สรุปประเด็นสำคัญในการเข้ารับการฝึกอบรม
หลักสูตร "นักบริหารความเสี่ยงมืออาชีพ RISK MANAGEMENT SPECIALIST (RMS)"
ณ โรงแรมเมอร์เคียว สยาม ปทุมวัน
ระหว่างวันที่ ๒๑-๒๓ พฤษภาคม ๒๕๕๗

หลักการและเหตุผล

สถาบันวิทยาการจัดการ ภายในกำกับของบริษัท ทริส คอร์ปอเรชั่น จำกัด ให้บริการด้านวิชาการทั้งในรูปแบบของการเป็นที่ปรึกษาให้องค์ความรู้ ร่วมดำเนินงานการหรือส่งมอบผลงาน และการจัดฝึกอบรมสัมมนาในองค์ความรู้ต่าง ๆ ให้กับหน่วยงานทั้งภาคเอกชน ราชการรัฐวิสาหกิจ และองค์กรอิสระ ทั้งนี้ เพื่อเพิ่มศักยภาพด้านบริหารจัดการองค์กร ผู้บริหารอย่างเป็นระบบ โดยให้เกิดความสมดุลทั้งในด้านการเติบโตความยั่งยืน และความสามารถในการแข่งขัน ซึ่งความไม่แน่นอนและความเปลี่ยนแปลงในโลกยุคปัจจุบันเป็นไปอย่างรวดเร็วและรุนแรง องค์กรจำนวนไม่น้อยที่ต้องพบกับสถานการณ์หรือเหตุการณ์ที่ทำให้เกิดความไม่มั่นคงต่อองค์กร ทั้งการไม่บรรลุเป้าหมายที่กำหนดไว้ ทั้งด้านการเงินและไม่ใช่การเงินต่าง ๆ เช่น การขาดสภาพคล่องทางการเงิน การสูญเสียชื่อเสียงและภาพลักษณ์ความน่าเชื่อถือขององค์กร ซึ่งจะกลายเป็นต้นทุนขององค์กรในที่สุด อย่างไรก็ตามเมื่อพิจารณาแล้วจะพบว่า มีองค์กรจำนวนหนึ่งที่มีความสามารถในการรับมือกับสถานการณ์ในลักษณะเหล่านั้นได้เป็นอย่างดี รวมทั้งอาจสามารถปรับเปลี่ยนสภานะการณ์วิกฤติเหล่านั้น กลับกลายเป็นโอกาสทางธุรกิจได้ท่ามกลางคู่แข่งขันที่อ่อนแอกว่า ซึ่งแน่นอนว่าองค์กรเหล่านั้นมีความเข้าใจในการบริหารความเสี่ยงและมีการวางระบบบริหารความเสี่ยงในองค์กร นอกจากนั้นแนวคิดการกำกับดูแลที่ดี หรือ Good Governance ที่แพร่หลายในปัจจุบันก็เป็นส่วนสำคัญในการสนับสนุนให้เกิดความตระหนักในความไม่แน่นอนดังกล่าวได้เป็นอย่างดีอีกส่วนหนึ่งด้วย

วัตถุประสงค์

๑. เพื่อเสริมสร้างความรู้ ความเข้าใจหลักการ กระบวนการแนวทางการพัฒนา และแนวปฏิบัติที่ดีเกี่ยวกับเรื่องการบริหารความเสี่ยงองค์กร รวมทั้งสามารถยกระดับการพัฒนาการบริหารความเสี่ยงต่อไปอย่างมีประสิทธิภาพ

๒. เพื่อเสริมสร้างองค์ความรู้และความเข้าใจในการบูรณาการแนวคิด GRC (Governance, Risk and Compliance)

๓. เพื่อนำความรู้ที่ได้ไปประยุกต์ใช้เป็นแนวทางการพัฒนาระบบการบริหารความเสี่ยง การกำกับดูแลองค์กร และการปฏิบัติตามกฎเกณฑ์ขององค์กรต่อไป

หลักสูตรการฝึกอบรม

หลักสูตร "นักบริหารความเสี่ยงมืออาชีพ RISK MANAGEMENT SPECIALIST (RMS)"

- การบริหารความเสี่ยง
  - กระบวนการและกลยุทธ์การบริหารความเสี่ยง
  - การบริหารความต่อเนื่องทางธุรกิจ

/การบริหาร...

- การบริหารความเสี่ยงองค์กร
  - กรอบแนวคิดในการบริหารความเสี่ยงตาม COSO-ERM
  - ความเชื่อมโยงของการบริหารความเสี่ยงกับการควบคุมภายใน
  - การพัฒนาระบบบริหารความเสี่ยงองค์กร
- มาตรฐานการบริหารความเสี่ยงตาม ISO ๓๑๐๐๐
- แนวทางการบริหารความเสี่ยงด้านสารสนเทศ COBIT
- การกำกับดูแลกิจการ
  - กรอบโครงสร้างของการกำกับดูแลกิจการที่มีประสิทธิผล
  - หน้าที่และความรับผิดชอบการกำกับดูแลกิจการของคณะกรรมการ
  - ความสัมพันธ์ระหว่างการกำกับดูแลกิจการ การบริหารความเสี่ยงและการปฏิบัติตามกฎเกณฑ์ (GRC)
  - การประยุกต์แนวคิด GRC สู่ภาคปฏิบัติ
- มาตรฐานแนวทางความรับผิดชอบต่อสังคม ISO ๒๖๐๐๐

คุณสมบัติของผู้เข้ารับการฝึกอบรม

สำหรับผู้จัดการทุกระดับ ผู้บริหารหน่วยงาน เจ้าหน้าที่ฝ่ายบริหารความเสี่ยง และควบคุมภายใน

วิธีการฝึกอบรม ประกอบด้วย

กิจกรรม

การบรรยาย การวิเคราะห์กรณีศึกษา การแลกเปลี่ยนความคิดเห็น และกิจกรรมการฝึกปฏิบัติ

ผลสัมฤทธิ์ที่คาดว่าจะได้รับ

ผู้เข้าอบรมสามารถวิเคราะห์ความเสี่ยงที่เกิดขึ้นในองค์กรได้และได้เรียนรู้แนวทาง ขั้นตอน วิธีการในการบริหารความเสี่ยงอย่างเป็นระบบตามแนวคิดสมัยใหม่

ระยะเวลาในการฝึกอบรม

หลักสูตร นักบริหารความเสี่ยงมืออาชีพ **(จำนวน ๓ วัน)**

ระหว่างวันที่ ๒๑-๒๓ พฤษภาคม ๒๕๕๗

สถานที่ฝึกอบรม

โรงแรมเมอร์เคียว สยาม ปทุมวัน

/คณะวิทยากร...

คณะวิทยากร

๑. รศ.ดร.นฤมล สอาดโฉม อาจารย์ประจำ NIDA ที่ปรึกษาสถาบันวิทยาการจัดการ

๒. คุณสุรเดช จองวรรณศิริ รองผู้อำนวยการ บริษัท ทริส คอร์ปอเรชั่น จำกัด

๓. ดร.พรเทพ อนุสสรนิติสาร อาจารย์ประจำมหาวิทยาลัยเกษตรศาสตร์ ที่ปรึกษาสถาบันวิทยาการจัดการ

๔. รศ.ดร.พรอนงค์ บุษราตระกูล อาจารย์ประจำมหาวิทยาลัยจุฬาลงกรณ์ ที่ปรึกษาสถาบันวิทยาการจัดการ

๕. คุณไวฑูรย์ โภคาชัยพัฒน์ ผู้ช่วยกรรมการผู้จัดการ บริษัท ทริส คอร์ปอเรชั่น จำกัด

