

COSO คืออะไร

หลักการและแนวคิดสากลเกี่ยวกับ COSO

COSO คือ กรอบแนวคิดการควบคุม เพื่อช่วยให้ผู้ปฏิบัติงานบรรลุเป้าหมาย ทั้งเรื่องของการปฏิบัติงานอย่างมีประสิทธิภาพ ประสิทธิภาพ ความถูกต้องครบถ้วนของรายงาน และการปฏิบัติตามกฎเกณฑ์ที่กำหนด

COSO ย่อมาจาก Committee of Sponsoring of the Treadway Commission เป็นคณะทำงานที่ก่อตั้งขึ้น โดยคณะกรรมการการบัญชีของสหรัฐอเมริกา ที่ชื่อว่า Treadway Commission ในปี 1985 โดยจัดตั้งขึ้นเพื่อศึกษาและพัฒนาแนวทางการบริหารความเสี่ยง รูปแบบการควบคุมภายในที่มีประสิทธิภาพ และป้องกันการทุจริตของรายงานทางการเงิน

ทั้งนี้ COSO ประกอบด้วย ผู้แทนจากสถาบันวิชาชีพ ๕ แห่ง ในประเทศสหรัฐอเมริกา ได้แก่

๑. สถาบันผู้สอบบัญชีรับอนุญาตแห่งสหรัฐอเมริกา: American Institute of Certified Public Accountants (AICPA)

๒. สถาบันผู้ตรวจสอบภายในสากล: Institute of Internal Auditors (IIA)

๓. สถาบันผู้บริหารการเงิน: Financial Executives Institute (FEI)

๔. สมาคมนักบัญชีแห่งสหรัฐอเมริกา: American Accounting Association (AAA)

๕. สถาบันนักบัญชีเพื่อการบริหาร: Institute of Management Accountants (IMA)

ค.ศ. 1985 มีการจัดตั้งคณะกรรมการการบัญชีของสหรัฐอเมริกา ที่ชื่อว่า Treadway Commission โดยตั้งขึ้นเพื่อป้องกันการทุจริตของรายงานทางการเงิน

ค.ศ. 1987 Treadway Commission ได้เสนอให้ตั้งคณะทำงาน ในนามว่า Committee of Sponsoring of the Treadway Commission หรือ COSO เพื่อศึกษาและพัฒนากรอบการควบคุมภายในที่มีประสิทธิภาพ

ค.ศ. 1992 COSO ได้เสนอรายงานกรอบการควบคุมภายใน (Internal Control - Integrated Framework) ประกอบด้วยองค์ประกอบของการควบคุมภายใน ๕ ด้านที่สัมพันธ์กัน กรอบงานการควบคุมนี้ บางที่เรียกกันว่า COSO 1

ค.ศ. 2004 COSO ได้เสนอกรอบงานการประเมินความเสี่ยงระดับองค์กร (Enterprise Risk Management- Integrated Framework) ประกอบด้วยองค์ประกอบ ๘ ด้านที่สัมพันธ์กัน ซึ่งพัฒนาจากกรอบงานการควบคุมภายในที่มีองค์ประกอบ ๕ ด้าน และองค์ประกอบเหล่านี้ใช้เป็นเกณฑ์ในการประเมินความเพียงพอของการบริหารความเสี่ยงและการควบคุม กรอบงาน การควบคุมนี้ บางที่เรียกกันว่า COSO 2

ค.ศ. 2006 COSO ได้ประกาศแนวทางการควบคุมภายในด้านการจัดทำงบการเงิน ประกอบด้วย ๕ องค์ประกอบ และ ๒๐ หลักการ โดยได้ดัดแปลงกรอบงานการควบคุมภายในเดิม (COSO 1) เพื่อลดต้นทุนในการควบคุมภายในด้านการจัดทำงบการเงินตามกฎหมาย US. Sarbanes - Oxley Act (2002) สำหรับกิจการขนาดเล็ก Internal Control over Financial Report - Guidance for Small Public Companies แนวทางนี้นิยมเรียกกันว่า COSO 3

ค.ศ. 2009 COSO 4 เป็นแนวทางด้านการกำกับติดตาม Guidance on Monitoring of Internal Control

ค.ศ. 2013 COSO ได้ประกาศแนวทางการควบคุมภายในด้านการจัดทำรายงานทางการเงิน และรายงานที่ไม่ใช่งบการเงิน ซึ่งยังคงยึดกรอบแนวคิดเดิมของปี ค.ศ.1992 (Internal Control - Integrated Framework) ที่กำหนดให้การควบคุมภายในมีองค์ประกอบหลัก ๕ องค์ประกอบ แต่เพิ่มเติมในส่วนอื่นๆ ให้ชัดเจนขึ้น เรียกกันว่า COSO 2013

