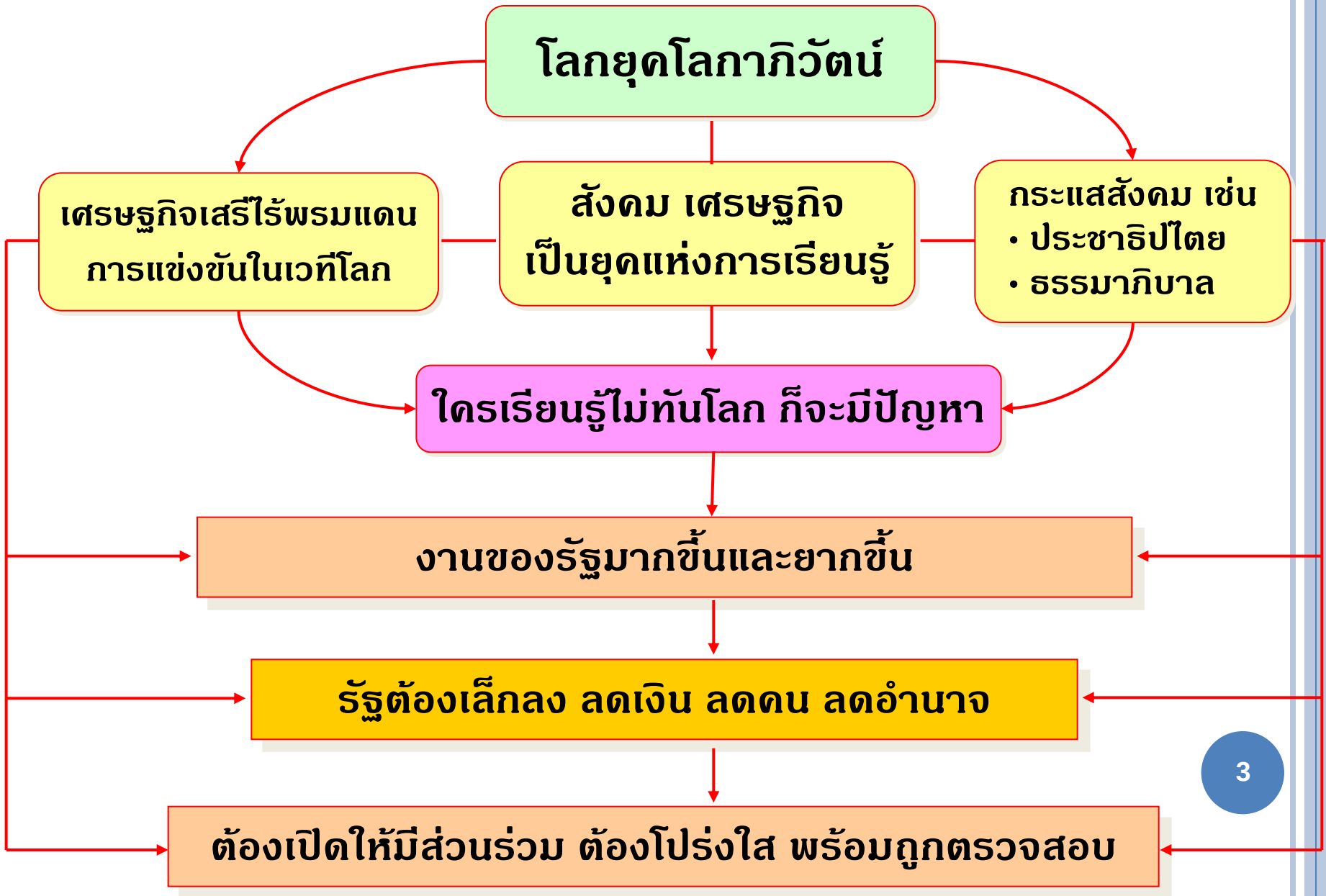
การบริหารความเสี่ยง
และ
การควบคุมภายใน

โดย เกศริน ภัทรเปรมเจริญ
สำนักกำกับและพัฒนาการตรวจสอบภาครัฐ
กรมบัญชีกลาง

การบริหารความเสี่ยงและการควบคุมภายใน

- หลักการและแนวคิด
- กระบวนการ
- การประยุกต์ใช้
- การรายงานและการติดตาม

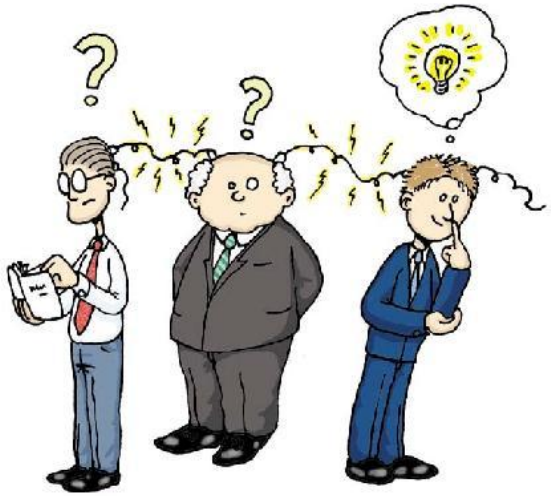
สภาพแวดล้อมปัจจุบัน




Good Governance
Internal Control
องค์กร
Risk Management
Internal Audit

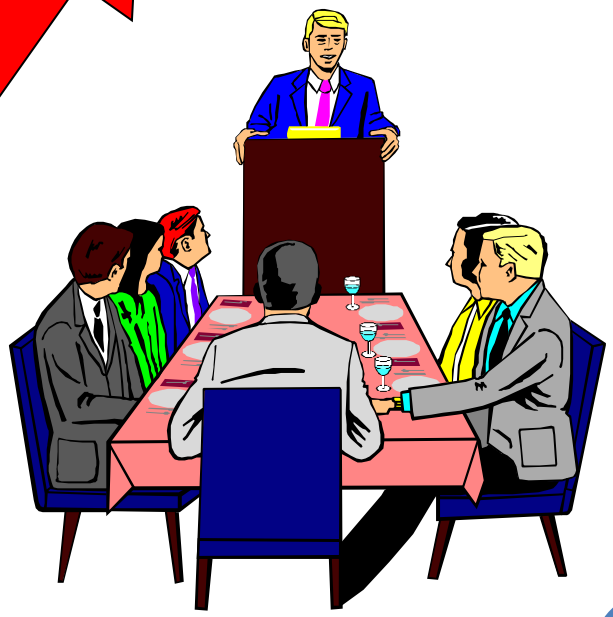
TOPIC

- What Enterprise Risk Management (ERM) & Internal Control (IC) ?
- COSO ERM and Internal Control Framework
- Definition - ERM and IC
- Objective and Components - ERM & IC



การบริหารความเสี่ยงองค์กร (Enterprise Risk Management)

COSO



การควบคุมภายใน (Internal Control)

What is COSO ?

COSO : The Committee of Sponsoring Organizations of the Treadway Commission

is a joint initiative of the five private sector organizations listed on the left and is dedicated to providing thought leadership through the development of frameworks and guidance on enterprise risk management, internal control and fraud deterrence

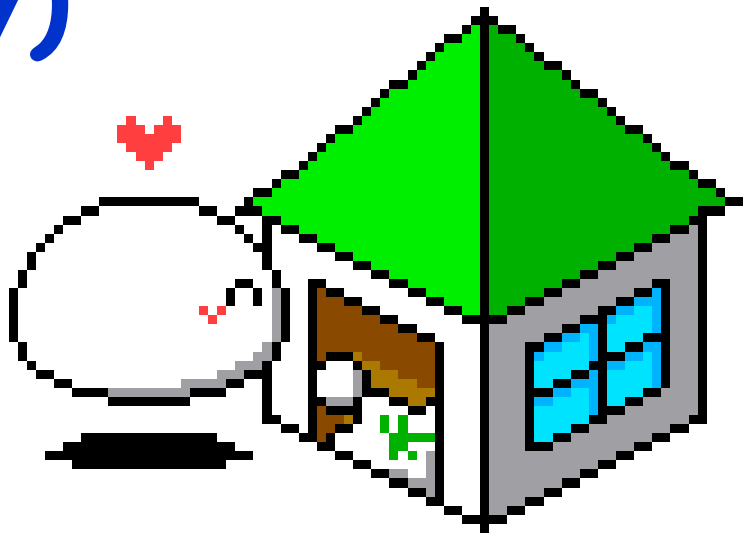
SPONSORING ORGANIZATIONS

COSO : The Committee of Sponsoring Organizations of the Treadway Commission

- สถาบันผู้สอบบัญชีรับอนุญาตแห่งสหรัฐอเมริกา
  (American Institute of Certified Public Accountants : AICPA)
- สถาบันนักบัญชีแห่งสหรัฐอเมริกา
  (American Accounting Association : AAA)
- สถาบันผู้บริหารการเงิน
  (Financial Executives Institute : FEI)
- สถาบันผู้ตรวจสอบภายใน
  (The Institute of Internal Auditors : IIA)
- สถาบันนักบัญชีเพื่อการบริหาร
  (Institute of Management Accountants : IMA)

เป้าหมายหลักขององค์กร

- ✓ กำไร (Profitability)
- ✓ มั่นคง (Stability)
- ✓ เติบโต (Growth)



ทำไมต้องมีการบริหารความเสี่ยง

- ทุกองค์กรดำรงอยู่ เพื่อมอบคุณค่า (Value) แก่ผู้มีส่วนได้ส่วนเสีย
- คุณค่าเกิดขึ้น รักษาไว้ หรือถูกทำลายได้จากการตัดสินใจในการดำเนินกิจกรรมต่าง ๆ ของผู้บริหาร ไม่ว่าจะเป็นการตัดสินใจในการกำหนดกลยุทธ์ไปจนถึงการตัดสินใจในปฏิบัติงานประจำวัน

การบริหารความเสี่ยง

- เพื่อให้ผลการดำเนินงานขององค์กรเป็นไปตามวัตถุประสงค์และเป้าหมายที่วางไว้
- เพื่อให้เกิดการรับรู้ ตระหนัก และเข้าใจถึงความเสี่ยงด้านต่าง ๆ ที่เกิดขึ้นกับองค์กร และหาวิธีจัดการที่เหมาะสมในการลดความเสี่ยงให้อยู่ในระดับที่องค์กรยอมรับได้
- เพื่อสร้างกรอบและแนวทางการดำเนินงานให้แก่บุคลากรขององค์กรให้สามารถบริหารจัดการความไม่แน่นอนที่จะเกิดขึ้นกับองค์กรได้อย่างเป็นระบบ และมีประสิทธิภาพ
- เพื่อให้มีระบบในการติดตามตรวจสอบผลการดำเนินการบริหารความเสี่ยง และเฝ้าระวังความเสี่ยงใหม่ ๆที่อาจเกิดขึ้นได้ตลอดเวลา
- เพิ่มมูลค่าให้ผู้มีส่วนได้ส่วนเสียกับองค์กร

ERM *is a process, effected by an entity's board of director, management and other personnel, apply in strategy setting and across the enterprise, design to identify potential events that may effect the entity, and manage risk to be with in its risk appetite, to provide reasonable assurance regarding the achievement of entity objective*

กระบวนการที่ได้รับอิทธิพลมาจากคณะกรรมการขององค์กร ผู้บริหารและบุคลากรอื่น ๆ เป็นกระบวนการที่จะถูกนำมาประยุกต์ใช้ในการตั้งกลยุทธ์ทั่วทั้งองค์กร ได้รับการออกแบบมาเพื่อให้สามารถระบุเหตุการณ์อันอาจเกิดขึ้นและส่งผลกระทบต่อองค์กร และเพื่อจัดการความเสี่ยงให้อยู่ภายในระดับความเสี่ยงที่องค์กรยอมรับได้ (risk appetite) ซึ่งจะทำให้เกิดความเชื่อมั่นได้อย่างสมเหตุสมผลเกี่ยวกับการบรรลุวัตถุประสงค์ขององค์กร

สรุปได้ว่าERM

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

สรุปได้ว่าERM

- จัดการกับความเสี่ยงให้อยู่ภายในระดับที่องค์กรยอมรับได้ (manage risk to be within its risk appetite)
- เพื่อก่อให้เกิดความเชื่อมั่นได้อย่างสมเหตุสมผลว่าสามารถนำทางไปสู่ความสำเร็จตามวัตถุประสงค์ต่าง ๆ (*to provide reasonable assurance regarding the achievement of entity objective*)

New COSO-ERM Framework

Exhibit 1

- The four objectives categories – strategic, operations, reporting and compliance – are represented by the vertical columns.
- The eight components are represented by horizontal rows.
- The entity and its organizational units are depicted by the third dimension of the matrix.

