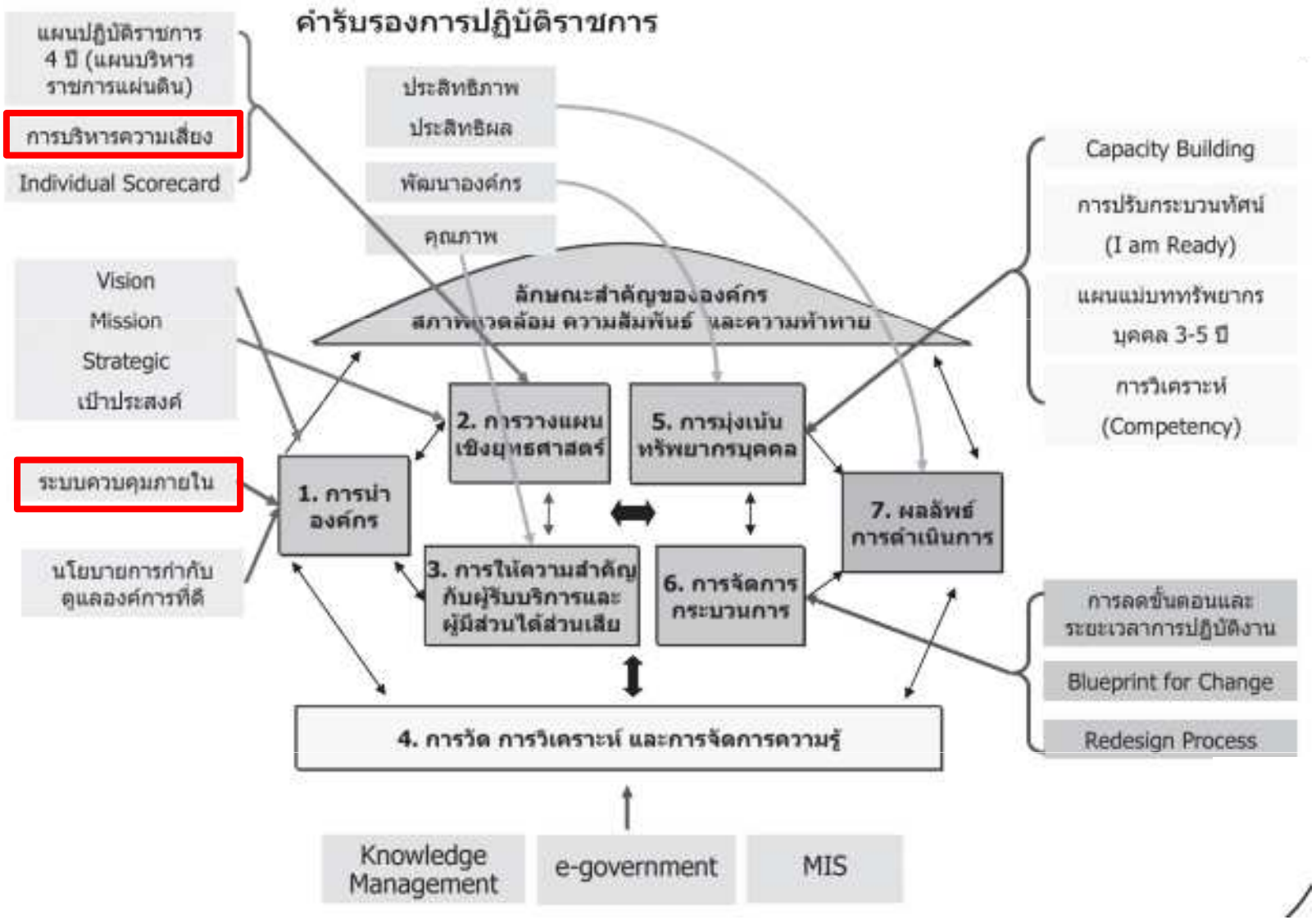

Risk Management
Monitor
Identify
Treat
Evaluate

การพัฒนาคุณภาพการบริหารจัดการ (PMQA) กับการบริหารความเสี่ยง (Risk Management)



ที่มา : คู่มือคำอธิบายตัวชี้วัด การพัฒนาคุณภาพการบริหารจัดการภาครัฐ ปีงบประมาณ พ.ศ. 2554 หน้า 13

LD 6 : ส่วนราชการต้องจัดให้มีระบบการควบคุมภายในและการบริหารความเสี่ยงที่ดีตามแนวทางของคณะกรรมการตรวจเงินแผ่นดิน

การควบคุมภายในเป็นปัจจัยสำคัญที่จะช่วยให้การดำเนินงานตามภารกิจมีประสิทธิภาพ ประหยัด และมีประสิทธิผล และช่วยป้องกันหรือลดความเสี่ยงจากการผิดพลาด ความเสียหาย ไม่ว่าจะในรูปของความสิ้นเปลือง ความสูญเปล่าของการใช้ทรัพย์สิน หรือการกระทำอันเป็นการทุจริต

SP 7 : ส่วนราชการต้องมีการวิเคราะห์และจัดทำแผนบริหารความเสี่ยงตามมาตรฐาน COSO เพื่อเตรียมการรองรับการเปลี่ยนแปลงที่อาจจะเกิดขึ้นจากการดำเนินแผนงาน/โครงการที่สำคัญซึ่งต้องครอบคลุมความเสี่ยงด้านธรรมาภิบาล

การบริหารความเสี่ยง คือ กระบวนการที่เป็นระบบในการบริหารปัจจัยและควบคุมกิจกรรมรวมทั้งกระบวนการการดำเนินการต่างๆ เพื่อลดมูลเหตุของโอกาสที่จะทำให้เกิดความเสียหายจากการดำเนินการที่ไม่เป็นไปตามแผน เพื่อให้ระดับของความเสี่ยงและผลกระทบที่จะเกิดขึ้นในอนาคตอยู่ในระดับที่สามารถยอมรับได้ ควบคุมได้ และตรวจสอบได้อย่างเป็นระบบ โดยในการดำเนินการบริหารความเสี่ยงตาม SP 7 นั้น มุ่งเน้นแผนงาน/โครงการที่สำคัญซึ่งผลสำเร็จของแผนงาน/โครงการมีผลกระทบสูงต่อการบรรลุความสำเร็จตามประเด็นยุทธศาสตร์

ที่มา : คู่มือคำอธิบายตัวชั้วัด การพัฒนาคุณภาพการบริหารจัดการภาครัฐ ปีงบประมาณ พ.ศ. 2554 หน้า 91 และ 101

IT 6 : ส่วนราชการต้องมีระบบบริหารความเสี่ยงของระบบฐานข้อมูลและสารสนเทศ

ส่วนราชการอาจจัดให้มีระบบบริหารความเสี่ยงของระบบฐานข้อมูลและสารสนเทศ ดังนี้

1. มีการบริหารความเสี่ยงเพื่อกำจัด ป้องกันหรือลดการเกิดความเสียหายในรูปแบบต่าง ๆ โดยมีแนวทาง/มาตรการที่จะป้องกันความเสียหาย และมีการสำรองข้อมูลสารสนเทศ (Back up) ซึ่งเมื่อเกิดความเสียหายส่วนราชการสามารถฟื้นฟูระบบสารสนเทศและกู้คืนข้อมูลจากความเสียหายได้ (Recovery)

