วารสารวิชาชีพบัญชี
บทความวิชาการ

COSO: ERM กับงานตรวจสอบภายใน

จันทนา สาขากร*

ในแวดวงวิชาการและวิชาชีพตรวจสอบในระดับสากลและในระดับประเทศไทยเอง เมื่อกล่าวถึง COSO หรือ The Committee of Sponsoring Organization of the Tread way Commission ที่เป็นคณะกรรมการร่วมของสถาบันวิชาชีพ 5 สถาบันคือ

1. American Institute of Certified Public Accountants (AICPA)
2. American Accounting Association (AAA)
3. Institute of Internal Auditors (IIA)
4. Institute of Management Accountants (IMA)
5. Financial Executives Institute (FEI)

ย่อมต้องนึกถึงกรอบการควบคุมภายในหรือโครงสร้างการควบคุมภายใน เนื่องจาก COSO ได้เสนอรายงานผลการศึกษาวิจัยและการพัฒนาแนวความคิดเกี่ยวกับการควบคุมภายในไว้กว่า 15 ปีที่ผ่านมา ตามแนวคิดการควบคุมภายใน 5 ประการที่สัมพันธ์ซึ่งกันและกันไว้เพื่อบรรลุวัตถุประสงค์ 3 ประการของการควบคุมภายในคือ

* รองศาสตราจารย์ประจำ ภาควิชาการบัญชี คณะพาณิชยศาสตร์และการบัญชี
มหาวิทยาลัยธรรมศาสตร์
ผู้สอบบัญชีรับอนุญาต

ปีที่ 3 ฉบับที่ 8
มีนาคม 2550
หน้า 75-79

1. ความมีประสิทธิภาพและประสิทธิผลของการดำเนินงาน (Effectiveness and Efficiency of Operation หรือ O) เป็นวัตถุประสงค์ที่มุ่งเน้นให้มีการใช้ทรัพยากรอย่างมีประสิทธิภาพและบรรลุเป้าหมายที่กำหนดไว้ขององค์การ

2. ความเชื่อถือได้ของรายงานทางการเงิน (Reliability of Financial Reporting หรือ F) เพื่อให้ผู้ใช้รายงานทางการเงินขององค์การที่เป็นบุคคลทั้งภายในและภายนอกได้ข้อมูลที่ถูกต้องไปใช้ในการตัดสินใจ

3. การปฏิบัติตามกฎหมาย ข้อกำหนด กฎระเบียบ และข้อบังคับ (Compliance with Laws and Regulations หรือ C) เพื่อป้องกันมิให้องค์การเกิดความเสียหายจากการละเว้นไม่ปฏิบัติหรือปฏิบัติผิดกฎหมาย ข้อกำหนด กฎ ระเบียบ และข้อบังคับขององค์การเอง

โครงสร้างการควบคุมภายในตามแนวคิดของ COSO ดังกล่าวประกอบด้วย

1. สภาพแวดล้อมของการควบคุม (Control Environment)

2. การประเมินความเสี่ยง (Risk Assessment)

3. กิจกรรมการควบคุม (Control Activities)

4. สารสนเทศและการสื่อสาร (Information and Communication)

5. การติดตามและประเมินผล (Monitoring)