การบริหารความเสี่ยงองค์กร

วัตถุประสงค์

เพื่อช่วยบริหารโอกาสและควบคุมความเสี่ยง

ความไม่แน่นอน (UNCERTAINTY)

- อาจเป็นได้ทั้งบั่นทอน และเพิ่มคุณค่า (Risk and Opportunity)
- ERM เป็นกระบวนการที่มีประสิทธิผลต่อการจัดการกับความไม่แน่นอน
- ความสำเร็จในการจัดการกับความ **“ไม่แน่นอน”** เป็นโอกาสที่บรรลุผลสำเร็จ ทั้งด้านการปฏิบัติ ผลกำไรที่ต้องการและป้องกันความสูญเสีย

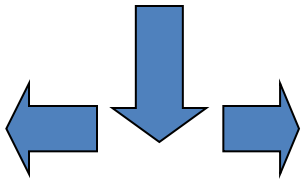
เหตุการณ์ (Events) อาจเป็นเหตุการณ์ที่ส่งผลทั้งทางดีและร้าย

- **เหตุการณ์ที่ส่งผลทางร้าย** คือ **ความเสี่ยง** ซึ่งสามารถกันไม่ให้เกิดคุณค่า หรือทำให้คุณค่าที่กิจการมีอยู่อาจเสื่อมได้
- **เหตุการณ์ที่ส่งผลในทางดี** อาจหักกลบกับผลกระทบที่ไม่ดี หรืออาจก่อ **“โอกาส”** ให้กับกิจการได้วัตถุประสงค์ ซึ่งจะเป็นสิ่งที่ส่งเสริมให้เกิดคุณค่าหรือรักษาไว้ซึ่งคุณค่า

ความเสี่ยงและโอกาส

ความไม่แน่นอน

การไม่สามารถคาดการณ์ล่วงหน้าได้อย่างแม่นยำถึงโอกาสเกิดของเหตุการณ์ในอนาคตและผลกระทบที่อาจเกิดขึ้น



ความเสี่ยง

เหตุการณ์ในเชิงลบ หากเกิดขึ้นแล้วอาจสร้างความเสียหาย

โอกาส

เหตุการณ์ที่มีผลในเชิงบวก ซึ่งผู้บริหารควรนำไปพิจารณากำหนดกลยุทธ์เพื่อนำไปปฏิบัติ

ความเสี่ยง หมายถึง เหตุการณ์ที่มีความไม่แน่นอน ซึ่งหากเกิดขึ้นจะมีผลกระทบในเชิงลบต่อวัตถุประสงค์หรือเป้าหมายขององค์กร

โอกาส หมายถึง เหตุการณ์ที่มีความไม่แน่นอน ซึ่งหากเกิดขึ้นจะมีผลกระทบในเชิงบวกต่อวัตถุประสงค์หรือเป้าหมายขององค์กร

ดุลยภาพในการบริหารความเสี่ยงและการสร้างโอกาส

การบริหารความเสี่ยงองค์กร

เครื่องมือนำไปสู่การบรรลุวัตถุประสงค์ :-

- ด้านกลยุทธ์ (Strategic)
- ด้านการดำเนินงาน (Operation)
- ด้านการรายงาน (Reporting)
- ด้านการปฏิบัติตามกฎ/ระเบียบ/ข้อบังคับ (Compliance)

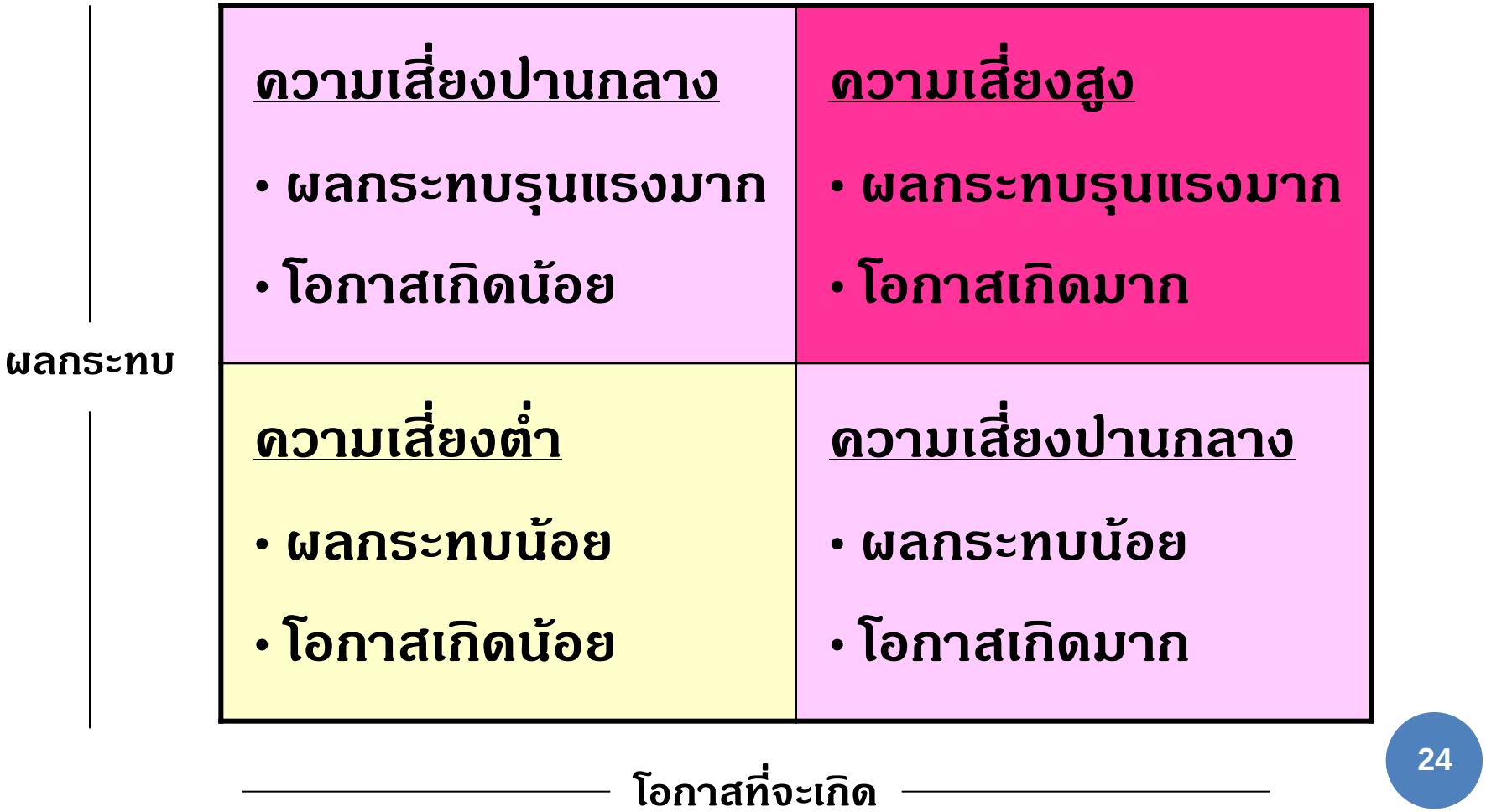
บทบาทหน้าที่และความรับผิดชอบในการบริหารความเสี่ยง

- **ทุกคนในองค์กร** มีความรับผิดชอบต่อการบริหารความเสี่ยงองค์กรที่จะกระทบต่อวัตถุประสงค์หรือเป้าหมายที่รับผิดชอบ โดยสอดคล้องกับคำสั่งและร่างข้อตกลงที่ได้กำหนดไว้
- **คณะกรรมการ** มีหน้าที่กำกับดูแลให้มีนโยบายและการบริหารความเสี่ยงที่มีประสิทธิผล
- **ผู้บริหารสูงสุด** มีความรับผิดชอบสูงสุด และรับบทบาทเป็นเจ้าของหรือเจ้าภาพที่จะจัดให้มีกระบวนการบริหารความเสี่ยงที่มีประสิทธิภาพ
- **ผู้บริหารอื่น ๆ** มีหน้าที่สนับสนุนปรัชญาการบริหารความเสี่ยงองค์กร ส่งเสริมความร่วมมือต่อระดับความเสี่ยงที่องค์กรยอมรับได้ และจัดการกับความเสี่ยงภายในขอบเขตความรับผิดชอบที่สอดคล้องกับเกณฑ์ความคลาดเคลื่อนของความเสี่ยงที่องค์กรยอมรับได้
- **เจ้าหน้าที่ผู้ปฏิบัติงาน** มีหน้าที่สนับสนุนกระบวนการบริหารความเสี่ยง
- **ผู้ตรวจสอบภายใน** มีหน้าที่สอบทานและประเมินประสิทธิผลของการบริหารความเสี่ยง
- **ผู้สอบบัญชีภายนอก/หน่วยงาน/บุคคลอื่นภายนอกองค์กร** ไม่มีความรับผิดชอบต่อประสิทธิผลของการบริหารความเสี่ยง

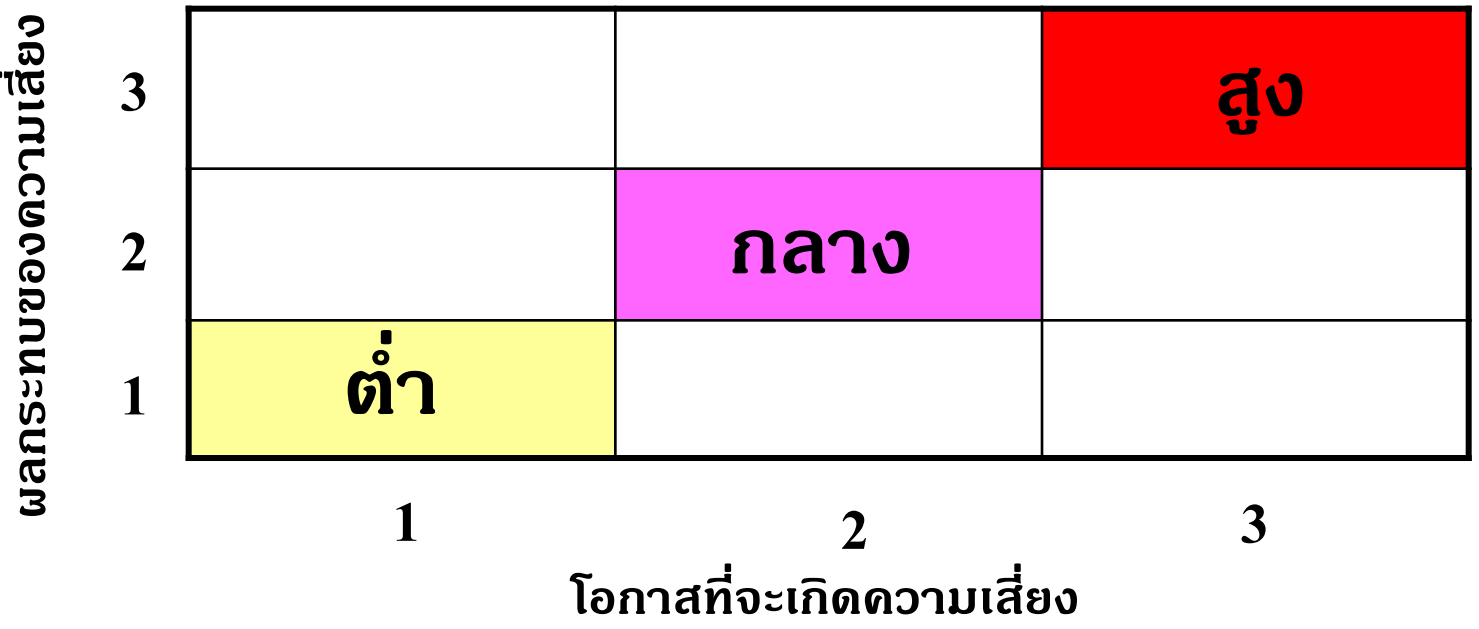
What is Risk ?

- High risk is high returns
- and requires high controls
- Change a crisis to opportunity
- The biggest risk is not to take risk at all

การวิเคราะห์โอกาสและผลกระทบ



ระดับของความเสี่ยง

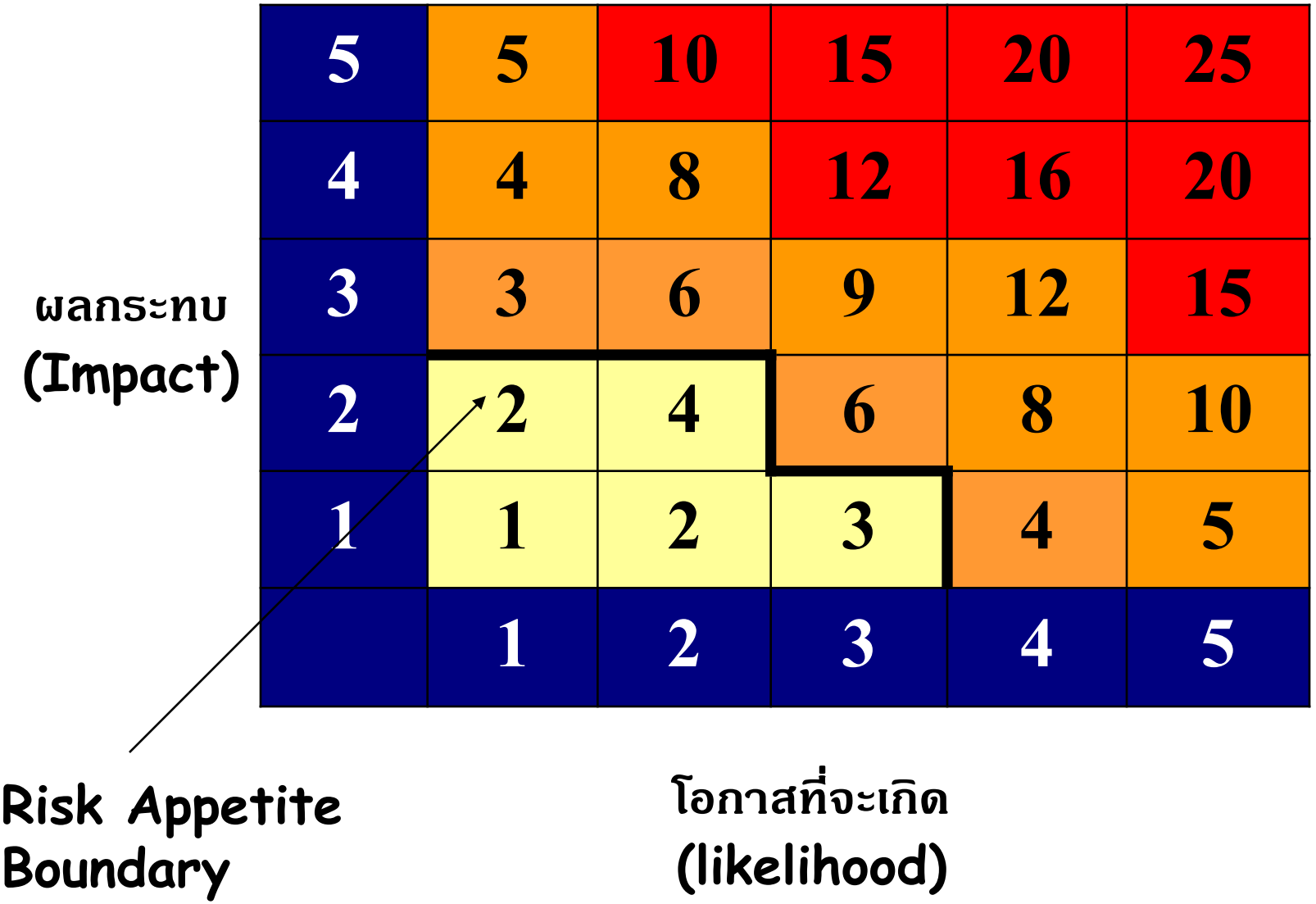


ระดับสูง มีค่าคะแนนมากกว่า 5 คะแนนขึ้นไป

ระดับกลาง มีค่าคะแนนตั้งแต่ 2 - 5 คะแนน

ระดับต่ำ มีค่าคะแนนน้อยกว่า 2 คะแนนลงมา

แผนภูมิความเสี่ยง (Risk Profile)



ตัวอย่างโอกาสที่จะเกิดเหตุการณ์ที่เป็นความเสี่ยง

โอกาสที่จะเกิดความเสี่ยง	ความถี่ที่เกิดขึ้น (เฉลี่ย)	ระดับคะแนน
สูงมาก	มากกว่า 1 ครั้งต่อเดือน	5
สูง	ระหว่าง1-6 เดือนต่อครั้ง	4
ปานกลาง	ระหว่าง 6-12 เดือนต่อครั้ง	3
น้อย	มากกว่า 1 ปีต่อครั้ง	2
น้อยมาก	มากกว่า 5 ปีต่อครั้ง	1

ตัวอย่างโอกาสที่จะเกิดเหตุการณ์ที่เป็นความเสี่ยง

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

ตัวอย่างผลกระทบต่อองค์กร (ด้านการเงิน)

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

ตัวอย่างผลกระทบต่อองค์กร (ด้านเวลา)

