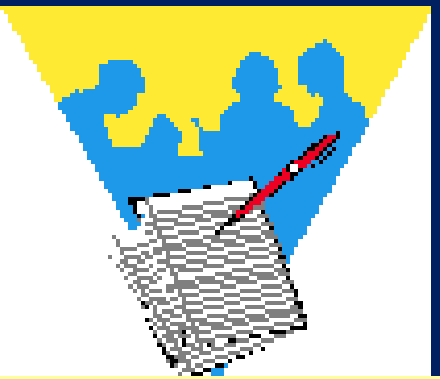
การบรรยาย
โครงการฝึกอบรมเชิงปฏิบัติการ เรื่อง
การบริหารความเสี่ยงโครงการ
(Project Risk Management)

สำนักงานจังหวัดสกลนคร
วันที่ ๑ - ๒ มิถุนายน ๒๕๖๐
ณ โรงแรมพีซี แกรนด์ พาเลซ จังหวัดสกลนคร

บรรยายโดย ประไพพิศ ลลิตาภรณ์
ผู้อำนวยการสำนักงานตรวจสอบภายใน ม.เกษตรศาสตร์
CIA no.30815

ขอบเขตการอบรม

- ทำไมต้องบริหารความเสี่ยง
- การบูรณาการเชื่อมโยงความเสี่ยง
- ความหมาย / ประเภท / แนวคิด
- กรอบ ERM (COSO II)
- เทคนิคการนำกรอบ ERM สู่การปฏิบัติ
- ข้อมูลที่ควรรู้ก่อนการประเมินความเสี่ยง
- ขั้นตอนและแบบฟอร์ม



การทำสิ่งใดก็ตามย่อมมีความเสี่ยงและต้นทุน แต่ก็ยังน้อยกว่าความเสี่ยงและต้นทุนหลายรูปแบบที่เกิดจากการไม่ทำอะไรเลยแบบเอาสะดวก

จอห์น เอฟ. เคนเนดี้ , 1960

ทำไมต้องบริหารความเสี่ยง

ส่วนราชการ รัฐวิสาหกิจ

- พระราชกฤษฎีกา ว่าด้วยหลักเกณฑ์และวิธีการบริหารกิจการบ้านเมืองที่ดี พ.ศ.2546
- ระเบียบคณะกรรมการตรวจเงินแผ่นดินว่าด้วยการกำหนดมาตรฐานการควบคุมภายใน พ.ศ.2544
- มติคณะรัฐมนตรี เมื่อวันที่ 26 พ.ค.2552 เรื่องการวิเคราะห์ความเสี่ยงตามหลักธรรมาภิบาล

มหาวิทยาลัย (ภาครัฐ & เอกชน)

การประกันคุณภาพการศึกษาตาม พรบ. การศึกษาแห่งชาติ พ.ศ.2542 (แก้ไขเพิ่มเติม ฉบับที่ 2 พ.ศ.2545)

ภาคเอกชน

- หลักการกำกับดูแลกิจการที่ดีสำหรับบริษัทจดทะเบียน ปี 2549 ของตลาดหลักทรัพย์แห่งประเทศไทย
- ISO 31000

ความเชื่อมโยงของการพัฒนาระบบราชการ กับ เกณฑ์คุณภาพการบริหารจัดการภาครัฐ

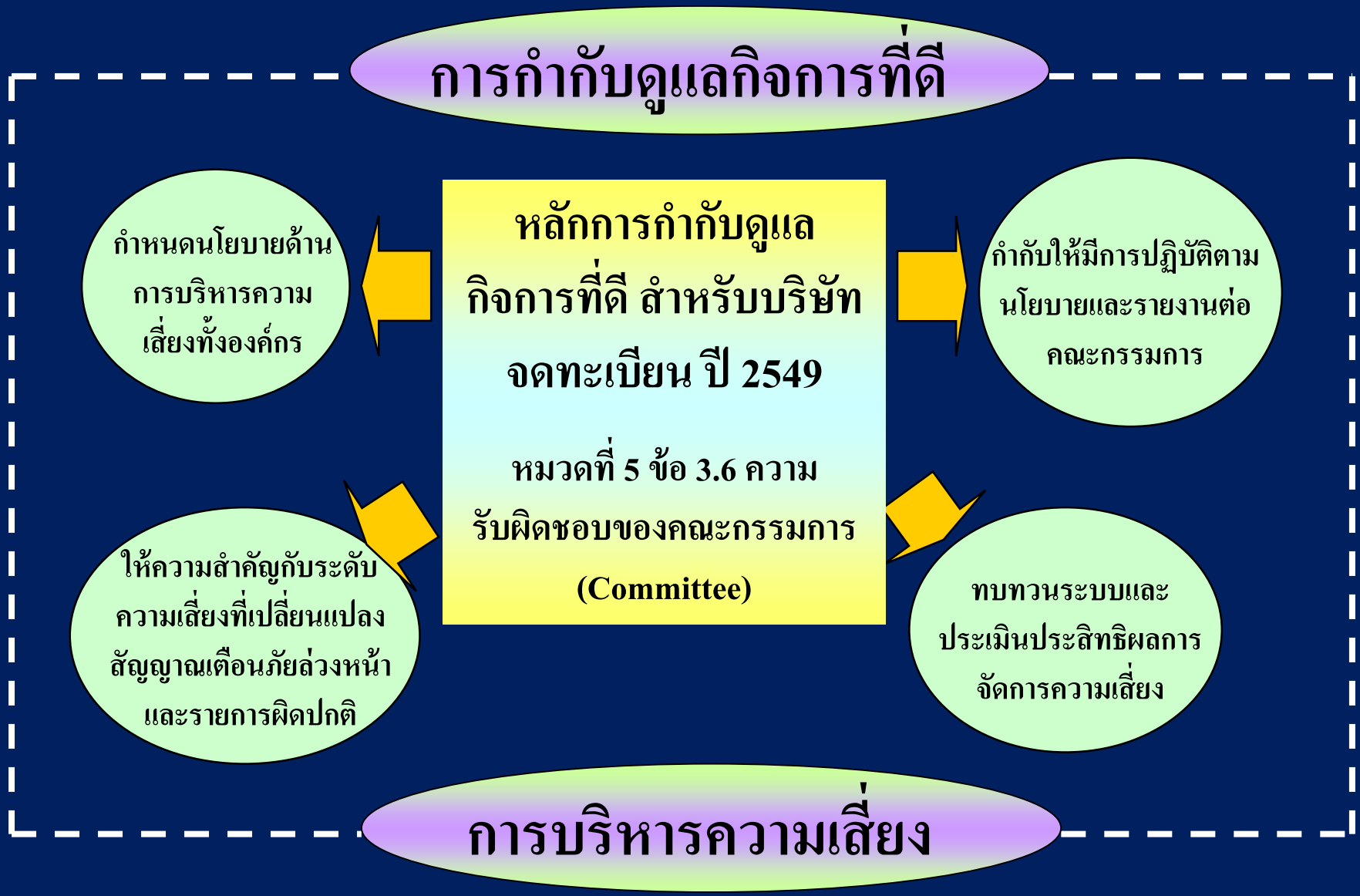
การบริหารความเสี่ยงกับมาตรฐานการควบคุมภายใน

ความเสี่ยงตามหลักธรรมาภิบาล

เปรียบเทียบหลักธรรมาภิบาล (Good Governance) / (Corporate Governance)

UNDP (9 ข้อ) United Nations Development Programme	สำนักงาน ก.พ.ร. (9 ข้อ)	มติ ครม. เรื่อง การวิเคราะห์ความเสี่ยงตามหลักธรรมาภิบาลของแผนงาน/โครงการสำคัญตามนโยบายรัฐบาล ของสำนักงบประมาณ (8 ข้อ)	พระราชกฤษฎีกาว่าด้วยหลักเกณฑ์และวิธีการบริหารกิจการบ้านเมืองที่ดี พ.ศ.2546 (6 ข้อ)
1. Participation การมีส่วนร่วม	1. Participation การมีส่วนร่วม	1. Public Participation หลักการมีส่วนร่วมของสาธารณะ	1. หลักคุณธรรม
2. Rule of law นิติธรรม	2. Rule of law นิติธรรม	2. Rule of law นิติธรรม	2. หลักนิติธรรม
3. Transparency ความโปร่งใส	3. Transparency ความโปร่งใส	3. Transparency หลักความโปร่งใส	3. หลักความโปร่งใส
4. Responsiveness การตอบสนอง	4. Responsiveness การตอบสนอง	4. Responsiveness หลักการสนองตอบรับ	4. หลักการมีส่วนร่วม
5. Equity ความเสมอภาค / ความเที่ยงธรรม	5. Equity ความเสมอภาค	5. Equity หลักความเสมอภาค	5. หลักความรับผิดชอบ
6. Effectiveness and Efficiency ประสิทธิผลและประสิทธิภาพ	6. Effectiveness ประสิทธิผล	6. Virtue หลักคุณธรรม	6. หลักความคุ้มค่า
7. Accountability ภาระรับผิดชอบ	7. Efficiency ประสิทธิภาพ	7. Value for Money หลักความคุ้มค่า	
8. Consensus oriented การมุ่งเน้นฉันทามติ	8. Accountability ภาระรับผิดชอบ	8. Public Accountability หลักความรับผิดรับชอบต่อสาธารณะ	
9. Strategic Vision วิสัยทัศน์เชิงยุทธศาสตร์	9. Decentralization กระจายอำนาจ		

การบริหารความเสี่ยงกับการกำกับดูแลกิจการที่ดี



การบริหารความเสี่ยง กับ ISO 31000

การบูรณาการเชื่อมโยงความเสี่ยง

ความหมายที่แตกต่าง

Enterprise Risk Management

Risk Management

การควบคุมภายใน COSO

ปัญหา

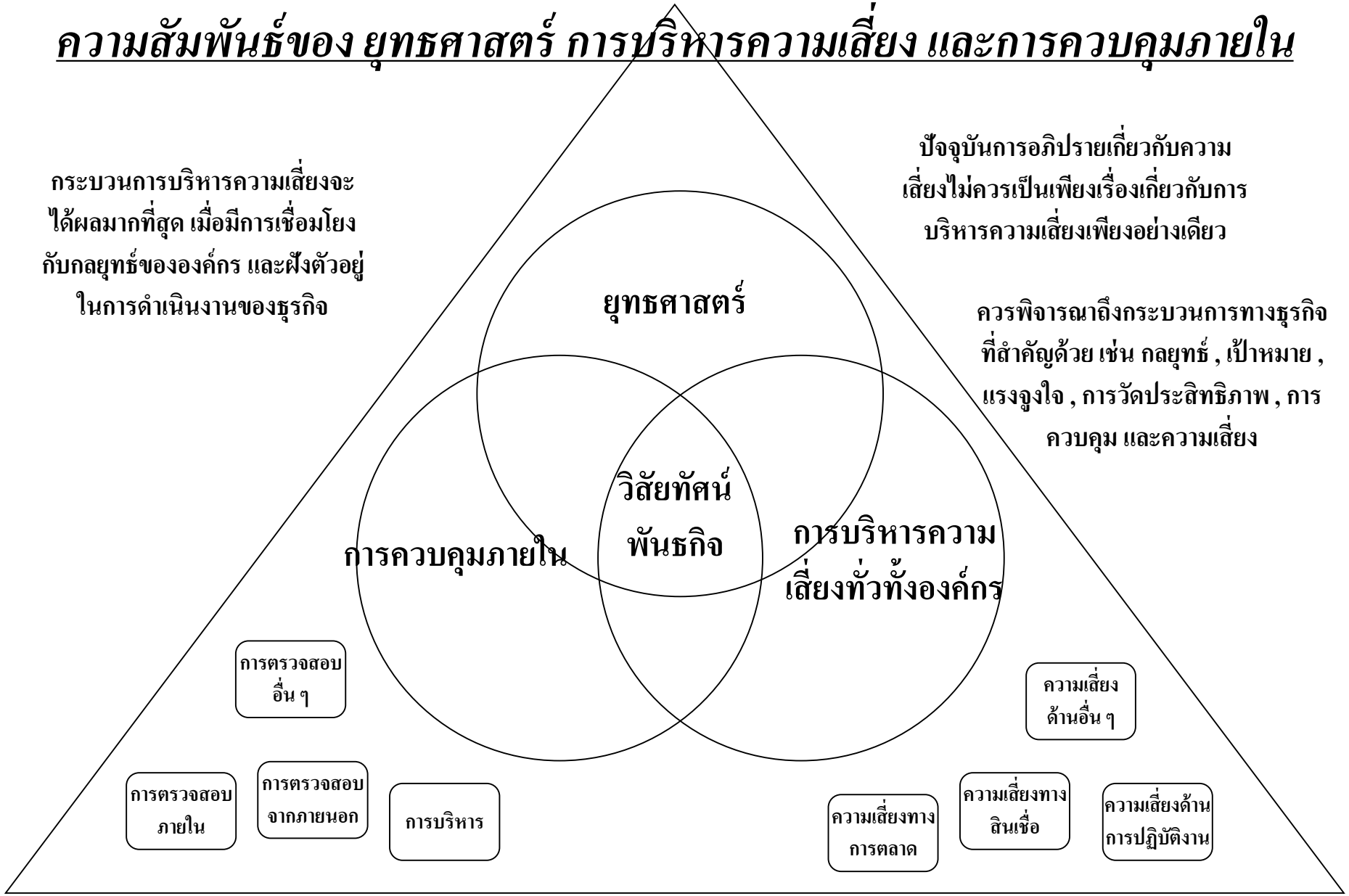
ความไม่แน่นอน

ความสัมพันธ์ของ ยุทธศาสตร์ การบริหารความเสี่ยง และการควบคุมภายใน

กระบวนการบริหารความเสี่ยงจะได้ผลมากที่สุด เมื่อมีการเชื่อมโยงกับกลยุทธ์ขององค์กร และฝังตัวอยู่ในการดำเนินงานของธุรกิจ

ปัจจุบันการอภิปรายเกี่ยวกับความเสี่ยงไม่ควรเป็นเพียงเรื่องเกี่ยวกับการบริหารความเสี่ยงเพียงอย่างเดียว

ควรพิจารณาถึงกระบวนการทางธุรกิจที่สำคัญด้วย เช่น กลยุทธ์ , เป้าหมาย , แรงจูงใจ , การวัดประสิทธิภาพ , การควบคุม และความเสี่ยง

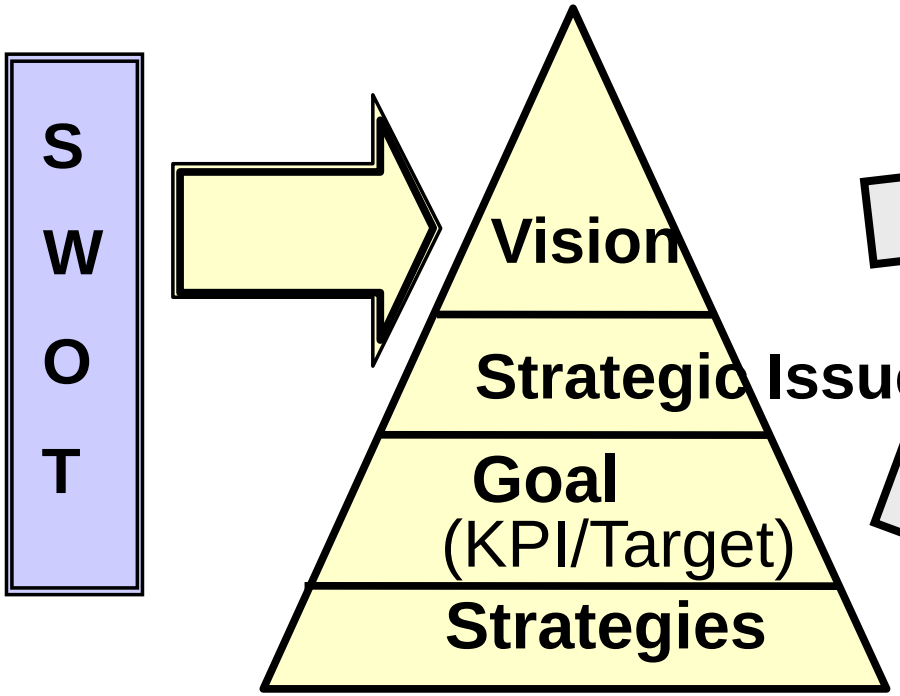


การเงิน | สภาพแวดล้อม | เทคโนโลยี | การพัฒนาธุรกิจ | กฎหมาย | ข้อมูลข่าวสาร | การปฏิบัติงาน | ระเบียบข้อบังคับ

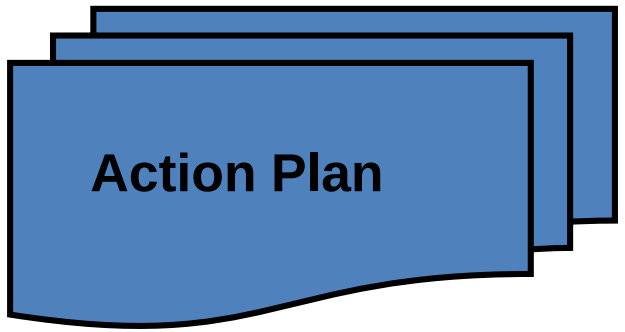
ที่มา : KPMG Phoomchai Business Advisory Ltd.,