ทำไมถึงเกิด COSO: ERM

แนวความคิดโครงสร้างการควบคุมภายในของ COSO ได้มีการยอมรับและนำไปใช้อย่างแพร่หลายในระดับสากล ตั้งแต่ปี พ.ศ. 2535 สำหรับในประเทศไทยเองก็มีการนำมาเผยแพร่และแนะนำให้ใช้เป็นแนวทางในการสร้างระบบการควบคุมภายในของบริษัทจดทะเบียนในตลาดหลักทรัพย์แห่งประเทศไทย เมื่อปี พ.ศ. 2540 และสำนักงานการตรวจเงินแผ่นดินโดยคณะกรรมการตรวจเงินแผ่นดินได้นำมาเป็นแนวทางพัฒนาและออกเป็นระเบียบคณะกรรมการตรวจเงินแผ่นดินว่าด้วยการกำหนดมาตรฐานการควบคุมภายใน พ.ศ. 2544 เพื่อเป็นแนวทางให้หน่วยรับตรวจใช้ในการจัดระบบการควบคุมภายในอย่างมีประสิทธิภาพและประสิทธิผล อันจะส่งผลให้เกิดประโยชน์สูงสุดในการดำเนินงาน และแก่การใช้จ่ายเงินและทรัพย์สินของประเทศชาติโดยรวม

องค์ประกอบของการควบคุมภายในตามแนวคิดของ COSO ดังกล่าวนี้เมื่อนำมาใช้แล้วก็มีการปรับปรุงจนกระทั่งช่วง 2-3 ปีที่ผ่านมาได้เกิดวิกฤตการณ์ที่บริษัทเอนรอน (Enron) ในประเทศสหรัฐอเมริกาล้มละลายเนื่องจากพฤติกรรมการฉ้อฉลของผู้บริหารปลายปี 2544 อันนำไปสู่การออกกฎหมาย Sarbanes Oxley Act 2002 ตามมาในปี พ.ศ. 2545 กฎหมายได้ให้ความสำคัญกับการควบคุมภายใน สาธารณชนและหน่วยงานกำกับดูแลต่างๆ จึงตื่นตัวหันมาพัฒนาระบบการดูแลกิจการให้มีความโปร่งใสมากขึ้นและเน้นถึงความสำคัญของการควบคุมภายในกันอีกครั้งหนึ่ง COSO จึงได้พัฒนาปรับปรุงและขยายแนวความคิดของการควบคุมภายในเดิมนำองค์ประกอบการควบคุมภายใน 5 ประการเดิมมาขยายขอบเขตให้กว้างขวางมากขึ้นและปรับใหม่ให้เหมาะสมและได้เน้นแนวคิดเรื่องกรอบการจัดการความเสี่ยงขององค์กร (Enterprise Risk Management-Integrated Framework: ERM) หลังจากนั้นได้เผยแพร่สู่สาธารณชนเมื่อเดือนกันยายน พ.ศ. 2547

COSO มิได้มีเจตนาที่จะให้นำกรอบการจัดการความเสี่ยง (COSO: ERM) มาทดแทนกรอบหรือโครงสร้างการควบคุมภายในเดิม เพียงแต่ได้ขยายกรอบการควบคุมภายในให้มีความเข้มข้นและกว้างขวางมากขึ้น ให้ความเข้าใจและนำไปถือปฏิบัติได้ง่ายขึ้น ให้ได้รับความสนใจจากสาธารณชนมากขึ้นเมื่อกล่าวเน้นเรื่องการจัดการความเสี่ยงในภาพรวมองค์การซึ่งต้องเชื่อมความเสี่ยงที่มีผลกระทบซึ่งกันและกันในองค์กร ทำให้สามารถมองเห็นโอกาสในอนาคตและสามารถเพิ่มผลผลิตของเงินทุนที่ลงไปอันเป็นเรื่องสำคัญยิ่งต่อการดำรงอยู่และความก้าวหน้าขององค์กร

COSO: ERM คืออะไร

COSO: ERM คือ กระบวนการซึ่งเป็นผลจากการที่คณะกรรมการ ผู้บริหารและบุคลากรขององค์การร่วมกันกำหนดขึ้นเพื่อนำไปประยุกต์ใช้ในการกำหนดกลยุทธ์และวางแผนขององค์กรในทุกระดับ โดยการออกแบบให้สามารถระบุเหตุการณ์ที่มีความเป็นไปได้อันจะมีผลกระทบต่อองค์การ และการจัดการความเสี่ยงให้อยู่ในระดับที่ยอมรับได้ เพื่อให้เกิดความมั่นใจอย่างสมเหตุสมผลว่าจะสามารถบรรลุวัตถุประสงค์ขององค์การโดยรวมได้

