ส่งผลต่อมูลค่าหลักทรัพย์หรือสัญญาฯ ในเงินลงทุนของลูกค้าและระดับอัตราผลตอบแทนที่ลูกค้าต้องการ

(2) การบริหารจัดการความเสี่ยง

การบริหารจัดการความเสี่ยงด้านตลาดอย่างน้อยควรครอบคลุมในเรื่องดังนี้

(2.1) บริษัท

- การลงทุนเพื่อบริษัท
  - จัดให้มีนโยบายและข้อกำหนดในการลงทุน การควบคุมความเสี่ยงที่รัดกุมเพียงพอ (เช่น cut loss limit, concentration limit, counterparty limit และ VaR limit เป็นต้น) และการลงทุนให้อยู่ในระดับความเสี่ยงที่ยอมรับได้ รวมถึงกำหนดผู้มีอำนาจในการอนุมัติในการลงทุนอย่างชัดเจน
  - รายงานผลการลงทุนกับผู้บริหาร คณะกรรมการบริษัทหรือคณะกรรมการที่ได้รับมอบหมายอย่างสม่ำเสมอ
  - ในการประชุมเพื่อพิจารณา/ดำเนินการใดกับเงินลงทุนเพื่อบริษัท บริษัทต้องจัดให้มีการจดบันทึกการประชุม รวมถึงบันทึกความเห็น/เหตุผลในการพิจารณา และจัดเก็บเป็นหลักฐาน
- การส่งคำสั่งซื้อขายหลักทรัพย์ผิดพลาด (trading error)
  - กำหนดขั้นตอนและวิธีการดำเนินการเป็นลายลักษณ์อักษรและการควบคุมดูแลให้ปฏิบัติตามกรณีส่งคำสั่งที่ผิดพลาด (trading error) เช่น แก้ไขรายการที่ผิดพลาดภายในวันทำการหรือภายในวันทำการถัดไป กำหนดให้มีการอนุมัติรายการผิดพลาดตามมูลค่านัยสำคัญ โดยมีการบันทึกเหตุผลและความเห็นประกอบการอนุมัติ เป็นต้น
  - มีการตรวจสอบ สอบทานรายการที่ผิดพลาด (trading error) ให้มั่นใจว่า การใช้บัญชี trading error ถูกต้องตามขั้นตอนที่กำหนดและเป็นไปตามวัตถุประสงค์ของบัญชีนั้น

(2.2) ลูกค้า

- การให้คำแนะนำการลงทุนและการดูแลลูกค้า
  - มีการติดตามข่าวสารและความเสี่ยงด้านตลาดที่อาจกระทบต่อราคาหลักทรัพย์หรือสัญญาฯ อย่างสม่ำเสมอ เพื่อให้การให้คำแนะนำแก่ลูกค้านั้นได้มีการคำนึงถึงความเสี่ยงด้านตลาดประกอบด้วย
  - มีการให้ความรู้ลูกค้าเกี่ยวกับความเสี่ยงด้านตลาด เพื่อให้ลูกค้าคำนึงถึงความเสี่ยงด้านตลาดในการประกอบการตัดสินใจในการลงทุนในหลักทรัพย์หรือสัญญาฯ ของลูกค้า
  - มีการติดตามและพิจารณาผลตอบแทนในการลงทุนของลูกค้า เพื่อประกอบการให้คำแนะนำการลงทุนแก่ลูกค้า

4.3 ความเสี่ยงด้านเครดิต (credit risk)

(1) ความเสี่ยง

ความเสี่ยงด้านเครดิตเป็นความเสี่ยงที่บริษัทจะได้รับความเสียหายจากการที่ลูกค้า หรือคู่สัญญาไม่สามารถปฏิบัติตามข้อตกลง สัญญา หรือภาระที่ได้ผูกพันไว้กับบริษัท เช่น ผิดนัดชำระเงิน/หลักประกัน/หนี้ และผิดนัดส่งมอบหลักทรัพย์ เป็นต้น อันจะส่งผลกระทบแก่รายได้ สภาพคล่อง และเงินกองทุนของบริษัท
ทั้งนี้ ความเสี่ยงด้านเครดิตอาจเกิดจากเหตุการณ์ต่าง ๆ เช่น

- การให้วงเงินลูกค้าสูงเกินฐานะหรือความสามารถในการชำระหนี้ของลูกค้า หรือสูงเกินขนาดของเงินกองทุนของบริษัท ซึ่งส่งผลกระทบต่อการชำระราคาและการส่งมอบหลักทรัพย์ รวมทั้งอาจก่อให้เกิดความเสียหายต่อฐานะของบริษัทด้วย
- การเปลี่ยนแปลงของสภาพเศรษฐกิจหรือภาวะตลาดส่งผลลบต่อฐานะการเงินของลูกค้าหรือคู่สัญญา ส่งผลให้ลูกค้าหรือคู่สัญญาอาจขาดสภาพคล่องหรือประสบปัญหาทางการเงินซึ่งนำไปสู่การไม่สามารถปฏิบัติตามข้อตกลง สัญญา หรือภาระที่ได้ตกลงไว้กับบริษัทได้
- ลูกค้าขาดทุนจากการลงทุนในสัญญาซื้อขายล่วงหน้า ซึ่งส่งผลให้หลักประกันไม่เพียงพอและลูกค้าไม่สามารถวางหลักประกันเพิ่ม
- หลักประกันของลูกค้าที่กู้ยืมเงินเพื่อซื้อหลักทรัพย์ลดลง ส่งผลให้หลักประกันไม่เพียงพอและลูกค้าไม่สามารถวางหลักประกันเพิ่ม ซึ่งนำไปสู่การผิดนัดชำระหนี้
- การกระจุกตัวของการให้บริการลูกค้าหรือคู่สัญญากลุ่มใดกลุ่มหนึ่ง ทำให้มีความเสี่ยงที่บริษัทจะเสียหายจากการที่ลูกค้าหรือคู่สัญญาไม่สามารถปฏิบัติตามข้อตกลงได้