Strategy Formulation ⇨ Strategy Implementation

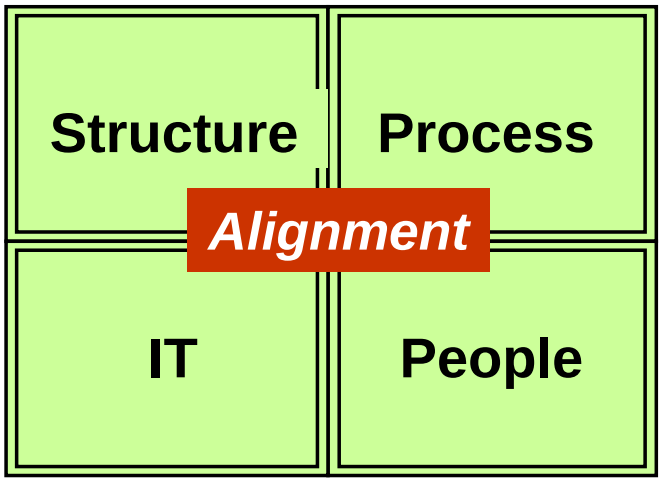
แผนปฏิบัติราชการ 4 ปี



แผนปฏิบัติราชการรายปี



Risk Assessment & Management



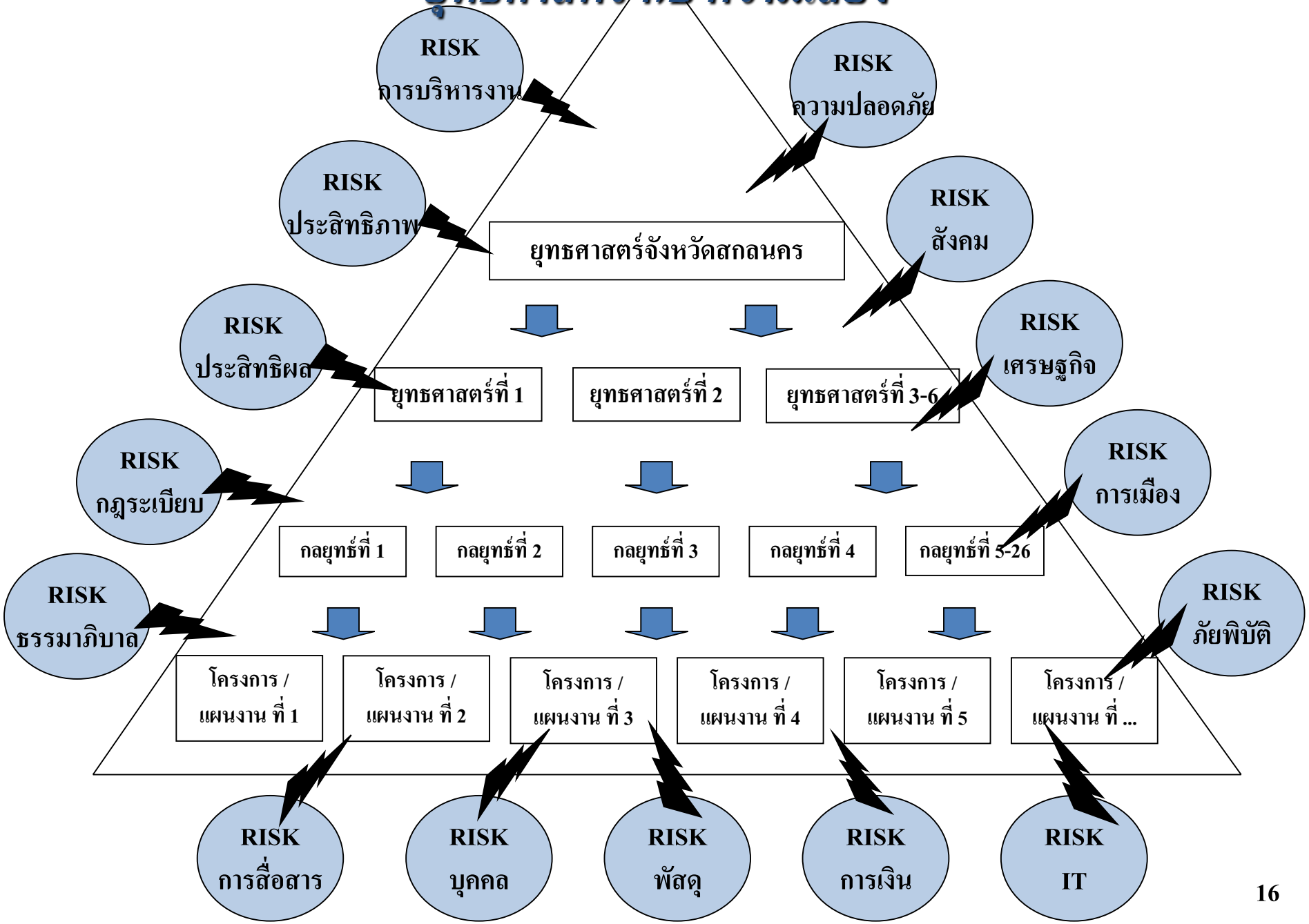
Blueprint for Change

ก.พ.ร.
สำนักงานคณะกรรมการพัฒนาระบบราชการ

การเชื่อมโยง Balance Scorecard กับ Risk

เป้าหมายของบริษัท	ปัจจัยเสี่ยงภายนอก	ปัจจัยเสี่ยงภายใน
ด้านการเงิน	- ปัจจัยเศรษฐศาสตร์มหภาค	- รายงานทางการเงิน
1. ทำให้รายได้สูงขึ้น	- อัตราแลกเปลี่ยน	- การชำระบัญชี
2. ได้รับผลลัพธ์ (รายได้) สูงขึ้นอย่างต่อเนื่อง	- สภาพแวดล้อมทางการเมือง	- กฎหมาย
3. เพิ่มผลผลิตสูงขึ้น	- สภาพแวดล้อมทางการแข่งขัน	- การผิดสัญญา
ด้านการตลาด-ลูกค้า	- ความมั่นคงของรายได้	- การบริหารสัญญา
4. ความสัมพันธ์ของลูกค้าพัฒนามากขึ้น	- เงินเฟ้อและโครงสร้างราคา	- การบริหารจัดการทรัพย์สิน
5. ข้อเสนอที่หลากหลายของลูกค้าแตกต่างกัน	- กฎเกณฑ์ของการตรวจคนเข้าเมือง	- การบริหารทรัพยากรมนุษย์
ด้านการปฏิบัติที่เป็นเลิศ	- ความปลอดภัย ความเชื่อมโยงของธุรกิจ	- วัฒนธรรม ค่านิยม ความเป็นผู้นำ
6. มุ่งเน้นมาตรฐานสากล	ฯ ล ฯ	ฯ ล ฯ
7. ควบคุมต้นทุนการดำเนินงาน		
8. ปรับปรุงคุณภาพผลผลิต		
ด้านการพัฒนาองค์การ		
9. พัฒนาและรักษาความสามารถเฉพาะของบุคคล		
10. พัฒนาฝีมือแรงงานระดับมาตรฐานสากล		
11. พัฒนาความเป็นผู้นำ		

ยุทธศาสตร์ กับ ความเสี่ยง



ความเสี่ยง คือ .....

- โอกาสที่จะเกิดความผิดพลาด ความเสียหาย การรั่วไหล ความสูญเปล่า หรือเหตุการณ์ที่ไม่พึงประสงค์ ที่ทำให้งานไม่ประสบความสำเร็จตามวัตถุประสงค์และเป้าหมายที่กำหนด :

  - Internal Risk ความเสี่ยงภายใน

  - External Risk ความเสี่ยงภายนอก

- เหตุการณ์หรือการกระทำใดๆ อาจเกิดขึ้นภายใต้สถานการณ์ที่ไม่แน่นอนและจะส่งผลกระทบหรือสร้างความเสียหาย หรือความล้มเหลว หรือลดโอกาสที่จะบรรลุความสำเร็จตามวัตถุประสงค์และเป้าหมายที่กำหนด

ประเภทความเสี่ยง

ประเภท

1. **Strategic Risk** (การเมือง เศรษฐกิจ กฎหมาย ตลาด ภาพลักษณ์ ผู้นำ ชื่อเสียง ลูกค้า)
2. **Operational Risk** (กระบวนการ เทคโนโลยี และคนในองค์กร)
3. **Financial Risk** (การผันผวนทางการเงิน อัตราดอกเบี้ย การขึ้นราคาสินค้า การให้เครดิต สภาพคล่อง และการตลาด)
4. **Compliance Risk** (กฎหมายทั้งในและต่างประเทศ)
5. **Hazard Risk** (ด้านภัยพิบัติทางธรรมชาติ การสูญเสียทางชีวิตและทรัพย์สิน การก่อการร้าย)

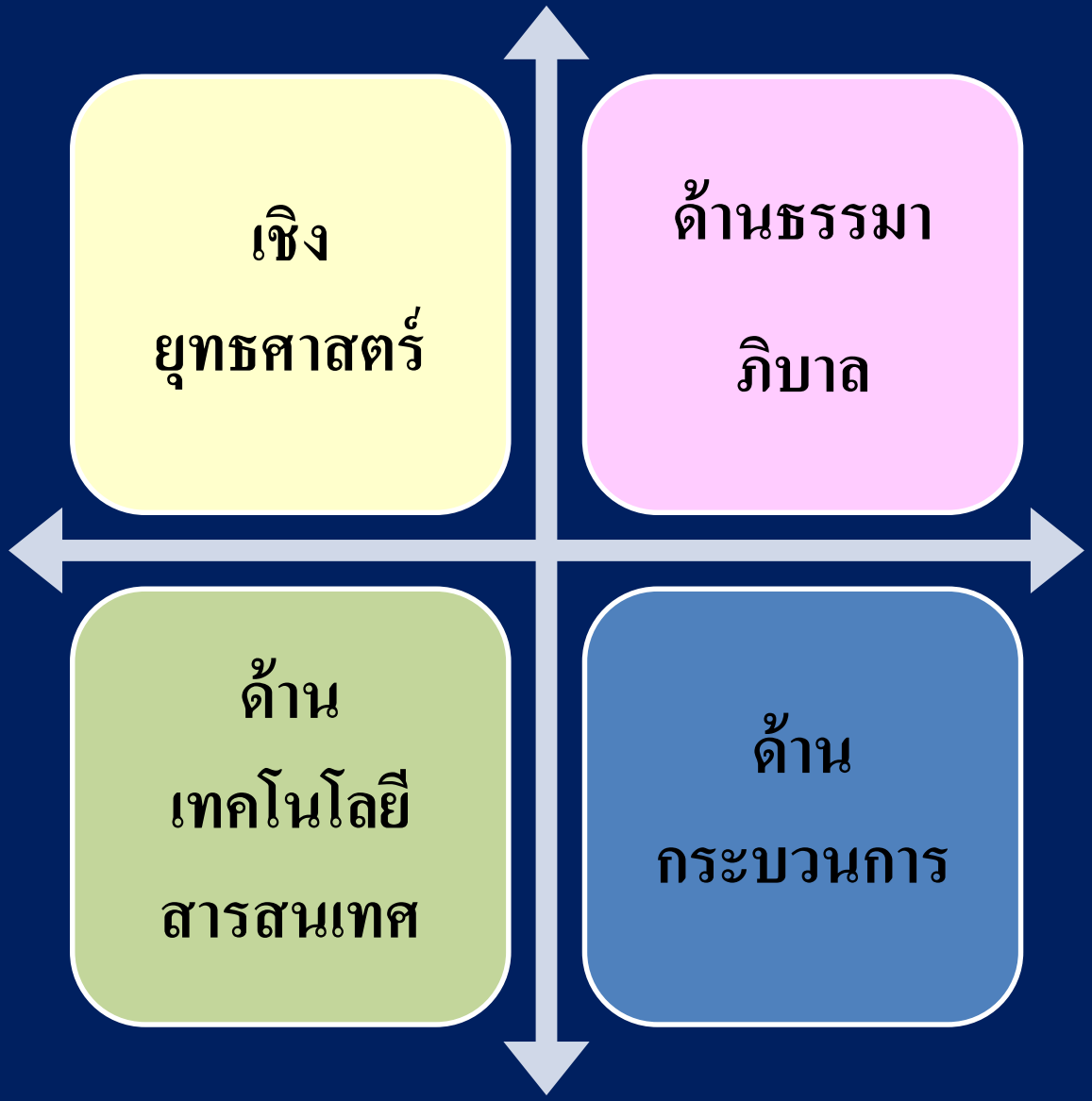
ERM

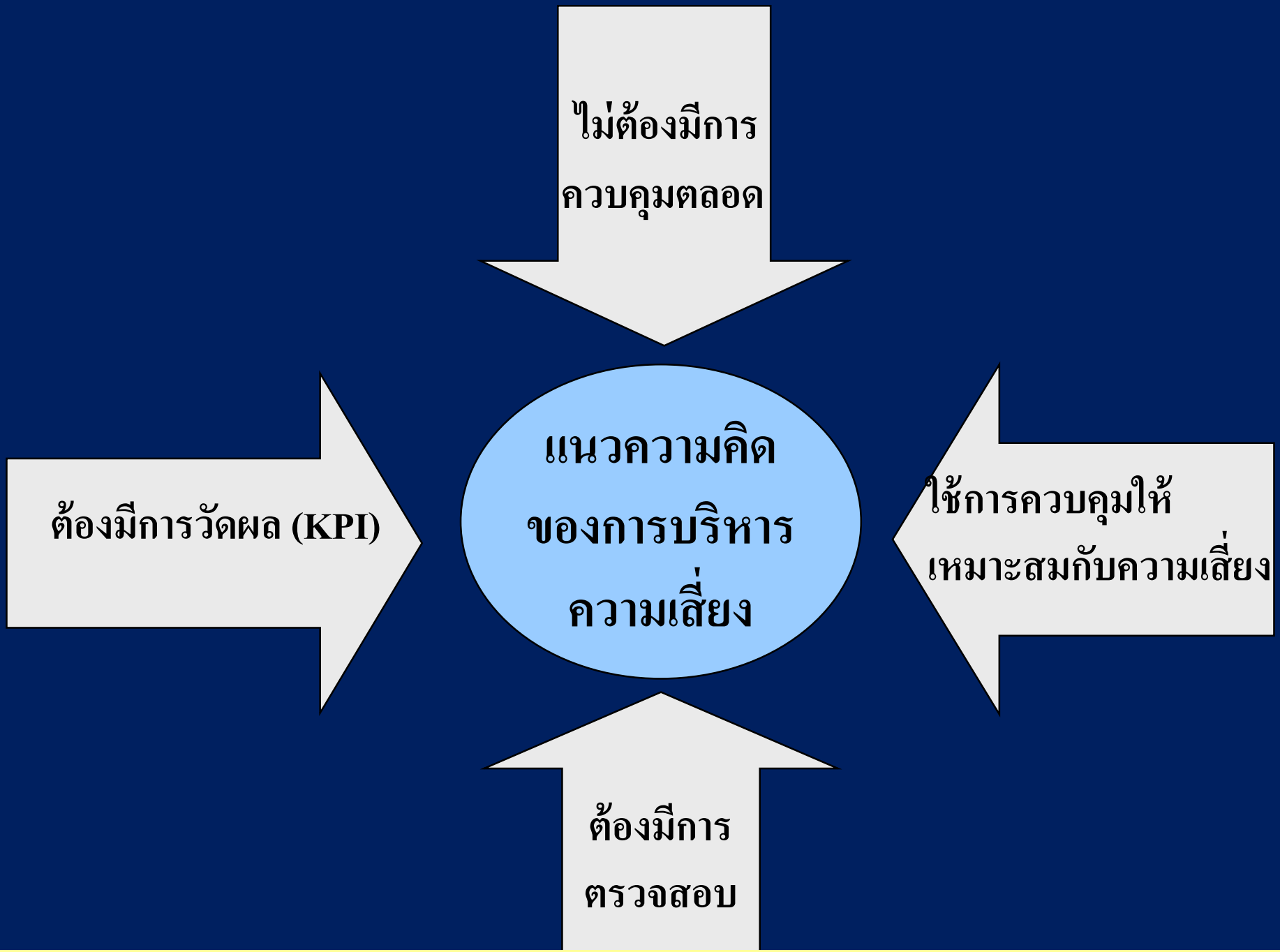
1. **Strategic Risk** (เป้าหมายตามแผนยุทธศาสตร์ กลยุทธ์)
2. **Operational Risk** (ประสิทธิภาพ ประสิทธิผล)
3. **Reporting Risk** (ความครบถ้วน ถูกต้อง น่าเชื่อถือของรายงานทางการเงินและรายงานต่าง ๆ ที่สำคัญ)
4. **Compliance Risk** (การปฏิบัติตามกฎระเบียบ ข้อบังคับ นโยบาย มาตรฐาน)

COSO

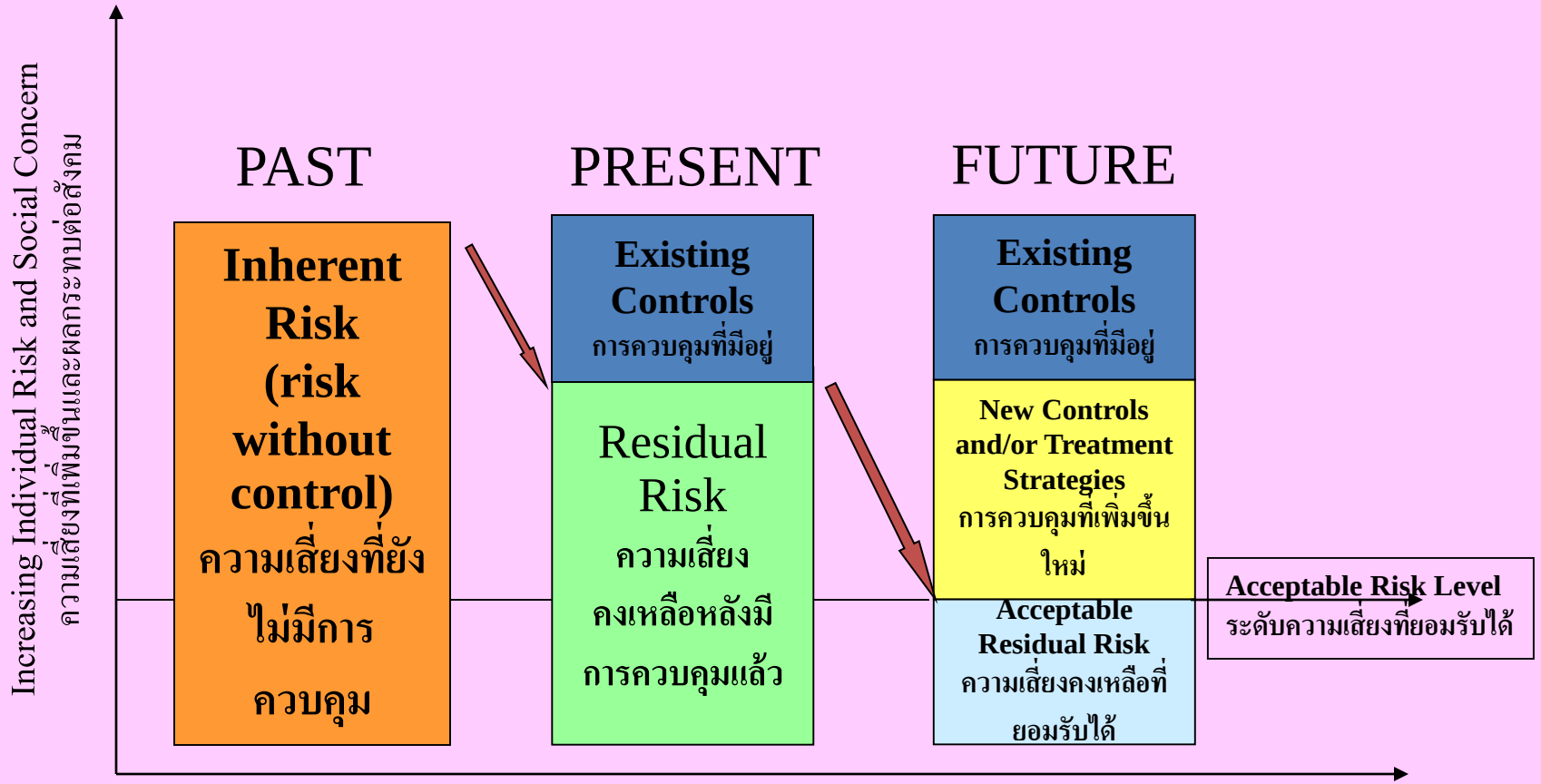
1. **Operational Risk** (ประสิทธิภาพ ประสิทธิผล)
2. **Financial Risk** (รายงานทางการเงิน)
3. **Compliance Risk** (การปฏิบัติตามกฎระเบียบ ข้อบังคับ นโยบาย มาตรฐาน)

ประเภทความเสี่ยง (ก.พ.ร.)




