201.01 วัตถุประสงค์การควบคุมภายใน

ธนาคารดำเนินการควบคุมภายในตามหลักเกณฑ์กระทรวงการคลังว่าด้วยมาตรฐานและหลักเกณฑ์ปฏิบัติการควบคุมภายในสำหรับหน่วยงานของรัฐ พ.ศ.2561 และแนวทางที่ผู้กำกับดูแลกำหนดตามวัตถุประสงค์ 3 ด้าน เพื่อสร้างความมั่นใจอย่างสมเหตุสมผลว่าการดำเนินงานจนบรรลุผลสำเร็จประกอบด้วย

1) การดำเนินงาน (Operation Objectives) เกี่ยวข้องกับประสิทธิภาพและประสิทธิผลในการดำเนินงานของกิจการ รวมถึงเป้าหมายการบรรลุปฏิบัติการด้านการดำเนินงาน ด้านการเงิน และใช้ทรัพยากร การดูแลทรัพย์สิน การป้องกันหรือลดความผิดพลาด ตลอดจนความเสียหาย การรั่วไหล การสิ้นเปลือง หรือการทุจริตในองค์กร

2) การรายงาน (Reporting Objectives) เกี่ยวข้องกับรายงานทางการเงินและไม่ใช่การเงินที่ใช้ภายในและภายนอกองค์กร ซึ่งอาจจะรวมการายงานที่เชื่อถือได้ ความทันเวลา โปร่งใส หรือข้อกำหนดอื่น ๆ ที่กำหนดโดยหน่วยงานที่กำกับดูแล หน่วยงานกำหนดมาตรฐาน หรือนโยบายที่กิจการกำหนดขึ้น

3) การปฏิบัติตามกฎหมาย (Commpliance Objectives) ระเบียบ ข้อบังคับ เกี่ยวกับการปฏิบัติให้ถูกต้องตามกฎหมายและระเบียบ ข้อบังคับที่เกี่ยวข้องกับการดำเนินงานขององค์กร และหน่วยงานที่กำกับดูแล

101.02 คำนิยาม

ผู้กำกับดูแล หมายถึง หน่วยงานที่ทำหน้าที่กำกับดูแลการปฏิบัติงาน ธ.ก.ส. เช่น ธนาคารแห่งประเทศไทย (ธปท.) เป็นต้น

คณะกรรมการ หมายถึง คณะกรรมการบริหารความเสี่ยงและควบคุมภายในระดับส่วนงาน

เลขานุการ หมายถึง ผู้ที่ได้รับมอบหมายให้ทำหน้าที่เป็นเลขานุการของคณะกรรมการบริหารความเสี่ยงและควบคุมภายในระดับส่วนงาน

การควบคุมภายใน (Internal Control) หมายถึง กระบวนการปฏิบัติงานที่ผู้กำกับดูแล คณะกรรมการธนาคาร ฝ่ายจัดการ ผู้บริหาร และพนักงาน จัดให้มีขึ้นเพื่อสร้างความมั่นใจอย่างสมเหตุสมผลว่าการดำเนินงานจะบรรลุวัตถุประสงค์ ด้านการดำเนินงาน ด้านการรายงาน และด้านการปฏิบัติตามกฎเกณฑ์ระเบียบ และข้อบังคับ

การประเมินความเสี่ยงและการควบคุมด้วยตนเอง (Risk and Control Self - Assessment : RCSA) หมายถึง กระบวนการที่พนักงานในส่วนงาน ร่วมกันวิเคราะห์ความเสี่ยงที่มีผลกระทบต่อการดำเนินงานของพนักงานทุกระดับ ดำเนินการประเมินความเสี่ยงที่มีอยู่ด้วยตนเอง และกำหนดมาตรการควบคุมเพิ่มเติมเพื่อลดระดับ/จัดการความเสี่ยงด้านปฏิบัติการ สามารถลดข้อผิดพลาดในการปฏิบัติงานของพนักงาน

แผนการประเมินความเสี่ยงและการควบคุมด้วยตนเอง (RCSA) หมายถึง แผนการประเมินความเสี่ยงและการควบคุมด้วยตนเอง ที่มาจากกระบวนการหรือขั้นตอนปฏิบัติงานของส่วนงานที่ยังไม่มีการควบคุมที่ดี อาจทำให้การปฏิบัติของส่วนงานไม่สำเร็จตามเป้าหมายต้องมีการจัดทำแผน RCSA เพื่อกำหนดมาตรการควบคุมเพิ่มเติม