สรุปเนื้อหาการฝึกอบรมดังนี้

Enterprise Risk Management การบริหารจัดการความเสี่ยง

ความเสี่ยง (Risk) คือ การวัดความสามารถ ที่จะดำเนินการให้วัตถุประสงค์ของงานประสบความสำเร็จ ภายใต้การตัดสินใจ งบประมาณ กำหนดเวลา และข้อจำกัดด้านเทคนิคที่เผชิญอยู่ อย่างเช่น การจัดทำโครงการเป็นชุดของกิจกรรม ที่จะดำเนินการเรื่องใดเรื่องหนึ่งในอนาคต โดยใช้ทรัพยากรที่มีอยู่อย่างจำกัด มาดำเนินการให้ประสบความสำเร็จ ภายใต้กรอบเวลาอันจำกัด ซึ่งเป็นกำหนดการปฏิบัติการในอนาคต ความเสี่ยงจึงอาจเกิดขึ้นได้ตลอดเวลา อันเนื่องมาจากความไม่แน่นอน และความจำกัดของทรัพยากรโครงการ ผู้บริหารโครงการจึงต้องจัดการความเสี่ยงของโครงการ เพื่อให้ปัญหาของโครงการลดน้อยลง และสามารถดำเนินการให้ประสบความสำเร็จ ตามเป้าหมายที่ตั้งไว้อย่างมีประสิทธิผลและประสิทธิภาพ

การบริหารความเสี่ยงระดับองค์กร (Enterprise Risk Management) หมายถึง กระบวนการที่บุคลากรทั่วทั้งองค์กรได้มีส่วนร่วมในการคิด วิเคราะห์ และคาดการณ์ถึงเหตุการณ์ หรือความเสี่ยงที่อาจจะเกิดขึ้น รวมทั้งการระบุแนวทางในการจัดการกับความเสี่ยงดังกล่าว ให้อยู่ในระดับที่เหมาะสมหรือยอมรับได้ เพื่อช่วยให้องค์กรบรรลุในวัตถุประสงค์ที่ต้องการ ตามกรอบวิสัยทัศน์ และพันธกิจขององค์กร

กรอบการบริหารความเสี่ยงองค์กรนั้น สามารถสะท้อนให้เห็นถึงนโยบายการบริหารจัดการและการกำกับดูแลกิจการของแต่ละองค์กร โดยหากองค์กรมีการบริหารความเสี่ยงอย่างมีประสิทธิภาพจะส่งผลให้สามารถบรรลุวัตถุประสงค์องค์กร ทั้งในเชิงประสิทธิภาพและประสิทธิผลของงาน

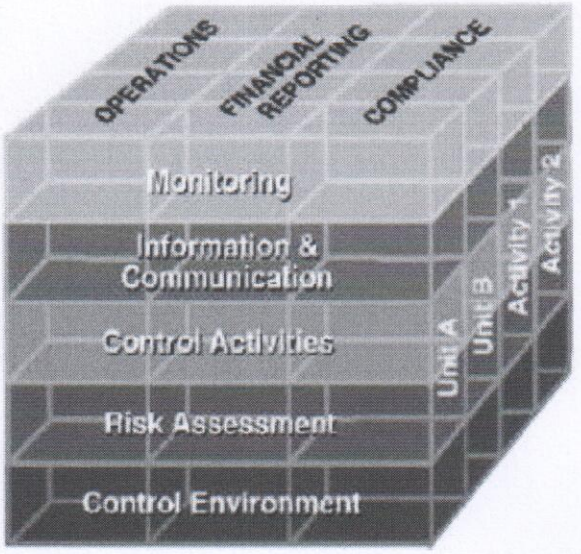
ทั้งนี้ การบริหารความเสี่ยงระดับองค์กร (Enterprise Risk Management) ใน ค.ศ. ๒๐๐๒ ได้กำหนดวัตถุประสงค์ไว้เพียง ๓ ชั้น และ ๕ องค์ประกอบเท่านั้น เป็นกระบวนการบริหารความเสี่ยงจากระดับบนลงระดับล่าง (ตามรูปภาพด้านล่าง) ซึ่งสมัยนั้นได้นำกระบวนการดังกล่าวไปใช้และปรากฏว่าบริษัทใหญ่ระดับโลกเกิดเหตุการณ์ล้มละลาย อย่างเช่น บริษัท ENRON และ บริษัท WORLDCOM จากการสืบสวนปรากฏว่า การทุจริตภายในองค์กรผู้บริหารและเจ้าของบริษัทเป็นบุคคลคนเดียวกันเป็นผู้อำนาจเบ็ดเสร็จ ไม่มีคณะกรรมการตรวจสอบอิสระ และผู้ที่เกี่ยวข้องซึ่งได้แก่บริษัทผู้ตรวจสอบบัญชีมีส่วนได้ส่วนเสียกับบริษัทกลัวเสียผลประโยชน์จึงได้ทำบัญชีเท็จให้บริษัทดังกล่าว ทำให้งบการเงินไม่สะท้อนความเป็นจริง สะท้อนให้เห็นว่าการควบคุมภายในหรือกระบวนการบริหารความเสี่ยงแบบเดิมยังไม่ครอบคลุมการดำเนินงาน (รูปภาพที่ ๑) จึงมีการปรับปรุงกระบวนการบริหารความเสี่ยง โดยกำหนดวัตถุประสงค์เพิ่มเป็น ๔ ข้อ และกำหนดองค์ประกอบเพิ่มเป็น ๘ ข้อ และการบริหารจากระดับล่างขึ้นมาระดับบน (รูปภาพที่ ๒) เพื่อให้การควบคุมภายในครอบคลุมการดำเนินงานยิ่งขึ้น และมีการปรับแนวคิดการบริหารความเสี่ยงด้วย (รูปภาพที่ ๓)

/๑. แผนภาพ...

๑. แผนภาพ ERM (Enterprise Risk Management) ยุค ค.ศ. ๒๐๐๒

๓ วัตถุประสงค์

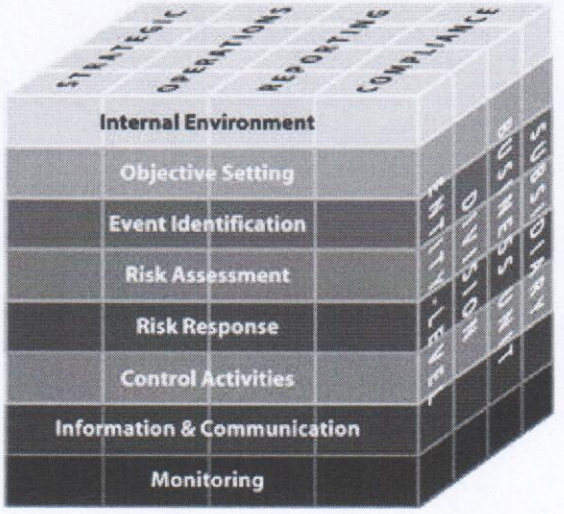
๕ องค์ประกอบ



๒. แผนภาพ ERM (Enterprise Risk Management) ยุคปัจจุบัน

๔ วัตถุประสงค์

๘ องค์ประกอบ



เปรียบเทียบแนวคิดการบริหารความเสี่ยงก่อนปรับและหลังปรับ

The Past	The Future
Risk as individual hazards	Risk in the context of business strategy
Risk identification and assessment	Risk “portfolio “ development
Focus on all risks	Focus on critical risks
Risk mitigation	Risk optimization
Risk limits	Risk strategy
Risk with no owners	Defined risk accountability
Haphazard risk quantification	Consistent with business objectives
Risk is not my responsibility	Risk is everyone is responsibility

/การบริหาร...

การบริหารความเสี่ยงตามมาตรฐาน COSO ประกอบด้วยองค์ประกอบ ๘ ประการ ซึ่งครอบคลุมแนวทางการกำหนดนโยบายการบริหารงาน การดำเนินงาน และการบริหารความเสี่ยง ดังนี้

(๑) สภาพแวดล้อมภายในองค์กร (Internal Environment)

สภาพแวดล้อมขององค์กรเป็นองค์ประกอบที่สำคัญ ในการกำหนดกรอบบริหารความเสี่ยง ประกอบด้วยปัจจัยหลายประการ เช่น วัฒนธรรมองค์กร นโยบายของผู้บริหาร แนวทางการปฏิบัติงานบุคลากร กระบวนการทำงาน ระบบสารสนเทศ ระเบียบ เป็นต้น สภาพแวดล้อมภายในองค์กรประกอบเป็นพื้นฐานสำคัญในการกำหนดทิศทางของกรอบการบริหารความเสี่ยงขององค์กร

(๒) การกำหนดวัตถุประสงค์ (Objective Setting)

องค์กรต้องพิจารณากำหนดวัตถุประสงค์ในการบริหารความเสี่ยงให้มีความสอดคล้องกับกลยุทธ์และความเสี่ยงที่องค์กรยอมรับได้ เพื่อวางเป้าหมายในการบริหารความเสี่ยงขององค์กรได้อย่างชัดเจน และเหมาะสม