ไม่ต้องมีการ
ควบคุมตลอด
ต้องมีการวัดผล (KPI)
แนวความคิด
ของการบริหาร
ความเสี่ยง
ใช้การควบคุมให้
เหมาะสมกับความเสี่ยง
ต้องมีการ
ตรวจสอบ

แนวคิดของการบริหารความเสี่ยง/ควบคุมภายใน



Key Risk Indicator (KRI)

- ดัชนีที่จะทำหน้าที่ชี้นำหรือส่งสัญญาณเตือนล่วงหน้า ให้ผู้บริหารเห็นถึงความเป็นไปได้ที่จะเกิดความสูญเสียในอนาคต

Risk Appetite : RA
ระดับความเสี่ยงที่ยอมรับได้

- จำนวน (amount) หรือข้อความ (statement) ของความเสี่ยงในภาพกว้าง (broad level) ที่องค์กรสามารถยอมรับได้ เพื่อสร้างมูลค่ากับผู้มีส่วนได้เสีย ใช้เป็นแนวทางการกำหนดกลยุทธ์องค์กร เพื่อการจัดสรรทรัพยากรอย่างเหมาะสม

ประโยชน์ที่ได้

- ตระหนักถึงภัยคุกคามที่ยังมาไม่ถึง
- บริหารเชิงรุก มีการป้องกันล่วงหน้าและลดการเผชิญหน้าเหตุการณ์ที่ไม่คาดหมาย
- ปรับปรุงระบบงานและการวางแผน
- ลดการสูญเสียที่อาจเกิดขึ้น
- สร้างโอกาสใหม่ๆ ให้เกิดการเปลี่ยนแปลงในองค์กรรวมถึงการสร้างสรรค์สิ่งใหม่ให้องค์กร
- สร้างคุณค่าให้การทำงาน

- สนับสนุนการตัดสินใจของผู้บริหาร
- สร้างความมั่นใจในความสำเร็จของกลยุทธ์ที่กำหนด
- สร้างความมั่นใจในการเติบโตในระยะยาว
- สร้างภาพลักษณ์ที่ดีให้องค์กร
- ปกป้องผู้ปฏิบัติงาน
- ช่วยยกประเด็นระดับปฏิบัติการไปสู่การพิจารณาของผู้บริหาร
- ส่วนหนึ่งของระบบธรรมภิบาล
- มองเป้าหมายในภาพรวม

กรอบ ERM (COSO II)

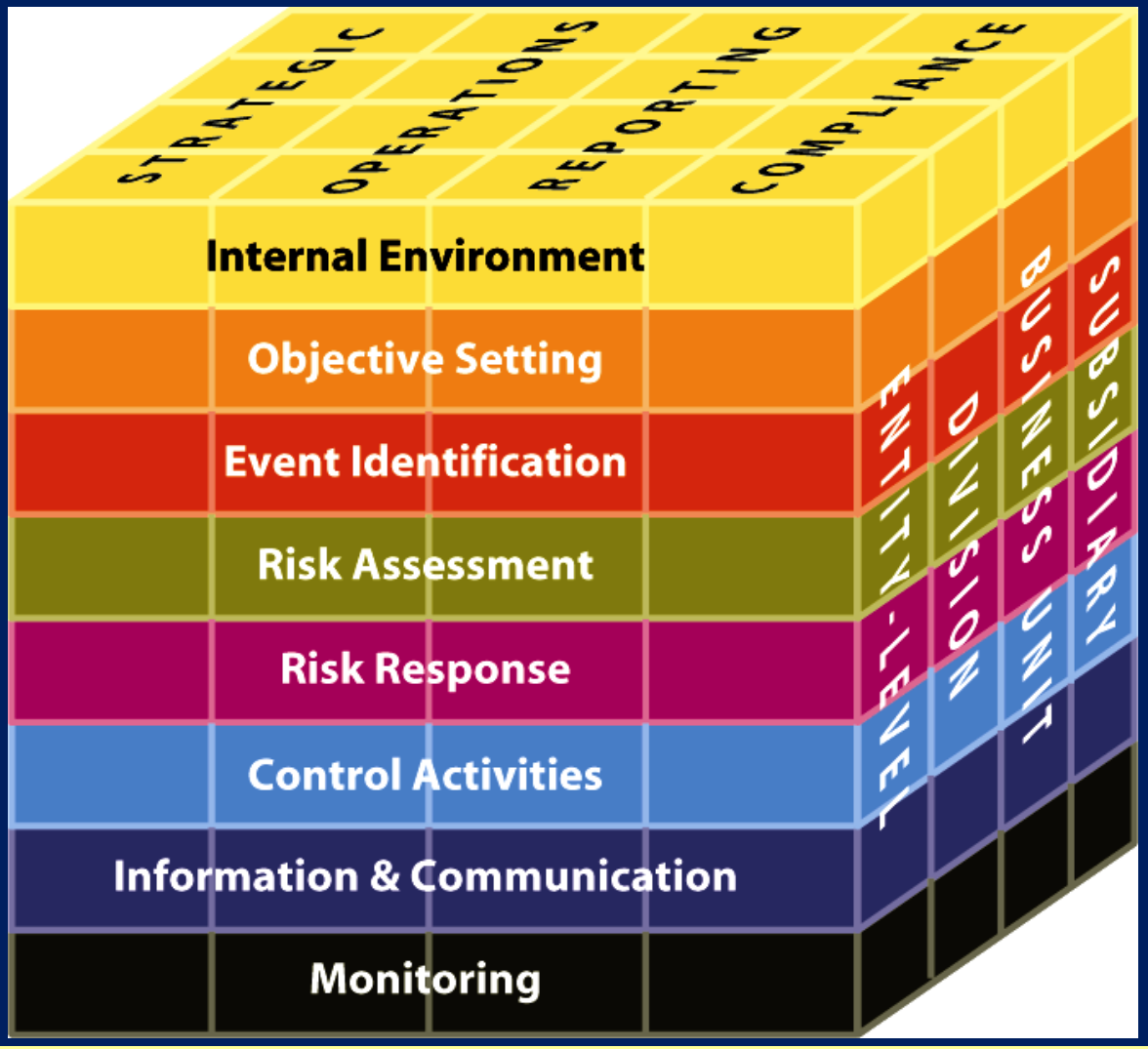
Enterprise Risk Management

(The Committee of Sponsoring Organization of Treadway Commission)

กรอบการบริหารความเสี่ยงทั่วทั้งองค์กร

วัตถุประสงค์ขององค์กรแบ่งออกเป็น 4 กลุ่มคือ

- Strategic
- Operations
- Reporting
- Compliance



การบริหารความเสี่ยงทั่วทั้งองค์กร (ERM)

คือ กระบวนการระบุและวิเคราะห์ความเสี่ยงในมุมของภาพที่เป็นองค์รวมแบบบูรณาการ และทั่วทั้งองค์กร ครอบคลุมทุกกิจกรรมที่จะนำไปสู่การบรรลุเป้าหมาย

8 องค์ประกอบของการบริหารความเสี่ยง

ERM

1. สภาพแวดล้อมภายใน (Internal Environment)
2. การกำหนดวัตถุประสงค์ (Objective Setting)
3. การระบุเหตุการณ์ (Event Identification)
4. การประเมินความเสี่ยง (Risk Assessment)
5. การตอบสนองต่อความเสี่ยง (Risk Response)
6. กิจกรรมการควบคุม (Control Activities)
7. การสื่อสารและระบบสารสนเทศ (Information and Communication)
8. การติดตามผล (Monitoring)

1. สภาพแวดล้อมภายใน

- ปรัชญาในการบริหารความเสี่ยงขององค์กร
- ระดับความเสี่ยงที่องค์กรรับมือได้
- วัฒนธรรมภายใน
- วัฒนธรรมกลุ่มย่อย
- การยอมรับในความเสี่ยงที่องค์กรกำลังเผชิญอยู่
- กรรมการบริหาร
- ความโปร่งใสและจรรยาบรรณของคนภายในองค์กร

1. สภาพแวดล้อมภายใน (ต่อ)

- ความมุ่งมั่นในการทำงานอย่างมีประสิทธิภาพ
- รูปแบบการบริหารและการสั่งการ
- โครงสร้างองค์กร
- การมอบหมายความรับผิดชอบและอำนาจหน้าที่
- นโยบายการบริหารบุคคล
- ความหลากหลายของสภาพแวดล้อมที่แตกต่างกัน

2. การกำหนดวัตถุประสงค์

- วิสัยทัศน์ พันธกิจ เป้าหมาย
- วัตถุประสงค์ด้านยุทธศาสตร์
- วัตถุประสงค์ด้านดำเนินงาน / การรายงาน / กฎหมาย
- วัตถุประสงค์ระดับกิจกรรม , ระดับแผนก , ระดับบุคลากร

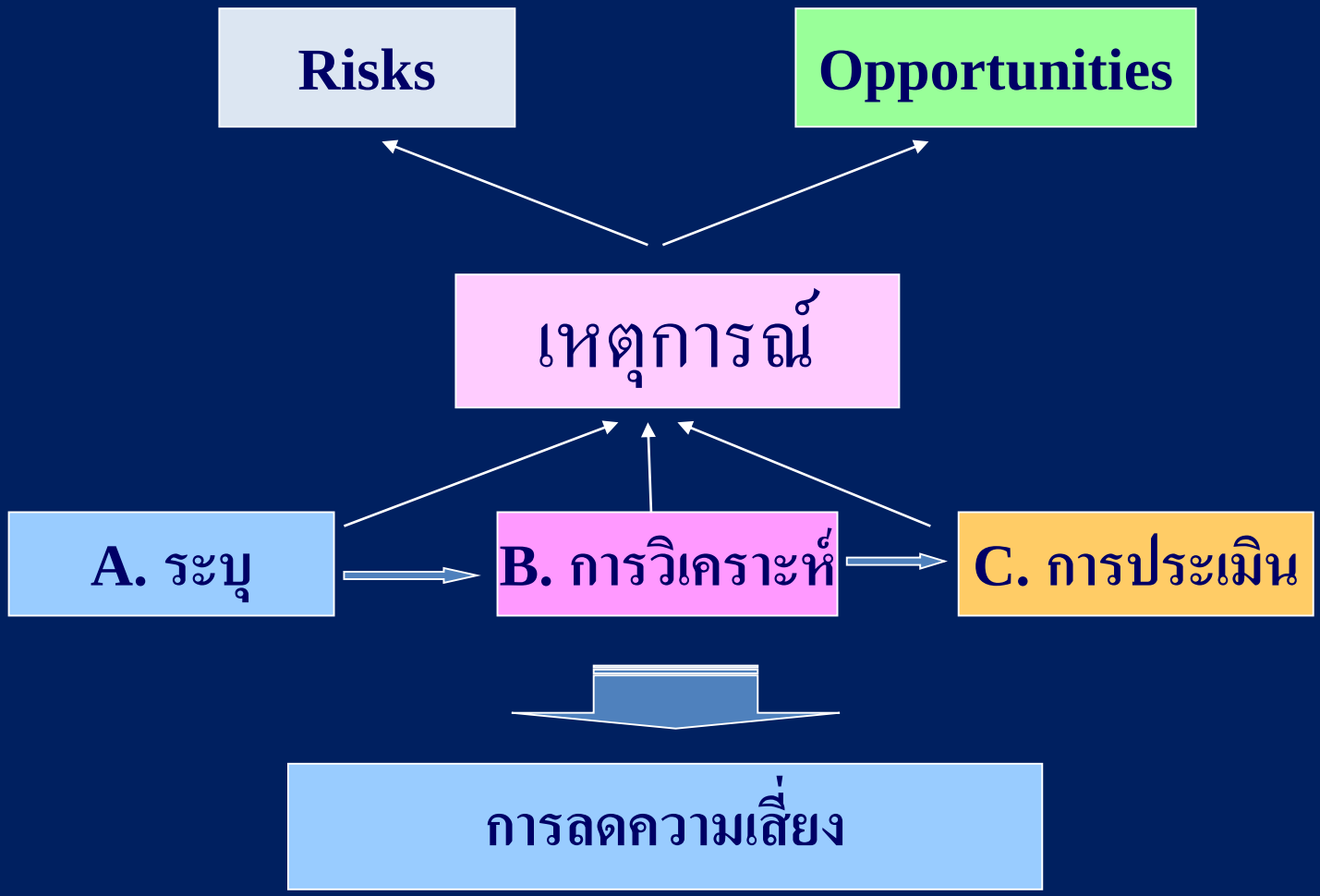
3. การระบุเหตุการณ์

- การค้นหาหรือชี้ให้เห็นความเสี่ยง
- เหตุการณ์ที่อาจมีผลต่อยุทธศาสตร์และการบรรลุเป้าหมาย
- ปัจจัยทั้งภายในและภายนอกที่อาจผนวกกันจนเป็นผลต่อระดับความเสี่ยง
- แยกแยะความเสี่ยงและโอกาส
  - เหตุการณ์ที่ส่งผลลบคือความเสี่ยง
  - เหตุการณ์ที่ส่งผลบวกหรือคือโอกาสหรือสัญญาณการเปลี่ยนแปลงที่ควรนำไปสู่การวางแผนกลยุทธ์ต่อไป

4. การประเมินความเสี่ยง

- ประเมินจากสองมิติคือ ความน่าจะเป็นและผลกระทบ
- ประเมินผลกระทบที่เกิดกับวัตถุประสงค์
- ประเมินทั้งเชิงปริมาณและคุณภาพ
- ประเมินทั้งเชิงบวกและเชิงลบ

การประเมินความเสี่ยง



เทคนิคในการระบุความเสี่ยง

การระดมกำลังสมองจากกลุ่ม

การใช้ checklist ในกรณีที่มีข้อจำกัดด้านงบประมาณและทรัพยากร

แผนภูมิการไหล การวิเคราะห์ระบบ การวิเคราะห์โครงข่าย

เทคนิค"what-if" การวิเคราะห์สถานการณ์

5. การสนองตอบ (จัดการ) ต่อความเสี่ยง

- ผู้บริหารตัดสินใจว่า จะจัดการกับความเสี่ยงอย่างไร
  - Avoid (Terminate) ลดโอกาสที่จะเกิดให้เหลือศูนย์ (หลีกเลี่ยง)
  - Accept (Take) ยอมรับความเสี่ยงนั้น (เฝ้าระวัง)
  - Prevent (Treat) ลดโอกาสที่จะเกิดให้น้อยลง (ควบคุม)
  - Reduce (Treat) ลดปริมาณความเสียหายให้น้อยลง (ควบคุม)
  - Share ร่วมกันรับความเสี่ยงกับองค์กรอื่น หรือคนอื่น
  - Transfer โอนความเสี่ยงไปให้องค์กรอื่น หรือคนอื่น

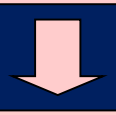
5. การสนองตอบ (จัดการ) ต่อความเสี่ยง (ต่อ)

- การประเมินทางเลือกดูจาก
  - ระดับความเสี่ยงที่องค์กรยอมรับได้
  - ผลที่ได้
  - ต้นทุน

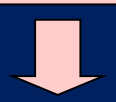
  } จุดคุ้มทุน

5. การสนองตอบ (จัดการ) ต่อความเสี่ยง (ต่อ)

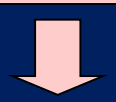
ปัจจัยภายนอก



การบริหารความเสี่ยง



หลีกเลี่ยง / ยอมรับ



แบ่ง / โอน

ปัจจัยภายใน

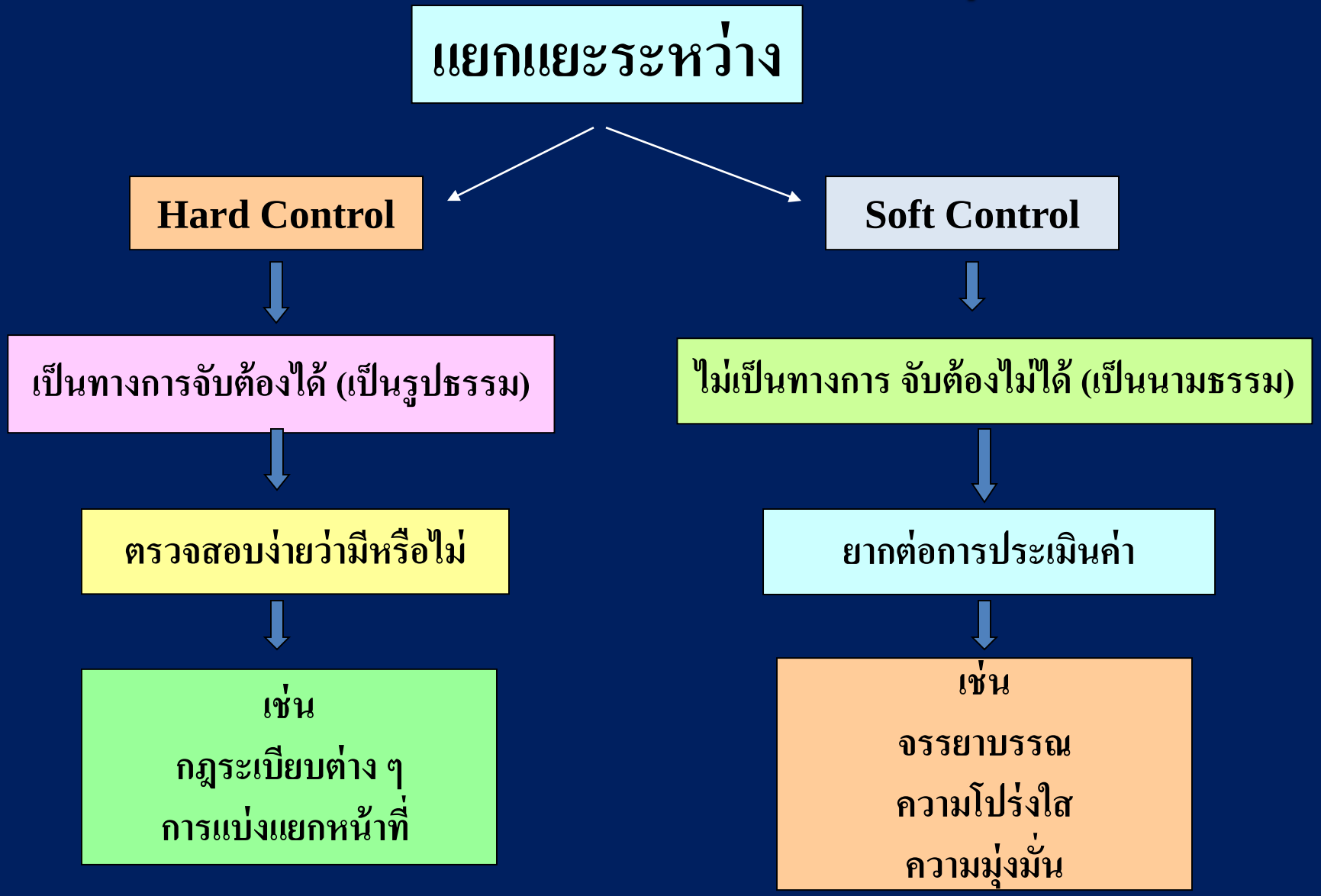
การควบคุม

ลดปริมาณความเสี่ยง / ลดโอกาสที่จะเกิด

6. กิจกรรมการควบคุม

- นโยบายและกฎระเบียบขั้นตอนที่จะช่วยให้การจัดการกับความเสี่ยงเกิดประสิทธิผล
- เป็นการปฏิบัติในทุกหน่วยงานและทุกระดับ
- การควบคุมทั้งปฏิบัติการและสารสนเทศ
- สัมพันธ์กับรูปแบบและวัฒนธรรมภายใน

