การพัฒนาระบบบริหารความเสี่ยง

บุปผา ชวะพงษ์

ขอบเขตการศึกษา

1. กรอบแนวคิดเกี่ยวกับการบริหารความเสี่ยง

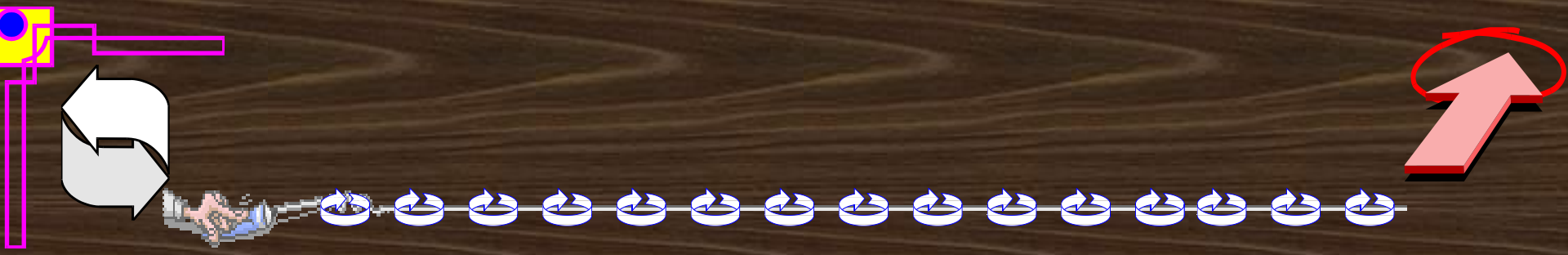
2. กระบวนการบริหารความเสี่ยง

2.1 การควบคุมภายใน

2.2 การบริหารความเสี่ยงทั้งองค์กร

3. การนำหลักการบริหารความเสี่ยงไปใช้ในองค์กร

1. กรอบแนวคิดเกี่ยวกับการบริหารความเสี่ยง



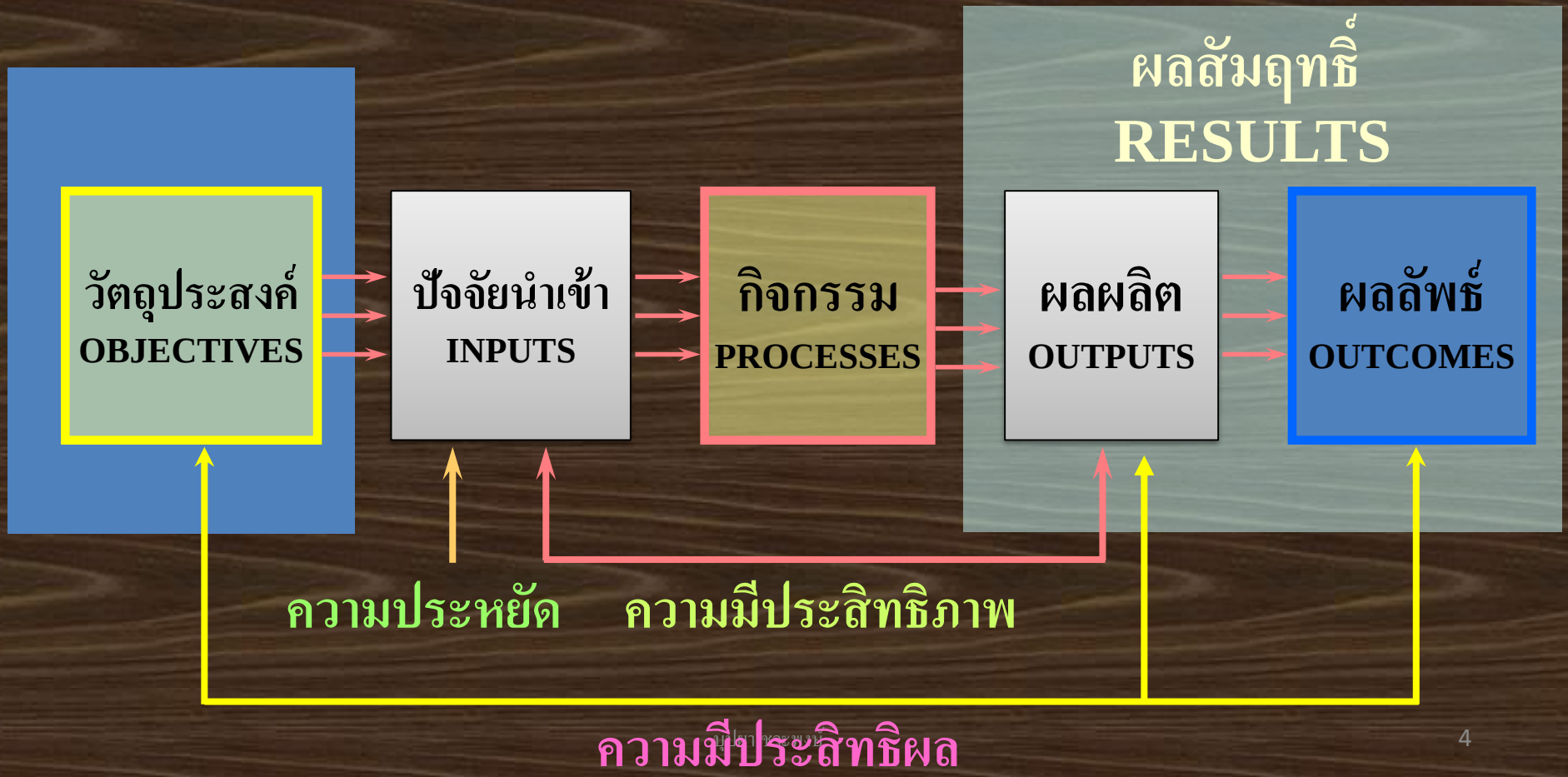
กรอบแนวคิด เรื่องการวัดผลสัมฤทธิ์

ปฏิบัติงานถูกต้องหรือไม่

Doing the things right

ทำในสิ่งที่ถูกต้องหรือไม่

Doing the right things



ความเสี่ยงคืออะไร

1.1 ความเสี่ยงคืออะไร

- เหตุการณ์หรือการกระทำที่อาจจะเกิดขึ้น (Potential Event) และมีผลทำให้องค์กรเสียหายหรือไม่สามารถบรรลุวัตถุประสงค์ / เป้าหมายที่กำหนด
- วัดความเสี่ยงโดยพิจารณาจากผลกระทบต่อเป้าหมาย กลยุทธ์ และวัตถุประสงค์ขององค์กร และโอกาสที่จะเกิดขึ้น

ความเสี่ยง = โอกาส x ผลกระทบ

ทำไมต้องมีการบริหารความเสี่ยง

- เป็นแนวทางที่ช่วยให้องค์กรมุ่งสู่ Good Governance
- SET กำหนดให้บริษัทจดทะเบียนฯ ปฏิบัติตามหลักการกำกับดูแลกิจการที่ดี 15ข้อ ซึ่งมี Risk Management รวมอยู่ด้วย
- เป็นหน้าที่ของผู้บริหารองค์กรที่ต้องจัดให้มีระบบบริหารความเสี่ยงเพื่อสร้างมูลค่าเพิ่มให้กับองค์กร และ Stakeholder
- สาเหตุของความล้มเหลวขององค์กรส่วนหนึ่งมาจากการที่ไม่มีระบบบริหารความเสี่ยง