(2) การบริหารจัดการความเสี่ยง

การบริหารจัดการความเสี่ยงด้านเครดิตให้สอดคล้องกับธุรกรรมของบริษัท อย่างน้อยควรครอบคลุมในเรื่องดังนี้

- การทำความรู้จักลูกค้า (KYC/CDD) และการให้วงเงินลูกค้า
  - วิเคราะห์ความสามารถในการชำระหนี้ของลูกค้าด้วยความรอบคอบรัดกุม โดยมีการรวบรวมข้อมูลและประเมินฐานะทางการเงิน แหล่งที่มาของรายได้ที่นำมาใช้ในการชำระหนี้และการวางหลักประกันของลูกค้า
  - กำหนดวงเงินซื้อขายให้เหมาะสมกับฐานะ ความสามารถในการชำระหนี้ของลูกค้า รวมถึงกำหนดอำนาจอนุมัติวงเงินในระดับต่าง ๆ อย่างเหมาะสม
  - ในกรณีที่ลูกค้ามีหลายบัญชี (หลายผลิตภัณฑ์ที่ลงทุน) ให้พิจารณาวงเงินซื้อขายรวม (total exposure) ให้สอดคล้องกับฐานะและความสามารถในการชำระหนี้ของลูกค้า
  - กำหนดวงเงินของลูกค้าต่อราย เทียบเคียงกับขนาดของเงินกองทุนของบริษัทอย่างเหมาะสม เพื่อมิให้เกิดการกระจุกตัวในการให้วงเงินแก่ลูกค้ารายใดรายหนึ่งมากเกินไป รวมทั้งเพื่อมิให้บริษัทให้วงเงินลูกค้าสูงเกินฐานะของบริษัท อันอาจจะส่งผลกระทบต่อเสถียรภาพของระบบชำระราคาและส่งมอบหลักทรัพย์โดยรวม
  - มีการทบทวนวงเงินให้เป็นปัจจุบันและเหมาะสมกับข้อมูลลูกค้าที่อาจเปลี่ยนแปลงไป โดยต้องดำเนินการอย่างน้อยปีละครั้ง หรือเมื่อมีเหตุการณ์ที่ต้องทบทวนทันที เช่น ลูกค้าชำระหนี้ล่าช้า ลูกค้าผิดนัดชำระหนี้ และธุรกิจของลูกค้าประสบความเสียหาย เป็นต้น

- การควบคุมดูแลหลักประกัน
  - มีการควบคุมดูแลหลักประกัน โดยคำนึงถึงคุณภาพ ความเพียงพอและประเภทของหลักประกันให้เป็นไปตามเกณฑ์ เพื่อป้องกันความเสี่ยงจากการขาดทุนจำนวนมากในบัญชีลูกค้า รวมถึงการบังคับขายหลักทรัพย์ (force sell)/ หรือปิดฐานะสัญญาซื้อขายล่วงหน้า (force close) หากลูกค้าไม่สามารถนำหลักประกันมาวางเพิ่มตามข้อกำหนดของบริษัท
  - กำหนดแนวทางการปฏิบัติในการวางหลักประกัน การเรียกหลักประกัน การบังคับหลักประกัน เพื่อป้องกันความเสียหายที่อาจจะเกิดขึ้นทั้งแก่ลูกค้าและบริษัท

- การให้กู้ยืมเงินเพื่อซื้อหลักทรัพย์
  - กำหนดรายชื่อหลักทรัพย์ที่อนุญาตให้ซื้อขายในบัญชีมาร์จิ้นได้ โดยคำนึงถึงคุณภาพหลักทรัพย์ สภาพคล่อง ความผันผวนของราคา และความเสี่ยงของแต่ละหลักทรัพย์เป็นสำคัญ และกำหนด

อัตรามาร์จิ้นเริ่มต้นที่เหมาะสมสำหรับแต่ละหลักทรัพย์ รวมถึงกำหนดจำนวนหลักทรัพย์ที่อนุญาตให้ซื้อหรือวางเป็นประกันเพื่อควบคุมมิให้มีการกระจุกตัวในหลักทรัพย์ใดหลักทรัพย์หนึ่งมากเกินไป

- กำหนดการให้วงเงินลูกค้าในบัญชีมาร์จิ้นที่เหมาะสมกับฐานะการเงินของลูกค้า
- มีการติดตามและรายงานธุรกรรมที่มีนัยสำคัญให้คณะกรรมการบริษัทหรือคณะกรรมการที่ได้รับมอบหมายรับทราบ
- ควบคุมยอดหนี้คงค้างเนื่องจากการให้กู้ยืมเงินเพื่อซื้อหลักทรัพย์ให้เป็นไปตามหลักเกณฑ์ที่กำหนด เช่น ลูกค้ารายใดรายหนึ่ง เมื่อสิ้นวันหนึ่ง ๆ ต้องไม่เกินร้อยละ 25 ของเงินกองทุนของบริษัทหลักทรัพย์/ ลูกค้าทุกรายรวมกันภายหลังหักค่าเผื่อหนี้สงสัยจะสูญแล้ว เมื่อสิ้นวันหนึ่ง ๆ ต้องไม่เกินกว่า 5 เท่าของเงินกองทุนของบริษัทหลักทรัพย์ เป็นต้น