(๓) การบ่งชี้เหตุการณ์ (Event Identification)

เป็นการรวบรวมเหตุการณ์ที่อาจเกิดขึ้นกับหน่วยงาน ทั้งในส่วนของปัจจัยเสี่ยงที่เกิดจากภายในและภายนอกองค์กร เช่น นโยบายบริหารงาน บุคลากร การปฏิบัติงาน การเงิน ระบบสารสนเทศ ระเบียบ กฎหมาย ระบบบัญชี ภาษีอากร ทั้งนี้เพื่อทำความเข้าใจต่อเหตุการณ์และสถานการณ์นั้น เพื่อให้ผู้บริหารสามารถพิจารณากำหนดแนวทางและนโยบายในการจัดการกับความเสี่ยงที่อาจจะเกิดขึ้นได้เป็นอย่างดี

(๔) การประเมินความเสี่ยง (Risk Assessment)

การประเมินความเสี่ยงเป็นการจำแนกและพิจารณาจัดลำดับความสำคัญของความเสี่ยงที่มีอยู่ โดยการประเมินจากโอกาสที่จะเกิด (Likelihood) และผลกระทบ (Impact) โดยสามารถประเมินความเสี่ยงได้ทั้งจากปัจจัยความเสี่ยงภายนอกและปัจจัยความเสี่ยงภายในองค์กร

(๕) การตอบสนองความเสี่ยง (Risk Response)

เป็นการดำเนินการหลังจากที่องค์กรสามารถบ่งชี้ความเสี่ยงขององค์กรและประเมินความสำคัญของความเสี่ยงแล้ว โดยจะต้องนำความเสี่ยงไปดำเนินการตอบสนองด้วยวิธีการที่เหมาะสม เพื่อลดความสูญเสียหรือโอกาสที่จะเกิดผลกระทบให้อยู่ในระดับที่องค์กรยอมรับได้

(๖) กิจกรรมการควบคุม (Control Activities)

การกำหนดกิจกรรมและการปฏิบัติต่างๆ ที่กระทำเพื่อลดความเสี่ยงและทำให้การดำเนินงานบรรลุตามวัตถุประสงค์และเป้าหมายขององค์กร เช่น การกำหนดกระบวนการปฏิบัติงานที่เกี่ยวข้องกับการจัดการความเสี่ยงให้กับบุคลากรภายในองค์กรเพื่อเป็นการสร้างความมั่นใจว่าจะสามารถจัดการกับความเสี่ยงนั้นได้อย่างถูกต้องและเป็นไปตามเป้าหมายที่กำหนด

(๗) สารสนเทศและการสื่อสาร (Information and Communication)

องค์กรจะต้องมีระบบสารสนเทศและการติดต่อสื่อสารที่มีประสิทธิภาพเพราะเป็นพื้นฐานสำคัญที่จะนำไปพิจารณาดำเนินการบริหารความเสี่ยงให้เป็นไปตามกรอบและขั้นตอนการปฏิบัติที่องค์กรกำหนด

(๘) การติดตามประเมินผล (Monitoring)

องค์กรจะต้องมีการติดตามผลเพื่อให้ทราบถึงผลการดำเนินการว่ามีความเหมาะสมและสามารถจัดการความเสี่ยงได้อย่างมีประสิทธิภาพหรือไม่

ประโยชน์ของระบบ ERM

ระบบ ERM (Enterprise Risk Management) เป็นระบบที่ได้ถูกออกแบบตามหลักการ ๘ ขั้นตอน ของการจัดการบริหารความเสี่ยงของ COSO เพื่อให้องค์กรที่นำไปใช้งานได้ประโยชน์ดังนี้

(๑) ระบบนี้สามารถเป็นเครื่องมือ เพื่อช่วยผู้บริหารในการประเมินความเพียงพอเหมาะสมของการควบคุมและทำให้มีการแก้ไขปัญหา ปรับปรุงการทำงานให้ดีขึ้น ซึ่งจะส่งผลให้งานของทั้งส่วนงานย่อย ฝ่ายงานและสายการบังคับบัญชาบรรลุวัตถุประสงค์ได้อย่างมีประสิทธิภาพมากขึ้น

/(๒) ข้อมูล...

(๒) ข้อมูลที่ได้รับจากระบบ เป็นข้อมูลรวมจากระดับปฏิบัติการที่มีอยู่ของหน่วยงานย่อยในองค์กร ซึ่งจะช่วยให้ค้นพบปัญหาที่เกิดขึ้นหรือมีแนวโน้มที่จะเกิดขึ้นก่อนที่จะเกิดความเสียหายทำให้หน่วยงานสามารถวางแผนเพื่อจัดการแก้ไขได้

(๓) การใช้งานระบบนี้เป็นการเปิดโอกาสให้ผู้ปฏิบัติงานในทุกระดับแสดงความเห็น ข้อเสนอแนะ และร่วมกันกำจัดอุปสรรค และข้อขัดข้องต่าง ๆ

(๔) ขั้นตอนการทำงานของระบบเป็นการนำเสนอแนวทางปฏิบัติตามกรอบของนโยบายองค์กรทำให้พนักงานเข้าใจเป้าหมายขององค์กรที่ตนได้มีส่วนร่วมอีกทั้งช่วยสร้างบรรยากาศที่ดีของการทำงาน และการรับผิดชอบร่วมกันต่อผลสำเร็จขององค์กร

(๕) ระบบมีแบบแผนขั้นตอนการดำเนินการที่ชัดเจนในการกำหนดเป้าหมายขององค์กร, ตัวชี้วัดความสำเร็จ, การวิเคราะห์งานเพื่อระบุความเสี่ยง, ประเมินความเสี่ยง, การควบคุมความเสี่ยง และการติดตามความเสี่ยง โดยสามารถนำรายละเอียดดังกล่าวมาสร้างเป็นรายงานต่างๆได้

(๖) จากการให้พนักงานมีส่วนร่วมในการให้ข้อมูลจะทำให้เกิดความเข้าใจและการยอมรับจากผู้ปฏิบัติงานได้ดีมากกว่าการควบคุมสั่งการโดยผู้บริหารแต่ฝ่ายเดียว

โดยองค์กรแรก ๆ ที่มีการบริหารความเสี่ยง ได้แก่ บริษัทประกอบธุรกิจประกันภัย ธนาคาร ตลาดหลักทรัพย์ ธุรกิจการค้า โรงแรม องค์กรรัฐวิสาหกิจ เป็นต้น ซึ่งองค์กรดังกล่าววัตถุประสงค์เพื่อผลตอบแทนด้านรายได้เป็นหลัก ต่อมาหน่วยงานภาครัฐได้มีการนำหลักการบริหารความเสี่ยงมาใช้วัตถุประสงค์เพื่อให้องค์บรรลุเป้าหมายในการดำเนินงานที่กำหนดมากกว่ารายได้

<u>มาตรฐานการบริหารความเสี่ยงตาม ISO ๓๑๐๐๐</u>

สถานการณ์ต่าง ๆ ในระยะที่ผ่านมาได้ชี้ชัดว่ากิจการต่าง ๆ ทั่วโลกกำลังเผชิญกับความเสี่ยงที่เพิ่มขึ้นอย่างไม่เคยเป็นมาก่อน โดยเฉพาะอย่างยิ่งจากเหตุการณ์ที่ทำให้เกิดการหยุดชะงักของการดำเนินงานไม่ต่อเนื่องตามปกติ และความผันผวนไร้เสถียรภาพทางการเงิน ซึ่งล้วนแต่ท้าทายความสามารถในการบริหารจัดการทางกลยุทธ์และด้านปฏิบัติการ

ขณะเดียวกัน แนวคิดที่จะกำจัดความเสี่ยงสำคัญ ๆ ของกิจการดูเหมือนจะเป็นไปไม่ได้ จึงคงเหลือแต่เพียงการพยายามบริหารจัดการในเชิงควบคุมให้มีประสิทธิภาพเป็นหลัก ซึ่งการบริหารจัดการความเสี่ยงได้อย่างมีประสิทธิภาพจะต้องใช้แนวทางที่เป็นระบบ ไม่ใช่การจัดการแบบสะเปะสะปะ โดยมาตรฐาน ISO ๓๑๐๐๐:๒๐๐๙ – Risk Management Principles and Guidelines เป็นหนึ่งในกรอบแนวปฏิบัติที่จะช่วยกิจการต่าง ๆ ได้

