หลักสูตรผู้บริหารเทคโนโลยีสารสนเทศระดับสูง

CIO (Chief Information Officer) รุ่นที่ 26

การบริหารความเสี่ยงด้านไอซีที

ICT Risk Management

วันที่ 2 เมษายน 2558

ณ ห้องกมลมาส ชั้น 6 โรงแรมเดอะสุโกศล

++ Integrated Risk Management

โดย

นาย เมธา สุวรรณสาร

CGEIT; CRISC; CRMA; CIA; CPA

www.itgthailand.com

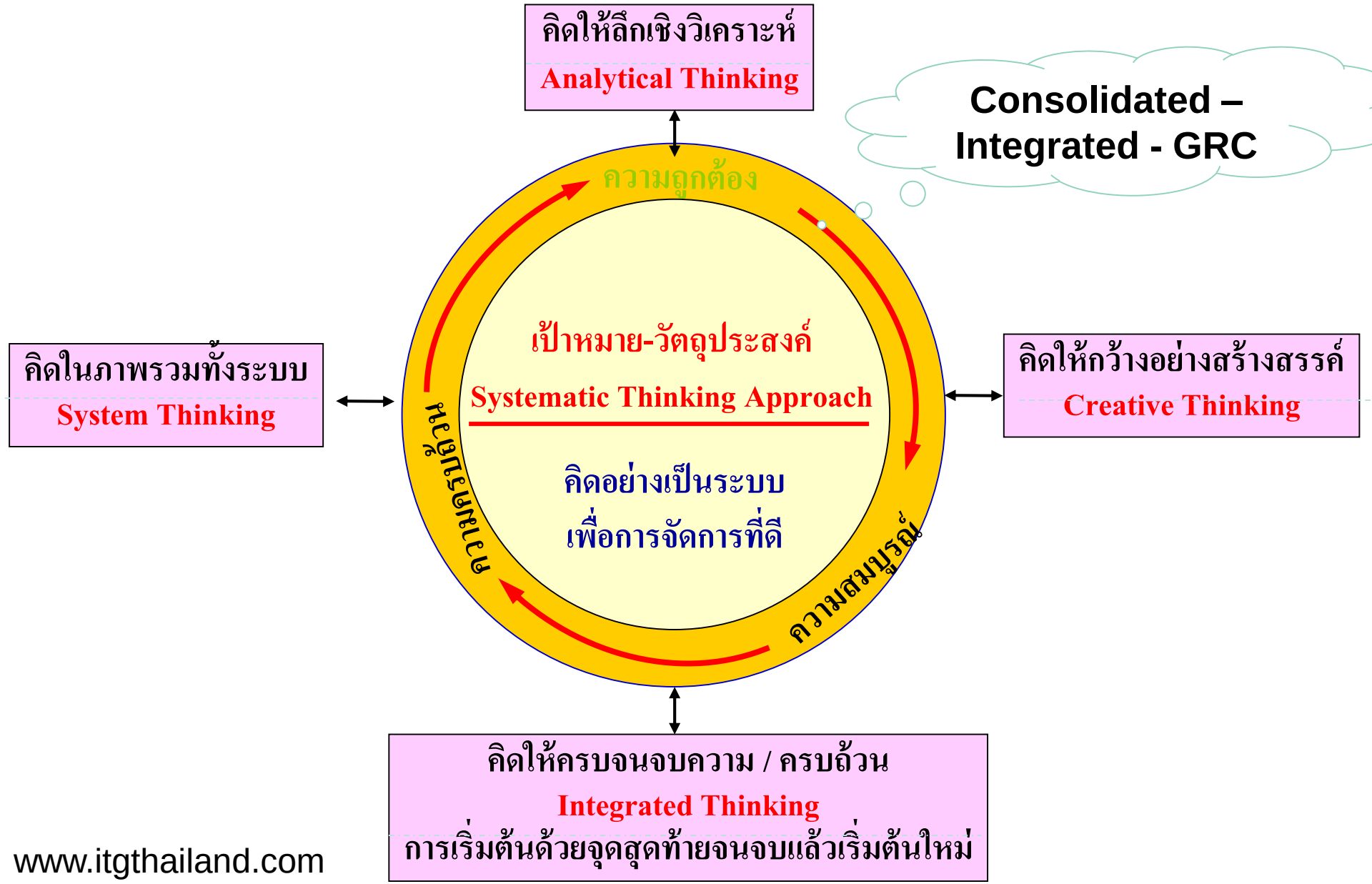
หัวข้อที่จะแลกเปลี่ยนกันในหัวข้อ “ ICT Risk Management ”

1.ข้อมูลและสารสนเทศ เป็นทรัพย์สินที่มีมูลค่ายิ่ง ของทุกองค์กร กับการบริหาร ICT ยุคปัจจุบัน– ฟังไป คิดไป
2.ความเข้าใจในบริบทขององค์กร กับ การสร้างคุณค่าเพิ่ม กับ ธรรมภิบาล และ IT Governance คืออะไร?
3.CIO & CEO กับ แรงขับเคลื่อนใหม่ จากสภาพแวดล้อม และแนวความคิดใหม่ สู่ โลกยุคใหม่ของการ กำกับ&การบริหาร
4.การบริหารแบบ Silo-Based กับ Integrated Management ในมุมมองต่างๆ
5.องค์ประกอบของการกำกับกิจการ และการบริหารที่ดี
6. ท่านอยู่ในระดับใด ของกระบวนการบริหารและการจัดการที่ดี กับ ธรรมาภิบาล
7.กระบวนการธรรมภิบาล กับ วิวัฒนาการ และความหมายที่แท้จริง ที่ควรทำความเข้าใจ ให้ตรงกัน
8. COBIT5 …Best Practice and / or Standard และ ผลลัพธ์ ที่เกิดขึ้น
9. IT Governance กับ การก้าวสู่ COBIT5 & Integrated Single Framework
10.ดุลยภาพ ของ การสร้างคุณค่าเพิ่ม กับ Governance & Stakeholders
11.การบริหารความเสี่ยงแบบบูรณาการ กับ การบริหารทรัพยากร แบะ Balanced Scorecards
12.หลักการที่ว่า “ หากการควบคุมไม่ได้ ก็ กำกับและบริหารไม่ได้ “
13.ความสัมพันธ์กันระหว่าง IT & Business ที่แยกกันไม่ได้ กับ CIO & CEO +++
14.คำถามที่สำคัญบางประการ ในมุมมองของ Govenance และ คณะกรรมการ ผู้บริหาร
15.สรุป และ ทบทวน เราได้อะไรจากเรื่อง “ ICT Risk Management “-> Business Impact
16. เราควรดำเนินการอย่างไรต่อไป
16.ถาม-ตอบ

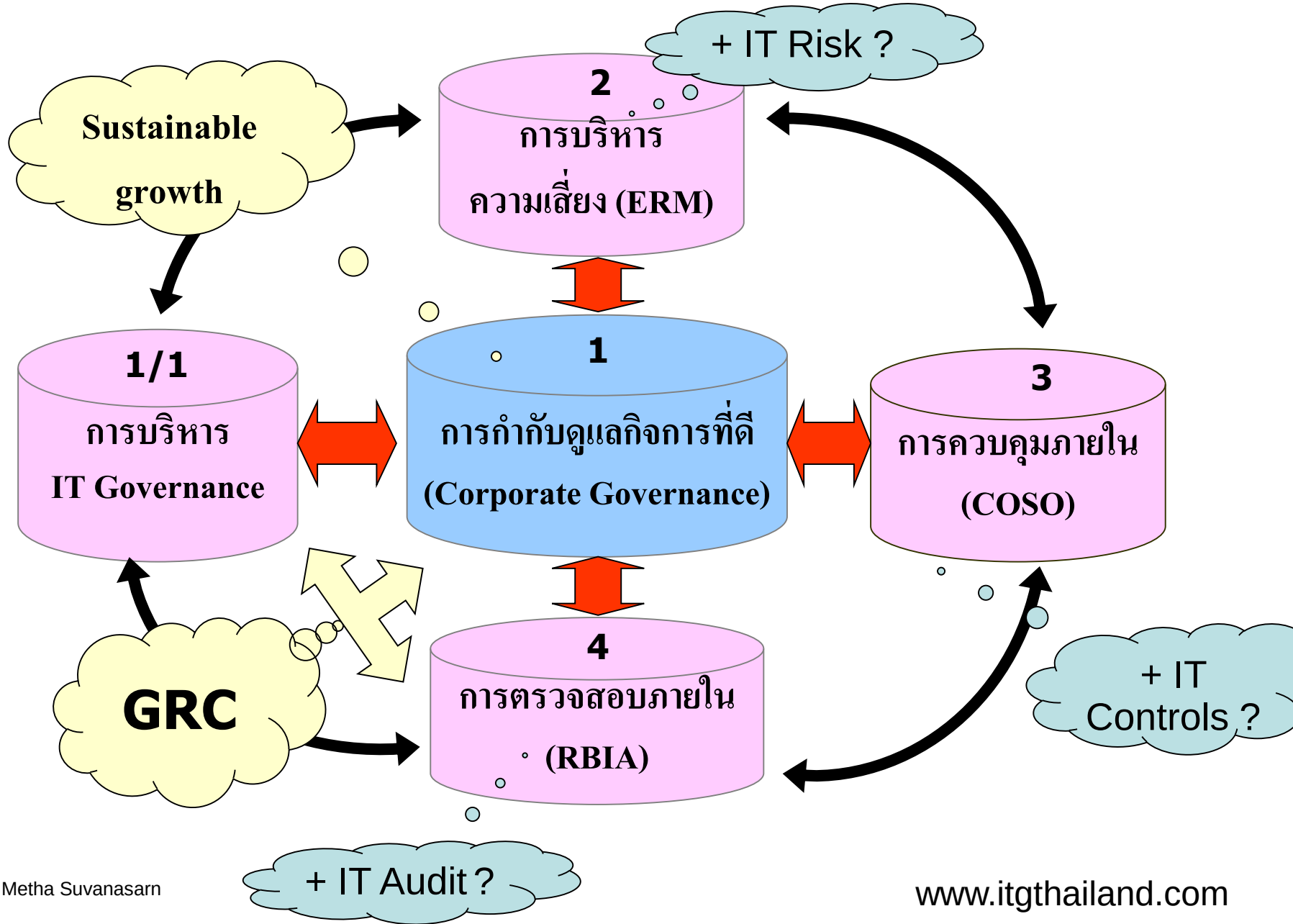
G/COBIT 5 / -> Governance-> GEIT- Governance of Enterprise

Source: www.itgthailand.com

การบริหารความเสี่ยง กับ ความคิดอย่างเป็นระบบ / IT & Non IT เพื่อการจัดการที่ดี



Value Creation for Effectiveness & Efficiency of Operations

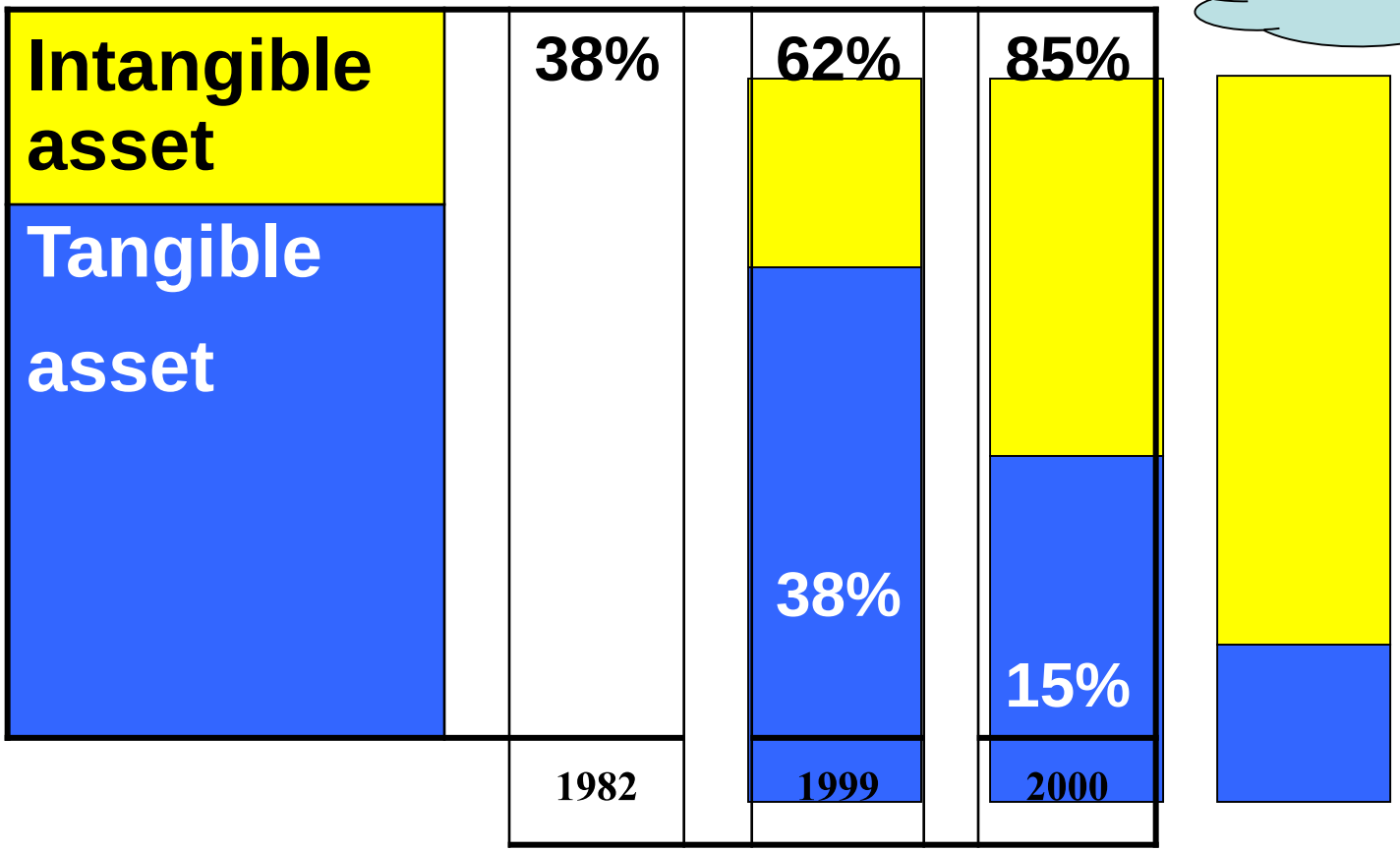


Source : Metha Suvanasarn

Tangible to Intangible asset

and Value Creation / GRC & ITG Perspective

ทบทวน บางมุมมองหากมีเวลา พอนะครับ



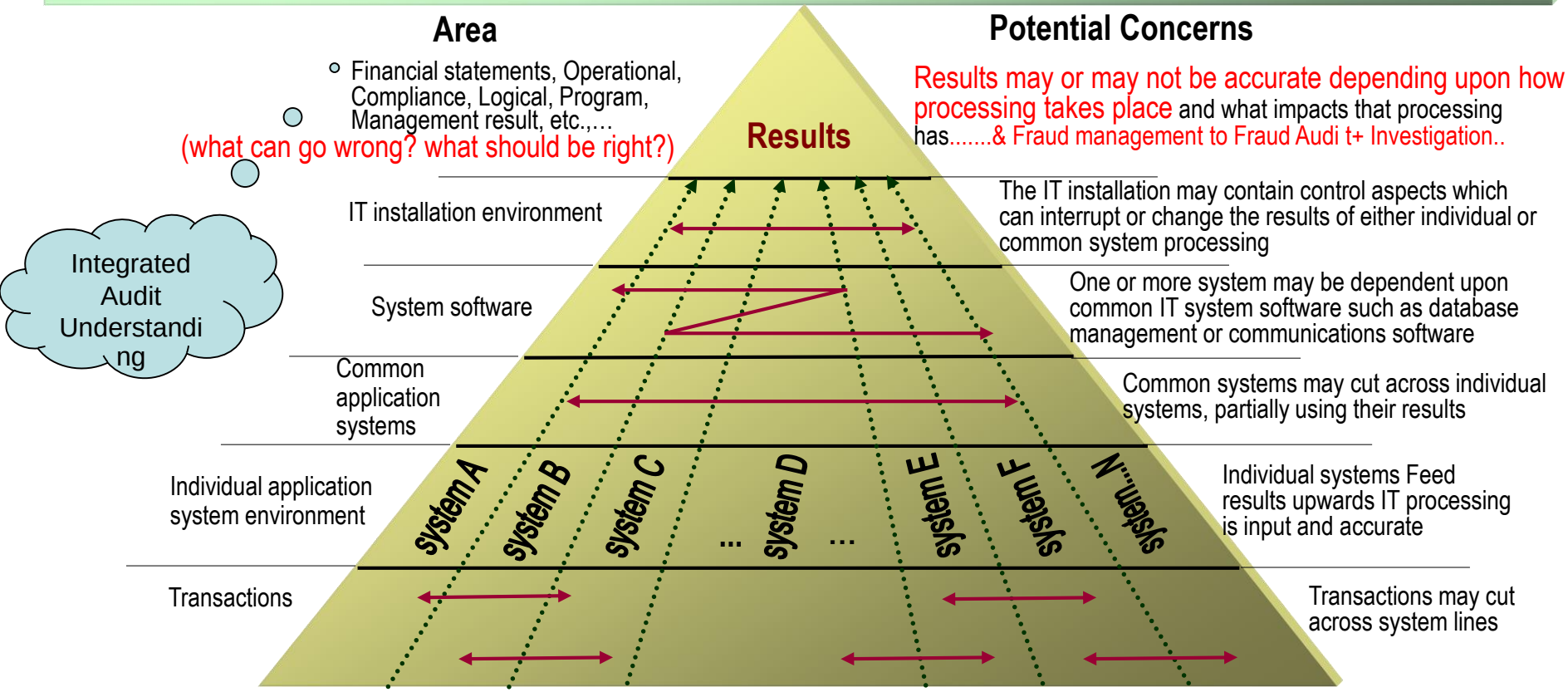
1. **Brooking Institute**
2. **Baruch Law Analysis of S&P 500 Companies**

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

IT Governance+Business Processเป็นส่วนหนึ่งที่สำคัญยิ่งของ Good Corporate Governance

การบริหารความเสี่ยงขององค์กรที่ใช้เทคโนโลยีสารสนเทศในบางมุมมอง กับ Interdependent & Audit Committee

COSO-ERM+ COBIT และการบรรลุวัตถุประสงค์การควบคุมภายในของทุกองค์กร/ทุกประเภททั้ง 4 ประการการคือ S+O+F+C