หลักการและแนวคิดในประเทศไทย

ความมุ่งมั่นพิทักษ์รักษาเงินของแผ่นดินที่มาจากภาษีอากรของประชาชน ทุกหน่วยงานควรตระหนักและช่วยกันรักษาสถิติไทยไว้ เนื่องจากการบริหารราชการแผ่นดินที่มีระบบระเบียบและคุณธรรมองค์ประกอบเหล่านี้จำเป็นต้องมีการค้นหาและพบให้ได้ด้วยวิธีปฏิบัติที่เป็นไปโดยธรรมชาติและยั่งยืน ระบบการควบคุมภายในที่มีมาตรฐาน ไม่ใช่สิ่งที่เป็นวิชาการด้านเดียว หากแต่เป็นการปฏิบัติที่สามารถตรวจสอบได้ถึงอุดมคติและจริยธรรมที่ซ่อนเร้นในตัวบุคคลทุกระดับขององค์การ ตั้งแต่ผู้บริหารระดับสูงจนถึงผู้ปฏิบัติงานระดับล่าง การที่หน่วยงานต่างๆ มีระบบการควบคุมภายในที่มีมาตรฐานที่ตุนั้นย่อมแสดงได้ว่าองค์การนั้นๆ ตระหนักถึงการดำเนินงานแบบมืออาชีพเพื่อการบรรลุผลสัมฤทธิ์ตามวัตถุประสงค์และพันธกิจของหน่วยงาน ทำให้หน่วยงานที่มีการจัดวางระบบการควบคุมภายในและการประเมินผลการควบคุมภายใน จะสามารถลดภาระงานตลอดจนปัญหาอุปสรรคต่างๆ ของการปฏิบัติงานลงได้ อันเป็นประโยชน์ที่ทำให้หน่วยงานต่างๆ มีการพัฒนาระบบการควบคุมภายในให้สามารถปฏิบัติได้จริงและมีความทันสมัยของการบริหารจัดการองค์การอยู่เสมอ ทั้งยังส่งเสริมให้หน่วยงานนั้นๆ ปฏิบัติตามกฎหมาย ระเบียบ ข้อบังคับต่างๆ ของการควบคุมภายใน ก่อเกิดการบริหารจัดการแบบธรรมาภิบาลและการบริหารกิจการบ้านเมืองที่ดีอีกด้วย

กิจกรรมการควบคุมภายใน/แนวทางการกำหนดวัตถุประสงค์กิจกรรมการควบคุมภายใน

กิจกรรมการควบคุมภายในเป็นวิธีการต่างๆ ที่นำมาใช้ในการปฏิบัติงานซึ่งกำหนดหรือออกแบบเพื่อป้องกันหรือลดความเสี่ยงอย่างมีประสิทธิภาพและประสิทธิผล ฝ่ายบริหารต้องจัดให้มีกิจกรรมการควบคุมที่มีประสิทธิภาพและประสิทธิผล เพื่อป้องกันหรือลดความเสี่ยง ความผิดพลาดที่อาจเกิดขึ้น และให้สามารถบรรลุผลสำเร็จตามวัตถุประสงค์ของการควบคุมภายใน

กิจกรรมการควบคุมภายใน หมายถึง นโยบาย และระเบียบ วิธีปฏิบัติ รวมถึงมาตรการต่างๆ ที่ฝ่ายบริหารกำหนดขึ้นเพื่อให้บุคลากรนำไปปฏิบัติเพื่อลดหรือควบคุมความเสี่ยงและได้รับการสนองตอบโดยมีการปฏิบัติตามตัวอย่างกิจกรรมการควบคุมภายใน เช่น การสอบทาน การดูแลป้องกันทรัพย์สิน และการแบ่งแยกหน้าที่ เป็นต้น

กิจกรรมการควบคุมภายในมีอยู่ในทุกหน้าที่ และทุกระดับการปฏิบัติงาน เช่น การควบคุมงาน การให้คำแนะนำ การมอบอำนาจ การอนุมัติ การตรวจสอบ การสอบทานผลการปฏิบัติงาน การรักษาความปลอดภัย การแบ่งแยกหน้าที่ การจัดบันทึกกิจกรรมต่างๆ รวมทั้งการรวบรวมและจัดเก็บเอกสารที่เกี่ยวข้อง ซึ่งเป็นหลักฐานแสดงการปฏิบัติกิจกรรมนั้นๆ ดังนั้นในการปฏิบัติงานทุกด้าน ผู้บริหารจะต้องจัดให้มีกิจกรรมการควบคุมภายในอย่างเหมาะสมและเพียงพอกับระดับความเสี่ยงที่จะก่อให้เกิดความเสียหาย