หลักการจัดการความเสี่ยงมีพื้นฐานจากแนวความคิดที่ว่า องค์การจะดำรงอยู่ได้เมื่อสร้างมูลค่าหรือคุณค่าเพิ่มให้ผู้มีส่วนได้เสียขององค์การ ความเสี่ยงและโอกาสมีผลกระทบต่อการเพิ่มหรือลดมูลค่าดังนั้น การจัดการความเสี่ยงจะเป็นเครื่องมือที่ช่วยให้ผู้บริหารจัดการกับความเสี่ยงและโอกาสที่เกี่ยวข้องได้อย่างมีประสิทธิภาพและมีประสิทธิผลโดยสอดคล้องกับเป้าหมายขององค์การโดยรวม

วัตถุประสงค์ขององค์การใน ERM

วัตถุประสงค์ขององค์กรตามแนวคิดของ COSO: ERM มี 4 อย่างคือ

1. วัตถุประสงค์เชิงกลยุทธ์ (Strategic: S)

   เป็นวัตถุประสงค์ระดับสูงที่เน้นเป้าหมายรวมและสัมพันธ์กับการสนับสนุนพันธกิจ

2. วัตถุประสงค์การดำเนินงาน (Operations: O)

   เป็นวัตถุประสงค์ของการใช้ทรัพยากรอย่างมีประสิทธิภาพ มีประสิทธิผลและคุ้มค่า

3. วัตถุประสงค์การรายงาน (Reporting: R)

   เป็นวัตถุประสงค์เพื่อความเชื่อถือได้ของการรายงานโดยเน้นทุกรายงานมิใช่เฉพาะรายงานการเงิน

4. วัตถุประสงค์การปฏิบัติตามกฎหมาย ระเบียบข้อบังคับ (Compliance: C)

   เป็นวัตถุประสงค์ที่มุ่งให้มีการปฏิบัติตามกฎหมายและข้อบังคับที่เกี่ยวข้องกับองค์การ

ระดับของหน่วยงานในองค์การ

หน่วยงานขององค์การแบ่งออกเป็น 4 ระดับคือ

1. ระดับทั่วทั้งองค์การ (Entity-level: EL)
2. ระดับส่วนงาน (Division: D)
3. ระดับหน่วยงาน (Business Unit: BU)
4. ระดับหน่วยงานย่อย (Subsidiary: S)

COSO: ERM จะใช้ในทุกระดับของหน่วยงานในองค์การโดยเน้นภาพรวมไม่ใช่เพียงหน่วยงานหนึ่งหน่วยงานใดหรือกิจกรรมใดกิจกรรมหนึ่ง

องค์ประกอบของการจัดการความเสี่ยงของ COSO (COSO: ERM)

COSO ได้นำองค์ประกอบการควบคุมภายใน 5 ประการมาขยายเป็นองค์ประกอบของการจัดการความเสี่ยง 8 ประการที่สัมพันธ์กัน คือ

1. สภาพแวดล้อมภายใน
   (Internal Environment: IE)
2. การกำหนดวัตถุประสงค์
   (Objective Setting: OS)
3. การระบุเหตุการณ์ (Event Identification: EI)
4. การประเมินความเสี่ยง (Risk Assessment: RA)
5. การตอบสนองความเสี่ยง
   (Risk Responses:RR)
6. กิจกรรมควบคุม (Control Activities: CA)
7. สารสนเทศและการสื่อสาร
   (Information and Communication: IC)
8. การติดตามผล (Monitoring: M)

สภาพแวดล้อมภายใน (IE)