1.1 (1) ตัวอย่างการวัดโอกาสที่อาจเกิดขึ้น

- โอกาสที่อาคารจะถูกไฟไหม้ 1 5
- โอกาสที่ระบบคอมพิวเตอร์จะติดไวรัส 1 5
- โอกาสที่อัตราดอกเบี้ยจะขึ้นอีก1% ในปี 2550 1 5
- โอกาสที่จะเกิดแผ่นดินไหวใน ปี 2550 1 5
- โอกาสที่พนักงานคนเก่งลาออก 10% 1 5

1.1 (2) ตัวอย่างการวัดผลกระทบ

- ผลกระทบที่อาคารจะถูกไฟไหม้ 1 5
- ผลกระทบจากระบบคอมพิวเตอร์จะติดไวรัส 1 5
- ผลกระทบที่อัตราดอกเบี้ยขึ้นอีก 1% ในปี 2550 1 5
- ผลกระทบจากแผ่นดินไหว 1 5
- ผลกระทบที่พนักงานคนเก่งลาออก 10% 1 5

1.1 (3) ผลกระทบ

ผลกระทบที่อาจจะเกิดขึ้นไม่ได้วัดเป็นตัวเงินเพียงอย่างเดียว

- ทรัพย์สิน ทรัพยากรอื่นๆ และบุคลากร
- รายได้และชื่อขององค์กร
- ต้นทุนกิจกรรม
- ประชาชน ชุมชน
- ผลการปฏิบัติงาน

1.1 (3) ผลกระทบ (ต่อ)

ผลกระทบที่อาจจะเกิดขึ้นไม่ได้วัดเป็นตัวเงินเพียงอย่างเดียว (ต่อ)

- เวลาขั้นตอนการปฏิบัติงาน
- สิ่งแวดล้อม
- ชื่อเสียง ค่านิยม และคุณภาพชีวิต
- พฤติกรรมองค์กร

1.2 ประเภทของความเสี่ยง

จำแนกตามแหล่งที่มา : -

- Externally-driven (environment)
  - Competitors, Legal &Regulatory, Capital &Financial Markets, Industry, Catastrophic events etc
- Internally-driven (process)
  - Operation, IT, Financial, Fraud, empowerment, Information for decision making

1.2 ประเภทของความเสี่ยง

จำแนกตามการดำเนินงาน :-

- ☹ ความเสี่ยงด้านกลยุทธ์
- ☹ ความเสี่ยงด้านการเงิน และงบประมาณ
- ☹ ความเสี่ยงด้านการจัดซื้อจัดจ้าง และบริหารสัญญา
- ☹ ความเสี่ยงด้านบำรุงรักษา และบริหารจัดการระบบ
- ☹ ความเสี่ยงด้านการบริหารงานบุคคล
- ☹ ความเสี่ยงด้านการปฏิบัติงาน

ฯลฯ

1.2 (1) ความเสี่ยงด้านกลยุทธ์

- การดำเนินกลยุทธ์ที่ผิดพลาด หรือไม่เหมาะสม
- การไม่ปฏิบัติตามกลยุทธ์
- การนำกลยุทธ์ไปปฏิบัติอย่างไม่เหมาะสม
- คุณภาพการบริหารไม่ดี/ความไม่เหมาะสมในการจัดการ
- ใช้คน/เงิน/สิ่งของ ในการดำเนินงานไม่เหมาะสม --- รั่วไหล/เสียหาย

1.2 (2) ความเสี่ยงด้านการเงินและงบประมาณ

- การกำหนดแนวทาง แผนการจัดการ และการควบคุมการใช้งบประมาณอย่างไม่เหมาะสม
- การกำหนดนโยบายและวิธีการทางบัญชี ไม่เหมาะสม
- การวางระบบตลอดจนการบันทึกบัญชี และรายงานทางการเงินที่ผิดพลาด
- ความไม่ปลอดภัยในการเก็บรักษาเงินสด และเอกสารแทนตัวเงิน

1.2 (3) ความเสี่ยงด้านการจัดซื้อจัดจ้าง และการบริหารสัญญา

- การจัดซื้อจัดจ้างที่ไม่มีหลักเกณฑ์การปฏิบัติที่ดี
- การจัดซื้อจัดจ้างที่ขาดการวางแผน
- การจัดซื้อจัดจ้างที่ขัดต่อกฎหมาย ระเบียบ ข้อบังคับฯ
- ข้อกำหนด/ข้อบังคับของสัญญา ทำให้องค์กรได้รับความเสียหาย
- การบริหารสัญญาที่ผิดพลาด
- การใช้ประโยชน์จากการจัดซื้อ จัดจ้างไม่คุ้มค่า

1.2 (4) ความเสี่ยงด้านการบำรุงรักษา และบริหารจัดการระบบ

- การเปลี่ยนแปลงของนโยบายและแผน
- การได้รับงบประมาณไม่เพียงพอ
- การสำรวจออกแบบก่อสร้างไม่ครบถ้วนสมบูรณ์ ไม่ถูกต้องตามหลักวิชาการ
- การบริหารจัดการไม่ดี (ขาดคู่มือ, ขาดผู้นำที่ดี)
- บุคลากรที่เกี่ยวข้องไม่มีศักยภาพ & ประสบการณ์
- ความซับซ้อนของระบบงาน

1.2 (5) ความเสี่ยงด้านการบริหารงานบุคคล

- กระบวนการสรรหาไม่โปร่งใส ไม่เป็นธรรม
- กระบวนการบรรจุ แต่งตั้ง โยกย้าย ไม่เหมาะสม ไม่เป็นธรรม
- กระบวนการพัฒนาไม่เหมาะสม ไม่มีความต่อเนื่อง

- กระบวนการสร้างขวัญและกำลังใจในการปฏิบัติงานไม่เหมาะสม

1.2 (6) ความเสี่ยงด้านการปฏิบัติงาน

กระบวนการจัดการขาดความพร้อม

- บุคลากร
- ระบบงาน
- เทคโนโลยีสารสนเทศ
- เครื่องมือ อุปกรณ์
- ด้านกายภาพของสำนักงาน

1.3 แหล่งที่มาของความเสี่ยง (Sources of Risks)