ประเภทของการควบคุม



การควบคุมที่ดี 10 ประการ

1. มีการมอบหมายความรับผิดชอบในองค์กรระดับสูงสำหรับการควบคุมอย่างเป็นทางการ
2. มีคู่มือความประพฤติของบุคลากรในองค์กร
3. มีมาตรการจัดการกับผลประโยชน์ทับซ้อน
4. มีระบบการอนุมัติที่รัดกุมชัดเจน
5. มีการลงโทษโดยอัตโนมัติสำหรับความผิดร้ายแรง
6. มีระบบให้รางวัลเมื่อทำดี
7. มีการบังคับลาพักร้อน
8. มีการหมุนเวียนหน้าที่
9. มีการทำสัญญาค้ำประกันในการทำงานกับบุคลากรทุกคน
10. มีการเก็บรักษาเอกสารและบันทึกอย่างมีมาตรฐาน

7. สารสนเทศและการติดต่อสื่อสาร

- สารสนเทศจำเป็นต้องใช้เพื่อช่วยสนับสนุนให้การปฏิบัติงาน ดำเนินไปได้อย่างมีประสิทธิภาพ ทันต่อเวลาและรูปแบบใช้ได้อย่างสะดวก
- การสื่อสารเป็นช่องทางที่เปิดให้ทั้งบุคคลภายในและภายนอก ติดต่อสื่อสารกับองค์กร

8. การติดตามประเมินผล

- ตามดูการเปลี่ยนแปลงปัจจัยเสี่ยงต่างๆ
- ดูการเปลี่ยนแปลงของโอกาสเกิดและผลกระทบ
- ดูการเปลี่ยนแปลงของจุดคุ้มทุนต่างๆ
- ติดตามอย่างสม่ำเสมอภายใต้กระบวนการของการรายงานข้อมูลและตัวชี้วัดในระบบความเสี่ยง เช่น ระดับน้ำเสีย การทำผิด สภาพคล่อง
- การทบทวนของฝ่ายจัดการในส่วนงานต่างๆ ผ่านรายงานการควบคุมภายในและแบบประเมิน CSA (Control self assessment) ซึ่งควรรายงานตามเงื่อนไขของความเสี่ยงที่เกี่ยวข้อง(Risk-weighted criteria)
- ระบบการตรวจสอบทั้งภายในและภายนอกซึ่งจะช่วยในการตรวจสอบประสิทธิผลของระบบบริหารความเสี่ยงในภาพรวม

เปรียบเทียบ ERM กับ COSO

(Enterprise Risk Management VS. The Committee of Sponsoring Organization of Treadway Commission)

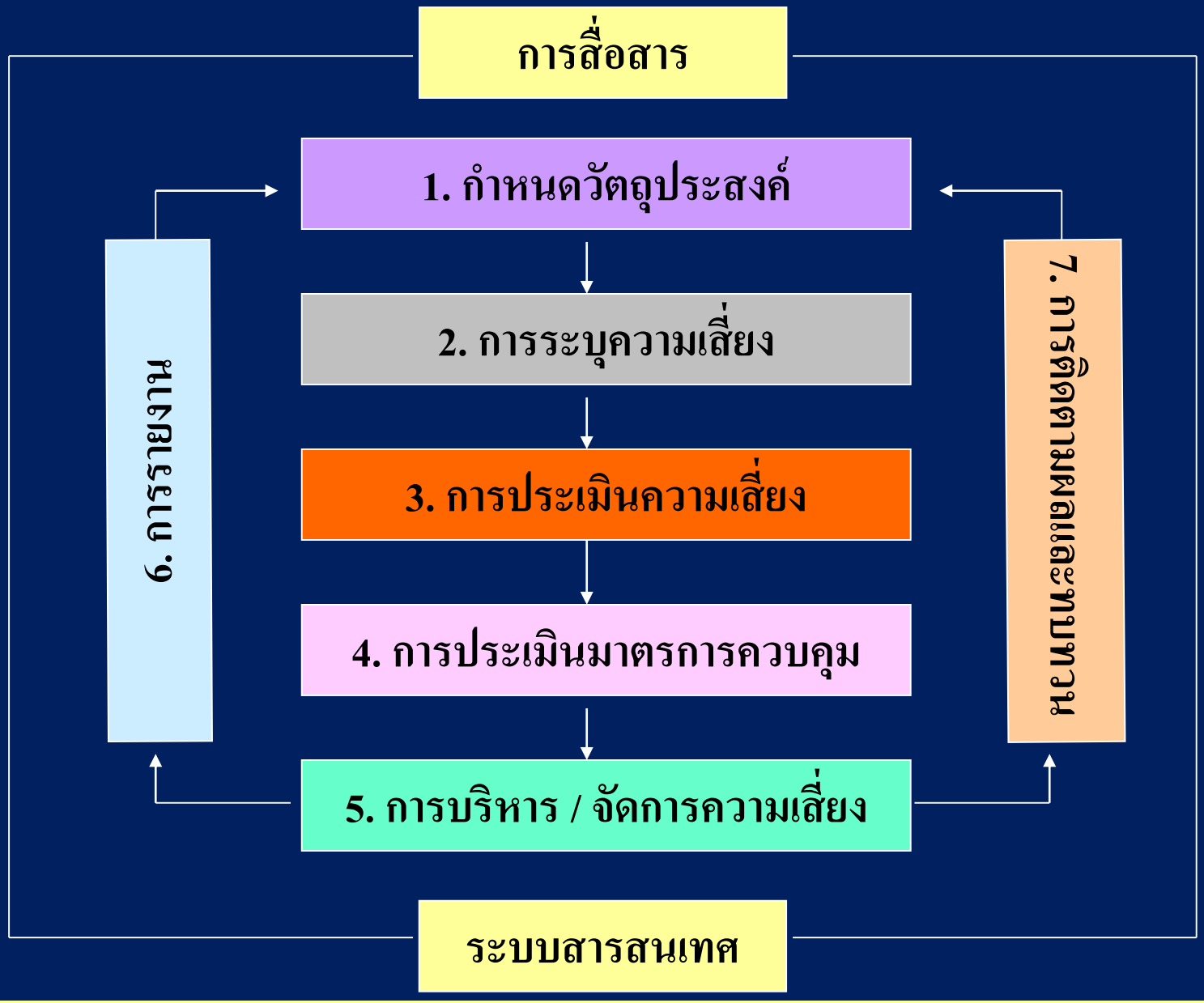
วัตถุประสงค์ ERM	*วัตถุประสงค์ COSO*
1. ยุทธศาสตร์	
2. ประสิทธิภาพ ประสิทธิผล	1. ประสิทธิภาพ ประสิทธิผล
3. ความเชื่อถือได้ของรายงาน	2. ความเชื่อถือได้ของรายงานทางการเงิน
4. การปฏิบัติตามกฎหมายและระเบียบต่าง ๆ	3. การปฏิบัติตามกฎหมายและระเบียบต่าง ๆ

เปรียบเทียบ ERM กับ COSO

(Enterprise Risk Management VS. The Committee of Sponsoring Organization of Treadway Commission)

องค์ประกอบ ERM	***องค์ประกอบ COSO***
1. สภาพแวดล้อม	1. สภาพแวดล้อมเพื่อการควบคุม
2. การตั้งเป้าประสงค์ขององค์กร	
3. การระบุเหตุการณ์ที่เสี่ยง	
4. การประเมินความเสี่ยง	2. การประเมินความเสี่ยง
5. การสนองตอบต่อความเสี่ยง	
6. กิจกรรมที่ใช้ในการควบคุม	3. กิจกรรมเพื่อการควบคุม
7. สารสนเทศและการสื่อสาร	4. ข้อมูลสารสนเทศและการติดต่อสื่อสาร
8. การติดตามผล	5. การติดตามผล

กระบวนการบริหารความเสี่ยง



Information Required

for

Risk Assessment and Internal Control Evaluation

Key Process (กระบวนการหลัก)	Objectives (วัตถุประสงค์)	Risk Outcome (ผลลัพธ์ของความเสี่ยง)	Risk Cause (สาเหตุของความเสี่ยง)	Desirable Control (การควบคุมที่ควรจะมี)	Control Existed? (การควบคุมที่มีอยู่ ?)	Control Working? (การควบคุมใช้ได้หรือไม่ ?)
Critical path for a system life cycle. Key functions that help a system achieves its mission.	What the process try to achieved? What are the key success criteria for the process?	The outcomes of the process that we do not want to happen. They are indicators of a process failure.	The event that cause or lead to the undesirable outcomes.	Things that should be in place to reduce the likelihood and/or consequence of the undesirable events to an acceptable level.	Verify whether the desirable controls are actually being implemented in the system.	Verify whether the existed controls are producing results as intended.

ข้อจำกัดของกระบวนการบริหารความเสี่ยง

- ความเสี่ยงมีความเกี่ยวข้องกับอนาคต ซึ่งมีความไม่แน่นอน
- การบริหารความเสี่ยงจะต้องมีการปฏิบัติใช้ในหลายระดับที่แตกต่างกัน โดยมีความสอดคล้องกับวัตถุประสงค์ที่แตกต่างกัน (กลยุทธ์ , การดำเนินงาน , การรายงาน และการปฏิบัติตามกฎ)
- การบริหารความเสี่ยงไม่สามารถทำให้มั่นใจได้ 100% ว่า องค์กรจะบรรลุวัตถุประสงค์ที่กำหนดไว้ เพราะมีปัจจัยของข้อจำกัด ดังนี้
  - การใช้ดุลพินิจในการตัดสินใจ (Judgement)
  - ความล้มเหลวหรือข้อบกพร่องของระบบการควบคุมภายใน อันเกิดจากความประมาทเลินเล่อ และความเข้าใจของบุคลากร (Breakdown)
  - การแทรกแซงโดยฝ่ายบริหาร (Management Override)
  - การสมรู้ร่วมคิด (Collusion)
  - ความคุ้มค่าของต้นทุน และผลประโยชน์ที่จะได้รับ (Cost & Benefit)

Risk Intelligence capability model

1.Tribal&Heroic (ทำคนเดียว)	2. Specialist silos (ผู้เชี่ยวชาญ)	3. Top-down (บน-ล่าง)	4. Systematic (เชิงระบบ)	5. Risk intelligent
Ad-hoc/Chaotic; depends primarily on individual heroics,capabilities and verbal wisdom ดำเนินการเพียงคนเดียว	Reaction to adverse events by specialists Discrete roles established for small set of risks Typically finance, insurance, compliance ต่างฝ่ายต่างแยกส่วนกันทำ ในแต่ละด้าน ไม่มีการเชื่อมโยงกัน	Tone set at the top Policies, procedures, risk authorities defined and communicated Business function Primarily qualitative Reactive นโยบาย บทบาท หลักเกณฑ์ กำหนดและสั่งการโดยผู้บริหารระดับสูง	Integrated response to adverse events Performance-linked metrics Rapid escalation Cultural, transformation Underway Bottom-up Proactive ระบบการบริหารแบบ Top-up เน้นระบบการคิดเชิงรุก	Built into decision-making Conformance with enterprise risk management process is incentivized Intelligent risk-taking Sustainable “Risk management is everyone’s job” 1.กำหนดให้ส่วนหนึ่งของการตัดสินใจ 2.มีการสร้างแรงจูงใจในการบริหารความเสี่ยง 3.สามารถยอมรับได้อย่างชาญฉลาด 4.เป็นหน้าที่ของบุคลากรทุกคน

Un-rewarded risk → **Rewarded risk**

ที่มา : Deloitte Touche Tohmatsu Jaiyos Advisory Co.,Ltd.

บทสรุป : ข้อมูลที่ควรรู้ก่อนการประเมินความเสี่ยง

1. ความเสี่ยงรอบโลก / ความเสี่ยงที่น่ากังวล / ความเสี่ยงที่ร้ายแรง
2. ความเสี่ยงตามแผนบริหารความเสี่ยงปีที่ผ่านมา
3. ผลการดำเนินงานตามแผนการบริหารความเสี่ยงปีที่ผ่านมา
4. ผลการดำเนินงานตามแผนยุทธศาสตร์ / แผนปฏิบัติราชการปีที่ผ่านมา
5. ข้อคิดเห็นของผู้มีส่วนได้ส่วนเสีย

http://www.prachachat.net/news_detail.php?newsid=1327377666&grpid=09&catid=no

ความเสี่ยงที่น่ากังวล

- ความเปลี่ยนแปลงของตลาด
- ความพร้อมในการรับมือกับวิกฤติการณ์
- การเปลี่ยนแปลงนโยบายของรัฐบาล
- การสืบทอดตำแหน่ง CEO
- การปฏิบัติตามกฎหมายข้อบังคับของทางการ
- คุณภาพการผลิต
- ขาดสมรรถภาพและความเพรียบพร้อมของระบบในองค์กร
- ความเสี่ยงทางการเงิน
- การสูญเสียทรัพย์สินทางปัญญา
- มีคู่แข่งรายใหม่
- ความเสื่อมเสียชื่อเสียงขององค์กร
- ความหลากหลายของธุรกิจ
- คณะกรรมการไร้ความสามารถขาดความรู้ความชำนาญ
- การบริหารความเสี่ยงขาดคุณภาพ

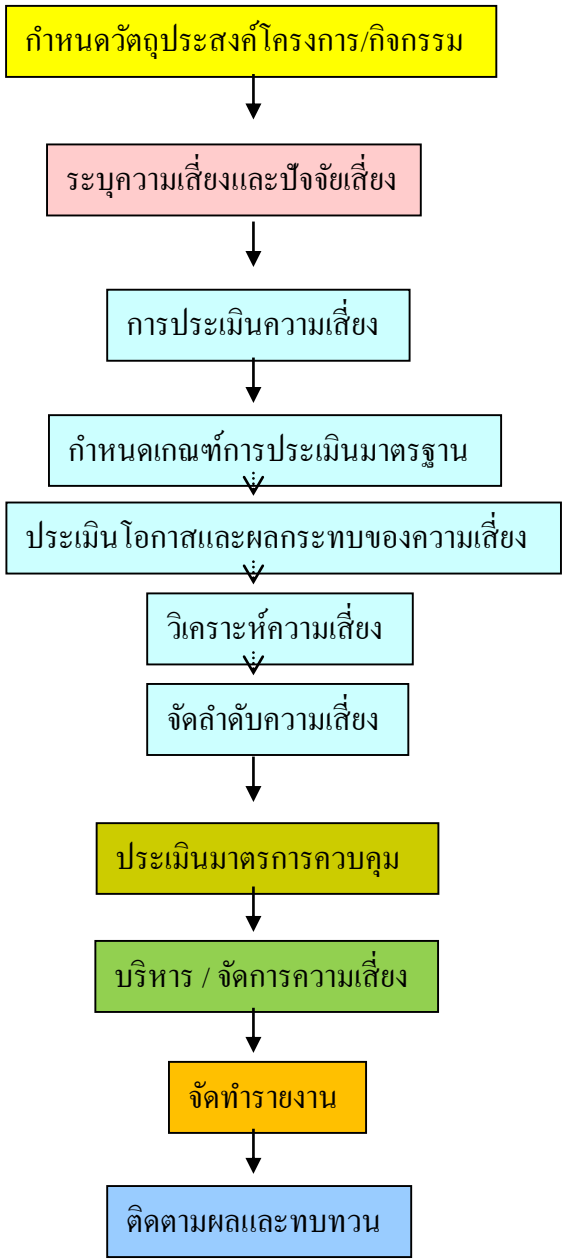
ที่มา : ผลการวิจัยโดย Nell Buek and Associated Ply.Ltd.

ความเสี่ยงร้ายแรง

1. มีการเสียชีวิตและถูกทำร้ายร่างกายหรือจิตใจอย่างรุนแรงของบุคลากรภายในองค์กร ทั้งๆ ที่อยู่ในวิสัยที่องค์กรสามารถป้องกันหรือลดผลกระทบในเหตุการณ์ที่เกิดขึ้นได้ แต่ไม่พบแผนการจัดการความเสี่ยงหรือไม่พบความพยายามขององค์กรในการระงับเหตุการณ์ดังกล่าว
2. องค์กรเสื่อมเสียชื่อเสียงหรือมีภาพลักษณ์ที่ไม่ดี อันเนื่องมาจากปัจจัยต่างๆ หรือบุคลากรขาดจริยธรรม จรรยาบรรณการไม่ปฏิบัติตามมาตรฐานหรือกฎหมาย และเกิดเป็นข่าวปรากฏให้เห็นตามสื่อต่าง ๆ เช่น หนังสือพิมพ์ ข่าว online เป็นต้น
3. องค์กรขาดสภาพคล่องในด้านการเงิน

เทคนิคการนำกรอบ ERM สู่การปฏิบัติ

สรุปขั้นตอนและแบบฟอร์มการบริหารความเสี่ยงและควบคุมภายใน



KU-ERM 1 "Key Process"

KU-ERM 2 "Objectives"

KU-ERM 3 "Risk"

KU-ERM 6 "แบบการประเมินความเสี่ยง" ช่อง 4

KU-ERM 4 "เกณฑ์มาตรฐานระดับโอกาสที่จะเกิดความเสี่ยง"
"เกณฑ์มาตรฐานระดับความรุนแรงของผลกระทบ"

KU-ERM 5 "เกณฑ์มาตรฐานระดับของความเสี่ยง"

KU-ERM 6 "แบบการประเมินความเสี่ยง" ช่อง 5,6

KU-ERM 6 "แบบการประเมินความเสี่ยง" ช่อง 7

KU-ERM 5(1) "Risk Map"

KU-ERM 6 "แบบการประเมินความเสี่ยง" ช่อง 8

KU-ERM 7 "แบบการประเมินการควบคุม"

KU-ERM 8 "แบบสรุปการจัดการความเสี่ยง"

"แผนบริหารความเสี่ยง"