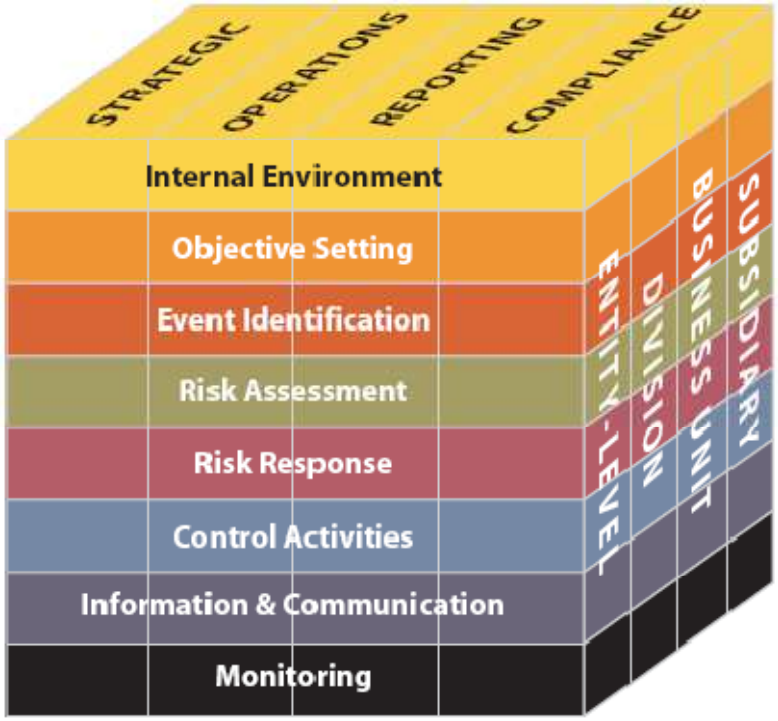
2. มีการจัดทำแผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติที่อาจจะเกิดกับระบบสารสนเทศ (IT Contingency Plan)

3. มีระบบรักษาความมั่นคงและปลอดภัย (Security) ของระบบสารสนเทศและระบบฐานข้อมูล เช่น ระบบ Anti-Virus ระบบไฟฟ้าสำรอง มีการกำหนดสิทธิให้ผู้ใช้ในแต่ละระดับ (Access rights) เป็นต้น

ที่มา : คู่มือคำอธิบายตัวชั้วัด การพัฒนาคุณภาพการบริหารจัดการภาครัฐ ปีงบประมาณ พ.ศ. 2554 หน้า 117

ส่วนราชการต้องมีขั้นตอนการดำเนินการ หลักเกณฑ์ในการวิเคราะห์ ประเมิน และจัดการความเสี่ยงอย่างเหมาะสม ตามกระบวนการบริหารความเสี่ยงตามมาตรฐาน COSO (The Committee of Sponsoring Organizations of the Treadway Commission) คือ

ส่วนราชการต้องมีการวิเคราะห์ และบริหารจัดการความเสี่ยงตามประเด็นยุทธศาสตร์ให้ครบถ้วน ทุกประเด็นยุทธศาสตร์ของส่วนราชการ โดยคัดเลือกแผนงาน/โครงการที่สำคัญและมีผลกระทบสูงต่อการบรรลุความสำเร็จตามประเด็นยุทธศาสตร์ที่ได้รับงบประมาณอย่างน้อยประเด็นยุทธศาสตร์ละ 1 แผนงาน/โครงการ มาดำเนินการบริหารจัดการความเสี่ยง เพื่อจัดการกับการเปลี่ยนแปลงที่อาจส่งผลกระทบต่อความสำเร็จหรือการบรรลุเป้าหมายของแผนงาน/โครงการ



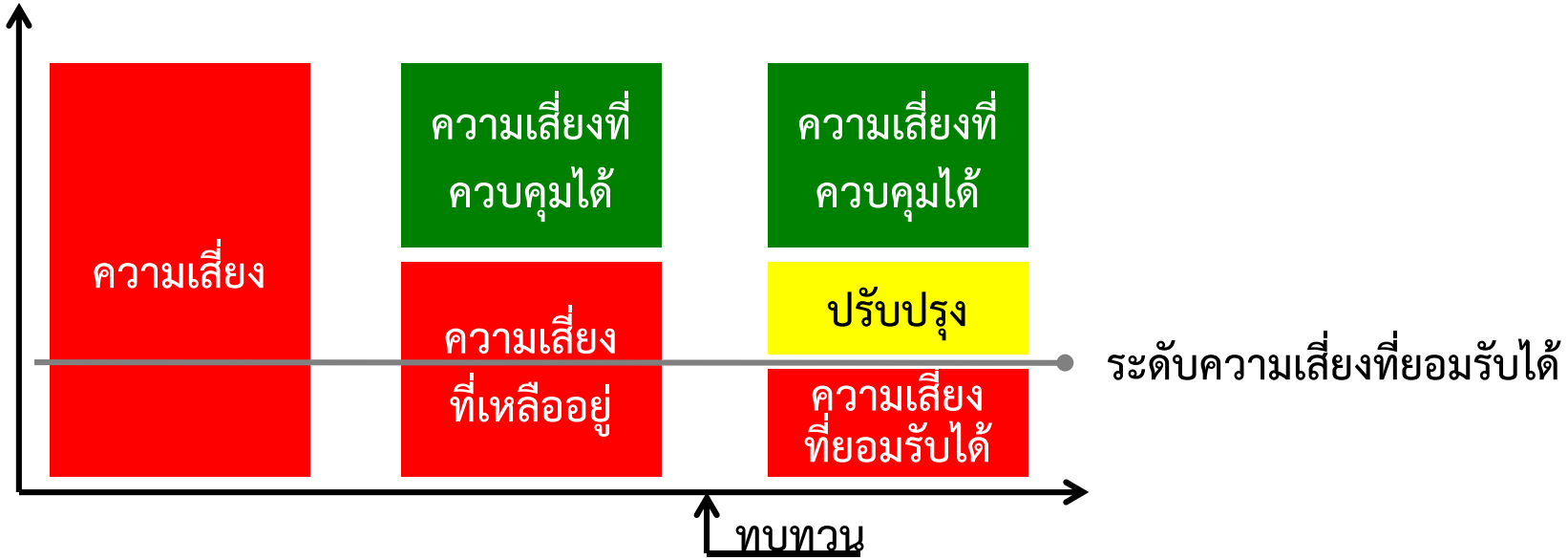
1. การกำหนดเป้าหมายการบริหารความเสี่ยง (Objective Setting)
2. การระบุความเสี่ยงต่างๆ (Event Identification)
3. การประเมินความเสี่ยง (Risk Assessment)
4. กลยุทธ์ที่ใช้ในการจัดการกับแต่ละความเสี่ยง (Risk Response)
5. กิจกรรมการบริหารความเสี่ยง (Control Activities)
6. ข้อมูลและการสื่อสารด้านบริหารความเสี่ยง (Information and Communication)
7. การติดตามผลและเฝ้าระวังความเสี่ยงต่างๆ (Monitoring)