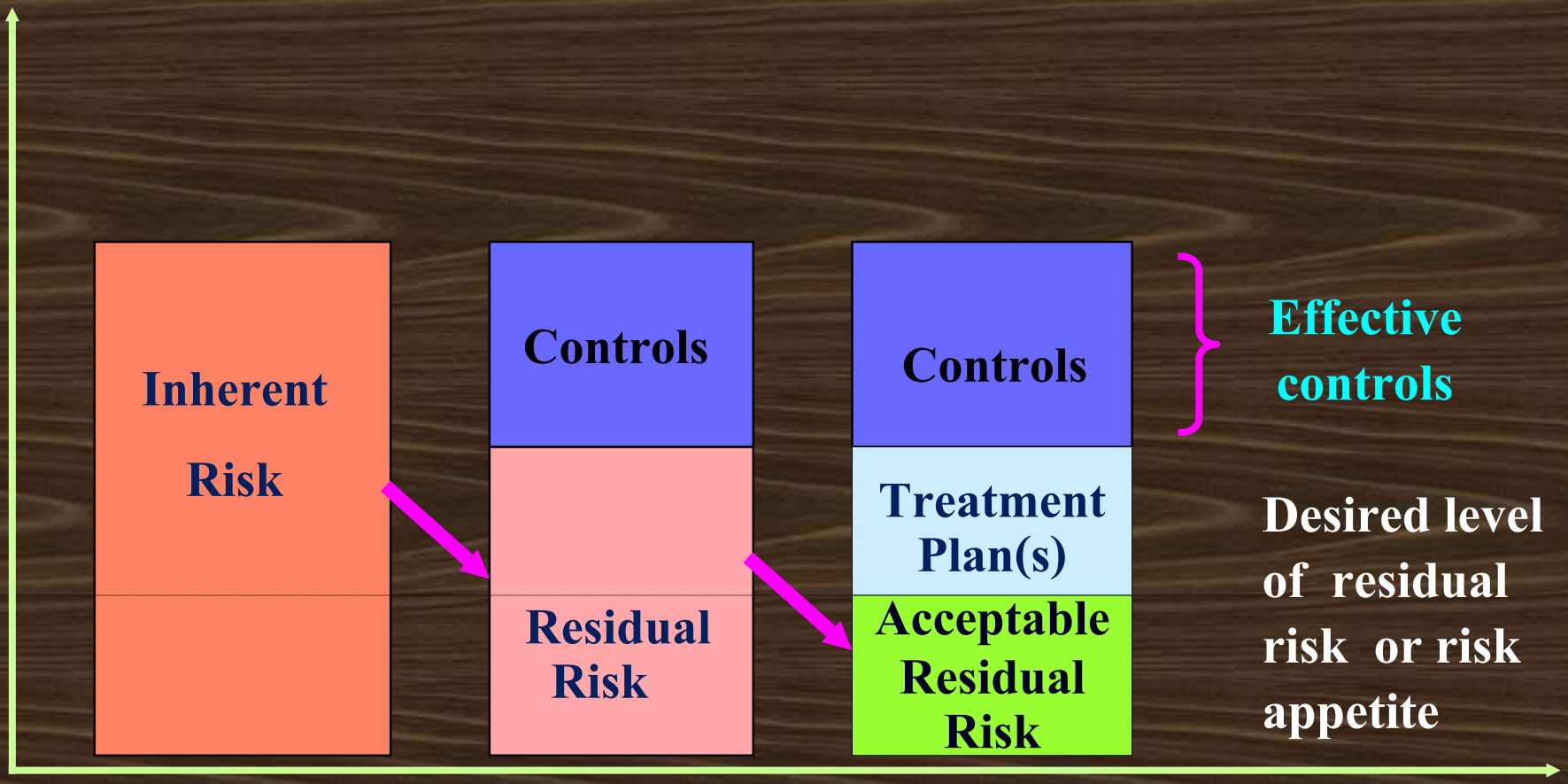
- Commercial and legal relationships
- Economic circumstances
- Human behavior
- Natural events
- Political circumstances
- Technology and technical issues
- Management activities and controls
- Individual activities.

1.4 Inherent Risk & Residual Risk

- **Inherent Risk** คือความเสี่ยงก่อนที่จะมีมาตรการควบคุมหรือการบริหารจัดการ

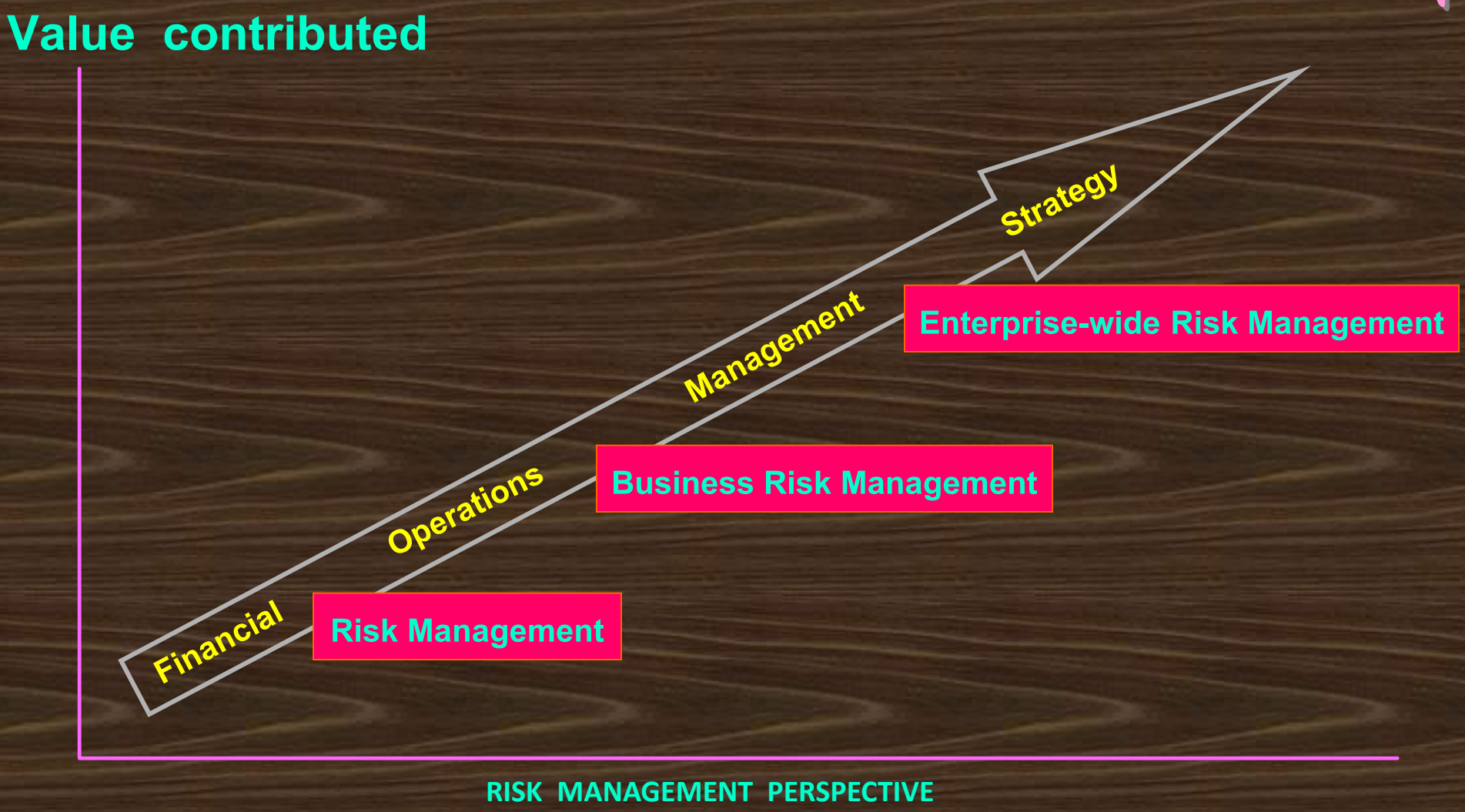
- **Residual Risk** คือความเสี่ยงที่เหลืออยู่หลังจากมีการควบคุมหรือบริหารจัดการเพื่อลดโอกาสที่จะเกิดและหรือผลกระทบแล้ว

1.5 Risk Management Concept



Cost & Benefit of controls must be considered

1.6 พัฒนาการของการบริหารความเสี่ยง



1.7 ประโยชน์ของการบริหารความเสี่ยง ที่มีประสิทธิภาพ

- ช่วยให้องค์กรสามารถบริหารความเสี่ยงหรือเหตุการณ์ ที่อาจจะเกิดขึ้นได้อย่างมีประสิทธิภาพ
- ช่วยให้สามารถกำหนดแผนกลยุทธ์และวัตถุประสงค์ที่สอดคล้องกับความเสี่ยงที่ยอมรับได้
- ช่วยให้สามารถตัดสินใจและเลือกกลยุทธ์ในการบริหารความเสี่ยงได้ดีขึ้น