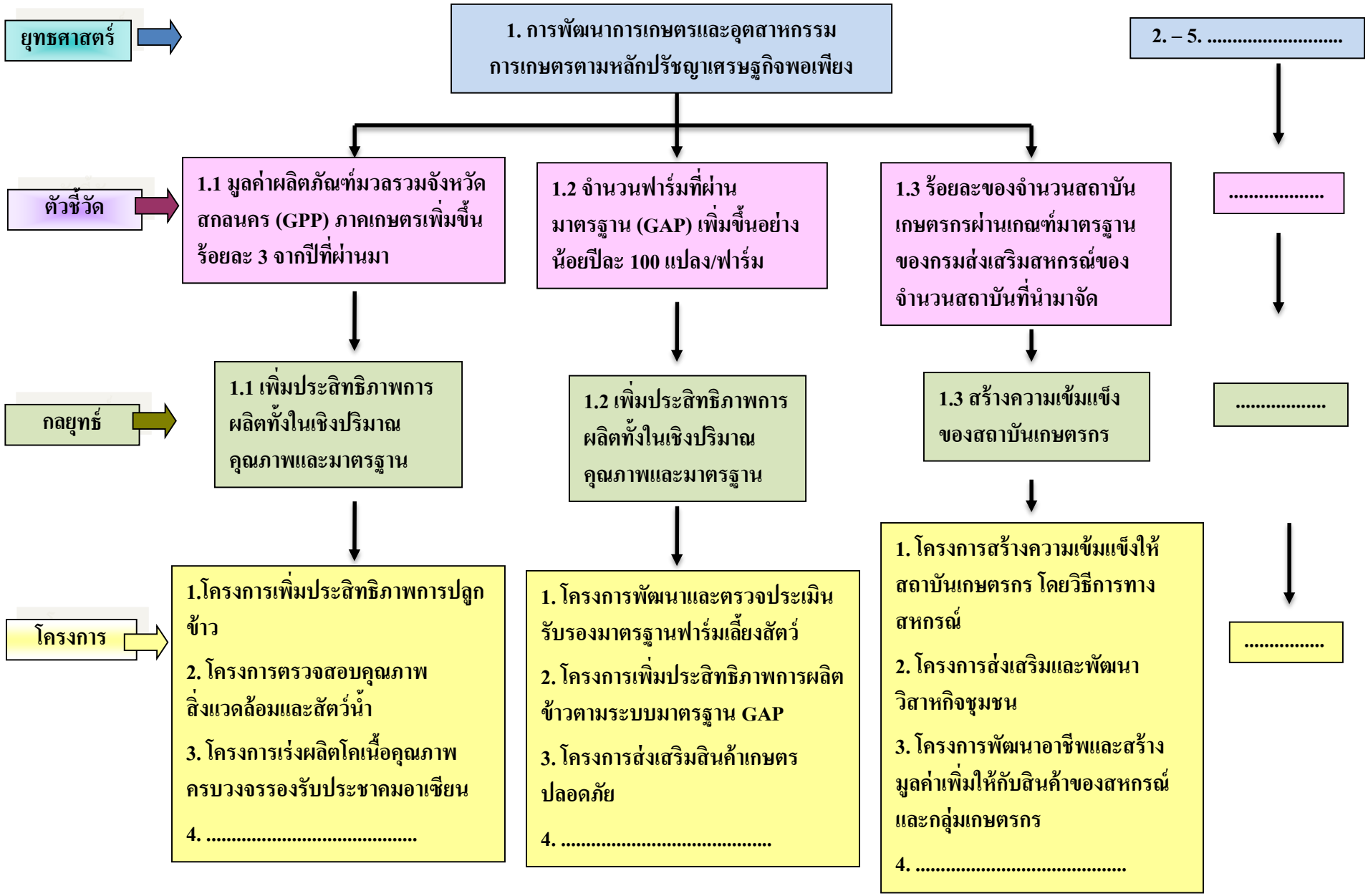
"แบบติดตามผลการบริหารความเสี่ยง

ขั้นตอนที่ 1
การกำหนดวัตถุประสงค์โครงการ / กิจกรรม

หลักการ / วิธีการคัดเลือกโครงการ / กิจกรรม

1. โครงการ / กิจกรรมที่มีความสำคัญต่อภารกิจหลักขององค์กรและมีผลกระทบต่อผู้มีส่วนได้ส่วนเสีย
2. โครงการ / กิจกรรมที่มีผลการดำเนินงานต่ำกว่าเป้าหมายตามแผนยุทธศาสตร์ แผนปฏิบัติราชการ 4 ปี
3. โครงการ / กิจกรรมที่ต้องการเพิ่มผลผลิตมากกว่าเป้าหมายในปีที่ผ่านมา
4. โครงการ / กิจกรรมที่ได้รับงบประมาณจำนวนมากที่สุด

ยุทธศาสตร์จังหวัดสกลนคร



ระดับของการกำหนดวัตถุประสงค์

★ *วัตถุประสงค์ในระดับองค์กร (Entity –Level Objectives)*

เป็นวัตถุประสงค์ของการดำเนินงานในภาพรวมขององค์กร โดยทั่วไปวัตถุประสงค์ในระดับองค์กรจะระบุไว้ในแผนกลยุทธ์ และการปฏิบัติงานประจำปีขององค์กร

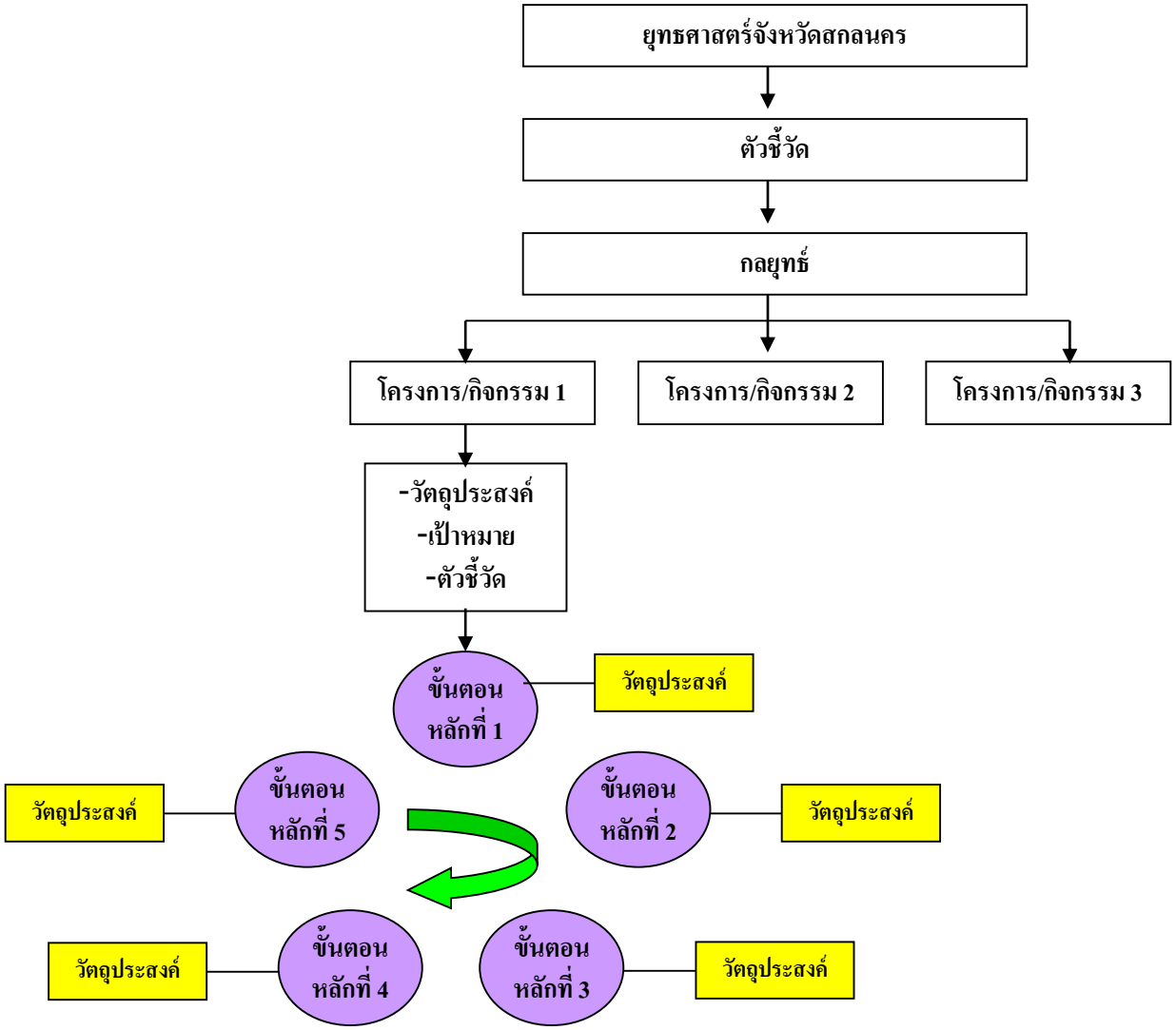
★ *วัตถุประสงค์ในระดับกิจกรรม (Activity-Level Objectives)*

เป็นวัตถุประสงค์ของการดำเนินงานที่เฉพาะเจาะจงลงไปสำหรับแต่ละกิจกรรมที่องค์กรกำหนดเพื่อให้บรรลุวัตถุประสงค์ขององค์กร ซึ่งวัตถุประสงค์ของแต่ละกิจกรรมจะต้องสนับสนุนและสอดคล้องกับวัตถุประสงค์ในระดับองค์กร

★ *วัตถุประสงค์ในระดับขั้นตอนหลักของกิจกรรม (Key Process Objectives)*

เป็นวัตถุประสงค์ของแต่ละขั้นตอนหลักของแต่ละกิจกรรม ที่ผู้ปฏิบัติกำหนดขึ้น เพื่อให้บรรลุวัตถุประสงค์ของกิจกรรม ซึ่งวัตถุประสงค์ของแต่ละขั้นตอนหลักต้องสนับสนุนและสอดคล้องกับวัตถุประสงค์ของกิจกรรม

ความสัมพันธ์ของวัตถุประสงค์ระดับองค์กร หน่วยงาน โครงการและกระบวนการหรือขั้นตอนหลัก



วัตถุประสงค์

คืออะไร?

- สิ่งที่ตอบสนองหรือเป็นผลลัพธ์ของการดำเนินการ
- วัตถุประสงค์จึงไม่ใช่วิธีการ
- และไม่ใช่เครื่องมือหรือการดำเนินการ
- อาจเป็นข้อบังคับของหน่วยงาน

เทคนิคการกำหนดวัตถุประสงค์

Strategic ยุทธศาสตร์ (KPI ตามแผนยุทธศาสตร์ แผนปฏิบัติราชการ 4 ปี แผนปฏิบัติราชการประจำปี และตามคำรับรองการปฏิบัติราชการ)

Operations ประสิทธิภาพและประสิทธิผลการปฏิบัติงาน

Reporting หรือ ***Financial*** ความครบถ้วนถูกต้องและเชื่อถือได้ของข้อมูลทางการเงินและข้อมูลต่าง ๆ

Compliance การปฏิบัติตามกฎหมายและกฎระเบียบที่เกี่ยวข้อง

+ ธรรมาภิบาล ------ โปร่งใส เป็นธรรม มีส่วนร่วม ฯลฯ

+ ความปลอดภัยในชีวิต / ทรัพย์สิน

หลักการกำหนดวัตถุประสงค์

SMART

1. Specific ชัดเจน
2. Measurable วัดได้
3. Achievable ปฏิบัติได้
4. Reasonable สมเหตุสมผล
5. Time constrained กรอบเวลา

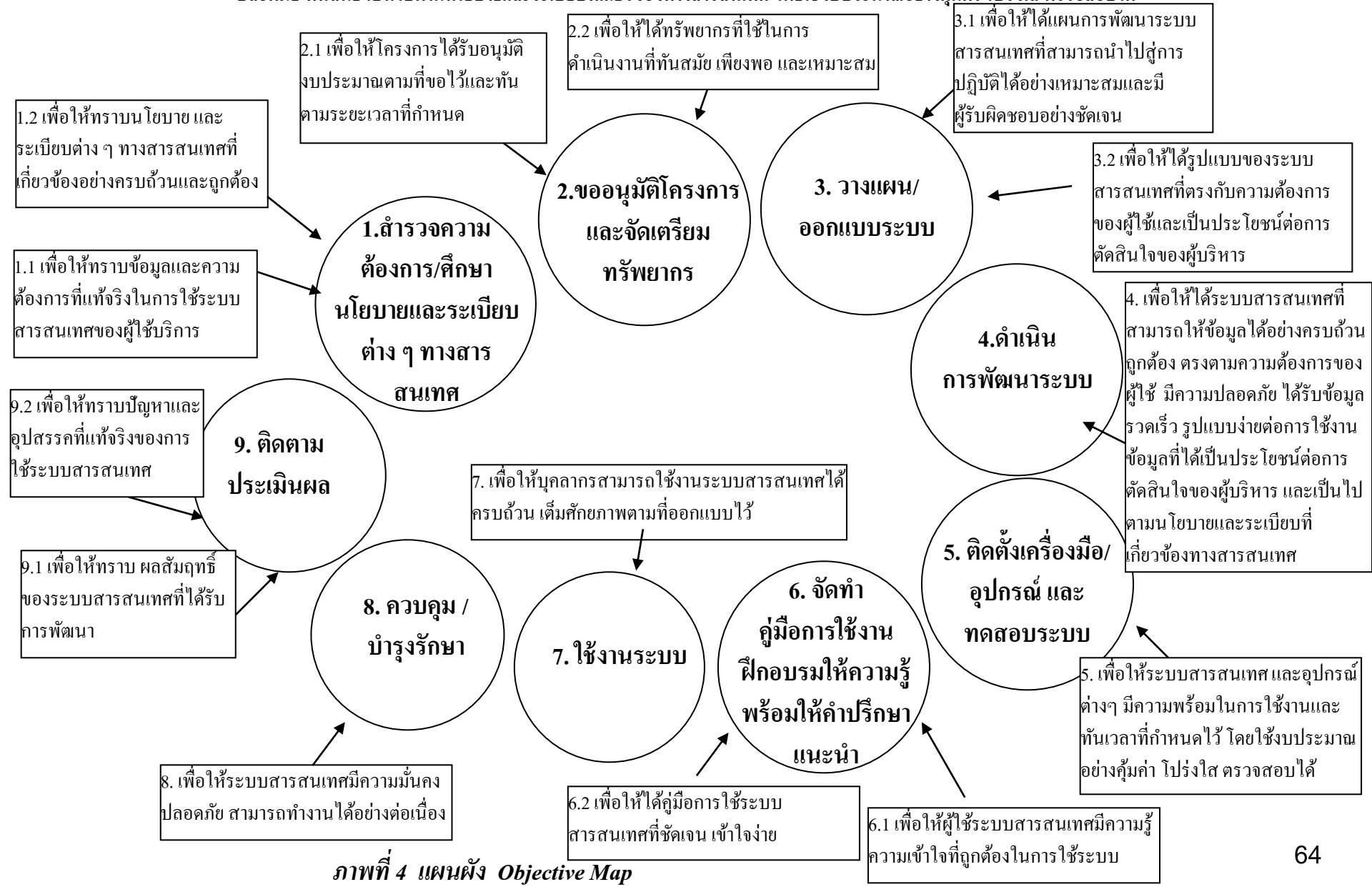
(ตัวอย่าง) โครงการการพัฒนาระบบสารสนเทศ

วัตถุประสงค์ : เพื่อให้ระบบสารสนเทศสามารถให้ข้อมูลได้อย่างครบถ้วนถูกต้อง เป็นปัจจุบัน ตรงความต้องการของผู้ใช้ เป็นประโยชน์ต่อการตัดสินใจของผู้บริหาร มีรูปแบบการใช้งานที่ง่าย ปลอดภัย ทันสมัย เป็นไปตามนโยบายและระเบียบที่เกี่ยวข้องทางสารสนเทศ โดยใช้งบประมาณอย่างคุ้มค่าโปร่งใส ตรวจสอบได้

แผนผัง Key Process

(ตัวอย่าง) โครงการพัฒนาระบบสารสนเทศ

วัตถุประสงค์ : เพื่อให้ระบบสารสนเทศสามารถให้ข้อมูลได้อย่างครบถ้วนถูกต้อง เป็นปัจจุบัน ตรงความต้องการของผู้ใช้ เป็นประโยชน์ต่อการตัดสินใจของผู้บริหาร มีรูปแบบการใช้งานที่ง่าย ปลอดภัย ทันสมัย เป็นไปตามนโยบายและระเบียบที่เกี่ยวข้องทางสารสนเทศ โดยใช้งบประมาณอย่างคุ้มค่า โปร่งใส ตรวจสอบได้



ภาพที่ 4 แผนผัง Objective Map

ขั้นตอนที่ 2
การระบุความเสี่ยงและปัจจัยเสี่ยง

เทคนิคการระบุความเสี่ยง

1. เป็นผลของความเสี่ยง (Risk Outcome)
2. ตรงกันข้ามกับวัตถุประสงค์

   S ความเสี่ยงเชิงยุทธศาสตร์ “โครงการ / กิจกรรม ไม่บรรลุเป้าหมาย KPI ตามแผนยุทธศาสตร์”

   O ความเสี่ยงด้านการปฏิบัติงาน “กระบวนการไม่มีประสิทธิภาพ / ประสิทธิผล”

   R (F) ความเสี่ยงด้านความไม่ครบถ้วนถูกต้องของข้อมูลการเงินและอื่น ๆ

   C ความเสี่ยงการไม่ปฏิบัติตามกฎระเบียบ ข้อบังคับ

3. หลักธรรมาภิบาล 9 ประการ (การมีส่วนร่วม , นิติธรรม , ความโปร่งใส , การตอบสนอง , การมุ่งเน้นฉันทามติ , ความเสมอภาค / ความเที่ยงธรรม , ประสิทธิผลและประสิทธิภาพ , ภาระรับผิดชอบ , วิสัยทัศน์เชิงยุทธศาสตร์)

เทคนิคการระบุปัจจัยเสี่ยง

1. เป็นสาเหตุของความเสี่ยง
2. พิจารณาปัจจัยเสี่ยงทั้งภายในและภายนอกองค์กร
3. พิจารณาจาก 8 องค์ประกอบ ของ ERM อาทิ สภาพแวดล้อมภายใน การสื่อสารและสารสนเทศ การติดตามประเมินผล เป็นต้น
4. พิจารณาจากขั้นตอนย่อยของการปฏิบัติงานแต่ละขั้นตอนหลัก
5. หลักธรรมาภิบาล 9 ประการ

ตัวอย่าง ความเสี่ยงหรือผลของความเสี่ยง

- ☹ การตัดสินใจที่ผิดพลาดจากการใช้ข้อมูลที่ไม่ถูกต้อง ไม่สมบูรณ์หรือไม่เป็นปัจจุบัน
- ☹ การบันทึกบัญชีผิดพลาด
- ☹ การปฏิบัติงานไม่มีประสิทธิภาพและประสิทธิผล (ไม่คุ้มค่า ต้นทุนสูง หรือใช้เวลานาน ฯลฯ)
- ☹ เกิดการทุจริตในองค์กร
- ☹ สูญเสียทรัพยากร
- ☹ รายงานทางการเงินไม่น่าเชื่อถือ
- ☹ เกิดความเสียหายต่อชื่อเสียงของหน่วยงาน
- ☹ การไม่ปฏิบัติตามกฎระเบียบ วิธีปฏิบัติงาน กฎหมาย
- ☹ การใช้ทรัพยากรที่ไม่ประหยัด,ไม่มีประสิทธิภาพ