มาตรฐาน ISO ๓๑๐๐๐:๒๐๐๙ เป็นมาตรฐานที่ออกมาจากองค์กร ISO โดยมาจากการพัฒนาที่มาจากความร่วมมือของผู้ที่เกี่ยวข้อง ๓๐ ประเทศ เพื่อให้เกิดเป็นมาตรฐานใหม่ระดับสากลที่พยายามลดจุดอ่อนของมาตรฐานเดิม ๆ ที่มีอยู่ และสามารถใช้ได้ในผู้ประกอบการอุตสาหกรรมประเภทต่าง ๆ ได้หลากหลาย และกิจการทั้งที่เป็นหน่วยงานภาครัฐและภาคธุรกิจ รวมทั้งกิจการที่มิได้มุ่งแสวงกำไร

ISO ๓๑๐๐๐:๒๐๐๙ มีความแตกต่างจากมาตรฐานการบริหารความเสี่ยง AS/NZ ๔๓๖๐ และ COSO ERM – Integrated Framework เพราะ

(๑) ISO ๓๑๐๐๐:๒๐๐๙ เจาะจงที่ระบบบริหารความเสี่ยงทั้งระบบ ตั้งแต่ การออกแบบระบบ การนำไปใช้ในกิจการ และการธำรงรักษาระบบ ตลอดจนการปรับปรุงกระบวนการบริหารความเสี่ยง ไม่ได้เป็นเพียงกระบวนการที่บอกกิจกรรมการบริหารความเสี่ยงแบบง่าย ๆ กว้าง ๆ ไม่ลึกซึ้ง

(๒) แม้ว่ามาตรฐานการบริหารความเสี่ยงจะไม่ใช่ข้อบังคับ แต่ที่ผ่านมาธุรกิจประเภทต่าง ๆ ได้ให้ความสนใจในการเพิ่มความเข้มแข็งของการบริหารจัดการความเสี่ยงควรจะพิจารณาว่าจะเพิ่มเติมองค์ประกอบใดในกรอบการบริหารจัดการความเสี่ยงปัจจุบันในกระบวนการดำเนินการที่ใช้อยู่แล้ว

/(๓) สาระ...

(๓) สาระสำคัญของ ISO ๓๑๐๐๐:๒๐๐๙ อาจจะแบ่งองค์ประกอบเป็น ๓ ส่วน

ส่วนที่ ๑ หลักการและแนวพึงปฏิบัติ (Principles and Guidelines)

ส่วนที่ ๒ กรอบแนวทางปฏิบัติ (Framework)

ส่วนที่ ๓ กระบวนการที่เกี่ยวข้อง (Process)

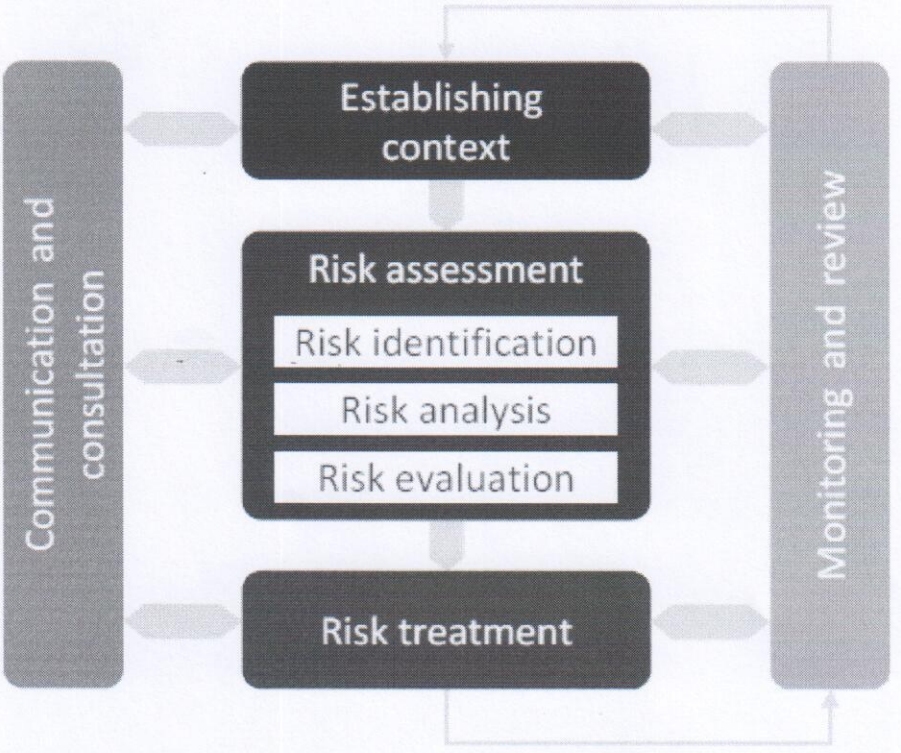
นอกจากนั้น ISO ๓๑๐๐๐:๒๐๐๙ ยังได้บรรจุเนื้อหาในส่วนของการนำเอามาตรฐานไปใช้และการตีความ

(๔) ผู้คิดจะใช้มาตรฐาน ISO ๓๑๐๐๐:๒๐๐๙ มีความคาดหวังว่า ISO คงไม่หยุดอยู่เพียงแค่มาตรฐานนี้เท่านั้น แต่ในอนาคตน่าจะมีแนวพึงปฏิบัติอื่นออกมาใช้เพิ่มเติม ซึ่งจะทำให้เกิดความชัดเจนมากขึ้น

ความสัมพันธ์ระหว่างหลักการบริหารความเสี่ยงกรอบแนวปฏิบัติและกระบวนการการบริหารความเสี่ยง คือ

- แนวทางการสร้างคุณค่าซึ่งเป็นส่วนสำคัญที่บูรณาการของกระบวนการดำเนินงานของกิจการ
- เป็นส่วนหนึ่งของการตัดสินใจทางธุรกิจ
- ขั้นตอนที่จะระบุความไม่แน่นอนที่จะก่อให้เกิดความเสี่ยง
- เป็นวิธีดำเนินการอย่างเป็นระบบ มีโครงสร้างรองรับชัดเจนและต้องดำเนินการให้เหมาะสม
- เป็นการดำเนินการที่ต้องอาศัยสารสนเทศที่ดีที่สุด
- ต้องดัดแปลงให้เหมาะสมกับแต่ละกิจการ
- ต้องนำเอารูปแบบและโครงสร้างของบุคลากรและปัจจัยเชิงวัฒนธรรมมาพิจารณาด้วย
- ต้องดำเนินการอย่างโปร่งใสและรอบคอบ
- ต้องเปลี่ยนแปลงและปรับปรุงเพื่อตอบสนองให้ทันต่อความเปลี่ยนแปลงของสภาพแวดล้อม
- ต้องสร้างสิ่งอำนวยความสะดวกและโครงสร้างพื้นฐานที่สนับสนุนการดำเนินงานที่ต่อเนื่อง
- ต้องมีการทบทวนและปรับปรุงตนเองอย่างต่อเนื่อง

<u>Process Overview ISO ๓๑๐๐๐:๒๐๐๙</u>



/แนวทาง...