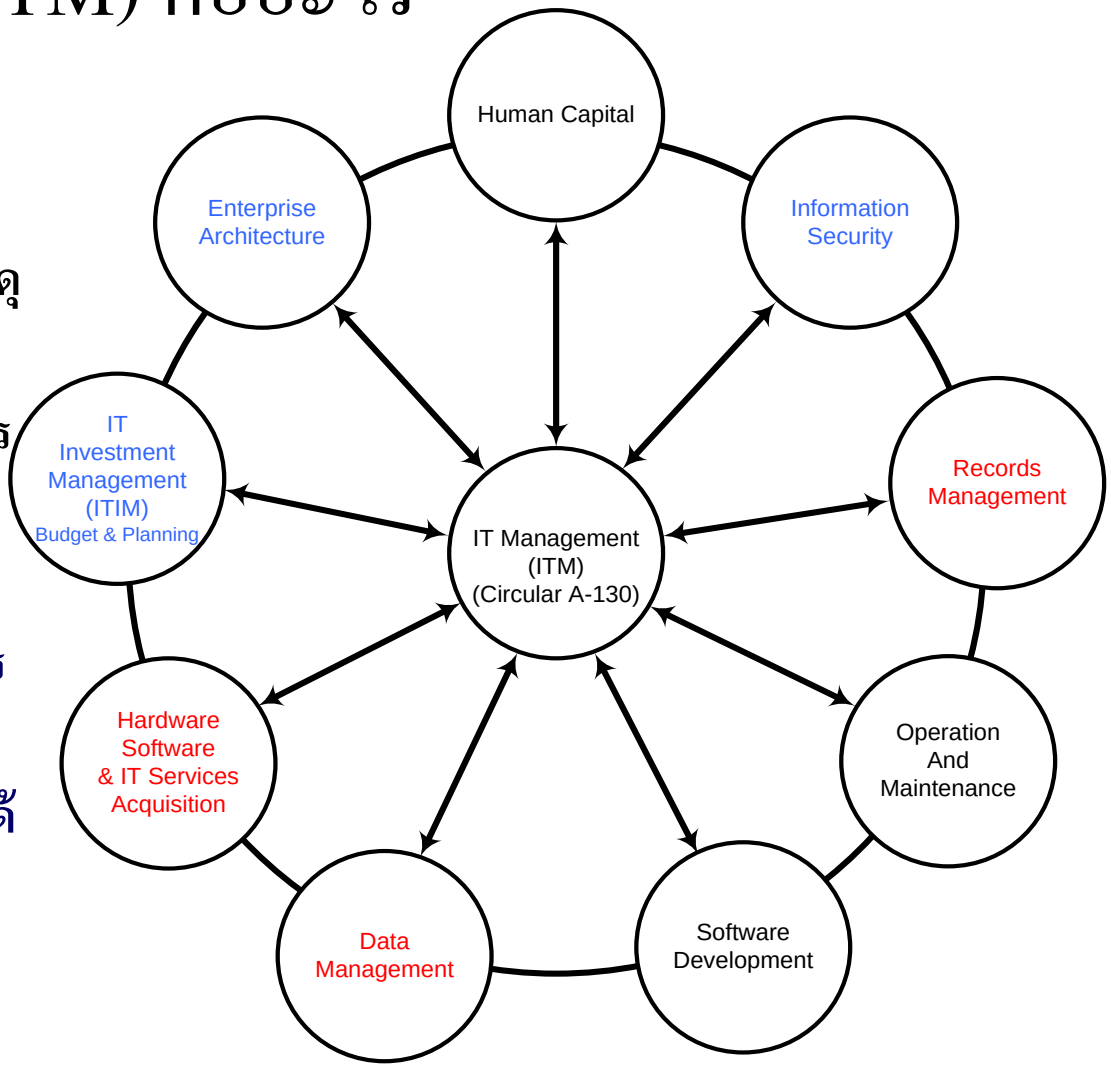
The horizontal and vertical impacts of Information Technology (IT) on the organization and risk management

: แสดงถึง **Total System Approaches** ของระบบงานภาพกว้าง ๆ ขององค์กรที่ใช้เทคโนโลยีสารสนเทศซึ่งต้องการความร่วมมือและการประสานงานจากผู้เชี่ยวชาญกับผู้บริหารงานการตรวจสอบอย่างเข้าใจจริงทั้งทางด้าน IT และอื่น ๆ

สำหรับองค์กรที่ไม่ได้จัดให้มีการตรวจสอบ **IT Governance** และ **IT Audit** ที่เหมาะสม จึงควรพิจารณาในเรื่องมาตรฐานการจัดการตรวจสอบและการบริหารความเสี่ยงในภาพรวมและการพัฒนาบุคคลากรขององค์กรเพิ่มขึ้นอีกมากในเรื่อง**IT Governance** และในเรื่องการตรวจสอบ **IT**

การบริหารสารสนเทศ (ITM) คืออะไร

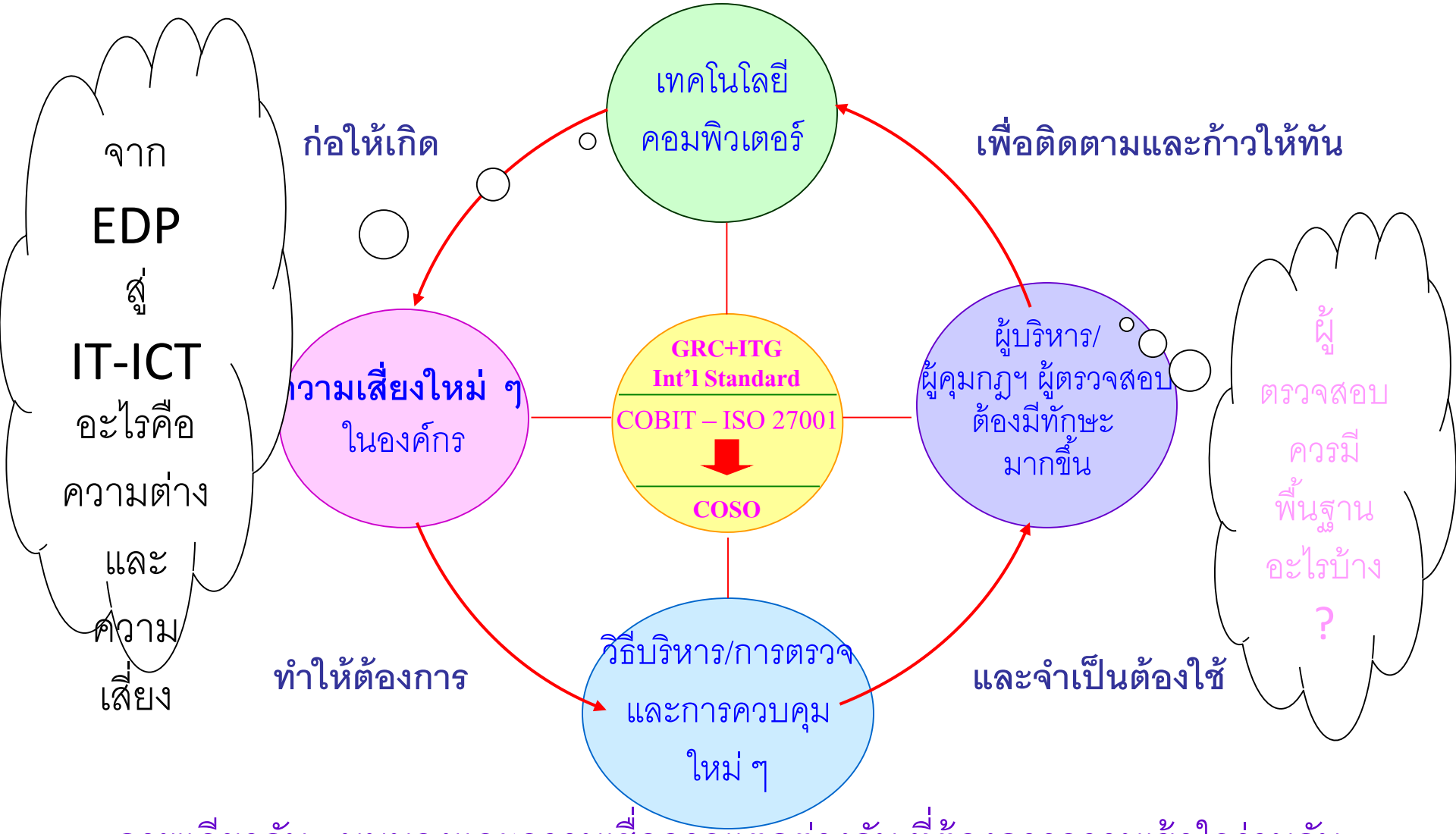
- การบริหารจัดการทรัพยากรในองค์กร โดยในอดีตนั้นมุ่งไปที่การเงิน การบุคคล และ วัสดุ แต่ในปัจจุบันจำเป็นต้องนำเอาทรัพยากรด้านข้อมูลข่าวสาร และ กระบวนการในการจัดการเข้ามาร่วมด้วย
- **ITM คือวิธีการเพื่อให้แน่ใจว่าองค์กรมีกระบวนการสำหรับการบริหารข้อมูลข่าวสาร ใช้ประโยชน์ทรัพยากร และข้อมูลด้านเทคโนโลยีเพื่อรองรับและพัฒนาธุรกิจอย่างได้อย่างเต็มประสิทธิภาพ**



Example ITM include creating an enterprise architecture, establishing metrics for IT functions, managing portfolios of projects, creating and maintaining a strategic IT plan, and setting up the organizational structure of an IT organization.

ที่มา : Forrester Research

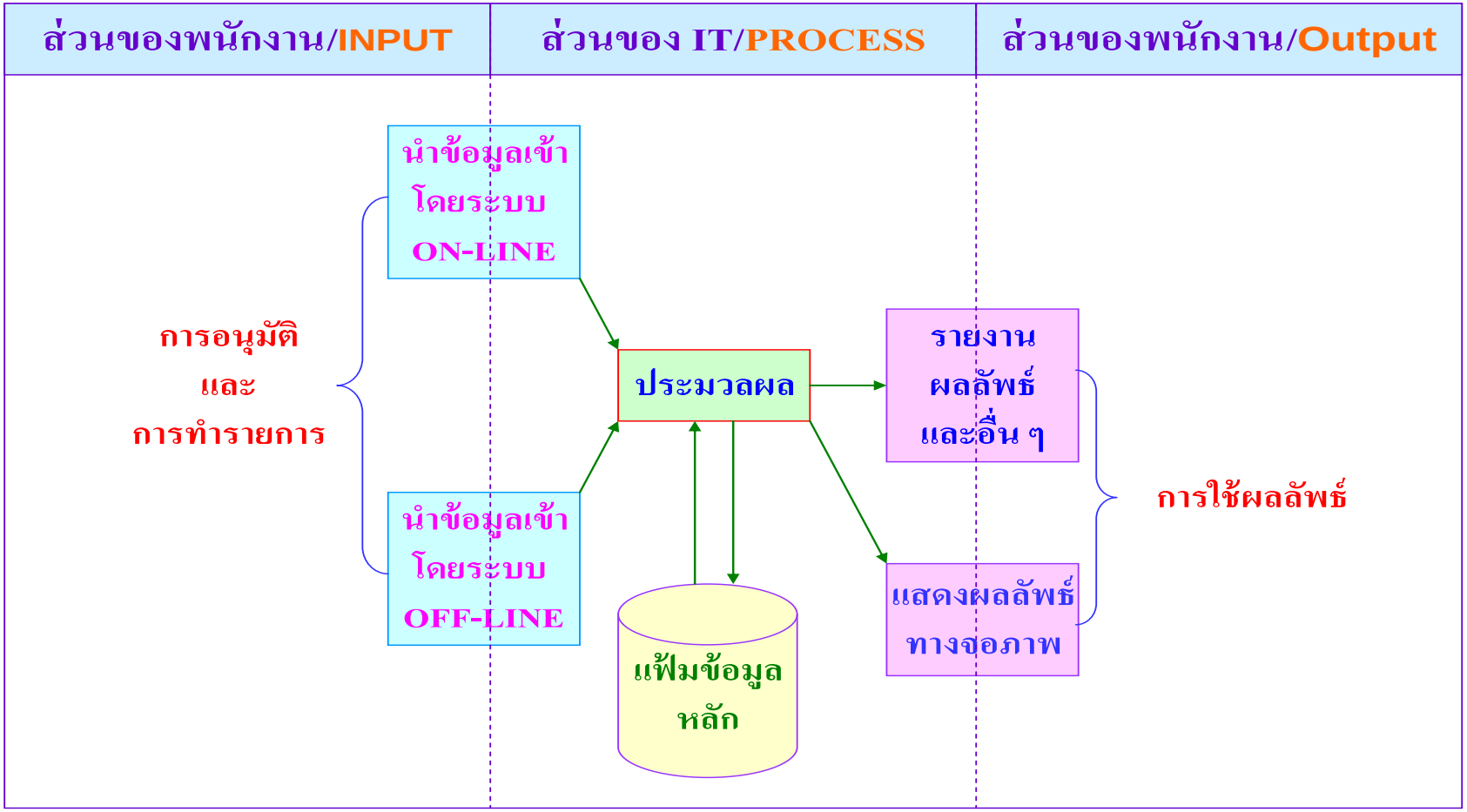
:การหลอมรวมความเข้าใจในการบริหารมิติต่าง ๆ เพื่อการสร้างคุณค่าเพิ่มให้กับ Stakeh



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

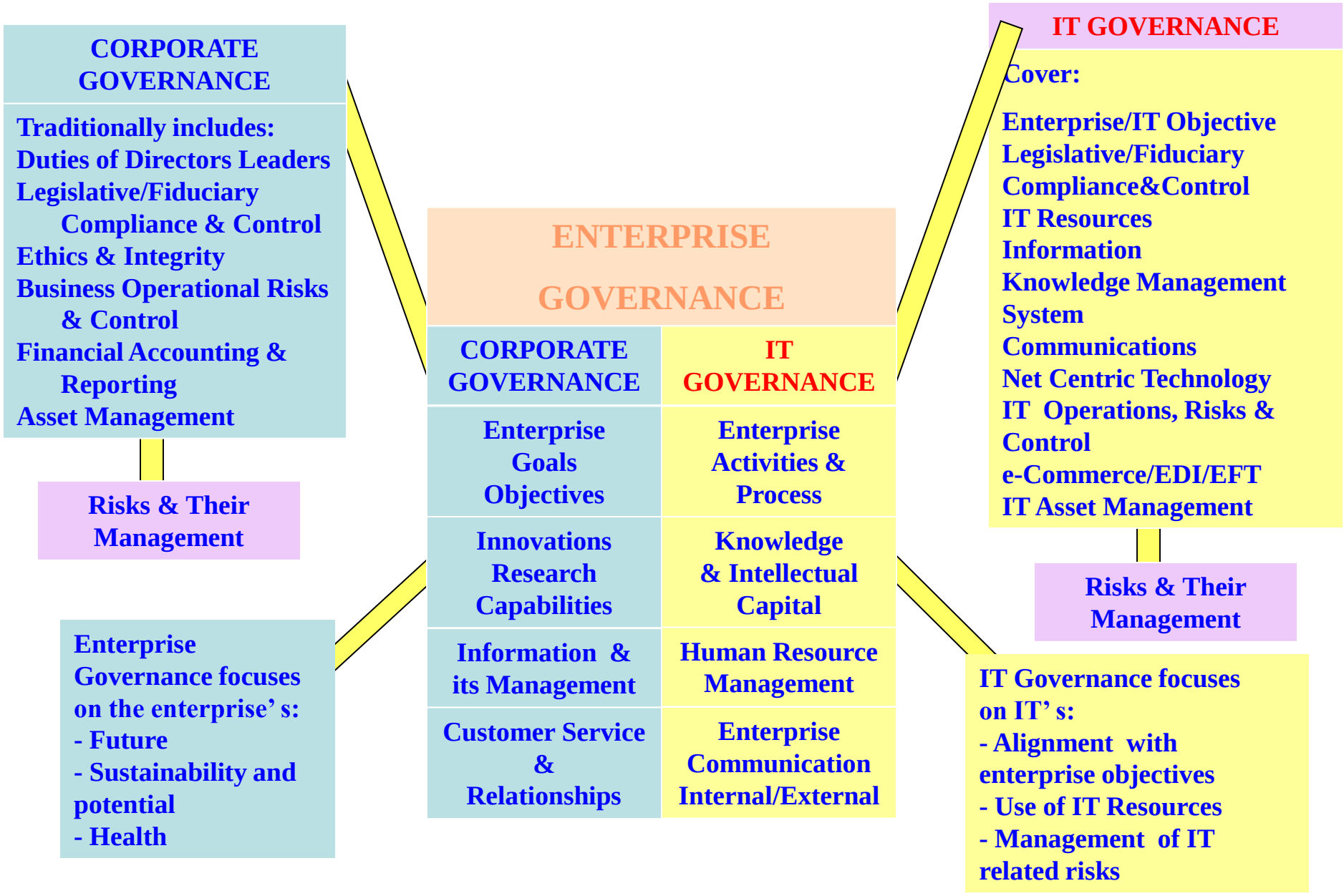
GRC : Value Creation for Effectiveness & Efficiency of Operations

ส่วนของคอมพิวเตอร์ในระบบงานต่าง ๆ ของทุกองค์กร กับความเสี่ยง



การโยงใยและความสัมพันธ์ของ
การกำกับดูแลกิจการที่ดีกับการบริหารความเสี่ยงขององค์กร

ความสัมพันธ์ของ IT Governance และ Corporate Governance



Enterprise Information Security Architecture

How Does the business work?

People					Things
Sales	Process	Resource	Supply	AR/AP	Cost
Market	Work Flow	Transform	Inventory	Collect	Shrinkage
Brand	Results	Value	Transport	Write Off	Collapse

GRC & Holistic Understanding

Oversight

- Laws
- Owners
- Board
- Auditors
- CEO

Business Risk Management

Capabilities & Internet

Technical / Human
Structural / Organizational

Brand, Value, Time, Costs

Threats → Vulnerabilities → Consequences

Accept / Transfer / Avoid / Mitigate

Risk and Surety Level and Matching

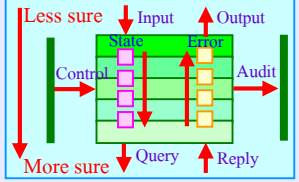
Executive Security Management

- Life cycles
- Business
- People

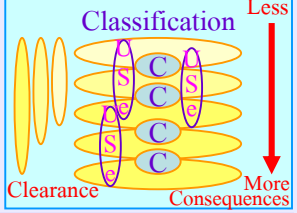
Control Architecture

R & D — Testing
Change Control — Testing
Production

Functional units



Access Control



Technical Security Architecture

- Process
  - Deter
  - Prevent
  - Detect
  - React
  - Adapt
- Data State
  - At rest
  - In Use
  - In Motion

Protection Processes

Protective Mechanisms

Perception : - obscurity - profile - appearance - deception

Structure : - M/D-A/C - POsets - diodes - firewalls - barriers

Content : - transforms - filters - markings - syntax - situation

Behavior : - change - time - tail-safe - FTC - I/A-DRS - human

Content and its Business Utility

- Systems
- Data
- Context
  - Time
  - Location
  - Purpose
  - Behavior
  - Identity
  - Method

Objectives

Source/Change Reflects reality	Attribution Situation Activity	Intolerance Redundancy	Identify Authenticate Authorize	Access Utility
Integrity		Availability		Confidentiality
Accountability		Use Control		

Organizational Governance Architecture

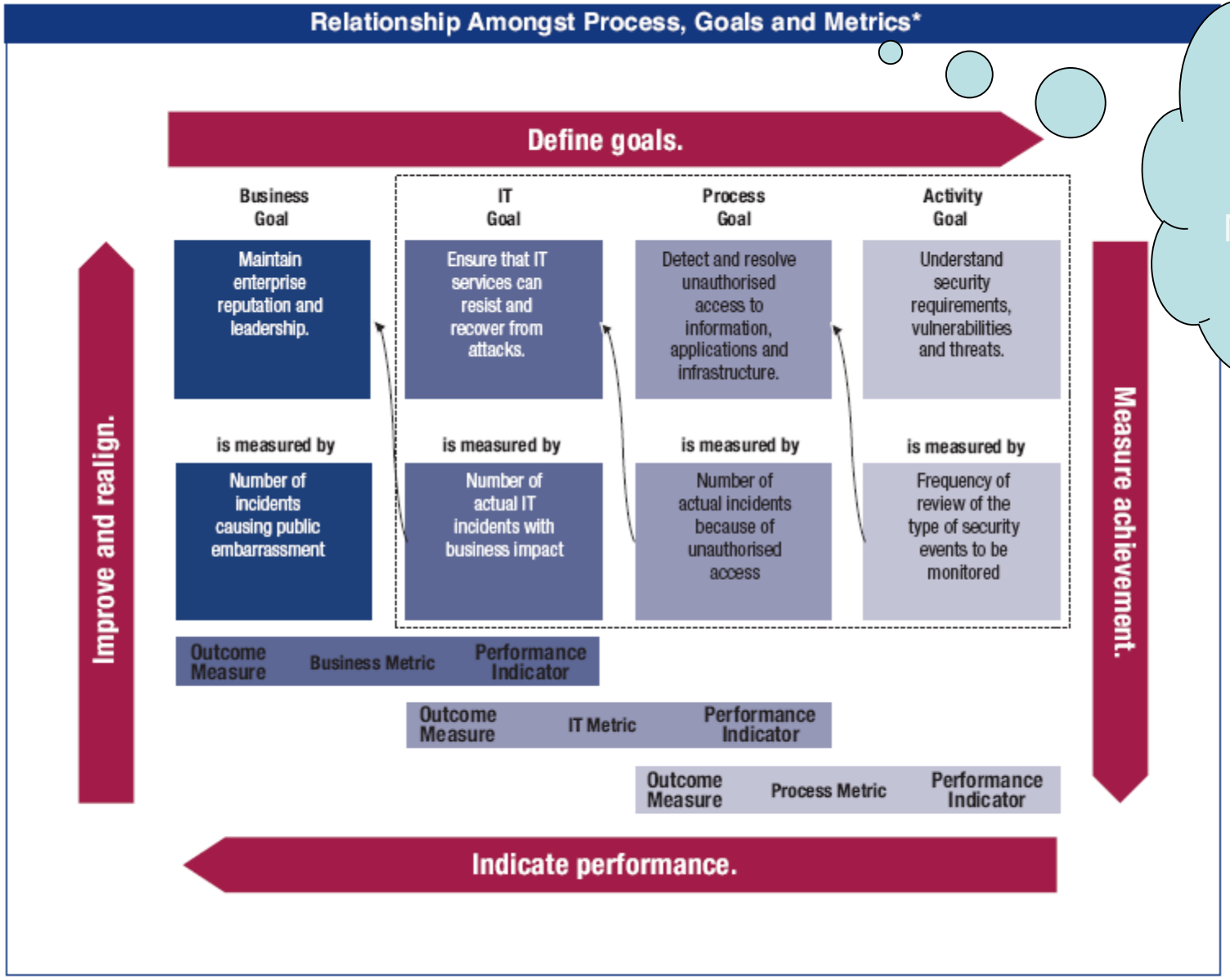
Organizational Perspectives & Business Processes