ระบบประเมินความเสี่ยงและการควบคุมตนเอง (Risk and Control Self-Assessment System: RCSA) หมายถึง ระบบสารสนเทศเพื่อการบริหารเพื่อจัดทำการประเมินความเสี่ยงและการควบคุมด้วยตนเอง (Risk and Control Self-Assessment: RCSA)

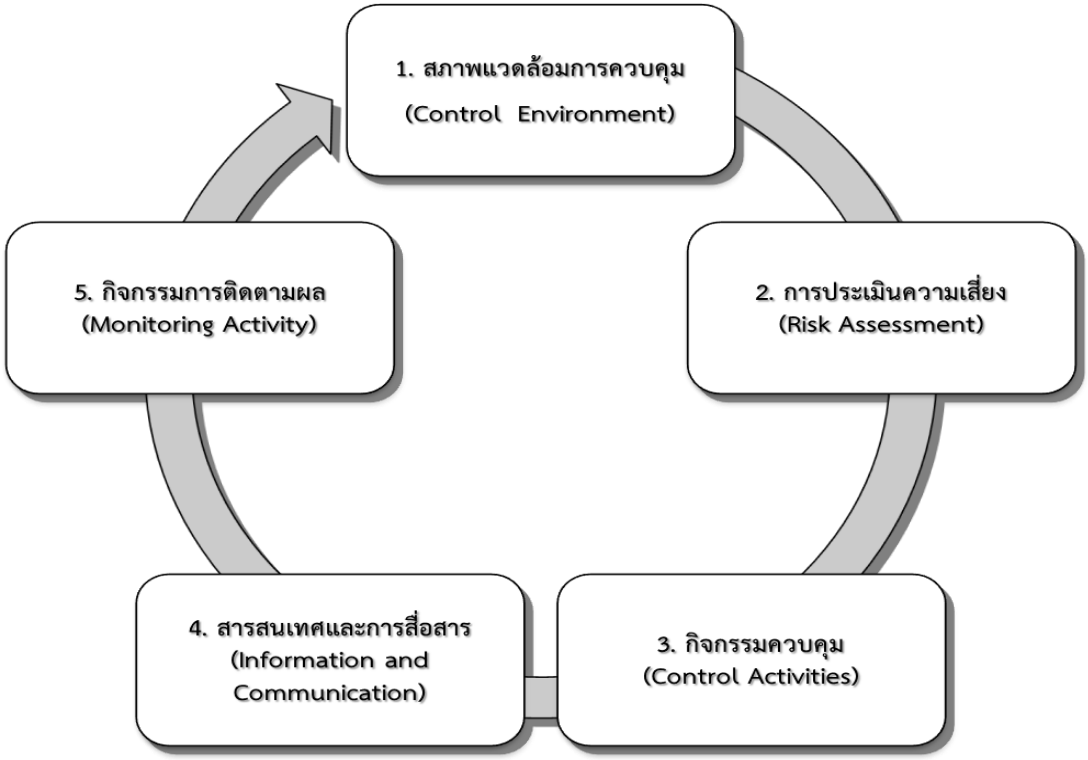
แบบประเมินผลการควบคุมภายในระดับส่วนงาน (ปค.ส่วนงาน) หมายถึง แบบประเมินผลการควบคุมภายในระดับส่วนงาน ตามมาตรฐาน 5 องค์ประกอบ ได้แก่ สภาพแวดล้อมการควบคุม ประเมินความเสี่ยง กิจกรรมการควบคุม สารสนเทศและการสื่อสาร กิจกรรมการกำกับติดตามและประเมินผล

แบบกระดาษทำการ หมายถึง แบบร่างแผนการประเมินการควบคุมด้วยตนเอง เพื่อประกอบการพิจารณาจากคณะกรรมการบริหารความเสี่ยงและควบคุมภายในระดับส่วนงาน ก่อนบันทึกลงระบบประเมินความเสี่ยงและการควบคุมด้วยตนเอง

