Continuity of Operations in the Risky World

IT Governance:Enterprise Risk Management

วันที่ 23 เมษายน 2551 เวลา 9.30 – 10.30 น.

ณ โรงแรม เอเวอร์กรีน ลอเรล

โดย : เมธา สุวรรณสาร

Metha Suvanasarn

แนวทางการนำเสนอ

1.CGกับความเสี่ยงใหม่ๆเมื่อมีการนำคอมพิวเตอร์เข้ามาใช้งานกับผู้บริหาร

2.การจัดการ/ การควบคุมความเสี่ยงให้อยู่ในระดับที่องค์กรยอมรับได้

3.บางมุมมองด้าน IT Governance กับ BCM และ Balance Scorecard

4.องค์ประกอบและความสัมพันธ์ของ ITG & COSO/ ERM

5. ITG-COBIT-ISO27001 และการหลอมรวม COSO/ERM เพื่อการบริหารแบบสอดประสานและบูรณาการทั่วทั้งองค์กร เพื่อบรรลุเป้าหมาย

6. Key Success Factors และ KPI ด้าน IT/ITG บางมุมมองตามหลัก Bsc.

7. การติดตามและการตรวจสอบแบบสอดประสานและบูรณาการทางด้านIT/ITG

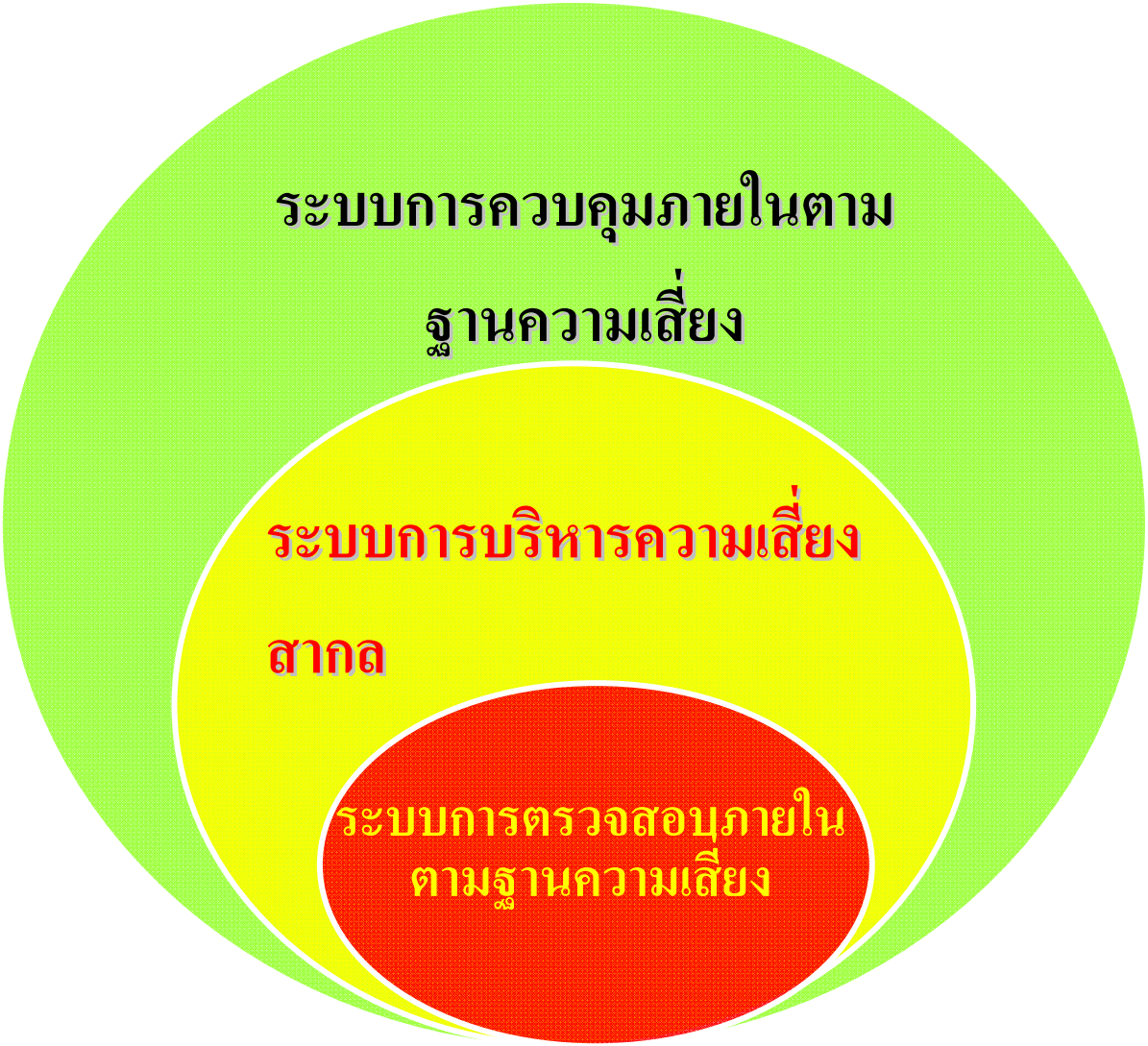
8. การขับเคลื่อน และ การแนวทางการประเมินผลด้าน ITG/IT & ERM

9. สรุปและ ถาม-ตอบ

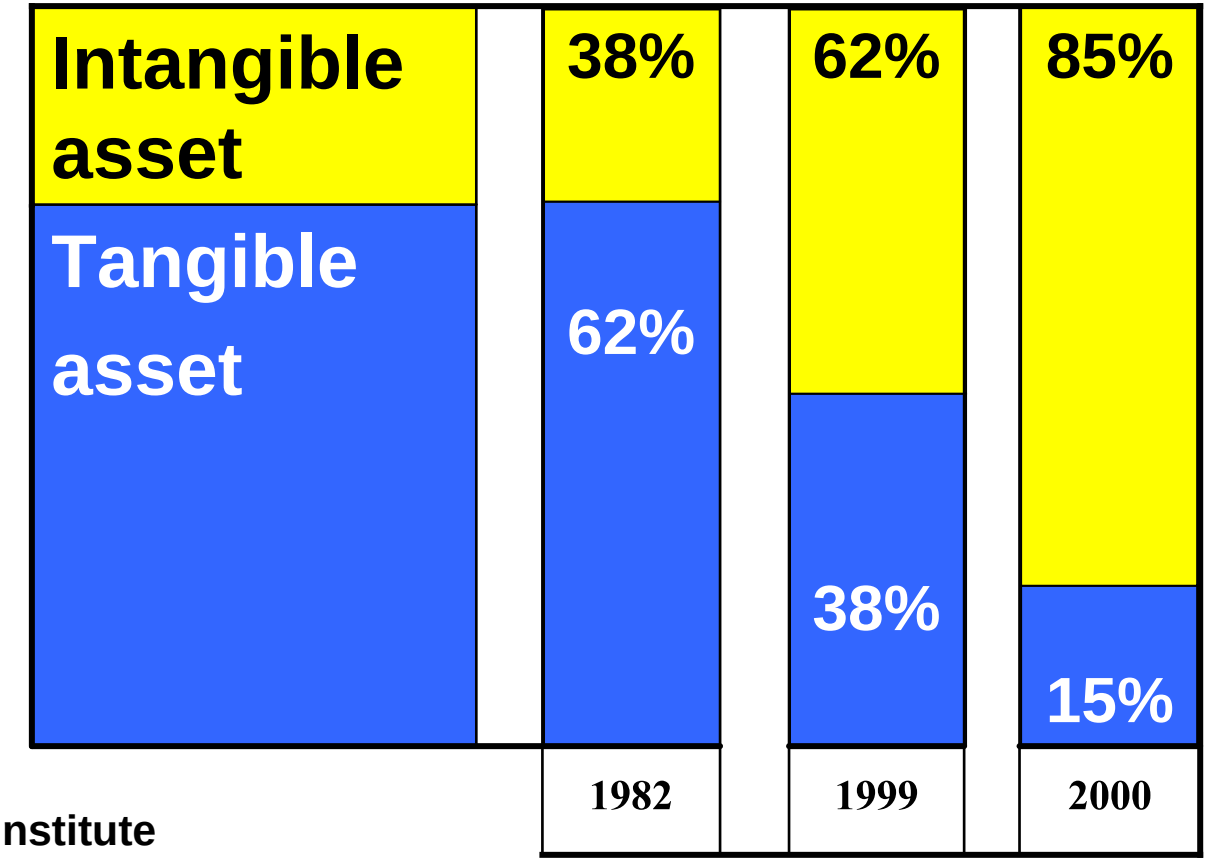
การกำกับดูแลกิจการที่ดี
เพื่อการบรรลุผลการปฏิบัติงานขององค์กร
การบริหารกิจการบ้านเมืองที่ดี
มิติที่1 ประสิทธิผลตามพันธกิจ
มิติที่2 ประสิทธิภาพของการปฏิบัติราชการ
มิติที่3 คุณภาพการให้บริการ
มิติที่4 การพัฒนาองค์กร
1. เกิดประโยชน์สุขของประชาชน
2. เกิดผลสัมฤทธิ์ต่อภารกิจของรัฐทั้งในระดับชาติและระดับส่วนราชการ
3. มีประสิทธิภาพและเกิดความคุ้มค่าในเชิงภารกิจของรัฐ
4. ขั้นตอนการปฏิบัติงานเกินความจำเป็น
5. มีการปรับปรุงภารกิจของส่วนราชการให้ทันต่อสถานการณ์
6. ประชาชนได้รับการอำนวยความสะดวกและได้รับการตอบสนองความต้องการ
7. มีการประเมินผลการปฏิบัติราชการอย่างสม่ำเสมอ
Accountability
Equitable Treatment
Transparency
Soul and Mental Aware
Protocol Best Practices
Operational Team Value

หลักบรรษัทภิบาล (Corporate Governance)
ระบบบริหารกิจการบ้านเมือง
และสัง ค มที่ดี
ระบบการ ควบคุ มภายใน
การประเมิ น คุณ ภาพ
ภายนอก(QAR)และผู้ควบคุม
ระบบบริหารความเสี่ยง
แผนการพัฒนา องค์กร
ระบบการตรวจสอบภายใน
เกณฑ์รางวัล คุณภาา
พแห่งชาติ(TQA)
ระบบการบริหารความเสี่ยงทั่วทั้งองค์กร(ERM)

