

แนวทางบริหารความเสี่ยงของ COSO

The Committee of Sponsoring Organization of Treachery Commission (COSO) (2004) ได้เสนอ Enterprise Risk Management – Integrated Framework ให้แก่บริษัทเอกชน ไว้เป็นการทั่วไป ในการทำงานภายใต้บริษัทภิบาล ทั้งนี้การบริหารความเสี่ยงตามแนวทางนี้ เป็นการบริหารความเสี่ยงเชิงบูรณาการ ซึ่งมีความเสี่ยงด้านการปฏิบัติงาน เป็นความเสี่ยงหนึ่งที่ต้องบริหาร COSO พิจารณาความเสี่ยงว่าเป็นโอกาสที่บริษัทจะดำเนินการแล้วเกิดผลลัพธ์ที่เบี่ยงเบนจากวัตถุประสงค์ในทางลบ ซึ่งโดยทั่วไปจะเกี่ยวกับผลประกอบการ กำไร การทำให้กิจการเติบโต การไม่มีคืดความ หรือเหตุการณ์ร้ายต่างๆ ซึ่งไม่เคยคาดคิดมาก่อน ขึ้นกับปัจจัยของความเสี่ยง แล้วทำให้บริษัทได้รับความเสียหาย ทั้งนี้ความเสี่ยงที่เกิดขึ้นกับบริษัทอาจเกิดขึ้นพร้อมกันหลายประเภท และในกิจกรรมขององค์กรทุกระดับชั้นของการทำงานและทุกหน่วยงาน โดยที่ความเสี่ยงทั้งหลายที่เกิดขึ้นพร้อมกันย่อมมีสหสัมพันธ์ซึ่งกัน หรือเป็นเหตุปัจจัยของความเสี่ยงอื่นที่อาจเกิดขึ้นเพิ่มเติมหรือลดลงเป็นผลลัพธ์สืบเนื่องกัน จึงต้องพิจารณาความเสี่ยงทุกประเภทพร้อมกันสำหรับการปฏิบัติการในทุกระดับขององค์กร

COSO พิจารณาความเสี่ยงและจัดการกับความเสี่ยงแบ่งเป็น 3 มิติ

1. ประเภทของความเสี่ยง (Risk Objectives)

1.1 ความเสี่ยงด้านกลยุทธ์ (Strategic Objectives) เป็นความเสี่ยงจากการกำหนดกลยุทธ์และการดำเนินงานตามกลยุทธ์ ซึ่งให้ผลลัพธ์ผิดไปจากวัตถุประสงค์ด้วยเหตุปัจจัยภายนอกที่เปลี่ยนแปลง หรือจากการที่กลยุทธ์เป็นกลยุทธ์ที่ไม่เหมาะสม ขาดประสิทธิภาพและประสิทธิผล

1.2 ความเสี่ยงด้านการปฏิบัติการ (Operations Objectives) เป็นความเสี่ยงจากการปฏิบัติการ

1.3 ความเสี่ยงประเภทที่ต้องรายงาน (Reporting Objectives) ส่วนใหญ่เป็นความเสี่ยงทางการเงิน ซึ่งสำหรับบริษัทประกันภัยแล้ว ความเสี่ยงในกลุ่มนี้เป็นความเสี่ยงด้านกาตลาด ด้านเครดิต ด้านการประกันภัย และด้านสภาพคล่อง

1.4 ความเสี่ยงต่อการผิดกฎ ระเบียบ และข้อบังคับ (Compliance Objectives) เป็นความเสี่ยงด้านการปฏิบัติงาน ซึ่งแยกออกเป็นการเฉพาะว่ามีเหตุปัจจัยจากการปฏิบัติการที่ผิดพลาด เนื่องจากบริษัทไปฝ่าฝืนต่อกฎ ระเบียบ และข้อบังคับ ที่กำหนดตามกฎหมายหรือโดยหน่วยงานภาครัฐ ซึ่งกำกับดูแล และยังสามารถขยายผลไปให้ครอบคลุมการฝ่าฝืนกฎระเบียบ และข้อบังคับที่ได้กำหนดขึ้นเองเป็นการภายในบริษัท

คณะกรรมการศึกษาความเสี่ยงด้านการปฏิบัติการเพียงด้านเดียวเป็นการเฉพาะ แยกจากความเสี่ยงประเภทอื่น

2. การจัดองค์กร (Organizational Levels) แบ่งเป็น 4 ระดับ

2.1 ระดับสูงสุดเป็นภาพรวม (Entity Level) ซึ่งกิจกรรมส่วนใหญ่เป็นความเสี่ยงที่พิจารณาจากมุมมองของผู้บริหารระดับสูงของบริษัท ที่ต้องพยายามพิจารณาความเสี่ยงทุกด้าน ประกอบกันเข้าอย่างเป็นระบบและเป็นเชิงบูรณาการมากที่สุด

2.2 ระดับสายงาน (Division) เป็น ความเสี่ยงที่เกิดขึ้นจากการดำเนินงานของสายงานหรือฝ่ายงานแต่ละฝ่ายขององค์กร

2.3 ระดับหน่วยธุรกิจ (Business Unit) ซึ่งเกิดขึ้นในหน่วยงานย่อยแต่ละหน่วยของสายงาน

2.4 ระดับบริษัทในเครือ (Subsidiary) โดยที่การบริหารงานเชิงบูรณาการของ COSO ได้ขยายขอบเขตการพิจารณาความเสี่ยงที่เกิดขึ้นภายนอกบริษัท ให้ไปครอบคลุมถึงความเสี่ยงของบริษัทในเครือด้วย

คณะทำงานเห็นด้วยกับแนวทางของ COSO ที่บริษัทประกันภัยจะต้องพิจารณาความเสี่ยงด้านการปฏิบัติการซึ่งเกิดจากการดำเนินงานในทุกระดับขององค์กร

3. ขั้นตอนการบริหารความเสี่ยง (Interrelated Components) COSO เสนอเป็นแนวทางให้บริษัทดำเนินการ ซึ่งที่ปรึกษาให้อ้างอิงขั้นตอนเหล่านี้

3.1 การสร้างและพัฒนาสภาพแวดล้อมภายในที่เอื้อต่อการบริหารความเสี่ยงด้านการปฏิบัติงาน (Internal Environment)

3.2 การระบุนโยบายและวัตถุประสงค์ของการบริหารความเสี่ยง (Objective Setting)

3.3 การระบุเหตุปัจจัยที่เป็นความเสี่ยงซึ่งจะนำไปสู่ความเสียหาย (Event Identification)

3.4 การวัดระดับความเสี่ยง (Risk Assessment)

3.5 การจัดการกับความเสี่ยง (Risk Response)

3.6 การลงมือบริหารความเสี่ยง (Control Activities)

3.7 การกระจายข่าวสารข้อมูลและการติดต่อสื่อสารในบริษัท (Information and Communication)

3.8 การติดตามสอดส่องดูแลระดับความเสี่ยง (Monitoring)

คณะทำงานเห็นด้วยกับขั้นตอนการบริหารความเสี่ยง เนื่องจากเป็นขั้นตอนขั้นพื้นฐานขั้นต่ำที่พึงมีในการกำกับความเสี่ยงด้านการปฏิบัติการ ทั้งนี้ได้เพิ่มเติมเรื่องการเปิดเผยข้อมูลเพื่อให้เป็นไปตามเกณฑ์การกำกับดูแลที่เป็นสากล Pillar III Market Discipline