กิจกรรมการควบคุมภายในมีอยู่หลายประเภท การจัดให้มีกิจกรรมการควบคุมมากน้อยเพียงใด ประเภทกับกิจกรรมใดขึ้นอยู่กับลักษณะความเสี่ยงของหน่วยรับตรวจนั้น ซึ่งแต่ละหน่วยรับตรวจอาจมีความเสี่ยงที่แตกต่างกัน ดังนั้น ผู้บริหารจำเป็นต้องทราบถึงลักษณะความเสี่ยง ปัจจัยเสี่ยงด้านต่างๆ และวิธีประเมินความเสี่ยง เพื่อพิจารณาจัดกิจกรรมการควบคุมภายในที่มีความสัมพันธ์และเหมาะสมกับความเสี่ยงนั้นๆ

ตัวอย่างกิจกรรมการควบคุมภายในที่ปฏิบัติโดยทั่วไป ผู้บริหารอาจพิจารณานำไปใช้เหมาะสมกับหน่วยงานที่รับผิดชอบ ดังนี้

๑. การกำหนดนโยบายและระเบียบวิธี

ผู้บริหารระดับสูงเป็นผู้กำหนดนโยบายและแผนงาน เพื่อแสดงให้เห็นถึงทิศทางของหน่วยงาน ส่วนผู้บริหารระดับรองลงมาเป็นผู้กำหนดระเบียบ วิธีปฏิบัติ เพื่อใช้ในการดำเนินงานด้านต่างๆ ที่ตนเองรับผิดชอบ โดยระเบียบวิธีปฏิบัตินั้นจะต้องสอดคล้องและรองรับตามนโยบายและแผนงาน และปรับปรุงให้เหมาะสมกับสภาพแวดล้อมอยู่เสมอ รวมทั้งจัดให้มีระบบการรายงานผลการปฏิบัติงานเป็นระยะๆ เพื่อวัดผลการดำเนินงานที่ผ่านมา และนำมาปรับปรุงให้ดียิ่งขึ้น

๒. การสอบทานโดยผู้บริหาร

การสอบทานรายงานและข้อมูลข่าวสารต่างๆ โดยผู้บริหาร เป็นกิจกรรมการควบคุมที่สำคัญที่ควรกระทำอย่างต่อเนื่องโดยสม่ำเสมอ และควรบันทึกผลการสอบทานการปฏิบัติงานและสถานการณ์ที่ผู้บริหารจำเป็นต้องติดตามแก้ไขเป็นลายลักษณ์อักษร ซึ่งการสอบทานผลการปฏิบัติงานของผู้บริหารในแต่ละระดับอาจมุ่งเน้นให้ความสนใจในประเด็นที่แตกต่างกัน

- การสอบทานโดยผู้บริหารสูงสุด

ผู้บริหารสูงสุด ควรมุ่งมั่นให้ความสนใจกับการบรรลุผลสำเร็จตามวัตถุประสงค์ของหน่วยรับตรวจในภาพรวมและวัตถุประสงค์ที่สำคัญของหน่วยรับตรวจ โดยการวิเคราะห์เปรียบเทียบระหว่างข้อมูลผลการปฏิบัติงานจริงกับงบประมาณ เป้าหมายตามแผนงาน ประสิทธิภาพ รวมทั้งเปรียบเทียบกับข้อมูลในงวดที่ผ่านมา หรือเปรียบเทียบกับข้อมูลของหน่วยงานอื่นที่มีลักษณะใกล้เคียงกัน หรือตัวชี้วัดความสำเร็จอื่นๆ ซึ่งจะทำให้เห็นภาพรวมของการดำเนินงานว่ามีปัญหาในด้านใดบ้าง รวมทั้งช่วยให้ผู้บริหารสามารถวิเคราะห์หาสาเหตุ และแนวทางการแก้ไขที่จำเป็น

- การสอบทานโดยผู้บริหารระดับรองลงมา

ผู้บริหารระดับรองลงมาหรือผู้บริหารระดับกลางเป็นผู้มีหน้าที่รับผิดชอบเฉพาะงานด้านใดด้านหนึ่งในหน่วยรับตรวจ ตามที่ได้รับมอบหมายจากผู้บริหารสูงสุด จึงควรมุ่งเน้นสอบทานผลการปฏิบัติงานที่เกิดขึ้นจริงในหน่วยงานหรือกิจกรรมที่ตนรับผิดชอบเปรียบเทียบกับเป้าหมายตามแผนงานที่กำหนดไว้ และวิเคราะห์หาสาเหตุของความแตกต่างที่มีสาระสำคัญที่เกิดขึ้น รวมทั้งสอบทานการปฏิบัติงานจริงกับระเบียบและวิธีการปฏิบัติต่างๆ การสอบทานควรเข้มงวดหรือกระทำบ่อยครั้ง มากน้อยเพียงใดขึ้นกับลักษณะและระดับความเสี่ยงของงานนั้นๆ