ความสัมพันธ์ของการควบคุมภายใน การบริหารความเสี่ยง และการตรวจสอบภายใน



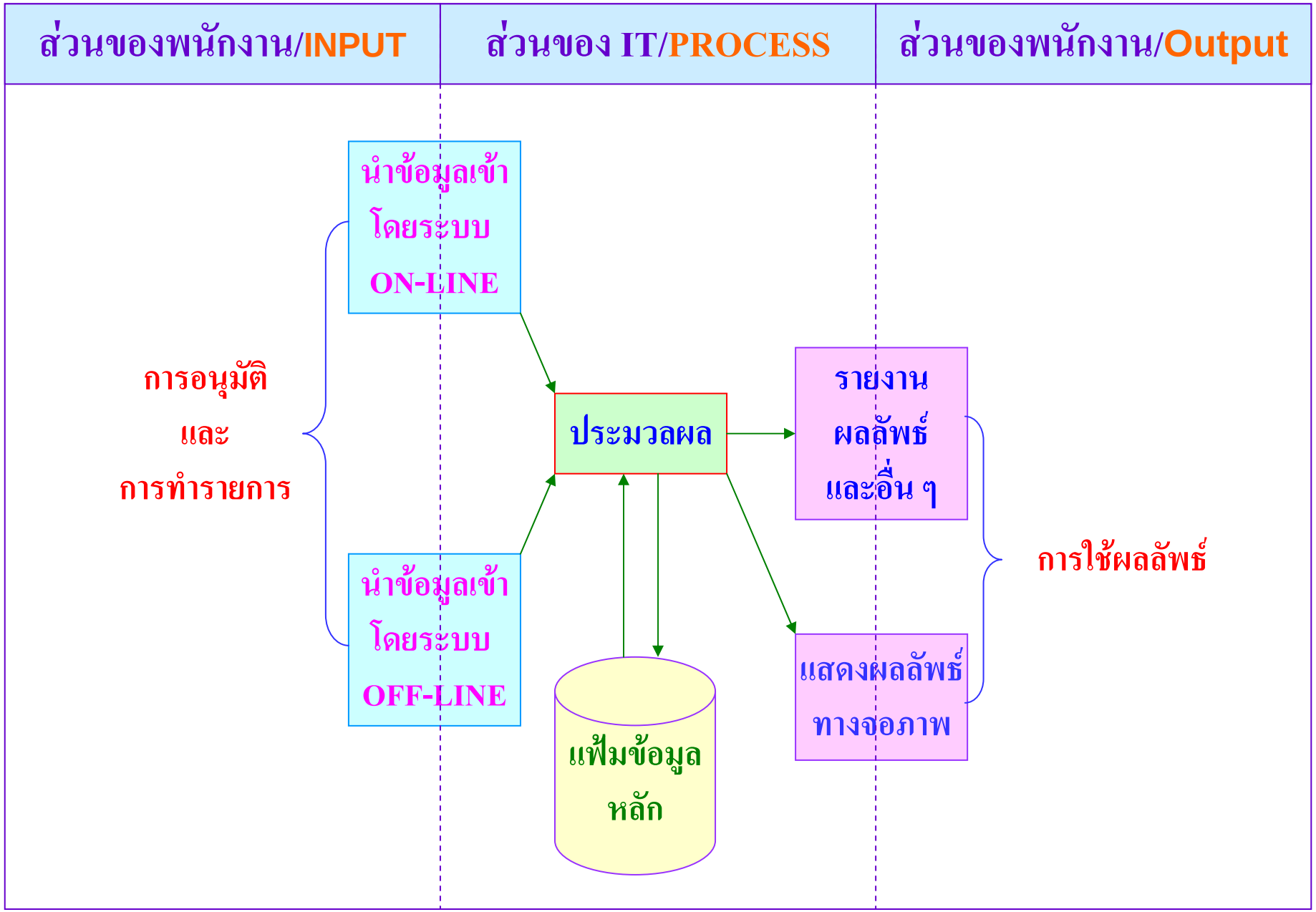
Tangible to Intangible asset
and Value Creation to CG/ITG Strategy



1. **Brooking Institute**
2. **Baruch Law Analysis of S&P 500 Companies**

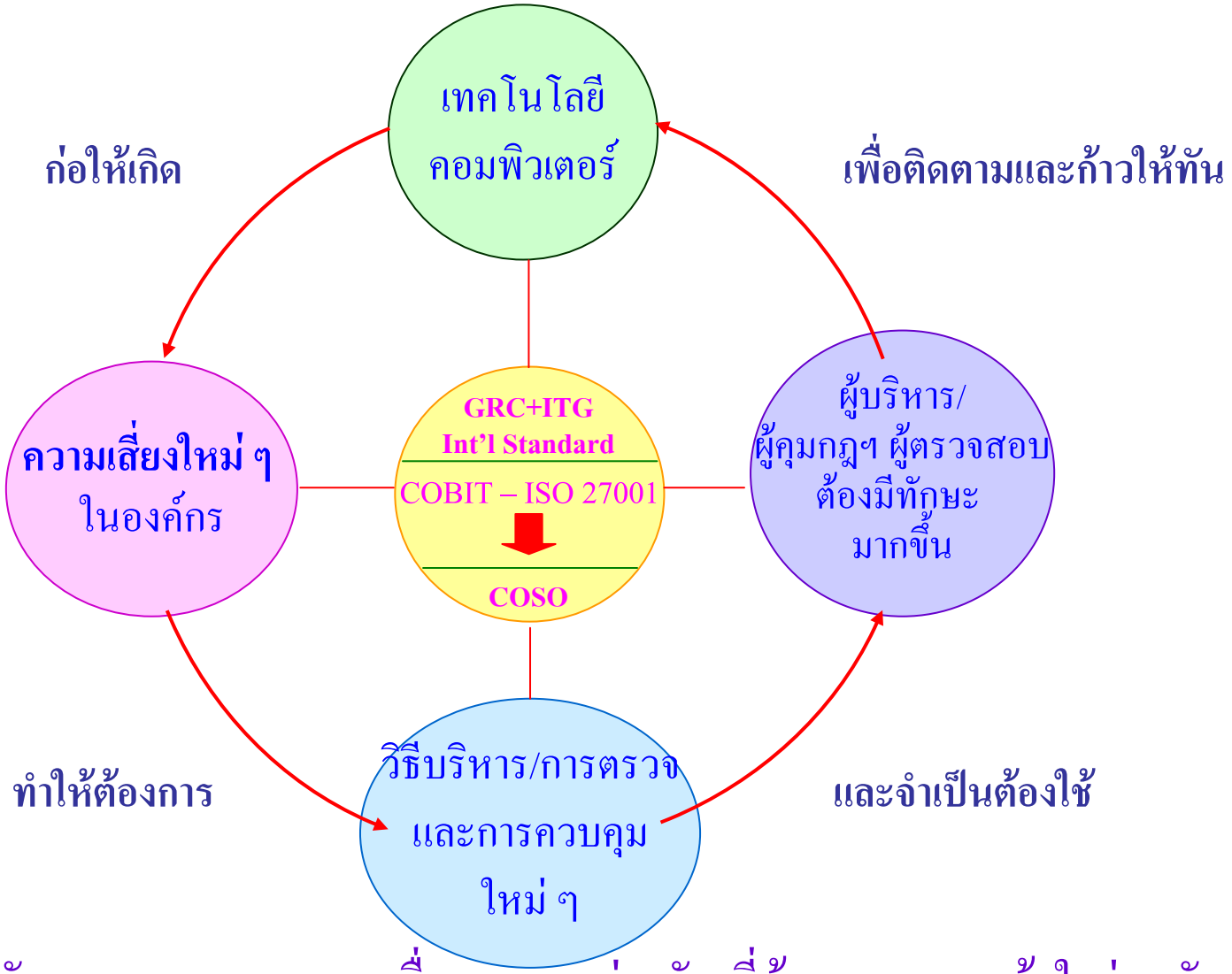
Source : Balance Scorecard Collaborative Inc. & Robert S. Kaplan

ส่วนของคอมพิวเตอร์ในระบบงานต่าง ๆ ของทุกองค์กร กับความเสี่ยง



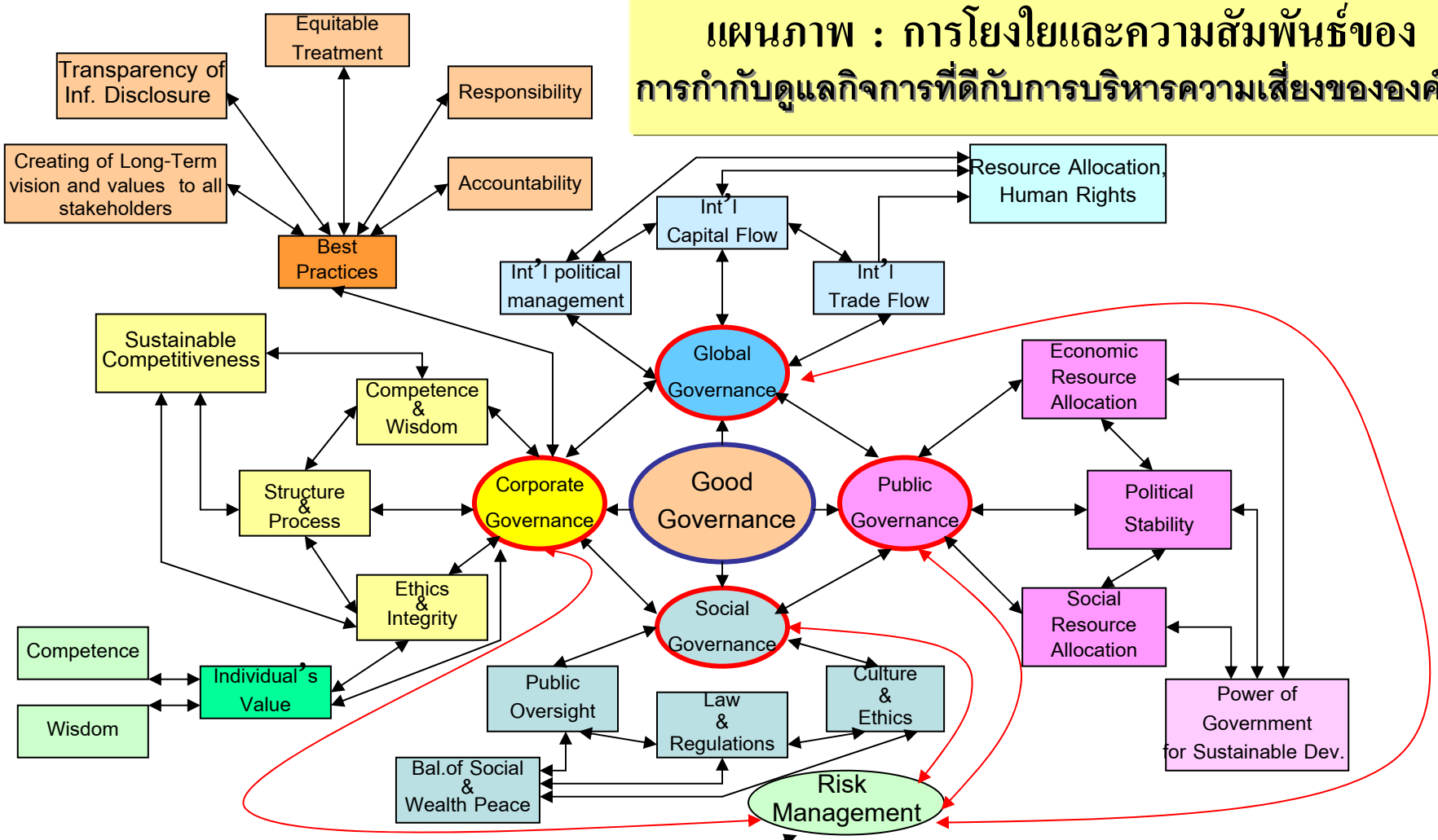
กรอบการกำกับดูแลกิจการที่ดี CG&ITG และการบริหารเพื่อสร้างคุณค่าเพิ่มกับ Soft Controls