ระดับความเสี่ยงเกินกว่าระดับที่ยอมรับได้ หมายถึง ค่าความเสี่ยงตั้งแต่ระดับ 5 - 25 โดย ค่า 5 - 9 เท่ากับ ระดับปานกลาง ค่า 10 - 16 เท่ากับระดับค่อนข้างสูง และค่า 17 - 25 เท่ากับระดับสูง โดยระดับที่ยอมรับได้ (Risk Appetite) ธนาคารกำหนดไว้ที่ระดับ 2 และระดับความเบี่ยงเบนจากระดับความเสี่ยงที่ยอมรับได้ (Risk Tolerance) ธนาคารกำหนดไว้ที่ระดับ 4

201.02 องค์ประกอบการควบคุมภายใน

ธนาคารกำหนดในส่วนงานทบทวนองค์ระกอบการควบคุมภายในเป็นประจำทุกปี ตามมาตรฐานสากลของ The Committee of Sponsoring Organizations of the Treadway Commission: COSO 2013 ประกอบด้วย 5 องค์ประกอบ 17 หลักการ



1) สภาพแวดล้อมการควบคุม (Control Environment) กระบวนการและโครงสร้างที่ใช้เป็นพื้นฐานของการนำการควบคุมภายในไปปฏิบัติทั่วทั้งองค์กร คณะกรรมการธนาคารและผู้บริหารระดับสูงเป็นแบบอย่างในการให้ความสำคัญของการควบคุมภายใน รวมทั้งกำหนดมาตรฐานที่พึงปฏิบัติที่องค์กรคาดหวัง ผู้บริหารเป็นผู้เน้นย้ำความคาดหวังนี้กับบุคลากรในระดับต่าง ๆ ส่งเสริมให้บุคลากรตระหนักถึงความจำเป็น ความซื่อสัตย์ (Integrity) และจริยธรรม ความรู้ ทักษะ และความสามารถ (Competence) ประกอบด้วยหลักการ ดังนี้

หลักการที่ 1 แสดงให้เห็นถึงความยึดมั่นในคุณค่าของความซื่อตรงและจริยธรรม

1.1 แสดงให้เห็นผ่าน คำสั่ง การกระทำ พฤติกรรม

1.2 จัดทำมาตรฐานของจรรยาบรรณ

1.3 การปฏิบัติตามมาตรฐาน จรรยาบรรณ

1.4 การปรับปรุงให้เป็นไปตามมาตรฐาน

หลักการที่ 2 คณะกรรมการแสดงให้เห็นถึงความเป็นอิสระจากผู้บริหารและทำหน้าที่สอดส่องดูแลการพัฒนาและการดำเนินการด้านการควบคุมภายใน

2.1 กำหนดความรับผิดชอบในการสอดส่องดูแล

2.2 กำหนด รักษา ประเมินทักษะและความเชี่ยวชาญที่จำเป็นของคณะกรรมการ

2.3 คณะกรรมการเป็นอิสระจากผู้บริหาร

2.4 คณะกรรมการรับผิดชอบในการสอดส่องดูแลการออกแบบ การนำไปใช้ และการดำเนินงานของการควบคุมภายในของผู้บริหาร

หลักการที่ 3 ผู้บริหารจัดให้มีโครงสร้าง สายการรายงาน รวมทั้งการกำหนดอำนาจหน้าที่และความรับผิดชอบที่เหมาะสมเพื่อให้องค์กรบรรลุวัตถุประสงค์ ภายใต้การสอดส่องดูแลของคณะกรรมการ

3.1 กำหนดโครงสร้างองค์กร เพื่อสนับสนุนการบรรลุวัตถุประสงค์

3.2 การรายงานตามสายบังคับบัญชา

3.3 กำหนด มอบหมาย ขอบเขตอำนาจสั่งการ และความรับผิดชอบ

หลักการที่ 4 องค์กรจะแสดงให้เห็นถึงความมุ่งมั่นในการจูงใจ พัฒนาและรักษาบุคลากรที่มีความรู้ ความสามารถที่สอดคล้องกับวัตถุประสงค์ขององค์กร