1.7 ประโยชน์ของการบริหารความเสี่ยงที่มีประสิทธิภาพ

- บริหารความเสี่ยงในภาพรวมและทั่วทั้งองค์กร
- สร้างโอกาสทางธุรกิจ
- จัดสรรทรัพยากรได้ดีขึ้น
- การดำเนินงานเป็นไปตามกฎหมาย
- ระบบข้อมูลเพื่อการตัดสินใจดีขึ้น
- ช่วยให้การวางแผนตรวจสอบภายในดีขึ้น

1.8 บทบาทและหน้าที่ในการบริหารความเสี่ยง

- ทุกคนในองค์กรมีหน้าที่ในการบริหารความเสี่ยงที่จะกระทบต่อวัตถุประสงค์หรือเป้าหมายที่รับผิดชอบ
- คณะกรรมการบริษัท มีหน้าที่ในการกำกับดูแลให้มีนโยบายและการบริหารความเสี่ยงที่มีประสิทธิผล
- คณะกรรมการตรวจสอบ ทำหน้าที่ในการสอบทานระบบบริหารความเสี่ยงให้มีประสิทธิผล

1.8 บทบาทและหน้าที่ในการบริหารความเสี่ยง

- ผู้ตรวจสอบภายใน
  - มีหน้าที่ในการตรวจสอบและประเมินประสิทธิภาพ / ประสิทธิผลของระบบบริหารความเสี่ยง
  - ในบางองค์กรอาจทำหน้าที่เป็นที่ปรึกษาในการจัดระบบ ประเมินระบบการควบคุม จัดอบรม ประเมินความเสี่ยง และกำกับดูแลกระบวนการบริหารความเสี่ยง

2. กระบวนการบริหารความเสี่ยง

กระบวนการบริหารความเสี่ยงในองค์กร

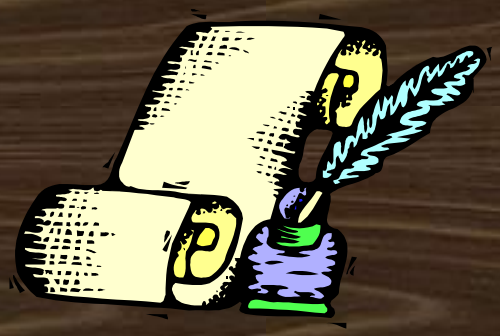
- ความเสี่ยงในองค์กรมีอยู่กระจัดกระจายในกระบวนการทำงาน
- หน่วยงานที่มีความเสี่ยงต้องจัดให้มีการบริหารความเสี่ยงอย่างเป็นระบบ
- กำหนดขึ้นเป็นแนวทางในการบริหารความเสี่ยง
- ดำเนินการบริหารความเสี่ยงตามแนวทางที่กำหนด

กระบวนการบริหารความเสี่ยง

COSO คือใคร

COSO คือ Committee of Sponsoring Organization of Treadway Commission ประกอบด้วย

1. สถาบันผู้สอบบัญชีรับอนุญาตแห่งสหรัฐอเมริกา
2. สถาบันผู้ตรวจสอบภายในสากล
3. สถาบันผู้บริหารการเงิน
4. สมาคมนักบัญชีแห่งสหรัฐอเมริกา
5. สถาบันนักบัญชีเพื่อการบริหาร



องค์ประกอบหลักของการบริหารความเสี่ยง

จากแนวคิดของ COSO

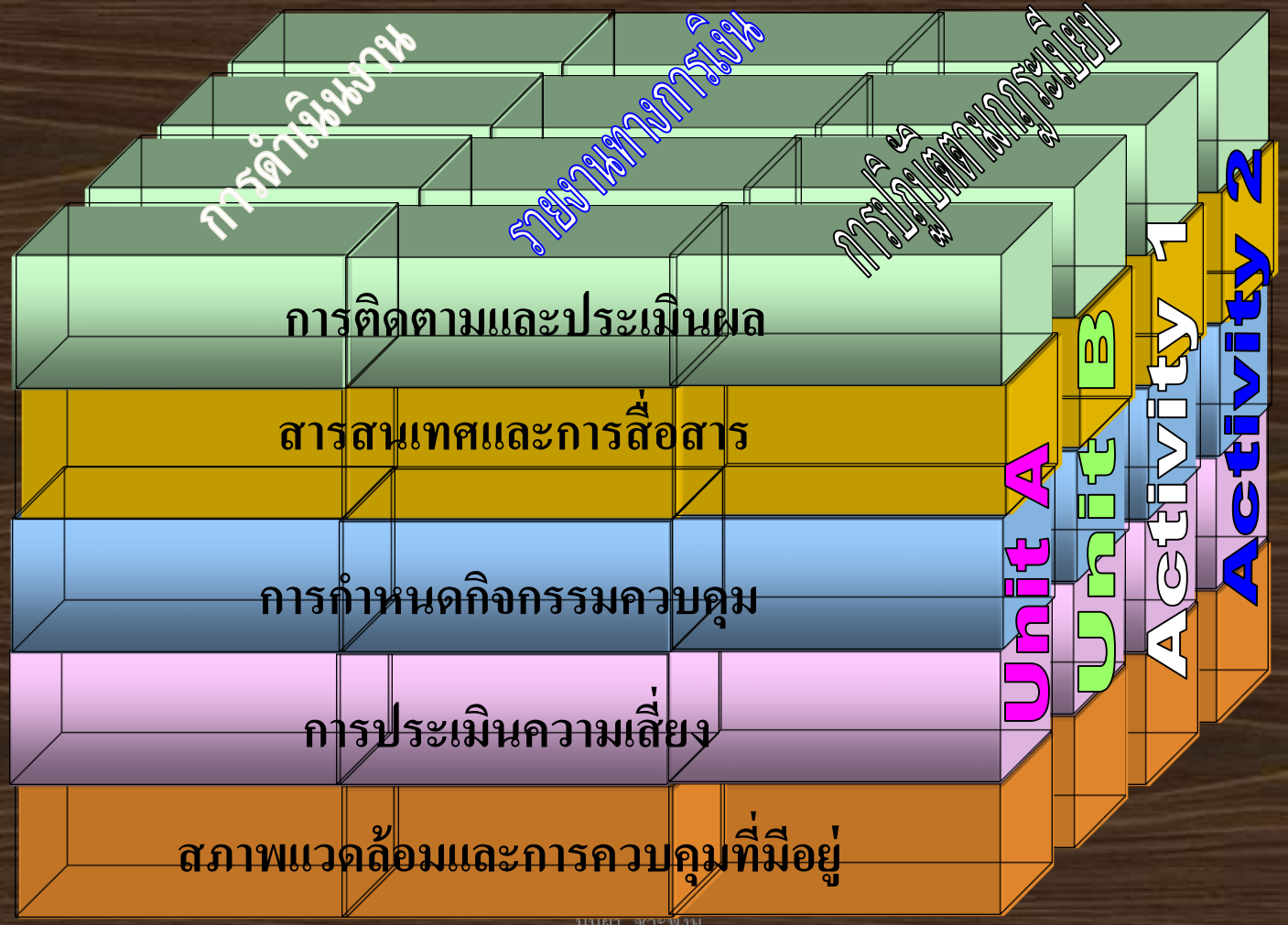
เดิม Internal Control : 5 Components

ใหม่ ERM Framework : 8 Components

Entity ’s objectives and Units

หลักการควบคุมภายในตามแนวคิดของ COSO

COSO INTERNAL CONTROL FRAMEWORK



หลักการบริหารความเสี่ยงทั้งองค์กรตามแนวคิดของ COSO

COSO ERM Framework

2.1 การควบคุมภายใน

(INTERNAL CONTROL FRAMEWORK)