Actuate — Sense

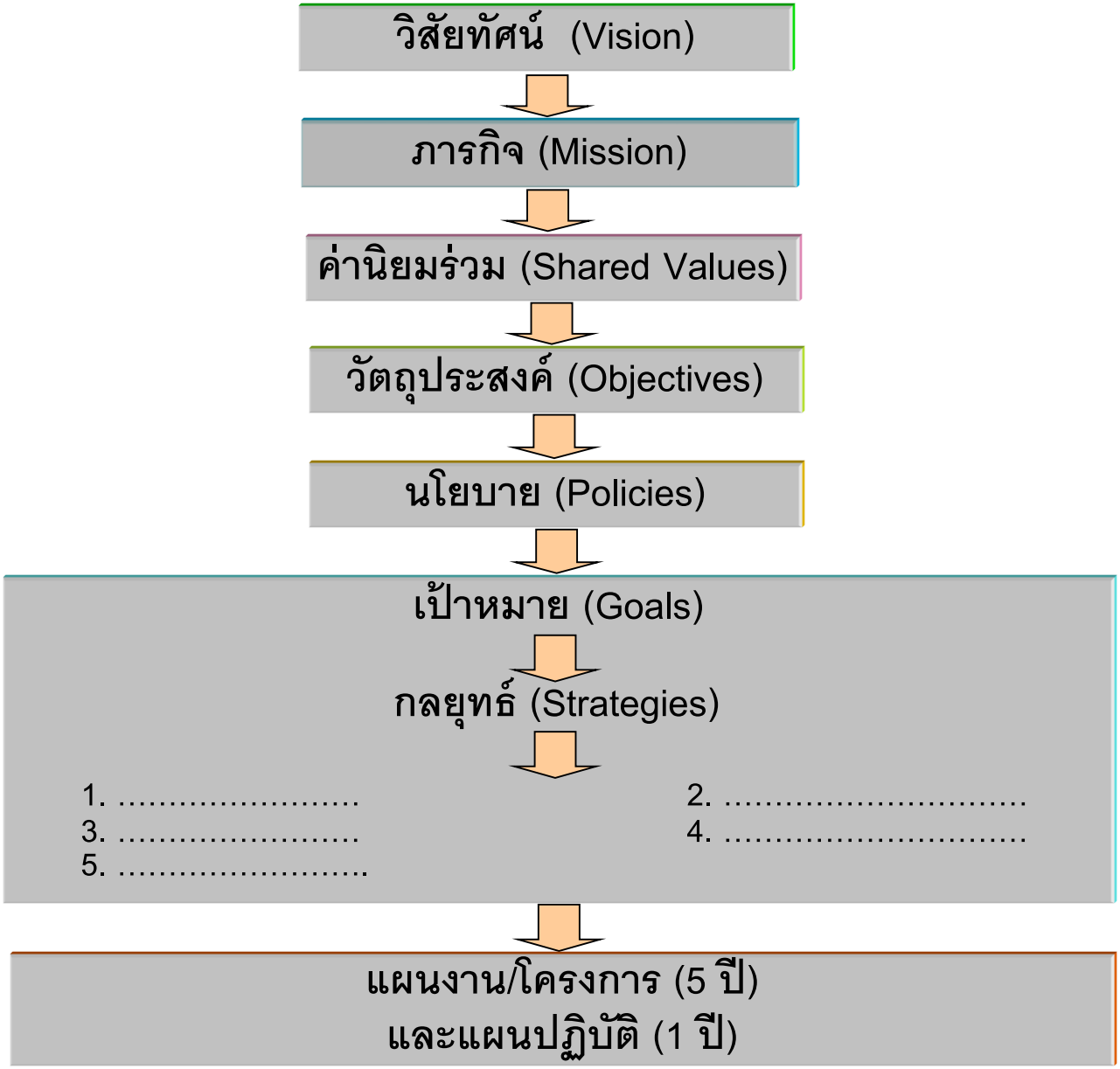
- Management
- Policy
- Standards
- Procedures
- Documentation
- Auditing
- Testing
- Technology
- Personnel
- Incidents
- Legal
- Physical
- Knowledge
- Awareness
- Organization

Source : IT Security Governance Guidebook / FRED COHEN

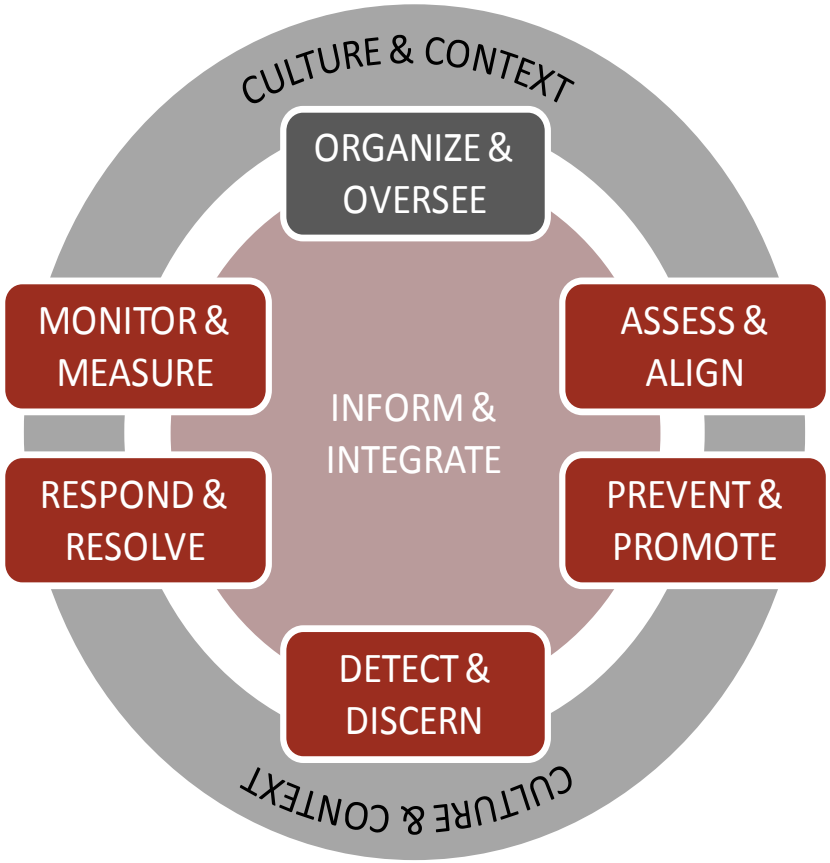
Relationship Amongst Process, Goal and Metrics



มุมมองโลกแห่งการเปลี่ยนแปลง กับ
การบริหารความเสี่ยง & โครงสร้างแผนบริหารขององค์กร



8 INTEGRATED COMPONENTS



8 UNIVERSAL OUTCOMES

- Achieve Business Objectives
- Enhance Organizational Culture
- Increase Stakeholder Confidence
- Prepare & Protect the Organization
- Prevent, Detect & Reduce Adversity
- Motivate & Inspire Desired Conduct
- Improve Responsiveness & Efficiency
- Optimize Economic & Social Value

Source: Open Compliance and Ethics Group

เรา จะนำเป้าหมายข้างต้น ไป ดำเนินการให้ได้ผลอย่างไร?

iGRC in / and COBIT 5

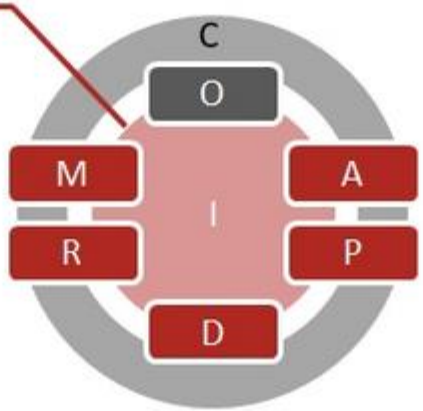
GRC Capability Model: Element View

MONITOR & MEASURE
M1 – Context Monitoring
M2 – Performance Monitoring
M3 – Systemic Improvement
M4 – Audit & Assurance

CONTEXT & CULTURE
C1 – External Business Context
C2 – Internal Business Context
C3 – Organizational Culture
C4 – Values & Objectives

ORGANIZE & OVERSEE
O1 – Outcomes & Commitment
O2 – Roles & Responsibilities
O3 – Approach & Accountability

INFORM & INTEGRATE
I1 – Info Management & Documentation
I2 – Internal & External Communication
I3 – Technology & Infrastructure



ASSESS & ALIGN
A1 – Risk Identification
A2 – Risk Analysis
A3 – Risk Optimization

RESPOND & RESOLVE
R1 – Internal Review & Investigation
R2 – Third-Party Inquiry &Investigation
R3 – Corrective Controls
R4 – Crisis Response & Recovery
R5 – Remediation & Discipline

PREVENT & PROMOTE
P1 – Codes of Conduct
P2 – Policies
P3 – Preventive Controls
P4 – Awareness & Education
P5 – Human Capital Incentives
P6 – Stakeholder Relations
P7 – Risk Financing & Insurance

DETECT & DISCERN
D1 – Hotline & Notification
D2 – Inquiry & Survey
D3 – Detective Controls

Source: OCEG Red Book
www.oceg.org/standards

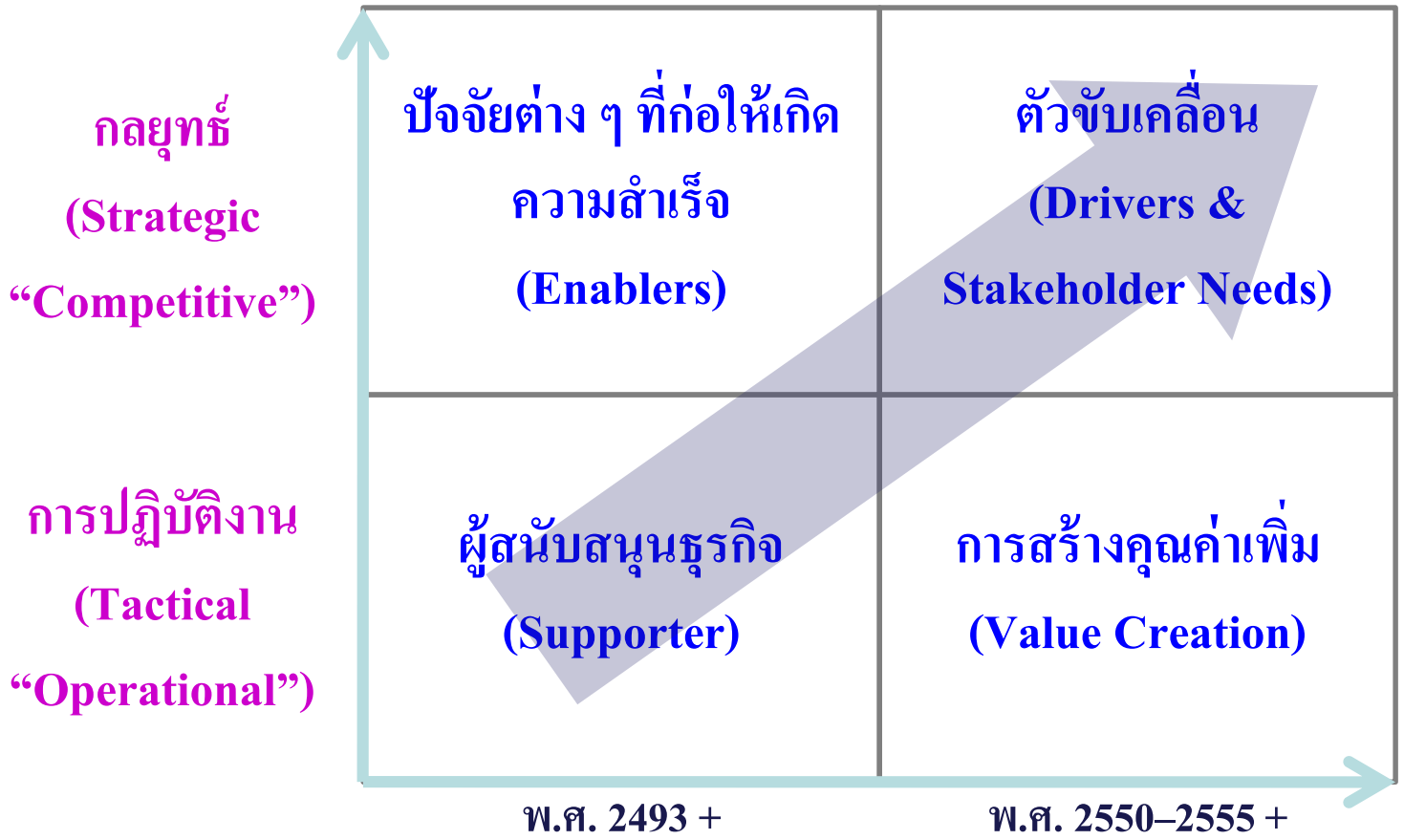
Thai CIOs are crossing the borders everyday

"Integrated Single Framework for Business and ICT to meet Stakeholder needs"

Source: Microsoft

"Evolution, Business Innovation & Leadership"

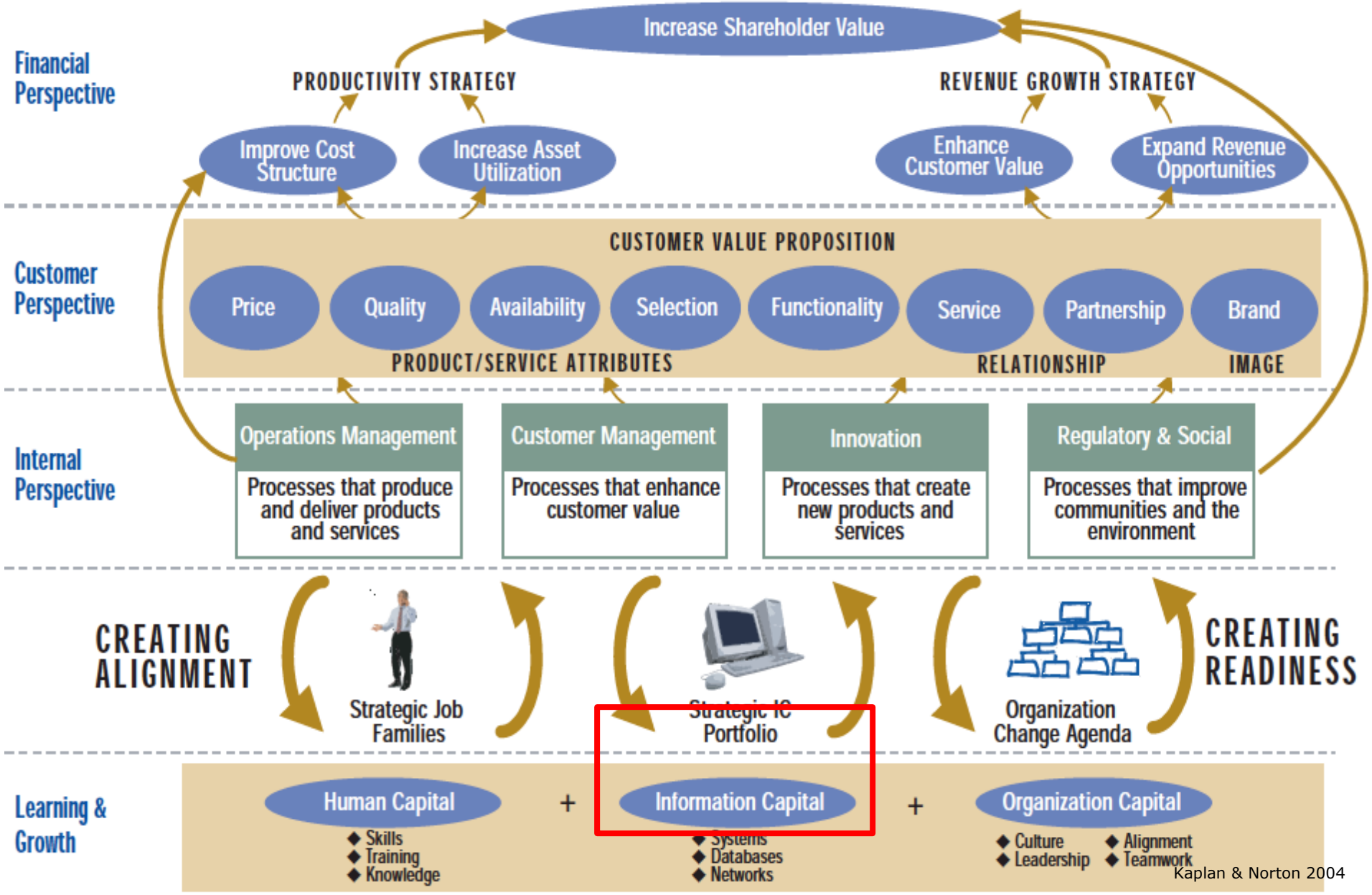
ICT ศตวรรษที่ 21 กับบทบาทของ CIO & CEO



ICT จากผู้ตาม เป็น ผู้นำ ในการบริหารยุคใหม่

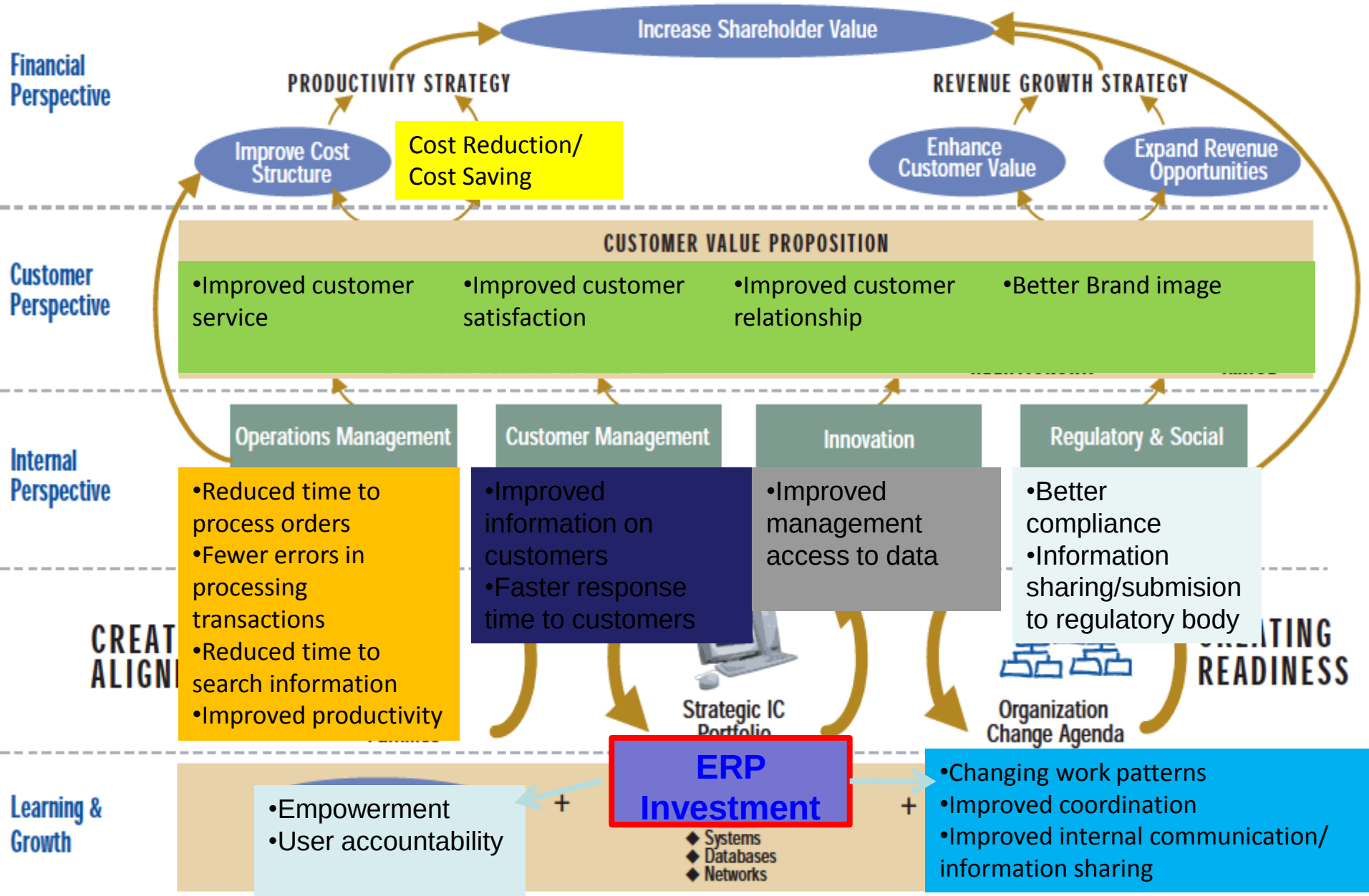
Source : www.itgthailand.com , www.itgthailand.wordpress.com