4.1 กำหนดนโยบายการปฏิบัติ

4.2 ประเมินความรู้ความสามารถและจัดการข้อบกพร่อง

4.3 จูงใจและพัฒนาบุคลากร

4.4 วางแผนและเตรียมหาผู้สืบทอดตำแหน่ง

หลักการที่ 5 องค์กรกำหนดให้บุคลากรมีหน้าที่และความรับผิดชอบต่อผลการปฏิบัติงานตามหน้าที่การควบคุมภายในเพื่อให้องค์กรบรรลุวัตถุประสงค์

5.1 กำหนดให้บุคลากรต้องรับผิดชอบต่อผลการปฏิบัติงานตามหน้าที่โดยผ่านโครงสร้าง อำนาจหน้าที่และความรับผิดชอบ

5.2 สร้างมาตรการวัดผลการปฏิบัติงาน

5.3 ประเมินมาตรการวัดผลการปฏิบัติงาน สิ่งจูงใจ และการให้รางวัล

5.4 ประเมินผลการปฏิบัติงาน การให้รางวัล การลงโทษ

2) การประเมินความเสี่ยง (Risk Assessment) ความเป็นไปได้ที่เหตุการณ์ใดเหตุการณ์หนึ่งอาจเกิดขึ้นและเป็นอุปสรรคต่อการบรรลุวัตถุประสงค์ เป็นกระบวนการที่สามารถเปลี่ยนแปลงและเกิดซ้ำอย่างต่อเนื่อง เพื่อระบุและประเมินความเสี่ยงที่อาจกระทบต่อวัตถุประสงค์ของกิจการ คำนึงถึงผลกระทบของการเปลี่ยนแปลงสภาพแวดล้อมภายนอกและภายใน รูปแบบการดำเนินงานที่อาจส่งผลให้การควบคุมภายในไม่มีประสิทธิผล ต้องมีการกำหนดวัตถุประสงค์/เป้าหมายที่ชัดเจน วัดผลได้ตามหลัก SMART ได้แก่

Specific : กำหนดสิ่งที่จะทำให้ชัดเจน มีลักษณะเฉพาะเจาะจง และเชื่อมโยงกับกลยุทธ์

Measurable : กำหนดตัววัดความสำเร็จได้อย่างเป็นรูปธรรมในเชิงปริมาณและ/หรือเชิงคุณภาพ

- ตัวชี้วัดเชิงปริมาณ เช่น ปริมาณการจ่ายสินเชื่อ ปริมาณการรับชำระหนี้ อัตรา NPL/Loan ค่าใช้จ่ายดำเนินงานต่อรายได้สุทธิ เป็นต้น

- ตัวชี้วัดเชิงคุณภาพ เช่น การวัดระดับความพึงพอใจของลูกค้าและผู้มีส่วนได้ส่วนเสีย เป็นต้น

Achievable : กำหนดเป้าหมายที่ท้าทายกับความสามารถ โดยไม่ต่ำหรือสูงเกินไป

Relevant : มีความเกี่ยวข้องสัมพันธ์ และเป็นไปในทิศทางเดียวกับวิสัยทัศน์ขององค์กร

Timely : กำหนดระยะเวลาที่ต้องการชัดเจนในการดำเนินงาน

การระบุปัจจัยความเสี่ยงมีผลต่อการกำหนดวัตถุประสงค์ ต้องประเมินความเสี่ยง ข้อบ่งชี้ความเสี่ยงทุกประเภทโดยให้ครอบคลุมความเสี่ยงจากการทุจริตด้วย หลักในการประเมินความเสี่ยงประกอบด้วย

<u>หลักการที่ 6</u> ระบุวัตถุประสงค์ขององค์กรไว้อย่างชัดเจน เพื่อให้สามารถระบุความเสี่ยงขององค์การ/ส่วนงาน รวมทั้งกำหนดระดับความเสี่ยงที่ยอมรับได้ (Risk Appetite) และ ค่าเบี่ยงเบนของระดับความเสี่ยงที่ยอมรับได้ (Risk Tolerance)

6.1 ด้านการดำเนินงาน

- ผลการดำเนินงาน สภาพแวดล้อม สะท้อนถึงทางเลือกของผู้บริหารเกี่ยวกับโครงสร้าง
- ผู้บริหารพิจารณาระดับความเบี่ยงเบนที่ยอมรับได้
- องค์กรสะท้อนระดับผลการปฏิบัติงานด้านการเงินและการดำเนินงาน
- เกณฑ์จัดสรรทรัพยากร