(1) ความหมาย วัตถุประสงค์ ของการควบคุมภายใน

การควบคุมภายในตามความหมายของ COSO

"กระบวนการปฏิบัติงานที่ทุกคนในองค์การตั้งแต่คณะกรรมการบริหาร ผู้บริหารทุกระดับ และพนักงานทุกคน ร่วมกันกำหนดให้เกิดขึ้น เพื่อสร้างความมั่นใจในระดับที่สมเหตุสมผลในการบรรลุวัตถุประสงค์ 3 ด้าน" ได้แก่

1. ด้านการปฏิบัติการ (O)
2. ด้านการรายงานทางการเงิน (F)
3. ด้านการปฏิบัติตามกฎหมายและกฎระเบียบที่เกี่ยวข้อง (C)

(1) ความหมาย วัตถุประสงค์ ของการควบคุมภายใน

การบรรลุวัตถุประสงค์ :-

O • ประสิทธิภาพ และประสิทธิผลของการดำเนินงาน

• การดำเนินงานบรรลุวัตถุประสงค์และเป้าหมายที่กำหนด

F • ความเชื่อถือได้ของข้อมูลและรายงานการเงิน

• การควบคุมดูแลทรัพย์สิน

C • การปฏิบัติตามกฎหมายและกฎระเบียบที่เกี่ยวข้อง

All the things you have to do for sustainable and ethical achievement of business objectives.

(1) ความหมาย วัตถุประสงค์ ของการควบคุมภายใน (ต่อ)

1. เป็น “กระบวนการ” คือสิ่งที่ต้องกระทำอย่างเป็นขั้นตอน แต่ไม่ได้เป็นผลสุดท้าย เช่น นักกีฬาต้องซ้อม ต้องสุขภาพดี จึงจะชนะ

2. ไม่ใช่เพียงกำหนดนโยบาย แบบฟอร์มสวยงาม หรือไม่ใช่คู่มือที่วางไว้บนหิ้งหนังสือ แต่เป็นกระบวนการที่ทุกคนในองค์กรร่วมมือกันทำและมีการปรับปรุงอย่างต่อเนื่อง

(1) ความหมาย วัตถุประสงค์ ของการควบคุมภายใน (ต่อ)

3. ให้ความเชื่อมั่นในการบรรลุตามวัตถุประสงค์

อย่างสมเหตุสมผลเท่านั้น ไม่ใช่สมบูรณ์

100% เพราะมีข้อจำกัดที่แฝงอยู่

4. เพื่อความสำเร็จตามวัตถุประสงค์ 3 ด้าน

ของการควบคุม

(3) การควบคุมภายใน แบ่งเป็น 5 ประเภท

1. การควบคุมแบบป้องกัน (Preventive Controls)
   เช่น การอนุมัติ การจัดโครงสร้างองค์กร การแบ่งแยกหน้าที่ การใช้และการควบคุมเอกสารที่ดี การควบคุมการเข้าถึงเอกสาร ฯลฯ

2. การควบคุมแบบตรวจค้น (Detective Controls)
   เช่น การสอบทาน การวิเคราะห์ การยืนยันยอด การตรวจนับ การรายงานข้อบกพร่อง การตรวจสอบ ฯลฯ

(3) การควบคุมภายใน แบ่งเป็น 5 ประเภท (ต่อ)

3. การควบคุมแบบแก้ไข (Corrective Controls) : ควบคุม เพื่อแก้ไขข้อผิดพลาดที่เกิดขึ้นให้ถูกต้อง หรือไม่ให้เกิดซ้ำอีก

4. การควบคุมแบบสั่งการ (Directive Controls) : เป็นการกระตุ้นให้เกิดความสำเร็จ

5. การควบคุมทดแทน (Compensative Controls) : เช่น เช็คสอบการบันทึกข้อมูล 2 จุด จัดทำรายงานความแตกต่าง

(4) ตัวอย่างกิจกรรมการควบคุม

<u>ตัวอย่างกิจกรรมควบคุมที่ระบุในรายงาน COSO</u>

- การกำหนดนโยบายและวิธีปฏิบัติงานที่ชัดเจน
- การสอบทานโดยผู้บริหารสูงสุด
- การสอบทานโดยผู้บริหารระดับกลาง
- การควบคุมการประมวลผลข้อมูล
- การควบคุมทางกายภาพ
- การแบ่งแยกหน้าที่
- การใช้ดัชนีวัดผลการดำเนินงานที่สำคัญ

(4) ตัวอย่างกิจกรรมการควบคุม (ต่อ)

ตัวอย่างกิจกรรมควบคุมที่ระบุในรายงาน COSO

- การจัดทำหลักฐานเอกสาร
- การรักษาความปลอดภัย
- การสอบทานและการกำกับดูแลการปฏิบัติงาน
- ระบบงานคอมพิวเตอร์และการควบคุมด้านคอมพิวเตอร์

ฯลฯ

(5) ลักษณะของการควบคุมที่ดี

1. ไม่เสียค่าใช้จ่ายเกินควร
2. ควบคุมในจุดที่สำคัญ
3. เหมาะสมและเข้าใจง่าย
4. สอดคล้องกับเป้าหมาย
5. ทันกาล

(6) อุปสรรค ข้อจำกัดและปัญหา

ข้อจำกัดเกี่ยวกับการควบคุมภายใน (Inherent Limitations)

- การใช้ดุลยพินิจของฝ่ายบริหาร
- การละเว้นการปฏิบัติตาม
- เหตุการณ์พิเศษ
- การร่วมมือกันของบุคคลภายในหรือกับบุคคลภายนอกเพื่อหลีกเลี่ยงการควบคุมที่มีอยู่
- การก้าวก่ายของฝ่ายบริหาร
- ค่าใช้จ่ายในการควบคุมสูงกว่าค่าเสียหายที่อาจเกิดขึ้น

(7) การควบคุมภายในสมัยใหม่

สรุป

- เน้นให้เกิดการกำกับดูแลและการควบคุมที่ดีทั้งองค์กร
- โดยผู้บริหารทุกฝ่ายทุกระดับมีหน้าที่รับผิดชอบโดยตรง
- ต้องบริหารและควบคุมเพื่อลดความเสี่ยง

2.2 การบริหารความเสี่ยงทั้งองค์กร

(ERM : Enterprise wide Risk Management)

(1) ความหมายของ ERM ตามแนวคิดของ COSO

"การบริหารความเสี่ยงทั่วทั้งองค์กร" คือ กระบวนการที่กำหนดขึ้นและนำไปใช้โดยคณะกรรมการ ฝ่ายบริหาร และบุคลากรอื่นๆ ขององค์กร เพื่อกำหนดกลยุทธ์ และใช้กับหน่วยงานทั้งหมดในองค์กร โดยได้รับการออกแบบมาเพื่อระบุเหตุการณ์ที่อาจเกิดขึ้น ซึ่งอาจมีผลกระทบต่อองค์กร และจัดการความเสี่ยงให้อยู่ภายใต้ระดับความเสี่ยงที่องค์กรยอมรับได้ เพื่อให้ความเชื่อมั่นสมเหตุสมผลว่าองค์กรจะบรรลุวัตถุประสงค์ที่ตั้งไว้