ที่มา : คู่มือคำอธิบายตัวชั้วัด การพัฒนาคุณภาพการบริหารจัดการภาครัฐ ปีงบประมาณ พ.ศ. 2554 หน้า 101

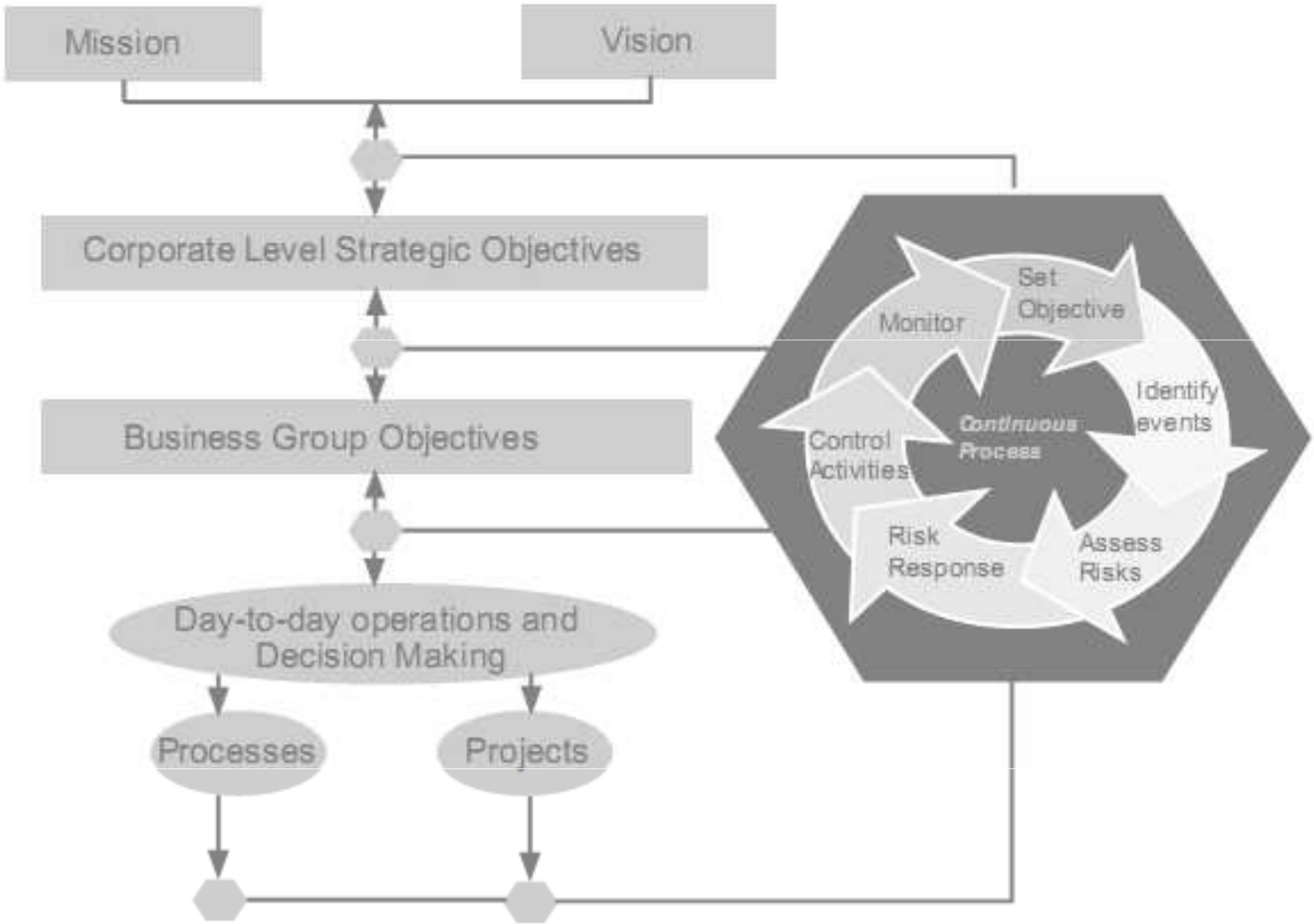
เมื่อหลายปีที่แล้วหน่วยงานที่ชื่อว่า COSO หรือ The Committee of Sponsoring Organization of the Treadway Commission ได้ออกเอกสาร Internal Control – Integrated Framework ออกมาเพื่อให้องค์กรธุรกิจและหน่วยงานอื่นใช้ในการประเมินและปรับปรุงระบบการควบคุมภายใน ซึ่งในเวลาต่อมาได้มีการผสมผสานแนวคิดเรื่องการจัดการความเสี่ยงเข้าไป จนทำให้พัฒนาขึ้นมาเป็นแนวคิดที่เรียกว่า Enterprise Risk Management – Integrated Framework โดยมีกระบวนการจัดการความเสี่ยงตามแนวทางของ COSO ทั้งสิ้น 8 ขั้นตอน ซึ่งในเวลาต่อมาได้กลายมาเป็นแม่บทของการควบคุมภายในด้วย

การจัดการความเสี่ยงต้องมองปัญหาความเสี่ยงแบบองค์รวม จึงจะสามารถควบคุมความเสี่ยงให้อยู่ในระดับที่รับได้

ทั้งนี้ความเสี่ยงที่ยอมรับได้ (Risk Appetite) คือประเภทของความเสี่ยงโดยรวมที่ผู้บริหารยอมรับได้ และระดับความเสี่ยงที่ยอมรับได้ (Risk Tolerance) คือ ระดับความเบี่ยงเบนที่องค์กรยอมรับจากเกณฑ์หรือตัวชี้วัดของการบรรลุวัตถุประสงค์ที่กำหนดไว้



ดังนั้นการจัดการความเสี่ยงที่เหมาะสมจะต้องอาศัยการมีส่วนร่วมจากผู้บริหารและผู้ปฏิบัติการจากทุกระดับร่วมกันพิจารณาทั้ง ความเสี่ยงที่ยอมรับได้ และระดับความเสี่ยงที่ยอมรับได้ เพื่อให้เกิดความเข้าใจและเห็นพ้องร่วมกันทั่วทั้งองค์กร



การบริหารความเสี่ยงเป็นความรับผิดชอบที่สำคัญอย่างสูงของคณะกรรมการขององค์กร ซึ่งการบริหารความเสี่ยงจะเป็นประโยชน์อย่างมากถ้าได้รับการเชื่อมโยงอย่างเหมาะสมกับกระบวนการวางแผนทางกลยุทธ์และการตัดสินใจขององค์กร