ผลกระทบต่อองค์กร	ความเสียหาย	ระดับคะแนน
สูงมาก	ทำให้เกิดความล่าช้าของโครงการ มากกว่า 6 เดือนขึ้นไป	5
สูง	ทำให้เกิดความล่าช้าของโครงการ มากกว่า 4.5 เดือน ถึง 6 เดือน	4
ปานกลาง	ทำให้เกิดความล่าช้าของโครงการ มากกว่า 3 เดือน ถึง 4.5 เดือน	3
น้อย	ทำให้เกิดความล่าช้าของโครงการ มากกว่า 1.5 เดือน ถึง 3 เดือน	2
น้อยมาก	ทำให้เกิดความล่าช้าของโครงการ ไม่เกิน 1.5 เดือน	1

ตัวอย่างผลกระทบต่อองค์กร (ด้านชื่อเสียง)

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

ตัวอย่างผลกระทบต่อองค์กร (ด้านลูกค้า)

ผลกระทบต่อองค์กร	ความเสียหาย	ระดับคะแนน
สูงมาก	ผู้ใช้บริการลดลงมากกว่า 50 คน ต่อเดือน	5
สูง	ผู้ใช้บริการลดลงตั้งแต่ 40-50 คน ต่อเดือน	4
ปานกลาง	ผู้ใช้บริการลดลงตั้งแต่ 30-39 คน ต่อเดือน	3
น้อย	ผู้ใช้บริการลดลงตั้งแต่ 20-29 คน ต่อเดือน	2
น้อยมาก	ผู้ใช้บริการลดลงไม่เกิน 19 คน ต่อเดือน	1

ตัวอย่างผลกระทบต่อองค์กร (ด้านความสำเร็จ)

ผลกระทบต่อองค์กร	ความเสียหาย	ระดับคะแนน
สูงมาก	ดำเนินงานสำเร็จตามแผนได้น้อยกว่า 60%	5
สูง	ดำเนินงานสำเร็จตามแผนได้ 60-70%	4
ปานกลาง	ดำเนินงานสำเร็จตามแผนได้ 71-80%	3
น้อย	ดำเนินงานสำเร็จตามแผนได้ 81-90%	2
น้อยมาก	ดำเนินงานสำเร็จตามแผนได้มากกว่า 90%	1

ตัวอย่างผลกระทบต่อองค์กร (ด้านบุคลากร)

ผลกระทบต่อองค์กร	ความเสียหาย	ระดับคะแนน
สูงมาก	มีบุคลากรเสียชีวิตมากกว่า 3 คน	5
สูง	มีบุคลากรเสียชีวิตไม่เกิน 3 คน	4
ปานกลาง	มีบุคลากรได้รับบาดเจ็บจนพิการ แต่ไม่มีผู้เสียชีวิต	3
น้อย	มีบุคลากรได้รับบาดเจ็บจนต้องรักษาตัวที่โรงพยาบาล	2
น้อยมาก	มีบุคลากรได้รับบาดเจ็บเล็กน้อย	1

องค์ประกอบการบริหารความเสี่ยง

1. สภาพแวดล้อมในองค์กร (Internal Environment)
2. การกำหนดวัตถุประสงค์ (Objective Setting)
3. การบ่งชี้เหตุการณ์ (Event Identification)
4. การประเมินความเสี่ยง (Risk Assessment)
5. การตอบสนองความเสี่ยง (Risk Response)
6. กิจกรรมการควบคุม (Control Activities)
7. สารสนเทศและการสื่อสาร (Information & Communication)
8. การติดตามผล (Monitoring)

สภาพแวดล้อมภายในองค์การ (INTERNAL ENVIRONMENT)

เป็นองค์ประกอบพื้นฐานของการบริหารความเสี่ยง ที่ส่งผลต่อวิธีการกำหนดกลยุทธ์และเป้าหมายของการดำเนินงาน

การกำหนดวัตถุประสงค์ (OBJECTIVE SETTING)

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

การกำหนดวัตถุประสงค์ที่ SMART

- **Specific** (เฉพาะเจาะจง) มีความชัดเจนและกำหนดผลตอบแทนหรือผลลัพธ์ที่ต้องการที่ทุกคนสามารถเข้าใจได้อย่างชัดเจน
- **Measurable** (สามารถวัดได้) สามารถวัดผลการบรรลุวัตถุประสงค์ได้
- **Achievable** (สามารถบรรลุผลได้) มีความเป็นไปได้ที่จะบรรลุวัตถุประสงค์ภายใต้เงื่อนไขการใช้ทรัพยากรที่มีอยู่ในปัจจุบัน
- **Relevant** (มีความเกี่ยวข้อง) มีความสอดคล้องกับกลยุทธ์และเป้าหมายในการดำเนินงานขององค์กร
- **Timeliness** (มีกำหนดเวลา) สามารถกำหนดระยะเวลาที่ต้องการบรรลุผล

การบ่งชี้เหตุการณ์ (EVENT IDENTIFICATION)

เป็นการระบุเหตุการณ์ความเสี่ยงหรือความไม่แน่นอนที่อาจเกิดขึ้น โดยพิจารณาจากปัจจัยทั้งภายในและภายนอก

การประเมินความเสี่ยง
(RISK ASSESSMENT)

การประเมินความเสี่ยงจะช่วยให้องค์กรทราบว่าเหตุการณ์ความเสี่ยง/ความไม่แน่นอนที่เกิดขึ้นส่งผลกระทบต่อการบรรลุเป้าหมายขององค์กรเป็นอย่างไร โดยการวิเคราะห์จากโอกาสที่จะเกิดเหตุการณ์และผลกระทบหากเกิดเหตุการณ์นั้นขึ้น

การตอบสนองความเสี่ยง (RISK RESPONSE)

การคัดเลือกทางเลือกที่เหมาะสมกับการจัดการความเสี่ยงที่เกิดขึ้น โดยจะต้องเลือกทางเลือกที่คาดว่าจะสามารถทำให้โอกาสและผลกระทบของความเสี่ยงให้อยู่ในระดับที่องค์กรยอมรับได้

การตอบสนองความเสี่ยง (การจัดการความเสี่ยง)

1. การหลีกเลี่ยง (Avoidance)
2. การยอมรับ (Acceptance)
3. การลด (Reduction)
4. การโอน/กระจาย (Sharing)

การตอบสนอง (การจัดการ) ความเสี่ยง (Risk Response) มี 4 แนวทางหลัก

- การหลีกเลี่ยงความเสี่ยง (Avoidance/Terminate) ไม่ทำ / เลิกกิจกรรมนั้น
- การยอมรับความเสี่ยง (Acceptance /Take)) อาจเป็นเพราะระดับความเสี่ยงต่ำมากจนไม่คุ้ม หรือสูงเกินไปเสียจนไม่มีหนทางที่จะจัดการกับความเสี่ยงนั้น
- การลดความเสี่ยง (Reduction/Treat) อาจลดโอกาส หรือผลกระทบ หรือลดทั้ง 2 อย่าง
- การโอนหรือกระจายความเสี่ยง (Sharing/Transfer) อาจลดโอกาส หรือผลกระทบ โดยการโอนความเสี่ยง (ทำประกัน) หรือแชร์บางส่วนของความเสี่ยง หรือการ Outsourcing

กิจกรรมการควบคุม (CONTROL ACTIVITIES)

นโยบาย มาตรการ และวิธีการต่าง ๆ ที่ฝ่ายบริหารกำหนดหรือนำมาใช้ที่ทำให้มั่นใจได้ว่าการจัดการความเสี่ยงที่จะทำขึ้นได้ถูกนำไปปฏิบัติอย่างทั่วถึงทั้งองค์กรอย่างเหมาะสม

ตัวอย่างกิจกรรมการควบคุม

1. การกำหนดระเบียบ ข้อบังคับ วิธีปฏิบัติ

2. การแบ่งแยกหน้าที่ความรับผิดชอบ

3. การควบคุมทางกายภาพ

4. การจัดทำบัญชี ทะเบียน รายงาน

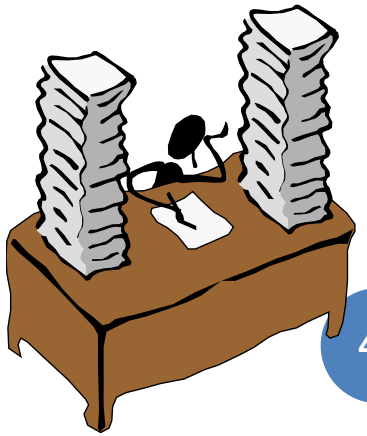
5. การกำหนดขอบเขต อำนาจหน้าที่ความรับผิดชอบ

6. การสับเปลี่ยนหมุนเวียนงาน

7. การควบคุมการประมวลผลข้อมูล

8. การกำหนดดัชนีวัดผลการดำเนินงาน

ฯลฯ



ตัวอย่างกิจกรรมการควบคุม
เพื่อการป้องกันสิ่งที่ไม่พึงประสงค์ ข้อผิดพลาด ทุจริต

- ระบบคอมพิวเตอร์ ตรวจเลขที่บัญชี ที่พนักงานคีย์เข้า
- ทำลายเอกสาร ที่มีข้อมูลสำคัญเพื่อกันการรั่วไหล
- พนักงานอ่านและ ทำความเข้าใจ นโยบายและคู่มือ
- ผู้บริหาร อนุมัติ คำขอจัดซื้อ
- ระบบ ให้สิทธิ การเข้าถึงข้อมูลเฉพาะผู้มีอำนาจหน้าที่
- อาคารและระบบความปลอดภัย จำกัด การเข้าถึงสินทรัพย์
- ไม่วาง อาหารและเครื่องดื่มใกล้อุปกรณ์คอมพิวเตอร์
- สำรองข้อมูล เป็นระยะตามระดับความสำคัญ
- เก็บ รหัสผ่าน เป็นความลับ
- ติดตั้งและใช้งานซอฟแวร์ ป้องกันไวรัส

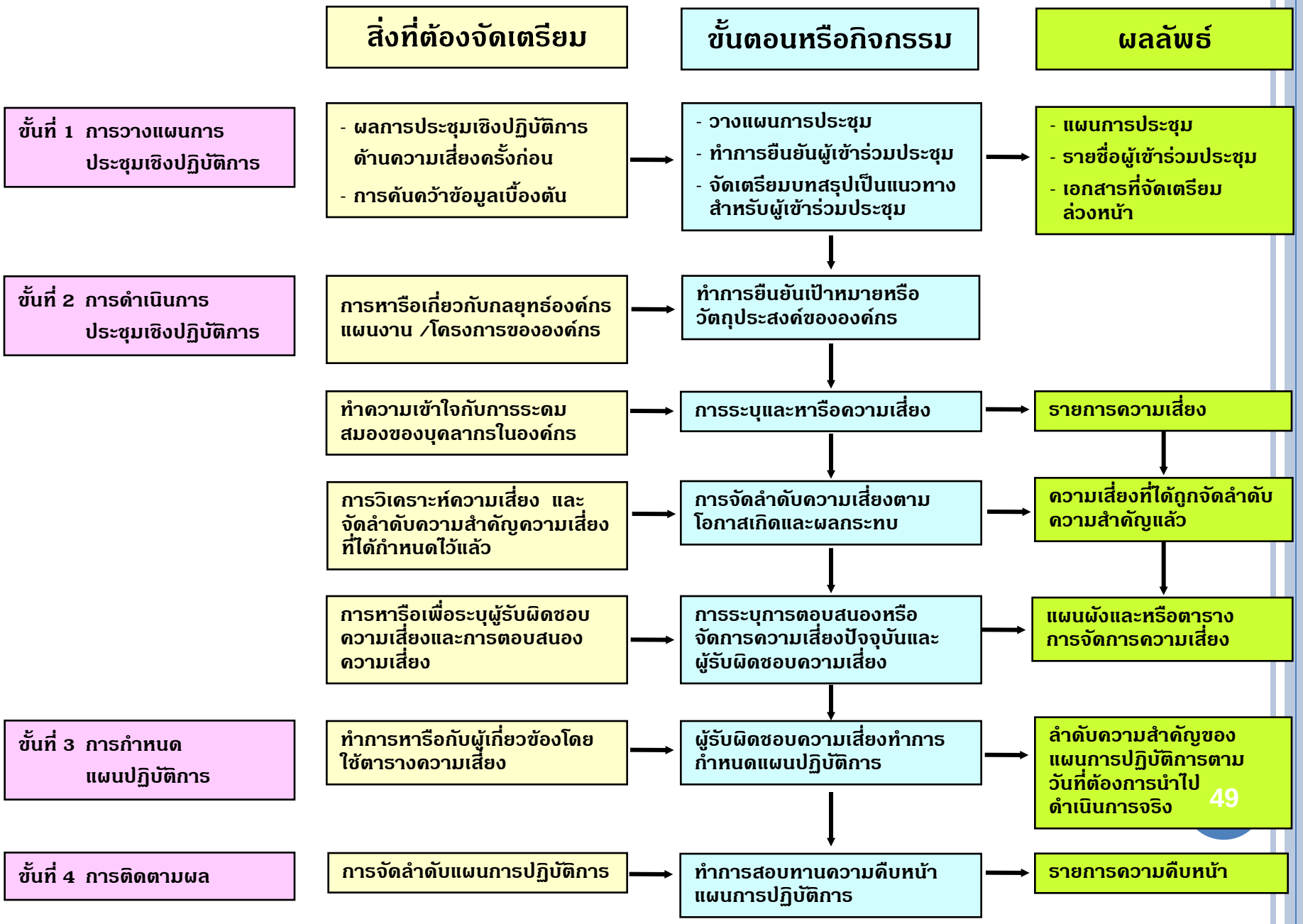
สารสนเทศและการสื่อสาร
(Information and Communication)

การระบุสารสนเทศที่จำเป็นทั้งจากแหล่งข้อมูลภายในและภายนอกองค์กร และมีระบบการสื่อสารไปถึงบุคลากรในองค์กร เพื่อให้สามารถปฏิบัติงานตามหน้าที่ความรับผิดชอบได้อย่างถูกต้อง

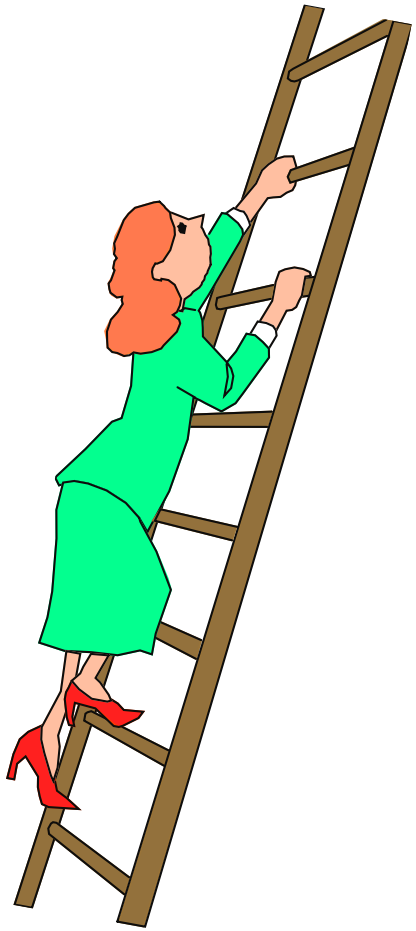
การติดตามผล (Monitoring)