ICT Risk and Impact of IT on cost and revenue - Services drivers

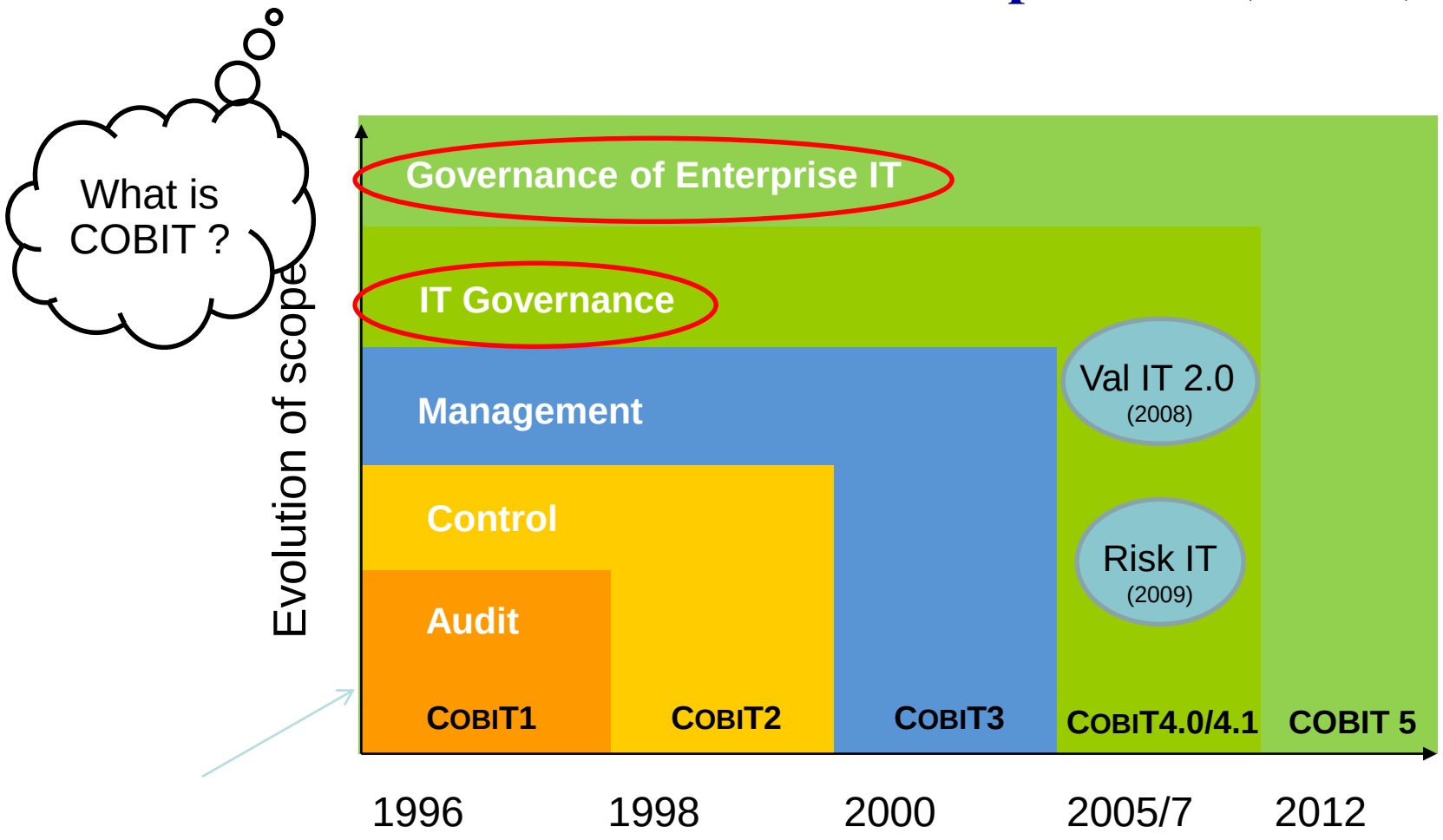


Kaplan & Norton 2004

Sample : Balanced Scorecard & Perspectives Business value of ERP

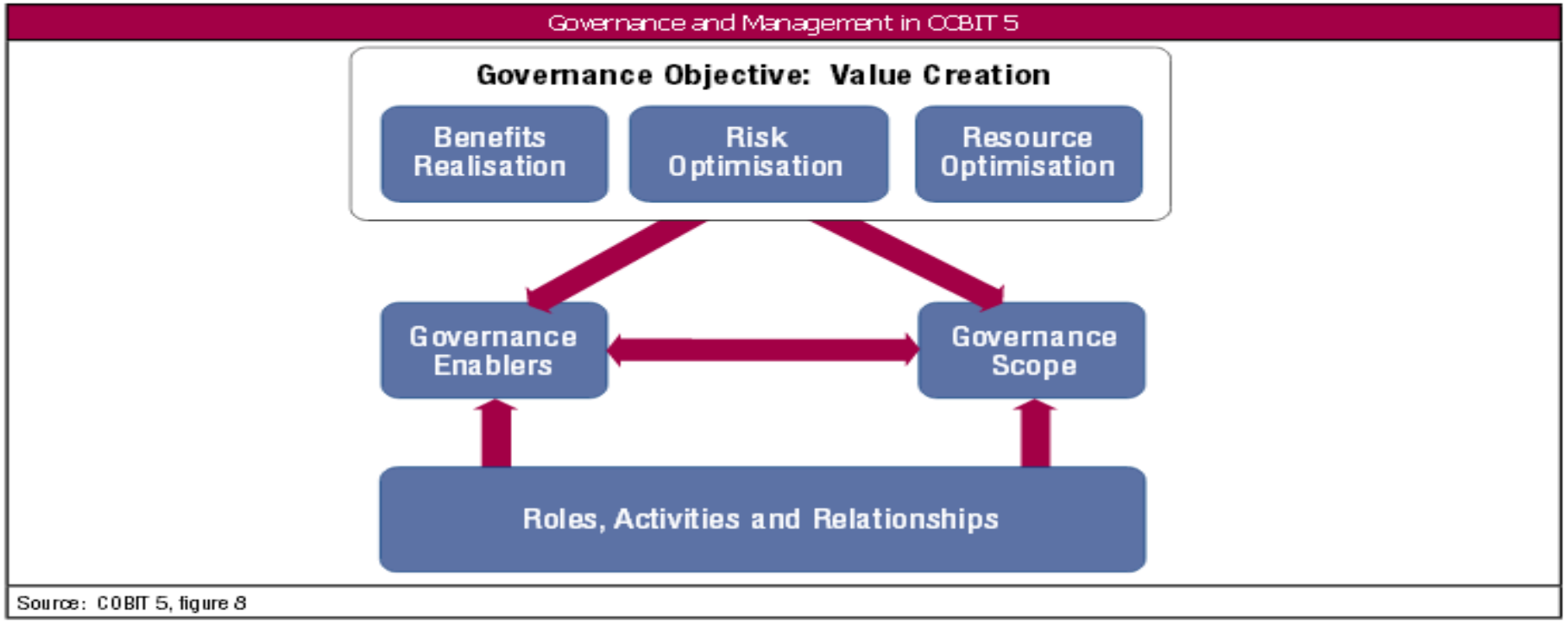


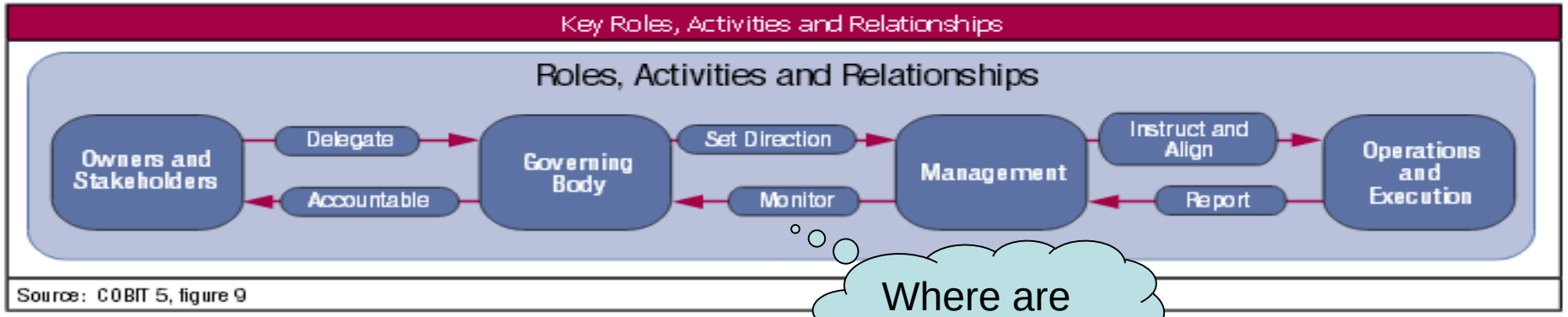
COBIT: Governance of Enterprise IT (GEIT)



A business framework from ISACA, at www.isaca.org/cobit

COBIT 5 and Key Roles-Activities- Relationship

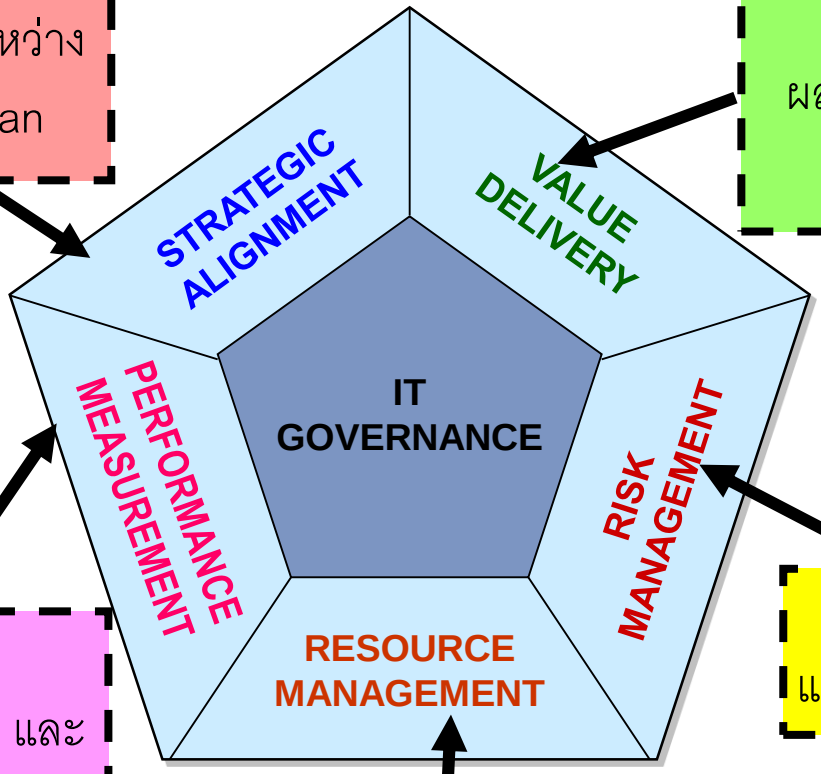




Where are you ?

Source : ISACA

IT Governance Needs Management Frameworks



สร้างความเชื่อมโยงระหว่าง Business กับ IT Plan

สร้างความสำเร็จโดยผลประโยชน์ที่ได้จาก IT สอดคล้องกับกลยุทธ์

วัดผลสำเร็จของงานทุกกิจกรรมย่อย ทั้ง Lead และ Lag Indicator

ประเมินความเสี่ยงไอทีและหามาตรการ ลด ละ เลิก

การลงทุนที่เหมาะสมและการจัดการทรัพยากร

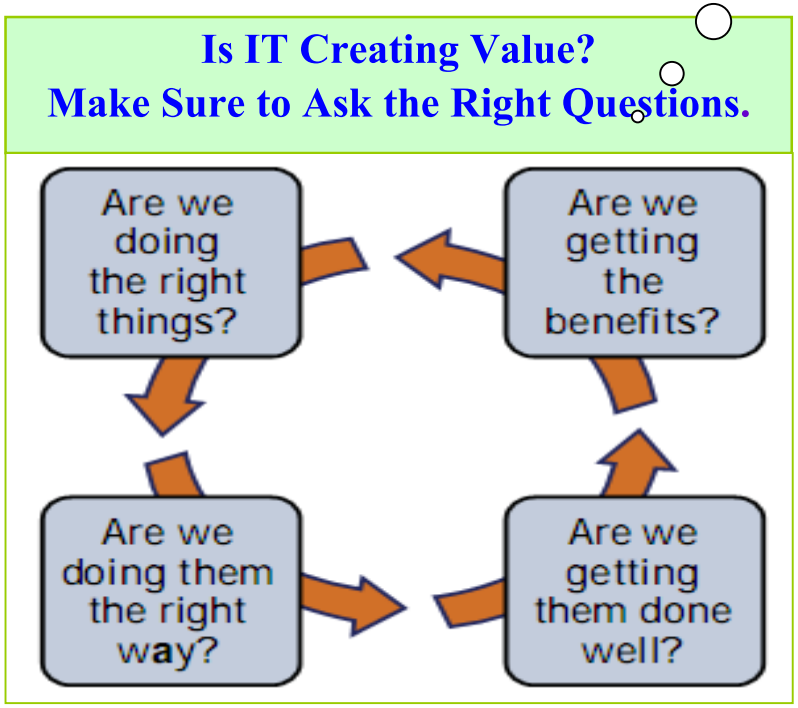
Unlocking Value & Val IT

How is Effective IT Governance Best Accomplished?

- Asking—and Answering—Four Fundamental Questions
  1. The strategic question: Are we doing the right things?
  2. The architecture question: Are we doing these things the right way?
  3. The delivery question: Are we getting these things done well?
  4. The value question: Are we getting the benefits?