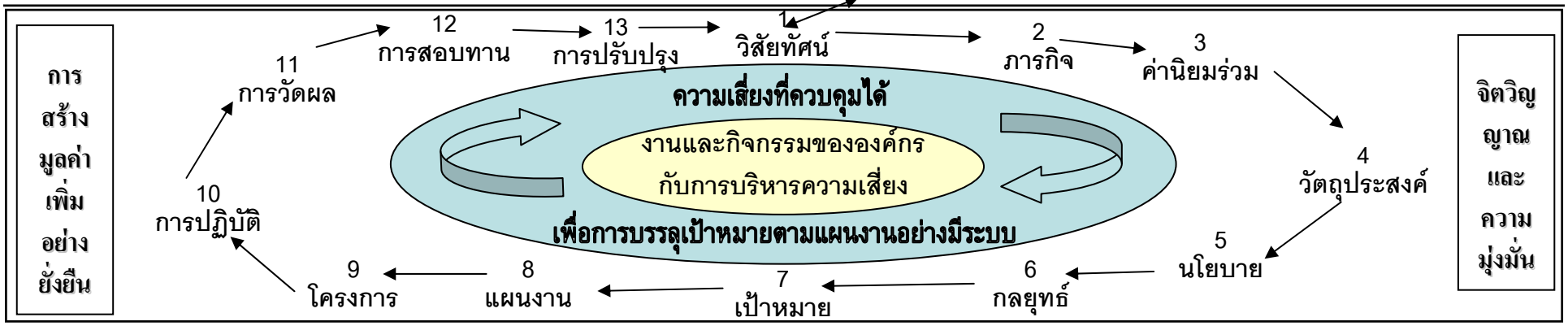
GRC:การหลอมรวมความเข้าใจในการบริหารมิติต่างๆ เพื่อการสร้างคุณค่าเพิ่มให้กับ Stakeholders



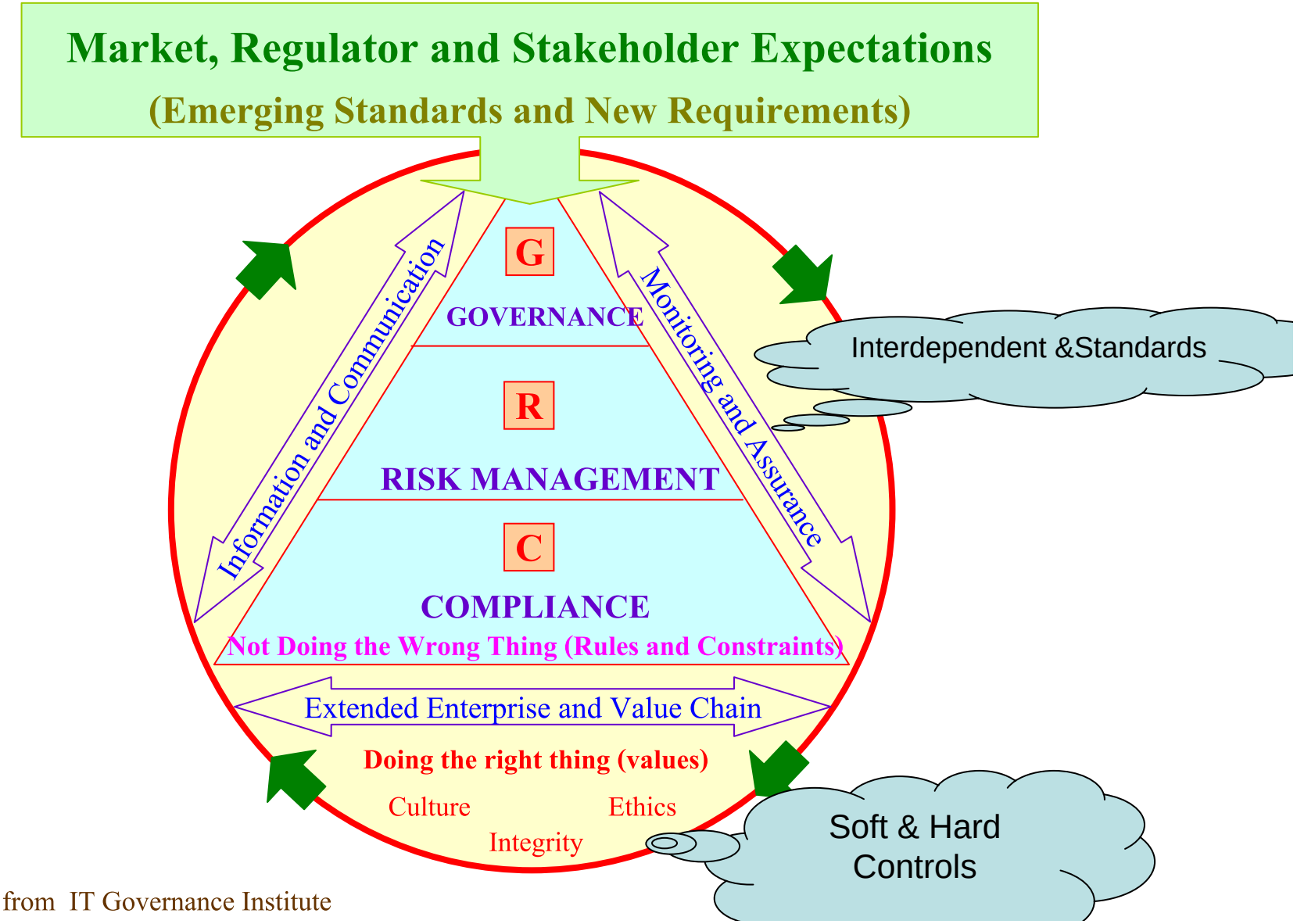
ภาพเดียวกัน : มุมมองและความเชื่ออาจแตกต่างกัน ที่ต้องการความเข้าใจร่วมกัน
ระหว่าง Regulators กับ Operators และ Stakeholders ต้องการเชื่อมโยงด้วยกฎเกณฑ์&มาตรฐาน

แผนภาพ : การโยงใยและความสัมพันธ์ของ
การกำกับดูแลกิจการที่ดีกับการบริหารความเสี่ยงขององค์กร





Managing Risk by GRC
From the Boardroom to the Mailroom



Source :Adopt from IT Governance Institute

ความสัมพันธ์ของ IT Governance และ Corporate Governance

CORPORATE GOVERNANCE

Traditionally includes:
Duties of Directors Leaders
Legislative/Fiduciary Compliance & Control
Ethics & Integrity
Business Operational Risks & Control
Financial Accounting & Reporting
Asset Management

Risks & Their Management

IT GOVERNANCE

Cover:

Enterprise/IT Objective
Legislative/Fiduciary Compliance&Control
IT Resources
Information
Knowledge Management System
Communications
Net Centric Technology
IT Operations, Risks & Control
e-Commerce/EDI/EFT
IT Asset Management