การบริหารความเสี่ยงขององค์กร จะมีความสมบูรณ์ครบถ้วนได้ จะต้องมีการทบทวน ติดตาม และปรับปรุงแก้ไขการบริหารความเสี่ยงตามความจำเป็นและเหมาะสม การติดตามผลสามารถจะบรรลุความสำเร็จได้ โดยอาศัยกิจกรรมการจัดการระหว่างการปฏิบัติงานอย่างต่อเนื่อง (ongoing management activities) และ/หรือ การประเมินผลอย่างอิสระ (separate evaluations)

ตัวอย่าง – การจัดระบบการบริหารความเสี่ยงขององค์กร



กระบวนการบริหารความเสี่ยง



1. การกำหนดวัตถุประสงค์
2. การระบุความเสี่ยง
3. การประเมินความเสี่ยง
4. การเลือกวิธีการจัดการความเสี่ยง
5. การติดตามและประเมินผล

แนวทางดำเนินการ

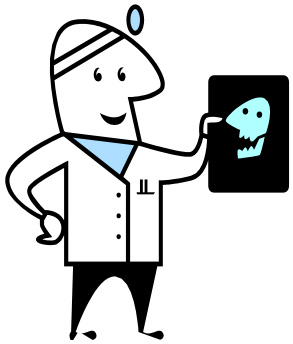
- มีวิธีการที่หลากหลาย
- ขึ้นอยู่กับความพร้อม ขนาด และความซับซ้อนขององค์กร
- จัดให้มีบรรยากาศและวัฒนธรรมที่สนับสนุนการบริหารความเสี่ยง

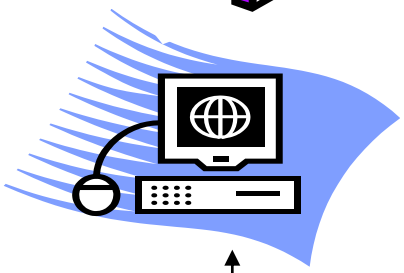
เป้าหมาย ความเสี่ยง และการควบคุม

เป้าหมาย	→	สิ่งที่หน่วยงานต้องการ
ความเสี่ยง	→	สิ่งที่ทำให้ไม่สามารถบรรลุเป้าหมาย
การควบคุม	→	สิ่งที่ช่วยให้สามารถบรรลุเป้าหมาย

การควบคุมภายใน

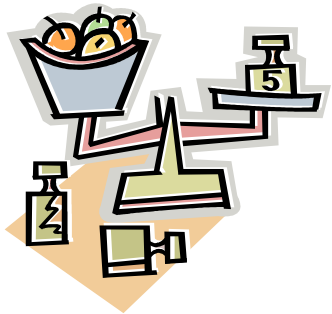
Input





Process

Output



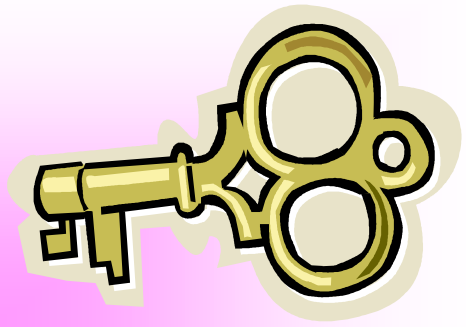
ประสิทธิภาพ / ประสิทธิผล / คุ้มค่า

การประเมินผลการควบคุมภายใน

การดำเนินงานของแต่ละหน่วยงาน

สิ่งที่ต้องการ

ลดความเสี่ยง



ระบบ
ปฏิบัติงาน

ระบบ
ควบคุม

กระบวนการทำงาน

IC is a process, effected by an entity's board of director, management and other personnel, designed to provide reasonable assurance regarding the achievement of objectives in the follow categories :

1. E&E of operation 2. Reliable of reporting

3. Comply with law and regulations

กระบวนการในการปฏิบัติงานที่ผู้กำกับดูแล ฝ่ายบริหาร และบุคลากรของหน่วยงานจัดให้มีขึ้น เพื่อสร้างความมั่นใจอย่างสมเหตุสมผลว่าการดำเนินงานของหน่วยงานจะบรรลุวัตถุประสงค์ ดังต่อไปนี้

เพื่อให้เกิดประสิทธิผลและประสิทธิภาพของการดำเนินงาน

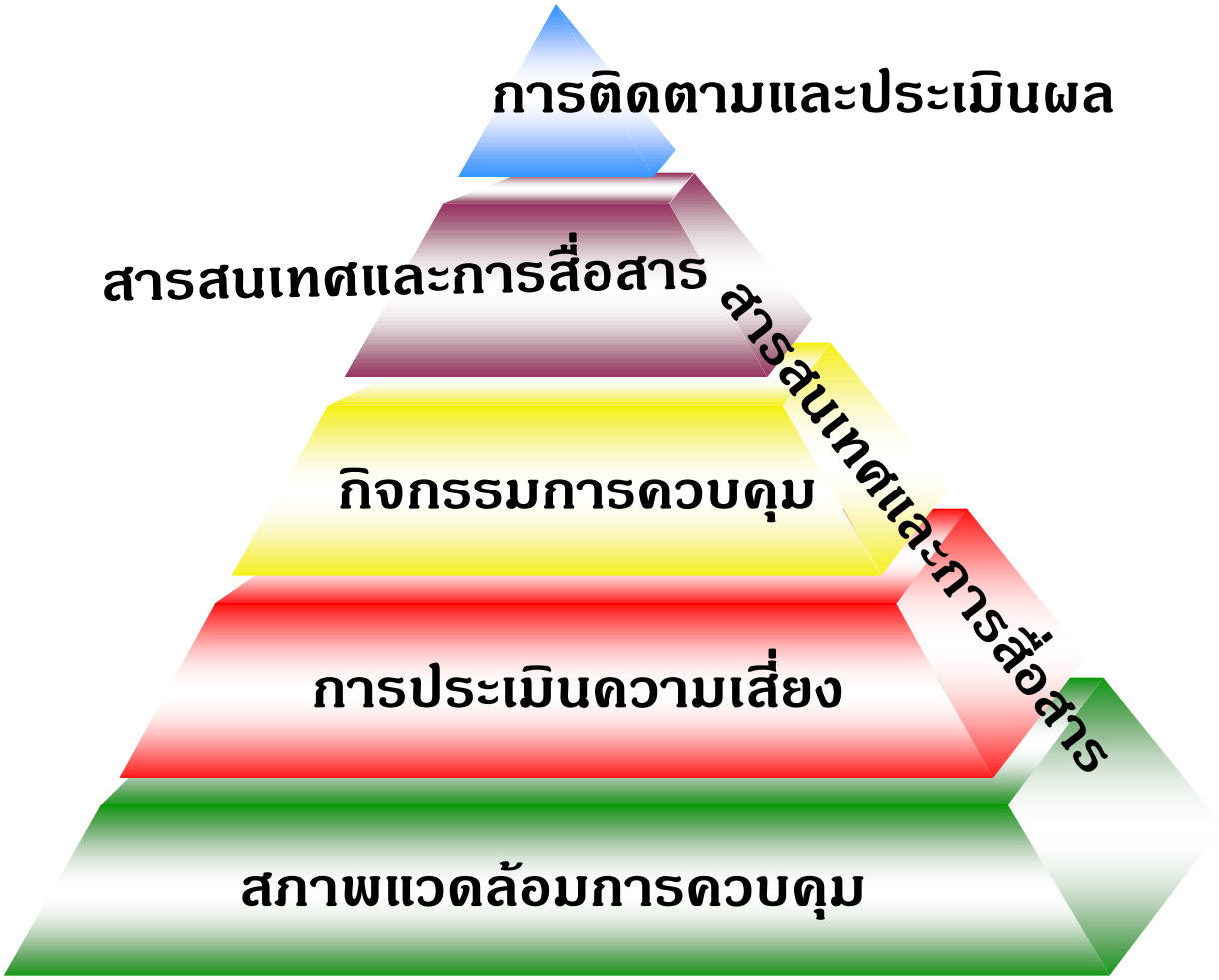
เพื่อให้เกิดความเชื่อถือได้ของการรายงานทางการเงิน

เพื่อให้เกิดการปฏิบัติตามกฎหมายและระเบียบข้อบังคับที่เกี่ยวข้อง

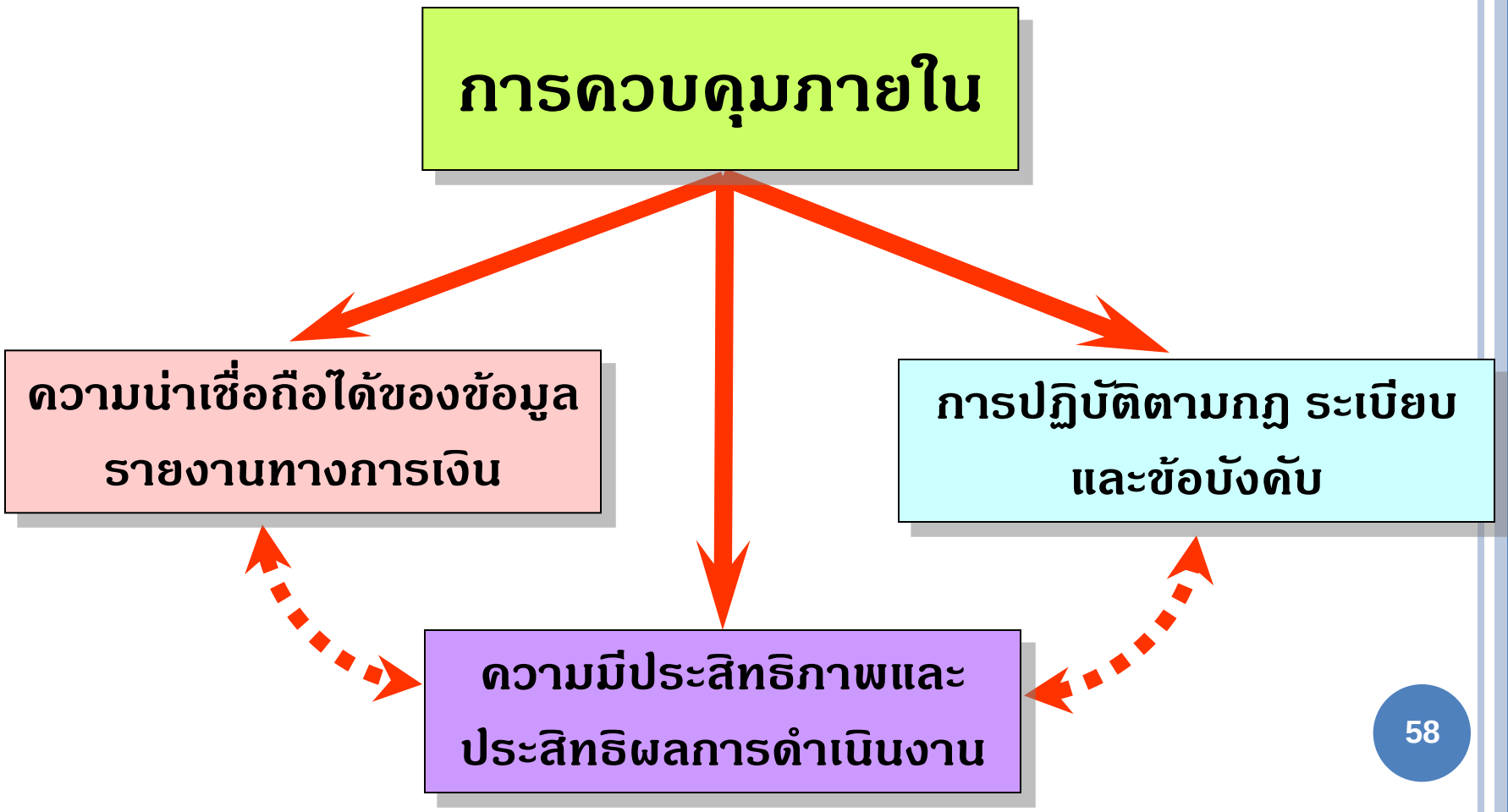
สรุปแนวคิดพื้นฐานของการควบคุมภายใน

- เป็น “ กระบวนการ ” ที่แทรกอยู่ในการปฏิบัติงานตามปกติ
- เกิดขึ้นได้จาก “ บุคลากรทุกระดับ ” ในองค์กร
- ทำให้เกิด “ ความมั่นใจอย่างสมเหตุสมผล ” ว่าการดำเนินงานจะบรรลุผลสำเร็จตามวัตถุประสงค์

