การบริหารความเสี่ยง

หัวข้อบรรยาย

แบ่งเป็นสองส่วนใหญ่ ๆ

- ความรู้ทั่วไปเกี่ยวกับการบริหารความเสี่ยง
- การบริหารความเสี่ยงตามกรอบของ COSO

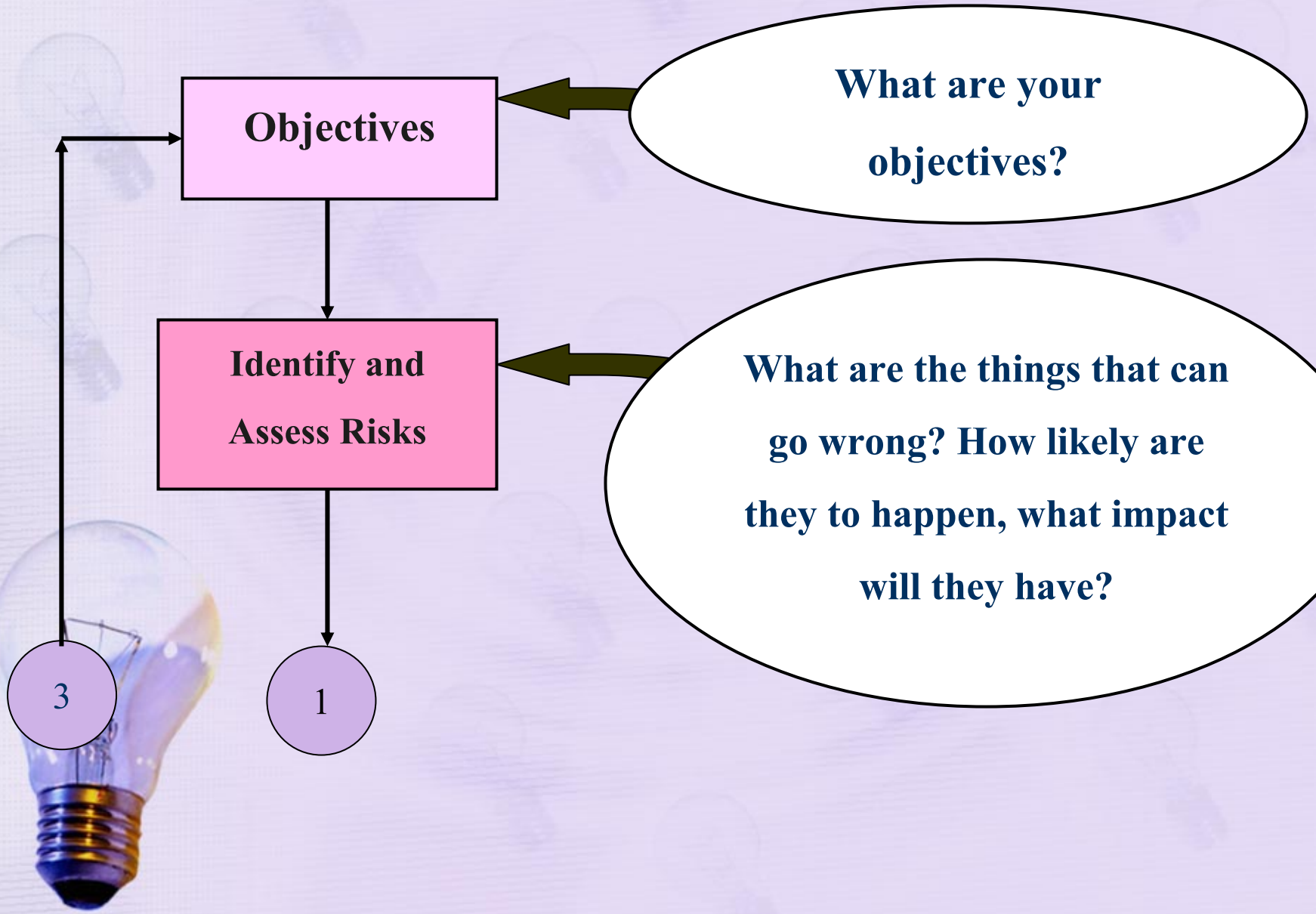
วัตถุประสงค์

- เพื่อให้เกิดความเข้าใจในภาพรวมของการบริหารความเสี่ยง
- เพื่อให้เกิดความเข้าใจในกรอบการบริหารความเสี่ยงฉบับบูรณาการตามแนว COSO (COSO ERM Integrated Framework)
- เกิดความเข้าใจเบื้องต้นในการนำเอากรอบการบริหารความเสี่ยงไปใช้ปฏิบัติ (ERM Implementation)