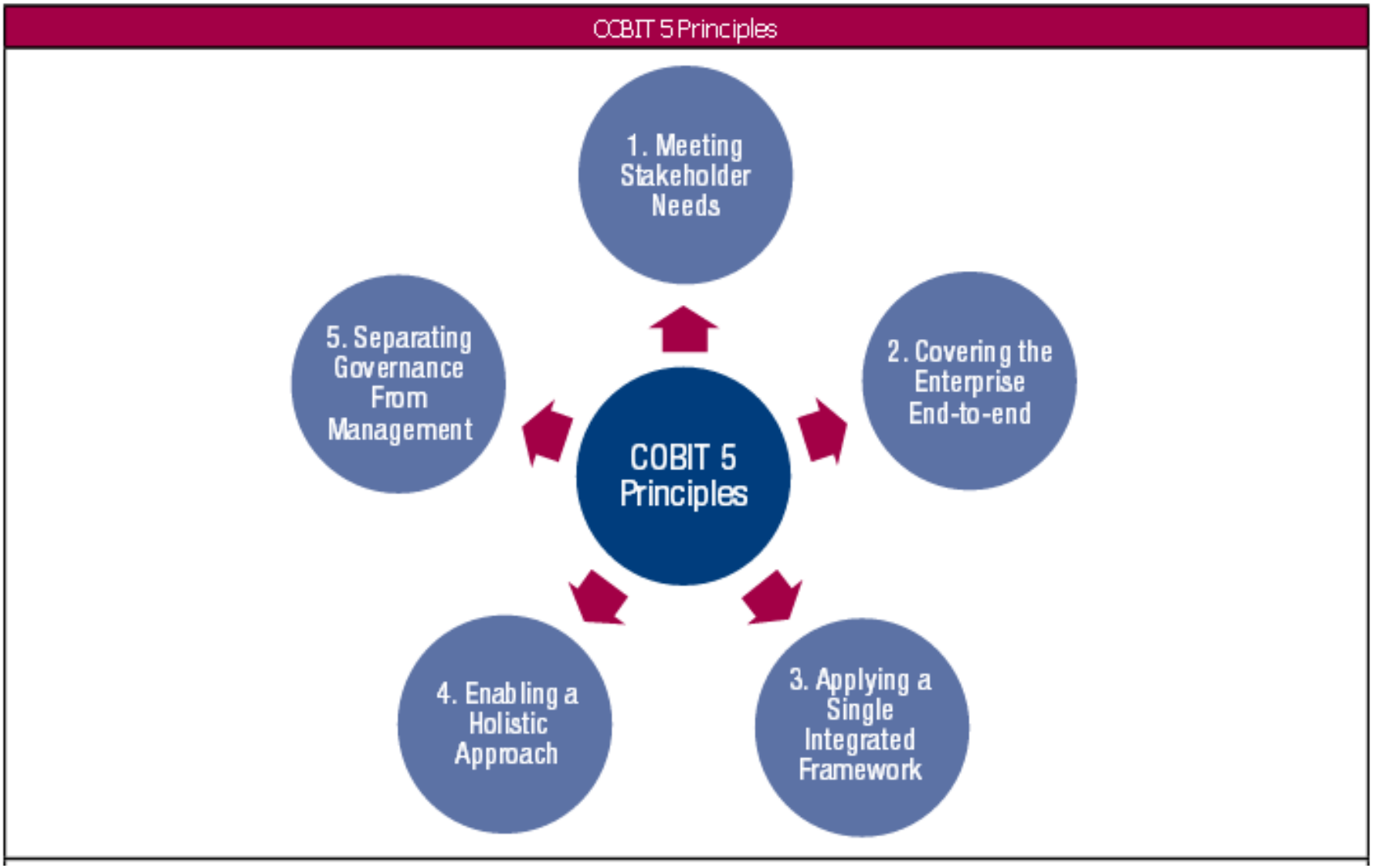
You are here…

- Using a Comprehensive IT Governance Framework
  - ☞ COBIT
  - ☞ Val IT



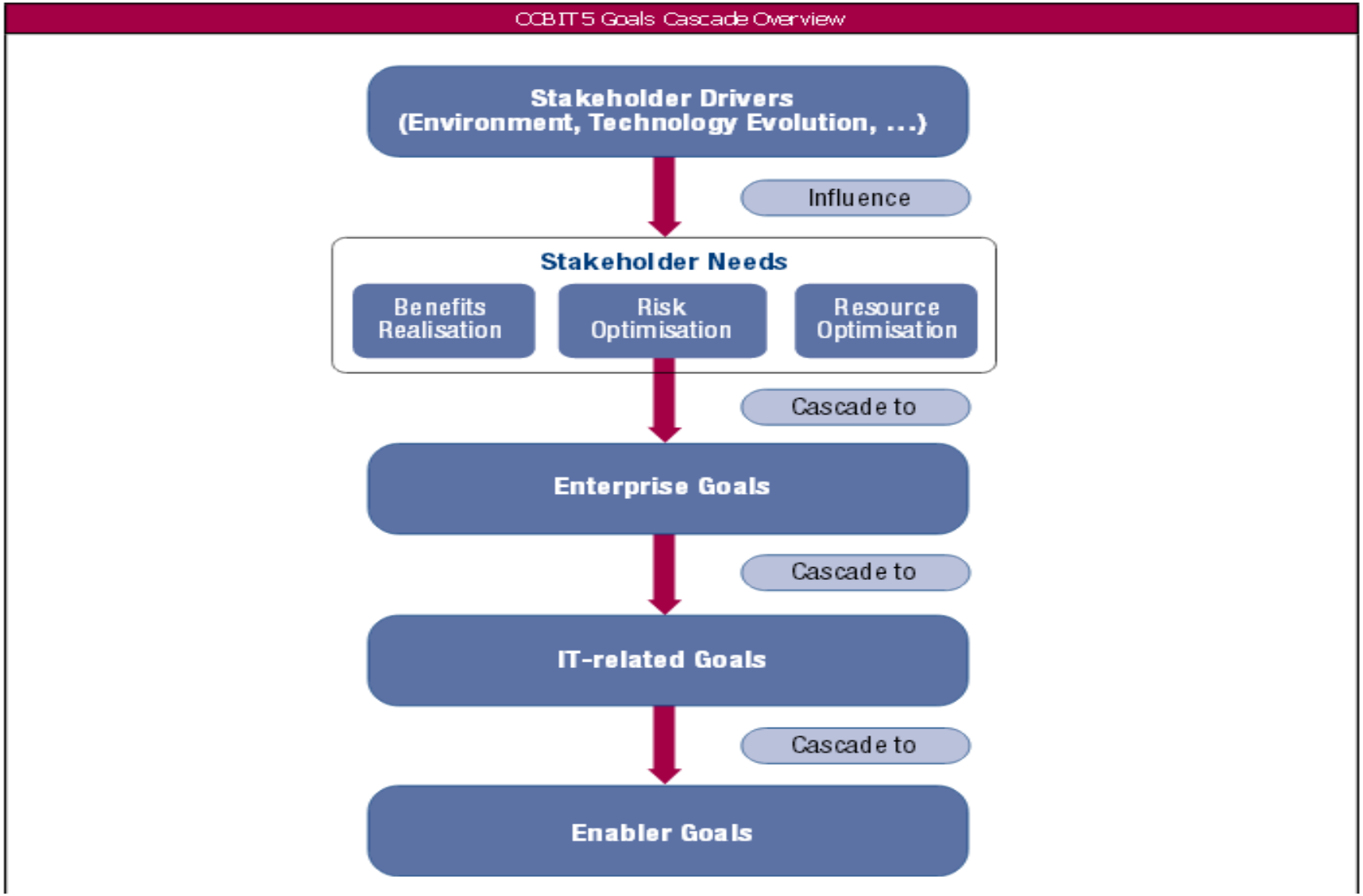
Resource : IT Governance Institute

COBIT 5 for ICT Risk Management



Source : ISACA

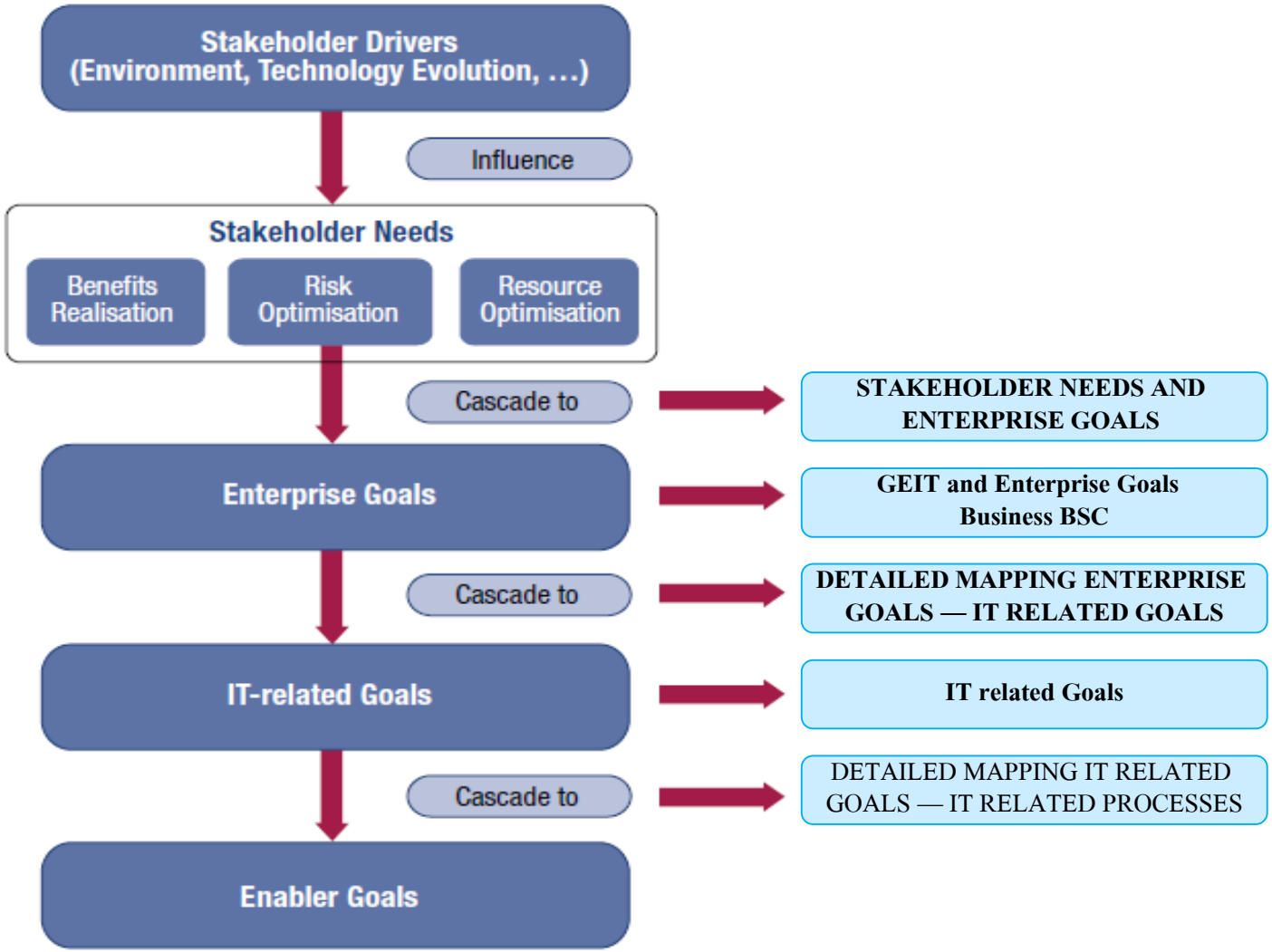
COBIT 5 for Stakeholder needs



Source : ISACA

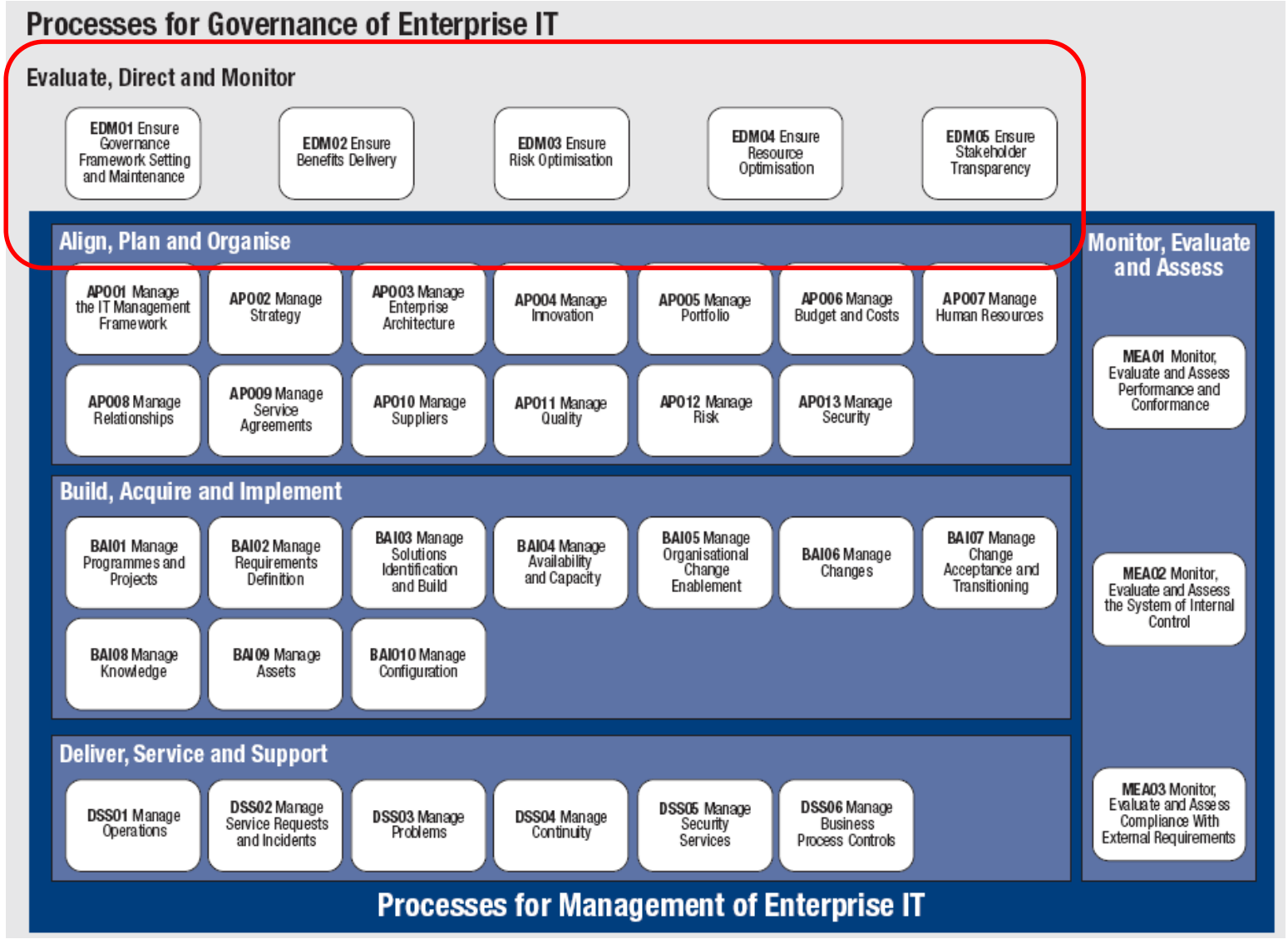
A Business Framework Perspective for the Governance and Management of Enterprise IT

Goals Cascade Overview / GEIT – Governance Enterprise of IT



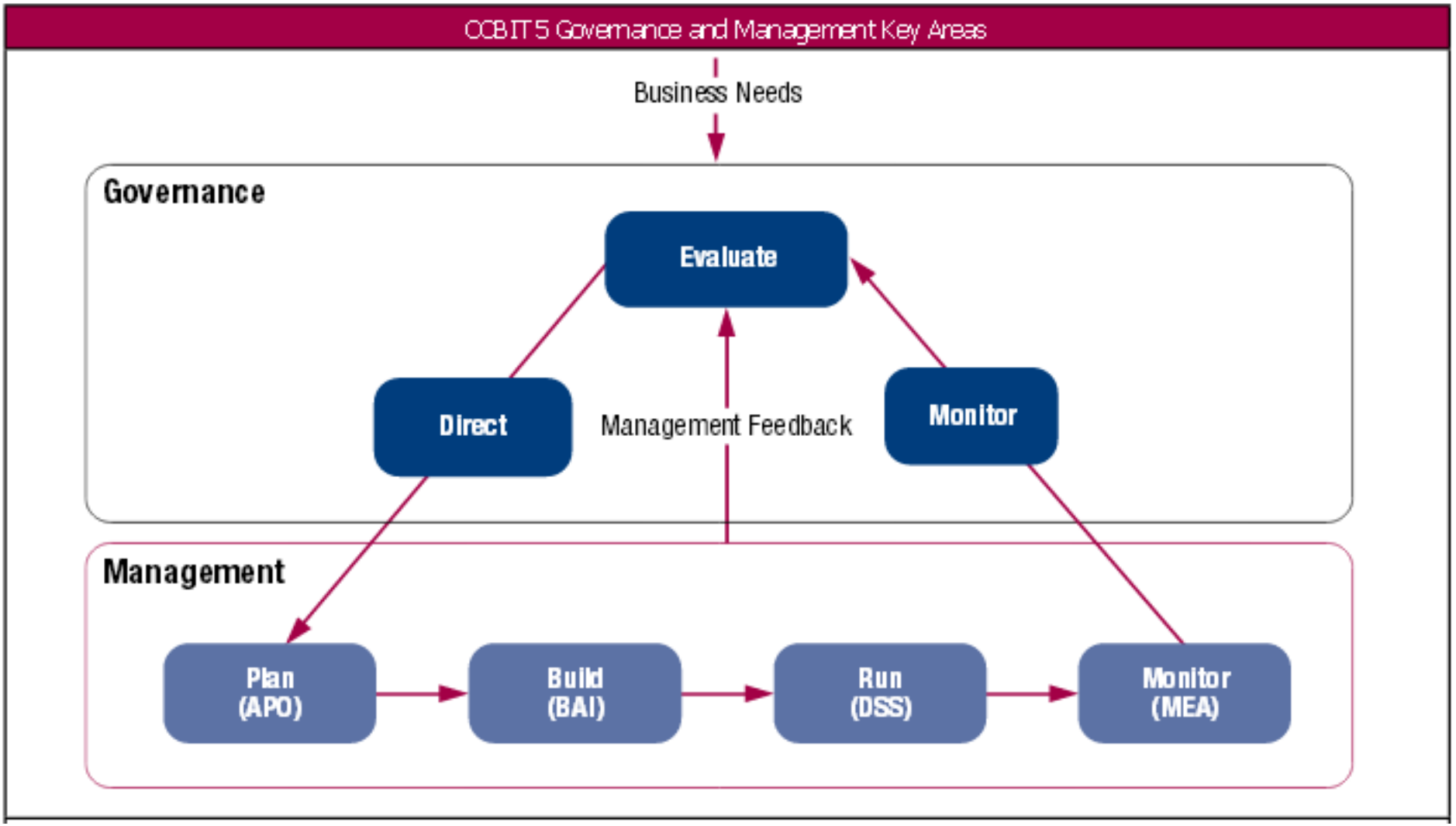
Resource : ISACA / GEIT (GRC Described Under COBIT 5)

Stakeholders & Governance in COBIT 5 (cont.)



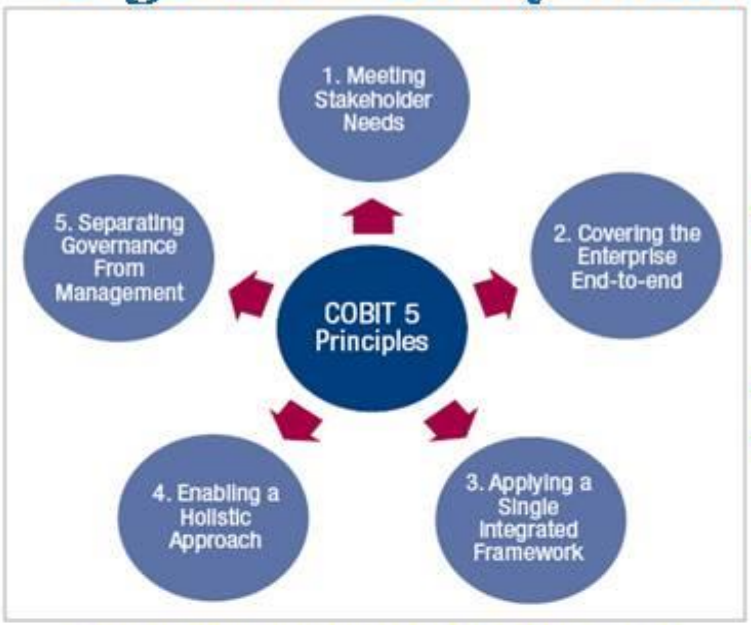
Source: COBIT® 5, figure 16.

Integrated Single Framework Governance & Management

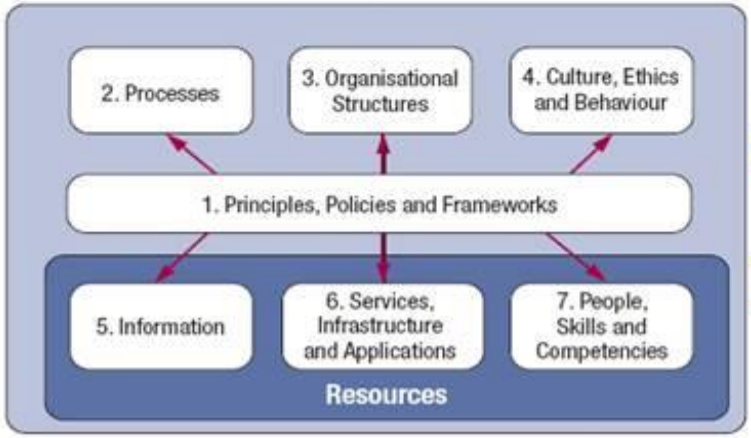


Source : ISACA

Digital Economy/Business and Technology Architecture



Effective governance and management framework based on a holistic set of seven enablers that optimises information and technology investment and use for the benefit of stakeholders.



Governance -> Value Creation

- Benefits Realization
- Risk Optimization
- Resource Optimization

Does not focus only on the "IT Function"

Business and IT Alignment

Anytime

Deep Insights

Digital Economy and Business

Big Data

Anywhere

All Digital

Interaction | Core Platform | Analysis

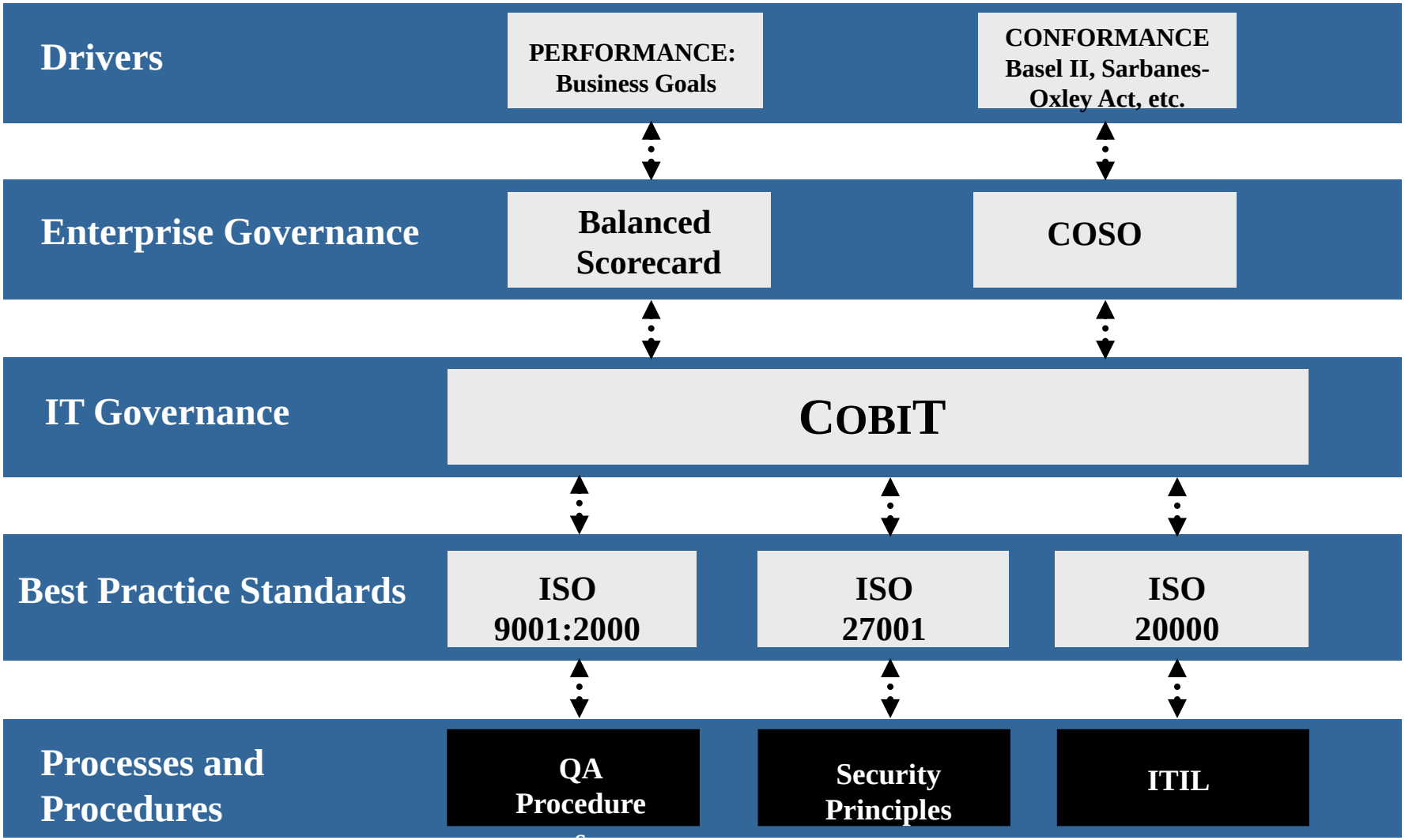
Infrastructure

Vision – Mission – Policy – Strategy – Leadership

Integrated Management – Assurance - Capability

Source : iGRC and COBIT 5 and Approach to Implementation for Digital Economy/Business Framework adopt and adapt by www.itgthailand.com