(2) แนวคิดพื้นฐานของการบริหารความเสี่ยงทั้งองค์กร

1) เป็นกระบวนการ ซึ่งดำเนินไปอย่างต่อเนื่องทั้งองค์กร

2) ร่วมกันทำให้บังเกิดผลโดยบุคลากรทุกระดับขององค์กร

3) ประยุกต์ใช้ในการกำหนดกลยุทธ์และใช้ทั่วทั้งองค์กร

(2) แนวคิดพื้นฐานของการบริหารความเสี่ยงทั้งองค์กร (ต่อ)

4) กำหนดขึ้นเพื่อระบุถึงเหตุการณ์ที่อาจเกิดขึ้น และเมื่อเกิดแล้วมีผลกระทบทำให้องค์กรเสียหาย เพื่อจัดการให้ความเสี่ยงนั้นอยู่ในระดับที่ยอมรับได้

5) ให้ความเชื่อมั่นอย่างสมเหตุสมผลเท่านั้น ไม่ใช่ 100%

6) ช่วยให้องค์กรบรรลุวัตถุประสงค์อย่างใดอย่างหนึ่งหรือหลายๆ วัตถุประสงค์ที่เชื่อมโยงกัน

(3) วัตถุประสงค์ของ ERM

แบ่งเป็น 4 ประเภทคือ

1) ด้านกลยุทธ์

เป้าหมายระดับสูง สอดคล้องและสนับสนุนพันธกิจขององค์กร

2) ด้านการปฏิบัติงาน

การใช้ประโยชน์จากทรัพยากรมีประสิทธิภาพและประสิทธิผล

(3) วัตถุประสงค์ของ ERM (ต่อ)

3) ด้านการรายงาน

- ความถูกต้อง เชื่อถือได้ของรายงานการเงินและรายงานการปฏิบัติงาน

- เป็นประโยชน์ในการตัดสินใจ

4) ด้านการปฏิบัติตามกฎระเบียบ

- มีการปฏิบัติตามกฎหมาย กฎ ระเบียบ นโยบาย คำสั่งและคู่มือที่กำหนดไว้

(4) ความสำคัญและประโยชน์ของการบริหารความเสี่ยง

1) สมมติฐานเบื้องต้นของ ERM

- ทุกองค์กรดำรงอยู่เพื่อสร้างมูลค่าสูงสุดให้ผู้มีส่วนได้เสีย
- ทุกองค์กรต้องเผชิญความไม่แน่นอน ซึ่งเป็นทั้งโอกาสและความเสี่ยง
- ผู้บริหารต้องตัดสินใจว่าจะยอมรับความไม่แน่นอนในระดับใด → Risk Appetite

(4) ความสำคัญและประโยชน์ของการบริหารความเสี่ยง (ต่อ)

➡ จึงต้องกำหนดกลยุทธ์และวัตถุประสงค์ให้สมดุล และเหมาะสมที่สุด ระหว่าง

เป้าหมายการเติบโต / ผลกำไร กับ ความเสี่ยงที่เกี่ยวข้อง

(4) ความสำคัญและประโยชน์ของการบริหารความเสี่ยง (ต่อ)

2) ประโยชน์ของการบริหารความเสี่ยงทั้งองค์กร

- การจัดความสอดคล้องของระดับความเสี่ยงที่องค์กรยอมรับได้และกลยุทธ์
- การยกระดับการตัดสินใจตอบสนองต่อความเสี่ยง
- การลดโอกาสที่จะเกิดเหตุการณ์ที่ไม่คาดหมายและความสูญเสียในการปฏิบัติงาน
- การบ่งชี้และจัดการกับความเสี่ยงที่สลับซับซ้อนและทั่วทั้งองค์กร

(4) ความสำคัญและประโยชน์ของการบริหารความเสี่ยง (ต่อ)

2) ประโยชน์ของการบริหารความเสี่ยงทั้งองค์กร (ต่อ)

- การรู้จักใช้โอกาสที่เหมาะสม
- การปรับปรุงการจัดสรรเงินทุนและทรัพยากรอื่นๆ

(5) ข้อคิดที่สำคัญของ ERM

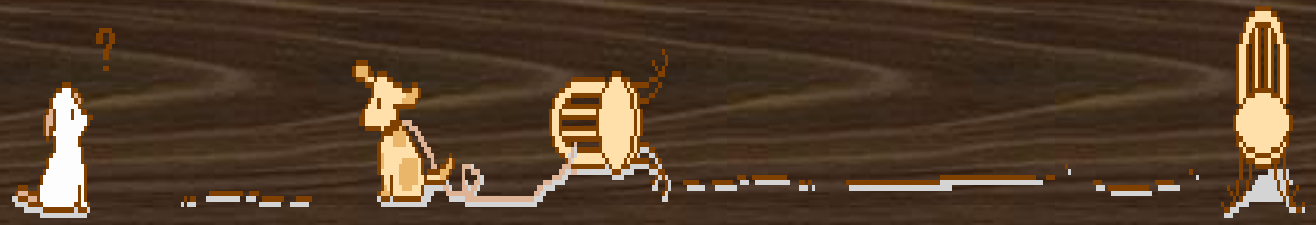
- ประกอบด้วย 8 องค์ประกอบ
- ไม่ได้เจตนากำหนดขึ้นทดแทนการควบคุมภายในเดิมที่มี 5 องค์ประกอบ
- แต่กำหนดขึ้นเพื่อลดจุดอ่อนบางประการ และเพิ่มความเข้มแข็ง ช่วยให้ระบบการบริหารความเสี่ยงทั้งองค์กรมีความสมบูรณ์มากยิ่งขึ้น

ได้ผนวกเอาการควบคุมภายในเดิมเข้าเป็นส่วนหนึ่งของ ERM

องค์ประกอบที่ 1 สภาพแวดล้อมในองค์กร

- หมายถึง บรรยากาศภายในองค์กรซึ่งมีอิทธิพลต่อจิตสำนึกเรื่องความเสี่ยงของบุคลากร

- เป็นพื้นฐานสำคัญ สำคัญสำหรับองค์ประกอบอื่นๆ ตัวอย่างเช่น



องค์ประกอบที่ 1 สภาพแวดล้อมในองค์กร (ต่อ)

* ปรัชญาและวัฒนธรรมในการบริหารความเสี่ยง
* ระดับความเสี่ยงที่องค์กรยอมรับได้
* บทบาทของคณะกรรมการในการกำกับดูแล
* ความซื่อสัตย์สุจริต และคุณค่าทางจริยธรรม
* ความสามารถของบุคลากร

องค์ประกอบที่ 1 สภาพแวดล้อมในองค์กร (ต่อ)

* การมอบหมายอำนาจหน้าที่และความรับผิดชอบ

* การจัดโครงสร้างองค์กร

* การพัฒนาบุคลากร

ฯลฯ

องค์ประกอบที่ 2 การกำหนดวัตถุประสงค์

- กำหนดวัตถุประสงค์ ทั้งระดับกลยุทธ์ การปฏิบัติงาน การรายงาน และการปฏิบัติตามกฎระเบียบ ให้สอดคล้องเชื่อมโยงกันตามลำดับชั้นตลอดทั้งองค์กร