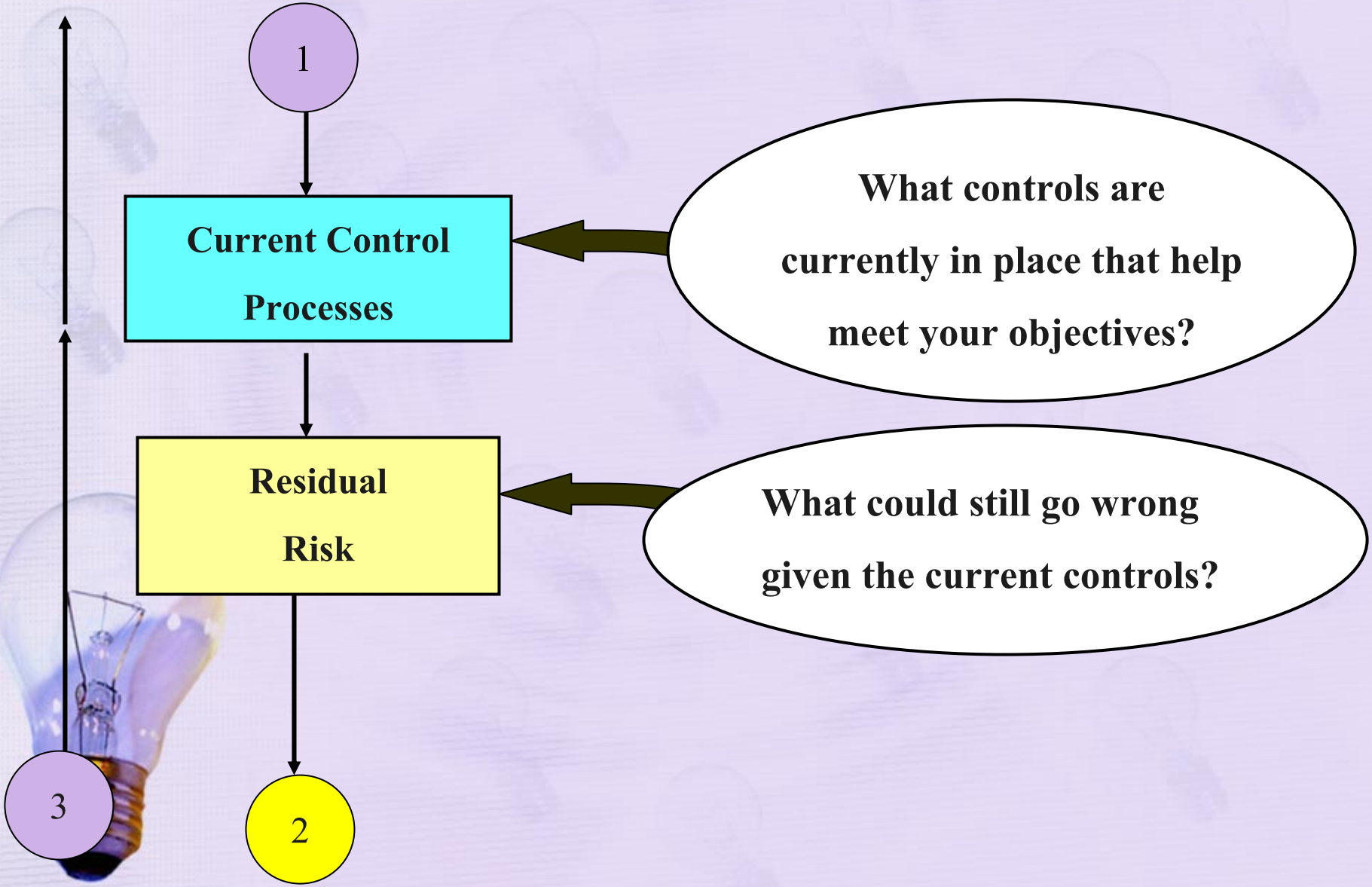
ความเสี่ยงคืออะไร

- ความเสี่ยงคือ โอกาสที่เหตุการณ์บางอย่างอาจเกิดขึ้นและมีผลกระทบต่อการบรรลุวัตถุประสงค์ขององค์กร
- ระดับของความเสี่ยงที่สูงหรือต่ำสามารถวัดได้จากผลที่ตามมา (Consequence) และโอกาสที่เหตุการณ์ ๆ หนึ่งจะเกิดขึ้น (Likelihood)
- ผลกระทบ(Consequence) คือผลลัพธ์หรือผลกระทบจากเหตุการณ์ ๆ หนึ่ง เป็นไปได้ทั้งในทางบวกหรือลบ