Risks & Their Management

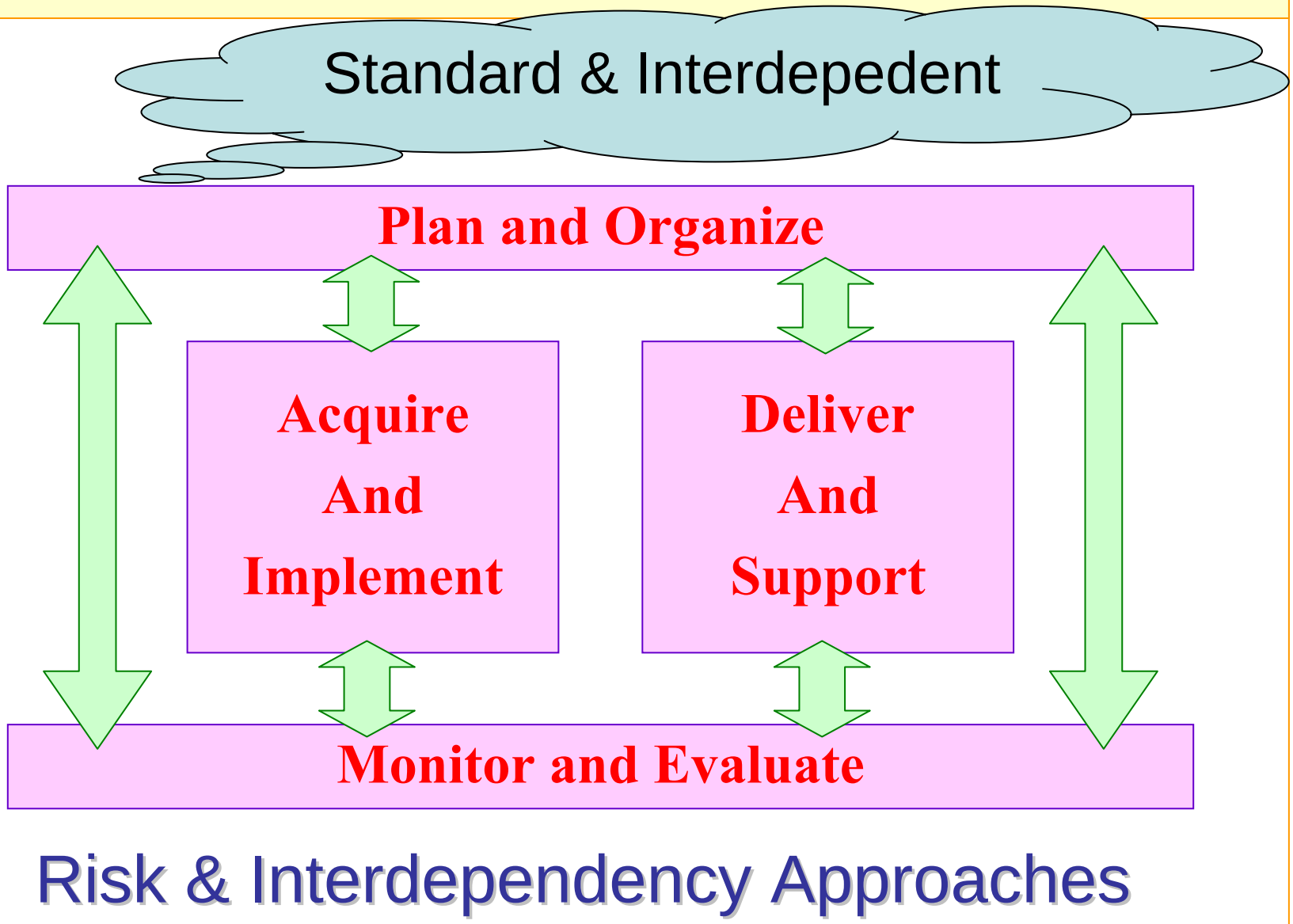
ENTERPRISE GOVERNANCE

CORPORATE GOVERNANCE	IT GOVERNANCE
Enterprise Goals Objectives	Enterprise Activities & Process
Innovations Research Capabilities	Knowledge & Intellectual Capital
Information & its Management	Human Resource Management
Customer Service & Relationships	Enterprise Communication Internal/External

Enterprise Governance focuses on the enterprise' s:
- Future
- Sustainability and potential
- Health

IT Governance focuses on IT' s:
- Alignment with enterprise objectives
- Use of IT Resources
- Management of IT related risks

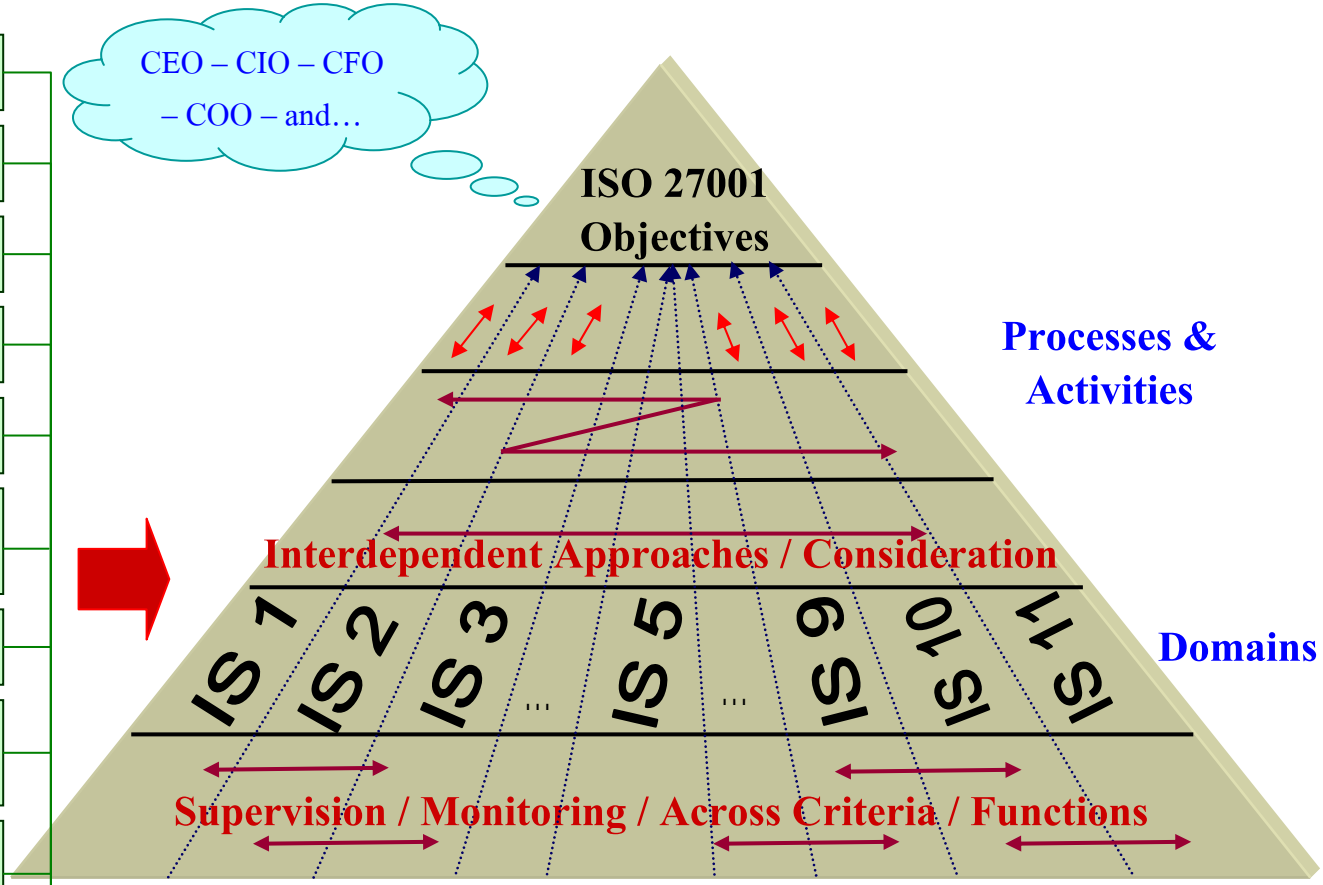
Understanding The Four Interrelated Domains of COBIT



Source : Adopt from IT Governance Institute

Information Security – International Standard (ISO 27001)

1. Security policy
2. Organization of information security
3. Asset management
4. Human resources security
5. Physical and environmental security
6. Communications and operations management
7. Access control
8. Information systems acquisition, development and maintenance
9. Information security incident management
10. ***Business continuity management***
11. Compliance



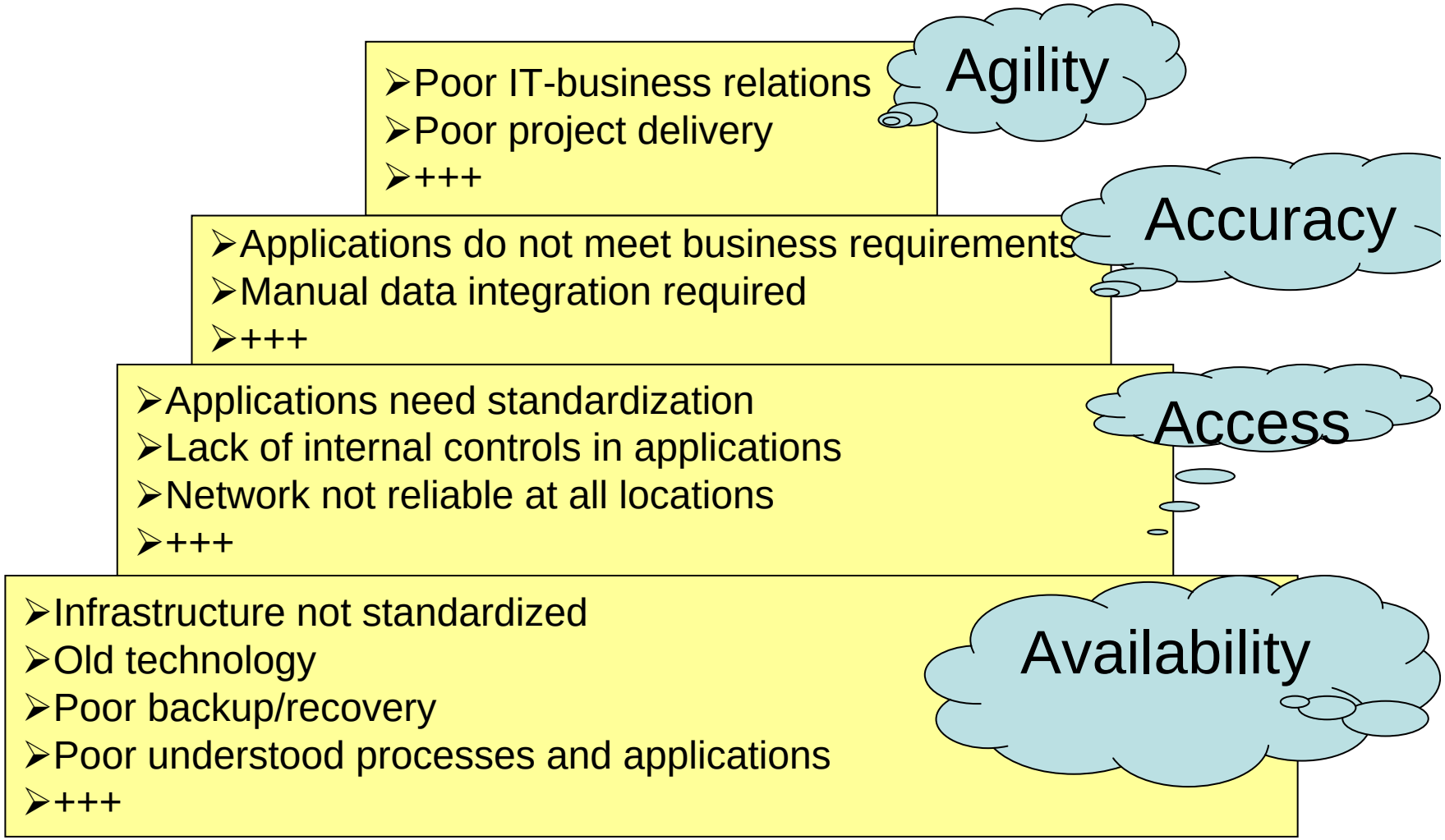
Consideration of common errors in identifying objectives & negative consequences

Identifying a means as an end.

Failing to consider each type & all types of objectives.

Failing to consider the relationships between objectives.