- การลงทุนเพื่อบริษัท
  - มีการกระจายการลงทุน ไม่ลงทุนกระจุกตัวในหลักทรัพย์ใดหนึ่งหรือหลักทรัพย์ของบริษัทที่อยู่ในเครือเดียวกันที่สูงเกินไป รวมถึงลงทุนในหลักทรัพย์ที่ได้รับการจัดอันดับความน่าเชื่อถือทางเครดิตที่ดี

4.4 ความเสี่ยงด้านการให้บริการและติดต่อลูกค้า (client conduct risk)

(1) ความเสี่ยงด้านการให้บริการและติดต่อลูกค้า

ความเสี่ยงด้านการให้บริการและติดต่อลูกค้าเป็นความเสี่ยงที่บริษัทจะได้รับความเสียหาย จากการที่ลูกค้าได้รับความเสียหาย หรือได้รับบริการที่ไม่มีคุณภาพ ไม่เป็นธรรม ไม่เหมาะสม หรือไม่เป็นไปตามมาตรฐานการปฏิบัติงาน/กฎเกณฑ์ที่เกี่ยวข้อง ซึ่งในการให้บริการและติดต่อลูกค้าของบริษัทควรดำเนินการโดยคำนึงถึงประโยชน์ที่ดีที่สุดของลูกค้าเป็นสำคัญ ทั้งนี้ ความเสี่ยงด้านการให้บริการและติดต่อลูกค้าอาจเกิดจากเหตุการณ์ต่าง ๆ เช่น

- การให้คำแนะนำการลงทุนและข้อมูล หรือการให้บริการที่ไม่เหมาะสมกับลูกค้า ทั้งด้านความรู้ความเข้าใจ ความต้องการ และระดับความเสี่ยงของลูกค้า
- การให้คำแนะนำการลงทุนและข้อมูลที่ไม่ถูกต้อง/ไม่ครบถ้วน/ไม่เพียงพอต่อการตัดสินใจ
- บริษัทถูกใช้เป็นช่องทางในการกระทำไม่เหมาะสม เช่น ลูกค้าส่งคำสั่งซื้อขายที่ไม่เหมาะสม หรือเปิดบัญชี nominee เพื่อใช้ดำเนินการที่อาจเกี่ยวข้องกับการฟอกเงินหรือการกระทำผิดกฎหมายอื่น ๆ เป็นต้น
- ทรัพย์สินของลูกค้าภายใต้การดูแลของบริษัทเกิดความเสียหายหรือถูกนำไปใช้โดยมิชอบ
- ข้อมูลของลูกค้ารั่วไหลหรือถูกนำไปใช้ประโยชน์

(2) การบริหารจัดการความเสี่ยง

การบริหารจัดการความเสี่ยงด้านการให้บริการและติดต่อลูกค้าในแต่ละธุรกรรมที่เกี่ยวข้องของบริษัท อย่างน้อยควรครอบคลุมเรื่องดังนี้

- **การทำความรู้จักลูกค้า**
  - รวบรวมและประเมินข้อมูลลูกค้าเพื่อทำความรู้จักลูกค้า (สามารถระบุตัวตนที่แท้จริงของลูกค้าและผู้ได้รับผลประโยชน์ที่แท้จริง (beneficial owner) ได้) จัดประเภทลูกค้า ประเมินความเหมาะสมในการลงทุนหรือการทำธุรกรรม รวมถึงพิจารณาศักยภาพและความสามารถในการปฏิบัติตามข้อตกลงในการใช้บริการ
  - มีการจัดประเภทลูกค้าเป็นกลุ่มต่าง ๆ เพื่อให้สามารถนำเสนอบริการที่สอดคล้องกับประเภทลูกค้าและสามารถติดตามพฤติกรรม การซื้อขาย ในกลุ่มลูกค้าที่มีความเสี่ยงต่อบริษัท และแจ้งให้ลูกค้าทราบเกี่ยวกับกลุ่มประเภทลูกค้าและสิทธิต่าง ๆ ที่เกี่ยวข้อง
  - ทบทวนและปรับปรุงข้อมูลลูกค้าให้เป็นปัจจุบันในระยะเวลาที่เหมาะสม หรือเมื่อปรากฏข้อเท็จจริงที่พึงทราบได้ว่า ข้อมูลที่มีอยู่นั้นไม่ถูกต้องหรือมีความคลาดเคลื่อนไปจากความเป็นจริง
- **การให้คำแนะนำการลงทุนให้กับลูกค้า**
  - พิจารณาถึงความเหมาะสมในการลงทุน วัตถุประสงค์ในการลงทุน ฐานะการเงิน และความต้องการของลูกค้า ในการให้คำแนะนำการลงทุนแก่ลูกค้า
  - มีกระบวนการ/ขั้นตอนในการให้คำแนะนำการลงทุนและข้อมูลที่เหมาะสมกับลูกค้าอย่างครบถ้วน ถูกต้อง และเพียงพอต่อการตัดสินใจลงทุน รวมถึงเปิดเผยลักษณะของผลิตภัณฑ์ เงื่อนไข และความเสี่ยงของผลิตภัณฑ์
  - มีกระบวนการที่ทำให้มั่นใจว่าลูกค้าได้รับคำแนะนำเกี่ยวกับบริการหรือผลิตภัณฑ์อย่างถูกต้อง ครบถ้วน สมเหตุสมผล และไม่ทำให้เกิดความเข้าใจผิด
  - ศึกษาและทำความเข้าใจผลิตภัณฑ์ที่จะนำมาให้บริการลูกค้า
  - กำหนดนโยบาย หลักเกณฑ์การคัดเลือกผลิตภัณฑ์ที่นำมาเสนอให้ลูกค้า และมีกระบวนการประเมินความเสี่ยงและความเหมาะสมของผลิตภัณฑ์ที่จะนำมาเสนอให้ลูกค้า