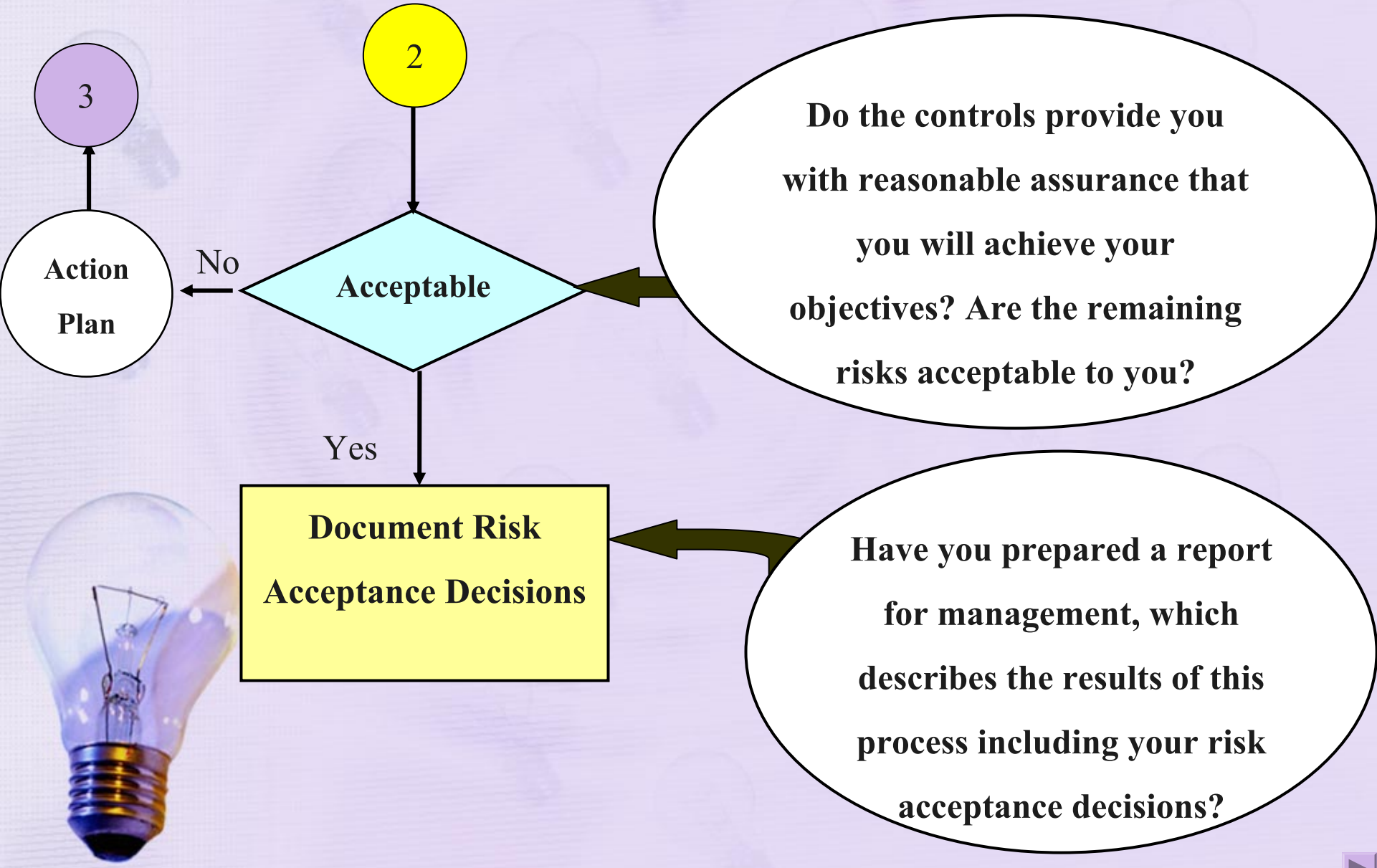
ภาพรวมกระบวนการบริหารความเสี่ยง



ภาพรวมกระบวนการบริหารความเสี่ยง

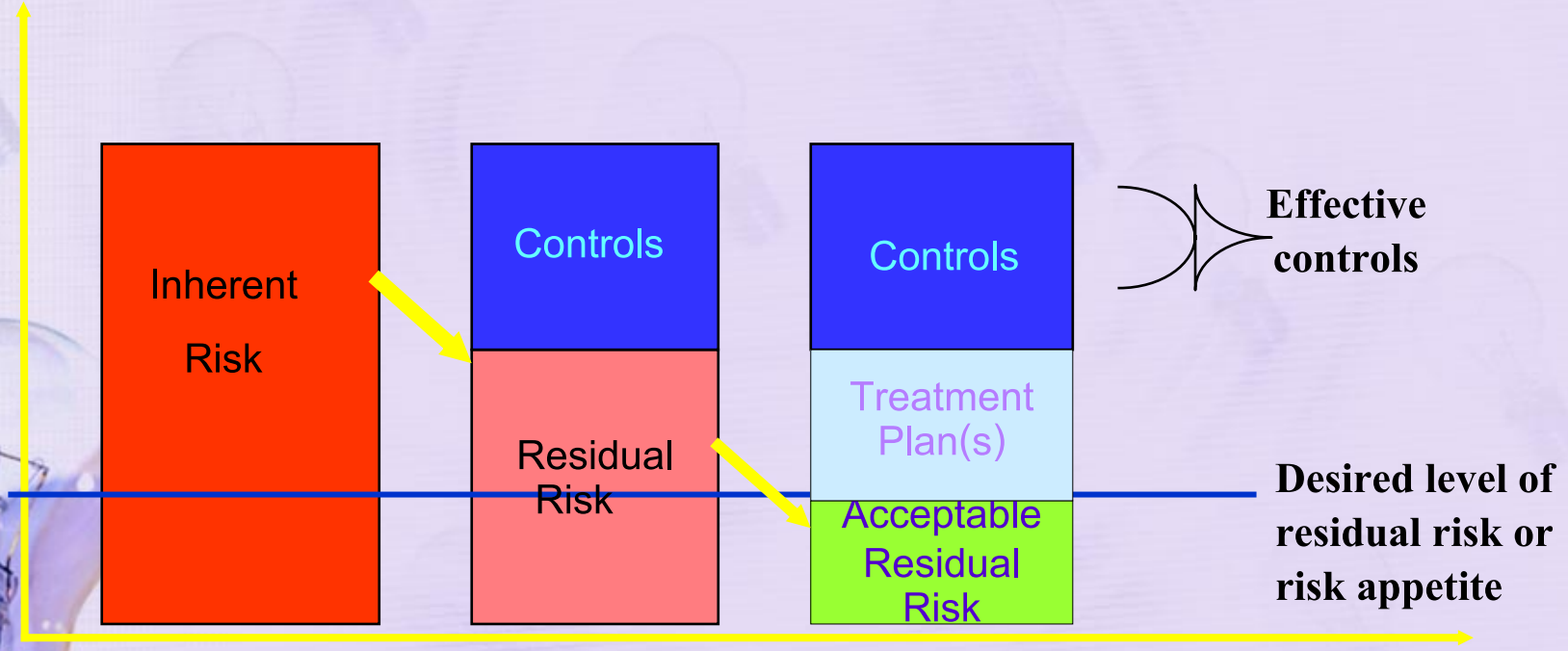


ภาพรวมกระบวนการบริหารความเสี่ยง



หลักการของความเสี่ยง

(Risk Management Concept)



Cost & Benefit of controls must be considered

กรอบการบริหารความเสี่ยง ฉบับบูรณาการตามแนว COSO

คำศัพท์ที่เกี่ยวข้องของERM

- เหตุการณ์ : ความเสี่ยง และ โอกาส (Events: Risks and Opportunities)
- เหตุการณ์ อาจส่งผลทั้งทางดีและร้าย
  - เหตุการณ์ ที่ส่งผลทางร้าย ก็คือ ความเสี่ยง ซึ่งสามารถกันไม่ให้เกิดคุณค่า หรือทำให้คุณค่าที่กิจการมีอยู่อาจเสื่อมได้
  - เหตุการณ์ ที่ส่งผลทางดีอาจหักกลบกับผลกระทบที่ไม่ดี หรืออาจก่อให้เกิด “โอกาส” กับกิจการได้