ที่มา : 10 คำถาม-คำตอบ ที่หน้ารู้เรื่องการบริหารความเสี่ยง หน้า 9

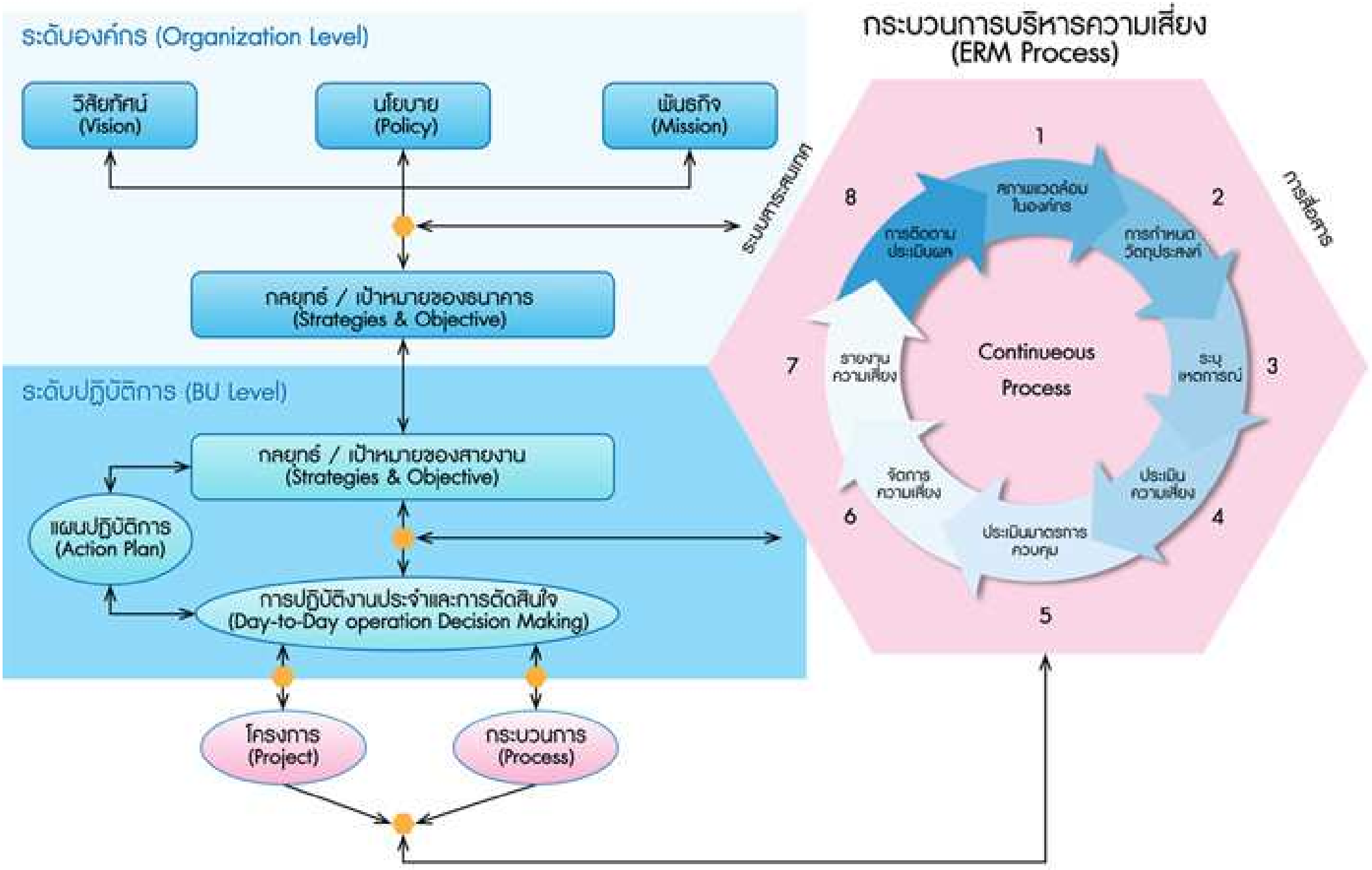
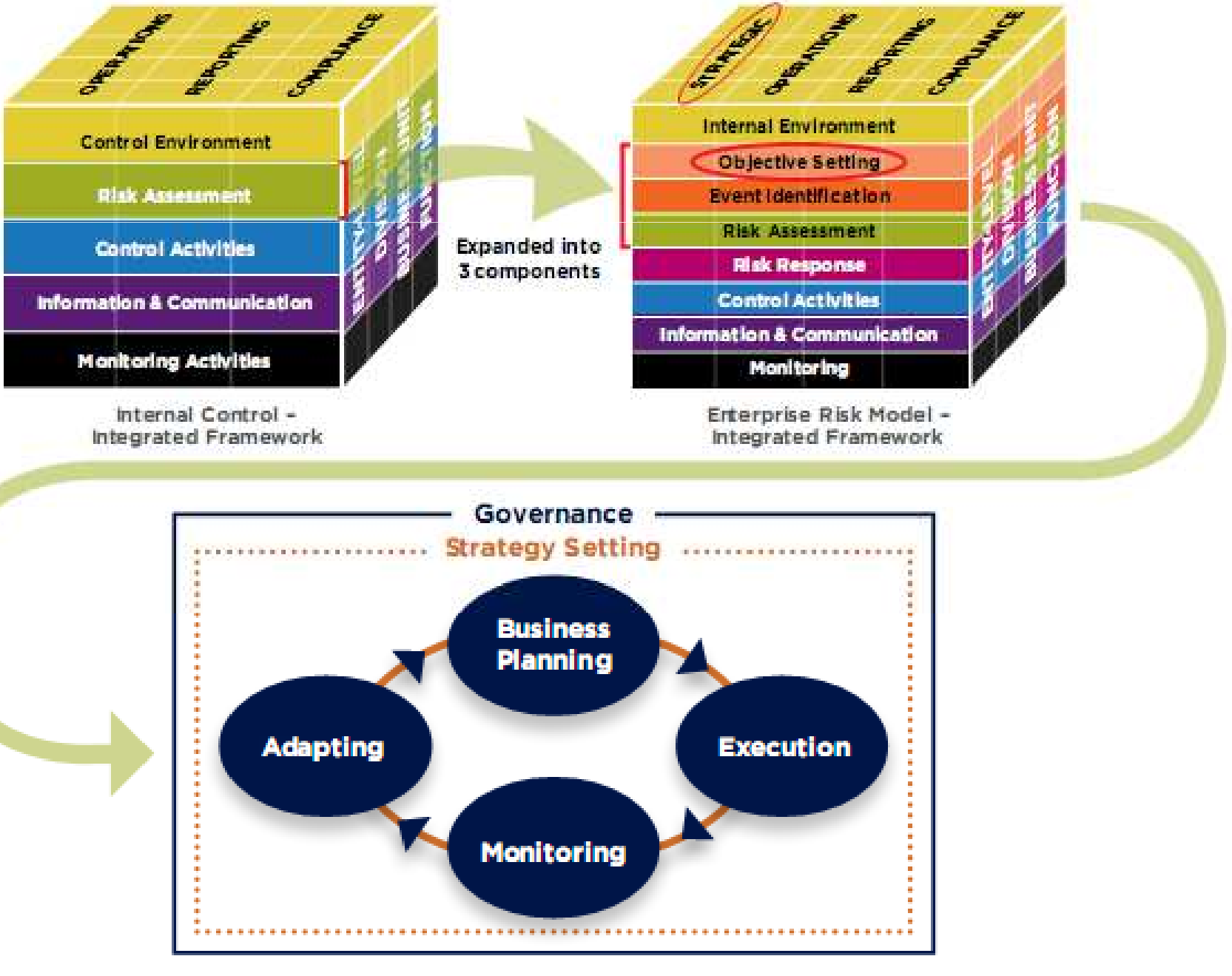
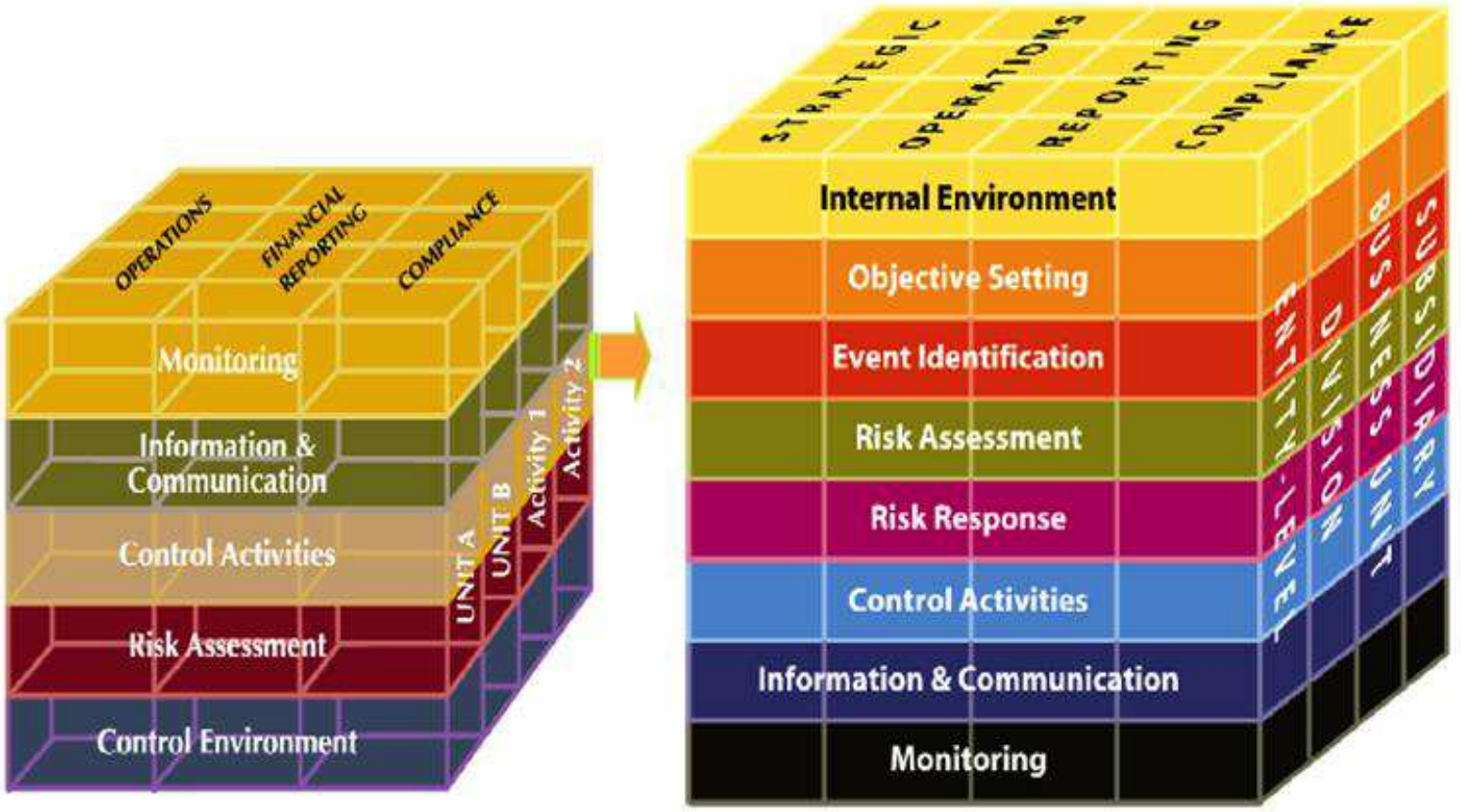