๓. การควบคุมการประมวลผลข้อมูล

ผู้บริหารต้องใช้ข้อมูลสารสนเทศภายในหน่วยรับตรวจประกอบการตัดสินใจในการบริหารจัดการ ทั้งข้อมูลทางบัญชีการเงินและข้อมูลอื่นที่สำคัญ ดังนั้นข้อมูลที่ผ่านมาผ่านการประมวลผลทั้งในรูปแบบสารสนเทศหรือรายงาน จะต้องมีความถูกต้อง ครบถ้วน ทันเวลา และให้เนื้อหาที่เป็นประโยชน์ต่อการตัดสินใจ กิจกรรมการควบคุมที่ควรมีเพื่อให้ได้สารสนเทศและรายงานที่มีความสมบูรณ์ ได้แก่ มีการอนุมัติรายการทุกครั้งก่อนทำการบันทึกบัญชี ทะเบียนหรือแฟ้มหลักฐานอื่น การสอบทานหรือการเปรียบเทียบข้อมูลก่อนการบันทึกการรายนั้น การสอบทานหรือการเปรียบเทียบข้อมูลระหว่างกัน การใช้เทคโนโลยีที่เหมาะสมช่วยในการประมวลผลข้อมูลทั้งอุปกรณ์ รายงาน และบุคคล

๔. การอนุมัติ

ในการดำเนินงานของทุกหน่วยรับตรวจ ผู้บริหารไม่สามารถดำเนินงานให้บรรลุวัตถุประสงค์ของหน่วยรับตรวจที่ได้กำหนดไว้โดยลำพัง จึงจำเป็นต้องมอบหมายให้บุคลากรระดับรองลงมาปฏิบัติแทน โดยการมอบอำนาจ ในการมอบอำนาจให้แก่บุคลากรระดับต่างๆ นั้น ควรกำหนดขอบเขตของอำนาจในการอนุมัติให้ชัดเจนเป็นลายลักษณ์อักษรและควรสื่อสารให้บุคลากรทราบโดยทั่วกัน ผู้ที่ได้รับมอบอำนาจหน้าที่ให้เป็นผู้อนุมัติ ควรสอบทานความเพียงพอของเอกสารประกอบการขออนุมัติ ว่าถูกต้อง เหมาะสม และเป็นไปตามกฎหมาย ระเบียบ นโยบาย และแนวทางการปฏิบัติงานที่เกี่ยวข้อง และมีวงเงินที่อนุมัติอยู่ภายใต้ขอบเขตอำนาจที่ตนสามารถอนุมัติได้ รวมทั้งควรสอบถามเกี่ยวกับรายการที่ผิดปกติจากผู้ที่เกี่ยวข้อง ก่อนลงนามอนุมัติให้ดำเนินการ นอกจากนี้ผู้ที่มีอำนาจอนุมัติไม่ควรลงนามอนุมัติในแบบฟอร์มเปล่าหรือแบบฟอร์มที่ไม่มีข้อมูลรายการที่ขออนุมัติอย่างเพียงพอ

๕. การดูแลป้องกันทรัพย์สิน

การดูแลป้องกันทรัพย์สินเป็นการจำกัดการเข้าถึงทรัพย์สินที่มีความเสี่ยง เช่น เงินสด ทรัพย์สินที่มีค่า เอกสารหลักฐานและระบบงานที่สำคัญ ข้อมูลสารสนเทศที่เป็นความลับขององค์กร เป็นต้น เพื่อป้องกันการสูญหาย การทุจริต และการนำไปใช้ประโยชน์โดยผู้ที่ไม่ได้อำนาจหน้าที่ที่เกี่ยวข้อง ฝ่ายบริหาร ควรจัดให้มีการดูแลทรัพย์สินอย่างรัดกุมและเพียงพอ การดูแลป้องกันทรัพย์สินที่ดี คือ การควบคุมการเข้าถึงทรัพย์สินนั้น เช่น การเก็บเงินสดและของมีค่าในเซฟที่ปลอดภัย การใส่กุญแจห้องเก็บพัสดุหรือตู้เก็บเอกสารหลักฐานที่สำคัญ การใช้ระบบรักษาความปลอดภัยโดยใช้การ์ดหรือแผงสัญญาณ การใช้รหัสผ่าน การจัดเวรยามรักษาความปลอดภัย เป็นต้น นอกจากนี้ฝ่ายบริหารควรกำหนดให้มีการจัดทำทะเบียนทรัพย์สินและมีการตรวจนับทรัพย์สินเป็นระยะๆ โดยบุคคลที่ไม่ได้อำนาจหน้าที่เกี่ยวกับการจัดหาและดูแลรักษาทรัพย์สินนั้นๆ และเปรียบเทียบผลที่ได้จากการตรวจนับกับทะเบียนทรัพย์สิน หากมีผลต่างเกิดขึ้น ควรติดตามหาสาเหตุแล้ว ดำเนินการตามควรแก่กรณี และปรับปรุงทะเบียนทรัพย์สินให้ถูกต้อง