COSO ได้ให้ความสำคัญเรื่องสภาพแวดล้อมหรือบรรยากาศภายในขององค์การว่าเป็นรากฐานที่จะเสริมสร้างให้เกิดกาควบคุมภายใน ปัจจัยในการวิเคราะห์สภาพแวดล้อมภายใน คือ ความซื่อสัตย์และจริยธรรมของบุคลากรโดยเฉพาะอย่างยิ่งคือตัวผู้บริหาร ความรู้ความสามารถของบุคลากร ปรัชญาและรูปแบบการทำ

งานของผู้บริหาร การมอบหมายอำนาจ หน้าที่และความรับผิดชอบ โครงสร้างการจัดองค์การและนโยบายการจัดการด้วนบุคลากร ทั้งนี้ COSO ยังคงถือว่าจิตสำนึกและคุณภาพของคนในองค์การเป็นปัจจัยที่สำคัญที่สุด เช่นเดียวกับที่กำหนดไว้ในกรอบการควบคุมภายใน

การกำหนดวัตถุประสงค์ (OS)

จากนั้น COSO ได้อธิบายต่อมาว่า องค์การจะบริหารจัดการความเสี่ยงได้ก็ต่อเมื่อรู้วัตถุประสงค์ หรือสิ่งที่องค์การต้องการก่อน ดังนั้นจึงจำเป็นต้องมีการกำหนดวัตถุประสงค์ขึ้นในทุกระดับของหน่วยงานขององค์การจึงจะสามารถที่จะนำไปสู่การระบุเหตุการณ์ที่อาจเป็นไปได้อันทำให้เกิดความเสี่ยง การกำหนดวัตถุประสงค์จะต้องสอดคล้องกับพันธกิจ

การระบุเหตุการณ์ (EI)

สำหรับการระบุเหตุการณ์ หมายความถึง ต้องสามารถระบุได้ถึงเหตุการณ์ทั้งภายในและภายนอกองค์การ โดยพิจารณาทั้งตัวเหตุการณ์และโอกาสที่จะเกิดซึ่งมีผลกระทบให้เกิดความเสียหายหรือการไม่บรรลุวัตถุประสงค์ขององค์กร

การประเมินความเสี่ยง (RA)

เมื่อสามารถระบุเหตุการณ์ได้แล้วยังไม่เพียงพอจะต้องพิจารณาความน่าจะเกิดขึ้น และผลกระทบจากการเกิดเหตุการณ์ดังกล่าวเพื่อใช้เป็นพื้นฐานในการจัดการความเสี่ยงต่อไป

การตอบสนองความเสี่ยง (RR)

เป็นการกล่าวถึงช่องทางการตัดสินใจของผู้บริหารที่จะใช้ตอบสนองความเสี่ยงจากผลการประเมินความเสี่ยง ผู้บริหารอาจเลือกกระทำกิจกรรมที่มีความสอดคล้องกับความเสี่ยงได้ 4 แนวทางคือ

1. การหลีกเลี่ยง (Avoidance) คือ การกระทำเพื่อลดความน่าจะเป็น หรือเลิกทำกิจกรรมที่ก่อให้เกิดความเสี่ยง

2. การลด (Reduction) คือ การกระทำเพื่อลดความน่าจะเป็นหรือลดผลกระทบจากความเสี่ยง ส่วนใหญ่มักเกี่ยวกับความเสี่ยงที่เกิดจากปัจจัยภายในองค์กรหรือปัจจัยที่องค์กรสามารถควบคุมได้

3. การร่วมรับ หรือ โอนความเสี่ยง (Sharing or Transferring) เป็นการลดความน่าจะเป็นหรือลดผลกระทบจากความเสี่ยงโดยการแบ่งปันหรือโอนความเสี่ยงให้กับบุคคลอื่น มักจะใช้กรณีที่ไม่สามารถเกิดความเสี่ยงมาจากปัจจัยที่เหนือความควบคุมขององค์การ