ระดับองค์กร (Organization Level)
วิสัยทัศน์ (Vision)
นโยบาย (Policy)
พันธกิจ (Mission)
ระบบการควบคุมภายใน
กลยุทธ์ / เป้าหมายของธนาคาร (Strategies & Objective)
ระดับปฏิบัติการ (BU Level)
กลยุทธ์ / เป้าหมายของสายงาน (Strategies & Objective)
แผนปฏิบัติการ (Action Plan)
การปฏิบัติงานประจำและการตัดสินใจ (Day-to-Day operation Decision Making)
โครงการ (Project)
กระบวนการ (Process)
กระบวนการบริหารความเสี่ยง (ERM Process)
Continueous Process
1
2
3
4
5
6
7
8
การสื่อสาร

Figure 2: Relationship of ERM and Internal Control to Contextual Business Model



Relationship between COSO 1 and COSO 2

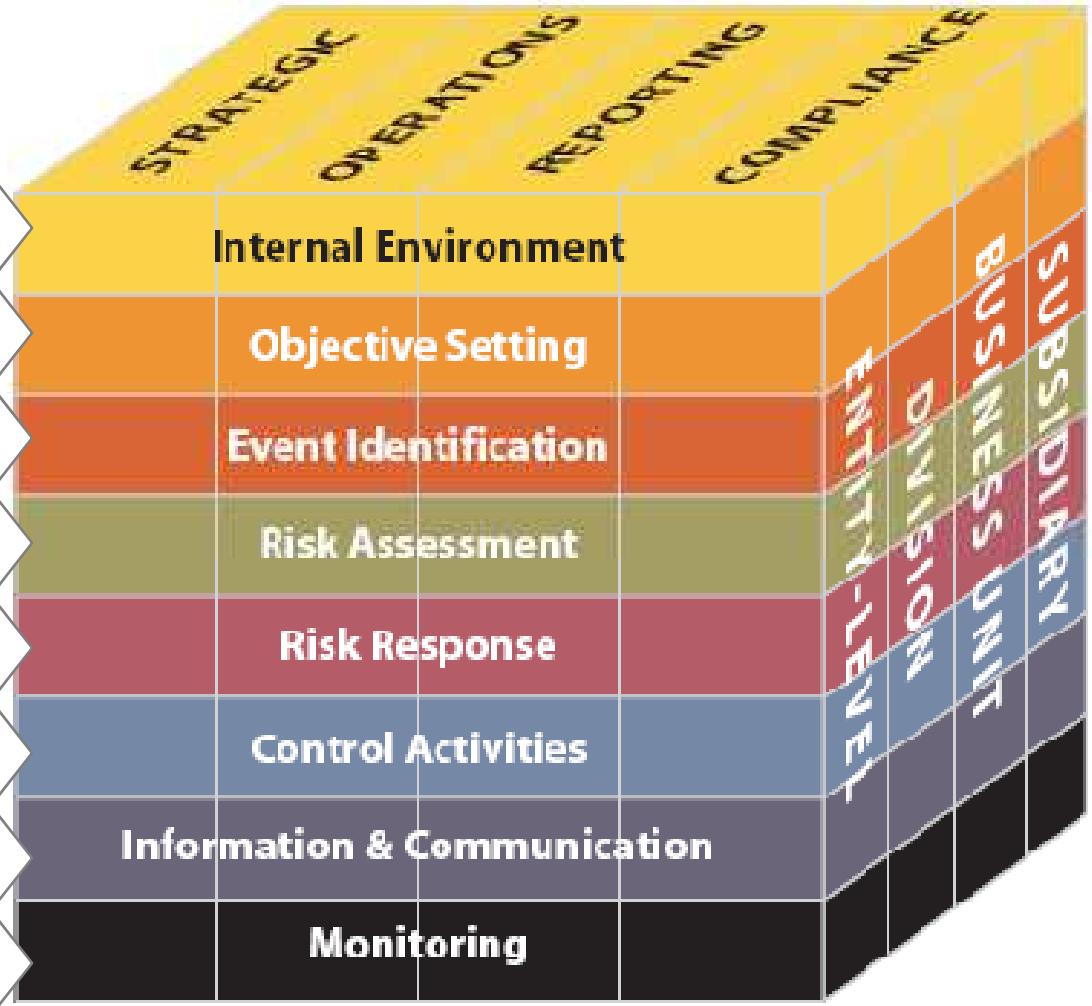
ERM is fully aligned with the COSO Internal Control- Integrated Framework