- ต้องกำหนดวัตถุประสงค์ก่อนระบุเหตุการณ์ที่เป็นปัจจัยเสี่ยง การประเมินความเสี่ยง และการตอบสนองต่อความเสี่ยง

องค์ประกอบที่ 3 การระบุเหตุการณ์ที่เป็นปัจจัยเสี่ยง

ปัจจัยเสี่ยง = สาเหตุที่มาของความเสี่ยงที่ทำให้องค์กรไม่สามารถบรรลุวัตถุประสงค์

แยกได้เป็น
- ปัจจัยภายนอก
- ปัจจัยภายใน

วิธีการและเทคนิคที่ใช้ในการระบุปัจจัยเสี่ยง

- การรวมกลุ่มระดมสมอง
- การใช้แบบสอบถาม
- การสำรวจและวิจัย
- การประชุมเชิงปฏิบัติการ (workshop) ของผู้มีส่วนเกี่ยวข้อง
- การเก็บสถิติและการวิเคราะห์แนวโน้มเหตุการณ์ที่อาจจะเกิด

องค์ประกอบที่ 4 การประเมินความเสี่ยง

- หมายถึง การวิเคราะห์และจัดระดับความเสี่ยง

- ค่าความเสี่ยง = โอกาสเกิด X ผลกระทบ / หรือ ความเสียหาย

- โดยทั่วไป มักให้ค่าโอกาสและผลกระทบ ตั้งแต่ 1-5

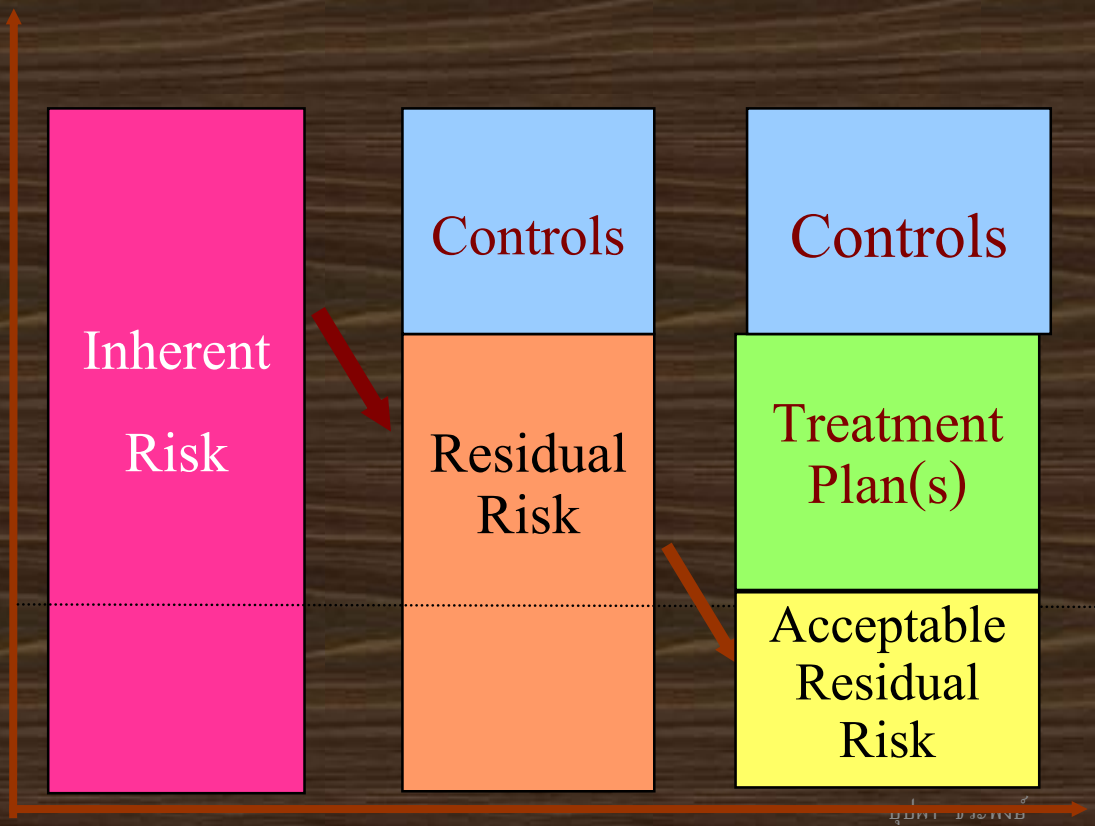
- ควรกำหนดเกณฑ์มาตรฐานที่ใช้ในการประเมินค่า

การประเมินความเสี่ยง

ประเมินระดับความรุนแรง ของความเสี่ยงและโอกาสที่อาจจะเกิดขึ้นก่อนการควบคุม (Inherent Risks)

ประเมินระบบการควบคุมที่มีอยู่ (Controls)

ประเมินความเสี่ยงที่เหลืออยู่หลังจากระบบการควบคุม (Residual Risks)



จัดลำดับความเสี่ยงโดยพิจารณาจากระดับความเสี่ยงสูง และ สูงมากเพื่อดำเนินการบริหารและจัดการ

Acceptable Residual Risk

องค์ประกอบที่ 5 การตอบสนองต่อความเสี่ยง

- เป็นการระบุมาตรการตอบสนองต่อความเสี่ยง เพื่อพิจารณาเลือกวิธีการที่เหมาะสมที่สุด เป็นวิธีการจัดการความเสี่ยงในองค์ประกอบที่ 6

- เพื่อลดโอกาสเกิดความเสี่ยง และ/หรือ ลดผลกระทบให้อยู่ในระดับความเสี่ยงที่ยอมรับได้ (Risk Appetite)

Basic Risk Management strategy

1. **Avoid** ขาย / หยุด / หลีกเลี่ยง
   ขจัดความเสี่ยงที่ยอมรับไม่ได้
2. **Retain / Accept** ยอมรับความเสี่ยง
   เมื่อมีการควบคุมที่มีประสิทธิภาพ
3. **Reduce / Control** ลด / ควบคุม
   จากกระบวนการภายใน

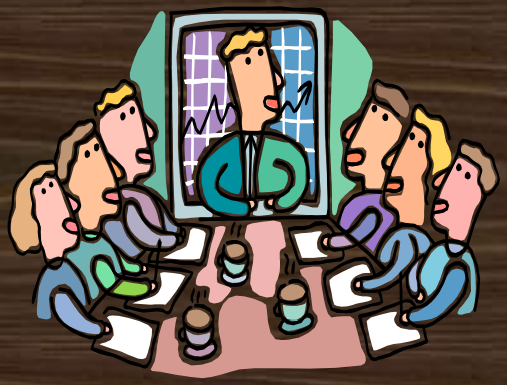
Basic Risk Management strategy

4. **Transfer** โอนไปให้บุคคลที่ 3 / ประกันภัย

   Hedging / Outsource

5. **Exploit** ใช้ประโยชน์ / หาธุรกิจใหม่

   เปลี่ยน **Profile** / ออกสินค้าใหม่



องค์ประกอบที่ 6 กิจกรรมการควบคุม

หมายถึง นโยบาย ระเบียบปฏิบัติ และมาตรการต่างๆ ที่ฝ่ายบริหารร่วมกันกำหนดและนำมาใช้

➡ เพื่อให้มั่นใจว่า สามารถตอบสนองต่อความเสี่ยงและบรรลุผลสำเร็จได้อย่างมีประสิทธิผล