องค์ประกอบการควบคุมภายใน



วัตถุประสงค์ของการควบคุมภายใน

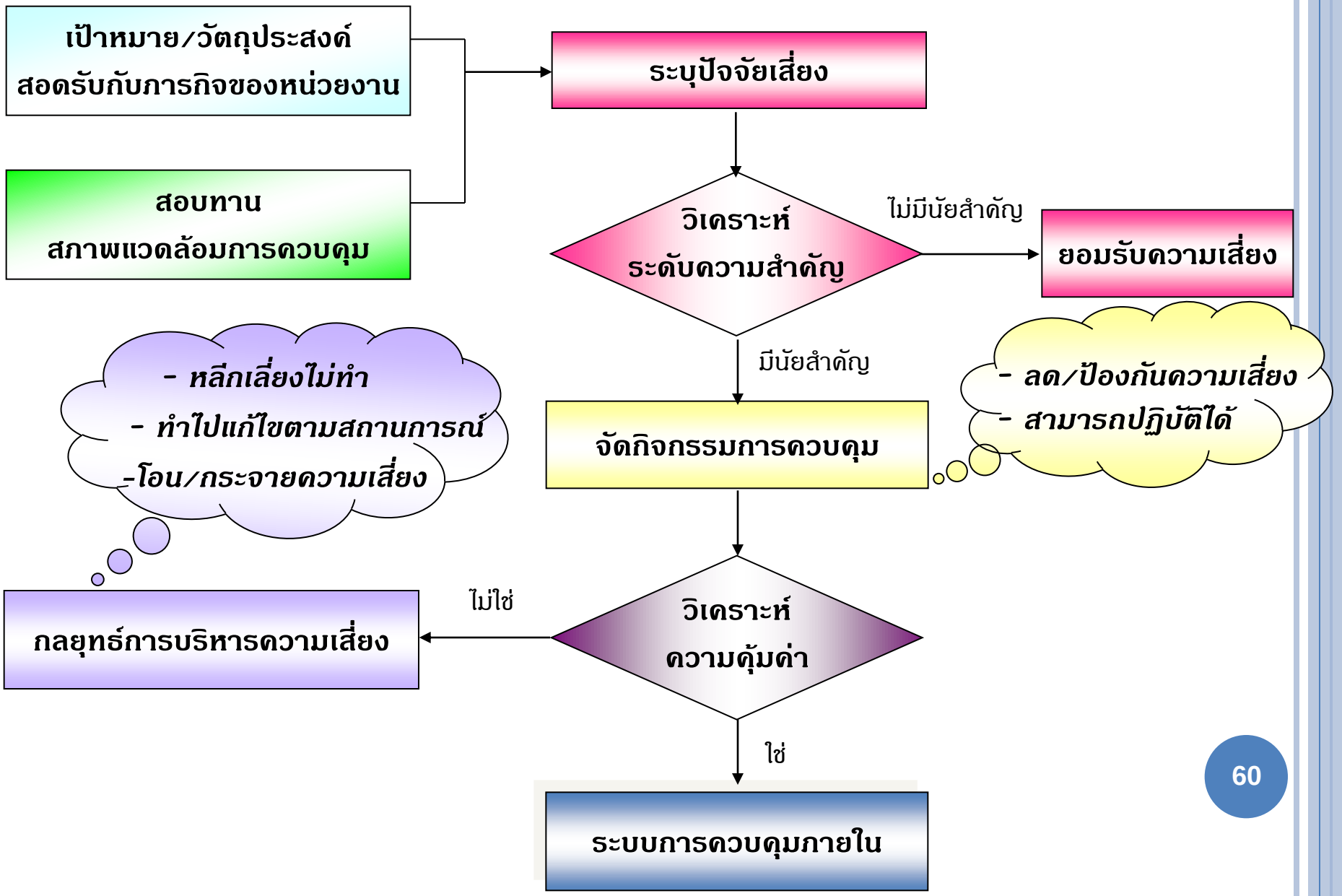


ลักษณะของการควบคุมภายใน

1. *Hard Controls*

2. *Soft Controls*

ความเสี่ยง การควบคุม การบริหารความเสี่ยง



COSO : ERM	COSO : IC
1. Strategic	
2. Operation	1. Operation
3. Reporting	2. Financial Reporting
4. Compliance	3. Compliance

COSO : ERM	COSO : IC
1. Internal Environment	1. Control Environment
2. Objective Setting	
3. Event Identification	
4. Risk Assessment	2. Risk Assessment
5. Risk Response	
6. Control Activities	3. Control Activities
7. Information & Communication	4. Information & Communication
8. Monitoring	5. Monitoring

COSO IC VS. COSO ERM

- ERM ขยายและต่อเติมมาจากองค์ประกอบที่กำหนดไว้ใน IC Framework
- ERM แยกเรื่องของการกำหนดวัตถุประสงค์ออกมาเป็นหนึ่งองค์ประกอบ แต่ใน IC นั้น วัตถุประสงค์เป็นเรื่องที่ต้องมาก่อนเหนือสิ่งอื่นใด
- ERM ขยายเรื่องการรายงานทางการเงิน (Financial Reporting) และเรื่องการประเมินความเสี่ยง (Risk Assessment) ของ IC Framework ให้กว้างขึ้น

COSO : ERM Framework

- การบริหารความเสี่ยงนั้น องค์กรโดยฝ่ายบริหารต้องมองภาพความเสี่ยงทั้งหมด (*portfolio view* of risk) ซึ่งก็คือ "Big Picture" ในการที่จะเลือกดำเนินการกับความเสี่ยง
- ฝ่ายบริหารต้องพิจารณาว่าความเสี่ยงแต่ละอย่างมีความเกี่ยวข้องกันอย่างไร

ประโยชน์ของ ERM

- ✓ จัดให้กลยุทธ์ต่าง ๆ เข้ากันได้กับ risk appetite
- ✓ ช่วยให้การตัดสินใจในเรื่องการโต้ตอบกับความเสี่ยงทำได้ดีขึ้น
- ✓ ลดสิ่งที่ไม่คาดฝันและความสูญเสียที่จะเกิดในการดำเนินงาน
- ✓ ทำให้การระบุและจัดการความเสี่ยงที่ต่อเนื่องกันอย่างทั่วถึงทุกระดับ เนื่องมาจากการมองถึงเหตุการณ์ในอนาคตที่อาจเกิดขึ้นได้
- ✓ ทำให้อาจมองเห็น "โอกาส" และฉวยโอกาสนั้นอย่างเชิงรุกได้

ความเสี่ยงทางธุรกิจที่พบได้ทั่วไป

- ความไม่เหมาะสมของนโยบายทางการบริหารหรือกระบวนการตัดสินใจ
- ความเสี่ยงด้านการเมือง การแทรกแซงโดยภาครัฐหรือกฎหมายที่เกี่ยวข้อง
- ความเสี่ยงทางกฎหมาย
- ความเสี่ยงเกี่ยวกับความปลอดภัยและสุขอนามัย
- ความเสี่ยงในการส่งสินค้าหรือให้บริการ
- การใช้หลักการบัญชีที่ไม่เป็นที่ยอมรับ

ความเสี่ยงทางธุรกิจที่พบได้ทั่วไป

- การดำเนินธุรกิจหยุดชะงัก
- การดำเนินการโดยใช้ต้นทุนสูง
- การสูญเสียรายได้หรือการที่ไม่ได้รับรู้รายได้
- ผลขาดทุนหรือความเสียหายต่อสินทรัพย์
- การสูญเสียความสามารถในการแข่งขัน
- ความไม่พึงพอใจของประชาชนทั่วไป
- การทุจริตหรือความขัดแย้งทางผลประโยชน์

ตัวอย่างการบริหารความเสี่ยง

วัตถุประสงค์

การเพิ่มประสิทธิภาพของผลผลิตหรือการให้บริการ

ความเสี่ยง

ไม่สามารถเพิ่มประสิทธิภาพของผลผลิตหรือการให้บริการ

การระบุเหตุการณ์

การดำเนินงานอาจหยุดชะงัก เนื่องจากระบบงานและโครงสร้างพื้นฐานถูกทำลายจากภัยพิบัติ

ตัวอย่างการบริหารความเสี่ยง

วิธีการบริหารความเสี่ยง:

1. จัดลำดับความสำคัญของระบบงานและโครงสร้างพื้นฐาน
2. จัดทำ Recovery Plan
3. ทดสอบและ Update Recovery Plan อย่างสม่ำเสมอ

การบริหารความเสี่ยงองค์กร

แนวคิดเดิม	แนวคิดใหม่
แยกส่วน	บรูณาการ
ทำเป็นครั้งคราว	ทำอย่างต่อเนื่อง
เน้นมุมแคบ	เน้นมุมกว้าง
ควบคุมกระบวนการ	บรรลุยุทธศาสตร์

ข้อจำกัดของ ERM

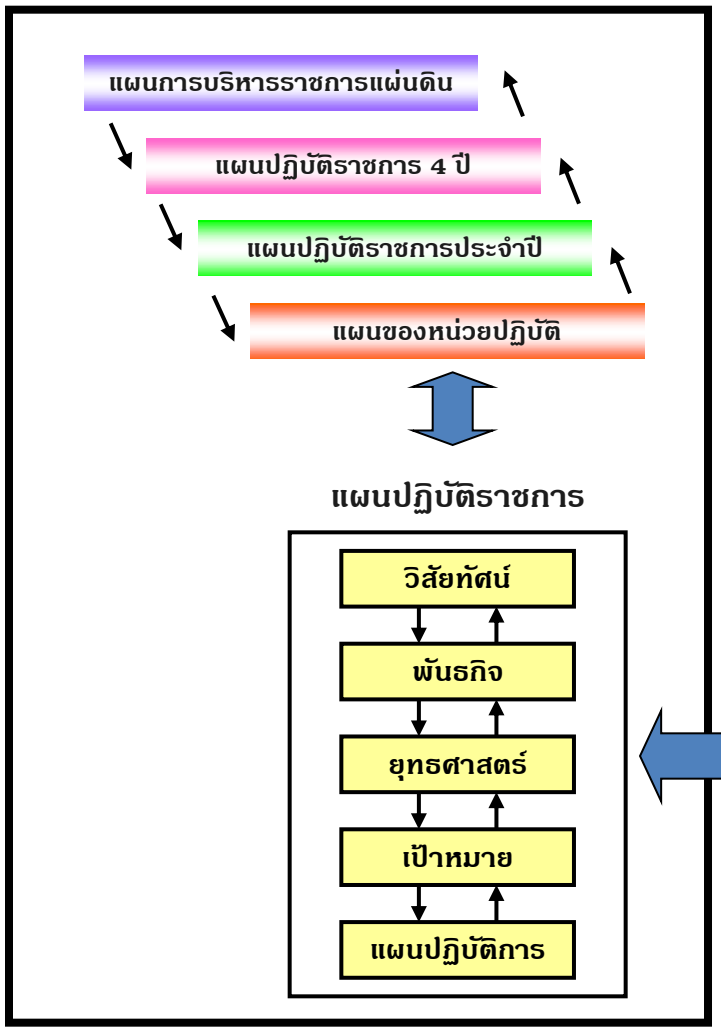
- ความเสี่ยงเป็นเรื่องของอนาคตซึ่งมีความไม่แน่นอน
- การบริหารความเสี่ยงในแต่ละระดับขององค์กร ต่างมีวัตถุประสงค์ต่างกัน ดังนั้น ERM จะช่วยให้คณะกรรมการหรือผู้บริหารทราบได้ในเวลาอันเหมาะสม เพียงแค่ว่าองค์กรกำลังมุ่งสู่ทิศทางใด และเข้าใกล้ความสำเร็จมากน้อยแค่ไหน แต่ไม่สามารถให้ความเชื่อมั่นได้ว่าจะสามารถบรรลุวัตถุประสงค์ได้
- ERM ไม่สามารถให้ความเชื่อมั่นในวัตถุประสงค์กลุ่มใดกลุ่มหนึ่งได้เต็มที่

ข้อจำกัดของ ERM

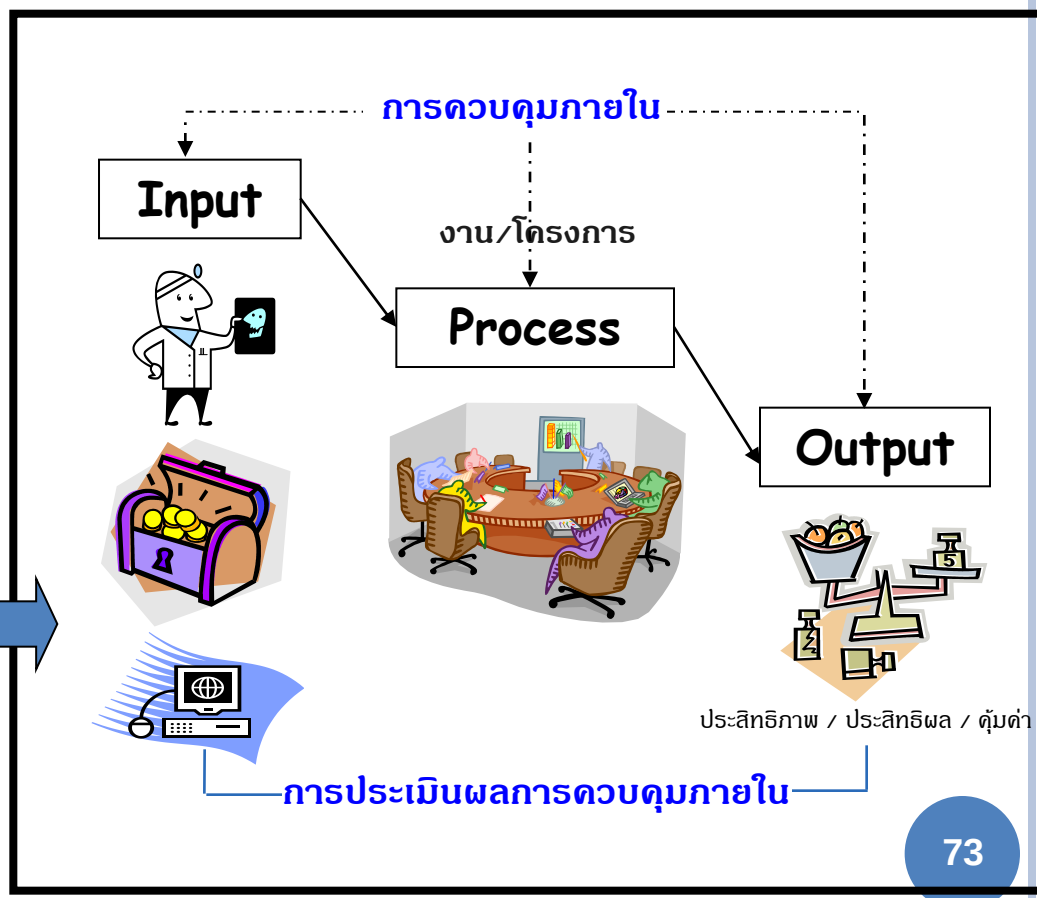
ERM ไม่สามารถให้ความเชื่อมั่นอย่างเต็มที่ (Absolute Assurance) เนื่องจากปัจจัยหลายกรณี เช่น