- “โอกาส” คือความเป็นไปได้ซึ่งเหตุการณ์ใดเหตุการณ์หนึ่งจะเกิดและส่งผลดีในการบรรลุวัตถุประสงค์ ซึ่งจะเป็นสิ่งที่ส่งเสริมให้เกิดคุณค่า หรือรักษาไว้ซึ่งคุณค่า
- เมื่อเกิด “โอกาส” ผู้บริหารจะต้องนำ “โอกาส” นั้นกลับไปพิจารณากับกลยุทธ์หรือกระบวนการกำหนดวัตถุประสงค์เพื่อสร้างแผนดำเนินการที่จะฉวยโอกาสนั้นไว้

คำจำกัดความ (ERM Definition)

Enterprise risk management is

- *a process, effected by an entity's board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, and to provide reasonable assurance regarding the achievement of entity objectives.*

คำจำกัดความ (ERM Definition)

การบริหารความเสี่ยงองค์กรคือ

- *กระบวนการซึ่งได้รับอิทธิพลมาจากคณะกรรมการขององค์กร ผู้บริหารและบุคลากรอื่น ๆ เป็นกระบวนการที่จะถูกนำมาประยุกต์ใช้ในการตั้งกลยุทธ์ทั่วทั้งองค์กร ได้รับการออกแบบมาเพื่อให้สามารถระบุเหตุการณ์อันอาจเกิดขึ้นและส่งผลกระทบต่อองค์กร และ เพื่อจัดการความเสี่ยงให้อยู่ภายในระดับความเสี่ยงที่องค์กรยอมรับได้ (risk appetite) การบริหารความเสี่ยงขององค์กรจะทำให้เกิดความเชื่อมั่นได้อย่างสมเหตุสมผลเกี่ยวกับการบรรลุวัตถุประสงค์ขององค์กร*

คำจำกัดความ (ERM Definition)

- เป็นกระบวนการ *(process)*
- **ได้รับอิทธิพลจากคน** ***(effected by people)***
- เป็นกระบวนการที่ใช้ในการกำหนดกลยุทธ์ (*applied in strategy setting)*
- นำไปใช้ปฏิบัติทั่วทั้งองค์กร *(applied across the enterprise)*
- เพื่อระบุเหตุการณ์ที่อาจเกิดซึ่งก่อให้เกิดผลกระทบต่อองค์กร *(to identify potential events)*

คำจำกัดความ (ERM Definition)

- จัดการกับความเสี่ยงให้อยู่ภายในระดับที่องค์กรยอมรับได้ *(manage risk to be within its risk appetite)*
- เพื่อก่อให้เกิดความเชื่อมั่นได้อย่างสมเหตุสมผล แก่ผู้บริหาร และคณะกรรมการ *(to provide reasonable assurance to an entity's management and board)*
- นำทางไปสู่ความสำเร็จ บรรลุวัตถุประสงค์ต่างๆ ซึ่งอาจคาบเกี่ยวกันได้ *(achievement of objectives in one or more separate but overlapping)*

เหตุผลที่ต้องมี ERM

- ทุกองค์กรดำรงอยู่เพื่อมอบคุณค่า (Value) ให้แก่ผู้มีส่วนได้เสีย
- ทุกองค์กรย่อมต้องประสบกับความไม่แน่นอน (Uncertainty) ผู้บริหารมีหน้าที่ที่จะตัดสินใจว่าจะยอมรับความไม่แน่นอนได้เพียงใด เนื่องจากจะต้องเพิ่มคุณค่าให้แก่ผู้มีส่วนได้เสีย
- ความไม่แน่นอน ก่อให้เกิดได้ทั้งความเสี่ยงและโอกาส ลด/เพิ่มคุณค่า
- ERM สามารถช่วยให้ฝ่ายบริหารจัดการความไม่แน่นอนที่มีทั้งความเสี่ยงและโอกาส ได้อย่างมีประสิทธิผล และช่วยเพิ่มความสามารถแก่ผู้บริหารในการสร้างคุณค่าได้

คุณค่า (Value) จะมีหรือเกิดได้มากที่สุดถ้าหาก

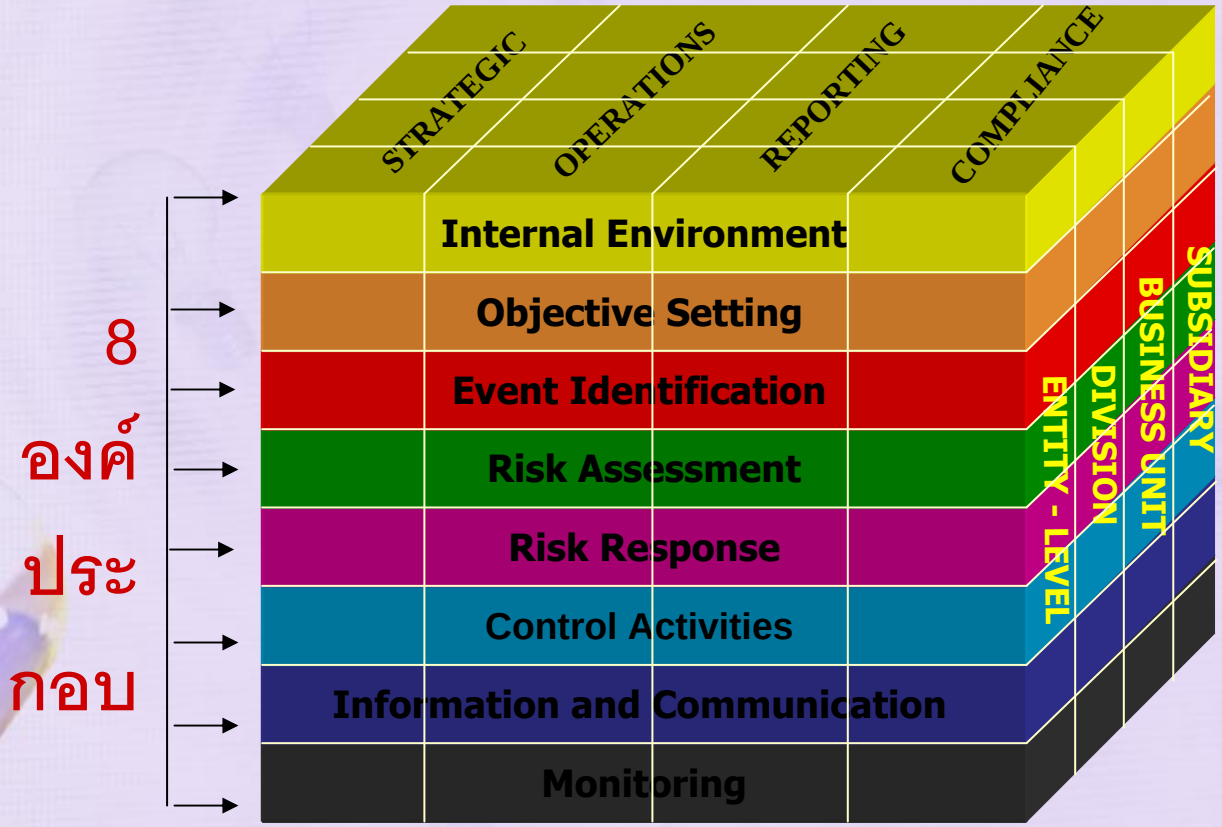
- ฝ่ายบริหารได้มีการกำหนดกลยุทธ์ เพื่อให้เกิดความสมดุลที่ดีที่สุด (Optimal balance) ระหว่างเป้าหมายในเรื่องการเจริญเติบโตและผลตอบแทนขององค์กร กับ ความเสี่ยงที่เกี่ยวข้อง
- ฝ่ายบริหารได้ใช้ทรัพยากรในการที่จะให้ไปถึงจุดมุ่งหมายหรือวัตถุประสงค์ขององค์กรอย่างมีประสิทธิภาพและประสิทธิผล