- มีระบบงานในการให้บริการผลิตภัณฑ์ที่มีความเสี่ยงสูงหรือมีความซับซ้อน โดยอย่างน้อยต้องเป็นไปตามที่ประกาศกำหนด
- กรณีลูกค้าเปราะบาง ต้องให้บริการอย่างระมัดระวังและเสนอขายสินค้าที่เหมาะสม

- **การดูแลทรัพย์สินและข้อมูลลูกค้า**
  - ปฏิบัติตามกฎเกณฑ์เกี่ยวกับการดูแลรักษาทรัพย์สินของลูกค้าและกฎหมายคุ้มครองข้อมูลส่วนบุคคล
  - มีระบบควบคุมภายในที่ดีในการดูแลรักษาทรัพย์สินของลูกค้า เพื่อให้มั่นใจว่าทรัพย์สินของลูกค้าครบถ้วน ปลอดภัย และมีระบบในการดูแลรักษาข้อมูลของลูกค้า ไม่ให้ถูกนำไปใช้ประโยชน์
  - จัดส่งเอกสารหลักฐานเกี่ยวกับการทำธุรกรรมของลูกค้าและรายงานแสดงทรัพย์สินให้แก่ลูกค้า เพื่อให้ลูกค้าได้รับทราบถึงรายการที่เกิดขึ้นในบัญชีของตน ตลอดจนภาระในการชำระค่าหลักทรัพย์หรือหนี้สินที่เกิดขึ้นระหว่างลูกค้าและบริษัท
  - การแก้ไขเปลี่ยนแปลงข้อมูลของลูกค้าทุกครั้งต้องมีระบบการควบคุมภายในที่เหมาะสมและสอบยันการแก้ไขเปลี่ยนแปลงข้อมูลของลูกค้าที่ต้องดำเนินการก่อนที่จะทำรายการเพื่อให้มั่นใจว่าการดำเนินการดังกล่าวเป็นความประสงค์ของลูกค้าที่แท้จริง
  - มีการสอบทานความถูกต้องและครบถ้วนในการแยกทรัพย์สินลูกค้า (maker-checker) และรายงานต่อผู้บริหารที่รับผิดชอบในสายงาน

- **การส่งคำสั่งซื้อขายไม่เหมาะสม**

  จัดให้มีระบบงานติดตามพฤติกรรมการส่งคำสั่งซื้อขายที่อาจเข้าข่ายไม่เหมาะสมและดำเนินการอย่างเข้มงวด ตลอดจนรายงานให้ผู้บริหารทราบเพื่อป้องกันการซื้อขายที่ไม่เหมาะสมและคำนึงถึงความเชื่อมั่นต่อระบบโดยรวม

4.5 ความเสี่ยงด้านฐานะการเงิน (prudential risk)

(1) ความเสี่ยง

ความเสี่ยงด้านฐานะการเงินเป็นความเสี่ยงที่เกิดจากการที่บริษัทไม่สามารถดำรงเงินกองทุนได้ตามเกณฑ์ที่สำนักงานกำหนด โดยการดำรงเงินกองทุนของบริษัทมีวัตถุประสงค์เพื่อให้เชื่อมั่นได้ว่า บริษัทมีทรัพย์สินที่สามารถนำไปใช้ชำระหนี้สินได้ทั้งหมดและมีส่วนเกินที่เพียงพอรองรับความเสี่ยงจากการประกอบธุรกิจหรือ

ภาระอื่น ๆ ที่อาจมีผลกระทบกับความสามารถในการชำระหนี้ได้ โดยเหตุการณ์ความเสี่ยงด้านฐานะการเงินที่อาจเกิดขึ้นจากการประกอบธุรกิจ มีดังนี้

- การทำธุรกรรมของบริษัทที่ส่งผลกระทบต่อเงินทุน สภาพคล่องของบริษัท เช่น ธุรกรรมนายหน้าซื้อขายหลักทรัพย์ ตัวแทนซื้อขายสัญญาซื้อขายล่วงหน้า ธุรกรรมการซื้อขายรายใหญ่ (block trade) การให้กู้ยืมเงินเพื่อซื้อหลักทรัพย์ (margin) การจัดจำหน่ายหลักทรัพย์ (underwrite) การลงทุนเพื่อเป็นทรัพย์สินของบริษัท (proprietary trading)
- ปริมาณการซื้อขายมีการเปลี่ยนแปลงอย่างมีนัยสำคัญจากการทำธุรกรรมการซื้อขายรายใหญ่ (block trade) หรือมีการปรับสัดส่วนของหุ้นไทยจาก MSCI Index Review
- ลูกค้าผิดนัดชำระราคา/ส่งมอบหลักทรัพย์
- ไม่สามารถกระจายหรือเสนอขายหลักทรัพย์ได้เต็มจำนวนตามที่รับประกันไว้ ในกรณี firm underwriting ทำให้บริษัทรับเข้าบัญชีบริษัท
- บริษัทภายในกลุ่มธุรกิจประสบปัญหา ส่งผลให้บริษัทอาจจะมีการให้ความช่วยเหลือทางการเงิน เช่น ให้เงินกู้ยืมเพิ่มมากขึ้น เป็นต้น และส่งผลต่อฐานะของบริษัท หากบริษัทดังกล่าวไม่สามารถชำระหนี้คืนได้เมื่อบริษัทขาดสภาพคล่อง