แนวทางการบริหารความเสี่ยงด้านสารสนเทศ COBIT

คำว่า COBIT ย่อมาจาก The Control Objectives for Information and related Technology ซึ่งได้วางแนวพึงปฏิบัติที่ดีในการบริหาร IT ขึ้นโดย ๒ หน่วยงาน คือ ISACA และ ITGI ในปี ๑๙๙๒ โดย COBIT ได้ให้ความสนใจกับกลุ่ม ผู้บริหาร ผู้ตรวจสอบ และผู้ใช้งาน IT เพื่อให้สามารถวัดด้วยเกณฑ์ที่ยอมรับกันโดยทั่วไป สามารถหาดัชนีชี้วัด สามารถใช้กระบวนการ และแนวปฏิบัติที่ดี เพื่อช่วยในการทำให้เกิดประโยชน์สูงสุดแก่กิจการผ่านการใช้ IT และการพัฒนาการกำกับไอทีหรือไอทีภิบาล (IT Governance) และการควบคุมที่ดีในกิจการ

นอกจากนั้น กรอบการดำเนินงานตามแนวทาง COBIT ยังช่วยให้เครื่องมือในการบริหารทุกขั้นตอนของวงจรชีวิตของระบบสารสนเทศ การวางแผนและการจัดโครงสร้าง การจัดหาและการนำมาใช้งานของระบบสารสนเทศ การให้บริการในการดำเนินงาน การกำกับติดตาม และประเมินผล

ในการนำเอามาตรฐาน COSO และมาตรฐาน COBIT มาใช้ในกิจการ จะต้องรวบรวมประเด็นหลักตามกรอบการดำเนินงานของทั้งสองมาตรฐาน มาเชื่อมโยงกับกฎเกณฑ์ระเบียบที่สำคัญของกิจการ ดังนี้

(๑) COSO จะเป็นองค์ประกอบที่ระบุว่าจะต้องทำอย่างไรบ้าง

(๒) COBIT จะแสดงการควบคุมว่าต้องดำเนินการในเรื่องใดบ้าง เป็นกระบวนการบริหาร IT ที่ต้องใช้กิจกรรมการกำกับการปฏิบัติตามกฎเกณฑ์อย่างไรก็ดี การนำ COSO และ COBIT มาใช้ไม่ใช่เรื่องง่าย และยังต้องการการลงทุนจากกิจการ ผลกระทบที่จะเกิดแก่กิจการ คือ กิจการอาจจะต้อง

(๑) รื้อปรับระบบ (Reengineering) กระบวนการทั้งหมดในวงจรชีวิตด้าน IT

(๒) วางรูปแบบอย่างเป็นทางการเกี่ยวกับกิจกรรมที่เกี่ยวกับ IT ที่ต้องดำเนินการตามอย่างเคร่งครัด

(๓) มีเกณฑ์มาตรฐานของการดำเนินการด้าน IT

COBIT เป็นบทสรุปรวมของความรู้หรือข้อมูลต่าง ๆ ที่องค์กรต้องการสำหรับการนำไปปรับใช้เพื่อให้องค์กรมีการควบคุมภายในด้านเทคโนโลยีสารสนเทศที่ดีและเพื่อพัฒนาองค์กรให้เข้าสู่การเป็นองค์กรที่มี “ธรรมาภิบาลด้านเทคโนโลยีสารสนเทศ” หรือ IT Governance กล่าวคือ สามารถบริหารจัดการระบบสารสนเทศขององค์กรให้สามารถใช้งานได้อย่างมี ประสิทธิภาพ มีความคุ้มค่ากับการลงทุน และมีการบริหารจัดการที่โปร่งใสสามารถตรวจสอบได้ โดย COBIT จะรวบรวมตัววัด (Measures) เครื่องบ่งชี้ (Indicators) ขั้นตอนการปฏิบัติงาน (Processes) และแนวทางการปฏิบัติที่ดีที่สุด (Best Practices) ซึ่งเป็นข้อมูลที่มีโครงสร้างสามารถเข้าใจและนำไปใช้ได้โดยง่ายอีกทั้งเป็นที่ยอมรับกันโดยทั่วไปผู้ที่นำ COBIT ไปใช้ ได้แก่ ผู้บริหารธุรกิจ ผู้บริหารระบบสารสนเทศ และผู้ตรวจสอบ สามารถนำสิ่งต่างๆ เหล่านี้ไปใช้เป็นเครื่องมือเพื่อสร้างประโยชน์สูงสุดจากการนำเทคโนโลยีสารสนเทศเข้ามาใช้งานภายในองค์กรและช่วยให้การลงทุนทางด้านเทคโนโลยีสารสนเทศประสบความสำเร็จอย่างตรงตามความต้องการทางด้านธุรกิจเนื่องจากการนำ COBIT เข้ามาใช้จะช่วยให้ผู้ที่ปฏิบัติงานต่าง ๆ มีความเข้าใจในระบบเทคโนโลยีสารสนเทศที่ตนเองเกี่ยวข้องมากยิ่งขึ้น อีกทั้งยังช่วยในเรื่องของการยกระดับของการควบคุมด้านความปลอดภัยที่จำเป็นสำหรับการป้องกันสินทรัพย์ต่าง ๆ ขององค์กร

- แนวทางในการบริหารจัดการของ COBIT เขียนขึ้นเพื่อให้สามารถนำไปใช้ปฏิบัติได้จริงและเพื่อให้สามารถตอบคำถามต่าง ๆ ของผู้บริหารได้ เช่น
- องค์กรสามารถเติบโตได้ถึงขั้นไหน (ในด้านของการนำเทคโนโลยีสารสนเทศมาใช้ในองค์กร)

/การลงทุน...

- การลงทุนทางด้านเทคโนโลยีสารสนเทศคุ้มค่ากับประโยชน์ที่องค์กรจะได้รับหรือไม่
- ควรใช้อะไรเป็นตัวชี้วัดถึงประสิทธิภาพในการดำเนินงานด้านเทคโนโลยีสารสนเทศที่ดี
- อะไรเป็นปัจจัยที่สำคัญที่จะทำให้องค์กรประสบความสำเร็จได้ตรงตามเป้าหมายที่กำหนดไว้
- ความเสี่ยงที่จะทำให้องค์กรไม่สามารถบรรลุวัตถุประสงค์ที่ตั้งไว้มีอะไรบ้างจะมีวิธีการตรวจสอบและการควบคุมอย่างไร เพื่อลดโอกาสเกิดของความเสี่ยงดังกล่าวให้น้อยลง

สามารถนำมาตรฐาน หรือ แนวทางปฏิบัติอื่น ๆ ที่มีจุดมุ่งหมายที่ต้องการจะเน้นที่การควบคุมเฉพาะจุดใดจุดหนึ่งมาประยุกต์ใช้ร่วมกับ COBIT ได้ เช่น กลุ่มมาตรฐานของ ISO/IEC ๒๗๐๐๐ (ISO/IEC ๒๗๐๐๐ series) ซึ่งเป็นมาตรฐานที่เน้นในเรื่องของการรักษาความปลอดภัยของเทคโนโลยีสารสนเทศ หรือ มาตรฐาน ISO/IEC ๙๐๐๑:๒๐๐๐ ซึ่งเป็นมาตรฐานที่เน้นในเรื่องของการจัดการความต้องการทางด้านคุณภาพของ ระบบ (Quality Management Systems Requirement) หรือ มาตรฐานของ Information Technology Infrastructure Library (ITIL) ซึ่งเป็นมาตรฐานที่เน้นในเรื่องของการให้บริการด้านเทคโนโลยีสารสนเทศที่มีคุณภาพ หรือ มาตรฐาน Capability Maturity Model Integration (CMMI) ซึ่งเป็นมาตรฐานที่เน้นในเรื่องของการพัฒนาและผลิตซอร์ฟแวร์ที่มีคุณภาพ รวมไปถึงมาตรฐาน Projects in Controlled Environments ๒ (PRINCE๒) ซึ่งเป็นมาตรฐานที่เน้นในเรื่องของการบริหารจัดการโครงการที่มีประสิทธิภาพ เป็นต้น เนื่องจาก COBIT เป็นกรอบการปฏิบัติที่บอกให้ผู้ปฏิบัติทราบว่าต้องการอะไร บ้าง (what to do) แต่ไม่มีรายละเอียดในแง่ของวิธีการปฏิบัติที่จะนำไปสู่จุดนั้น (how to do) ดังนั้นผู้ปฏิบัติจึงควรนำมาตรฐาน หรือแนวทางปฏิบัติอื่น ๆ เข้ามาช่วยเสริมในส่วนของรายละเอียดที่เจาะลึกลงไปในเรื่องที่ต้องการได้โครงสร้างของโคบิตถูกออกแบบให้อยู่บนพื้นฐานของกระบวนการทางธุรกิจ (Business Process) ซึ่งแบ่งเป็น ๔ กระบวนการหลัก (Domains) ได้แก่

(๑) การวางแผนและการจัดองค์กร (Plan and Organize : PO)

(๒) การจัดหาและนำระบบออกใช้งานจริง (Acquire and Implement : AI)

(๓) การส่งมอบและการสนับสนุน (Delivery and Support : DS)

