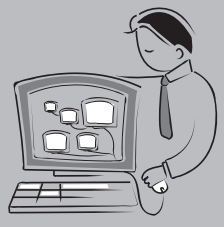


Corporate Governance

ดร.ศิลปพร ศรีจั่นเพชร
อาจารย์ประจำภาควิชาการบัญชี
คณะพาณิชยศาสตร์และการบัญชี มหาวิทยาลัยธรรมศาสตร์
sillapaporn@hotmail.com

การควบคุมภายใน : กรอบแนวทางการบริหารความเสี่ยง

ในฉบับก่อนได้เกริ่นให้ท่านผู้อ่านได้รู้จักกับการควบคุมภายในมาบ้างแล้ว การควบคุมภายในที่กล่าวถึงเป็นไปตามแนวคิดของโคโซ่ (COSO) โคโซ่เป็นใครที่ไหนกัน จึงมีอิทธิพลต่อแนวคิดของการควบคุมภายในได้เพียงนั้น คำตอบก็คือโคโซ่เป็นคณะกรรมการร่วม ซึ่งมาจากสถาบันวิชาชีพในระดับโลก เช่น สมาคมผู้ตรวจสอบภายใน สมาคมนักบัญชีบริหาร สมาคมผู้บริหารทางการเงิน สมาคมผู้สอบบัญชีและสมาคมการบัญชีของสหรัฐอเมริกา

คณะกรรมการกลุ่มนี้ได้ร่วมกันศึกษาวิจัย และพัฒนาแนวคิดของการควบคุมภายใน และได้ให้ความหมายของการควบคุมภายในว่าหมายถึง "กระบวนการปฏิบัติงานที่ถูกกำหนดร่วมกันโดยคณะกรรมการผู้บริหาร ตลอดจนพนักงานขององค์กรทุกระดับชั้น เพื่อให้เกิดความมั่นใจอย่างสมเหตุสมผลว่า วิธีการหรือการปฏิบัติงานตามที่กำหนดไว้จะทำให้บรรลุวัตถุประสงค์ของการควบคุม"

ระบบการควบคุมภายใน จึงประกอบด้วยนโยบายและวิธีปฏิบัติงานที่กำหนดขึ้นในองค์กร เพื่อให้เกิดความมั่นใจอย่างสมเหตุสมผลว่า กิจการจะบรรลุวัตถุประสงค์และเป้าหมาย ในเรื่องต่อไปนี้

- ความเชื่อถือได้ของรายงานทางการเงิน (Financial Objective)
- ประสิทธิภาพ (Efficiency) และประสิทธิผล (Effectiveness) ของการดำเนินงาน (Operational Objective)
- การปฏิบัติตามกฎหมายและข้อบังคับที่เกี่ยวข้อง (Compliance Objective)

องค์ประกอบของการควบคุมภายในตามแนวคิดของโคโซ่มี 5 ประการที่สัมพันธ์กัน ซึ่งได้แนะนำให้ท่านผู้อ่านรู้จักแล้วในฉบับก่อนนั้นประกอบด้วย (1) สภาพแวดล้อมของการควบคุม (2) การประเมินความเสี่ยง (3) กิจกรรมการควบคุม (4) สารสนเทศและการสื่อสาร และ (5) การติดตาม และประเมินผล

แนวคิดและโครงสร้างของการควบคุมภายในที่นำเสนอโดยโคโซ่ มีนัยความหมายที่ซ่อนไว้ในคำนิยาม ดังนี้

(1) การควบคุมภายในเป็นเรื่องของระบบ หรือกระบวนการที่ต้องจัดให้มีขึ้นเพื่อให้องค์กรบรรลุวัตถุประสงค์ที่กำหนดไว้

(2) การควบคุมภายในจะดีหรือไม่นั้น ขึ้นอยู่กับคน (ซึ่งหมายรวมถึงผู้บริหารและผู้ปฏิบัติงานทุกระดับในองค์กร) และที่สำคัญกว่านั้น ผู้บริหารมีส่วนสำคัญยิ่งในการสร้างบรรยากาศให้เกิดการควบคุมขึ้นในองค์กร