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

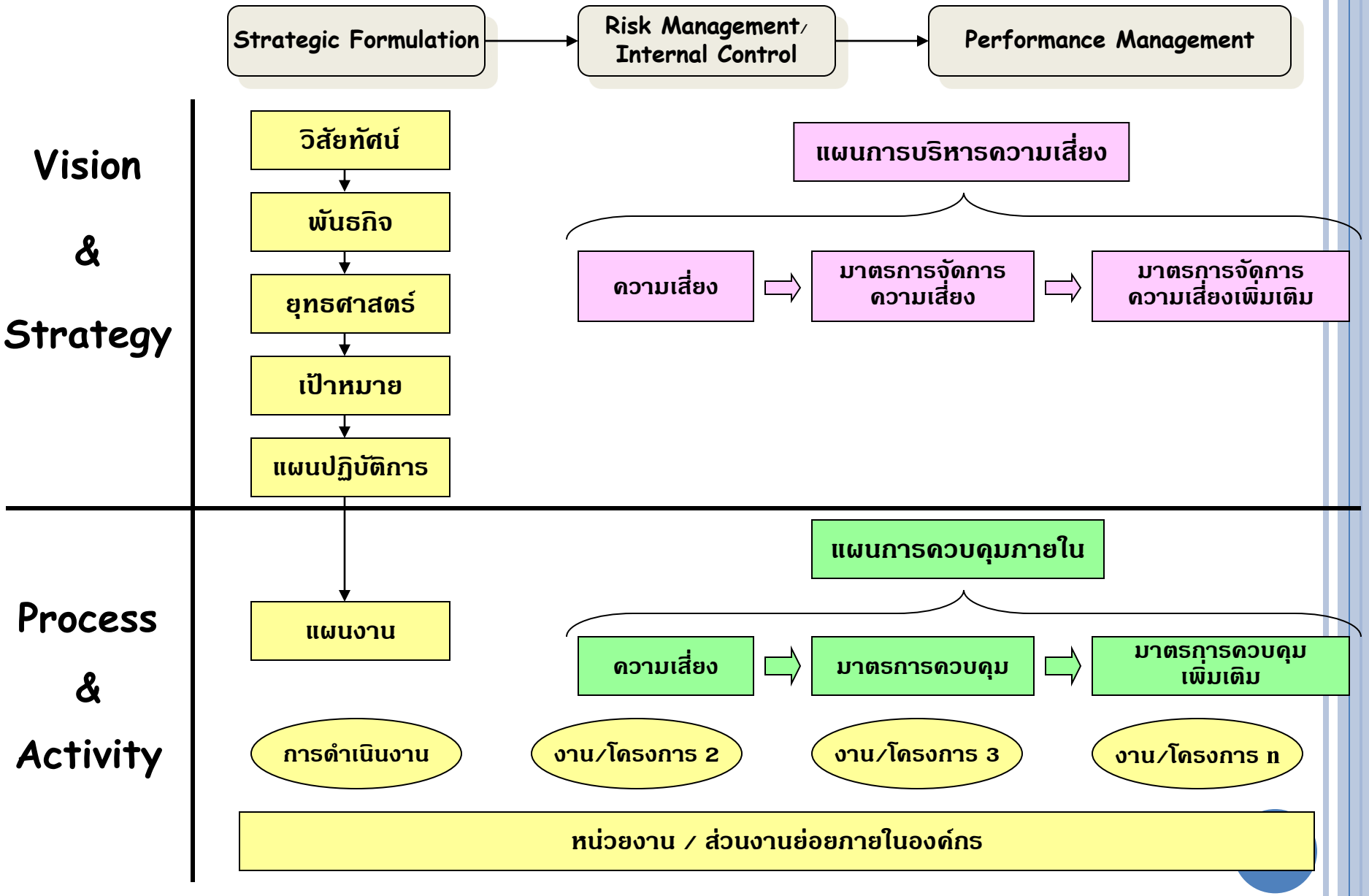
การบริหารราชการให้บรรลุเป้าหมายตามนโยบายรัฐบาล



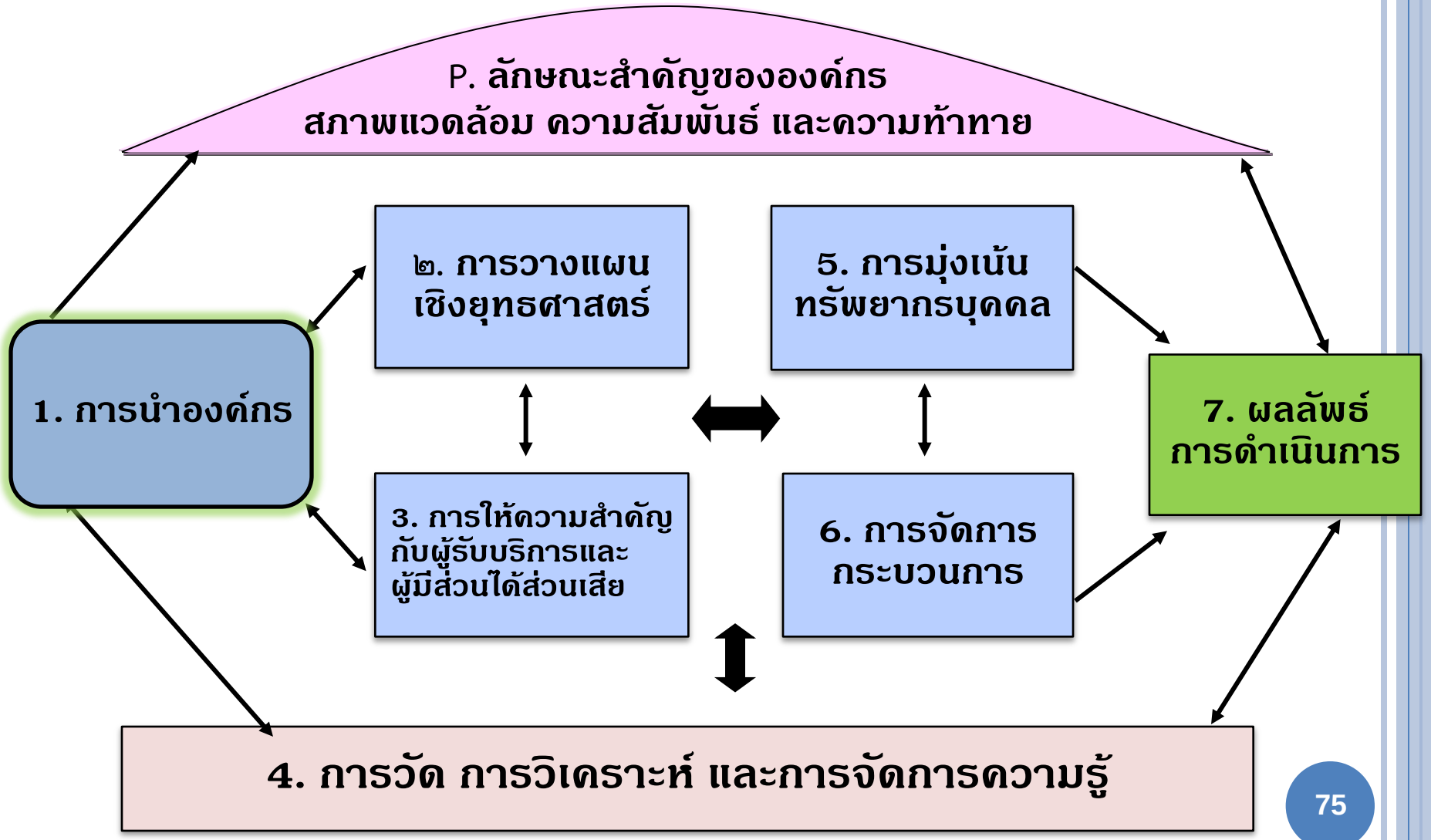
การบริหารความเสี่ยงองค์กร

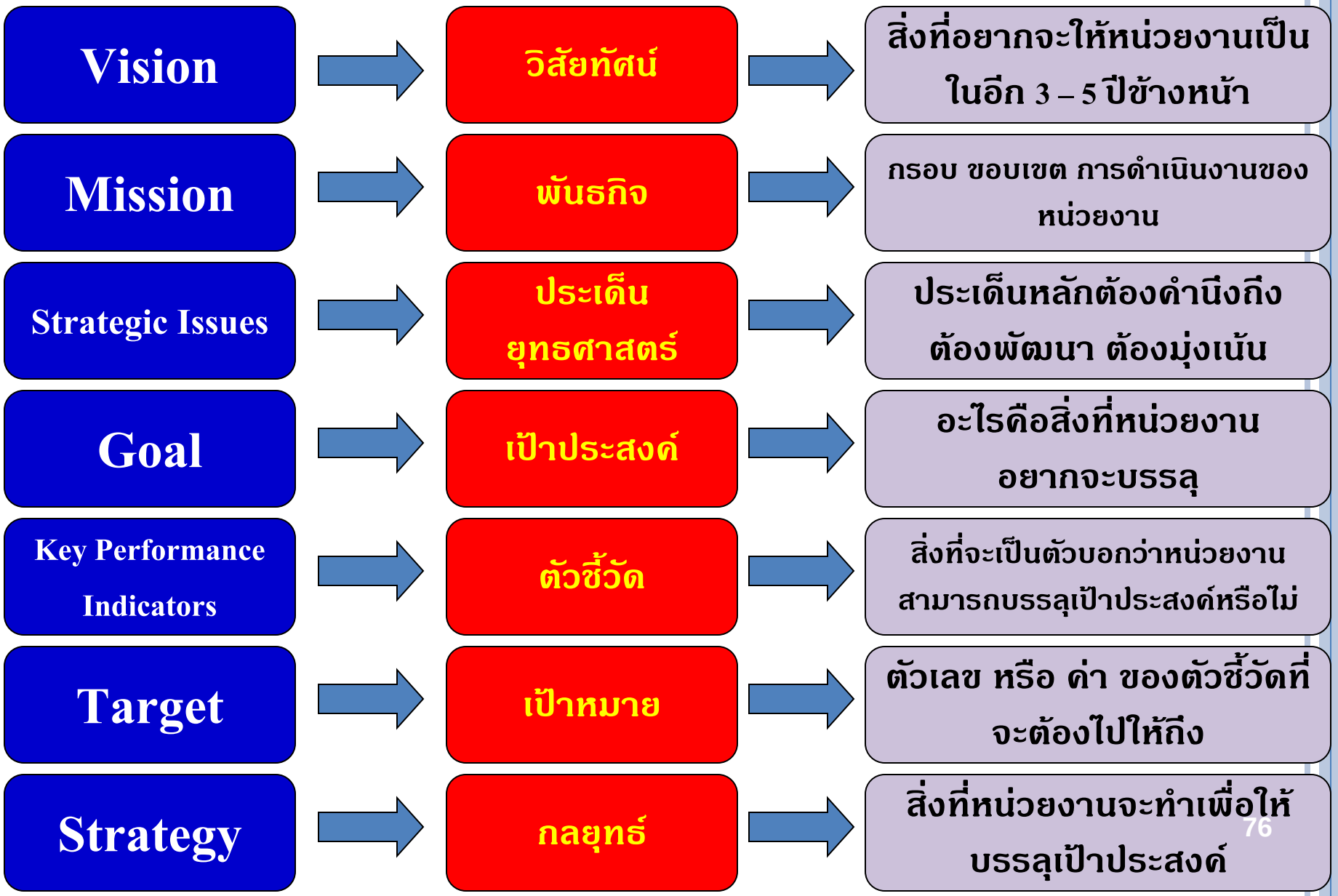


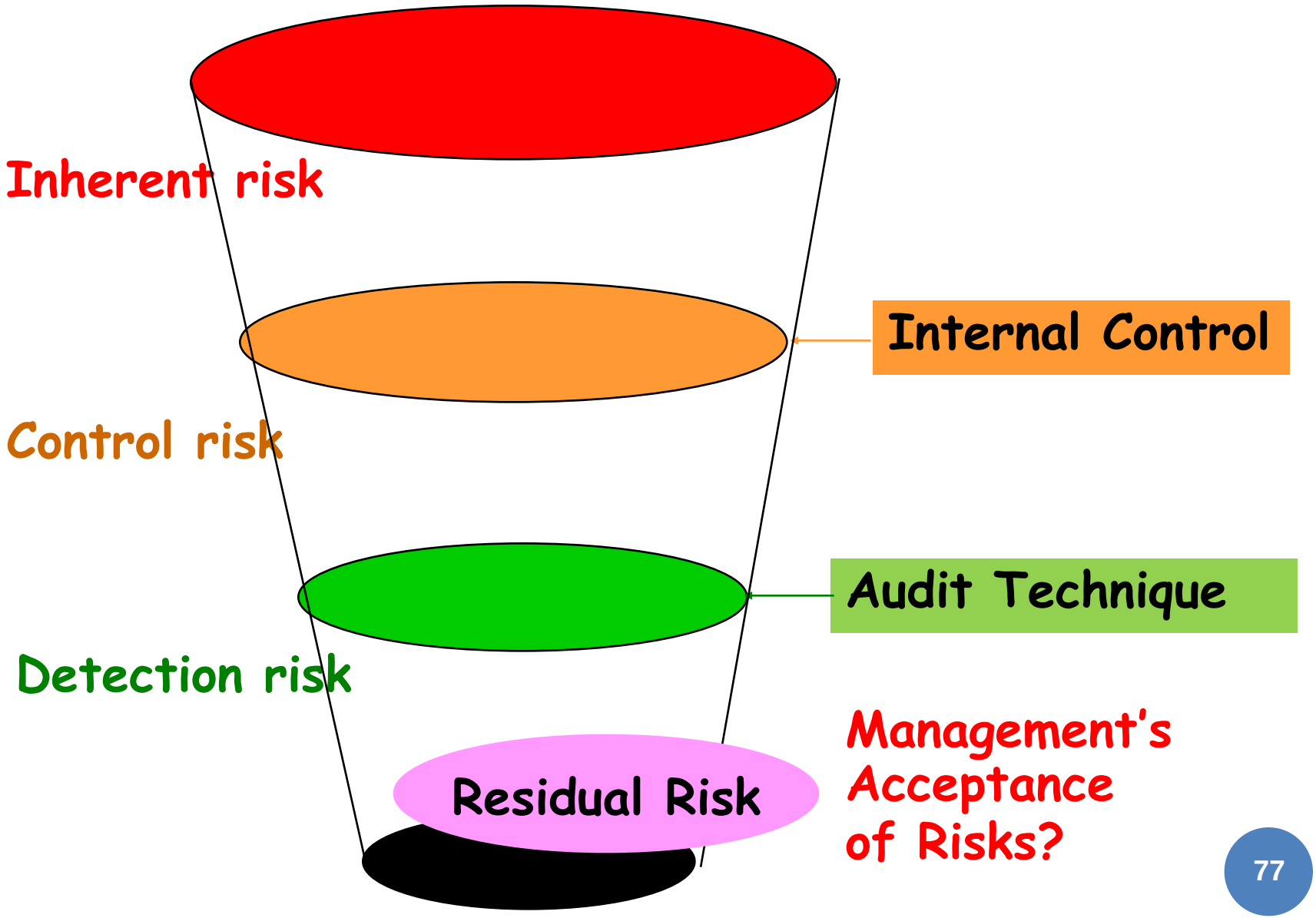
PMQA


Strategic Formulation
Risk Management/ Internal Control
Performance Management
Vision & Strategy
วิสัยทัศน์
พันธกิจ
ยุทธศาสตร์
เป้าหมาย
แผนปฏิบัติการ
แผนการบริหารความเสี่ยง
ความเสี่ยง
มาตรการจัดการความเสี่ยง
มาตรการจัดการความเสี่ยงเพิ่มเติม
Process & Activity
แผนงาน
แผนการควบคุมภายใน
ความเสี่ยง
มาตรการควบคุม
มาตรการควบคุมเพิ่มเติม
การดำเนินงาน
งาน/โครงการ 2
งาน/โครงการ 3
งาน/โครงการ n
หน่วยงาน / ส่วนงานย่อยภายในองค์กร

PMQA MODEL


P. ลักษณะสำคัญขององค์กร
สภาพแวดล้อม ความสัมพันธ์ และความท้าทาย
1. การนำองค์กร
๒. การวางแผน
เชิงยุทธศาสตร์
5. การมุ่งเน้น
ทรัพยากรบุคคล
7. ผลลัพธ์
การดำเนินการ
3. การให้ความสำคัญ
กับผู้รับบริการและ
ผู้มีส่วนได้ส่วนเสีย
6. การจัดการ
กระบวนการ
4. การวัด การวิเคราะห์ และการจัดการความรู้