ตัวอย่าง
ปัจจัยความเสี่ยง / ต้นเหตุ / สาเหตุของความเสี่ยง

- บรรยากาศทางจริยธรรม
- ความกดดันจากฝ่ายบริหาร
- ความรู้ ความสามารถของบุคลากร
- ราคาทรัพย์สิน
- ความสามารถในการเปลี่ยนเป็นตัวเงินของทรัพย์สิน
- ปริมาณการบันทึกรายการและจำนวนเอกสาร
- สภาพความเป็นจริงทางการเงินและเศรษฐกิจ
- สภาพความเป็นจริงในการแข่งขัน

ตัวอย่าง
ปัจจัยความเสี่ยง / ต้นเหตุ / สาเหตุของความเสี่ยง (ต่อ)

- กิจกรรมที่ซับซ้อนหรือมีการเปลี่ยนแปลงได้ง่าย
- ระเบียบต่างๆของทางราชการ
- ระบบข้อมูลสารสนเทศที่ประมวลผลด้วยคอมพิวเตอร์
- การกระจายของสถานที่ในการปฏิบัติงาน
- ความเพียงพอและประสิทธิผลของการควบคุมภายใน
- การเปลี่ยนแปลงองค์กร,การปฏิบัติงาน,เทคโนโลยี
- การตัดสินใจของฝ่ายบริหาร

ตัวอย่าง
ปัจจัยความเสี่ยง / ต้นเหตุ / สาเหตุของความเสี่ยง (ต่อ)

- การประมาณการด้วยตัวเลขทางบัญชี
- การยอมรับสิ่งที่ตรวจพบ
- ความไม่ทันการณ์ของการติดตามและบอกเหตุ
- ขาดการรายงานและติดตามผลอย่างสม่ำเสมอ
- ขาดขวัญและกำลังใจ
- การประเมินผลงานไม่เป็นธรรม

ฯลฯ

ตัวอย่าง ความเสี่ยง / ปัจจัยเสี่ยง ด้านธรรมาภิบาล

ความเสี่ยง (ผลกระทบของความเสี่ยง)	ปัจจัยเสี่ยง
<u>ด้านธรรมาภิบาล</u> 1.เจ้าหน้าที่และ/หรือผู้บริหารไม่มีความซื่อสัตย์	1.1 มีการใช้อำนาจหน้าที่เพื่อเอื้อประโยชน์ต่อพวกพ้อง 1.2 มีการใช้ช่องโหว่ทางกฎหมายเพื่อแสวงหาประโยชน์ส่วนตัว
2.การดำเนินงานของโครงการฯ/กิจกรรมขาดความโปร่งใส	2.1 ไม่เปิดเผยข้อมูลและขั้นตอนการดำเนินการของโครงการฯ/กิจกรรม 2.2 การเปิดเผยข้อมูลไม่ครบถ้วน มีการบิดเบือนข้อมูล 2.3 ไม่เปิดเผยข้อมูลเพื่อการตรวจสอบการทำงาน
3.เจ้าหน้าที่และ/หรือผู้บริหารไม่มีความยุติธรรม	3.1 มีการปฏิบัติต่อผู้รับบริการอย่างไม่เป็นธรรมและไม่เสมอภาค 3.2 มีการเอื้อประโยชน์ให้กับกลุ่มใด กลุ่มหนึ่งเป็นพิเศษ
4.เจ้าหน้าที่และ/หรือผู้บริหารขาดความสามัคคี	4.1 มีการแบ่งพรรคแบ่งพวกในการทำงาน 4.2 ไม่ให้ความร่วมมือในการทำงาน

ตัวอย่าง ความเสี่ยง / ปัจจัยเสี่ยง ด้านธรรมาภิบาล

ความเสี่ยง (ผลกระทบของความเสี่ยง)	ปัจจัยเสี่ยง
5.การดำเนินงานของโครงการฯ/กิจกรรม ไม่มีประสิทธิภาพ	5.1 มีการปฏิบัติงานที่ล่าช้ากว่ากำหนด 5.2 ขาดระบบและขั้นตอนการดำเนินการที่ชัดเจนและมีประสิทธิภาพ
6.เจ้าหน้าที่และ/หรือผู้บริหารขาดความรับผิดชอบต่อการตัดสินใจในการปฏิบัติงานและผลที่เกิดขึ้น	6.1 มีการโยนความผิดให้แก่ผู้อื่น 6.2 ไม่ยินดีให้มีการตรวจสอบ 6.3 ไม่รับผิดชอบต่อผลที่เกิดขึ้น
7.การดำเนินงานของโครงการฯ /กิจกรรมไม่มุ่งเน้นผลสำเร็จของงาน	7. ขาดเป้าหมายและแผนงานในการดำเนินการที่ชัดเจน
8.การดำเนินงานของโครงการฯ /กิจกรรมขาดความคล่องตัว	8. เจ้าหน้าที่และ/หรือผู้บริหารไม่ปรับตัวต่อการเปลี่ยนแปลงทางเศรษฐกิจ สังคมและสิ่งแวดล้อม
9.เจ้าหน้าที่และ/หรือผู้บริหารมีการทุจริตคอรัปชั่น	9. เจ้าหน้าที่และ/หรือผู้บริหารรับสินบนในการทำงาน

ตัวอย่างความเสี่ยงของโครงการ

- ไม่เปิดโอกาสให้ผู้มีส่วนได้ส่วนเสียแสดงความคิดเห็น
- ขั้นตอนการศึกษา การออกแบบ การวิเคราะห์เป้าประสงค์ของโครงการไม่สามารถใช้งานได้จริง
- ภาพวาดและคำอธิบายเกี่ยวกับการออกแบบสิ่งปลูกสร้าง ไม่ชัดเจนและไม่ครอบคลุม
- ไม่มีความยืดหยุ่นในกรยอมรับการเปลี่ยนแปลงและมาตรฐานในการควบคุม
- ไม่มีตารางระยะเวลาในการก่อสร้างที่ชัดเจน และข้อมูลค่าใช้จ่ายต่างๆ ที่เกิดขึ้นในระหว่างก่อสร้างสูง
- การประกาศขอบเขตของงาน (TOR) และขั้นตอนการดำเนินการไม่แล้วเสร็จภายในปีงบประมาณ
- เกิดการร้องเรียนในประเด็นสาระสำคัญของ (TOR) เช่น ล็อคสเปค หรือ สินค้าด้อยคุณภาพ

ตัวอย่างความเสี่ยงของโครงการ

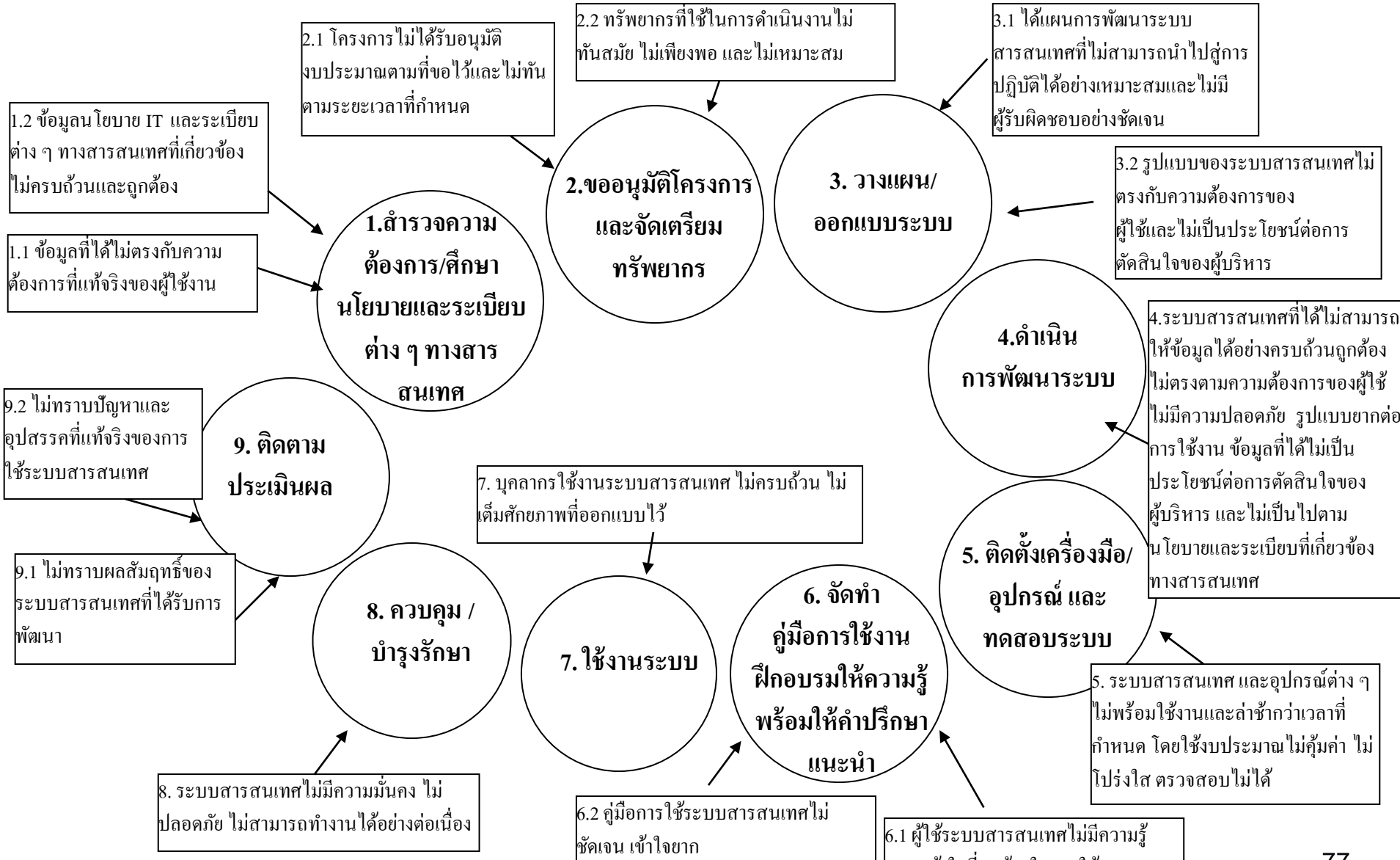
- ได้รับสินค้าไม่ตรงตามสเปคที่ตกลงกันไว้
- คุณภาพของงานไม่เป็นไปตามสัญญา
- ไม่ดำเนินการตามมาตรการด้านสิ่งแวดล้อมตามที่กฎหมายกำหนด
- ไม่ดำเนินการตามระเบียบพัสดุฯ
- ขาดการทำสัญญาการประกันภัย และเอกสรการกำกับดูแลที่ชัดเจน
- กระบวนการผลิตขาดประสิทธิภาพ ไม่มีการประสานงานและอุปสรรคที่เกิดขึ้น
- ไม่มีการทดสอบและการประกันคุณภาพ การตรวจสอบไม่ได้มาตรฐาน และไม่มีการบันทึกข้อมูลจุดที่ผิดพลาด
- การดำเนินงานล่าช้า

ตัวอย่างความเสี่ยงของโครงการ

- การเบิกจ่ายเงินให้ผู้รับจ้างล่าช้า
- งบกระแสเงินสดไม่เพียงพอ
- ขาดกระบวนการติดต่อประสานงานด้านธุรการ และขั้นตอนการอนุมัติล่าช้า
- ไม่มีรายงานกิจกรรมภาคสนามการตรวจสอบและการบันทึก
- ไม่ตรวจรับงานตามวัตถุประสงค์ของโครงการ
- ไม่มีระบบควบคุมและติดตามการรายงานผล
- ไม่มีการรายงานหรือติดตาม ปัญหาอุปสรรคในการดำเนินการ
- ไม่มีการติดตามและประเมินความสำเร็จของโครงการ หรือมีแต่ไม่เพียงพอ

(ตัวอย่าง) โครงการพัฒนาระบบสารสนเทศ

ความเสี่ยง : ระบบสารสนเทศให้ข้อมูลได้ไม่ครบถ้วนถูกต้อง ไม่เป็นปัจจุบัน ไม่ตรงความต้องการของผู้ใช้ ไม่เป็นประโยชน์ต่อการตัดสินใจของผู้บริหาร มีรูปแบบยากต่อการใช้งาน ไม่มีความปลอดภัย ล้าสมัย ไม่เป็นไปตามนโยบายและระเบียบที่เกี่ยวข้องทางสารสนเทศ ใช้งบประมาณไม่คุ้มค่า ไม่โปร่งใส ตรวจสอบไม่ได้



ภาพที่ 5 แผนผัง Risk Map

ตัวอย่าง การระบุความเสี่ยง

โครงการ *การพัฒนาระบบสารสนเทศ*

ความเสี่ยง : ระบบสารสนเทศให้ข้อมูลได้ไม่ครบถ้วนถูกต้อง ไม่เป็นปัจจุบัน ไม่ตรงความต้องการของผู้ใช้ ไม่เป็นประโยชน์ต่อการตัดสินใจของผู้บริหาร มีรูปแบบยากต่อการใช้งาน ไม่มีความปลอดภัย ล้าสมัย ไม่เป็นไปตามนโยบายและระเบียบที่เกี่ยวข้องทางสารสนเทศ ใช้งบประมาณไม่คุ้มค่า ไม่โปร่งใส ตรวจสอบไม่ได้

ขั้นตอน	วัตถุประสงค์ขั้นตอน	ความเสี่ยง	ปัจจัยเสี่ยง
1.สำรวจความต้องการ/ศึกษานโยบายและระเบียบต่าง ๆ ทางสารสนเทศ	1.1 เพื่อให้ทราบข้อมูลและความต้องการที่แท้จริงในการใช้ระบบสารสนเทศของผู้ใช้บริการ 1.2 เพื่อให้ทราบนโยบายและระเบียบต่าง ๆ ทางสารสนเทศที่เกี่ยวข้องอย่างครบถ้วนและถูกต้อง	1.1 ข้อมูลที่ได้ไม่ตรงกับความต้องการที่แท้จริงของผู้ใช้งาน 1.2 ข้อมูลนโยบาย IT และระเบียบต่าง ๆ ทางสารสนเทศที่เกี่ยวข้อง ไม่ครบถ้วนและถูกต้อง	1.1 ระยะเวลาในการสำรวจ / ศึกษาข้อมูลจำกัด 1.2 การสำรวจความต้องการของผู้ใช้บริการไม่ครอบคลุมทุกหน่วยงาน 1.3 เครื่องมือที่ใช้สำรวจข้อมูลความต้องการใช้ระบบ ไม่ได้มาตรฐาน ไม่ชัดเจนและไม่ครอบคลุมข้อมูลที่ต้องการ 1.4 บุคลากร / หน่วยงาน ไม่ให้ความร่วมมือในการให้ข้อมูลที่แท้จริง 1.5 ผู้บริหารให้ข้อมูลความต้องการใช้ระบบสารสนเทศไม่ชัดเจน 1.6 ไม่มีการรวบรวมข้อมูลกฎหมาย ระเบียบทางสารสนเทศที่ประกาศใช้และที่เปลี่ยนแปลงไว้ 1.7 หน่วยงานและบุคลากรไม่ได้รับแจ้งการเปลี่ยนแปลงกฎหมาย กฎเกณฑ์ที่เกี่ยวกับการใช้ระบบสารสนเทศ 1.8 นโยบายด้านสารสนเทศของหน่วยงานยังไม่ชัดเจน

ขั้นตอนที่ 3 การประเมินความเสี่ยง

3.1 กำหนดเกณฑ์การประเมินปัจจัยเสี่ยง (L / I)

3.2 ให้ค่าโอกาสและผลกระทบ

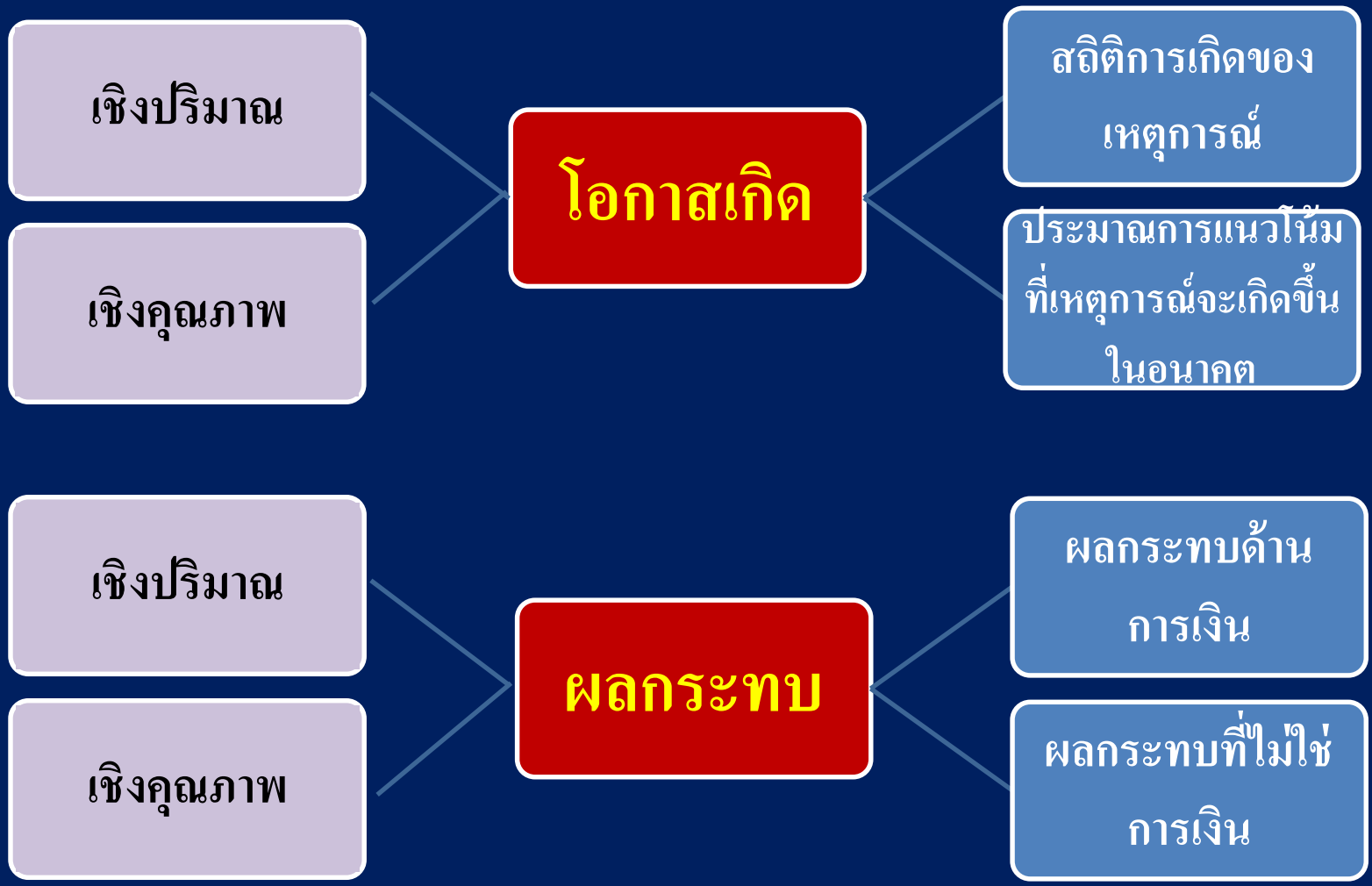
3.3 วิเคราะห์ความเสี่ยง (Plot ใน Risk Profile)