ประโยชน์ของ ERM

- จัดให้กลยุทธ์ต่างๆ เข้ากันได้กับ risk appetite
- ช่วยให้การตัดสินใจในเรื่องการโต้ตอบกับความเสี่ยงทำได้ดีขึ้น
- ลดสิ่งที่ไม่คาดฝันและความสูญเสียที่จะเกิดในการดำเนินงาน
- ทำให้การระบุและจัดการความเสี่ยงที่ต่อเนื่องกันหรือคาบเกี่ยวกันอย่างทั่วถึงทุกระดับ
- เนื่องมาจากการมองถึงเหตุการณ์ในอนาคตที่อาจเกิดขึ้นได้ ทำให้อาจมองเห็น “โอกาส” และฉวยโอกาสนั้นอย่างเชิงรุกได้
- การบริหารและใช้เงินทุนได้อย่างเหมาะสม

COSO ERM Framework

4 วัตถุประสงค์



8 องค์ประกอบ

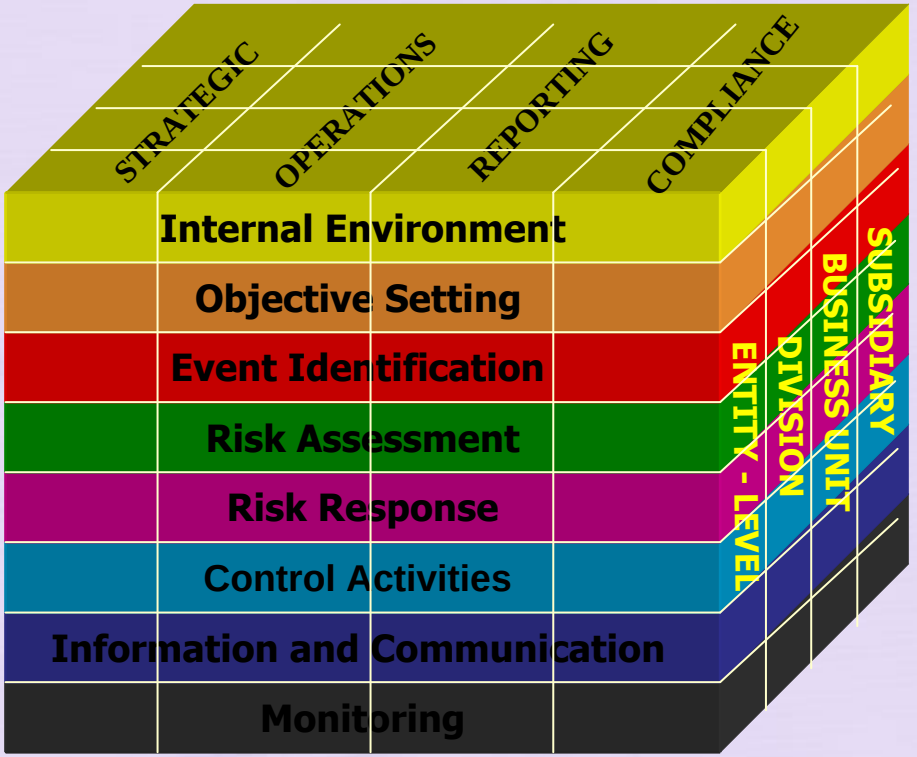
หน่วยงานในระดับต่างๆ

COSO ERM Framework

- การบริหารความเสี่ยงทั่วทั้งองค์กรนั้น ฝ่ายบริหารขององค์กร ต้องมองภาพความเสี่ยงทั้งหมด (*portfolio view* of risk) ซึ่งก็คือ “Big Picture” ในการที่จะเลือกดำเนินการกับความเสี่ยง
- ฝ่ายบริหารต้องพิจารณาว่าความเสี่ยงแต่ละอย่างมีความเกี่ยวข้องกันอย่างไร

- ERM ขยายและต่อเติมมาจากองค์ประกอบที่กำหนดไว้ใน COSO Control Framework
- ERM แยกเรื่องของการกำหนดวัตถุประสงค์ , การระบุเหตุการณ์ความเสี่ยงหรือโอกาส , การตอบสนองความเสี่ยง เป็นองค์ประกอบเพิ่มขึ้นจาก Control Framework
- ERM ขยายเรื่องการรายงานทางการเงิน (Financial Reporting) และเรื่องการประเมินความเสี่ยง (Risk Assessment) ของ Control Framework ให้กว้างขึ้น