Vision
วิสัยทัศน์
สิ่งที่อยากจะให้หน่วยงานเป็นในอีก 3 – 5 ปีข้างหน้า
Mission
พันธกิจ
กรอบ ขอบเขต การดำเนินงานของหน่วยงาน
Strategic Issues
ประเด็นยุทธศาสตร์
ประเด็นหลักต้องคำนึงถึง ต้องพัฒนา ต้องมุ่งเน้น
Goal
เป้าประสงค์
อะไรคือสิ่งที่หน่วยงานอยากจะบรรลุ
Key Performance Indicators
ตัวชี้วัด
สิ่งที่จะเป็นตัวบอกว่าหน่วยงานสามารถบรรลุเป้าประสงค์หรือไม่
Target
เป้าหมาย
ตัวเลข หรือ ค่า ของตัวชี้วัดที่จะต้องไปให้ถึง
Strategy
กลยุทธ์
สิ่งที่หน่วยงานจะทำเพื่อให้บรรลุเป้าประสงค์

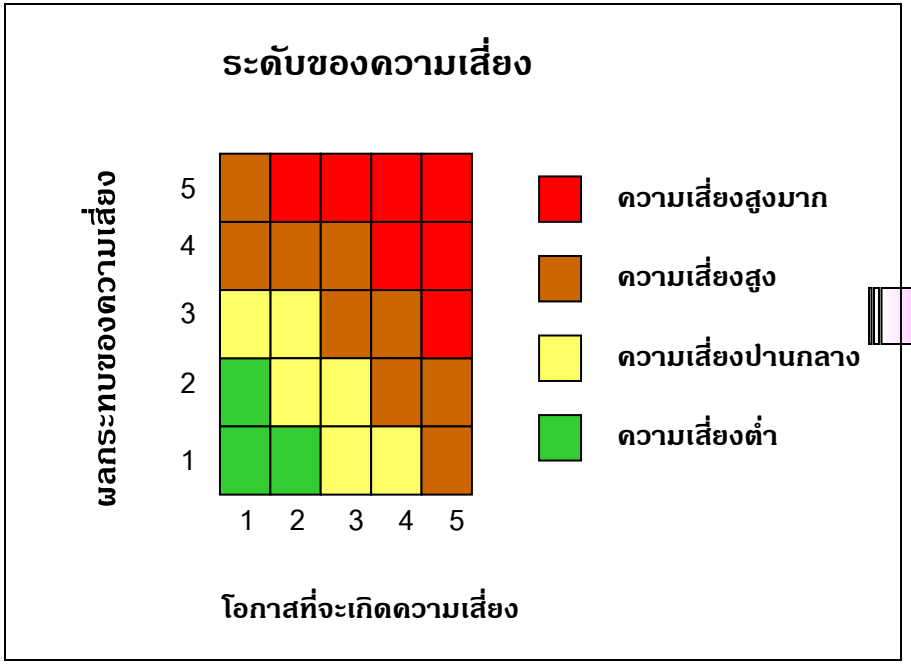


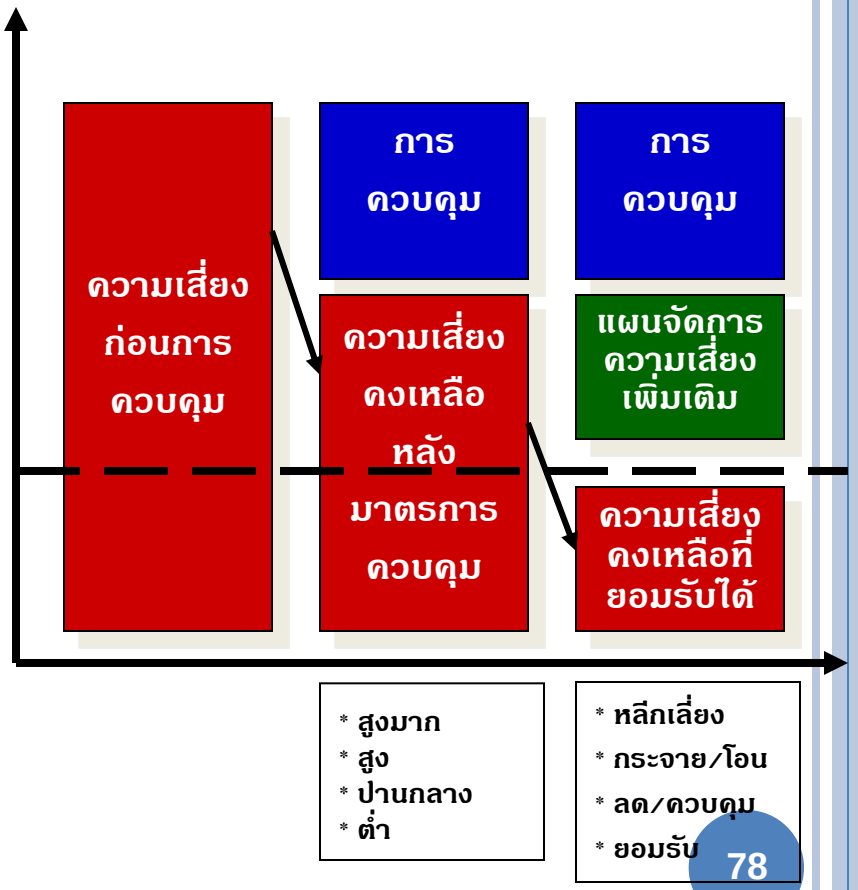
Audit Risk = IR x CR x DR

การตอบสนองความเสี่ยง

การระบุวิธีการจัดการความเสี่ยงให้อยู่ในระดับที่ยอมรับได้

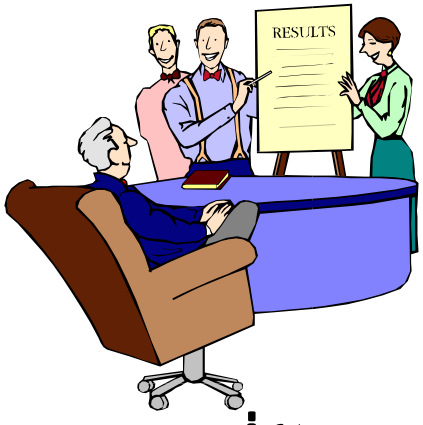
การประเมินความเสี่ยง



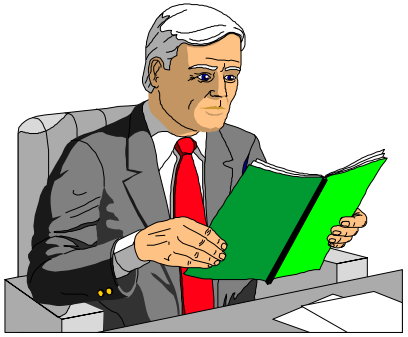


โดยคำนึงถึงต้นทุนและผลประโยชน์ที่จะได้รับ

การสนับสนุนจากผู้บริหาร



เป้าหมายที่ชัดเจน



ความรับผิดชอบ

ปัจจัยสู่ความสำเร็จ

การดำเนินการต่อเนื่อง

การวัดและติดตามผล

การสื่อสารมีประสิทธิผล


แนวทาง :
การจัดวางระบบการควบคุมภายใน
สำนักงานการตรวจเงินแผ่นดิน

ระเบียบคณะกรรมการตรวจเงินแผ่นดินว่าด้วย การกำหนดมาตรฐานการควบคุมภายใน พ.ศ. 2544

ให้ หน่วยรับตรวจเป็นผู้จัดวางระบบการควบคุมภายใน และให้มีการรายงานผลการประเมินความเพียงพอและประสิทธิผลของระบบการควบคุมภายใน โดยเสนอรายงานต่อคณะกรรมการตรวจเงินแผ่นดิน ผู้กำกับดูแล และคณะกรรมการตรวจสอบ (ถ้ามี) ภายใน 90 วันนับจากวันสิ้นปีงบประมาณหรือปีปฏิทิน โดยมีรายละเอียดดังนี้

(1) ทำความเห็นว่าระบบการควบคุมภายในของหน่วยรับตรวจที่ใช้อยู่มีมาตรฐานตามระเบียบฯ

(2) รายงานผลการประเมินความเพียงพอและประสิทธิผลของระบบการควบคุมภายใน ในการบรรลุวัตถุประสงค์และเป้าหมายที่กำหนด รวมทั้งข้อมูลสรุปผลการประเมิน แต่ละองค์ประกอบของการควบคุมภายใน ประกอบด้วย 5 องค์ประกอบ

(3) จุดอ่อนของระบบการควบคุมภายในพร้อมข้อเสนอแนะและแผนการปรับปรุงระบบการควบคุมภายใน

ข้อกำหนดตามระเบียบฯ คตง.

ฝ่ายบริหารต้องจัดให้มีการติดตามประเมินผลอย่างต่อเนื่องและสม่ำเสมอ โดย

- ☞ การติดตามผลในระหว่างการปฏิบัติงาน
- ☞ การประเมินผลเป็นรายครั้ง
  - ✓ การประเมินการควบคุมด้วยตนเอง (Control Self Assessment : CSA.)
  - ✓ การประเมินการควบคุมอย่างเป็นอิสระ (Independent Assessment)

รูปแบบการประเมินผลการควบคุมภายใน

- การประเมินผลการควบคุมด้วยตนเอง (Control Self Assessment)
- การประเมินผลการควบคุมอย่างเป็นอิสระ (Independent Assessment)

รูปแบบการประเมินผลการควบคุมภายใน

- ***การประเมินผลการควบคุมด้วยตนเอง (Control Self Assessment)***

*เป็นการประเมินผลในลักษณะความร่วมมือกันระหว่าง**ผู้บริหาร กับผู้ปฏิบัติงาน** ที่มีส่วนเกี่ยวข้องโดยตรงกับ การปฏิบัติงานตามระบบการควบคุมภายในที่วางไว้*

การประเมินผลภายในส่วนราชการ/จังหวัด

- **การประเมินผลการควบคุมภายในของส่วนราชการ/จังหวัด**
- **การประเมินผลการควบคุมภายในภาพรวม**

รูปแบบการประเมินผลการควบคุมภายใน

➢ **การประเมินผลการควบคุมอย่างเป็นอิสระ**
(Independent Assessment)

*เป็นการประเมินผลโดย**ผู้ที่ไม่มีที่มีส่วนเกี่ยวข้อง**โดยตรงกับการกำหนดมาตรการหรือออกแบบระบบการควบคุมภายในของหน่วยงาน เช่น ผู้ตรวจสอบภายใน ผู้ตรวจสอบ/ประเมินภายนอกหน่วยงานที่ทำหน้าที่ประเมินผล เป็นต้น*

การประเมินผลภายในส่วนราชการ/จังหวัด

- **การประเมินผลการควบคุมภายในโดยผู้ตรวจสอบภายใน**

การรายงานตามระเบียบฯ ข้อ 6

ระดับหน่วยงานย่อย

- รายงานผลการประเมินองค์ประกอบของการควบคุมภายใน - แบบ ปย. 1
- รายงานการประเมินผลและการปรับปรุงการควบคุมภายใน - แบบ ปย. 2

ระดับองค์การ

- หนังสือรับรองการประเมินผลการควบคุมภายใน - แบบ ปอ. 1
- รายงานผลการประเมินองค์ประกอบของการควบคุมภายใน - แบบ ปอ. 2
- รายงานแผนการปรับปรุงการควบคุมภายใน - แบบ ปอ. 3

ผู้ตรวจสอบภายใน

- รายงานผลการสอบทานการประเมินการควบคุมภายใน - แบบ ปส.

แนวทางการจัดวางระบบการควบคุมภายใน

แผนปฏิบัติงาน / โครงการ

กำหนดวัตถุประสงค์

ระบุปัจจัยเสี่ยง

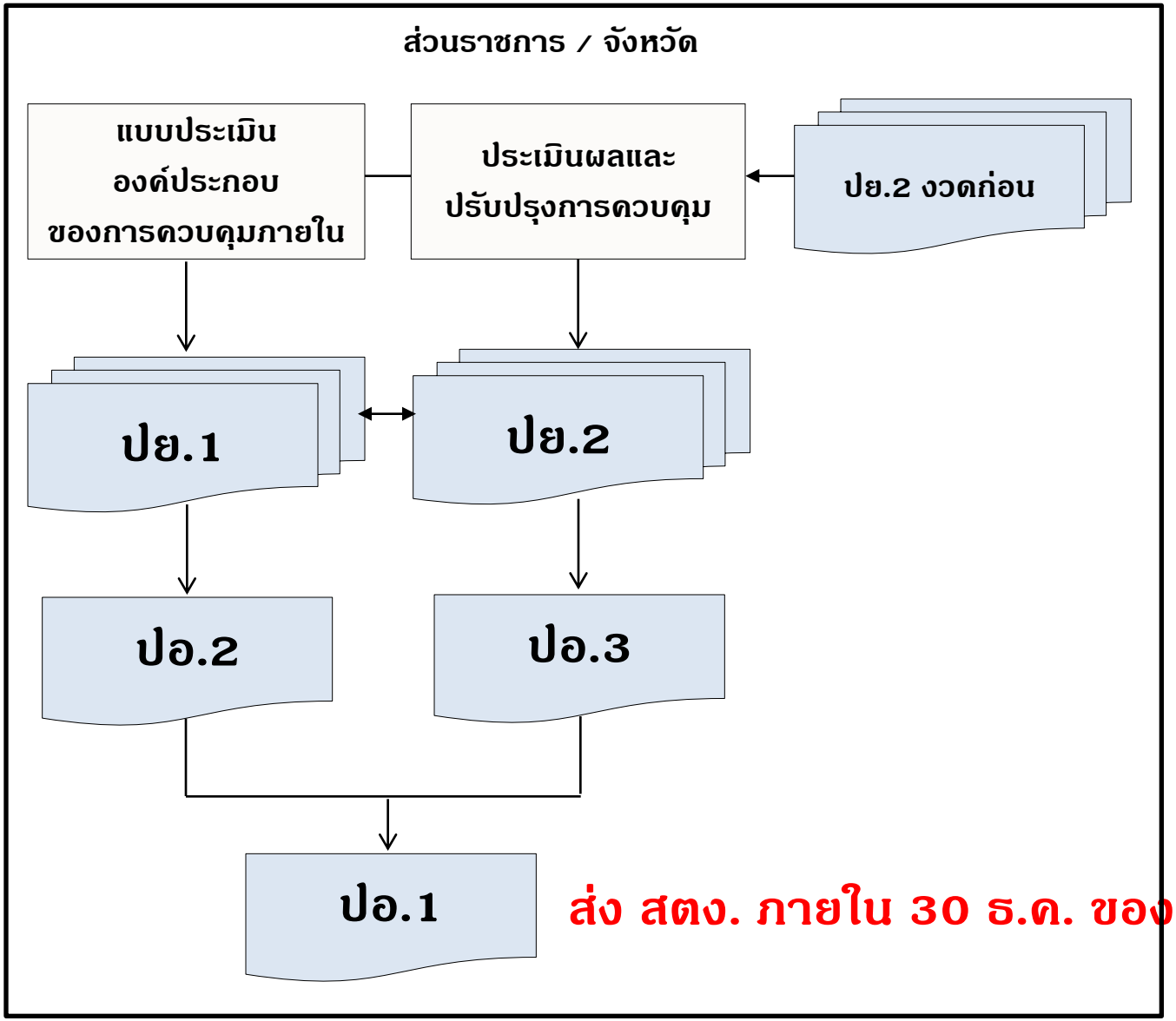
จัดกิจกรรมการควบคุม

ดำเนินการตามระบบ ฯ

ติดตามและประเมินผล

จัดทำรายงานการควบคุมภายใน

ขั้นตอนการจัดทำรายงานตามแนวทางของ คตง.