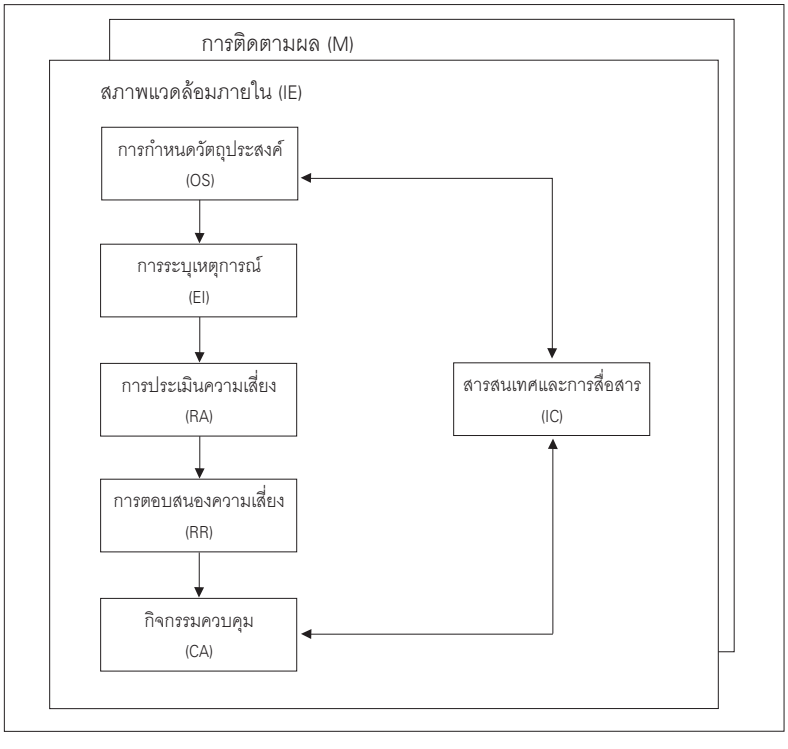
(3) การควบคุมภายในให้ความสำคัญกับเรื่องจริยธรรมและคุณภาพของคน ซึ่งเป็นการควบคุมที่มุ่งให้เกิดจิตสำนึก หรือที่เรียกว่าการควบคุมภายในแบบ Soft Control

(4) การควบคุมภายในเป็นการให้ความเชื่อมั่นอย่างสมเหตุสมผลเท่านั้น (Reasonable Assurance) ว่าองค์กรจะสามารถบรรลุวัตถุประสงค์ของการควบคุม ทั้งนี้เนื่องจากการควบคุมภายใน มีข้อจำกัดบางประการ เช่น ถึงแม้จะกำหนดระบบการควบคุมภายในไว้ดีเลิศเพียงใดก็ตาม แต่บุคลากรไม่ปฏิบัติตาม หรือผู้บริหารข้ามขั้นตอนของการควบคุมภายในเสียเอง

การจัดการความเสี่ยงขององค์กร

องค์ประกอบของการควบคุมภายในตามแนวคิดของโคโซ่ที่กล่าวข้างต้นนั้น เกิดขึ้นตั้งแต่ปี พ.ศ. 2535 และก็ไม่ได้มีการปรับปรุงจนกระทั่งในช่วง 2-3 ปีที่ผ่านมา หลังจากวิกฤตการณ์ที่เกิดขึ้นกับบริษัทเอนรอนในสหรัฐอเมริกา สาธารณชน และหน่วยงานกำกับดูแลต่างๆ รวมทั้งกฎหมาย Sarbanes Oxley Act 2002 ที่เกิดขึ้นตามมาก็หันมาเน้นถึงความสำคัญของการควบคุมภายในกันอีกครั้งหนึ่ง โคโซ่จึงได้โอกาสที่จะปรับปรุงแนวคิดของการควบคุมภายในเสียใหม่ในเดือนกันยายน พ.ศ. 2547

ตามแนวคิดใหม่นี้ โคโซ่ได้ขยายขอบเขตของการควบคุมภายในให้กว้างขวางมากขึ้นกว่าเดิม โดยการนำองค์ประกอบของการควบคุมภายในทั้ง 5 ประการมาปรับใหม่ให้เหมาะสม และเน้นแนวคิดเรื่องการจัดการความเสี่ยงขององค์กร (Enterprise Risk Management-Integrated Framework: ERM) ในปัจจุบันกลุ่มบุคคลในวิชาชีพไม่ว่าจะเป็นผู้บริหาร ผู้สอบบัญชี หรือผู้ตรวจสอบภายใน ล้วนแล้วแต่รู้จักและได้นำ COSO: ERM มาใช้งานกันแล้วทั้งนั้น