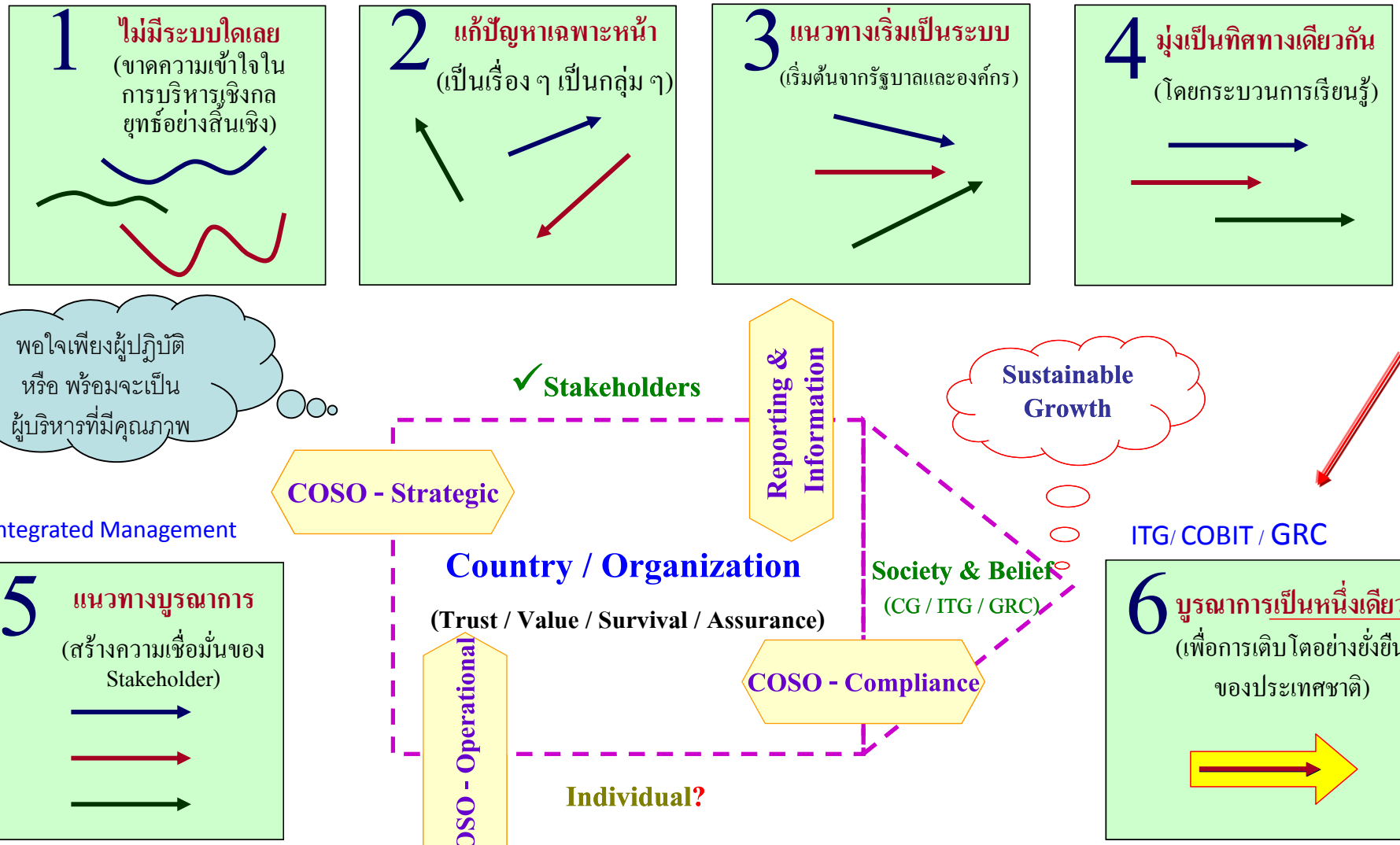
GRC Perspectives & Where Does COBIT Fit?



Source: ITGI

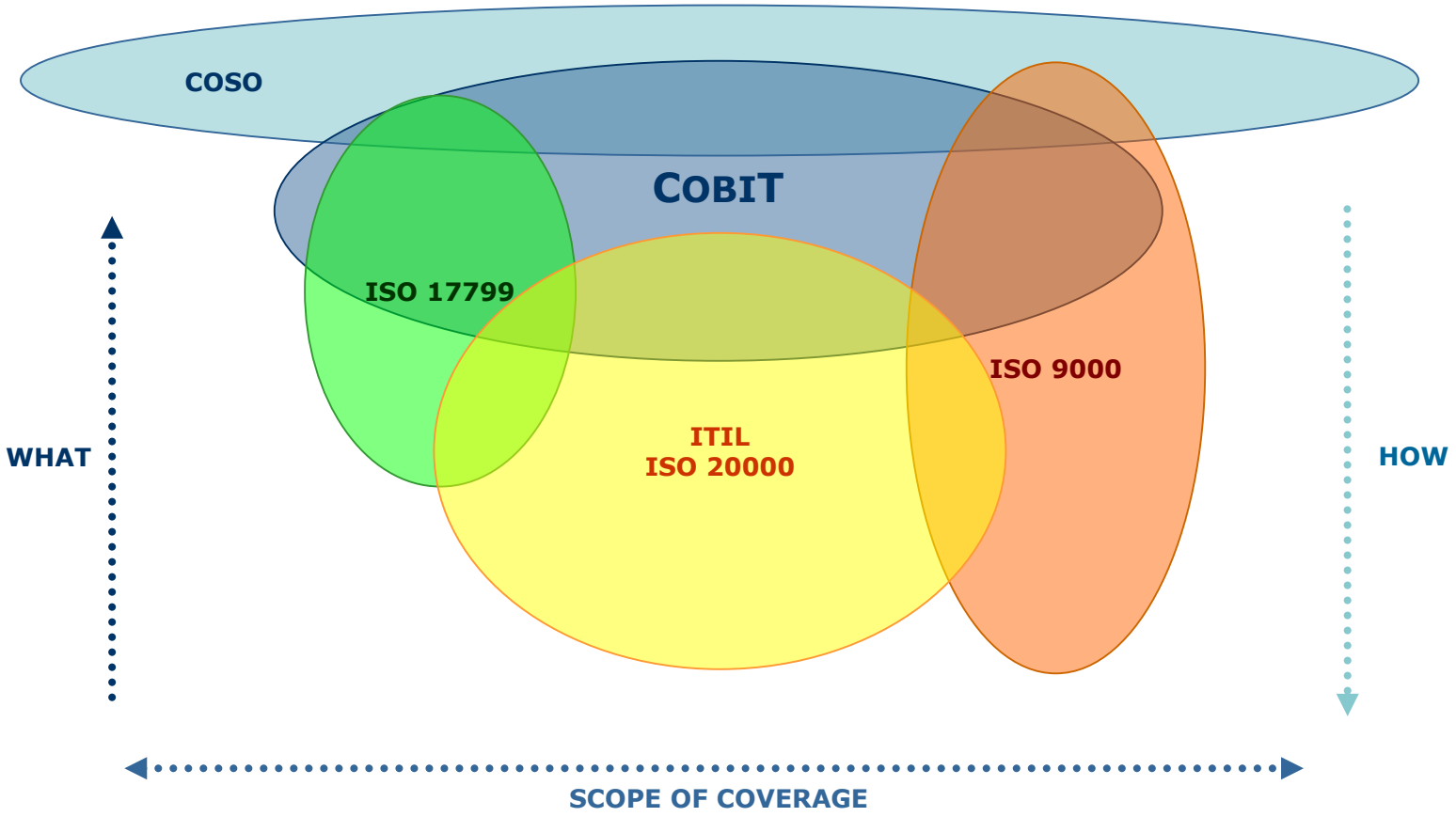
ความเข้มแข็งในการบริหารองค์กรและประเทศแบบบูรณาการ

ITG / COBIT -Governance – Risk Mgmt. – Compliance & Integrity Management



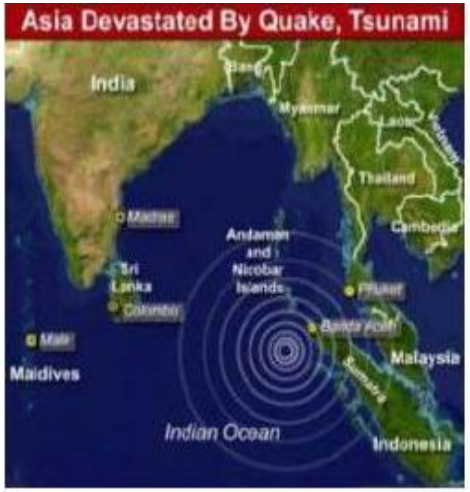
COBIT and Other IT/ Management Standards & Best Practices for IT and Non-IT Auditors

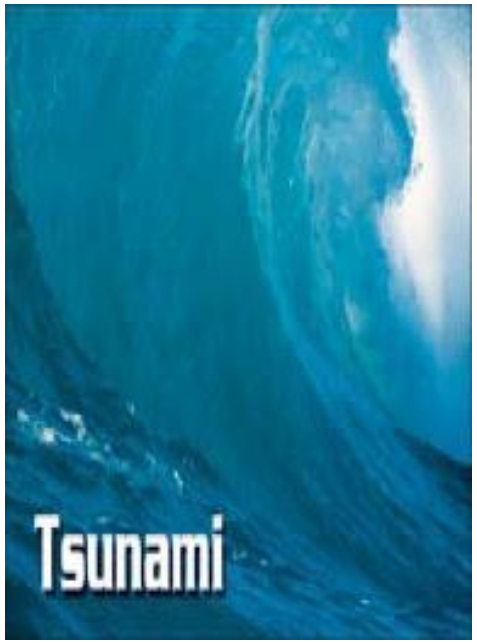
Organisations will consider and use a variety of IT models, standards and best practices. These must be understood in order to consider how they can be used together, with COBIT acting as the consolidator ('umbrella').



Source: ITGI

- **บทเรียนจากความเสี่ยง**





ความหมาย และ ทบทวนการบริหารความเสี่ยง - สั้นๆ

ความเสี่ยงที่เป็นอันตราย (Hazard)

เหตุการณ์ในเชิงลบที่หากเกิดขึ้นแล้วอาจเป็นอันตรายหรือสร้างความเสียหายต่อองค์กร

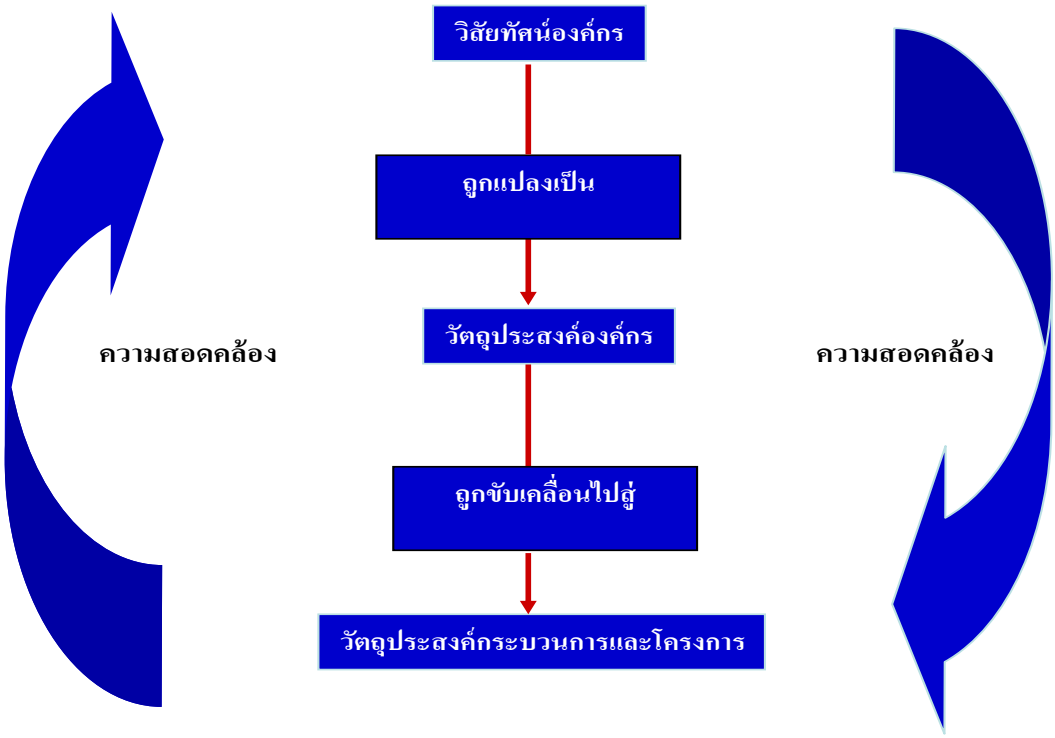
ความเสียงที่เป็นความไม่แน่นอน (Uncertainty)

เหตุการณ์ที่ทำให้ผลที่องค์กรได้รับจากเหตุการณ์จริงไม่เป็นไปตามที่คาดการณ์ไว้ อันเนื่องมาจากสาเหตุต่าง ๆ กัน

ความเสี่ยงที่เป็นโอกาส (Opportunity)

เหตุการณ์ที่ทำให้องค์กรเสียโอกาสในการแข่งขัน การดำเนินงานและการเพิ่มมูลค่าของผู้ถือหุ้น

การกำหนดวัตถุประสงค์แบบ SMART



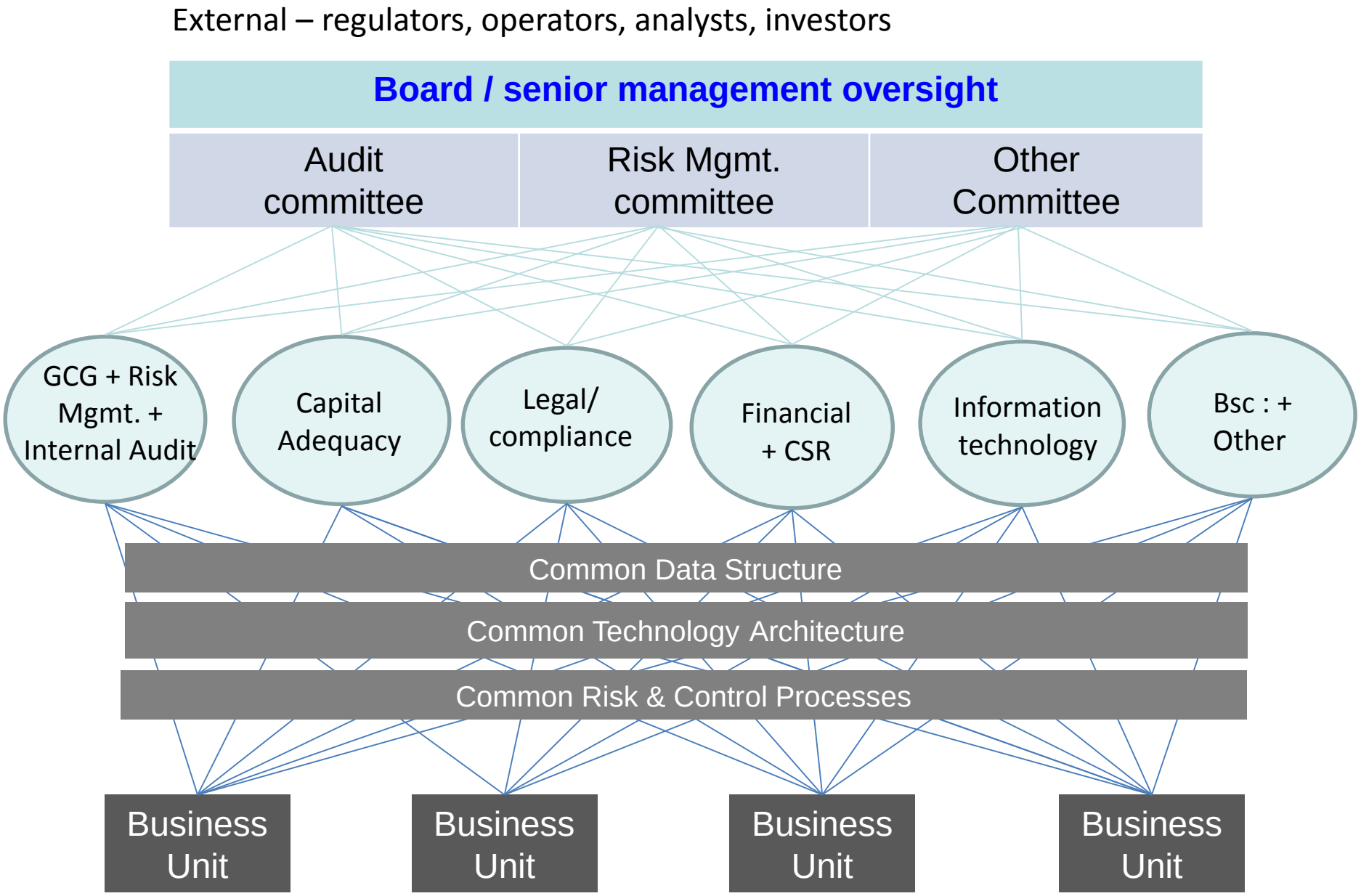
วัตถุประสงค์ที่ดีต้อง...