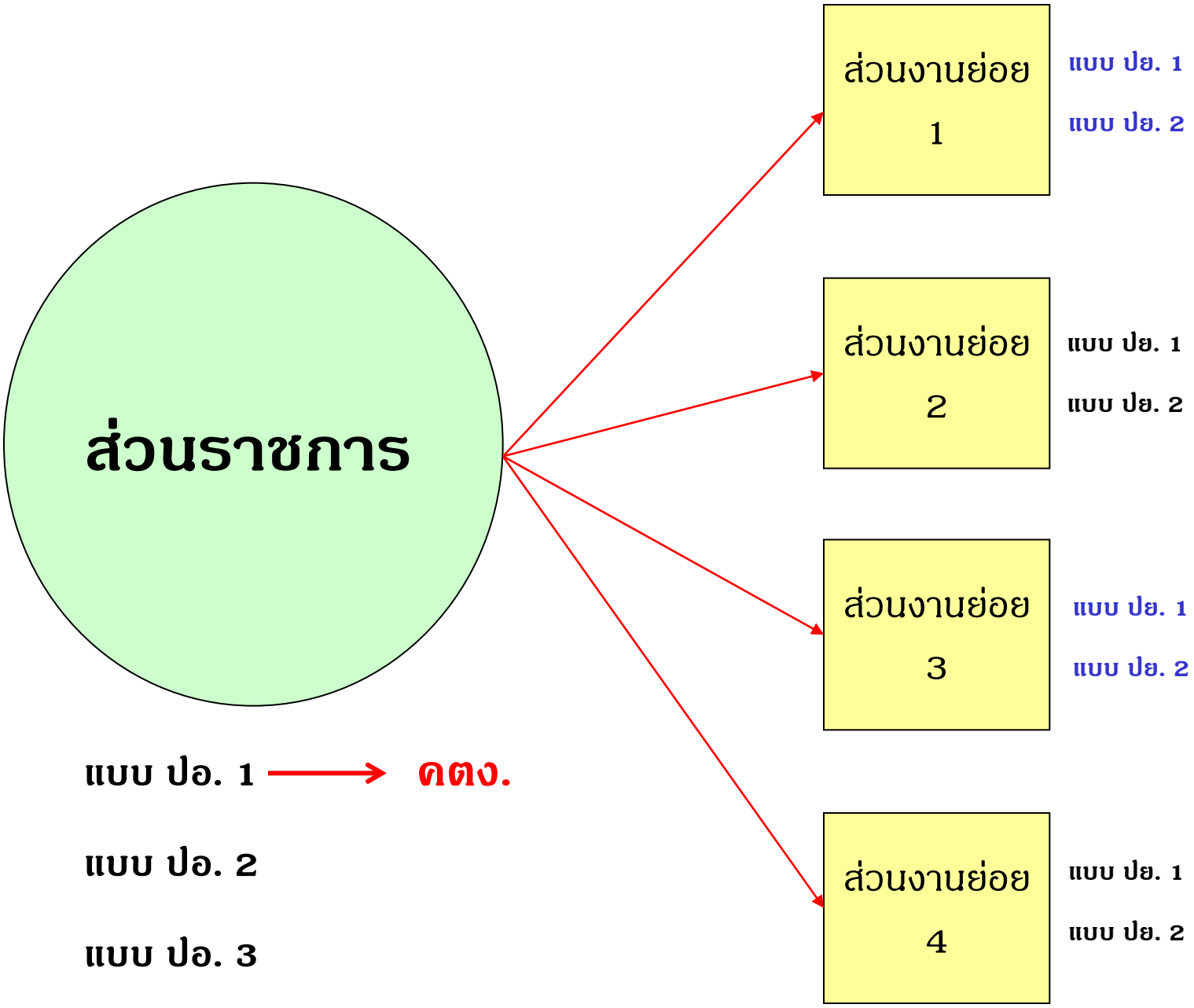


ผู้ตรวจสอบภายใน

สอบทานและ
ประเมินผล
การควบคุมภายใน

ปส.

ส่ง สตง. ภายใน 30 ธ.ค. ของทุกปี


ส่วนราชการ
ส่วนงานย่อย 1
แบบ ปย. 1
แบบ ปย. 2
ส่วนงานย่อย 2
แบบ ปย. 1
แบบ ปย. 2
ส่วนงานย่อย 3
แบบ ปย. 1
แบบ ปย. 2
ส่วนงานย่อย 4
แบบ ปย. 1
แบบ ปย. 2
แบบ ปอ. 1
คตง.
แบบ ปอ. 2
แบบ ปอ. 3

หนังสือรับรองการจัดวางระบบการควบคุมภายใน

เรียน คณะกรรมการตรวจเงินแผ่นดิน

.....(ชื่อหน่วยงาน)...ขอรับรองว่า ได้จัดวางระบบการควบคุมภายใน และนำมาใช้สำหรับการปฏิบัติงานในปัจจุบัน โดยมีวัตถุประสงค์เพื่อสร้างความมั่นใจอย่างสมเหตุสมผลว่า การดำเนินงานของ .....(ชื่อหน่วยงาน)..... จะบรรลุวัตถุประสงค์ของการควบคุมภายในด้านประสิทธิผลและประสิทธิภาพของการดำเนินงานและการใช้ทรัพยากร ซึ่งรวมถึงการดูแลรักษาทรัพย์สิน การป้องกันหรือลดความผิดพลาด ความเสียหาย การรั่วไหล การสิ้นเปลืองหรือการทุจริต ด้านความเชื่อถือได้ของรายงานทางการเงิน และด้านการปฏิบัติตามกฎหมาย ระเบียบ ข้อบังคับ มติคณะรัฐมนตรี และนโยบาย ซึ่งรวมถึงระเบียบปฏิบัติของฝ่ายบริหาร

ทั้งนี้ .....(ชื่อหน่วยงาน)... จะกำหนดให้มีการประเมินผลระบบการควบคุมภายในที่นำมาใช้ในปัจจุบัน เพื่อปรับปรุงให้มีประสิทธิผลและเพียงพอ ตามระเบียบคณะกรรมการตรวจเงินแผ่นดินว่าด้วยการกำหนดมาตรฐานการควบคุมภายใน พ.ศ.2544 ข้อ 6 ต่อไป

ลายมือชื่อ.....

( )

ตำแหน่ง .....ผู้บริหารสูงสุดของหน่วยงาน.....

วันที่.....เดือน.....พ.ศ.....

แบบ ปย. 1

ชื่อส่วนงานย่อย.....

รายงานผลการประเมินองค์ประกอบของการควบคุมภายใน

ณ วันที่.....เดือน.....พ.ศ.....

องค์ประกอบการควบคุมภายใน (1)	ผลการประเมิน / ข้อสรุป (2)
1. 2. 3. 4. 5.	
ผลการประเมินโดยรวม ลายมือชื่อ..... ตำแหน่ง..... วันที่.....	

แบบ ปย. 2

ชื่อส่วนงานย่อย.....

รายงานการประเมินผลและการปรับปรุงการควบคุมภายใน

ณ วันที่.....เดือน.....พ.ศ.....

กระบวนการปฏิบัติงาน โครงการ/กิจกรรม/ด้าน ของงานที่ประเมินและ วัตถุประสงค์ของ การควบคุม (1)	การควบคุม ที่มีอยู่ (2)	การประเมินผล การควบคุม (3)	ความเสี่ยง ที่ยังมีอยู่ (4)	การปรับปรุง การควบคุม (5)	กำหนดเสร็จ/ ผู้รับผิดชอบ (6)	หมายเหตุ (7)

ลายมือชื่อ.....

ตำแหน่ง.....

วันที่.....

หนังสือรับรองการประเมินผลการควบคุมภายใน

เรียน คณะกรรมการตรวจเงินแผ่นดิน / ผู้กำกับดูแล / คณะกรรมการตรวจสอบ

.....(ชื่อหน่วยงาน).....ได้ประเมินผลการควบคุมภายใน สำหรับปีสิ้นสุดวันที่.....เดือน.....พ.ศ. ..... ด้วยวิธีการที่ .....(ชื่อหน่วยงาน)..... กำหนด โดยมีวัตถุประสงค์เพื่อสร้างความมั่นใจอย่างสมเหตุสมผลว่า การดำเนินงานจะบรรลุวัตถุประสงค์ของการควบคุมภายใน ด้านประสิทธิผลและประสิทธิภาพของการดำเนินงาน และการใช้ทรัพยากร ซึ่งรวมถึงการดูแลรักษาทรัพย์สิน การป้องกันหรือลดความผิดพลาด ความเสียหาย การรั่วไหล การสิ้นเปลือง หรือการทุจริต ด้านความเชื่อถือได้ของรายงานทางการเงินและการดำเนินงาน และด้านการปฏิบัติตามกฎหมาย ระเบียบ ข้อบังคับ มติคณะรัฐมนตรี และนโยบาย ซึ่งรวมถึงระเบียบปฏิบัติของฝ่ายบริหาร

จากผลการประเมินดังกล่าวเห็นว่าการควบคุมภายในของ.....(ชื่อหน่วยงาน)..... สำหรับปีสิ้นสุดวันที่..... เดือน.....พ.ศ. ..... เป็นไปตามระบบการควบคุมภายในที่กำหนดไว้ มีความเพียงพอและบรรลุวัตถุประสงค์ของการควบคุมภายในตามที่กล่าวไว้ในวรรคแรก

ลายมือชื่อ.....

ตำแหน่ง.....

วันที่.....

หนังสือรับรองการประเมินผลการควบคุมภายใน (ต่อ)

★ กรณีมีจุดอ่อนของการควบคุมภายในสามารถรายงานจุดอ่อนที่มีนัยสำคัญ

จากผลการประเมินดังกล่าวเห็นว่าการควบคุมภายในของ.....(ชื่อหน่วยงาน)..... สำหรับปีสิ้นสุดวันที่..... เดือน.....พ.ศ. ..... เป็นไปตามระบบการควบคุมภายในที่กำหนดไว้ มีความเพียงพอและบรรลุวัตถุประสงค์ของการควบคุมภายในตามที่กล่าวไว้ในวรรคแรก

อนึ่งการควบคุมภายในยังคงมีจุดอ่อนที่มีนัยสำคัญ ดังนี้

1. .....

2. .....

3. .....

ซึ่ง.....(ชื่อหน่วยงาน)..... จะดำเนินการปรับปรุงการควบคุมโดยกำหนดไว้ในแผนปฏิบัติงานประจำปีต่อไป

ลายมือชื่อ.....

ตำแหน่ง.....

วันที่.....

ชื่อหน่วยงาน.....

รายงานผลการประเมินองค์ประกอบการควบคุมภายใน

ณ วันที่.....เดือน.....พ.ศ.....

องค์ประกอบการควบคุมภายใน (1)	ผลการประเมิน / ข้อสรุป (2)
1. 2. 3. 4. 5.	
ผลการประเมินโดยรวม ลายมือชื่อ..... ตำแหน่ง..... วันที่.....	

ชื่อหน่วยงาน.....

รายงานแผนการปรับปรุงการควบคุมภายใน

ณ วันที่.....เดือน.....พ.ศ.....

กระบวนการปฏิบัติงาน โครงการ/กิจกรรม/ด้าน ของงานที่ประเมินและ วัตถุประสงค์ของ การควบคุม (1)	ความเสี่ยง ที่ยังมีอยู่ (2)	งวด/เวลาที่ พบจุดอ่อน (3)	การปรับปรุงการควบคุม (4)	กำหนดเสร็จ/ ผู้รับผิดชอบ (5)	หมายเหตุ (6)

ลายมือชื่อ.....

ตำแหน่ง.....

วันที่.....

รายงานผลการสอบทานการประเมินผลการควบคุมภายใน

เรียน ผู้บริหารสูงสุดของหน่วยงาน

ข้าพเจ้าได้สอบทานการประเมินระบบการควบคุมภายในของ.....(ชื่อหน่วยงาน)..... สำหรับปีสิ้นสุดวันที่ ..... เดือน ..... พ.ศ. ..... การสอบทานได้ปฏิบัติอย่างสมเหตุสมผลและระมัดระวังอย่างรอบคอบ ผลการสอบทานพบว่า การประเมินผลการควบคุมภายในเป็นไปตามวิธีการที่กำหนด ระบบการควบคุมภายในมีความเพียงพอและสามารถบรรลุวัตถุประสงค์ของการควบคุมภายใน

ลายมือชื่อ.....

ตำแหน่ง หัวหน้าหน่วยตรวจสอบภายใน

วันที่.....

รายงานผลการสอบทานการประเมินผลการควบคุมภายใน

★กรณีมีข้อตรวจพบหรือข้อสังเกตที่มีนัยสำคัญ

ข้าพเจ้าได้สอบทานการประเมินผลการควบคุมภายในของ.....(ชื่อหน่วยงาน)..... สำหรับปีสิ้นสุดวันที่..... เดือน.....พ.ศ. ..... การสอบทานได้ปฏิบัติอย่างสมเหตุสมผลและระมัดระวังอย่างรอบคอบผลการสอบทานพบว่าการประเมินผลการควบคุมภายในเป็นไปตามวิธีการที่กำหนด ระบบการควบคุมภายในมีความเพียงพอและสามารถบรรลุวัตถุประสงค์ของการควบคุมภายใน อย่างไรก็ตามมีข้อสังเกตที่มีนัยสำคัญ ดังนี้

.....

.....

.....

.....

.....

ลายมือชื่อ.....

ตำแหน่ง หัวหน้าหน่วยตรวจสอบภายใน

วันที่.....

สวัสดี

สำนักกำกับและพัฒนาการตรวจสอบภาครัฐ

กรมบัญชีกลาง

โทร. 0 2127 7285

E-mail address : IASTD@cgd.go.th