IT Risk factors aligned with their tiers in the pyramid



Source: Adopt from IT Risk –turning business threats into competitive advantage by George Westerman & Richard Hunter

IT Governance & GRC Framework

Thai E-Transaction Laws / Thai Laws

Rules & Regulations by Regulators

Office of The Auditor General

Thai OAG

Rules & Regulations by Regulators & International Standard

COBIT

ISO / IEC

ITIL

(IT Infrastructure Library)

Lessons Learned/

Other Standard

COSO

S-O-F-C

ส่วนประกอบของ Enterprise Risk Management (ERM)

1. สภาพแวดล้อมภายในองค์กร (Internal Environment)

Risk Management Philosophy – Risk Culture – Board of director – Integrity and Ethical Values – Committee to Competence – Management's Philosophy and Operation Style – Risk Appetite – Organization – Assignment of Authority and responsibility – Human Resource Policy

2. การกำหนดเป้าหมาย (Objective Setting)

Strategic Objective – Related Objectives – Selected Objectives – Risk Appetite – Risk Tolerance

3. การระบุเหตุการณ์ (Event Identification)

Events – Factors Influencing Strategy and Objectives – Methodologies and Techniques – Event Interdependencies – Event Categories – - Risk and Opportunities

4. การประเมินความเสี่ยง (Risk Assessment)

Inherent and Residual Risk – Likelihood and Impact – Methodologies and Techniques - Correlation

5. การตอบสนองความเสี่ยง (Risk Response)

Identify Risk Response – Evaluate Possible Risk Responses – Select Risk Responses – Portfolio View

6. กิจกรรมควบคุม (Control Activities)

Integration with risk response – Types of Control Activities – General Controls – Application Controls – Entity Specific

7. ระบบสารสนเทศและการติดต่อสื่อสาร (Information and Communication)

Information – Strategic and Integrated Systems - Communication

8. การติดตามและประเมินผล (Monitoring)

Separate Evaluation – Ongoing Evaluation

Balancing Strategies on Balance Scorecard & S-O-F-C

(People – Process Technology & Other IT Resources)

IT Governance & Compliance Framework/GRC

Level 0 – Laws & Regulations

Level 1 – Internal Control Framework – COSO / Enterprise Risk Mgmt.

Level 2 – Internal Control Framework – IT Governance/ISO

(Enterprise Wide-What to do/ Check list)

Level 3 – IT Best Practices, Standard and Lessons Learned

(How to do…Lesson learned …What can go wrong ?)

Balancing Strategies on Balance Scorecard & S-O-F-C

(People – Process Technology & Other IT Resources)

Self-assessment focuses on objectives, risks and controls Management :

- **Objectives**

  If objectives are not clear,…What can go wrong?

  What is/are consequences to risks & controls & ERM?

  are things and organization wants to accomplish.

- **Risks**

  What can go wrong & it consequences …if we fail to identify risks from the causes.?

  are things that might prevent accomplishing and objective.

- **Control**

  Then…What is/are the end results of **ERM to Objectives & Business?**

  are things that help meet an objective by managing that risk.

Risk-Control-Internal Auditing

Risk Contrd

✗ ✓ Wastes

✓ ✗ Unacceptable

- **เป้าประสงค์** ที่ปราศจาก **การควบคุม** ทำให้ยากที่จะบรรลุ**เป้าหมาย**ได้
- **การควบคุม** โดยปราศจาก **ความเสี่ยง** คือความสูญเสียด้านทรัพยากร
- **ความเสี่ยง** ที่ปราศจาก **การควบคุม** เป็นเรื่องที่ยอมรับไม่ได้
- การตรวจสอบภายใน ที่ไม่ครอบคลุมทั้ง **ความเสี่ยง** และ**การควบคุม**

  เป็นเรื่องที่เสียเวลา = รายงานสิ่งผิดปกติ Abnormality Report
- **"Risk Based Auditing"**

องค์ประกอบสำคัญของการควบคุมภายใน

การควบคุมภายในมี 5 องค์ประกอบ

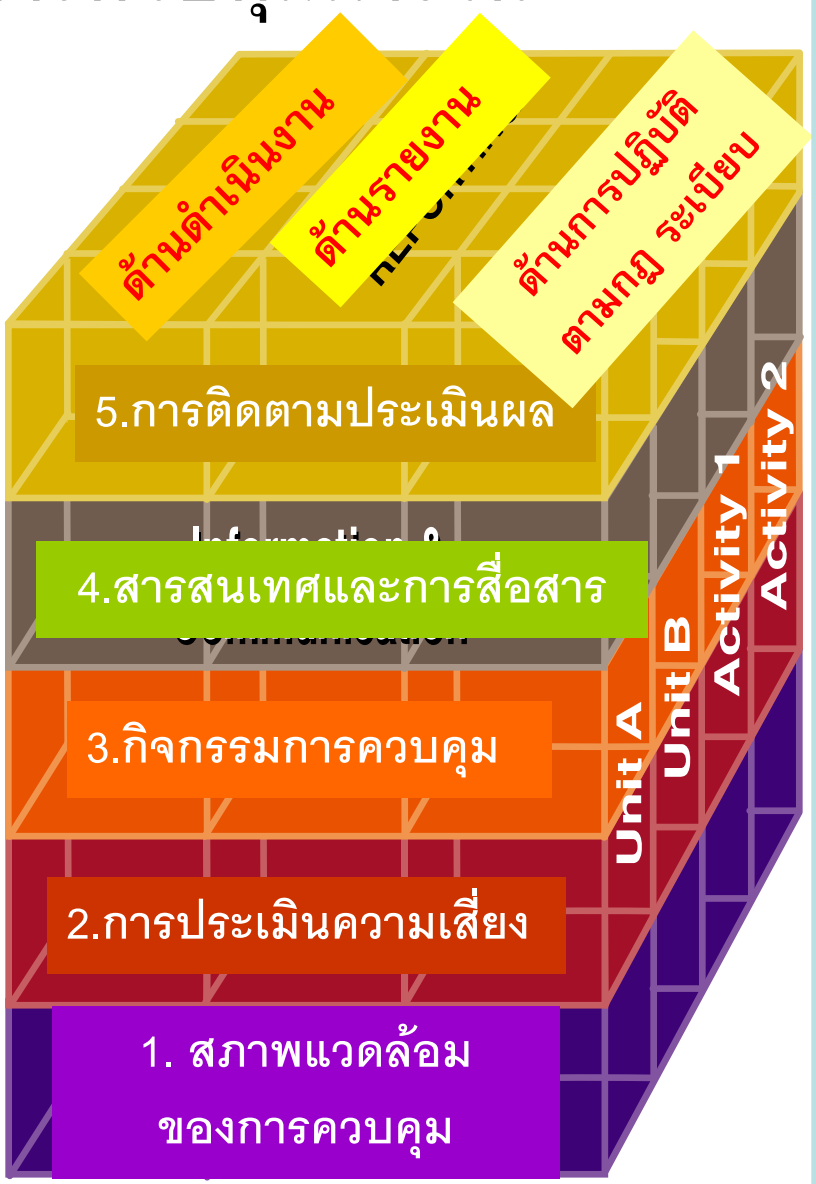
องค์ประกอบที่ 1: สภาพแวดล้อมการควบคุม
(Control environment)

องค์ประกอบที่ 2: การประเมินความเสี่ยง
(Risk assessment)

องค์ประกอบที่ 3: กิจกรรมการควบคุม
(Control activities)

องค์ประกอบที่ 4: สารสนเทศและการสื่อสาร
(Information and communication)

องค์ประกอบที่ 5: การติดตามประเมินผล
(Monitoring activities)



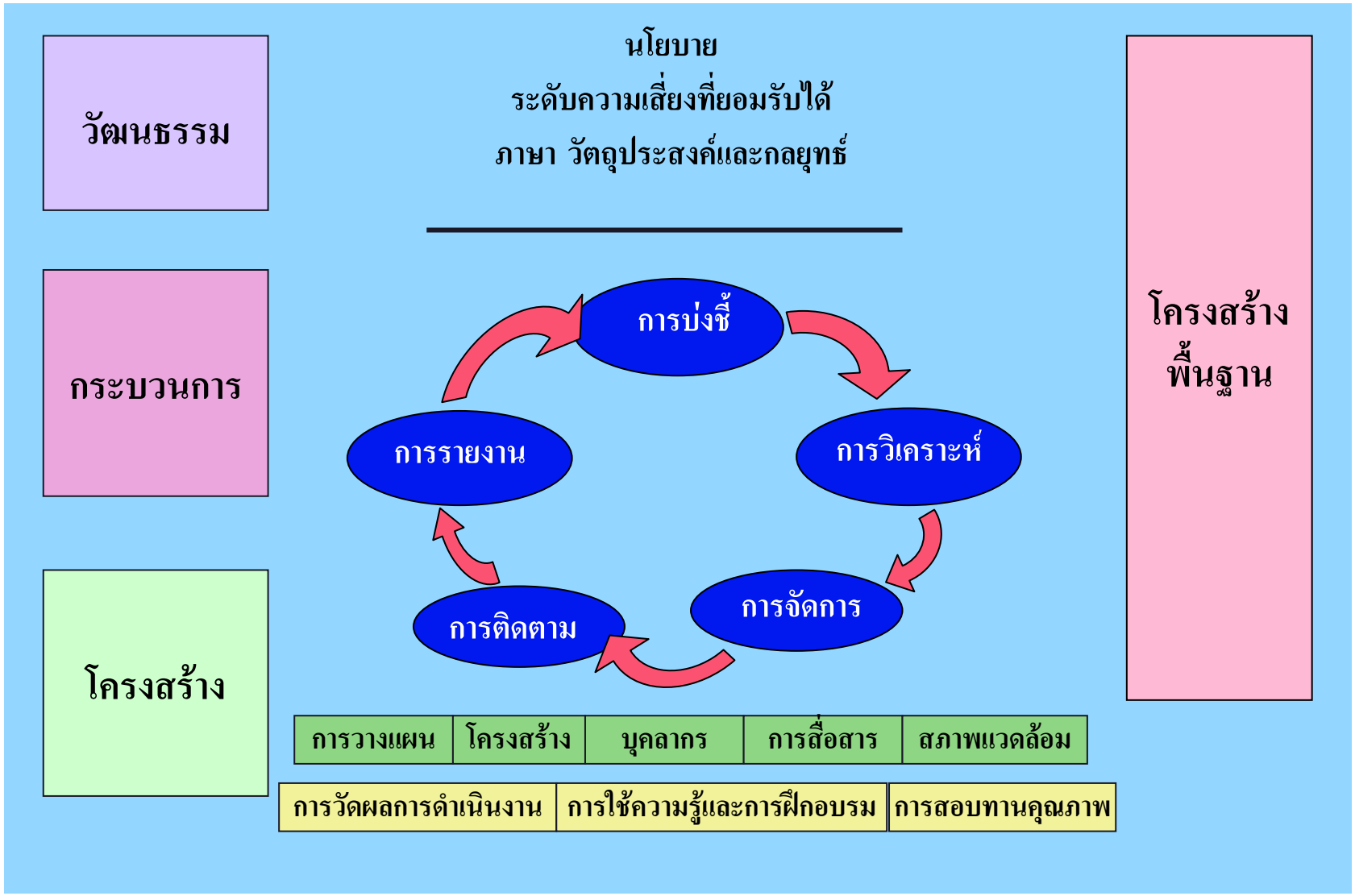
Relationship between COSO 1 and COSO 2

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

COSO 1 "Internal Control – Integrated Framework"