COSO 1 "Internal Control – Integrated Framework"

COSO 2 "Enterprise Risk Management – Integrated Framework"

การพัฒนาสภาพแวดล้อมภายในขององค์กรให้เอื้อ
การกำหนดวัตถุประสงค์ของการบริหารความเสี่ยง
การระบุถึงความเสี่ยงต่อเป้าหมายขององค์กร
การวิเคราะห์ความเสี่ยง (โอกาส / ผลกระทบ)
การกำหนดแนวทางในการจัดการความเสี่ยง
การกำหนดกิจกรรมควบคุมความเสี่ยง
การจัดการสารสนเทศและการสื่อสาร
การติดตามร่องรอยความเสี่ยง



การจัดการความเสี่ยงทั้ง 8 ขั้นตอนนี้เป็นกระบวนการที่สามารถประยุกต์ใช้ได้ทุกระดับขององค์กร ซึ่งถ้าองค์กรได้ดำเนินการตาม 8 ขั้นตอนนี้อย่างละเอียดรอบคอบก็สามารถที่จะป้องกันผลกระทบเชิงลบที่อาจจะเกิดขึ้นจากความเสี่ยงได้ รวมทั้งองค์กรยังสามารถมั่นใจได้ว่าการจัดการความเสี่ยงนั้นอยู่ในวิสัยที่สามารถควบคุมได้ด้วยความมั่นใจ

“ความเสี่ยง” หมายถึง โอกาสที่จะเกิดความผิดพลาด ความเสียหาย การรั่วไหล ความสูญเปล่า หรือเหตุการณ์ซึ่งไม่พึงประสงค์ที่ทำให้งานไม่ประสบความสำเร็จตามวัตถุประสงค์และเป้าหมายที่กำหนด ทั้งนี้ COSO ได้กำหนดความเสี่ยงไว้ 4 ประเภท

1. ความเสี่ยงด้านกลยุทธ์ (Strategic Risk)
2. ความเสี่ยงด้านการดำเนินงาน (Operational Risk)
3. ความเสี่ยงด้านการเงิน (Financial Risk)
4. ความเสี่ยงด้านกฎหมาย (Legal Risk)

แต่ก็อาจจะมีความเสี่ยงประเภทอื่นอีก เช่น ความเสี่ยงด้านการปลอดภัย (Hazard Risk) ความเสี่ยงด้านธรรมาภิบาล (Good Governance Risk) เป็นต้น

“การประเมินความเสี่ยง” หมายถึง กระบวนการที่ใช้ในการระบุและการวิเคราะห์ความเสี่ยงที่มีผลกระทบต่อการบรรลุวัตถุประสงค์ของหน่วยรับตรวจ รวมทั้งการกำหนดแนวทางที่จำเป็นต้องใช้ในการควบคุมความเสี่ยง หรือการบริหารความเสี่ยง

ในการดำเนินการเกี่ยวกับการประเมินความเสี่ยง ฝ่ายบริหารต้องประเมินความเสี่ยงทั้งจากปัจจัยภายในและภายนอกที่มผลกระทบต่อการบรรลุวัตถุประสงค์ขององค์กรอย่างเพียงพอและเหมาะสม

การประเมินความเสี่ยง (Risk Assessment) ประกอบด้วย 3 ขั้นตอน ดังนี้

1. การระบุปัจจัยเสี่ยง (Event Identification)
   องค์กรจะต้องทำความเข้าใจและระบุให้ได้ถึงปัจจัยที่เป็นสาเหตุของความเสี่ยง
2. การวิเคราะห์ความเสี่ยง (Risk Analysis)
   องค์กรจะต้องวิเคราะห์ถึงผลกระทบของความเสี่ยงที่มีต่อองค์กรและโอกาสที่จะเกิดความเสี่ยง
3. การกำหนดวิธีการจัดการความเสี่ยง (Risk Response)
   องค์กรจะต้องกำหนดวิธีการจัดการความเสี่ยงโดยจะต้องคำนึงถึงความเหมาะสมและความคุ้มค่าด้วย

การวิเคราะห์ความเสี่ยง คือการประมาณโอกาสของความเสี่ยงที่อาจจะเกิดขึ้นและประเมินผลกระทบจากความเสี่ยงว่ามีมากน้อยเพียงใด เพื่อจัดลำดับความสำคัญองความเสี่ยงที่มีผลต่อองค์กร โดยวัดคะแนนรวมที่ได้จากการคำนวนของโอกาสและผลกระทบของความเสี่ยง

โอกาสที่จะเกิดความเสี่ยง

โอกาสที่จะเกิดความเสี่ยง	ความถี่โดยเฉลี่ย	คะแนน
สูงมาก	1 เดือนต่อครั้งหรือมากกว่า	5
สูง	1 - 6 เดือนต่อครั้งแต่ไม่เกิน 5 ครั้ง	4
ปานกลาง	1 ปีต่อครั้ง	3
น้อย	2 - 3 ปีต่อครั้ง	2
น้อยมาก	5 ปีต่อครั้ง	1

ผลกระทบของความเสี่ยงต่อหน่วยรับตรวจ

ผลกระทบ	มูลค่าความเสียหาย	คะแนน
สูงมาก	>10 ล้านบาท	5
สูง	>2.5 แสนบาท-10 ล้านบาท	4
ปานกลาง	>50,000 บาท-2.5 แสนบาท	3
น้อย	>10,000 บาท-50,000 บาท	2
น้อยมาก	ไม่เกิน 10,000 บาท	1

เมื่อวิเคราะห์โอกาสและผลกระทบของความเสี่ยงอย่างรอบคอบแล้ว หน่วยรับตรวจต้องพิจารณาถึงระดับของความเสี่ยงว่ามีความเสี่ยงสูงหรือต่ำโดยพิจารณาจากแผนภูมิความเสี่ยง (Risk Map)