ควรเกิดขึ้นทั่วทั้งองค์กร ทุกระดับ และทุกกิจกรรม

องค์ประกอบที่ 7 สารสนเทศและการสื่อสาร

- มีสารสนเทศที่จำเป็นในทุกระดับ เพื่อช่วยในเรื่อง

  * การระบุ ประเมิน และตอบสนองความเสี่ยง

  * ช่วยขับเคลื่อนองค์กรให้บรรลุวัตถุประสงค์ที่กำหนด

องค์ประกอบที่ 7 สารสนเทศและการสื่อสาร (ต่อ)

- มีช่องทางการสื่อสารและการมอบหมายอำนาจหน้าที่ที่ชัดเจน โดยระบุถึง

* ความคาดหวังและความรับผิดชอบของบุคลากร
* ปรัชญาและการบริหารความเสี่ยงทั่วทั้งองค์กร
* วิธีการสื่อสารเรื่องสำคัญไปยังผู้บริหารระดับสูง
* การสื่อสารที่มีประสิทธิผลกับบุคคลภายนอกและผู้มีส่วนได้เสีย

องค์ประกอบที่ 8 การติดตามประเมินผล

องค์ประกอบที่ 8 การติดตามประเมินผล

- ต้องประเมินการมีอยู่และการทำหน้าที่ขององค์ประกอบทั้ง 8 อยู่เสมอ
- ติดตามทบทวน และปรับปรุงแก้ไขตามความจำเป็นและเหมาะสม
- วิธีการติดตาม ทำได้ทั้ง
  - ระหว่างปฏิบัติงาน
  - เป็นกรณีเฉพาะ

ข้อควรพิจารณาเกี่ยวกับ ERM

ไม่ใช่กระบวนการที่ต้องทำตามลำดับอย่างเข้มงวด แต่ต้องกระทำซ้ำๆ บ่อยๆ

เนื่องจาก องค์ประกอบใดก็ตามสามารถมีอิทธิพลต่อองค์ประกอบอื่น ๆได้เสมอ

3. การนำหลักการบริหารความเสี่ยงไปใช้ในองค์กร

3.1 แนวทางในการพัฒนาระบบบริหารความเสี่ยง

- มีวิธีและแนวทางที่หลากหลาย
- ขึ้นอยู่กับความพร้อม ขนาด และความซับซ้อนขององค์กร ลักษณะประกอบการ และวัฒนธรรมองค์กร
- ต้องจัดให้มีบรรยายและวัฒนธรรมที่สนับสนุนการบริหารความเสี่ยง เช่น จรรยาบรรณ การสื่อสารสองทางที่มีประสิทธิภาพ ความรับผิดชอบ ผู้บริหารรับฟังการท้วงติงถึงความเสี่ยง

3.1 แนวทางในการพัฒนาระบบบริหารความเสี่ยง (ต่อ)

- จัดตั้งทีมงานบริหารความเสี่ยงโดยมีตัวแทนของแต่ละฝ่ายเพื่อศึกษาหลักการและแนวทางการบริหารความเสี่ยงให้เข้าใจตรงกันและใช้ภาษาเดียวกัน
- สนับสนุนโดยคณะกรรมการ คณะกรรมการตรวจสอบ CEO และผู้บริหารระดับสูงและช่วยให้การดำเนินงานสำเร็จ
- CEO เป็น Champion ของโครงการ และมีหัวหน้าคณะทำงานที่คนยอมรับ

3.1 แนวทางในการพัฒนาระบบบริหารความเสี่ยง (ต่อ)

- จัดทำแผนการพัฒนาระบบบริหารความเสี่ยง
  - * กำหนดนโยบายโครงสร้างและความรับผิดชอบ
  - * พัฒนากระบวนการบริหารความเสี่ยงที่ดีและสอดคล้องกับวัฒนธรรมและปรัชญาการบริหารความเสี่ยงขององค์กร
  - * พัฒนาและอบรม สื่อสารให้ทุกคนเข้าใจตรงกัน
  - * ดำเนินการประเมินและบริหารความเสี่ยงที่มีอยู่

3.1 แนวทางในการพัฒนาระบบบริหารความเสี่ยง (ต่อ)

- บริหารความเสี่ยงที่มีอยู่ในระดับสูงก่อนแล้วค่อยดำเนินการในระดับฝ่าย
- อาจพิจารณาเลือกหน่วยงาน หรือโครงการเป็น Pilot Project ก่อนก็ได้

3.2 ข้อจำกัดของระบบบริหารความเสี่ยง

- ความเสี่ยงคือความไม่แน่นอน อาจจะเกิดหรือไม่เกิดก็ได้
- ถึงแม้ว่ามีระบบบริหารความเสี่ยงที่ดี ก็ไม่สามารถทำให้มั่นใจได้ 100% ว่าจะบรรลุเป้าหมายที่กำหนด แต่จะช่วยให้มั่นใจมากขึ้นว่าจะบรรลุ

3.3 การจัดทำแผนจัดการความเสี่ยง

- ระบุกลยุทธ์/วิธีการ มาตรการที่เป็นทางเลือกเพื่อกำจัดหรือลดความเสี่ยง และศึกษาความเป็นไปได้ และค่าใช้จ่ายของแต่ละทางเลือก
- เลือกวิธีการที่ดีที่สุด โดยกำหนดผู้รับผิดชอบ, ระยะเวลาเพื่อกำหนด Action Plan และมาตรการในการติดตามผล
- ขออนุมัติแผนจัดการความเสี่ยง
- รายงานผลการประเมินความเสี่ยงต่อผู้บริหารระดับสูง และ คณะกรรมการตรวจสอบ (แผนการจัดการความเสี่ยง และ risk profile)

Risk-Control-Internal Auditing

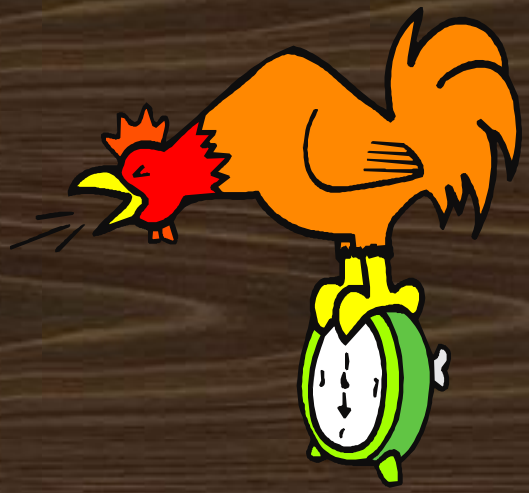
✗	✓	**Wastes**
✓	✗	**Unacceptable**

- ***วัตถุประสงค์*** /เป้าหมาย ที่ไม่มี ***การควบคุม*** ยอมรับไม่ได้
- ***การควบคุม*** โดยปราศจาก ***ความเสี่ยง***

  คือความสูญเสียด้านทรัพยากร
- ***ความเสี่ยง*** ที่ปราศจาก ***การควบคุม*** เป็นเรื่องที่ยอมรับไม่ได้
- การตรวจสอบภายใน ที่ไม่ครอบคลุมทั้ง ***ความเสี่ยง*** และ

  การควบคุม เป็นเรื่องที่เสียเวลา = รายงานผิดปกติ **Abnormality Report** "Risk Based Auditing"

ตื่นๆๆ ได้แล้ว



ถาม-ตอบ

บุปผา ชวะพงษ์

โทร. 081-6289953