COSO Control Framework vs. *COSO ERM*



4 วัตถุประสงค์ของ ERM

- วัตถุประสงค์ด้านกลยุทธ์ (Strategic) – เกี่ยวกับการกำหนดเป้าหมายในระดับสูงซึ่งต้องเป็นแนวทางเดียวกันและต้องสนับสนุนวัตถุประสงค์ขององค์กร
- วัตถุประสงค์ด้านการปฏิบัติงาน (Operations) – การใช้ทรัพยากรขององค์กร อย่างมีประสิทธิผลและประสิทธิภาพ
- วัตถุประสงค์ด้านการรายงาน (Reporting) – การรายงานขององค์กรมีความเชื่อถือได้
- วัตถุประสงค์ด้านการปฏิบัติตามข้อกำหนด (Compliance) – องค์กรได้ปฏิบัติตามข้อกำหนดหรือกฎหมายที่ใช้บังคับองค์กร

8 องค์ประกอบหลักของ ERM

1. สภาพแวดล้อมภายในองค์กร (Internal Environment)
   - คือ ท่าที (Tone) ที่องค์กรมองเรื่องความเสี่ยงและดำเนินการเรื่องความสี่ยงเช่นไร สภาพแวดล้อมภายในองค์กร จะเป็นตัวกำหนดพื้นฐานของการบริหารความเสี่ยงองค์กร

2. การกำหนดวัตถุประสงค์ (Objective Setting)

- องค์กรต้องกำหนดวัตถุประสงค์/เป้าหมายการดำเนินธุรกิจ ก่อนที่จะระบุเหตุการณ์ที่อาจส่งผลกระทบต่อการบรรลุวัตถุประสงค์/เป้าหมายนั้น ๆ
- วัตถุประสงค์ต้องสอดรับกับการยอมรับในความเสี่ยง (Risk Appetite)

3. การระบุเหตุการณ์ (Event Identification)

- การระบุเหตุการณ์ทั้งภายในและภายนอกองค์กร รวมทั้งที่องค์กรควบคุมได้และควบคุมไม่ได้ ที่อาจเกิดขึ้นแล้วส่งผลกระทบต่อการบรรลุวัตถุประสงค์ โดยจะต้องแยกแยะให้ออกระหว่าง “ความเสี่ยง” กับ “โอกาส”
- หากมี “โอกาส” จะต้องสื่อสารกลับไปยังฝ่ายจัดการเพื่อกำหนดวัตถุประสงค์และกลยุทธ์

4. การประเมินความเสี่ยง (Risk Assessment)

- การวิเคราะห์ระดับความเสี่ยงจะพิจารณาถึงโอกาส (Likelihood) และผลกระทบ (Impact) ที่จะเกิด เพื่อเป็นพื้นฐานในการที่จะจัดการกับความเสี่ยงนั้น ๆ
- การประเมินความเสี่ยงจะประเมินอยู่บนพื้นฐานของ Inherent risk และ Residual risk

การประเมินความเสี่ยง (Risk Assessment) (ต่อ)

- **โอกาสที่จะเกิดความเสียหายต่อองค์กร**

  คือการพิจารณาปัจจัยเสี่ยงแต่ละปัจจัยว่ามีโอกาสที่จะเกิดในระดับมากน้อยเพียงใด

- **ความเสียหายที่จะกระทบต่อองค์กร**

  คือการพิจารณาปัจจัยเสี่ยงแต่ละปัจจัยว่าหากเกิดขึ้นแล้วมีผลกระทบต่อหน่วยงานมากน้อยแค่ไหน

- **ความสำคัญของความเสี่ยงที่องค์กรเผชิญอยู่**

  คือการลำดับความสำคัญของแต่ละปัจจัยเสี่ยงเพื่อพิจารณาว่าความเสี่ยงใดควรพิจารณาจัดการก่อนหลัง

โอกาสที่จะเกิดความเสียหายต่อองค์กร และ ความเสียหายที่จะกระทบต่อองค์กร สามารถพิจารณาได้ 2 ลักษณะ ได้แก่

- <u>วิธีการประเมินความเสี่ยงเชิงคุณภาพ (Qualitative Approach)</u>

  ซึ่งจะไม่มีการระบุค่าของความเสียหายออกมาเป็นตัวเลขแต่ระบุออกเป็นระดับความรุนแรงของความเสียหาย และระดับของความเป็นไปได้ที่เหตุการณ์จะเกิดขึ้น

- <u>วิธีการประเมินความเสี่ยงเชิงปริมาณ (Quantitative Approach)</u>

  ซึ่งจะต้องระบุค่าของความเสียหายออกมาเป็นตัวเลข (โดยเฉพาะเป็นตัวเงิน) และโอกาสที่เหตุการณ์นั้นจะเกิดออกมาในรูปของความน่าจะเป็น (Probability)ซึ่งแสดงในรูปของตัวเลขเช่นกัน

โอกาสที่จะเกิดเหตุการณ์ที่เป็นความเสี่ยง

โอกาสที่จะเกิดความเสี่ยง	ความถี่ที่เกิดขึ้น (เฉลี่ย)	ระดับคะแนน
สูงมาก	1 เดือนต่อครั้ง	5
สูง	6 เดือนต่อครั้ง	4
ปานกลาง	12 เดือนต่อครั้ง	3
น้อย	มากกว่า 1 ปีต่อครั้ง	2
น้อยมาก	มากกว่า 5 ปีต่อครั้ง	1

โอกาสที่จะเกิดเหตุการณ์ที่เป็นความเสี่ยง

โอกาสที่จะเกิดความเสี่ยง	เปอร์เซ็นต์โอกาสที่จะเกิดขึ้น	ระดับคะแนน
สูงมาก	มากกว่า 80%	5
สูง	70-79%	4
ปานกลาง	60-69%	3
น้อย	50-59%	2
น้อยมาก	น้อยกว่า 50%	1