6.2 ด้านการรายงานทางการเงินต่อบุคคลภายนอก

- ปฏิบัติตามมาตรฐานรายงานทางการเงิน
- สาระสำคัญในการนำเสนองบการเงิน
- การรายงานต่อบุคคลภายนอก (รายการและเหตุการณ์ที่เกิดขึ้น) เพื่อแสดงถึงลักษณะเชิงคุณภาพ

6.3 ด้านการรายงานที่ไม่ใช่ทางการเงินต่อบุคคลภายนอก

- ปฏิบัติตามมาตรฐานและกรอบแนวคิดที่กำหนดจากภายนอก
- การรายงานต่อบุคคลภายนอก (รายการและเหตุการณ์ที่เกิดขึ้น) ภายใต้ช่วงขอบเขตที่ยอมรับได้

6.4 ด้านการรายงานภายใน

- รายงานมีความถูกต้องแม่นยำที่จำเป็นและเหมาะสมกับความต้องการของผู้ใช้
- การรายงานภายใน สะท้อนรายการและเหตุการณ์ที่เกิดขึ้นภายใต้ช่วงขอบเขตที่ยอมรับได้

6.5 ด้านการปฏิบัติตามกฎระเบียบข้อบังคับ

- มีกฎหมายและข้อบังคับกำหนดมาตรฐานที่พึงปฏิบัติ
- ผู้บริหารพิจารณาความเบี่ยงเบนที่ยอมรับได้ด้านการปฏิบัติตามกฎระเบียบข้อบังคับ

หลักการที่ 7 องค์กรระบุความเสี่ยงในการบรรลุวัตถุประสงค์อย่างครอบคลุมทั่วทั้งองค์กร และวิเคราะห์ความเสี่ยงเพื่อเป็นเกณฑ์ในการพิจารณาวิธีการจัดการความเสี่ยง พิจารณาถึงเหตุการณ์สำคัญที่มีอิทธิพลทั้งภายในและภายนอก ทั้งเหตุการณ์ที่เคยเกิดขึ้นมาในอดีตและคาดการณ์ในอนาคตที่มีความเป็นไปได้ว่าจะเกิดขึ้นแล้วส่งผลกระทบต่อการบรรลุวัตถุประสงค์ขององค์กร

7.1 ระบุและประเมินความเสี่ยง ทุกส่วนงาน

7.2 พิจารณาปัจจัยภายในและภายนอก และผลกระทบต่อวัตถุประสงค์

7.3 วางกลไกในการประเมินความเสี่ยง

7.4 มีการวิเคราะห์ความเสี่ยง

7.5 มีการประเมินความสี่ยง และมีการจัดการความเสี่ยง

หลักการที่ 8 องค์กรประเมินความเสี่ยงทางทุจริต โดยประเมินสองมิติ คือ ระดับโอกาสที่จะเกิด (likelihood) และ ระดับผลกระทบ (Impact) เพื่อให้ทราบระดับความเสี่ยงก่อนการจัดการ โดยหามาตรการจัดการความเสี่ยง ให้ระดับความเสี่ยงหลังการจัดการอยู่ในระดับที่ยอมรับได้ หลักการประเมินความเสี่ยงที่สำคัญ

8.1 การจัดทำนโยบายการบริหารความเสี่ยงด้านการทุจริต

8.2 การประเมินการทุจริตครอบคลุมถึงการจัดทำรายงานที่ทุจริต ความเป็นไปได้ที่สินทรัพย์สูญหาย และคอรัปชั่น

8.3 การประเมินแรงจูงใจและความกดดันที่ส่งผลต่อการทุจริต

8.4 การประเมินโอกาส (การจัดหา ใช้งาน การจำหน่ายสินทรัพย์ การแก้ไข) ที่ไม่ผ่านการอนุมัติ

8.5 การออกแบบและสร้างกิจกรรมควบคุม

8.6 การดำเนินการสอบสวน

8.7 ระบบการติดตามและประเมินผลการบริหารความเสี่ยงด้านการทุจริตทั่วทั้งองค์กร

หลักการที่ 9 องค์กรระบุและประเมินการเปลี่ยนแปลงที่อาจมีผลกระทบอย่างมีนัยสำคัญต่อระบบการควบคุมภายใน