(2) การบริหารจัดการความเสี่ยง

การบริหารจัดการความเสี่ยงด้านฐานะการเงิน ให้สอดคล้องกับธุรกรรมของบริษัท อย่างน้อยควรครอบคลุมเรื่องดังนี้

- กำหนดให้ฝ่ายงานต่าง ๆ ที่มีธุรกรรมใหม่ที่กระทบต่อฐานะการเงินของบริษัท ต้องตรวจสอบกับฝ่ายบัญชีและการเงิน เพื่อทดสอบให้แน่ใจว่าเงินกองทุนของบริษัทมีความเพียงพอให้การทำธุรกรรมนั้นไม่ส่งผลให้เงินกองทุนของบริษัทต่ำกว่าเกณฑ์ที่กำหนด และดำรงอยู่ในระดับที่เหมาะสม
- มีการทดสอบภาวะวิกฤต (stress test) ในสมมติฐานต่าง ๆ เพื่อประเมินผลกระทบต่อเงินกองทุนของบริษัทหากเกิดวิกฤตทางการเงิน
- กำหนดเกณฑ์อัตราส่วนความเพียงพอของเงินกองทุน (early warning level) ภายในบริษัทที่สูงกว่าเกณฑ์ที่สำนักงานกำหนด เพื่อเป็นสัญญาณให้บริษัทเฝ้าระวังหรือดำเนินการตามแผนของบริษัทเพื่อให้สามารถดำรงเงินกองทุนของบริษัทได้ ซึ่งรวมถึงกำหนดแนวทางการรายงานผู้บริหารระดับสูงให้รับทราบ

- กำหนดมาตรการเพื่อลดระดับความเสี่ยงที่บริษัทเผชิญอยู่ เช่น จำกัดหรือลดธุรกรรมที่มีความเสี่ยง เป็นต้น
- กำหนดแผนการเพิ่มเงินกองทุนและการจัดหาเงินทุนกรณีเร่งด่วนเพื่อดำรงเงินกองทุนให้เป็นไปตามเกณฑ์ของสำนักงาน เช่น วงเงินกู้ด้อยสิทธิ และแผนสนับสนุนเงินทุนจากบริษัทแม่ เป็นต้น

4.6 ความเสี่ยงด้านเทคโนโลยีสารสนเทศ (IT risk)

(1) ความเสี่ยง

ความเสี่ยงด้านเทคโนโลยีสารสนเทศเป็นความเสี่ยงที่บริษัทจะได้รับความเสียหายจากการนำเทคโนโลยีสารสนเทศมาใช้ในการดำเนินธุรกิจอย่างไม่เหมาะสม รวมทั้งความเสี่ยงที่เกิดขึ้นจากภัยคุกคามทางด้านเทคโนโลยีสารสนเทศหรือทางด้านไซเบอร์ที่ส่งผลกระทบต่อการดำเนินธุรกิจ ชื่อเสียง และความเชื่อมั่นในการใช้บริการและผลิตภัณฑ์ต่าง ๆ ในตลาดทุน โดยเหตุการณ์ความเสี่ยงด้านเทคโนโลยีสารสนเทศที่อาจเกิดขึ้นจากการประกอบธุรกิจ มีดังนี้

- ระบบซื้อขายหลักทรัพย์และสัญญาซื้อขายล่วงหน้าที่เชื่อมต่อกับตลาดหลักทรัพย์ และ/หรือ ตลาดสัญญาซื้อขายล่วงหน้า ในการส่งคำสั่งซื้อขาย เกิดความขัดข้อง
- เทคโนโลยีสารสนเทศของบริษัทไม่ตอบสนองต่อรูปแบบการดำเนินธุรกิจที่เปลี่ยนแปลง หรือไม่สามารถนำเทคโนโลยีสารสนเทศมาใช้ในการพัฒนาบริการหรือผลิตภัณฑ์ใหม่ หรือจัดการได้อย่างมีประสิทธิภาพ ซึ่งส่งผลต่อศักยภาพในการแข่งขันของบริษัท
- เกิดภัยคุกคามทางไซเบอร์ เช่น การพยายามบุกรุกโจมตีระบบ (hacking) การเรียกค่าไถ่ (Ransom) เป็นต้น
- เกิดข้อผิดพลาดที่ส่งผลก่อให้เกิดช่องโหว่ทางด้านเทคโนโลยีที่ใช้ในการดำเนินงานของบริษัทและความมั่นคงปลอดภัยของบริษัทและลูกค้า
- อุปกรณ์เครื่องมือทางด้านเทคโนโลยีสารสนเทศ ระบบงาน และระบบฐานข้อมูลต่าง ๆ สูญหายหรือถูกทำลาย ส่งผลให้เกิดการรั่วไหล ความผิดพลาดในการสำรองข้อมูล หรือการสูญหายของข้อมูล
- มีการบริหารจัดการและควบคุมกระบวนการและระบบด้านเทคโนโลยีสารสนเทศที่ไม่เพียงพอ หรือมีการดำเนินงานที่อาจขัดต่อกฎหมายหรือระเบียบข้อบังคับต่าง ๆ ส่งผลทำให้เกิดช่องโหว่ต่อการรักษาความปลอดภัย ความถูกต้องเชื่อถือได้ของระบบและข้อมูล รวมถึงความพร้อมใช้งานของระบบในการให้บริการแก่ลูกค้า

(2) การบริหารจัดการความเสี่ยง

การบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ ในแต่ละธุรกรรมที่เกี่ยวข้องของบริษัท อย่างน้อยควรครอบคลุมเรื่องดังนี้