๖. การแบ่งแยกหน้าที่

หน้าที่ความรับผิดชอบของงานที่เสี่ยงต่อความเสียหายจำเป็นต้องมีการแบ่งแยกหน้าที่ เพื่อป้องกันหรือลดความเสี่ยงจากข้อผิดพลาดหรือการทุจริต ตัวอย่างเช่น

(๑) การอนุมัติรายการ หรือการให้ความเห็นชอบ

(๒) การประมวลผล หรือการบันทึกรายการ

(๓) การดูแลทรัพย์สินที่เกี่ยวข้อง

ไม่ควรให้บุคลากรคนเดียวปฏิบัติงานนั้นตั้งแต่ต้นจนจบ ในกรณีที่หน่วยรับตรวจมีข้อจำกัดด้านบุคลากร ทำให้ไม่สามารถแบ่งแยกหน้าที่งานดังกล่าวได้ ควรกำหนดกิจกรรมอื่นทดแทน เช่น กำหนดให้มีการสอบทานรายละเอียดของกิจกรรมต่างๆ เพิ่มขึ้น หรือกำหนดให้มีการควบคุมดูแลอย่างใกล้ชิด นอกจากนี้อาจกำหนดให้มีการสับเปลี่ยนหน้าที่มีระหว่างบุคลากรภายในหน่วยรับตรวจเป็นครั้งคราว โดยเฉพาะหน้าที่งานที่มีความเสี่ยงต่อการเกิดข้อผิดพลาดหรือความเสียหายแก่หน่วยรับตรวจ เพื่อมิให้บุคคลใดบุคคลหนึ่งกระทำการอันไม่เหมาะสม หรือทุจริตโดยอาศัยระยะเวลาที่ทำงานต่อเนื่องในหน้าที่งานเดิมเป็นเวลานาน

๗. การจัดทำเอกสารหลักฐาน

การดำเนินงาน หรือระบบงานใดที่มีความสำคัญควรมีการจัดทำหลักฐานที่เป็นเอกสาร หรือหนังสือไว้ เพื่อให้บุคคลที่มีหน้าที่เกี่ยวข้องได้ทราบ เข้าใจวิธีปฏิบัติงาน และสามารถค้นคว้าหรืออ้างอิงได้ รวมทั้งสามารถใช้ในการตรวจสอบ สอบทานความถูกต้อง พิจารณาอนุมัติรายงานอย่างรัดกุม ตัวอย่างเช่น ระเบียบ คำสั่ง คู่มือการปฏิบัติงาน ผังทางเดินของระบบงานที่มีความสำคัญต่อการดำเนินงาน

องค์ประกอบ การควบคุมภายใน COSO 2013 ประกอบด้วย ๕ องค์ประกอบ ๑๗ หลักการ

องค์ประกอบที่ ๑ : สภาพแวดล้อมการควบคุม (Control Environment)

หลักการที่ ๑ - องค์กรยึดหลักความซื่อตรงและจริยธรรม

หลักการที่ ๒ - คณะกรรมการแสดงออกถึงความรับผิดชอบต่อการกำกับดูแล

หลักการที่ ๓ - คณะกรรมการและฝ่ายบริหาร มีอำนาจการสั่งการชัดเจน

หลักการที่ ๔ - องค์กร จูงใจ รักษาไว้ และจูงใจพนักงาน

หลักการที่ ๕ - องค์กรผลักดันให้ทุกตำแหน่งรับผิดชอบต่อการควบคุมภายใน

องค์ประกอบที่ ๒ : การประเมินความเสี่ยง (Risk Assessment)

หลักการที่ ๖ - กำหนดเป้าหมายชัดเจน

หลักการที่ ๗ - ระบุและวิเคราะห์ความเสี่ยงอย่างครอบคลุม

หลักการที่ ๘ - พิจารณาโอกาสที่จะเกิดการทุจริต

หลักการที่ ๙ - ระบุและประเมินความเปลี่ยนแปลงที่จะกระทบต่อการควบคุมภายใน

องค์ประกอบที่ ๓ : กิจกรรมการควบคุม (Control Activities)

หลักการที่ ๑๐ - ควบคุมความเสี่ยงให้อยู่ในระดับที่ยอมรับได้

หลักการที่ ๑๑ - พัฒนาระบบเทคโนโลยีที่ใช้ในการควบคุม

หลักการที่ ๑๒ - ควบคุมให้นโยบายสามารถปฏิบัติได้

องค์ประกอบที่ ๔ : สารสนเทศและการสื่อสาร (Information and Communication)