COSO 2 "Enterprise Risk Management – Integrated Framework"

กรอบการบริหารความเสี่ยงของทุกองค์กร



กรอบการบริหารความเสี่ยง

กรอบการบริหารความเสี่ยง

วัฒนธรรมองค์กร

- วัตถุประสงค์
- นโยบาย
- กลยุทธ์
- ความเสี่ยงที่ยอมรับได้ (Risk appetite)

ปัจจัยพื้นฐาน

- วิธีการ
- ระบบ
- เครื่องมือ
- ข้อมูลสำหรับผู้บริหาร

โครงสร้างการบริหารความเสี่ยง

- หน่วยงาน/คณะกรรมการ
- สายการรายงาน
- บทบาท/ความรับผิดชอบ
- ทักษะ/บุคลากร

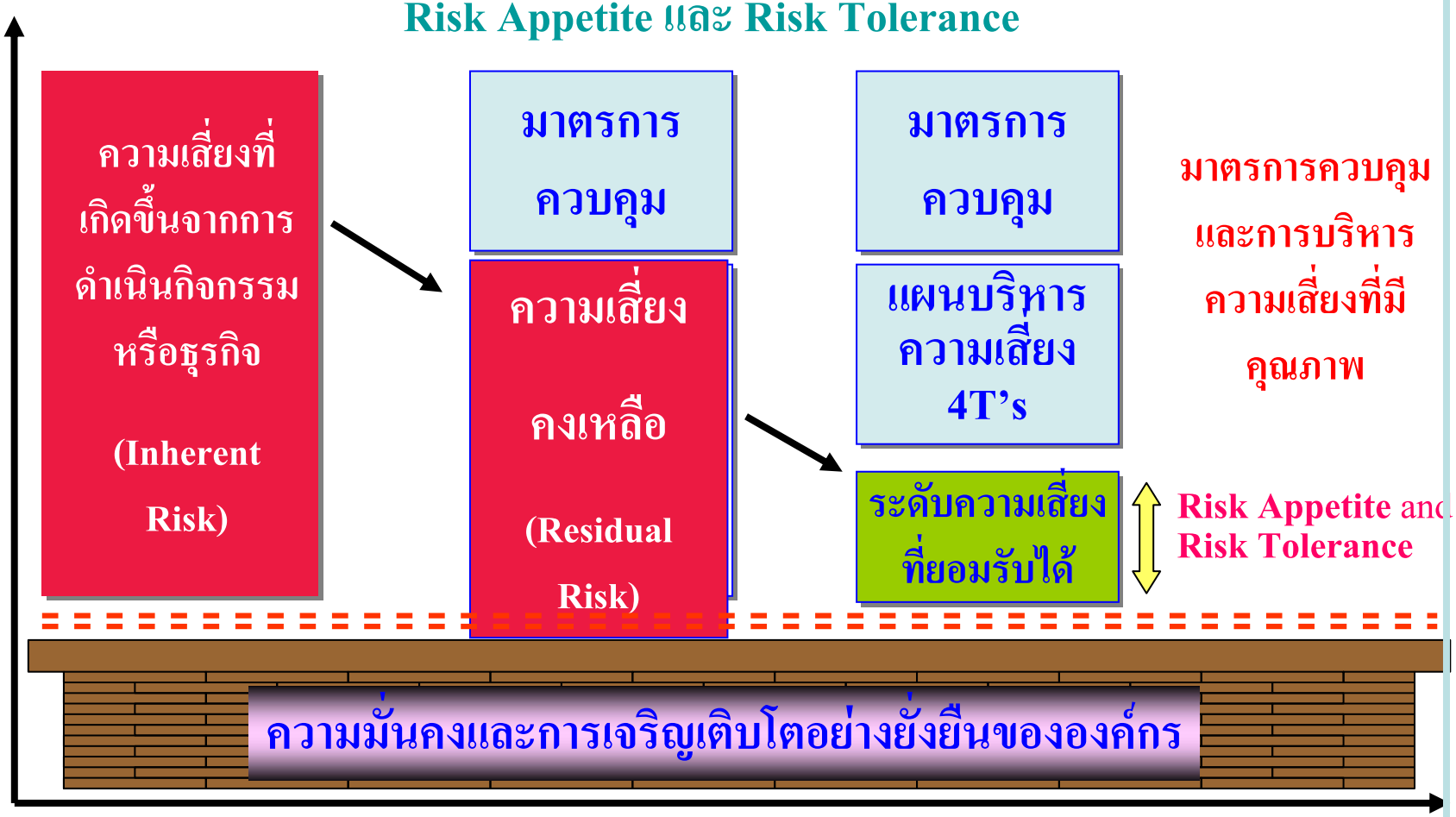
กระบวนการ

- การบ่งชี้ความเสี่ยง/การวัดความเสี่ยง
- การกำหนดขอบเขต
- การติดตามความเสี่ยง
- การระบุปัญหา (Issue escalation)

การสำรวจความเสี่ยงทั่วทั้งองค์กร

แผนการบริหารความเสี่ยง และ ระดับความเสี่ยงที่ยอมรับได้-

Risk Appetite และ Risk Tolerance



ความเสี่ยงวัดได้อย่างไร

Level of Risk

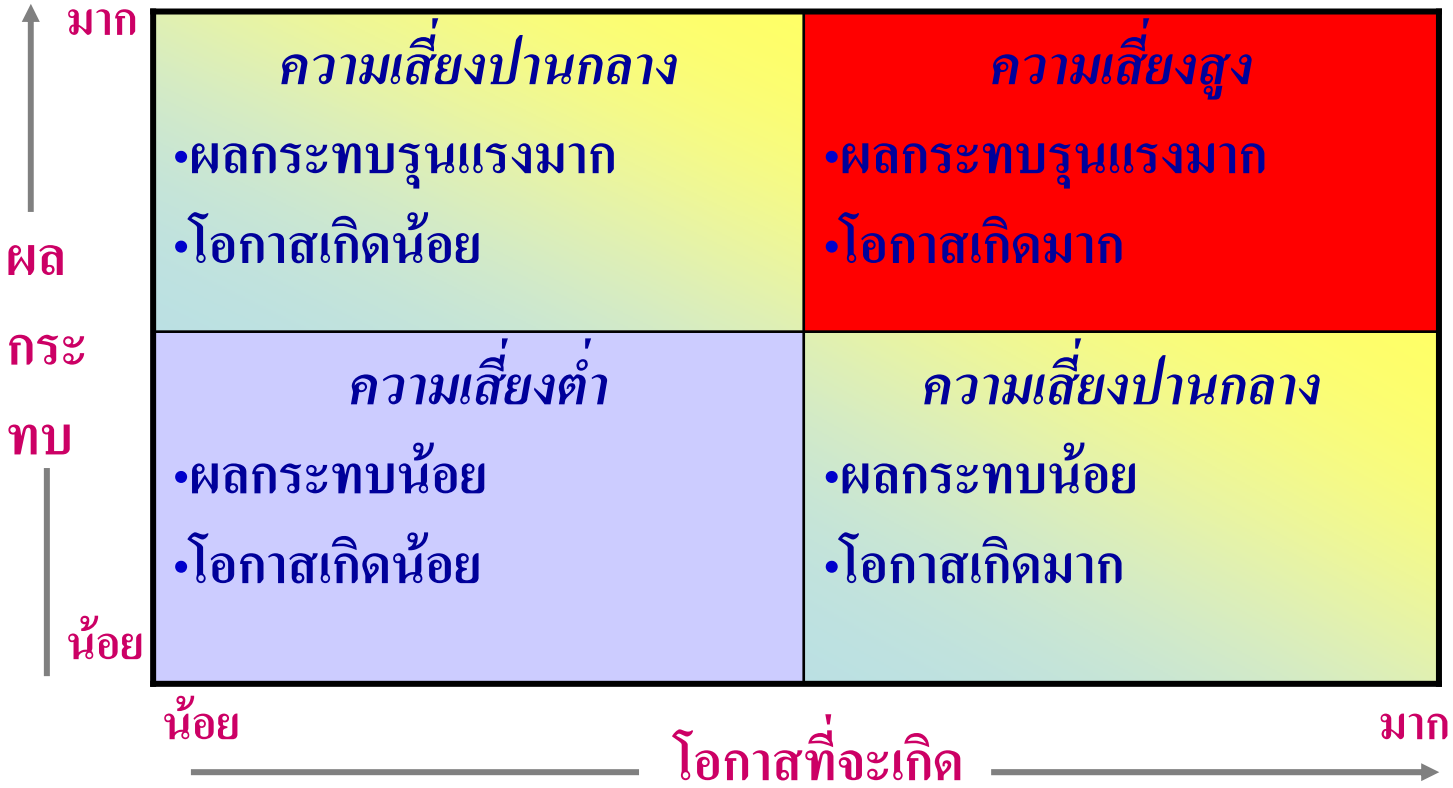
มาก

ความรุนแรงของผลกระทบ	โอกาสที่จะเกิดขึ้น				
	1-เกิดน้อยมาก	2-เกิดขึ้นน้อย	3-เกิดขึ้นบ้าง	4-เกิดบ่อยครั้ง	5-เกิดประจำ
5 - รุนแรงมาก	H	E	E	E	E
4 - รุนแรง	H	H	E	E	E
3 - ปานกลาง	M	M	H	H	E
2 - น้อย	L	L	M	H	H
1 - น้อยมาก	L	L	L	M	H