ผลกระทบ

5					
4				สูง	มาก
3			สูง		
2		ปาน	กลาง		
1	ต่ำ				
	1	2	3	4	5

โอกาสที่จะเกิด

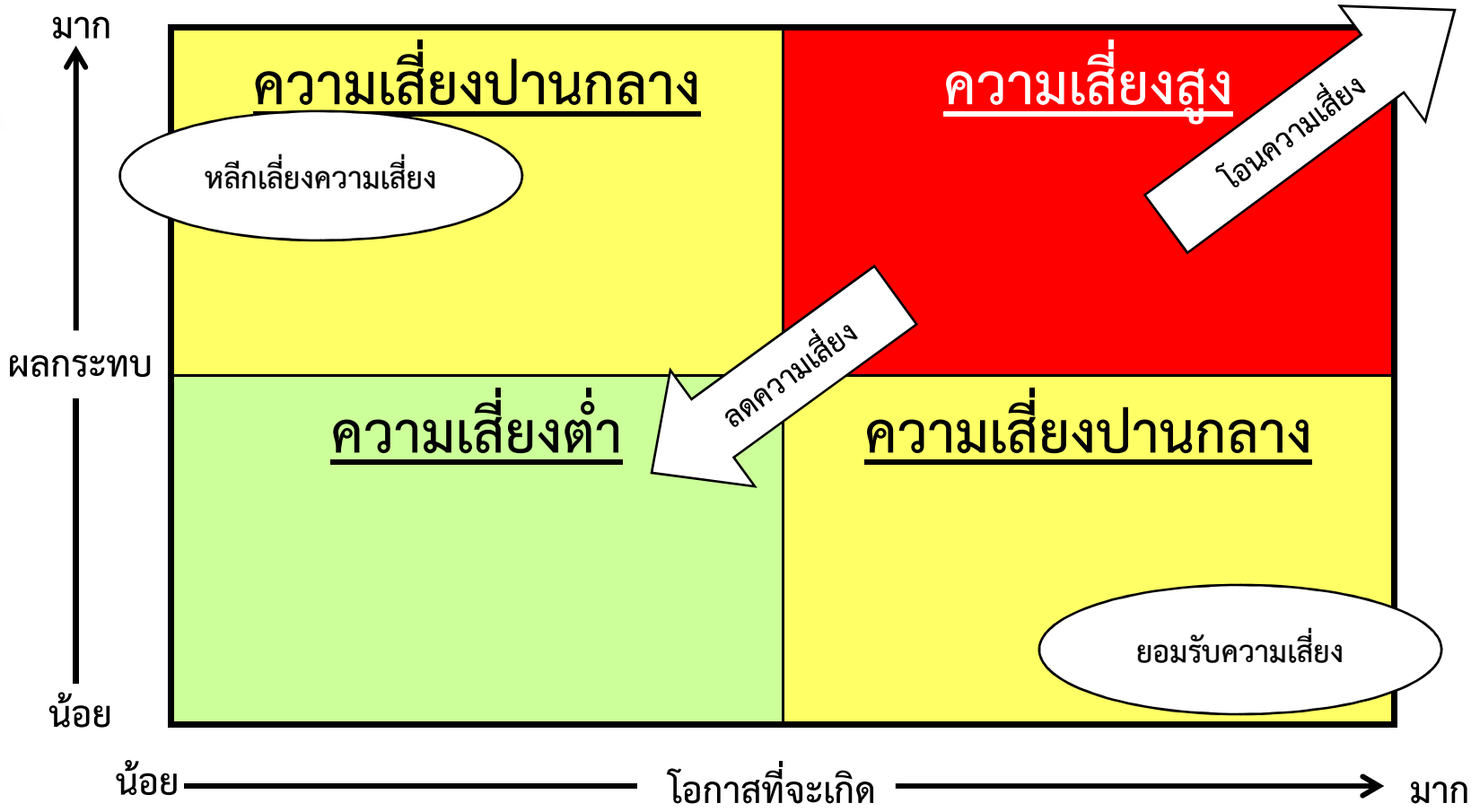
ฝ่ายบริหารขององค์กรควรพิจารณาว่าความเสี่ยงที่เกิดขึ้นนั้นเป็นความเสี่ยงที่เกิดจากปัจจัยภายใน หรือปัจจัยภายนอก เพื่อกำหนดวิธีการจัดการความเสี่ยงมีแนวทางดังต่อไปนี้

- กรณีที่เป็นความเสี่ยงที่เกิดจากปัจจัยภายนอก ซึ่งมิได้อยู่ภายใต้การควบคุมของฝ่ายบริหาร สามารถกำหนดวิธีการจัดการความเสี่ยง (บางทีก็เรียกว่า “กลยุทธ์การจัดการความเสี่ยง) ดังต่อไปนี้

    1. การหลีกเลี่ยง (Avoiding) คือการดำเนินการหลีกเลี่ยงความเสี่ยง
    2. การแบ่งปัน (Sharing) คือการแบ่งความรับผิดชอบให้ผู้อื่นร่วมรับความเสี่ยง
    3. การลด (Reducing) เป็นการดำเนินเพื่อลดโอกาสการเกิดขึ้นของความเสี่ยง
    4. การยอมรับ (Accepting) เป็นการยอมรับในความเสี่ยงที่อาจจะเกิดขึ้นแต่เป็นความเสี่ยงที่ยอมรับได้

- กรณีที่เป็นความเสี่ยงที่เกิดจากปัจจัยภายใน องค์กรควรจะมีกิจกรรมการควบคุมอย่างเพียงพอและเหมาะสม

กลยุทธ์ในการจัดการความเสี่ยง



การเลือกกลยุทธ์การจัดการความเสี่ยงอาจจะพิจารณาจากระดับของความเสี่ยงด้วย ซึ่งถ้าความเสี่ยงสูงอาจจะใช้กลยุทธ์การถ่ายโอนความเสี่ยงเพื่อที่จะไม่ต้องรับความเสี่ยงเอง หรืออาจจะใช้กลยุทธ์การลดความเสี่ยง (ลดโอกาส) ในขณะที่ความเสี่ยงที่มีผลกระทบสูงแต่โอกาสที่เกิดมีน้อยก็อาจจะเลือกที่จะหลีกเลี่ยงความเสี่ยง แต่ถ้าความเสี่ยงนั้นมีผลกระทบน้อยมากแม้ว่าโอกาสที่เกิดจะสูงก็อาจจะใช้กลยุทธ์การยอมรับความเสี่ยงได้

“กิจกรรมการควบคุม” หมายถึง นโยบายและวิธีการต่างๆ ที่ฝ่ายบริหารกำหนดให้บุคลากรขององค์กรปฏิบัติเพื่อลดหรือควบคุมความเสี่ยง และได้รับการสนองตอบโดยมีการปฏิบัติตาม ในการดำเนินการเกี่ยวกับกิจกรรมการควบคุม ฝ่ายบริหารต้องจัดให้มีกิจกรรมการควบคุมที่มีประสิทธิภาพและประสิทธิผล เพื่อป้องกันหรือลดความเสียหาย ความผิดพลาด ที่อาจเกิดขึ้นและให้สามารถบรรลุผลตามวัตถุประสงค์ของการควบคุมภายใน สำหรับกิจกรรมการควบคุมในเบื้องต้นจะต้องแบ่งแยกหน้าที่งานภายในองค์กรอย่างเหมาะสม ไม่มอบหมายให้บุคคลใดบุคคลหนึ่งมีหน้าที่เป็นผู้รับผิดชอบปฏิบัติงานที่สำคัญหรืองานที่เสี่ยงต่อความเสียหายตั้งแต่ต้นจนจบ แต่ถ้ามีความจำเป็นให้กำหนดกิจกรรมการควบคุมอื่นที่เหมาะสมทดแทน