หลักการที่ ๑๓ - องค์กรมีข้อมูลที่เกี่ยวข้องและมีคุณภาพ

หลักการที่ ๑๔ - มีการสื่อสารข้อมูลภายในองค์กร ให้การควบคุมภายในดำเนินต่อไปได้

หลักการที่ ๑๕ - มีการสื่อสารกับหน่วยงานภายนอก ในประเด็นที่อาจกระทบต่อการควบคุม

ภายใน

องค์ประกอบที่ ๕ : กิจกรรมการกำกับติดตามและประเมินผล (Monitoring Activities)

หลักการที่ ๑๖ - ติดตามและประเมินผลการควบคุมภายใน

หลักการที่ ๑๗ - ประเมินและสื่อสารข้อบกพร่องของการควบคุมภายในทันเวลา และเหมาะสม

ทั้งนี้ องค์ประกอบการควบคุมภายในแต่ละองค์ประกอบและหลักการจะต้อง Present & Function (มีอยู่จริง และนำไปปฏิบัติได้) อีกทั้งทำงานอย่างสอดคล้องและสัมพันธ์กัน จึงจะทำให้การควบคุมภายในมีประสิทธิภาพ

องค์ประกอบที่ ๑ : สภาพแวดล้อมการควบคุม (Control Environment)

หลักการที่ ๑ - องค์กรยึดหลักความซื่อตรงและจริยธรรม

๑.๑) แสดงให้เห็นโดยผ่านคำสั่ง การกระทำ พฤติกรรม

๑.๒) จัดทำมาตรฐานของจรรยาบรรณ

๑.๓) ประเมินการยึดมั่นในมาตรฐานของจรรยาบรรณ

๑.๔) รายงานการเบี่ยงเบนในเวลาที่เหมาะสม

หลักการที่ ๒ - คณะกรรมการแสดงออกถึงความรับผิดชอบต่อการกำกับดูแล

๒.๑) กำหนดความรับผิดชอบในการกำกับดูแล

๒.๒) กรรมการบริษัทมีความรู้ความชำนาญที่เกี่ยวข้องกับธุรกิจ

๒.๓) ดำเนินการอย่างเป็นอิสระ จากฝ่ายบริหาร

๒.๔) กำกับดูแลในเรื่องสภาพแวดล้อมของการควบคุม การประเมินความเสี่ยง กิจกรรมการ

ควบคุม ข้อมูลสารสนเทศและการสื่อสาร และการติดตามประเมินผล

หลักการที่ ๓ - คณะกรรมการและฝ่ายบริหาร มีอำนาจการสั่งการชัดเจน

๓.๑) พิจารณาโครงสร้างทั้งหมดของกิจการ

๓.๒) กำหนดสายการรายงาน

๓.๓) กำหนด มอบหมาย และจำกัดขอบเขตของอำนาจหน้าที่และความรับผิดชอบ

หลักการที่ ๔ - องค์กร จูงใจ รักษาไว้ และจูงใจพนักงาน

๔.๑) วางนโยบายและวิธีปฏิบัติเกี่ยวกับการบริหารบุคลากร

๔.๒) ประเมินความสามารถรายบุคคลและระบุส่วนที่ยังขาดอยู่เพื่อปรับปรุงแก้ไข

๔.๓) จูงใจ พัฒนาและรักษาบุคลากร

๔.๔) วางแผนและเตรียมสรรหาผู้สืบทอดตำแหน่ง (Succession)

หลักการที่ ๕ - องค์กรผลักดันให้ทุกตำแหน่งรับผิดชอบต่อการควบคุมภายใน

๕.๑) บังคับให้มีความรับผิดชอบต่อการควบคุมภายในผ่านโครงสร้างองค์กร อำนาจหน้าที่ และความรับผิดชอบ

๕.๒) กำหนดตัวชี้วัดผลการปฏิบัติงาน การสร้างแรงจูงใจและการให้รางวัล

๕.๓) ประเมินตัวชี้วัดผลการปฏิบัติงาน สิ่งจูงใจ และรางวัลอย่างต่อเนื่อง

๕.๔) พิจารณาความกดดันในการทำงานที่มากเกินไป

๕.๕) ประเมินผลการปฏิบัติงาน การให้รางวัล และการลงโทษพนักงานเป็นรายบุคคล

องค์ประกอบที่ ๒ : การประเมินความเสี่ยง (Risk Assessment)