- จัดให้มีการบริหารจัดการระบบและบุคลากรด้านเทคโนโลยีสารสนเทศที่เหมาะสมและรัดกุม
- กำหนดนโยบายและวิธีปฏิบัติการรักษาความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศ (IT security policy) เป็นลายลักษณ์อักษรและผ่านการพิจารณาอนุมัติโดยคณะกรรมการบริษัท
- มีการควบคุมไม่ให้บุคคลที่ไม่เกี่ยวข้องเข้าถึงหรือล่วงรู้ข้อมูลที่สำคัญ
- จัดให้มีระบบป้องกันการบุกรุกโจมตี ในระบบงานและระบบเครือข่ายของบริษัท
- จัดให้มีการสำรองข้อมูล และมีการทดสอบการนำข้อมูลสำรองกลับมาใช้งาน กรณีเกิดเหตุขัดข้อง
- ติดตามและวิเคราะห์แนวโน้มการเปลี่ยนแปลงด้านเทคโนโลยีดิจิทัลเพื่อนำมาพัฒนาบริการหรือผลิตภัณฑ์ใหม่ ให้ตอบสนองต่อการดำเนินธุรกิจในปัจจุบันมากขึ้น เช่น การวิเคราะห์ข้อมูลขนาดใหญ่ (big data) มาใช้วิเคราะห์ความต้องการและพฤติกรรมของลูกค้า ข้อมูลการซื้อขาย และข้อมูลหลักทรัพย์ต่าง ๆ เพื่อคงความสามารถในการแข่งขันของบริษัท เป็นต้น
- จัดให้มีการฝึกอบรมให้ความรู้ และสร้างความตระหนักรู้ในภัยคุกคามด้านเทคโนโลยีสารสนเทศในรูปแบบต่าง ๆ ให้แก่พนักงานของบริษัท
- จัดให้มีการทดสอบและทบทวนขั้นตอนปฏิบัติหรือแผนการบริหารจัดการเหตุการณ์ผิดปกติด้านเทคโนโลยีสารสนเทศ อย่างน้อยปีละ 1 ครั้ง โดยต้องครอบคลุมถึงการทดสอบการบริหารจัดการเหตุการณ์ด้านภัยคุกคามทางไซเบอร์ (cyber security drill)
- ภายหลังการทดสอบต้องมีการประเมินประสิทธิภาพของแผนการทดสอบ และให้รายงานผลการประเมินประสิทธิภาพต่อกรรมการบริษัท

บริษัทอาจมีการจัดประเภทความเสี่ยงที่แตกต่างออกไป แต่ครอบคลุมความเสี่ยงที่สำคัญ ตามที่กล่าวมาได้ทั้งนี้ ขึ้นอยู่กับลักษณะธุรกิจ ขนาด เป็นต้น

อนึ่ง บริษัทควรพิจารณาความเสี่ยงด้านอื่น ๆ ที่อาจมีผลกระทบต่อบริษัท เช่น ความเสี่ยงด้านชื่อเสียง (reputation risk) ความเสี่ยงด้านมหันตภัย (catastrophe risk) ความเสี่ยงที่เกิดขึ้นใหม่ (emerging risk) เป็นต้น เพื่อประกอบการกำหนดนโยบายการบริหารความเสี่ยงและกรอบการบริหารความเสี่ยงให้มีความครอบคลุมอย่างมีประสิทธิภาพและประสิทธิผลมากยิ่งขึ้น

5. การติดตามและทบทวนความเสี่ยง

บริษัทต้องจัดให้มีการติดตามและทบทวนความเสี่ยง อย่างน้อยดังนี้

5.1 ติดตามการดำเนินงานว่า หน่วยงานต่าง ๆ ได้ปฏิบัติตามแผนการบริหารความเสี่ยงที่กำหนดและเป้าหมายที่วางไว้ รวมถึงสอบทานการดำเนินธุรกิจให้มีการปฏิบัติงานเป็นไปตามกฎหมาย กฎเกณฑ์ และหลักเกณฑ์ของหน่วยงานกำกับดูแล เช่น สำนักงาน ก.ล.ต. ตลาดหลักทรัพย์แห่งประเทศไทย และสำนักงานป้องกันและปราบปรามการฟอกเงิน เป็นต้น

5.2 ทบทวนและประเมินประสิทธิภาพของระบบบริหารความเสี่ยง พร้อมทั้งความสอดคล้องของระบบบริหารความเสี่ยงกับกลยุทธ์ของบริษัทอย่างน้อยปีละหนึ่งครั้ง หรือเมื่อมีเหตุการณ์สำคัญ เช่น มีการเปลี่ยนแปลงรูปแบบธุรกิจ/มีการออกผลิตภัณฑ์/บริการใหม่ เป็นต้น ที่ส่งผลกระทบต่อความเสี่ยงของบริษัท เพื่อปรับปรุงให้เหมาะสมกับความเสี่ยงที่เปลี่ยนแปลงไป

5.3 ติดตามความเสี่ยงที่สำคัญและความเสี่ยงที่เกิดขึ้นใหม่ (emerging risk) ที่ส่งผลกระทบต่อการดำเนินงานของบริษัท