ภาพที่ 1 องค์ประกอบของ COSO: ERM

การจัดการความเสี่ยงขององค์กร หรือ ERM หมายถึง กระบวนการที่นำมาใช้ในการกำหนดกลยุทธ์ทั่วทั้งองค์กร และออกแบบไว้เพื่อระบุถึงเหตุการณ์ที่เป็นไปได้ ซึ่งอาจมีผลกระทบต่อองค์กร และจัดการกับความเสี่ยงให้อยู่ในขอบเขตที่ยอมรับได้ ทั้งนี้ เพื่อให้เกิดความมั่นใจอย่างสมเหตุสมผลว่าองค์กรจะบรรลุวัตถุประสงค์ในเรื่องต่อไปนี้

(1) วัตถุประสงค์เชิงกลยุทธ์ (Strategic: S) เป็นวัตถุประสงค์ระดับสูงและสัมพันธ์กับการสนับสนุนพันธกิจ

(2) วัตถุประสงค์การดำเนินการ (Operations: O) เป็นวัตถุประสงค์ของการใช้ทรัพยากรอย่างมีประสิทธิภาพ ประสิทธิผล และคุ้มค่า

(3) วัตถุประสงค์การรายงาน (Reporting: R) เป็นวัตถุประสงค์ เพื่อความเชื่อถือได้ของการรายงาน

(4) วัตถุประสงค์การปฏิบัติตามกฎระเบียบ (Compliance: C) เป็นวัตถุประสงค์ที่มุ่งให้มีการปฏิบัติตามกฎหมายและข้อบังคับที่เกี่ยวข้องกับองค์กร

เมื่อเปรียบเทียบกับการควบคุมภายในตามแนวคิดเดิม ท่านผู้อ่านคงสังเกตได้ว่าวัตถุประสงค์ของการควบคุมภายในตาม COSO: ERM ได้เพิ่มมาอีกหนึ่งอย่าง คือวัตถุประสงค์เชิงกลยุทธ์ นอกจากนี้องค์ประกอบของการจัดการความเสี่ยงมี 8 ประการที่สัมพันธ์กันดังแสดงในภาพที่ 1 (เปรียบเทียบกับ 5 องค์ประกอบตาม

แนวคิดเดิม) องค์ประกอบใหม่นี้ให้ความสำคัญกับเรื่องของความเสี่ยงมากขึ้นกว่าเดิม ซึ่งเชื่อมโยงกับกระบวนการจัดการ ดังนี้

(1) สภาพแวดล้อมภายใน

(Internal Environment: IE)

สภาพแวดล้อมภายในเป็นบรรยากาศหรือฐานรากที่เสริมสร้างให้เกิดการควบคุมขึ้นในองค์กร เช่น ความซื่อสัตย์และจริยธรรมของผู้บริหาร ปรัชญาการบริหารความเสี่ยง และการจัดให้มีการแบ่งแยกหน้าที่กันทำอย่างเพียงพอ

(2) การกำหนดวัตถุประสงค์

(Objective Setting: OS)

ในการดำเนินธุรกิจหรือในกิจกรรมใดๆ ก็ตาม องค์กรจะกำหนดวัตถุประสงค์ขึ้นมาก่อน เพื่อให้ผู้บริหารสามารถระบุเหตุการณ์ที่อาจเป็นไปได้ เพื่อให้บรรลุวัตถุประสงค์นั้น และสอดคล้องกับความเสี่ยงที่ยอมรับได้ เช่น ผู้บริหารกำหนดวัตถุประสงค์ทางด้านการดำเนินการผลิตโดยตั้งเป้าหมายว่าจะไม่ให้เกิดของเสียจากการผลิตเกิน 2%

(3) การระบุเหตุการณ์

(Event Identification: EI)

ผู้บริหารต้องระบุเหตุการณ์ภายในและภายนอก ซึ่งมีผลกระทบต่อการบรรลุวัตถุประสงค์ขององค์กร และมีการระบุถึงความเสี่ยง (เหตุการณ์ที่ส่งผลกระทบให้เกิดความเสียหายต่อวัตถุประสงค์ขององค์กร) และโอกาส (ความเป็นไปได้ที่จะเกิดเหตุการณ์ซึ่งส่งผลให้บรรลุวัตถุประสงค์ขององค์กร) ซึ่งเป็นช่องทางสนับสนุนกลยุทธ์ของผู้บริหาร

(4) การประเมินความเสี่ยง

(Risk Assessment: RA)