9.1 กระบวนการระบุความเสี่ยงครอบคลุมถึงการเปลี่ยนแปลงสภาพแวดล้อมด้านข้อกำหนดทางกฎหมาย ด้านเศรษฐกิจ และกายภาพที่กิจการดำเนินงานอยู่

9.2 ประเมินผลกระทบที่เกิดจากสายธุรกิจใหม่ และเทคโนโลยีใหม่

9.3 การเปลี่ยนแปลงของผู้บริหารกับทัศนคติต่อระบบการควบคุมภายใน

3) กิจกรรมการควบคุม (Control Activities) เป็นมาตรการ ขั้นตอนการปฏิบัติงานการทำงานตามแผนการดำเนินงาน รวมถึงการควบคุมด้านเทคโนโลยี หลักการของกิจกรรมการควบคุม ดังนี้

หลักการที่ 10 องค์กรเลือกและพัฒนากิจกรรมการควบคุมที่ลดความเสี่ยงในการบรรลุวัตถุประสงค์ให้อยู่ในระดับที่ยอมรับได้

10.1 ผู้บริหารเลือกและพัฒนากิจกรรมควบคุม ให้สอดคล้องกับองค์กร

10.2 กิจกรรมควบคุม ควบคุมโดยคน วิธีปฏิบัติ และระบบอัตโนมัติ ในเชิงป้องกันและตรวจจับ

10.3 กิจกรรมควบคุมได้ประยุกต์ใช้ในทุกระดับ

10.4 มีการแบ่งแยกหน้าที่ ที่เหมาะสม

หลักการที่ 11 องค์กรเลือกและพัฒนากิจกรรมการควบคุมทั่วไปด้านเทคโนโลยีเพื่อสนับสนุนการบรรลุวัตถุประสงค์

11.1 เลือกและพัฒนากิจกรรมควบคุมให้ครอบคลุมโครงสร้างพื้นฐานทางเทคโนโลยี

11.2 ออกแบบการจำกัดสิทธิการเข้าถึงเทคโนโลยี ตามระดับความรับผิดชอบเพื่อปกป้องภัยคุกคามภายนอก

11.3 มีกิจกรรมควบคุมสำหรับกระบวนการจัดหา พัฒนา บำรุงรักษาเทคโนโลยี และโครงสร้างพื้นฐานเทคโนโลยี

หลักการที่ 12 องค์กรจัดให้มีกิจกรรมควบคุมผ่านทางนโยบายซึ่งได้กำหนดสิ่งที่คาดหวังและวิธีการปฏิบัติเพื่อนำนโยบายไปสู่การปฏิบัติ

12.1 กิจกรรมควบคุมอยู่ในกระบวนการ กิจกรรมปฏิบัติงานประจำวัน ผ่านนโยบายที่กำหนด

12.2 ผู้บริหารกำหนดความรับผิดชอบและความรับผิดชอบต่อการปฏิบัติงานให้ผู้บริหารของส่วนงาน ในกิจกรรมควบคุมที่มีความเสี่ยงแฝงอยู่

12.3 กิจกรรมควบคุมมีกำหนดระยะเวลาที่ชัดเจน

12.4 ติดตาม/แก้ไข ประเด็นจากกิจกรรมควบคุม

12.5 สอบทานกิจกรรมควบคุมเป็นประจำอย่างต่อเนื่อง

แบ่งกิจกรรมของการควบคุมได้ 4 ประเภท คือ

1 การควบคุมแบบป้องกัน (Preventive Control) เป็นวิธีการควบคุมเพื่อป้องกันหรือลดระดับโอกาสที่จะเกิดความเสี่ยง เช่น การให้ความเห็นชอบ การใช้รหัสผ่านแบบเฉพาะ การแบ่งแยกหน้าที่ การกำหนดระดับอนุมัติ เป็นต้น

2 การควบคุมแบบค้นพบ (Detective Control) เป็นวิธีการควบคุมเพื่อค้นหาข้อผิดพลาดที่เกิดขึ้นให้เกิดผลกระทบน้อยที่สุด เช่น การสอบทานรายงาน การยืนยันยอด การกระทบยอด การตรวจนับสินค้า การควบคุมยอดรวม เป็นต้น