- ติดตามสถานการณ์ และกำหนดแนวทางติดตามเหตุการณ์ที่เป็นสาเหตุของปัจจัยความเสี่ยง เพื่อกำหนดมาตรการในการป้องกันและจำกัดความเสียหายได้อย่างทันการณ์ โดยปัจจัยที่ควรติดตามเช่น ภาวะการแข่งขัน การเปลี่ยนแปลงพฤติกรรมของกลุ่มลูกค้าเป้าหมาย การเปลี่ยนแปลงของเทคโนโลยี ปัจจัยทางเศรษฐกิจ และข้อกำหนดของทางการ เป็นต้น
- คณะกรรมการบริษัทควรรับทราบความเสี่ยงจากธุรกรรมต่าง ๆ ในบริษัท โดยคณะกรรมการบริหารความเสี่ยง ฝ่ายบริหารความเสี่ยงหรือหน่วยงานอื่นที่บริษัทมอบหมาย มีหน้าที่ควบคุม ติดตามความเสี่ยงในธุรกรรมต่าง ๆ และจัดทำรายงานสรุปผลการติดตามความเสี่ยงอย่างครบถ้วน เพื่อนำเสนอคณะกรรมการบริษัทตามระยะเวลาที่เหมาะสม หรือต้องรายงานทันทีเมื่อเกิดเหตุการณ์ที่มีนัยสำคัญ รวมถึงต้องสื่อสารให้ทุกหน่วยงานที่เกี่ยวข้องรับทราบอย่างชัดเจน

5.4 ติดตาม และพิจารณาแนวทางแก้ไขข้อบกพร่องจากการปฏิบัติงานของบริษัท เมื่อตรวจพบข้อบกพร่องที่สำคัญที่เกี่ยวข้องกับการปฏิบัติที่ไม่เป็นไปตามกฎหมาย กฎเกณฑ์ หรือมีประเด็นที่ตรวจพบจากการตรวจสอบของทางการหรือหน่วยงานกำกับดูแลของบริษัท โดยให้รายงานต่อกรรมการ เช่น คณะกรรมการบริษัท หรือคณะกรรมการบริหารความเสี่ยง เพื่อพิจารณาแนวทางการแก้ไขและสั่งการแก้ไขภายในระยะเวลาอันควร

6. การรายงาน

บริษัทต้องจัดให้มีกลไกการติดตามและรายงานในเรื่องดังต่อไปนี้ ไปยังผู้บริหาร คณะกรรมการที่ได้รับมอบหมาย และคณะกรรมการบริษัท ตามความเหมาะสม เพื่อให้บริษัทมั่นใจว่าสามารถตอบสนองกับเหตุการณ์ต่าง ๆ ได้อย่างทันท่วงที หรือการกำกับดูแลความเสี่ยงของบริษัทอยู่ในระดับความเสี่ยงที่ยอมรับได้ โดยอย่างน้อยมีการรายงานเรื่องต่อไปนี้

6.1 ผลการบริหารความเสี่ยงในเรื่องสำคัญ เพื่อให้ผู้บริหาร คณะกรรมการที่ได้รับมอบหมาย และคณะกรรมการบริษัทรับทราบถึงข้อมูลที่สำคัญในเรื่องของการบริหารความเสี่ยง และสั่งการให้ดำเนินการตามความจำเป็น

6.2 การปฏิบัติงานที่ไม่เป็นไปตามกฎหมายและกฎเกณฑ์ของทางการ รวมถึงมาตรการควบคุม/ระเบียบของบริษัท

7. การบริหารความต่อเนื่องทางธุรกิจ (BCP/BCM)

การจัดทำกลยุทธ์และนโยบายการบริหารความต่อเนื่องทางธุรกิจ (business continuity management: “BCM”) และแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่อง (business continuity plan : “BCP”) เป็นเครื่องมือสำคัญในการเตรียมความพร้อมให้บริษัทสามารถดำเนินธุรกิจได้อย่างต่อเนื่องเมื่อเกิดเหตุการณ์ที่ทำให้การปฏิบัติงานตามปกติของบริษัทต้องหยุดชะงัก เช่น อุบัติเหตุ ภัยธรรมชาติ ภัยทางการเมือง การสูญเสียผู้บริหารหรือบุคลากรหลักที่สำคัญ การหยุดทำงานของระบบเครือข่ายคอมพิวเตอร์ระบบสื่อสาร หรือโครงสร้างพื้นฐานในการดำเนินงานด้านต่าง ๆ เป็นต้น

ดังนั้น บริษัทควรมีการจัดทำแผนรองรับการดำเนินธุรกิจต่อเนื่องของกระบวนการปฏิบัติงานหรือระบบงานที่สำคัญ เพื่อรองรับความเสี่ยงในด้านต่าง ๆ และจำกัดหรือลดผลกระทบที่อาจเกิดขึ้นจากการหยุดชะงักของการดำเนินงานที่เกิดจากเหตุการณ์ความเสียหายในรูปแบบต่าง ๆ โดยในการจัดทำกลยุทธ์และนโยบาย BCM/BCP ที่เหมาะสมนั้น บริษัทต้องมีการดำเนินการอย่างน้อย ดังนี้

7.1. คณะกรรมการบริษัท หรือคณะกรรมการที่ได้รับมอบหมายมีหน้าที่ในการพิจารณาและอนุมัติ BCM และ BCP

- คณะกรรมการบริษัท หรือคณะกรรมการที่ได้รับมอบหมายมีหน้าที่ในการพิจารณาและอนุมัติกลยุทธ์และกรอบนโยบายการบริหารความต่อเนื่องทางธุรกิจของบริษัท กำกับดูแลให้มีการดำเนินการตามกลยุทธ์และนโยบายที่วางไว้ ตลอดจนจัดสรรทรัพยากรและงบประมาณแก่หน่วยงานที่เกี่ยวข้องอย่างเพียงพอ ทั้งนี้ คณะกรรมการบริษัทอาจแต่งตั้งคณะทำงานเป็นผู้รับผิดชอบงานด้านปฏิบัติการได้ โดยการมอบหมายควรทำเป็นลายลักษณ์อักษร และควรจัดให้มีกระบวนการรายงานการดำเนินการให้คณะกรรมการบริษัท หรือคณะกรรมการที่ได้รับมอบหมายรับทราบเพื่อติดตามติดตามดูแลการดำเนินการดังกล่าวด้วย
- คณะกรรมการบริษัท หรือคณะกรรมการที่ได้รับมอบหมายมีบทบาทในการปลูกฝังเรื่องการบริหารความต่อเนื่องทางธุรกิจให้เข้ามาเป็นส่วนหนึ่งของวัฒนธรรมองค์กรและกระบวนการปฏิบัติงานของพนักงานในบริษัท โดยส่งเสริมให้พนักงานมีความเข้าใจ ตระหนักถึงความสำคัญของการบริหารความต่อเนื่องทางธุรกิจ และเข้าใจในบทบาทหน้าที่ของตนเองเมื่อเกิดเหตุการณ์ที่ทำให้การปฏิบัติงานตามปกติของบริษัทต้องหยุดชะงัก รวมถึงสนับสนุนให้มีการอบรมพนักงาน เพื่อสร้างความเข้าใจในบทบาทหน้าที่