3.4 จัดลำดับปัจจัยเสี่ยง

ขั้นตอนที่ 3.1
การกำหนดเกณฑ์การประเมินมาตรฐาน

- ระดับโอกาสในการเกิดเหตุการณ์ต่าง ๆ (Likelihood)
- ระดับความรุนแรงของผลกระทบของความเสี่ยง (Impact)
- ระดับของความเสี่ยง (Degree of Risk / Risk Matrix)

ระดับความรุนแรงของปัจจัยเสี่ยง (Risk Factor)



ตัวอย่าง ระดับโอกาสในการเกิดเหตุการณ์ต่างๆ (Likelihood) ***เชิงปริมาณ***		
ระดับ	โอกาสที่จะเกิด	คำอธิบาย
5	สูงมาก	1 เดือนต่อครั้งหรือมากกว่า
4	สูง	1-6 เดือนต่อครั้งแต่ไม่เกิน 5 ครั้ง
3	ปานกลาง	1 ปีต่อครั้ง
2	น้อย	2-3 ปีต่อครั้ง
1	น้อยมาก	5 ปีต่อครั้ง

ตัวอย่าง ระดับโอกาสในการเกิดเหตุการณ์ต่างๆ (Likelihood) ***เชิงคุณภาพ***		
ระดับ	โอกาสที่จะเกิด	คำอธิบาย
5	สูงมาก	มีโอกาสในการเกิดเกือบทุกครั้ง
4	สูง	มีโอกาสในการเกิดค่อนข้างสูงหรือบ่อยๆ
3	ปานกลาง	มีโอกาสเกิดบางครั้ง
2	น้อย	อาจมีโอกาสเกิดแต่นานๆ ครั้ง
1	น้อยมาก	มีโอกาสเกิดในกรณียกเว้น

ตัวอย่าง ระดับความรุนแรงของผลกระทบของความเสี่ยง (Impact) ***เชิงปริมาณ***		
ระดับ	ผลกระทบ	คำอธิบาย
5	สูงมาก	> 10 ล้านบาท
4	สูง	> 2.5 แสนบาท - 10 ล้านบาท
3	ปานกลาง	> 50,000 - 2.5 แสนบาท
2	น้อย	> 10,000 - 50,000 บาท
1	น้อยมาก	ไม่เกิน 10,000 บาท

ตัวอย่าง ระดับความรุนแรงของผลกระทบของความเสี่ยง (Impact) ***เชิงคุณภาพ***		
ระดับ	ผลกระทบ	คำอธิบาย
5	รุนแรงที่สุด	มีการสูญเสียทรัพย์สินอย่างมหันต์ มีการบาดเจ็บถึงชีวิต
4	ค่อนข้างรุนแรง	มีการสูญเสียทรัพย์สินมาก มีการบาดเจ็บสาหัสถึงขั้นพักงาน
3	ปานกลาง	มีการสูญเสียทรัพย์สินมาก มีการบาดเจ็บสาหัสถึงขั้นหยุดงาน
2	น้อย	มีการสูญเสียทรัพย์สินพอสมควร มีการบาดเจ็บรุนแรง
1	น้อยมาก	มีการสูญเสียทรัพย์สินเล็กน้อย ไม่มีการบาดเจ็บรุนแรง

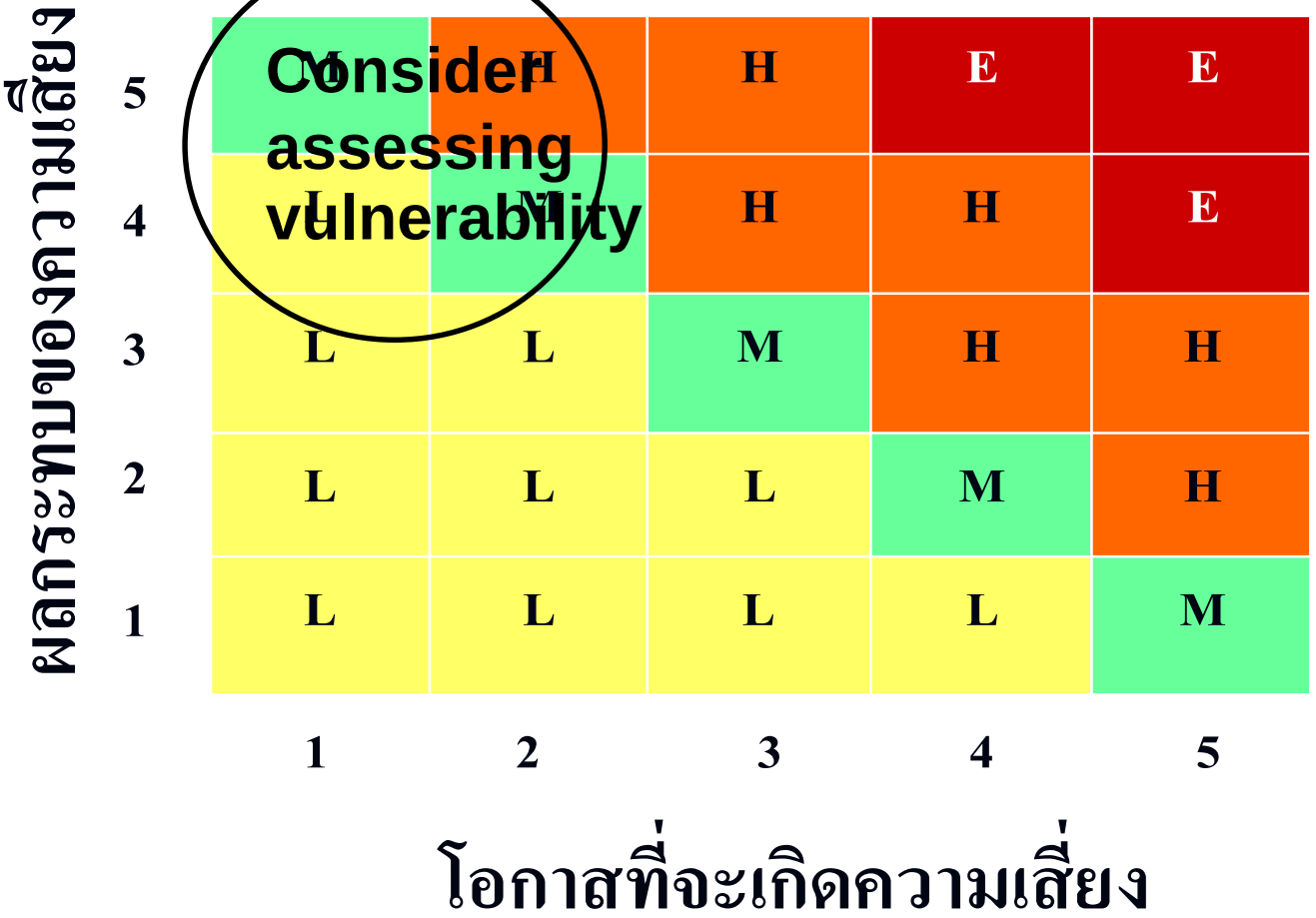
ตัวอย่าง การพัฒนาระบบสารสนเทศ

ตัวอย่าง ระดับโอกาสในการเกิดเหตุการณ์ต่างๆ (Likelihood) เชิงคุณภาพ		
ระดับ	โอกาสที่จะเกิด	คำอธิบาย
5	สูงมาก	มีโอกาสในการเกิดเกือบทุกครั้ง
4	สูง	มีโอกาสในการเกิดค่อนข้างสูงหรือบ่อยๆ
3	ปานกลาง	มีโอกาสเกิดบางครั้ง
2	น้อย	อาจมีโอกาสเกิดแต่นานๆ ครั้ง
1	น้อยมาก	มีโอกาสเกิดในกรณียกเว้น

ตัวอย่าง ระดับความรุนแรงของผลกระทบของความเสี่ยง (Impact) เชิงคุณภาพ		
ระดับ	ผลกระทบ	คำอธิบาย
5	รุนแรงที่สุด	ระบบสารสนเทศให้ข้อมูลได้ไม่ครบถ้วนถูกต้อง ไม่เป็นปัจจุบัน ไม่ตรงความต้องการของผู้ใช้ ไม่เป็นประโยชน์ต่อการตัดสินใจของผู้บริหาร มีรูปแบบยากต่อการใช้งาน ไม่มีความปลอดภัย ล้าสมัย ไม่เป็นไปตามระเบียบที่เกี่ยวข้องทางสารสนเทศ โดยใช้งบประมาณไม่คุ้มค่า ไม่โปร่งใส ตรวจสอบไม่ได้
4	ค่อนข้างรุนแรง	ระบบสารสนเทศเป็นประโยชน์ต่อการตัดสินใจของผู้บริหาร แต่ให้ข้อมูลได้ไม่ครบถ้วนถูกต้อง ไม่เป็นปัจจุบัน ไม่ตรงความต้องการของผู้ใช้ มีรูปแบบยากต่อการใช้งาน ไม่มีความปลอดภัย ล้าสมัย ไม่เป็นไปตามระเบียบที่เกี่ยวข้องทางสารสนเทศ โดยใช้งบประมาณไม่คุ้มค่า ไม่โปร่งใส ตรวจสอบไม่ได้
3	ปานกลาง	ระบบสารสนเทศเป็นประโยชน์ต่อการตัดสินใจของผู้บริหาร ให้ข้อมูลครบถ้วนถูกต้อง เป็นปัจจุบัน มีรูปแบบที่ง่ายต่อการใช้งาน มีความปลอดภัย ทันสมัย แต่ไม่ตรงความต้องการของผู้ใช้ ไม่เป็นไปตามระเบียบที่เกี่ยวข้องทางสารสนเทศ โดยใช้งบประมาณไม่คุ้มค่า ไม่โปร่งใส ตรวจสอบไม่ได้
2	น้อย	ระบบสารสนเทศเป็นประโยชน์ต่อการตัดสินใจของผู้บริหาร ให้ข้อมูลครบถ้วนถูกต้อง เป็นปัจจุบัน มีรูปแบบที่ง่ายต่อการใช้งาน มีความปลอดภัย ทันสมัย เป็นไปตามระเบียบที่เกี่ยวข้องทางสารสนเทศ โปร่งใส ตรวจสอบได้ แต่ยังใช้งบประมาณไม่คุ้มค่า และไม่ตรงความต้องการของผู้ใช้
1	น้อยมาก	ระบบสารสนเทศเป็นประโยชน์ต่อการตัดสินใจของผู้บริหาร ให้ข้อมูลครบถ้วนถูกต้อง เป็นปัจจุบัน มีรูปแบบที่ง่ายต่อการใช้งาน มีความปลอดภัย ทันสมัย เป็นไปตามระเบียบที่เกี่ยวข้องทางสารสนเทศ โดยใช้งบประมาณอย่างคุ้มค่า โปร่งใส ตรวจสอบได้ แต่ยังไม่ตรงความต้องการของผู้ใช้ เท่าที่ควร

เกณฑ์มาตรฐานระดับของความเสี่ยง

(Degree of Risk / Risk Matrix)



ขั้นตอนที่ 3.2
การประเมินโอกาสและผลกระทบของความเสี่ยง

ตัวอย่าง การประเมินโอกาสและผลกระทบของความเสี่ยง

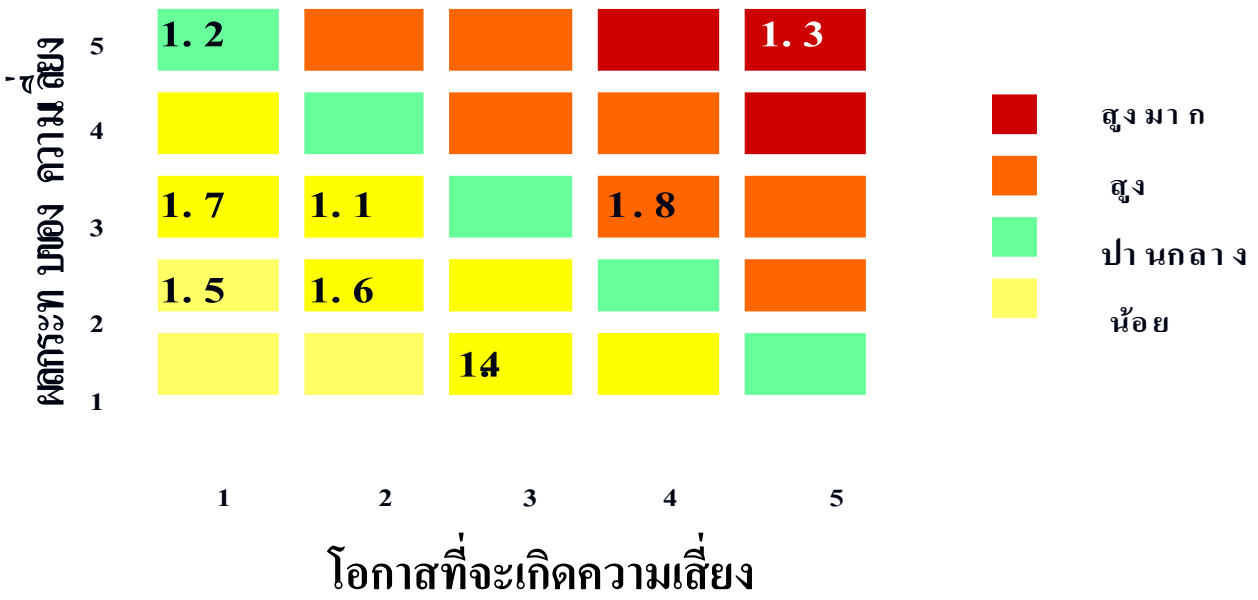
โครงการ *การพัฒนาระบบสารสนเทศ*

ความเสี่ยง : ระบบสารสนเทศให้ข้อมูลได้ไม่ครบถ้วนถูกต้อง ไม่เป็นปัจจุบัน ไม่ตรงความต้องการของผู้ใช้ ไม่เป็นประโยชน์ต่อการตัดสินใจของผู้บริหาร มีรูปแบบยากต่อการใช้งาน ไม่มีความปลอดภัย ล้าสมัย ไม่เป็นไปตามนโยบายและระเบียบที่เกี่ยวข้องทางสารสนเทศ ใช้งบประมาณไม่คุ้มค่า ไม่โปร่งใส ตรวจสอบไม่ได้

ขั้นตอน	วัตถุประสงค์ขั้นตอน	ความเสี่ยง	ปัจจัยเสี่ยง	การประเมินความเสี่ยง	
				โอกาส	ผลกระทบ
1.สำรวจความต้องการ/ศึกษานโยบายและระเบียบต่าง ๆ ทางสารสนเทศ	1.1 เพื่อให้ทราบข้อมูลและความต้องการที่แท้จริงในการใช้ระบบสารสนเทศของผู้ใช้บริการ 1.2 เพื่อให้ทราบนโยบาย และระเบียบต่าง ๆ ทางสารสนเทศที่เกี่ยวข้องอย่างครบถ้วนและถูกต้อง	1.1 ข้อมูลที่ได้ไม่ตรงกับความต้องการที่แท้จริงของผู้ใช้งาน 1.2 ข้อมูลนโยบาย IT และระเบียบต่าง ๆ ทางสารสนเทศที่เกี่ยวข้อง ไม่ครบถ้วนและถูกต้อง	1.1 ระยะเวลาในการสำรวจ / ศึกษาข้อมูลจำกัด	2	3
			1.2 การสำรวจความต้องการของผู้ใช้บริการไม่ครอบคลุมทุกหน่วยงาน	1	5
			1.3 เครื่องมือที่ใช้สำรวจข้อมูลความต้องการใช้ระบบ ไม่ได้มาตรฐาน ไม่ชัดเจน และไม่ครอบคลุมข้อมูลที่ต้องการ	5	5
			1.4 บุคลากร / หน่วยงาน ไม่ให้ความร่วมมือในการให้ข้อมูลที่แท้จริง	3	1
			1.5 ผู้บริหารให้ข้อมูลความต้องการใช้ระบบสารสนเทศไม่ชัดเจน	1	2
			1.6 ไม่มีการรวบรวมข้อมูลกฎหมาย ระเบียบทางสารสนเทศที่ประกาศใช้และที่เปลี่ยนแปลงไว้	2	2
			1.7 หน่วยงานและบุคลากรไม่ได้รับแจ้งการเปลี่ยนแปลงกฎหมาย กฎเกณฑ์ที่เกี่ยวกับการใช้ระบบสารสนเทศ	1	3
			1.8 นโยบายด้านสารสนเทศของหน่วยงานยังไม่ชัดเจน	4	3

ขั้นตอนที่ 3.3
การวิเคราะห์ความเสี่ยง

ตัวอย่าง ตารางระดับของความเสี่ยง (Degree of Risk)



1.1 - 1.9 หมายถึง ปัจจัยเสี่ยงแต่ละปัจจัย

1.1 ระยะเวลาในการสำรวจ / ศึกษาข้อมูลจำกัด

1.2 การสำรวจความต้องการของผู้ใช้บริการไม่ครอบคลุมทุกหน่วยงาน

1.3 เครื่องมือที่ใช้สำรวจข้อมูลความต้องการใช้ระบบ ไม่ได้มาตรฐาน ไม่ชัดเจน และไม่ครอบคลุมข้อมูลที่ต้องการ

1.4 บุคลากร / หน่วยงาน ไม่ให้ความร่วมมือในการให้ข้อมูลที่แท้จริง

1.5 ผู้บริหารให้ข้อมูลความต้องการใช้ระบบสารสนเทศไม่ชัดเจน

1.6 ไม่มีการรวบรวมข้อมูลกฎหมาย ระเบียบทางสารสนเทศที่ประกาศใช้และที่เปลี่ยนแปลงไว้

1.7 หน่วยงานและบุคลากรไม่ได้รับแจ้งการเปลี่ยนแปลงกฎหมาย กฎเกณฑ์ที่เกี่ยวกับการใช้ระบบสารสนเทศ

1.8 นโยบายด้านสารสนเทศของหน่วยงานยังไม่ชัดเจน

ตัวอย่าง การวิเคราะห์ระดับความเสี่ยง

โครงการ *การพัฒนาระบบสารสนเทศ*

ความเสี่ยง : ระบบสารสนเทศให้ข้อมูลได้ไม่ครบถ้วนถูกต้อง ไม่เป็นปัจจุบัน ไม่ตรงความต้องการของผู้ใช้ ไม่เป็นประโยชน์ต่อการตัดสินใจของผู้บริหาร มีรูปแบบยากต่อการใช้งาน ไม่มีความปลอดภัย ล้าสมัย ไม่เป็นไปตามนโยบายและระเบียบที่เกี่ยวข้องทางสารสนเทศ ใช้งบประมาณไม่คุ้มค่า ไม่โปร่งใส ตรวจสอบไม่ได้