3 การควบคุมแบบส่งเสริม (Directive Control) เป็นวิธีการควบคุมที่ส่งเสริมหรือกระตุ้นให้เกิดความสำเร็จในวัตถุประสงค์ที่ต้องการ เช่น การกำหนดนโยบาย และวิธีปฏิบัติงาน แผนการฝึกอบรม แผนการสร้างแรงจูงใจ เป็นต้น

4 การควบคุมแบบแก้ไข (Corrective Control) เป็นวิธีการควบคุมเพื่อแก้ไขข้อผิดพลาด อาจเป็นการสร้างวิธีการควบคุมใหม่ เช่น การปรับกระบวนการปฏิบัติงาน การปรับปรุงโครงสร้างส่วนงาน เป็นต้น

4) สารสนเทศและการสื่อสาร (Information and Communication) เป็นมีการสื่อสารเกี่ยวกับข้อมูลสารสนเทศ ที่เหมาะสม ให้ผู้บริหารและพนักงานในองค์กรทราบ เพื่อจัดการและตอบสนองต่อความเสี่ยงได้ตามเป้าหมาย ทันเวลา และสนับสนุนการบรรลุวัตถุประสงค์องค์กร หลักการสารสนเทศและการสื่อสาร ดังนี้

หลักการที่ 13 องค์กรได้รับหรือสร้างและใช้สารสนเทศที่เกี่ยวข้องและมีคุณภาพเพื่อสนับสนุนให้การควบคุมภายในทำหน้าที่ได้

13.1 มีกระบวนการเพื่อระบุสารสนเทศที่จำเป็นและที่คาดหวังเพื่อสนับสนุนองค์กร

13.2 มีระบบสารสนเทศที่รวบรวมข้อมูลจากแหล่งภายในและภายนอก

13.3 มีระบบที่ประมวลและแปลงข้อมูลที่เกี่ยวข้องให้เป็นสารสนเทศ

13.4 ความปลอดภัยของระบบสารสนเทศ

13.5 พิจารณาความเหมาะสมของต้นทุนและประโยชน์ที่ได้รับ

หลักการที่ 14 องค์กรมีการสื่อสารภายในเกี่ยวกับสารสนเทศ รวมถึงวัตถุประสงค์และความรับผิดชอบต่อการควบคุมภายในที่จำเป็นเพื่อสนับสนุนให้การควบคุมภายในทำหน้าที่ได้

14.1 มีกระบวนการเพื่อระบุสารสนเทศที่จำเป็นและที่คาดหวังเพื่อสนับสนุนองค์กร

14.2 มีระบบสารสนเทศที่รวบรวมข้อมูลจากแหล่งภายในและภายนอก

14.3 มีระบบที่ประมวลและแปลงข้อมูลที่เกี่ยวข้องให้เป็นสารสนเทศ

14.4 ความปลอดภัยของระบบสารสนเทศ

14.5 พิจารณาความเหมาะสมของต้นทุนและประโยชน์ที่ได้รับ

หลักการที่ 15 องค์กรมีการสื่อสารกับบุคคลภายนอกเกี่ยวกับประเด็นที่มีผลกระทบต่อการทำหน้าที่ของการควบคุมภายใน

15.1 มีกระบวนการสื่อสารสารสนเทศที่เกี่ยวข้องให้ทันเวลากับบุคคลภายนอก

15.2 มีช่องทางการสื่อสารแบบเปิด เพื่อรับข้อมูลจากภายนอก

15.3 มีการสื่อสารสารสนเทศที่เกี่ยวข้องไปยังผู้บริหาร

15.4 มีช่องทางการสื่อสารที่แยกต่างหาก เช่น ช่องทางร้องเรียน แจ้งเบาะแส เป็นต้น

5) กิจกรรมการกำกับติดตามและประเมินผล (Monitoring Activities) การติดตามประเมินผลทำได้โดยการติดตามผลระหว่างการปฏิบัติงาน (Ongoing Monitoring) การประเมินผลเป็นรายครั้ง (Separate Evaluation) หรือทั้งสองอย่าง การติดตามประเมินผลสามารถออกแบบการติดตามให้เหมาะสมได้ตามประเภทของกิจกรรมความเสี่ยง เพื่อรายงานให้ผู้บริหารและคณะกรรมการบริหารตามความเหมาะสม
หลักกิจกรรมการกำกับติดตามและประเมินผล ได้แก่