(SMART)

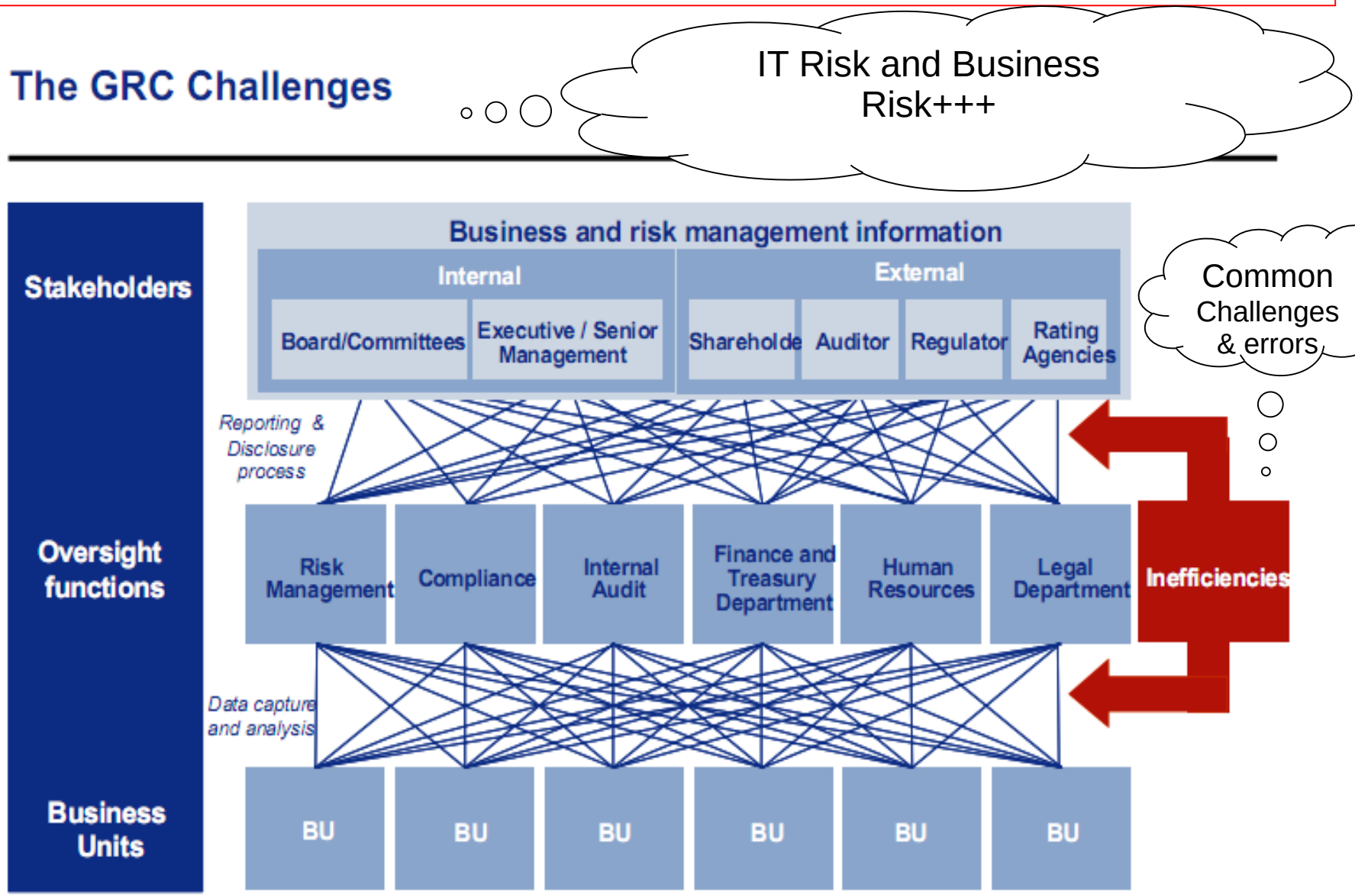
- เฉพาะเจาะจง
- สามารถวัดได้
- สามารถบรรลุผลได้
- เป็นจริงได้
- มีกำหนดเวลา

- ✓ **Specific** - มีความเฉพาะเจาะจง ทุกคนเข้าใจตรงกัน
- ✓ **Measurable** – สามารถวัดได้ทั้งเชิงปริมาณหรือเชิงคุณภาพ
- ✓ **Attainable** – สามารถทำให้บรรลุผลได้
- ✓ **Relevant** – มีความสัมพันธ์กับนโยบายหลักในระดับสูง
- ✓ **Timely** – มีกำหนดเวลาในการทำ

Risk Convergence & Management Model



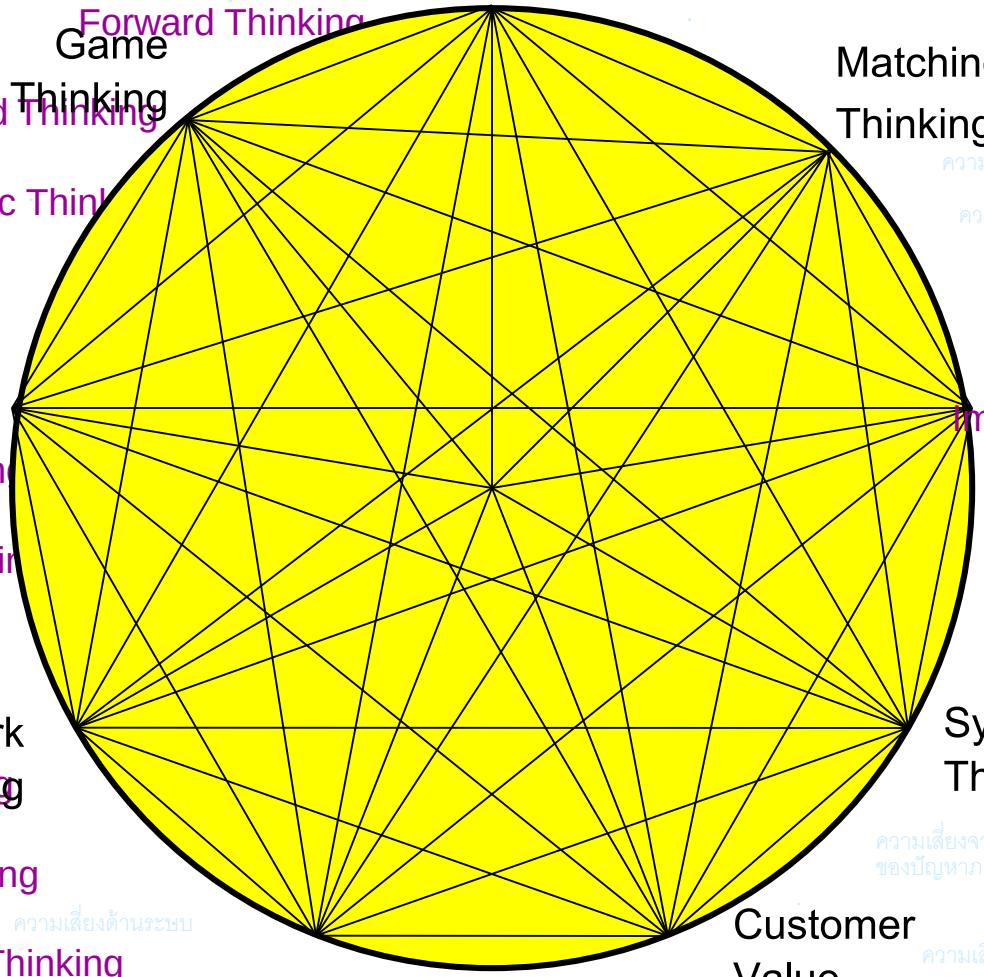
A Consolidated-Integrated Single Framework on COSO Model



Source: KPMG

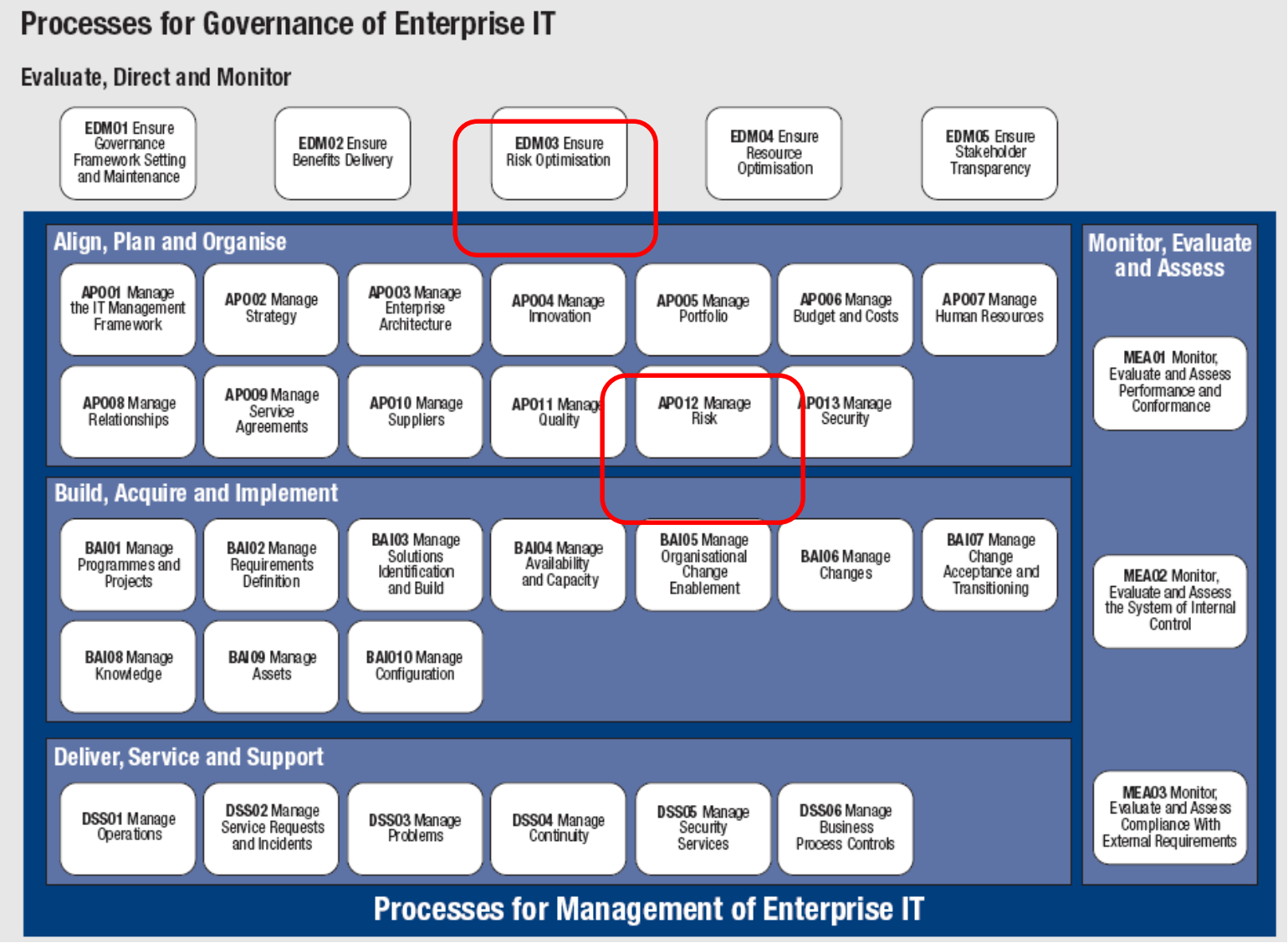
การบริหารความเสี่ยง
การเข้าใจความเสี่ยง กับ การบริหารขององค์กร

STRATEGIC THINKING AND RISK MANAGEMENT



Visionany Thinking
Context Thinking
Forward Thinking
Game Thinking
Weighted Thinking
Dynamic Think
Matching Thinking
Context Thinking
Forward Thinking
Weighted Thinking
Dynamic Thinking
Impact Thinking
Bottom Line Thinking
Quantity Thinking
Innovative Thinkin
Grey Thinkin
Planner Thinking
Holistic Thinking
Impact Thinking
Bottom Line Thinking
Innovative Thinking
Grey Thinking
Planner Thinking
Context Thinking
Benchmark Thinking
Forward Thinking
Weighted Thinking
Dynamic Thinking
Impact Thinking
Bottom Line Thinking
Systems Thinking
Context Thinking
Forward Thinking
Weighted Thinking
Dynamic Thinking
Innovative Thinking
Grey Thinking
Planner Thinking
Key Success Factor Thinking
Customer Value Thinking

Stakeholders & Risk Management in COBIT 5 (cont.)



COBIT 5 & Stakeholders Mapping

The In Depth Look Into Governance Framework

กระบวนการสำหรับการบริหารจัดการไอทีระดับองค์กร – ด้านการบริหารจัดการ กับ การบริหารความเสี่ยง ที่ CIO / CEO ควรเข้าใจ

จัดวางแนว จัดทำแผน และจัดระบบ

- บริหารจัดการกรอบการดำเนินงานการบริหารงานด้านไอที
- บริหารจัดการกลยุทธ์
- บริหารจัดการสถาปัตยกรรมองค์กร
- บริหารจัดการนวัตกรรม
- บริหารจัดการกลุ่มของชุดโครงการ
- บริหารจัดการงบประมาณและต้นทุน
- บริหารจัดการทรัพยากรบุคคล
- บริหารจัดการความสัมพันธ์
- บริหารจัดการข้อตกลงการให้บริการ
- บริหารจัดการผู้ขายหรือผู้ให้บริการ
- บริหารจัดการคุณภาพ
- บริหารจัดการความเสี่ยง
- บริหารจัดการความมั่นคงปลอดภัย

จัดสร้าง จัดหา และนำไปใช้

- บริหารจัดการโครงการและชุดโครงการ
- บริหารจัดการข้อกำหนดความต้องการ
- บริหารจัดการระบุและจัดสร้างกระบวนการแก้ปัญหาแบบเบ็ดเสร็จ
- บริหารจัดการความพร้อมใช้งานและจัดความสามารถ
- บริหารจัดการเพื่อให้การเปลี่ยนแปลงองค์กรสัมฤทธิ์ผล
- บริหารจัดการการเปลี่ยนแปลง
- บริหารจัดการการยอมรับการเปลี่ยนแปลงและการปรับเปลี่ยน
- บริหารจัดการความรู้
- บริหารจัดการสินทรัพย์
- บริหารจัดการองค์ประกอบของระบบ

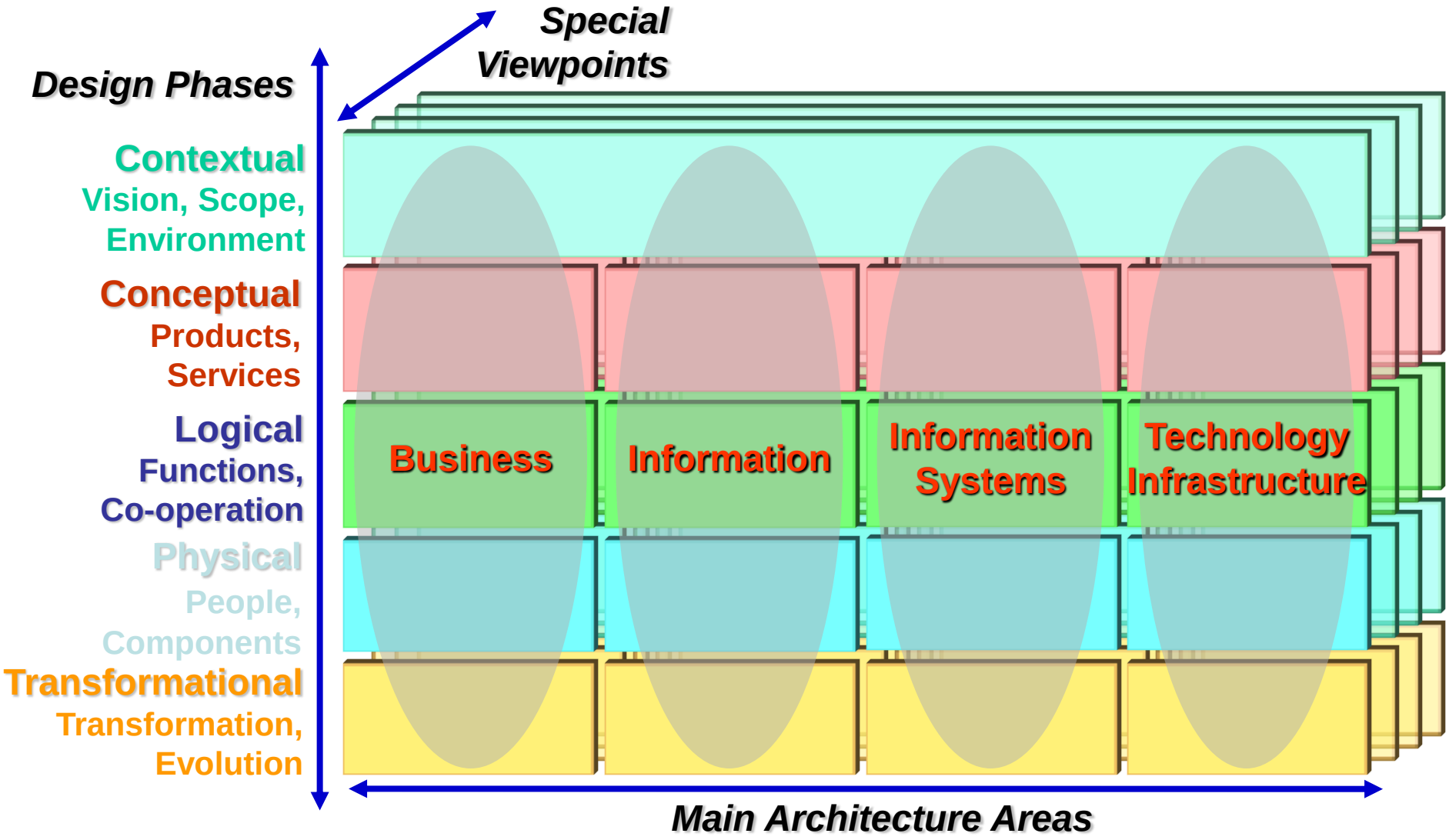
ส่งมอบ ให้บริการ และสนับสนุน

- บริหารจัดการการปฏิบัติการ
- บริหารจัดการคำร้องขอบริการและเหตุการณ์ที่เกิดขึ้น
- บริการจัดการมีปัญหา
- บริหารจัดการความต่อเนื่อง
- บริหารจัดการบริการผ่านความมั่นคงปลอดภัย
- บริหารจัดการการควบคุมกระบวนการทางธุรกิจ

เฝ้าติดตาม วัดผล และประเมิน

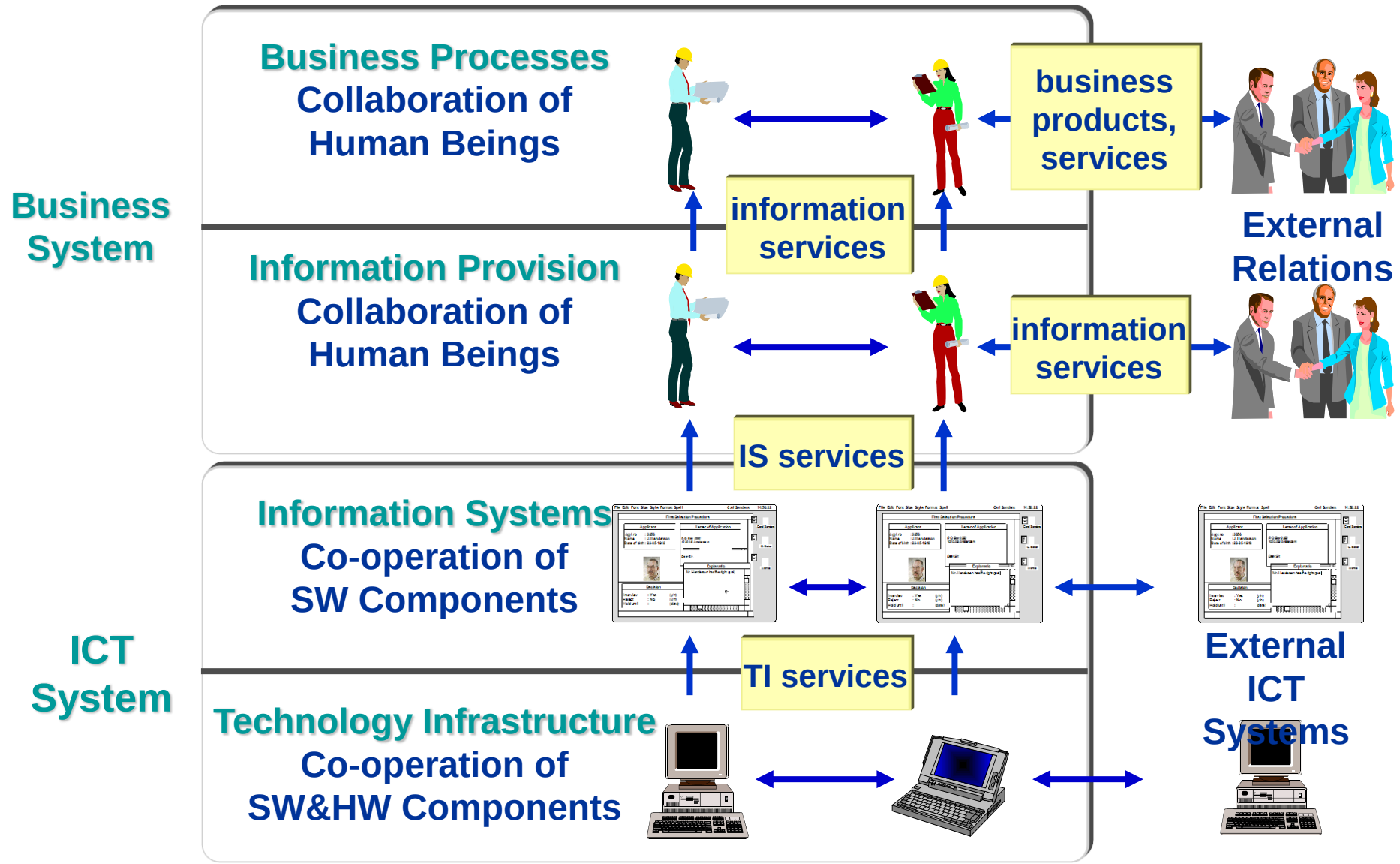
- เฝ้าติดตาม วัดผล และประเมินประสิทธิภาพและความสอดคล้องในการดำเนินงาน
- เฝ้าติดตาม วัดผล และประเมินระบบการควบคุมภายใน
- เฝ้าติดตาม วัดผล และประเมินการปฏิบัติตามข้อกำหนดจากหน่วยงานภายนอก