น้อย

มาก

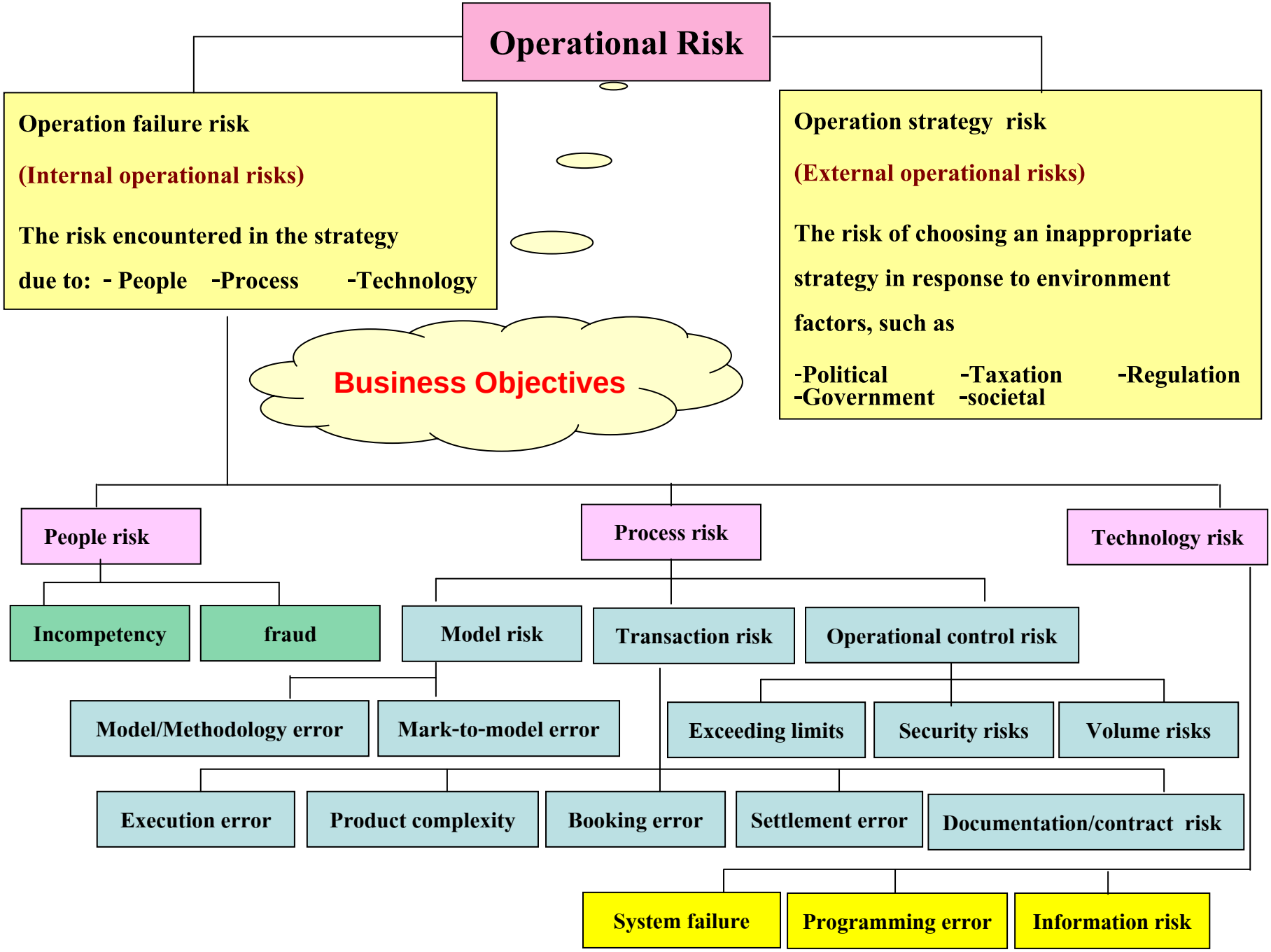
แผนภูมิความเสี่ยง (Risk Map)



กลยุทธ์ในการบริหารความเสี่ยง

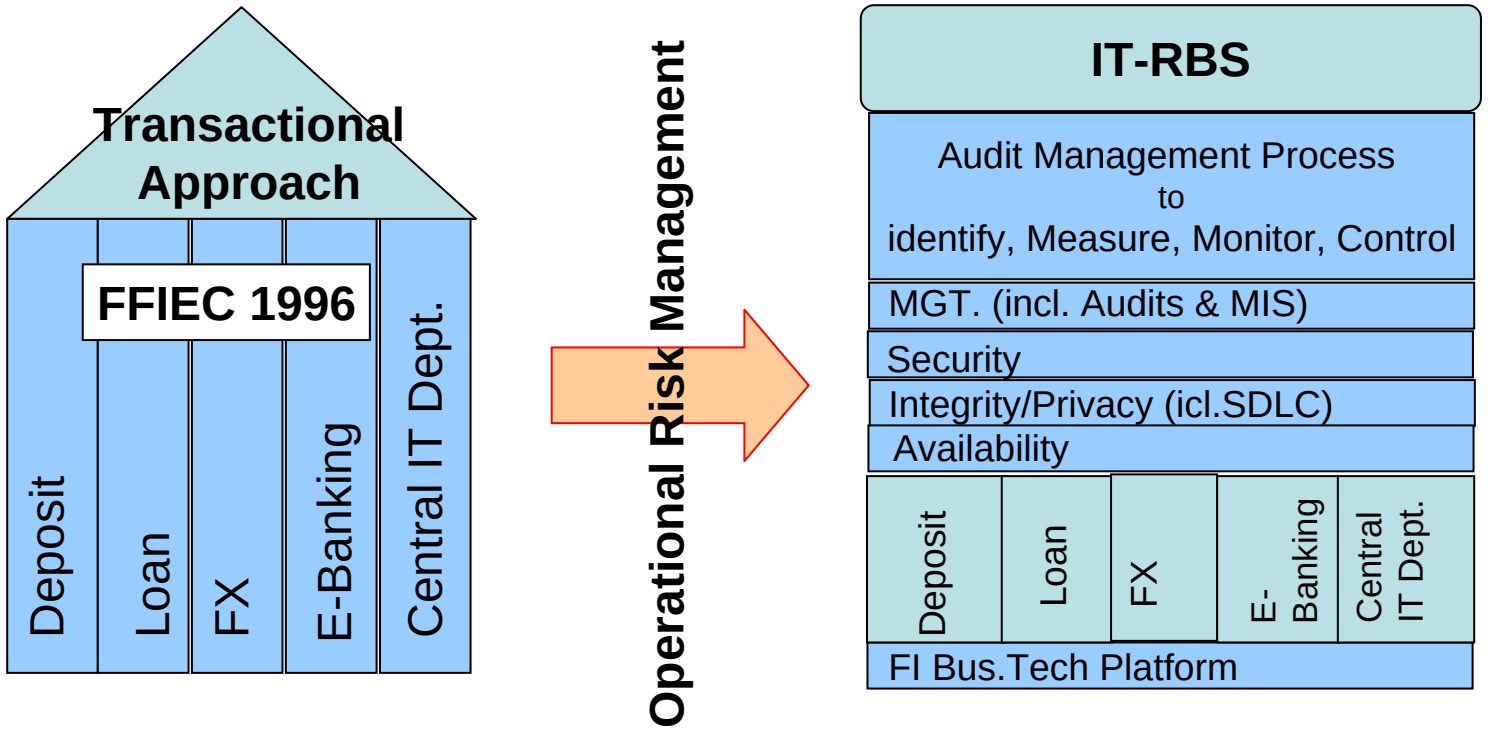
1. การยอมรับ (Take)	2. การลด / บรรเทา (Treat)	3. การโอน / แบ่ง (Transfer)	4. การหยุด / หลีกเลี่ยง (Terminate)
• ยอมรับความเสี่ยง • กำหนดงบประมาณรองรับเหตุการณ์ความสูญเสีย • ดูแลติดตามความเสี่ยงเป็นประจำ	• กำหนดนโยบายและวิธีการปฏิบัติงานใหม่ • การเพิ่มการควบคุม • การวางระบบงานใหม่ • การฝึกอบรมเพิ่มทักษะพนักงาน • การปรับปรุงกระบวนการปฏิบัติงาน	• ทำประกัน • การร่วมทุนหรือหาพันธมิตร • จ้างผู้ให้บริการภายนอกดำเนินการ • การกระจายการลงทุน	• หยุดกิจกรรมธุรกิจ • ลดสัดส่วนการลงทุน • ปรับเปลี่ยนเป้าหมายทางธุรกิจ • ออกแบบปรับปรุงกระบวนการหรือระบบ • ลดขนาดการลงทุน

ติดตาม ตรวจสอบอย่างสม่ำเสมอ


Operational Risk
Operation failure risk
(Internal operational risks)
The risk encountered in the strategy
due to: - People -Process -Technology
Operation strategy risk
(External operational risks)
The risk of choosing an inappropriate
strategy in response to environment
factors, such as
-Political -Taxation -Regulation
-Government -societal
Business Objectives
People risk
Process risk
Technology risk
Incompetency
fraud
Model risk
Transaction risk
Operational control risk
Model/Methodology error
Mark-to-model error
Exceeding limits
Security risks
Volume risks
Execution error
Product complexity
Booking error
Settlement error
Documentation/contract risk
System failure
Programming error
Information risk

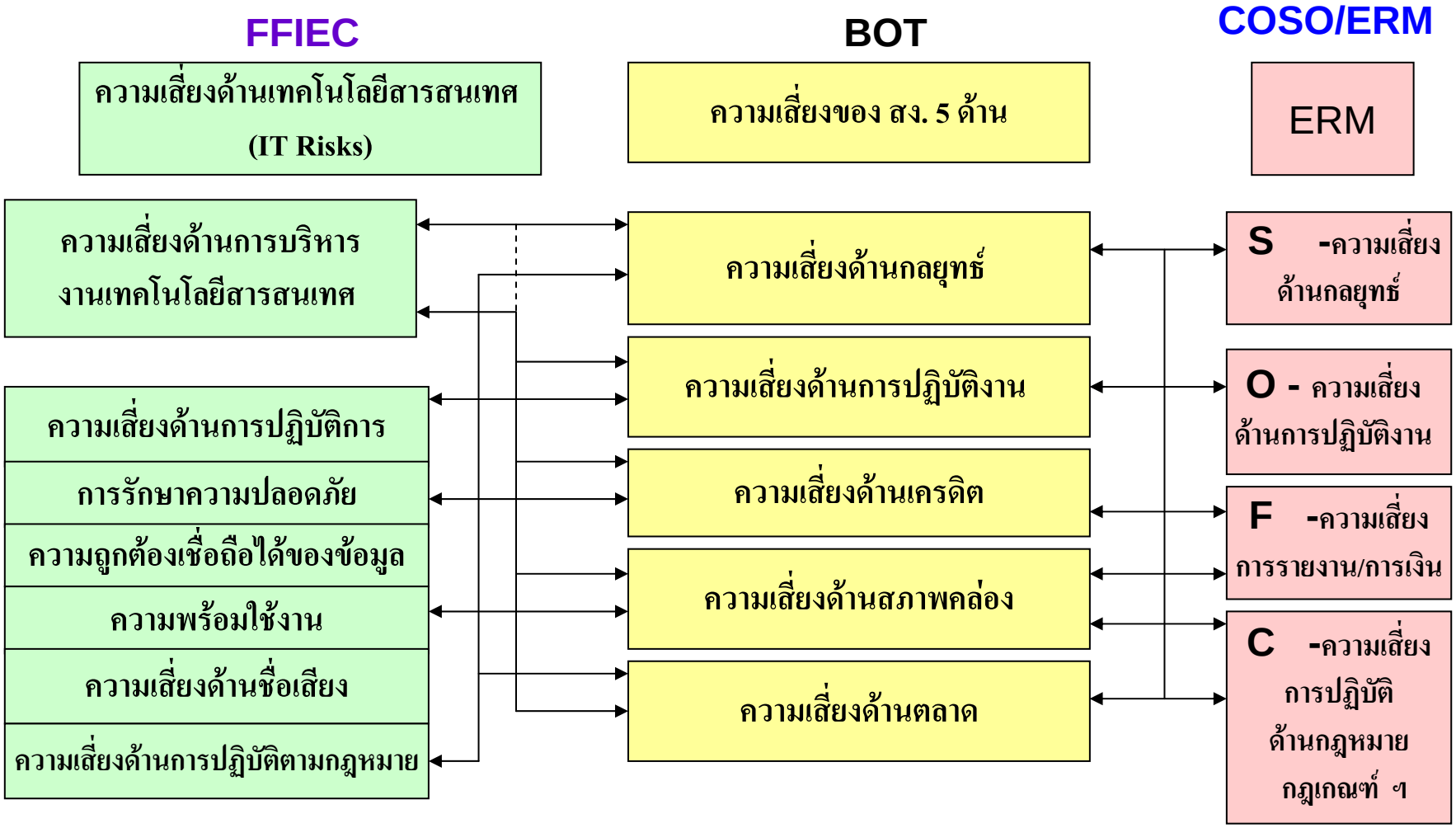
เปรียบเทียบการตรวจสอบแนวทางเดิมกับแนวทางใหม่ กับ มุมมองของ ITG&GRC เพื่อสร้างคุณค่าเพิ่มในการตรวจสอบ ให้กับ Stakeholders