ในแต่ละ กระบวนการหลักข้างต้น โคบิตยังได้แสดงถึงวัตถุประสงค์การควบคุมหลัก (High-Level Control Objectives) รวมทั้งหมด ๓๔ หัวข้อ และในแต่ละหัวข้อจะประกอบไปด้วยวัตถุประสงค์การควบคุมย่อย (Detailed Control Objectives) รวมทั้งหมดถึง ๓๑๘ หัวข้อย่อย พร้อมทั้งยังมีแนวทางการตรวจสอบ (Audit Guideline) สำหรับแต่ละหัวข้อการควบคุมอีกด้วย (ซึ่งรายละเอียดจะกล่าวในหัวข้อถัดไป) นอกจากนี้ COBIT ได้แสดงถึงความสัมพันธ์ต่อปัจจัยหลัก ๒ ตัว ในทุกๆ หัวข้อของวัตถุประสงค์การควบคุม ได้แก่

๑. คุณภาพของสารสนเทศ (Information Criteria)

๑. ทรัพยากรด้านเทคโนโลยี (IT Resources)

คุณภาพของสารสนเทศ ๗ ประการ

๑. ประสิทธิภาพ (Effectiveness)

๒. ประสิทธิผล (Efficiency)

๓. การรักษาความลับ (Confidentiality)

๔. ความสมบูรณ์ของข้อมูล (Integrity)

๕. ความพร้อมใช้งานของข้อมูล (Availability)

๖. ความน่าเชื่อถือของข้อมูล (Reliability)

/ทรัพยากร...

ทรัพยากรด้านเทคโนโลยีสารสนเทศ ๔ ประเภท

๑. ระบบงานประยุกต์ (Application Systems)

๒. สารสนเทศ (Information)

๓. โครงสร้างพื้นฐาน (Infrastructure)

๔. บุคลากร (People)

(๔) การติดตามและประเมินผล (Monitor and Evaluate : ME)

แนวทางการสร้างมูลค่าผ่าน IT Compliance

กิจการที่มีเป้าหมายที่จะสร้างมูลค่าผ่าน IT Compliance ควรจะต้องวางเป้าหมายให้ชัดเจนว่า

(๑) การนำเอา IT Compliance มาใช้จะต้องประหยัดต้นทุนให้มากที่สุด

(๒) หลังจากเริ่มใช้ IT Compliance แล้วจะต้องปรับเพิ่ม ขอบเขตและประโยชน์จากการนี้ขึ้นไปอย่างต่อเนื่อง

(๓) IT Compliance จะต้องยกระดับไปสู่การทำงานด้วยคอมพิวเตอร์และเป็นระบบงานอัตโนมัติมากขึ้น

ณ เวลานี้และในอนาคต IT Compliance ยังคงเป็นเรื่องที่ท้าทายกิจการทั้งหลายเพราะเป็นเรื่องที่มีต้นทุนหรือใช้การลงทุน และยากในการนำขึ้นมาใช้จริง เพราะการตัดสินใจจะต้องมั่นใจว่า สามารถสร้างมูลค่าแก่กิจการและมีองค์ประกอบเพียงพอตามแนวทาง GRC

การกำกับดูแลกิจการที่ดี Good Corporate Governance

ตามความหมายที่ระบุไว้โดยตลาดหลักทรัพย์แห่งประเทศไทย “การกำกับดูแลกิจการที่ดี (Good Governance) หมายถึง “ระบบที่จัดให้มีโครงสร้างและกระบวนการการของความสัมพันธ์ระหว่างฝ่ายจัดการคณะกรรมการ และผู้ถือหุ้น เพื่อสร้างความสามารถในการแข่งขัน นำไปสู่ความเจริญเติบโตและเพิ่มคุณค่าให้กับผู้ถือหุ้นระยะยาว โดยคำนึงถึงผู้มีส่วนได้เสียอื่นประกอบ วัตถุประสงค์หลักของการกำกับดูแลกิจการที่ดี คือ การติดตาม กำกับ ควบคุม และดูแลผู้ได้รับมอบอำนาจให้ทำหน้าที่บริหาร ให้มีการจัดกระบวนการเพื่อใช้ทรัพยากรอย่างมีประสิทธิภาพ ตรงเป้าหมายอย่างคุ้มค่าและประหยัด เพื่อให้เกิดประโยชน์สูงสุดต่อผู้มีส่วนเกี่ยวข้องเหตุที่ต้องมีการกำกับดูแลกิจการที่ดี เพราะองค์กรจำเป็นต้องมีการบริหารจัดการมีผู้ถือหุ้นหรือเจ้าของกิจการจำนวนมาก และทุกคนที่เป็นเจ้าของไม่สามารถเข้าไปร่วมบริหารองค์กรได้ด้วยตนเอง

องค์ประกอบของการกำกับดูแลกิจการที่ดี

- จะต้องมีการถ่วงดุลอำนาจอย่างเหมาะสม เพื่อไม่เปิดโอกาสให้มีการใช้อำนาจหน้าที่โดยมิชอบ
- มีการกำหนดภาระหน้าที่ของพนักงานทุกระดับอย่างชัดเจน เพื่อพนักงานทุกคนจะได้รู้ขอบเขต หน้าที่และความรับผิดชอบ ซึ่งจะสะดวกในการติดตามและประเมินผลการทำงาน นอกจากนี้ยังเป็นการเสริมสร้างจิตสำนึกในภาระหน้าที่ของตนเอง
- มีระเบียบ ข้อบังคับ และคู่มือการปฏิบัติงานที่ชัดเจน และง่ายต่อการปฏิบัติ เพื่อจะได้ไม่เกิดปัญหาการตีความซึ่งอาจนำไปสู่การหาประโยชน์ใส่ตนได้
- มีระบบข้อมูลและการรายงานที่ดีซึ่งข้อมูลจะต้องถูกต้อง ทันสมัย ทันการณ์

/ให้ผู้มี...

- ให้ผู้มีส่วนได้เสียได้รู้ข้อมูลข่าวสาร

- มีข้อกำหนด จริยธรรม หรือจรรยาบรรณของพนักงานทุกฝ่าย เพื่อไม่ให้เกิดการเอารัดเอาเปรียบองค์กรหรือแสวงหาผลประโยชน์จากหน้าที่การงานในความรับผิดชอบ

ความสัมพันธ์ระหว่างการกำกับดูแลกิจการที่ดี การควบคุมภายใน การบริหารความเสี่ยง และการตรวจสอบภายในสิ่งที่เป็นรากฐานที่จะช่วยให้มีการกำกับดูแลกิจที่ดีนั้น ประกอบด้วย

รากฐานที่ ๑ การควบคุมภายใน

การควบคุมภายใน คือ กระบวนการ (process) ปฏิบัติงานที่คณะกรรมการบริษัท ฝ่ายบริหาร และ บุคลากรขององค์กรจัดให้มีขึ้น เพื่อให้สามารถมั่นใจได้อย่างสมเหตุสมผลว่า หากได้มีการปฏิบัติตามกระบวนการเหล่านี้แล้วองค์กรจะสามารถบรรลุวัตถุประสงค์ทางธุรกิจที่ต้องการได้โดยวัตถุประสงค์ของ ธุรกิจได้แก่

๑. ความมีประสิทธิผลและประสิทธิภาพในการดำเนินงาน (Effectiveness and efficiency of operations)

๒. ความน่าเชื่อถือของรายงานทางการเงิน (Reliability of financial reporting)

๓. การปฏิบัติตามกฎหมายและระเบียบข้อบังคับที่เกี่ยวข้อง (Compliance with applicable with laws and regulations) การกำหนดวัตถุประสงค์ของธุรกิจขึ้นมานั้น ผู้บริหารจะต้องกำหนดวิธีการทำงานให้ไปสู่ วัตถุประสงค์นั้น และในขณะเดียวกันก็ต้องมีการควบคุมการปฏิบัติงานต่างๆ ในองค์กรให้ดำเนินไปอย่างมี ประสิทธิภาพและประสิทธิผลด้วย การควบคุมต่างๆ เหล่านี้ ก็คือ การควบคุมกระบวนการภายในองค์กร หรือเรียกสั้น ๆ ว่าการควบคุมภายในนั่นเอง