4. การยอมรับ (Acceptance) คือ การไม่ทำกิจกรรมใดๆ เพื่อลดความน่าจะเป็น หรือลดผลกระทบจากความเสี่ยง เนื่องจากผู้บริหารเห็นว่าความเสี่ยงนั้นอยู่ในระดับที่ยอมรับได้

ทั้งนี้ผู้บริหารควรเลือกแนวทางการตอบสนองความเสี่ยงที่ทำให้ความน่าจะเป็นและผลกระทบจากความเสี่ยงอยู่ในระดับที่ยอมรับได้

กิจกรรมควบคุม (CA)

คือ นโยบายและวิธีปฏิบัติที่กำหนดเพื่อตอบสนองความเสี่ยงที่อาจเกิดขึ้น เป็นกิจกรรมที่ช่วยให้เกิดความมั่นใจว่าความเสี่ยงได้รับการตอบสนองอย่างมีประสิทธิผล และมีการปฏิบัติตามวิธีการตอบสนองความเสี่ยงที่กำหนดและบรรลุความสำเร็จตามวัตถุประสงค์ภายในเวลาที่กำหนด

สารสนเทศและการสื่อสาร (IC)

ผู้บริหารควรกำหนดให้มีการบันทึกข้อมูลสารสนเทศที่เกี่ยวข้องกับองค์การไม่ว่าจะมาจากแหล่งภายในหรือภายนอกองค์การ และกำหนดให้มีการสื่อสารในรูปแบบที่เหมาะสมและทันกาล เพื่อให้บุคลากรตอบสนองต่อเหตุการณ์ต่างๆ ได้อย่างรวดเร็วและมีประสิทธิภาพ

การติดตามผล (M)

การบริหารจัดการความเสี่ยงขององค์การต้องมีการติดตามเพื่อประเมินกรอบการจัดการความเสี่ยงให้

เหมาะสม มีประสิทธิภาพอย่างต่อเนื่องและสม่ำเสมอ การติดตามผลถือเป็นมาตรการในการควบคุมคุณภาพของการจัดการความเสี่ยง

งานตรวจสอบภายในเกี่ยวข้องอย่างไรกับ COSO: ERM

ปัจจุบันงานตรวจสอบภายในมิใช่เป็นเพียงงานที่เข้าไปตรวจสอบและประเมินหน่วยงานหรือผู้ปฏิบัติงานในองค์กรว่ามีการดำเนินงานต่างๆเป็นไปโดยถูกต้องตามกฎระเบียบข้อบังคับ มีประสิทธิภาพและมีประสิทธิผลเป็นไปตามนโยบายของฝ่ายบริหารโดยให้ความเชื่อมั่น อย่างเที่ยงธรรม และเป็นอิสระเท่านั้น แต่ผู้ตรวจสอบภายในยังต้องสามารถทำหน้าที่ในการให้คำปรึกษาได้ด้วย การปฏิบัติงานทั้งหมดของงานตรวจสอบภายในจึงต้องมีวัตถุประสงค์ท้ายสุดเพื่อการเพิ่มคุณค่าและพัฒนาการดำเนินงานขององค์กรอย่างต่อเนื่อง ผู้ตรวจสอบภายในจะช่วยให้งานตรวจสอบภายในบรรลุเป้าหมายดังกล่าวได้โดยการประเมินและปรับปรุงประสิทธิภาพ และประสิทธิผลของกระบวนการจัดการความเสี่ยงและการพัฒนาและปรับปรุงระบบการควบคุมภายในที่เหมาะสมอย่างเป็นระบบและมีระเบียบแบบแผน