หลักการที่ ๖ - กำหนดเป้าหมายชัดเจน

๖.๑) องค์กรปฏิบัติตามมาตรฐานบัญชีที่รับรองโดยทั่วไป

๖.๒) องค์กรกำหนดสาระสำคัญของรายงานทางการเงิน

๖.๓) รายงานทางการเงินสะท้อนถึงกิจกรรมขององค์กร

๖.๔) คณะกรรมการอนุมัติและสื่อสารนโยบายบริหารความเสี่ยงให้ผู้บริหารและพนักงาน รับทราบ และเป็นส่วนหนึ่งของวัฒนธรรมองค์กร

หลักการที่ ๗ - ระบุและวิเคราะห์ความเสี่ยงอย่างครอบคลุม

๗.๑) ระบุความเสี่ยงทุกประเภท ทั้งระดับ องค์กร ฝ่ายงาน

๗.๒) วิเคราะห์ความเสี่ยงทั้งปัจจัยภายใน/ภายนอก

๗.๓) ให้ผู้บริหารทุกระดับมีส่วนร่วม

๗.๔) ประเมินนัยสำคัญของความเสี่ยงที่ระบุ

๗.๕) กำหนดว่าจะตอบสนองความเสี่ยงอย่างไร

หลักการที่ ๘ - พิจารณาโอกาสที่จะเกิดการทุจริต

๘.๑) ประเมินโอกาสที่จะเกิดการทุจริตประเภทต่างๆ

๘.๒) ทบทวนเป้าหมาย แรงจูงใจและแรงกดดัน

๘.๓) คณะกรรมการตรวจสอบได้พิจารณาและสอบถามผู้บริหารเกี่ยวกับโอกาสเกิดทุจริต และมาตรการป้องกัน

๘.๔) บริษัทได้สื่อสารให้พนักงานปฏิบัติตามนโยบาย

หลักการที่ ๙ - ระบุและประเมินความเปลี่ยนแปลงที่จะกระทบต่อการควบคุมภายใน

๙.๑) ประเมินการเปลี่ยนแปลงสภาพแวดล้อมภายนอก

๙.๒) ประเมินการเปลี่ยนแปลงรูปแบบการทำธุรกิจ

๙.๓) ประเมินการเปลี่ยนแปลงผู้นำองค์กร

องค์ประกอบที่ ๓ : กิจกรรมการควบคุม (Control Activities)

หลักการที่ ๑๐ - ควบคุมความเสี่ยงให้อยู่ในระดับที่ยอมรับได้

๑๐.๑) การควบคุมเหมาะสมกับความเสี่ยง และลักษณะเฉพาะขององค์กร สภาพแวดล้อม ลักษณะของงาน

๑๐.๒) มีมาตรการการควบคุมภายในที่กำหนดเป็นลายลักษณ์อักษร เช่น นโยบาย คู่มือ ระเบียบ

๑๐.๓) กำหนดกิจกรรมควบคุมให้มีความหลากหลายอย่างเหมาะสมการผสมผสานของ กิจกรรมการควบคุมหลายๆ ประเภท

๑๐.๔) กำหนดให้มีการควบคุมทุกระดับขององค์กร

๑๐.๕) มีการแบ่งแยกหน้าที่ ผู้อนุมัติ ผู้บันทึก ผู้ดูแลเก็บรักษา

หลักการที่ ๑๑ - พัฒนาระบบเทคโนโลยีที่ใช้ในการควบคุม

๑๑.๑) กำหนดความเกี่ยวข้องกันของการใช้ IT ในกระบวนการธุรกิจกับการควบคุมทั่วไป
ทางด้าน IT ให้เหมาะสม

๑๑.๒) กำหนดกิจกรรมการควบคุมด้านโครงสร้างพื้นฐานให้เหมาะสม

๑๑.๓) กำหนดกิจกรรมการควบคุมด้านความปลอดภัยให้เหมาะสม

๑๑.๔) กำหนดกิจกรรมการควบคุมด้านการจัดหา การพัฒนา และดูแลรักษาระบบ

หลักการที่ ๑๒ - ควบคุมให้นโยบายสามารถปฏิบัติได้

๑๒.๑) มีนโยบายที่รัดกุมเพื่อติดตามการทำธุรกรรมของผู้ถือหุ้นรายใหญ่ กรรมการ ผู้บริหาร

๑๒.๒) มีนโยบายเพื่อให้การอนุมัติการทำธุรกรรมกระทำโดยผู้ที่ไม่มีส่วนได้เสีย

๑๒.๓) มีนโยบายเพื่อให้การอนุมัติธุรกรรมคำนึงถึงประโยชน์สูงสุดของบริษัท เสมือนเป็น
รายการที่ทำกับบุคคลภายนอก (at arms' length basis)