ดังนั้น ทุกหน่วยงานในองค์กรจะจัดให้มีระบบการควบคุมภายในที่มีความเหมาะสมขึ้นมา ผู้เขียนได้เคยกล่าวมาแล้วว่า การจัดวางระบบการควบคุมภายในเป็นหน้าที่ของผู้บริหารหน่วยงาน ซึ่งเป็นผู้ที่ทราบดี ว่างานจุดใดของตนมีความเสี่ยง จากนั้นก็จะประเมินความเสี่ยงและสร้างระบบการควบคุมขึ้นเพื่อป้องกัน แก้ไข หรือตรวจหาความเสี่ยงเหล่านั้น โดยการควบคุมภายในมักจะถูกกำหนดออกมาในรูปของระเบียบ ข้อบังคับ หรือคู่มือการปฏิบัติงานต่างๆ และเช่นเดียวกันการปฏิบัติตามการควบคุมภายในที่กำหนดขึ้นมานั้นก็เป็นหน้าที่ของผู้ปฏิบัติงานของแต่ละหน่วยงาน การควบคุมภายในดังกล่าวจะช่วยเพิ่มประสิทธิภาพในการทำงานขององค์กร ช่วยให้ธุรกิจแข่งขันกับตลาดได้ ช่วยป้องกันการรั่วไหล ช่วยให้องค์กรเห็นฐานะการเงินที่ถูกต้องเชื่อถือได้ และในที่สุด ก็คือการช่วยให้องค์กรเติบโตได้อย่างมั่นคง

รากฐานที่ ๒ การบริหารความเสี่ยง

การบริหารความเสี่ยง (Risk Management) คือ การกำหนดแนวทางและกระบวนการในการระบุ ประเมิน จัดการและติดตามความเสี่ยงที่เกี่ยวข้องกับกิจกรรม หน่วยงาน หรือการดำเนินงานขององค์กร รวมทั้งการกำหนดวิธีการในการบริหารและควบคุมความเสี่ยงให้อยู่ในระดับที่ผู้บริหารยอมรับได้ซึ่งสามารถมองได้เป็น ๒ มุมมอง คือ

- การกำจัดหรือลดปัจจัยต่าง ๆ ที่จะขัดขวางไม่ให้องค์กรบรรลุวัตถุประสงค์ นั่นคือ การปกป้องมูลค่าที่องค์กรมีอยู่ไม่ให้ถูกทำลายไป

- มองหาโอกาสที่จะสร้างความได้เปรียบในการดำเนินธุรกิจ

/รากฐานที่...

รากฐานที่ ๓ การตรวจสอบภายใน

การตรวจสอบภายในมีบทบาททำให้มั่นใจว่ามีการควบคุมภายในที่เหมาะสมและการควบคุมเหล่านั้นได้รับการปฏิบัติตามภายในองค์กรตลอดจนมีนำระบบการบริหารความเสี่ยงมาปรับใช้อย่างเหมาะสม ตลอดจนช่วยถ่วงดุลอำนาจไม่ให้มีการใช้อำนาจไปในทางที่ผิดจากการที่หน่วยงานได้จัดให้มีระบบการควบคุมภายในของตนมีการบริหารความเสี่ยงและมีการปฏิบัติตามแล้วผู้ตรวจสอบภายในก็เหมือนเป็นคนที่มากรองอีกชั้นหนึ่ง เพื่อให้ผู้เป็นเจ้าของ/ผู้ถือหุ้นนั้นเกิดความมั่นใจการตรวจสอบภายในนั้นก็ถือเป็นกลไกอย่างหนึ่งที่จะช่วยผลักดันให้เกิดการควบคุมภายในและการบริหารความเสี่ยงที่เหมาะสมยิ่งขึ้น เพราะบางครั้งผู้ปฏิบัติงานอาจคิดว่าทำแค่นี้ก็เพียงพอแล้วแต่ผู้ตรวจสอบภายในก็จะมีวิธีทดสอบว่าการควบคุมที่ปฏิบัติกันอยู่นั้นความเพียงพอจริงหรือไมหรือบางครั้งอาจมีการการปฏิบัติงานกันมานานแม้ว่าจะมีความชำนาญแต่ก็อาจทำให้ประมาทโดยละเลยบางจุดที่ควรจะต้องควบคุมไปหากผู้ตรวจสอบภายในตรวจพบเป็นการเตือนให้ระมัดระวังมากขึ้น ดังนั้น หากผู้ตรวจสอบภายในเข้าไปปฏิบัติงานในหน่วยงาน

มาตรฐานการ ISO ๒๖๐๐๐

ISO ๒๖๐๐๐ Social Responsibility เป็นมาตรฐานการแสดงความรับผิดชอบต่อผลกระทบของสังคมและสิ่งแวดล้อมจากการตัดสินใจและดำเนินกิจกรรมต่าง ๆ ขององค์กร เพื่อความเป็นอยู่ที่ดีของคนในสังคม และการพัฒนาที่ยั่งยืนทางธุรกิจเหตุเกิดจาก CSR ปัจจุบันกระแสการสร้างความรับผิดชอบต่อสังคมขององค์กร (Corporate Social Responsibility : CSR) ได้เข้ามาสู่โลกธุรกิจอุตสาหกรรมอย่างจริงจัง เนื่องจากปัญหาวิกฤติด้านสิ่งแวดล้อมและแรงงานในทั่วทุกมุมโลก ดังนั้นจึงได้มีการแสวงหาแนวคิดและแนวทางดำเนินการ เพื่อให้เกิดความสันติและการสานสัมพันธ์อันดีในการอยู่ร่วมกันในสังคม

ด้วยเหตุนี้ องค์การระหว่างประเทศว่าด้วยการมาตรฐาน (International Organization for Standardization:ISO) จึงได้กำหนดมาตรฐานว่าด้วยความรับผิดชอบต่อสังคม (ISO ๒๖๐๐๐ Social Responsibility) เพื่อให้บริษัท องค์กร หน่วยงาน และสถาบันทั่วโลกรวมไปถึงผู้มีส่วนได้ส่วนเสียขององค์กรได้เพิ่มความตระหนักและสร้างความเข้าใจในเรื่องของความรับผิดชอบต่อสังคม ซึ่งมาตรฐานดังกล่าวจะเป็นข้อแนะนำ หลักการ วิธีการของความรับผิดชอบต่อสังคมที่องค์กรพึงปฏิบัติโดยความสมัครใจทุกองค์กรสามารถนำไปประยุกต์ใช้ได้โดยไม่ต้องมีการตรวจรับรอง ISO ๒๖๐๐๐ ได้เริ่มมีการพิจารณาตั้งแต่ พ.ศ. ๒๕๔๘ เป็นต้นมา และคาดว่าจะประกาศใช้ภายในปี พ.ศ. ๒๕๕๓ สำนักงานมาตรฐานผลิตภัณฑ์อุตสาหกรรม (สมอ.) ในฐานะหน่วยงานที่รับผิดชอบด้านงานมาตรฐาน จึงได้จัดสัมมนาเรื่อง “CEO Forum for ISO ๒๖๐๐๐ Social Responsibility” ขึ้น เพื่อเป็นการเตรียมความพร้อม ตลอดจนสร้างความรู้และความเข้าใจที่ถูกต้องตรงกันเกี่ยวกับมาตรฐานดังกล่าวก่อนที่จะมีการประกาศใช้อย่างเป็นทางการ โดยมุ่งหวังให้องค์กรสามารถนำไปใช้ดำเนินการด้านความรับผิดชอบต่อสังคมได้อย่างมีประสิทธิภาพและพะก่อให้เกิดประโยชน์ในทุกภาคส่วนของสังคม

หลัก ๗ ประการของ ISO ๒๖๐๐๐

ISO ๒๖๐๐๐ มีหลักการสำคัญ ๗ ประการ คือ

(๑) หลักการปฏิบัติตามกฎหมาย (Principle of legal compliance) องค์กรจะต้องมีการปฏิบัติที่สอดคล้องกับกฎหมาย และกฎระเบียบต่างๆ ที่เกี่ยวข้องกับชาติและระดับสากลทั้งในเชิงรุกและเชิงรับ

(๒) หลักการเคารพต่อแนวปฏิบัติระดับชาติหรือระดับสากล (Principle of respect for authoritative inter-government agreements or internationally recognized instruments) รวมถึงสนธิสัญญาสากล คำสั่ง ประกาศ ข้อตกลง มติ และข้อชี้นำต่างๆ ซึ่งได้รับการรับรองจากองค์กรสากลที่เกี่ยวข้องกับองค์กรนั้นๆ

/(๓) หลักการ...