จากที่กล่าวมาข้างต้นจึงพอสรุปได้ว่า ลักษณะของงานตรวจสอบภายในต้องเกี่ยวข้องกับการประเมินอย่างเป็นระบบและสนับสนุนให้มีการปรับปรุงความมีประสิทธิผลของการจัดการความเสี่ยง การมีและพัฒนาระบบการควบคุมภายในให้เหมาะสมและสม่ำเสมอเพื่อการสร้างมูลค่าเพิ่มให้แก่องค์การ ผู้ตรวจสอบภายในจะสามารถประเมินให้ข้อเสนอแนะหรือให้คำปรึกษาเพื่อการพัฒนาการจัดการความเสี่ยงได้อย่างที่มุ่งหวังก็ต่อเมื่อผู้ตรวจสอบภายในต้องเข้าใจอย่างถ่องแท้ในเรื่องการจัดความเสี่ยงตามแนวคิดของ COSO (COSO: ERM) ที่กล่าวข้างต้น ประกอบกับความสามารถเฉพาะบุคคลของผู้ตรวจสอบภายในเอง

สรุป

COSO: ERM เป็นกรอบแนวทางจัดการความเสี่ยง ซึ่งเป็นกระบวนการที่เกี่ยวข้องกับทุกคนใช้ปฏิบัติในระดับรวมขององค์กร มิใช่จัดทำขึ้นมาเพื่อทดแทนแนวคิดการควบคุมภายในของ COSO แต่เป็นพัฒนาการจากกรอบแนวคิดเรื่องการควบคุมภายในดังกล่าว โดยเพิ่มวัตถุประสงค์เชิงกลยุทธ์ที่สนับสนุนพันธกิจขององค์กร และมีวัตถุประสงค์ด้านการรายงานของทุกๆ รายงานมิใช่เฉพาะรายงานการเงินเท่านั้น ให้มองเหตุการณ์ที่ส่งผลกระทบต่อวัตถุประสงค์ขององค์การทั้งด้านที่เป็นความเสี่ยงและเป็นโอกาสควบคู่กันไป เมื่อมีเหตุการณ์ดังกล่าวก็มีแนวทางการจัดการความเสี่ยงให้อยู่ในระดับที่ยอมรับได้ อันเป็นส่วนขยายเพิ่มจากกรอบแนวความคิดการควบคุมภายในเดิม

ผู้ตรวจสอบภายในมีส่วนสำคัญยิ่งในการช่วยส่งเสริมและผลักดันให้มีการนำ COSO: ERM มาใช้ในองค์กร เพราะเป็นผู้ตรวจประเมินประสิทธิผลของการจัดการความเสี่ยงขององค์กรภายใต้ความเชื่อมั่นอย่างสมเหตุสมผลว่าองค์กรจะสามารถบรรลุวัตถุประสงค์ได้เมื่อนำ COSO: ERM มาใช้ปฏิบัติอย่างมีประสิทธิภาพ แต่มิได้หมายความว่าองค์การที่นำ COSO: ERM ไปใช้ทุกองค์การจะได้ผลเช่นเดียวกันหมด ทั้งนี้เนื่องจากยังมีข้อจำกัดที่การเลือกแนวทางการจัดการความเสี่ยงนั้นยังต้องใช้ “คน” เป็นผู้ตัดสินใจตลอดจนการตัดสินว่าความเสี่ยงที่มีอยู่ในระดับที่ยอมรับได้โดยคำนึงถึงต้นทุนและผลประโยชน์ว่าคุ้มค่าหรือไม่ ยังเป็นการตัดสินใจของคน (ผู้บริหาร) เช่นกัน

บรรณานุกรม

จันทนา สาขากร นิพันธ์ เห็นโชคชัยชนะ ศิลปพร ศรีจั่นเพชร การควบคุมภายในและการตรวจสอบภายใน กรุงเทพฯ: ห้างหุ้นส่วนจำกัด ทีพีเอ็นเพรส, 2550

นิพันธ์ เห็นโชคชัยชนะ ศิลปพร ศรีจั่นเพชร การสอบบัญชี กรุงเทพฯ: ห้างหุ้นส่วนจำกัด ทีพีเอ็นเพรส, 2550