หลักการที่ 16 องค์กรเลือก พัฒนา และดำเนินการประเมินผลอย่างต่อเนื่อง และ/หรือประเมินผลแยกต่างหาก เพื่อให้มั่นใจว่าองค์ประกอบของการควบคุมภายในมีปรากฏและทำหน้าที่อยู่

16.1 พิจารณาเลือกวิธีการประเมินผลให้เหมาะสมกับการปฏิบัติงาน

16.2 มีการออกแบบการนำผลการประเมินเพื่อนำไปใช้

16.3 ผู้ที่ประเมินผลมีความรู้อย่างเพียงพอ

16.4 การประเมินผลอย่างต่อเนื่องอยู่ในกระบวนการปฏิบัติงานตามปกติ และปรับไปตามสถานการณ์ที่มีการเปลี่ยนแปลง

16.5 มีการประเมินผลแยกต่างหากเป็นครั้งคราว เพื่อให้ได้ข้อมูลย้อนกลับที่เป็นจริง

หลักการที่ 17 องค์กรประเมินผลและสื่อสารข้อบกพร่องของการควบคุมภายในอย่างทันเวลา ต่อบุคคลที่รับผิดชอบในการดำเนินการแก้ไข รวมถึงผู้บริหารระดับสูงและคณะกรรมการตามความเหมาะสม

17.1 ผู้บริหารประเมินผลลัพธ์ที่ได้จากการประเมินผลอย่างต่อเนื่อง และการประเมินผลแยกต่างหาก

17.2 ข้อบกพร่อง ได้ถูกสื่อสารไปยังผู้ที่เกี่ยวข้องให้ดำเนินการแก้ไข

17.3 มีการติดตามการแก้ไขอย่างทันเวลา

301.06 ตารางการวิเคราะห์และอธิบายความหมายระดับความเสี่ยง

ตารางวิเคราะห์ระดับความเสี่ยง (Risk Matrix) (ISO31000)

		โอกาสที่จะเกิด (Likelihood Rating)				
		1 ต่ำ	2 ค่อนข้างต่ำ	3 ปานกลาง	4 ค่อนข้างสูง	5 สูง
ผลกระทบ (Impact Rating)	5 – สูง	M5	NH10	NH15	H20	H25
	4 – ค่อนข้างสูง	NL4	M8	NH12	NH16	H20
	3 – ปานกลาง	NL3	M6	M9	NH12	NH15
	2 – ค่อนข้างต่ำ	L2	NL4	M6	M8	NH10
	1 – ต่ำ	L1	L2	NL3	NL4	M5

ตารางความหมายระดับความเสี่ยง

เกณฑ์ระดับความเสี่ยง	ความหมาย
สูง (20 - 25) (H : High)	ความเสี่ยงที่มีความสำคัญสูงมาก จำเป็นต้องได้รับการจัดการทันที
ค่อนข้างสูง (10 - 16) (NH : Nearly High)	ความเสี่ยงที่มีความสำคัญสูง จะต้องได้รับการจัดการในลำดับถัดมา
ปานกลาง (5 - 9) (M : Medium)	ความเสี่ยงที่มีความสำคัญ และต้องติดตามการปฏิบัติตามมาตรการจัดการความเสี่ยงที่ดำเนินการอยู่ในปัจจุบันอย่างเคร่งครัด
ค่อนข้างต่ำ (3 - 4) (NL : Nearly Low)	ความเสี่ยงที่มีความสำคัญน้อย อยู่ในระดับที่ผู้บริหารยอมรับได้ แต่ต้องติดตามอย่างสม่ำเสมอ
ต่ำ (1 - 2) (L : Low)	ความเสี่ยงที่มีความสำคัญน้อย อยู่ในระดับที่ผู้บริหารยอมรับได้

แหล่งอ้างอิง : ISO 31000:2009 Guide Line และ Project Management Institution (PMI)