SR98-9 IT Risks



ที่มา : ธนาคารแห่งประเทศไทย

IT Risks VS Risk-based Audit and Supervision/Audit Approaches for IT Governance/GRC



ที่มา : ปรับปรุง/ดัดแปลง จากธนาคารแห่งประเทศไทย

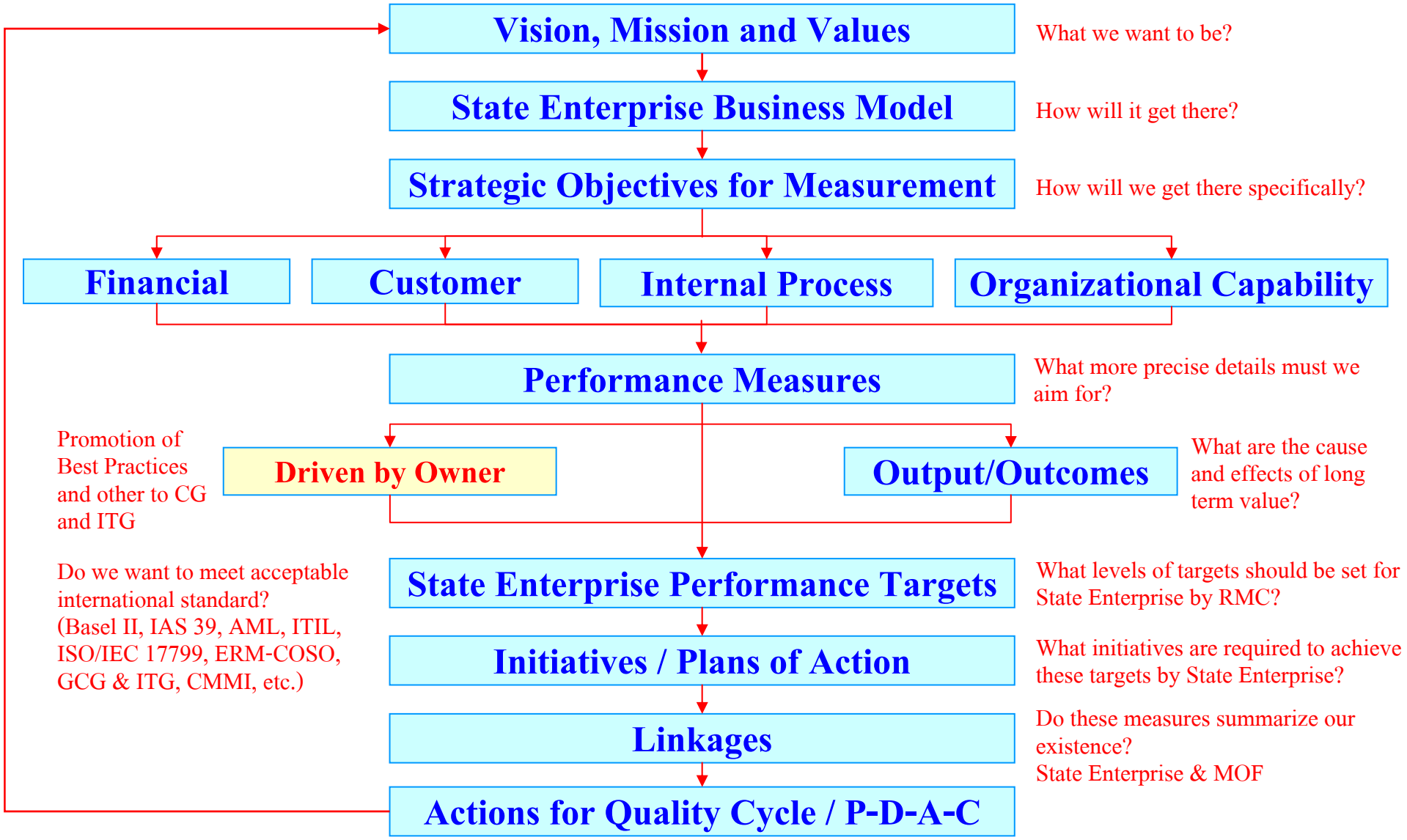
Changing the Internal Auditor's Paradigm & CG/ITG/GRC & Monitoring

Characteristic	Old Paradigm	New Paradigm
Internal Audit Focus	Internal Control	Business Risk
Internal Audit Response	Reactive, after-the-fact, discontinuous, observers of strategic planning initiatives	Proactive real-time, continuous monitoring, participants in strategic plans
Risk Assessment	Risk Factors	Scenario Planning
Internal Audit Tests	Important Controls	Important Risks
Internal Audit Methods	Emphasis on the Completeness of Detail Controls Testing	Emphasis on the Significance of Broad Business Risk Covered
	Internal Control: * Strengthened * Cost-Benefit * Efficient/Effective	Risk Management : * Avoid/Diversify Risk * Share/Transfer Risk * Control/Accept Risk
Internal Audit Reports	Addressing the Functional Controls	Addressing the Process Risk
Internal Audit Role in the Organization	Independent Appraisal Functional	Integrated Risk Management and corporate Governance

ที่มา : IIA Institute

Translating Vision and Strategy to

State Enterprise Performance Measurement – Drivers & Output/Outcome



ที่มา : ดัดแปลงบางส่วนจาก Hewitt Institute

สรุป : ข้อสังเกต สำหรับการบริหารความเสี่ยง เพื่อให้มีการบริหารความเสี่ยงทั่วทั้งองค์กรที่ดี

กลยุทธ์

- นโยบายบริหารความเสี่ยง
- การฝึกอบรมบริหารความเสี่ยง
- การประชาสัมพันธ์เรื่องการบริหารความเสี่ยง

- การกำหนด Risk appetite และ Risk tolerance
- การให้ความรู้เกี่ยวกับการบริหารความเสี่ยงอย่างต่อเนื่อง
- สื่อสารการบริหารความเสี่ยงต่อผู้มีส่วนได้เสียภายนอกเพื่อสร้างความเชื่อมั่นต่อองค์กร
- นำการบริหารความเสี่ยงรวมกับกระบวนการในการประเมินผลการดำเนินงาน (KPI)

ปัจจัยพื้นฐาน

- เก็บข้อมูลความเสี่ยงโดยใช้โปรแกรมพื้นฐาน เช่น Excel หรือ Word เป็นต้น
- มีการบันทึกข้อมูลความเสี่ยงเข้าในระบบ ขององค์กร และ Intranet เพื่อให้รับรู้ทั่วทั้งองค์กร

ความสอดคล้องกัน

โครงสร้างองค์กร

- โครงสร้างการบริหารความเสี่ยง
  - คณะอนุกรรมการพิจารณาแผนบริหารความเสี่ยง
  - คณะกรรมการบริหารความเสี่ยง
  - คณะกรรมการบริหารความเสี่ยงประจำสายงาน
  - ฝ่ายบริหารความเสี่ยง
  - ผู้ประสานงานความเสี่ยงสายงาน

- สอบทานโครงสร้างการบริหารความเสี่ยงรวมทั้งบทบาทและความรับผิดชอบ

กระบวนการ

- ประชุมเชิงปฏิบัติระดับองค์กร
- ติดตามผลการดำเนินงานตามแผนปฏิบัติการ
- รายงานความเสี่ยงต่อคณะกรรมการบริหารความเสี่ยง
- จัดทำคู่มือบริหารความเสี่ยง

- นำกระบวนการบริหารความเสี่ยงไปปฏิบัติอย่างต่อเนื่อง
- ทบทวนและพัฒนากรอบการบริหารความเสี่ยง
- สนับสนุนให้เกิดกระบวนการตรวจสอบภายในเชิงความเสี่ยง (Risk based internal audit- RBIA)

- ศึกษาการจัดทำระบบ Early Warning Indicator เช่น การทำ Risk Dashboard เป็นต้น
- ศึกษาการนำเอาระบบ Software มาใช้ในการบริหารความเสี่ยง

Summary of ERM Understanding & Identifying Risks / Controls sample

: Distinguish between the cause and effect of a risk

: It is easier to mange the cause with internal controls than to manage the effect of a risk

: For instance, **"being out of compliance with regulations."**

What is/are the effects or the causes?

- Penalties and/or
- Imprisonment and/or
- Bad reputation and/or
- Publicity for noncompliance and/or
- Cost increased and/or
- revenue decreased and/or
- Etc.

- lack knowledge of the regulations
- fraud,
- in competency,
- do not consider the laws to be important,
- etc.

How to manage risks & controls?

4 T's techniques

source : Adopt from The Institute of Internal Auditor

Q&A

การกำหนด Statement Of Direction หรือ **ทิศทางการบริหาร ของ ผู้กำกับกฎเกณฑ์** ของ บริษัทในตลาดหลักทรัพย์&บริษัททั่วไป