ขั้นตอน	วัตถุประสงค์ขั้นตอน	ความเสี่ยง	ปัจจัยเสี่ยง	การประเมินความเสี่ยง		
				โอกาส	ผลกระทบ	ระดับความเสี่ยง
1.สำรวจความต้องการ/ศึกษานโยบายและระเบียบต่าง ๆ ทางสารสนเทศ	1.1 เพื่อให้ทราบข้อมูลและความต้องการที่แท้จริงในการใช้ระบบสารสนเทศของผู้ใช้บริการ 1.2 เพื่อให้ทราบนโยบาย และระเบียบต่าง ๆ ทางสารสนเทศที่เกี่ยวข้องอย่างครบถ้วนและถูกต้อง	1.1 ข้อมูลที่ได้ไม่ตรงกับความต้องการที่แท้จริงของผู้ใช้งาน 1.2 ข้อมูลนโยบาย IT และระเบียบต่าง ๆ ทางสารสนเทศที่เกี่ยวข้อง ไม่ครบถ้วนและถูกต้อง	1.1 ระยะเวลาในการสำรวจ / ศึกษาข้อมูลจำกัด	2	3	น้อย
			1.2 การสำรวจความต้องการของผู้ใช้บริการไม่ครอบคลุมทุกหน่วยงาน	1	5	ปานกลาง
			1.3 เครื่องมือที่ใช้สำรวจข้อมูลความต้องการใช้ระบบ ไม่ได้มาตรฐาน ไม่ชัดเจน และไม่ครอบคลุมข้อมูลที่ต้องการ	5	5	สูงมาก
			1.4 บุคลากร / หน่วยงาน ไม่ให้ความร่วมมือในการให้ข้อมูลที่แท้จริง	3	1	น้อย
			1.5 ผู้บริหารให้ข้อมูลความต้องการใช้ระบบสารสนเทศไม่ชัดเจน	1	2	น้อย
			1.6 ไม่มีการรวบรวมข้อมูลกฎหมาย ระเบียบทางสารสนเทศที่ประกาศใช้และที่เปลี่ยนแปลงไว้	2	2	น้อย
			1.7 หน่วยงานและบุคลากรไม่ได้รับแจ้งการเปลี่ยนแปลงกฎหมาย กฎเกณฑ์ที่เกี่ยวกับการใช้ระบบสารสนเทศ	1	3	น้อย
			1.8 นโยบายด้านสารสนเทศของหน่วยงานยังไม่ชัดเจน	4	3	สูง

ขั้นตอนที่ 3.4
การจัดลำดับความเสี่ยง

โครงการ *การพัฒนาระบบสารสนเทศ*

ความเสี่ยง : ระบบสารสนเทศให้ข้อมูลได้ไม่ครบถ้วนถูกต้อง ไม่เป็นปัจจุบัน ไม่ตรงความต้องการของผู้ใช้ ไม่เป็นประโยชน์ต่อการตัดสินใจของผู้บริหาร มีรูปแบบยากต่อการใช้งาน ไม่มีความปลอดภัย ล้าสมัย ไม่เป็นไปตามนโยบายและระเบียบที่เกี่ยวข้องทางสารสนเทศ ใช้งบประมาณไม่คุ้มค่า ไม่โปร่งใส ตรวจสอบไม่ได้

ขั้นตอน	วัตถุประสงค์ขั้นตอน	ความเสี่ยง	ปัจจัยเสี่ยง	การประเมินความเสี่ยง			
				โอกาส	ผลกระทบ	ระดับความเสี่ยง	ลำดับ ความเสี่ยง
1.สำรวจความต้องการ/ศึกษานโยบายและระเบียบต่าง ๆ ทางสารสนเทศ	1.1 เพื่อให้ทราบข้อมูลและความต้องการที่แท้จริงในการใช้ระบบสารสนเทศของผู้ใช้บริการ 1.2 เพื่อให้ทราบนโยบาย และระเบียบต่าง ๆ ทางสารสนเทศที่เกี่ยวข้องอย่างครบถ้วนและถูกต้อง	1.1 ข้อมูลที่ได้ไม่ตรงกับความต้องการที่แท้จริงของผู้ใช้งาน 1.2 ข้อมูลนโยบาย IT และระเบียบต่าง ๆ ทางสารสนเทศที่เกี่ยวข้อง ไม่ครบถ้วนและถูกต้อง	1.1 ระยะเวลาในการสำรวจ / ศึกษาข้อมูลจำกัด	2	3	น้อย	4
			1.2 การสำรวจความต้องการของผู้ใช้บริการไม่ครอบคลุมทุกหน่วยงาน	1	5	ปานกลาง	3
			1.3 เครื่องมือที่ใช้สำรวจข้อมูลความต้องการใช้ระบบไม่ได้มาตรฐาน ไม่ชัดเจน และไม่ครอบคลุมข้อมูลที่ต้องการ	5	5	สูงมาก	1
			1.4 บุคลากร / หน่วยงาน ไม่ให้ความร่วมมือในการให้ข้อมูลที่แท้จริง	3	1	น้อย	7
			1.5 ผู้บริหารให้ข้อมูลความต้องการใช้ระบบสารสนเทศไม่ชัดเจน	1	2	น้อย	8
			1.6 ไม่มีการรวบรวมข้อมูลกฎหมาย ระเบียบทางสารสนเทศที่ประกาศใช้และที่เปลี่ยนแปลงไว้	2	2	น้อย	5
			1.7 หน่วยงานและบุคลากรไม่ได้รับแจ้งการเปลี่ยนแปลงกฎหมาย กฎเกณฑ์ที่เกี่ยวกับการใช้ระบบสารสนเทศ	1	3	น้อย	6
			1.8 นโยบายด้านสารสนเทศของหน่วยงานยังไม่ชัดเจน	4	3	สูง	2

ขั้นตอนที่ 4
การประเมินมาตรการควบคุมภายใน

การควบคุม (Controls)

การควบคุมเพื่อการป้องกัน
(Preventive Control)

การควบคุมเพื่อให้ตรวจพบ
(Detective Control)

การควบคุมเพื่อการแก้ไข
(Corrective Control)

การควบคุมโดยการชี้แนะ
(Directive Control)

โครงการ *การพัฒนาระบบสารสนเทศ*

ความเสี่ยง : **ระบบสารสนเทศให้ข้อมูลได้ไม่ครบถ้วนถูกต้อง ไม่เป็นปัจจุบัน ไม่ตรงความต้องการของผู้ใช้ ไม่เป็นประโยชน์ต่อการตัดสินใจของผู้บริหาร มีรูปแบบยากต่อการใช้งาน ไม่มีความปลอดภัย ล้าสมัย ไม่เป็นไปตามนโยบายและระเบียบที่เกี่ยวข้องทางสารสนเทศ ใช้งบประมาณไม่คุ้มค่า ไม่โปร่งใส ตรวจสอบไม่ได้**

สาเหตุของความเสี่ยง (Risk factors) (1)	การควบคุมที่ควรจะมี (2)	การควบคุมที่มีอยู่แล้ว (3)	ผลการประเมินการควบคุมที่มีอยู่แล้วว่าได้ผลหรือไม่ (4)
1. สำรวจความต้องการ/ศึกษานโยบายและระเบียบต่างๆ ทางสารสนเทศ ***ความเสี่ยง :*** ข้อมูลที่ได้ไม่ตรงกับความต้องการที่แท้จริงของผู้ใช้งาน ***ปัจจัยเสี่ยง :*** 1.1 เครื่องมือที่ใช้สำรวจข้อมูลความต้องการใช้ระบบ ไม่ได้มาตรฐาน ไม่ชัดเจน และไม่ครอบคลุมข้อมูลที่ต้องการ	1.1.1 แต่งตั้งคณะกรรมการจัดทำเครื่องมือในการสำรวจข้อมูล	√	?
	1.1.2 จัดหาข้อมูลในการพิจารณาจัดทำเครื่องมือให้คณะกรรมการ	?	X
	1.1.3 จัดงบประมาณให้เพียงพอในการจัดทำเครื่องมือที่มีคุณภาพ	X	X
	1.1.4 มีการทดสอบเครื่องมืออย่างเพียงพอก่อนนำไปใช้งาน	X	X

เครื่องหมายที่ระบุในช่อง (3)

√ = มี × = ไม่มี ? = มีแต่ไม่สมบูรณ์

เครื่องหมายที่ระบุในช่อง (4)

√ = ได้ผลตามที่คาดหมาย × = ไม่ได้ผลตามที่คาดหมาย ? = ได้ผลบ้างแต่ไม่สมบูรณ์

ขั้นตอนที่ 5
การบริหาร / จัดการความเสี่ยง

การสนองตอบ (จัดการ) ต่อความเสี่ยง

- ผู้บริหารตัดสินใจว่า จะจัดการกับความเสี่ยงอย่างไร
  - Avoid (Terminate) ลดโอกาสที่จะเกิดให้เหลือศูนย์ (หลีกเลี่ยง)
  - Accept (Take) ยอมรับความเสี่ยงนั้น (เฝ้าระวัง)
  - Reduce (Treat) ลดปริมาณความเสียหายให้น้อยลง (ควบคุม)
  - Prevent (Treat) ลดโอกาสที่จะเกิดให้น้อยลง (ควบคุม)
  - Share ร่วมกันรับความเสี่ยงกับองค์กรอื่น หรือคนอื่น
  - Transfer โอนความเสี่ยงไปให้องค์กรอื่น หรือคนอื่น

แผนจัดการความเสี่ยง

การจัดทำแผนบริหารความเสี่ยง / แผนกลยุทธ์

Risk Factors สาเหตุของความเสี่ยง	All the Controls that Should be in Place การควบคุมทั้งหลายที่ควรมี	Existing Controls (Yes/No) การควบคุมที่มีอยู่ (มี/ไม่มี)	Is the Existing Controls Working? (Yes/No) การควบคุมที่มีอยู่ได้ผลหรือไม่ (ได้ผล/ไม่ได้ผล)	แผนกลยุทธ์ / แผนบริหารความเสี่ยง Strategy
The event that cause or lead to the undersirable risk outcomes. เหตุการณ์ที่ก่อให้เกิดหรือนำไปสู่ผลลัพธ์ที่ไม่พึงปรารถนา	List of all possible controls that may help mitigating the risk cause ระบุการควบคุมที่เป็นไปได้ทั้งหลายที่อาจป้องกันสาเหตุของความเสี่ยง	Yes No Not Fully มี ไม่มี มีบ้างแต่ไม่สมบูรณ์	Yes No Not Fully ได้ผล ไม่ได้ผล ได้ผลบ้างแต่ยังไม่ดีพอ	*If existing control is working well, review later *If not, what action is required to improve the situation *ถ้าการควบคุมที่มีอยู่แล้วได้ผลดี ทำการทบทวนในภายหลัง *ถ้าการควบคุมที่มีอยู่แล้วไม่ได้ผลจะต้องทำอย่างไรจึงจะแก้ไขสถานการณ์ให้ดีขึ้น

แบบประเมินความเสี่ยง

KU-ERM 6

หน่วยงาน : .....

ยุทธศาสตร์ที่ : ..... กลยุทธ์ : .....

โครงการ / กิจกรรม : .....

วัตถุประสงค์ : .....

ขั้นตอน (1)	วัตถุประสงค์ขั้นตอน (2)	ความเสี่ยง (3)	ปัจจัยเสี่ยง (4)	การประเมินความเสี่ยง			
				โอกาส (5)	ผลกระทบ (6)	ระดับความเสี่ยง (7)	ลำดับความเสี่ยง (8)

แบบประเมินการควบคุม

KU-ERM 7

หน่วยงาน : .....

ยุทธศาสตร์ที่ : ..... กลยุทธ์ : .....

โครงการ / กิจกรรม : .....

วัตถุประสงค์ : .....

ปัจจัยเสี่ยง / สาเหตุของความเสี่ยง (Risk factors) (1)	การควบคุมที่ควรจะมี (2)	การควบคุมที่มีอยู่แล้ว (3)	ผลการประเมินการควบคุมที่มีอยู่แล้วว่าได้ผลหรือไม่ (4)

แบบสรุปการจัดการความเสี่ยง

KU-ERM 8

ยุทธศาสตร์ที่ : ..... กลยุทธ์ : .....

โครงการ .....

ความเสี่ยง .....

ขั้นตอนหลักและวัตถุประสงค์ (Key Process and Objectives) (1)	ความเสี่ยงที่ยังเหลืออยู่ (Residual Risks) (2)	ปัจจัยความเสี่ยง (Risk Factors) (3)	การจัดการความเสี่ยง (Risk Treatments) (4)	กำหนดเสร็จ/ผู้รับผิดชอบ (5)	หมายเหตุ (6)

แบบสรุปการจัดการความเสี่ยง

ยุทธศาสตร์ที่ : ..... **กลยุทธ์ :** .....

โครงการ *การพัฒนาระบบสารสนเทศ*

ความเสี่ยง : **ระบบสารสนเทศให้ข้อมูลได้ไม่ครบถ้วนถูกต้อง ไม่เป็นปัจจุบัน ไม่ตรงความต้องการของผู้ใช้ ไม่เป็นประโยชน์ต่อการตัดสินใจของผู้บริหาร มีรูปแบบยากต่อการใช้งาน ไม่มีความปลอดภัย ล้าสมัย ไม่เป็นไปตามนโยบายและระเบียบที่เกี่ยวข้องทางสารสนเทศ ใช้งบประมาณไม่คุ้มค่า ไม่โปร่งใส ตรวจสอบไม่ได้**

ขั้นตอนหลัก และวัตถุประสงค์ (Key Process and Objectives) (1)	ความเสี่ยงที่ยังเหลืออยู่ (Residual Risks) (2)	ปัจจัยความเสี่ยง (Risk Factors) (3)	การจัดการความเสี่ยง (Risk Treatments) (4)	กำหนดเสร็จ/ผู้รับผิดชอบ (5)	หมายเหตุ (6)
1. สำรวจความต้องการ/ศึกษานโยบายและระเบียบต่าง ๆ ทางสารสนเทศ ***วัตถุประสงค์ :*** เพื่อให้ทราบข้อมูลและความต้องการที่แท้จริงในการใช้ระบบสารสนเทศของผู้ใช้บริการ	- ข้อมูลที่ได้ไม่ตรงกับความต้องการที่แท้จริงของผู้ใช้งาน	- เครื่องมือที่ใช้สำรวจข้อมูลความต้องการใช้ระบบ ไม่ได้มาตรฐาน ไม่ชัดเจน และไม่ครอบคลุมข้อมูลที่ต้องการ	1.1.1 แต่งตั้งคณะกรรมการที่มีความรู้ ความชำนาญมาเป็นกรรมการจัดทำเครื่องมือ 1.1.2 จัดหาข้อมูลที่มีคุณภาพและเป็นปัจจุบันให้คณะกรรมการพิจารณาจัดทำเครื่องมือ 1.1.3 จัดงบประมาณให้เพียงพอในการจัดทำเครื่องมือที่มีคุณภาพ 1.1.4 มีการทดสอบเครื่องมืออย่างเพียงพอก่อนนำไปใช้งาน	30 ต.ค.60 / ผู้อำนวยการ	ค่าใช้จ่าย / งบประมาณ 20,000 บาท

ขั้นตอนที่ 6 / 7

การจัดทำรายงานการบริหารความเสี่ยงและการควบคุมภายใน / การติดตามผลและทบทวน

แผนบริหารความเสี่ยง ประจำปีงบประมาณ พ.ศ.25.....

หน่วยงาน .....

ยุทธศาสตร์ที่ ..... / กลยุทธ์ .....

โครงการ.....

วัตถุประสงค์ / เป้าหมาย (1)	ความเสี่ยงที่ยังเหลืออยู่ (2)	ปัจจัยความเสี่ยง (3)	การจัดการความเสี่ยง (4)	กำหนดเสร็จ/ ผู้รับผิดชอบ (5)	หมายเหตุ (งบประมาณ/ ค่าใช้จ่าย) (6)
เพื่อให้ระบบสารสนเทศสามารถให้ข้อมูลได้อย่างครบถ้วนถูกต้อง เป็นปัจจุบัน ตรงความต้องการของผู้ใช้ เป็นประโยชน์ต่อการตัดสินใจของผู้บริหาร มีรูปแบบการใช้งานที่ง่าย ปลอดภัย ทันสมัยเป็นไปตามนโยบายและระเบียบที่เกี่ยวข้องทางสารสนเทศ โดยใช้งบประมาณอย่างคุ้มค่า โปร่งใส ตรวจสอบได้	ระบบสารสนเทศให้ข้อมูลไม่ตรงกับความต้องการของผู้ใช้ ทำให้ข้อมูลที่ได้ไม่ถูกต้อง ไม่เป็นประโยชน์ต่อการตัดสินใจของผู้บริหาร	- เครื่องมือที่ใช้สำรวจข้อมูลความต้องการใช้ระบบ ไม่ได้มาตรฐาน ไม่ชัดเจน และไม่ครอบคลุมข้อมูลที่ต้องการ	1.1.1 แต่งตั้งคณะกรรมการที่มีความรู้ ความชำนาญมาเป็นกรรมการจัดทำเครื่องมือ 1.1.2 จัดหาข้อมูลที่มีคุณภาพและเป็นปัจจุบันให้คณะกรรมการพิจารณาจัดทำเครื่องมือ 1.1.3 จัดงบประมาณให้เพียงพอในการจัดทำเครื่องมือที่มีคุณภาพ 1.1.4 มีการทดสอบเครื่องมืออย่างเพียงพอก่อนนำไปใช้งาน	30 ต.ค.60 / ผู้อำนวยการ	ค่าใช้จ่าย / งบประมาณ 20,000 บาท

การติดตามผลและทบทวน

แบบติดตามผลการบริหารความเสี่ยง ประจำปี.....

หน่วยงาน .....

ยุทธศาสตร์ที่ ..... / กลยุทธ์ .....

โครงการ.....

ณ วันที่ ..... เดือน ..... พ.ศ. .....

วัตถุประสงค์ / เป้าหมาย (1)	ความเสี่ยงที่ยังเหลืออยู่ (2)	การจัดการความเสี่ยง (3)	กำหนดเสร็จ/ ผู้รับผิดชอบ (4)	สถานภาพการดำเนินงาน (5)	วิธีการติดตาม (Monitoring) และปัญหาอุปสรรค (6)	ผลสัมฤทธิ์ (7)
						ให้อธิบาย เมื่อดำเนินการตาม (๔) แล้วสามารถลดความเสี่ยงตาม (๓) ทำให้การทำงานมีประสิทธิภาพ ประสิทธิผลเพิ่มขึ้นในเชิงปริมาณหรือเชิงคุณภาพ อย่างไร

การเชื่อมโยงความเสี่ยงแต่ละยุทธศาสตร์ / ภารกิจ / โครงการ / กิจกรรม

ธรรมะที่ใช้ในการบริหารความเสี่ยง

อริยสัจ 4

ทุกข์ : การมีอยู่ของทุกข์

สมุทัย : เหตุแห่งทุกข์

นิโรธ : ความดับทุกข์

มรรค : หนทางนำไปสู่ความดับทุกข์

เชิญซักถามปัญหา

สำนักงานตรวจสอบภายใน ม.เกษตรศาสตร์

โทร. 0-2942-8164 , 0-2942-8116

เบอร์ภายใน 4822 – 4829

http://ia.psd.ku.ac.th