กิจกรรมการควบคุมประกอบด้วยกิจกรรมต่างๆที่สำคัญ คือ

- การกำหนดนโยบายและแผนงาน (Policies and Plans)
- การสอบทานโดยผู้บริหาร (Management Review)
- การประมวลผลข้อมูล (Information Processing)
- การควบคุมทางกายภาพ (Physical Control)
- การมอบอำนาจที่เหมาะสม (Appropriate Empowerment)
- การแบ่งแยกหน้าที่ (Segregation of Duties)
- ดัชนีวัดผลการดำเนินงาน (Performance Indicators)
- การจัดทำเอกสารหลักฐาน (Documentation)
- การตรวจสอบการปฏิบัติงานอย่างอิสระ (Independent Checks on Performance)
- การกำหนดสิทธิ์การเข้าถึงสินทรัพย์ (Accessing Rights)

ภายใต้แนวคิดการพิจารณาความเสี่ยงตามหลักธรรมาภิบาลที่สำนักงบประมาณได้จัดทำขึ้นนั้น ทำให้แต่ละส่วนราชการต้องดำเนินการคัดเลือกแผนงาน / โครงการที่สนองตอบนโยบายหลักตามแผนการบริหารราชการแผ่นดิน มาวิเคราะห์ความเสี่ยงตามหลักธรรมาภิบาล โดยมีหลักเกณฑ์การพิจารณาดังต่อไปนี้

กรณีที่ 1	กรณีที่ 2
เป็นแผนงาน/โครงการที่มีผลกระทบต่อความสำเร็จในการบรรลุผลตามเป้าหมายกระทรวง ส่วนราชการ/รัฐวิสาหกิจภายใต้กระทรวง กลุ่มจังหวัด หรือจังหวัด และ เป็นแผนงาน/โครงการที่มีผลกระทบต่อชีวิตความเป็นอยู่ของประชาชน สิ่งแวดล้อมหรือการให้บริการขั้นพื้นฐานของประชาชน และ เป็นแผนงาน/โครงการลงทุนที่ใช้งบประมาณสูงสุดอันดับแรกของกรม ในกระทรวงเดียวกัน รัฐวิสาหกิจและหน่วยงานอื่น	เป็นแผนงาน/โครงการอื่นที่ส่วนราชการ/รัฐวิสาหกิจหรือผู้ตรวจราชการสำนักนายกรัฐมนตรี หรือผู้ตรวจราชการกระทรวง หรือสำนักงบประมาณ เห็นควรให้มีการวิเคราะห์ความเสี่ยงตามหลักธรรมาภิบาล ก็ถือว่าเป็นแผนงาน/โครงการที่ต้องวิเคราะห์ความเสี่ยงตามหลักธรรมาภิบาล

การวิเคราะห์ความเสี่ยงของโครงการนั้นจะต้องวิเคราะห์ความเสี่ยงตามหลักธรรมาภิบาล และประเมินความเสี่ยงที่เกิดจากสภาพแวดล้อมภายในและภายนอก ดังมีรายละเอียดในแต่ละส่วนดังต่อไปนี้

ความเสี่ยงตามหลักธรรมาภิบาล

1. หลักประสิทธิผล (Effectiveness)
2. หลักประสิทธิภาพ (Efficiency)
3. หลักการมีส่วนร่วม (Participation)
4. หลักความโปร่งใส (Transparency)
5. หลักการสนองตอบรับ (Responsiveness)
6. หลักความรับผิดชอบ (Accountability)
7. หลักนิติธรรม (Rules of Law)
8. หลักการกระจายอำนาจ (Decentralization)
9. หลักเสมอภาค (Equity)
10. หลักมุ่งเน้นฉันทามติ (Consensus Oriented)

ที่มา : คู่มือคำอธิบายตัวชี้วัด การพัฒนาคุณภาพการบริหารจัดการภาครัฐ ปีงบประมาณ พ.ศ. 2554 หน้า 102-104

RM1

ตารางที่ 1 การระบุความเสี่ยงและการประเมินความเสี่ยง

ประเภทความเสี่ยง/วัตถุประสงค์	ปัจจัยเสี่ยง	โอกาส	ผลกระทบ	ระดับ ความเสี่ยง	รหัส
1.ความเสี่ยงด้านกลยุทธ์ 1.1 ..... 1.2					
2. ความเสี่ยงด้านธรรมภิบาล 2.1 ..... 2.2					
3.ความเสี่ยงด้านเทคโนโลยีสารสนเทศ 3.1 ..... 3.2					
4.ความเสี่ยงด้านกระบวนการ 4.1 ..... 4.2					

RM2

ตารางที่ 2 แผนการบริหารความเสี่ยง

ประเภทความเสี่ยง/วัตถุประสงค์	ปัจจัยเสี่ยง	แนวทางการตอบสนองความเสี่ยง	แผนงาน/กิจกรรมการจัดการความเสี่ยง	ผู้รับผิดชอบ	ระยะเวลาดำเนินการ
1.ความเสี่ยงด้านกลยุทธ์ 1.1 ..... 1.2					
2. ความเสี่ยงด้านธรรมภิบาล 2.1 ..... 2.2					
3.ความเสี่ยงด้านเทคโนโลยีสารสนเทศ 3.1 ..... 3.2					
4.ความเสี่ยงด้านกระบวนการ 4.1 ..... 4.2					

RM3

ตารางที่ 3 ผลการดำเนินงานตามแผนการบริหารความเสี่ยง

ประเภท/วัตถุประสงค์	ปัจจัยเสี่ยง	รายงานผลการดำเนินการ	โอกาสคงเหลือ	ผลกระทบคงเหลือ	ระดับความเสี่ยงคงเหลือ	ปัญหาอุปสรรค
1.ความเสี่ยงด้านกลยุทธ์ 1.1 ..... 1.2						
2. ความเสี่ยงด้านธรรมภิบาล 2.1 ..... 2.2						
3.ความเสี่ยงด้านเทคโนโลยีสารสนเทศ 3.1 ..... 3.2						
4.ความเสี่ยงด้านกระบวนการ 4.1 ..... 4.2						

ปัจจัยแห่งความสำเร็จของการจัดการความเสี่ยง

1. การมีส่วนร่วมและการสนับสนุนจากผู้บริหารระดับสูง
2. การใช้คำนิยามความเสี่ยงเพื่อให้เป็นที่เข้าใจแบบเดียวกันและใช้ร่วมกันในองค์กร
3. การปฏิบัติตามกระบวนการในการบริหารความเสี่ยงอย่างต่อเนื่อง
4. กระบวนการในการบริหารการเปลี่ยนแปลง
5. ระบบสารสนเทศเพื่อรองรับการจัดการความเสี่ยง
6. การสื่อสารภายในองค์กรและการสื่อสารให้แก่ผู้มีส่วนได้ส่วนเสียภายนอก
7. การติดตามและการวัดผลการ
8. การปรับปรุงกระบวนการทำง
9. การฝึกอบรมและกลไกด้านทร
10. การให้รางวัลจากผลสำเร็จ