(๓) หลักการให้ความสำคัญกับผู้มีส่วนได้ส่วนเสีย (Principle of recognition of stakeholders and concerns) องค์กรควรตระหนักถึงสิทธิและผลประโยชน์ของผู้มีส่วนได้ส่วนเสีย โดยเปิดโอกาสให้แสดงความคิดเห็นเกี่ยวกับกิจกรรมขององค์กร เช่น นโยบาย ข้อเสนอ หรือการตัดสินใจต่างๆ ก็ตามที่จะส่งผลต่อผู้มีส่วนได้ส่วนเสีย

(๔) หลักของการแสดงรับผิดชอบที่สามารถตรวจสอบได้ (Principle of accountability) ในการดำเนินงานใดๆก็ตามขององค์กรต้องสามารถตรวจสอบได้จากภายนอก

(๕) หลักการความโปร่งใส (Principle of transparency) องค์กรควรเปิดเผยข้อมูลต่างๆให้ผู้มีส่วนได้ส่วนเสีย รวมถึงผู้ที่เกี่ยวข้องได้รับทราบอย่างชัดแจ้ง

(๖) หลักการความเคารพในสิทธิมนุษยชน (Principle of respect of fundamental human right) องค์กรควรดำเนินนโยบายและดำเนินกิจกรรมที่สอดคล้องกับปฏิญญาสากลว่าด้วยสิทธิมนุษยชน

(๗) หลักการความเคารพในความหลากหลาย (Principle of respect for diversity) องค์กรควรจ้างพนักงาน โดยไม่มีการแบ่งแยกเชื้อชาติ สีผิว ความเชื่อ อายุ เพศ

องค์ประกอบของความรับผิดชอบต่อสังคม

ความรับผิดชอบต่อสังคมนั้นมีองค์ประกอบหลากหลาย ซึ่งใน ISO ๒๖๐๐๐ ได้กำหนดองค์ประกอบหลักของความรับผิดชอบไว้ ๗ ประการ ดังนี้

(๑) มีการกำกับดูแลกิจการที่ดี (Organization governance) กล่าวคือ องค์กรควรกำหนดหน้าที่ให้คณะกรรมการฝ่ายจัดการ ผู้ถือหุ้น และผู้มีส่วนได้ส่วนเสียสามารถสอดส่องดูแลผลงานและการปฏิบัติงานขององค์กรได้ เพื่อแสดงถึงความโปร่งใส พร้อมรับการตรวจสอบ และสามารถชี้แจงให้ผู้มีส่วนได้เสียได้รับทราบถึงผลการปฏิบัติงานได้

(๒) คำนึงถึงสิทธิมนุษยชน (Human rights) ซึ่งเป็นสิทธิขั้นพื้นฐานของมนุษย์ โดยสิทธิดังกล่าวควรครอบคลุมถึงสิทธิความเป็นพลเมือง สิทธิทางการเมือง สิทธิทางเศรษฐกิจ สังคม และวัฒนธรรม และสิทธิตามกฎหมายระหว่างประเทศด้วย

(๓) ข้อปฏิบัติด้านแรงงาน (Labor practices) องค์กรต้องตะหนักว่าแรงงานไม่ใช่สินค้า ดังนั้นแรงงานจึงไม่ควรถูกปฏิบัติเสมือนเป็นปัจจัยการผลิต

(๔) การดูแลสิ่งแวดล้อม (Environment) องค์กรจำเป็นที่จะต้องคำนึงถึงหลักการป้องกันปัญหามลพิษการบริโภคอย่างยั่งยืน (Sustainable consumption) และการใช้ทรัพยากรอย่างมีประสิทธิภาพในการดำเนินการผลิตและบริการ

(๕) การดำเนินธุรกิจอย่างเป็นธรรม (Fair operating practices) องค์กรต่างๆ ควรแข่งขันกันอย่างเป็นธรรมและเปิดกว้าง ซึ่งจะช่วยส่งเสริมประสิทธิภาพในการลดต้นทุนสินค้าและบริการ นวัตกรรมการพัฒนาสินค้าหรือกระบวนการใหม่ ๆ รวมถึงจะช่วยขยายการเติบโตทางเศรษฐกิจและมาตรฐานการครองชีพในระยะยาว

(๖) ใส่ใจต่อผู้บริโภค (Consumer issues) องค์กรจะต้องเปิดโอกาสให้ผู้บริโภคได้รับทราบข้อมูลในการใช้สินค้าและบริการอย่างเหมาะสม ทั้งยังต้องให้ความสำคัญกับการพัฒนาสินค้าและบริการที่เป็นประโยชน์ต่อสังคม โดยคำนึงถึงความปลอดภัยในการใช้งานและสุขภาพของผู้บริโภค นอกจากนี้เมื่อพบว่าสินค้าไม่เป็นไปตามเกณฑ์ที่กำหนดองค์กรก็จะต้องมีกลไกในการเรียกคืนสินค้า พร้อมทั้งยังต้องให้ความสำคัญกับกฎหมายคุ้มครองผู้บริโภค และถือปฏิบัติอย่างเคร่งครัดอีกด้วย

/(๗) การแบ่งปัน...

(๗) การแบ่งปันสู่สังคมและชุมชน (Contribution to the community and society) เริ่มทำ ISO ๒๖๐๐๐ ได้อย่างไรการดำเนินการเพื่อเป็นองค์กรที่มีความรับผิดชอบต่อสังคมนั้นสามารถปฏิบัติได้ไม่ยาก มีขั้นตอนดำเนินการคือ เริ่มแรกนั้นองค์กรจะต้องกำหนดให้การจัดทำ ISO ๒๖๐๐๐ เป็นนโยบายขององค์กร นโยบายเสียก่อนจากนั้นจึงกำหนดโครงสร้างหน้าที่ของผู้ที่จะมารับผิดชอบในการปฏิบัติตามนโยบาย พร้อมทั้งทำความเข้าใจถึงบริบทของความรับผิดชอบต่อสังคมขององค์กร หลังจากนั้นก็ปรับปรุงให้เข้ากับวิสัยทัศน์ พันธกิจ นโยบาย และกลยุทธ์ขององค์กร แล้วจึงจะนำไปปฏิบัติให้ตรงตามแผนงานที่ได้วางไว้ ทั้งนี้ในการปฏิบัติงานทุกครั้งจะต้องมีการติดตามและประเมินผลงานด้วย เพื่อให้สามารถนำไปปรับใช้และพัฒนาได้ต่อไป อย่างไรก็ดี ในการดำเนินงานองค์กรควรจะทำการสื่อสารและประสานงานกับคนภายในองค์กร รวมถึงผู้มีส่วนได้ส่วนเสียให้ได้รับรู้และมีความเข้าใจตรงกัน จึงจะทำให้การดำเนินงานมีประสิทธิภาพมากยิ่งขึ้น สำหรับประโยชน์ที่จะได้รับการดำเนินการตามมาตรฐาน ISO ๒๖๐๐๐ ในมุมมองด้านธุรกิจนั้น สามารถเพิ่มยอดขายและส่วนแบ่งทางการตลาดให้กับองค์กร สร้างจุดแข็งให้กับตราสินค้า ส่งเสริมภาพลักษณ์และความร่วมมือในการบริหารองค์กร ตลอดจนเพิ่มขีดความสามารถ แรงจูงใจ และสร้างขวัญกำลังใจให้กับพนักงาน ทำให้สามารถรักษาพนักงานที่ดีไว้ให้อยู่กับองค์กรตลอดไปได้ ส่วนประโยชน์ในด้านสังคมและสิ่งแวดล้อมนั้นเป็นการสร้างชื่อเสียงให้กับองค์กร ลดปัญหาและผลกระทบจากสิ่งแวดล้อม เสริมสร้างชุมชนและสังคมให้เข้มแข็ง

ทั้งนี้ ควรนำแนวทางการควบคุมภายในตามหลักการต่าง ๆ ที่กล่าวมาข้างต้นมาปรับใช้กับองค์กรอย่างเหมาะสม เพื่อให้ผลการดำเนินงานบรรลุตามเป้าหมายที่กำหนด และเพื่อความยั่งยืนขององค์กรต่อไป

.....