๑๒.๔) มีกระบวนการติดตามดูแลการดำเนินงานของบริษัทย่อย บริษัทร่วม

๑๒.๕) กำหนดหน้าที่และความรับผิดชอบในการนำนโยบายไปปฏิบัติ

๑๒.๖) นโยบายและกระบวนการปฏิบัติได้รับการนำไปใช้ในเวลาที่เหมาะสม

๑๒.๗) ทบทวนนโยบายและกระบวนการทำงานให้เหมาะสมอยู่เสมอ

องค์ประกอบที่ ๔: สารสนเทศและการสื่อสาร (Information and Communication)

หลักการที่ ๑๓ - องค์กรมีข้อมูลที่เกี่ยวข้องและมีคุณภาพ

๑๓.๑) ระบุสารสนเทศที่ต้องการใช้ในการดำเนินงาน

๑๓.๒) พิจารณา ต้นทุน ประโยชน์ รวมทั้งปริมาณและความถูกต้องของข้อมูล

๑๓.๓) ดำเนินการเพื่อให้กรรมการมีข้อมูลที่เพียงพอในการตัดสินใจ

๑๓.๔) ดำเนินการเพื่อให้กรรมการได้รับหนังสือเชิญประชุมและเอกสารล่วงหน้าก่อนการ
ประชุมตามที่กฎหมายกำหนด

๑๓.๕) ดำเนินการเพื่อให้รายงานการประชุมมีรายละเอียดสามารถสอบย้อนได้

๑๓.๖) องค์กรมีการดำเนินการดังนี้ เก็บเอกสารเป็นระบบ แก้ไขข้อบกพร่องการควบคุม ตาม
ความเห็นผู้สอบ

หลักการที่ ๑๔ - มีการสื่อสารข้อมูลภายในองค์กร ให้การควบคุมภายในดำเนินต่อไปได้

๑๔.๑) มีกระบวนการสื่อสารข้อมูลอย่างมีประสิทธิภาพ มีช่องทางที่เหมาะสม

๑๔.๒) มีการรายงานข้อมูลที่สำคัญถึงกรรมการอย่างสม่ำเสมอ

๑๔.๓) จัดให้มีช่องทางสื่อสารกลับเพื่อแจ้งเบาะแสเกี่ยวกับการทุจริต

หลักการที่ ๑๕ - มีการสื่อสารกับหน่วยงานภายนอก ในประเด็นที่อาจกระทบต่อการควบคุม

ภายใน

๑๕.๑) สื่อสารกับผู้มีส่วนได้เสียภายนอกอย่างมีประสิทธิภาพ มีช่องทางที่เหมาะสม

๑๕.๒) มีช่องทางสื่อสารกลับ สำหรับผู้มีส่วนได้เสียภายนอก แจ้งเบาะแสการทุจริต

องค์ประกอบที่ ๕: กิจกรรมการกำกับติดตามและประเมินผล (Monitoring Activities)

หลักการที่ ๑๖ - ติดตามและประเมินผลการควบคุมภายใน

๑๖.๑) จัดให้มีการติดตามการปฏิบัติตามจริยธรรมธุรกิจและข้อกำหนด ในลักษณะที่อาจ
ก่อให้เกิดความขัดแย้งทางผลประโยชน์

๑๖.๒) จัดให้มีการตรวจสอบการปฏิบัติตามระบบการควบคุมภายในที่วางไว้ โดยการประเมินตนเอง และ/หรือการประเมินโดยผู้ตรวจสอบภายใน

๑๖.๓) ความถี่การติดตามและประเมินผล มีความเหมาะสมกับการเปลี่ยนแปลงขององค์การ

๑๖.๔) ติดตามและประเมินผลการควบคุมภายใน โดยผู้มีความรู้ความสามารถ

๑๖.๕) กำหนดแนวทางการรายงานผลการตรวจสอบภายใน ขึ้นตรงต่อคณะกรรมการตรวจสอบ

๑๖.๖) ส่งเสริมให้ผู้ตรวจสอบภายในปฏิบัติหน้าที่ตามมาตรฐานสากล การปฏิบัติงานวิชาชีพ การตรวจสอบภายใน

หลักการที่ ๑๗ - ประเมินและสื่อสารข้อบกพร่องของการควบคุมภายในทันเวลา และเหมาะสม

๑๗.๑) ประเมินผลและสื่อสารข้อบกพร่องของการควบคุมภายใน และดำเนินการแก้ไขอย่างทันท่วงที

๑๗.๒) รายงานต่อคณะกรรมการบริษัททันทีที่เกิดเหตุการณ์ทุจริตร้ายแรง การฝ่าฝืนกฎหมาย หรือการกระทำที่ผิดปกติ ซึ่งกระทบชื่อเสียงและฐานะการเงินบริษัทอย่างมีนัยสำคัญ

๑๗.๓) รายงานข้อบกพร่องที่เป็นสาระสำคัญ พร้อมแนวทางแก้ไข ต่อคณะกรรมการบริษัท/คณะกรรมการตรวจสอบในเวลาอันควร