การวิเคราะห์ความเสี่ยง เป็นการพิจารณาโอกาสของการเกิดขึ้น และผลกระทบ เพื่อใช้เป็นพื้นฐานในการจัดการความเสี่ยง เกณฑ์การวัดระดับความเสี่ยงอาจเป็นระดับสูง กลาง หรือต่ำ

(5) การตอบสนองความเสี่ยง

(Risk Responses: RR)

ผู้บริหารจะตอบสนองความเสี่ยงโดยการหลีกเลี่ยง (Avoid) การยอมรับ (Accept) การลด (Reduce) หรือการร่วมรับ (Share) ความเสี่ยง

(6) กิจกรรมควบคุม

(Control Activities: CA)

ผู้บริหารจะกำหนดนโยบายและวิธีปฏิบัติที่จะสนับสนุนกิจกรรมที่จะป้องกันความเสี่ยงที่อาจเกิดขึ้น เพื่อช่วยให้เกิดความมั่นใจว่า ความเสี่ยงได้รับการตอบสนองอย่างมีประสิทธิผล เช่น การแบ่งแยกหน้าที่อย่างเหมาะสม การมีระบบเอกสารหลักฐานที่เหมาะสมและเพียงพอ

(7) สารสนเทศและการสื่อสาร

(Information and Communication : IC)

สารสนเทศและการสื่อสารมีวัตถุประสงค์เพื่อให้บุคลากรสามารถปฏิบัติงานตามความรับผิดชอบของตนได้อย่างมีประสิทธิผล ตลอดจนการกำหนดให้มีวิธีการควบคุมทรัพย์สินของกิจการ

(8) การติดตามผล

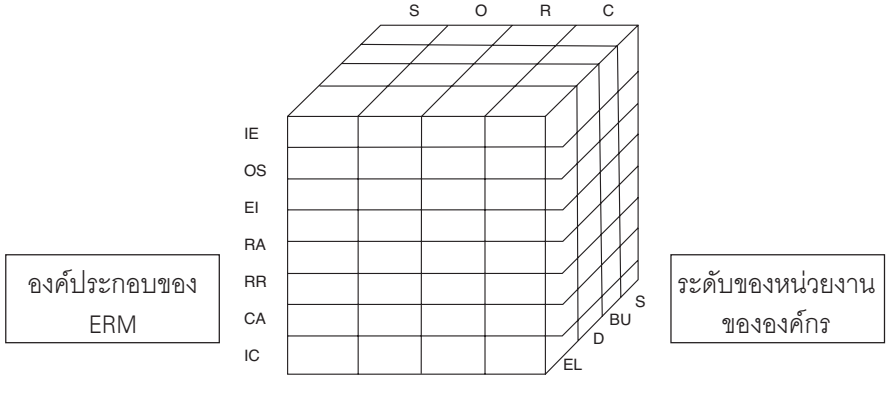
(Monitoring: M)

การติดตามและการประเมินผลช่วยให้ผู้บริหารมั่นใจได้ว่า นโยบายและวิธีการต่างๆ ที่กำหนดไว้มีการปฏิบัติตามอย่างมีประสิทธิผล ซึ่งอาจทำได้โดยการจัดให้มีระบบการรายงานผลการปฏิบัติงานและการตรวจสอบภายใน

COSO: ERM เป็นกรอบแนวทางการบริหารความเสี่ยงขององค์กร ซึ่งมีส่วนช่วยให้องค์กรบรรลุวัตถุประสงค์ที่กำหนดไว้และเป็นกระบวนการที่เกี่ยวข้องกับทุกคนและปัจจัยที่จะทำให้เกิดผลสำเร็จได้ก็คือผู้บริหารจะต้องให้การสนับสนุนอย่างจริงจัง

COSO: ERM อาจมาใช้ปฏิบัติโดยเน้นระดับในภาพรวมขององค์กร (1) ทั่วทั้งองค์กร (Entity-level: EL) (2) ระดับส่วนงาน (Division: D) (3) ระดับหน่วยงาน (Business units: BU) หรือ (4) ระดับหน่วยงานย่อย (Subsidiary: S) ดังแสดงในภาพที่ 2

ผู้บริหาร ผู้สอบบัญชี ผู้ตรวจสอบภายในและผู้ที่เกี่ยวข้อง ได้ใช้องค์ประกอบ COSO: ERM ในการปฏิบัติงานในหน้าที่ของตน ส่วนที่ว่าจะนำไปใช้งานอย่างไรนั้นจะกล่าวถึงในโอกาสต่อไป



ภาพที่ 2 ภาพสามมิติของ COSO: ERM