ผลกระทบต่อองค์กร (ด้านตัวเงิน)

ผลกระทบต่อองค์กร	ความเสียหาย	ระดับคะแนน
สูงมาก	มากกว่า 10 ล้านบาท	5
สูง	5แสนบาท -10 ล้านบาท	4
ปานกลาง	1แสนบาท - 5 แสนบาท	3
น้อย	1 หมื่นบาท - 1 แสนบาท	2
น้อยมาก	น้อยกว่า 1 หมื่นบาท	1

ผลกระทบต่อองค์กร (ด้านเวลา)

ผลกระทบต่อองค์กร	ความเสียหาย	ระดับคะแนน
สูงมาก	ทำให้เกิดความล่าช้าของโครงการ มากกว่า 6 เดือน	5
สูง	ทำให้เกิดความล่าช้าของโครงการ ระหว่าง 4 - 6 เดือน	4
ปานกลาง	ทำให้เกิดความล่าช้าของโครงการ ระหว่าง 3 - 4 เดือน	3
น้อย	ทำให้เกิดความล่าช้าของโครงการ ระหว่าง 2 - 3 เดือน	2
น้อยมาก	ทำให้เกิดความล่าช้าของโครงการน้อยกว่า 2 เดือน	1

ผลกระทบต่อองค์กร (ด้านชื่อเสียง)

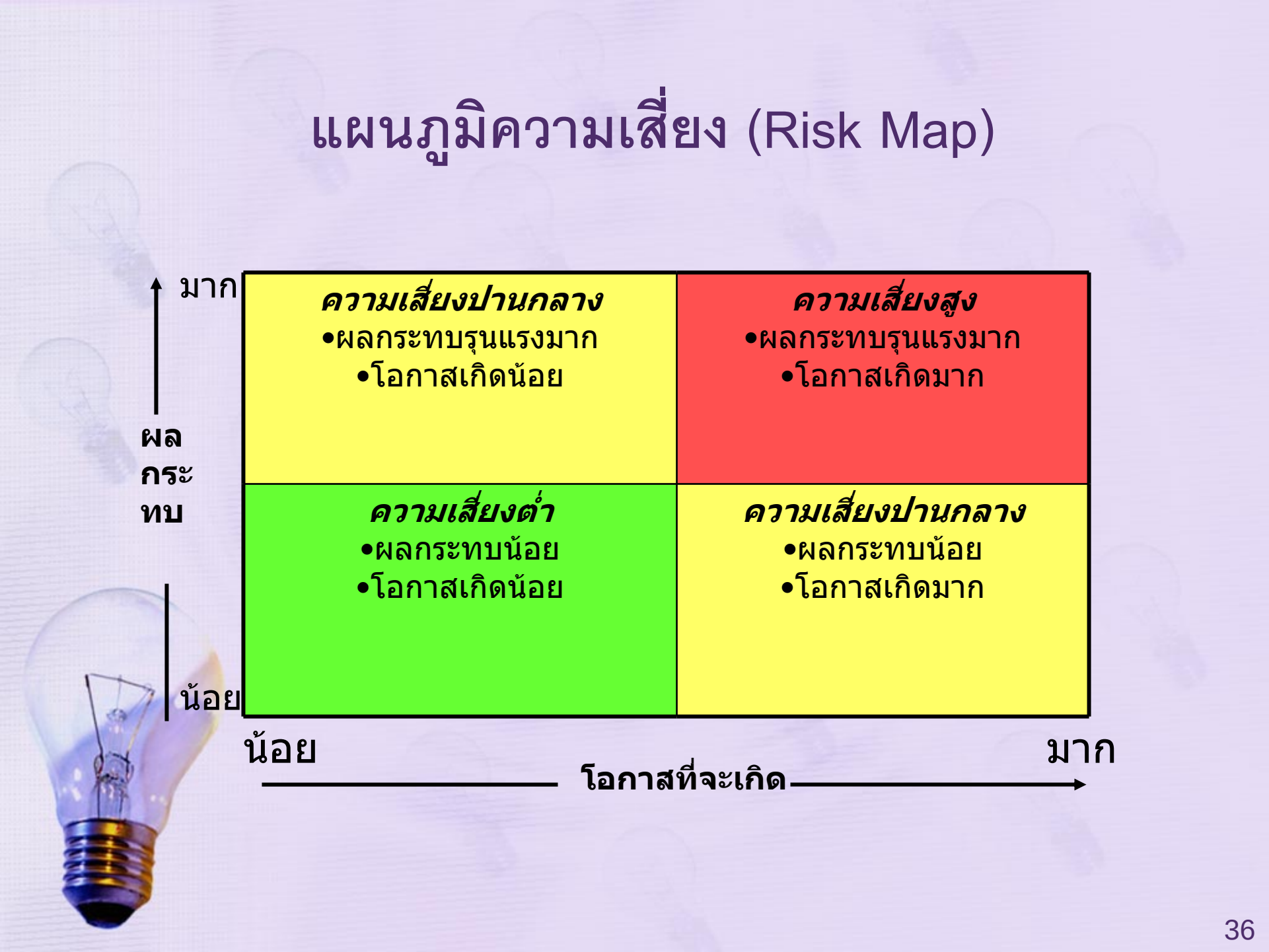
ผลกระทบต่อองค์กร	ความเสียหาย	ระดับคะแนน
สูงมาก	มีการเผยแพร่ข่าวทั้งจากสื่อภายในและต่างประเทศเป็นวงกว้าง	5
สูง	มีการลงข่าวในหนังสือพิมพ์ในประเทศหลายฉบับมากกว่า 15 วัน	4
ปานกลาง	มีการลงข่าวในหนังสือพิมพ์ในประเทศหลายฉบับ 2-3 วัน	3
น้อย	มีการลงข่าวในหนังสือพิมพ์ในประเทศบางฉบับ 1 วัน	2
น้อยมาก	ไม่มีการเผยแพร่ข่าว	1