7.2 การกำหนดสถานการณ์จำลอง

- กำหนดสถานการณ์จำลองเพื่อประเมินความเสี่ยงและผลกระทบของภัยด้านต่าง ๆ ที่อาจเกิดขึ้นในระดับความรุนแรง และรูปแบบความเสียหายที่แตกต่างกันประกอบการจัดทำแผนรองรับการดำเนินธุรกิจต่อเนื่องของบริษัทเพื่อจัดเตรียมมาตรการเพื่อรองรับภัยที่อาจเกิดขึ้น โดยสถานการณ์จำลองที่ก่อให้เกิดการหยุดชะงักในการประกอบธุรกิจ เช่น ภัยธรรมชาติ จราจล โรคระบาด และอุบัติภัย เป็นต้น
- มีการกำหนดสถานการณ์วิกฤตร้ายแรง (worst case scenario) ที่อาจเกิดขึ้นเป็นสมมติฐานหนึ่งที่ใช้ในการจัดทำแผนรองรับการดำเนินธุรกิจต่อเนื่อง รวมทั้งทำการประเมินข้อจำกัดต่าง ๆ ที่อาจเกิดขึ้นเมื่อเกิดเหตุการณ์ความเสียหายด้วย

7.3 การทดสอบแผนรองรับการดำเนินธุรกิจต่อเนื่องของบริษัท

- กำหนดแผนงานในการทดสอบแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่องอย่างชัดเจน สอดคล้องกับนโยบาย กลยุทธ์ของบริษัท และสถานการณ์ในปัจจุบัน โดยกำหนดสถานการณ์จำลองแตกต่างกันในการทดสอบแต่ละครั้งและควรจำลองสถานการณ์ให้ใกล้เคียงความเป็นจริงมากที่สุด
- จัดให้มีการทดสอบแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่องสำหรับธุรกรรมสำคัญอย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงปัจจัยที่มีผลต่อความเสี่ยงอย่างมีนัยสำคัญ เพื่อให้มั่นใจว่า แผนรองรับการดำเนินธุรกิจอย่างต่อเนื่องของบริษัทสามารถนำไปใช้ปฏิบัติได้จริงและสอดคล้องกับความเสี่ยงและสถานการณ์ในปัจจุบัน
- การทดสอบแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่องควรรวมถึงการติดต่อประสานงานกับหน่วยงานที่เกี่ยวข้อง เช่น หน่วยงานทางการ ผู้ให้บริการหลัก สถาบันการเงิน เป็นต้น
- หลังการทดสอบแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่อง ต้องมีการประเมินประสิทธิภาพของแผนการตรวจสอบ และผลการทดสอบแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่อง โดยผู้ประเมินที่สามารถให้ความเห็นได้อย่างอิสระ (ผู้ประเมินอาจเป็นบุคคลภายในหรือภายนอกบริษัทก็ได้) และให้รายงานผลการประเมินประสิทธิภาพของแผนการตรวจสอบ และผลการทดสอบแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่อง ต่อคณะกรรมการบริษัทหรือคณะกรรมการที่ได้รับมอบหมาย

7.4 การทบทวนแผนรองรับการดำเนินธุรกิจต่อเนื่องของบริษัท

- ปรับปรุงและทบทวนแผนรองรับการดำเนินธุรกิจต่อเนื่องทุกครั้งเมื่อมีการเปลี่ยนแปลงที่มีนัยสำคัญ เช่น การเปลี่ยนแปลงโครงสร้างองค์กร/โครงสร้างการบังคับบัญชา การควบรวมกิจการ การมีฝ่ายงานใหม่ เพื่อให้แผนรองรับการดำเนินธุรกิจต่อเนื่องมีความเป็นปัจจุบันและสามารถปฏิบัติได้อย่างมีประสิทธิภาพอยู่เสมอ

8. การทดสอบภาวะวิกฤต (stress test)

เพื่อให้บริษัทมีฐานะการเงินที่เพียงพอในการรองรับความเสี่ยงในการประกอบธุรกิจ โดยมีการเตรียมการและการดำเนินการที่เกี่ยวข้องกับเงินกองทุนของบริษัทอย่างมีประสิทธิภาพ บริษัทควรมีการทดสอบภาวะวิกฤต (stress test) ในสมมติฐานต่าง ๆ เพื่อประเมินผลกระทบต่อเงินกองทุนของบริษัทหากเกิดเหตุการณ์ร้ายแรง โดยควรมีการกำหนดสมมติฐานที่สอดคล้องกับธุรกรรมของบริษัทและสถานการณ์ปัจจุบัน และกำหนดให้มีการรายงานผลการทดสอบไปยังคณะกรรมการบริษัทหรือคณะกรรมการที่ได้รับมอบหมายด้วย