การจัดลำดับความเสี่ยง

-รวมคะแนนระหว่างโอกาสที่จะเกิดกับความเสียหายและผลกระทบความเสียหายที่เกิด เพื่อจัดลำดับความสำคัญ และใช้ในการตัดสินใจว่าปัจจัยความเสี่ยงใดต้องเร่งจัดการก่อน

-จัดทำแผนภูมิความเสี่ยงเพื่อให้ผู้บริหารและคนในองค์กรได้เห็นภาพรวมว่าความเสี่ยงมีการกระจายตัวอย่างไร

แผนภูมิความเสี่ยง (Risk Map)



5. การจัดการ/ตอบโต้ความเสี่ยง (Risk Response) 4 แนวทางหลัก

- การหลีกเลี่ยงความเสี่ยง (Avoidance) ไม่ทำ /เลิกกิจกรรมนั้น
- การลดความเสี่ยง (Reduction) อาจลดโอกาส หรือผลกระทบ หรือลดทั้ง 2 อย่าง
- การหาผู้ร่วมเสี่ยง (Sharing) อาจลดโอกาส หรือผลกระทบ โดยการโอนความเสี่ยง (ทำประกัน) หรือแชร์บางส่วนของความเสี่ยง หรือ การ Outsourcing
- การยอมรับความเสี่ยง (Acceptance) อาจเป็นเพราะระดับความเสี่ยงต่ำมากจนไม่คุ้ม หรือสูงเกินไปเสียจนไม่มีหนทางที่จะจัดการกับความเสี่ยงนั้น

6. กิจกรรมการควบคุม (Control Activities)

- คือ นโยบายและวิธีการต่าง ๆ ที่กำหนดขึ้นและนำไปปฏิบัติเพื่อช่วยก่อให้เกิดความเชื่อมั่นได้ว่า ได้มีการดำเนินการกับความเสี่ยงได้อย่างเหมาะสม
- กิจกรรมการควบคุม เกิดขึ้นทุกขณะ ในทุกหน้าที่และทุกระดับ ทั่วทั้งองค์กร
- กิจกรรมการควบคุมสามารถจัดกลุ่มได้ตามลักษณะของวัตถุประสงค์ขององค์กร อันได้แก่ วัตถุประสงค์ด้านกลยุทธ์ ด้านการปฏิบัติงาน ด้านการรายงาน และด้านการปฏิบัติตามกฎระเบียบ

7. **สารสนเทศและการสื่อสาร** (Information and Communication)

ต้องระบุสารสนเทศที่จำเป็น รับทราบได้ และสื่อสารไปยังบุคลากรในองค์กรในรูปแบบและช่วงเวลาที่เหมาะสมเพื่อให้บุคลากรปฏิบัติหน้าที่ของตนได้

- **สารสนเทศ** (Information)
- **การสื่อสาร** (Communication)

8. การติดตามประเมินผล (Monitoring)

มีการติดตามประเมินการบริหารความเสี่ยงแบบครบวงจร และมีการปรับแก้ตามความเหมาะสม การประเมินอาจทำได้ โดย

- การติดตาม/ประเมินในขณะที่ธุรกิจกำลังดำเนินไป (Ongoing Monitoring Activities)
- การประเมินแยกต่างหาก (Separate Evaluations)
- หรือทั้ง 2 แบบ

ข้อจำกัดของ ERM

- ความเสี่ยงเป็นเรื่องของอนาคตซึ่งมีความไม่แน่นอน
- การบริหารความเสี่ยงในแต่ละระดับขององค์กร ต่างมีวัตถุประสงค์ต่างกัน ดังนั้น ERM จะช่วยให้คณะกรรมการหรือผู้บริหารทราบได้ในเวลาอันเหมาะสม เพียงแค่ว่าองค์กรกำลังมุ่งสู่ทิศทางใด และเข้าใกล้ความสำเร็จมากน้อยแค่ไหน แต่ไม่สามารถให้ความเชื่อมั่นอย่างเต็มที่ได้ว่าจะสามารถบรรลุวัตถุประสงค์ได้

ERM ไม่สามารถให้ความเชื่อมั่นอย่างเต็มที่ (Absolute Assurance) เนื่องจากปัจจัยหลายกรณี เช่น

- ปัจจัยภายใน ได้แก่ management override, judgment (error, wrong decision), breakdowns, collusion, and cost vs. benefit
- ปัจจัยภายนอก ได้แก่ การเปลี่ยนแปลงในนโยบายของภาครัฐ เศรษฐกิจ การเมือง หรือการดำเนินการจากคู่แข่ง เป็นต้น

การนำเอา ERM ไปใช้ในองค์กร

ปัจจัยสู่ความสำเร็จ

- การสนับสนุนอย่างเต็มที่จากผู้บริหารและคณะกรรมการฯ
- กลุ่มคนที่จะช่วยผลักดันได้ข้ามสายงาน/หน่วยงานอย่างทุ่มเทและต่อเนื่อง
- เชื่อม ERM เข้ากับวัตถุประสงค์หลักในเชิงกลยุทธ์หรือวัตถุประสงค์ทางการเงิน และเชื่อมกับกระบวนการวางแผนธุรกิจเพื่อให้บรรลุวัตถุประสงค์
- นำเอา ERM มาใช้เสมือนเป็นสิ่งที่เสริมกระบวนการที่เป็นที่ยอมรับดีอยู่แล้ว ไม่ใช่เป็นสิ่งใหม่หรือกระบวนการที่แยกออกไปอยู่ต่างหาก
- แสวงหาหรือใช้แนวคิดจากภายนอก
- เลือกดำเนินให้เหมาะสมโดยอาจค่อย ๆ ดำเนินการเพิ่มขึ้น หรือดำเนินการพร้อมกันทั้งองค์กร

Q & A