Integrated Architecture Framework (IAF) and Enterprise + ICT Risk -> Impact



Adopt and Adapt from IAF

The ICT enabled Enterprise and control by design



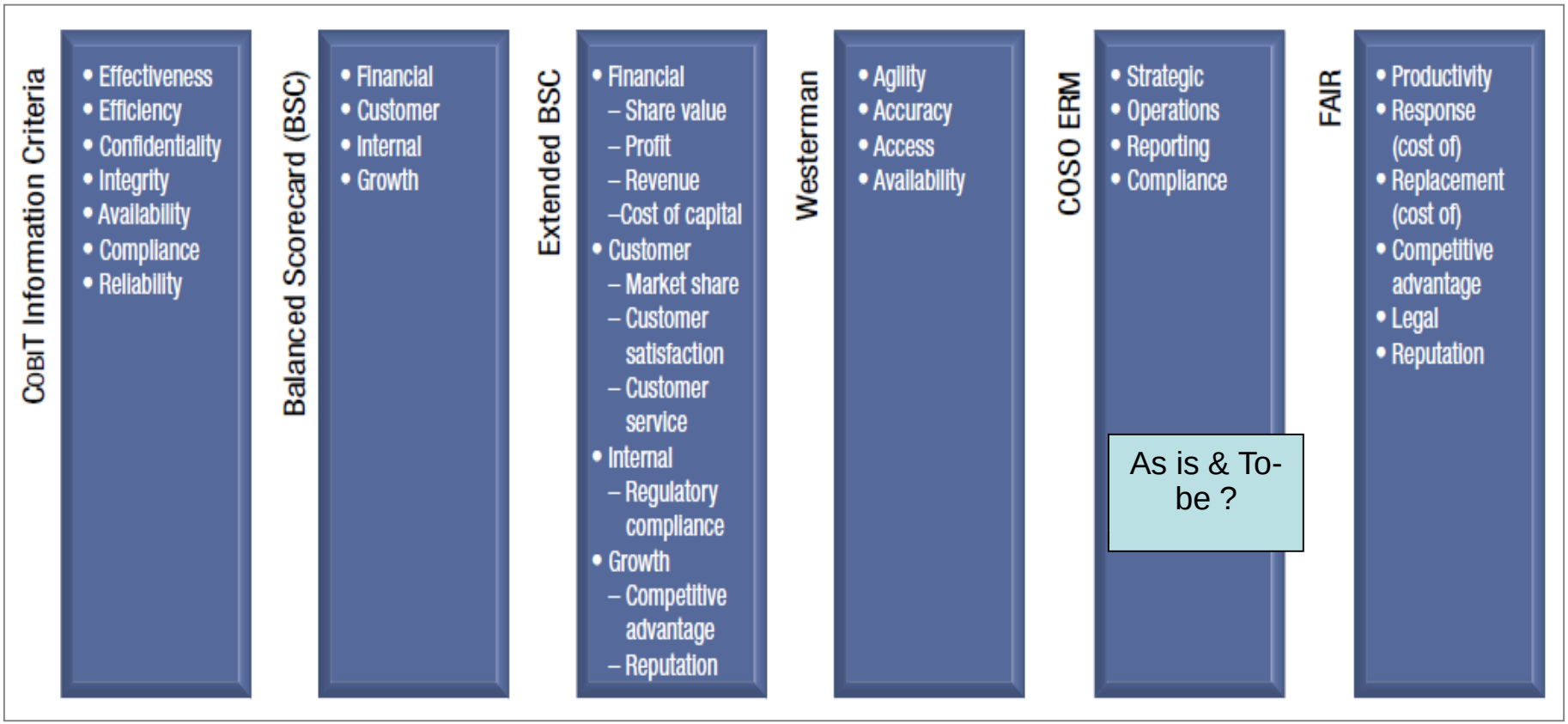
Adopt and Adapt from IAF

GRC & Risk IT Practitioner Guide

EXPRESSING AND DESCRIBING RISK

Where Mgmt. & Related Risk –Control-Audit Should be ?

Expressing IT Risk in Business Terms



The link between IT risk scenarios and ultimate business impact needs to be established to understand the effects of adverse events. Several techniques and options exist that can help the enterprise to describe IT risk in business terms. The Risk IT framework requires that IT risks be translated/expressed into business relevant terms, but does not prescribe any single method. Some available methods are shown in **figure 23** and they are briefly discussed in the remainder of this section.

Source : ISACA

IT Governance and IT Management for Value Creation->

Risk Governance & Controls

Risk is not always to be avoided. Doing business is about taking risk that is consistent with the risk appetite, i.e., many business propositions require IT risk to be taken to achieve the value proposition and realise enterprise goals and objectives, and this risk should be managed but not necessarily avoided.

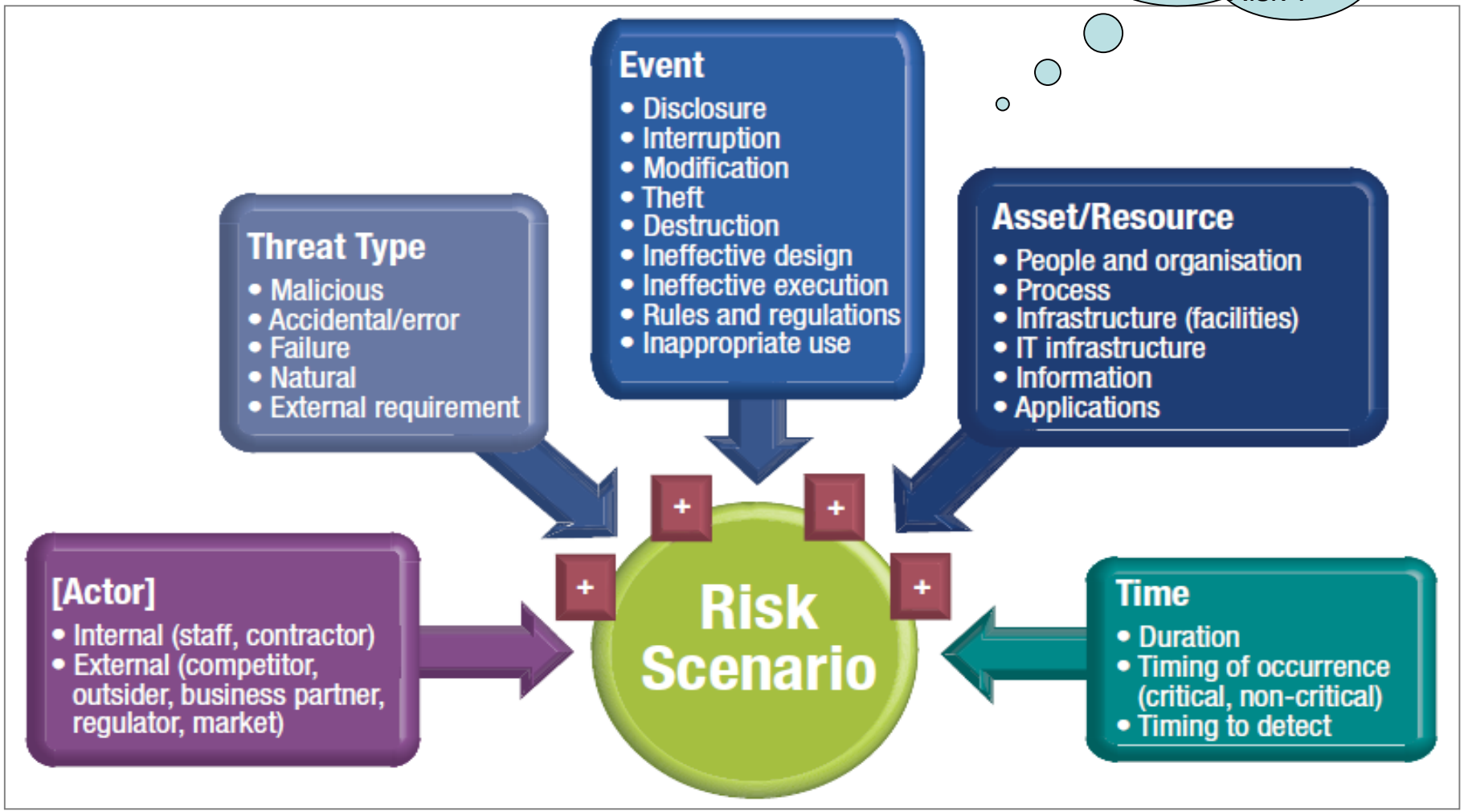
When risk is referenced in *COBIT 5 for Risk*, it is the **current** risk. The concept of inherent risk is rarely used in *COBIT 5 for Risk*. **Figure 7** shows how inherent, current and residual risk interrelate. Theoretically, *COBIT 5 for Risk* focuses on current risk because, in practice, that is what is used.

Figure 7—Interrelationship of Inherent, Current and Residual Risk

RISK SCENARIOS

What could be happened without identify IT Risk & it Impacts to Business Risk ?

IT Risk Scenario Components



Source : ISACA

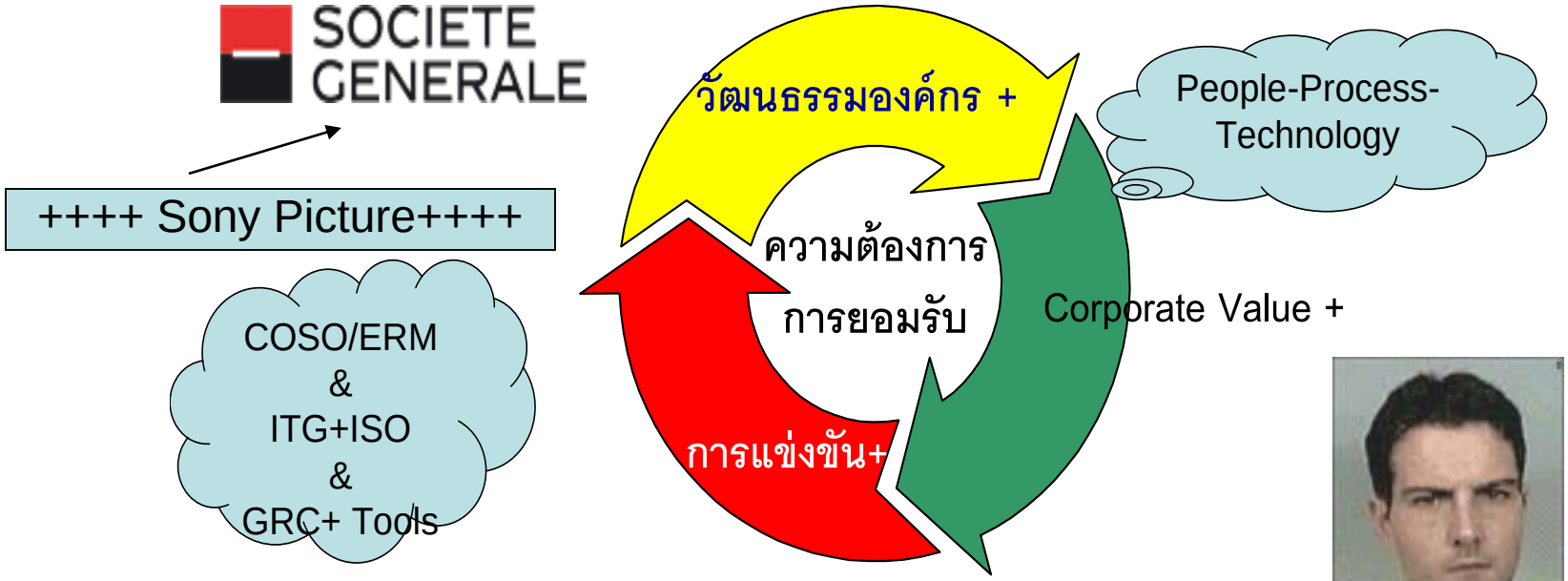
GRC : Value Creation & Lesson Learned

บทเรียน จากการ ทุจริต 340,000.00 ล้านบาท ทางด้าน IT Risk

ของธนาคาร โซซิเอเต้ เจเนอราล [Soc Gen]/ ฝรั่งเศส/ Jan.08

SOCIETE GENERALE

++++ Sony Picture++++

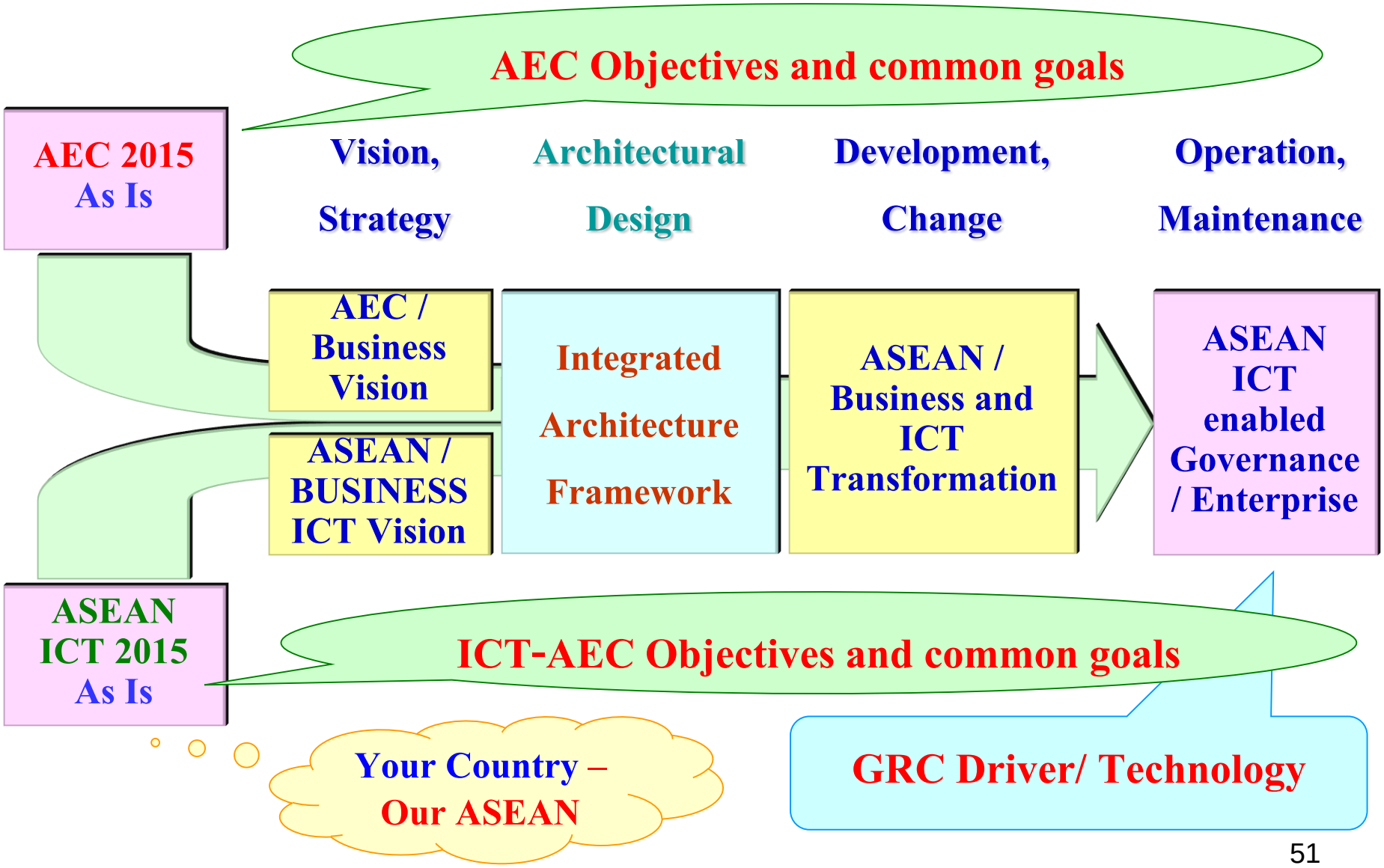


❖ความรู้ ความเข้าใจในกระบวนการ / ขั้นตอน ระบบงาน การตรวจสอบและ การควบคุมภายใน + ของนาย Kerviel ผู้บริหาร และ คณะกรรมการต่างๆ

ร่วมกันทบทวน กำหนด นโยบาย กลยุทธ กระบวนการทำงาน++ จากบทเรียนนี้

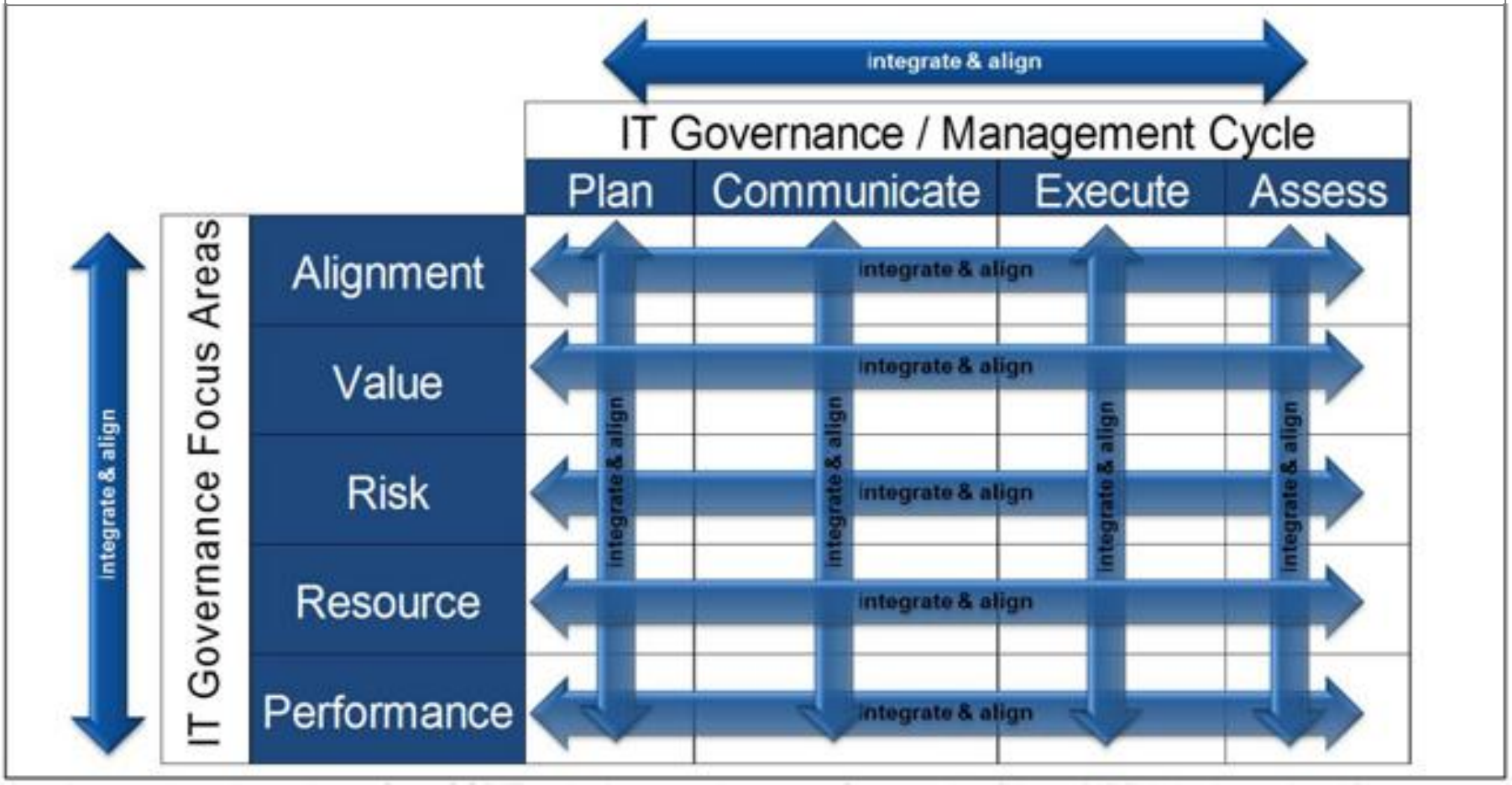
Source: www.itgthailand.com

ICT Enabled Governance and The Role of ICT



COBIT5/GRC – Integrated Management / monitoring and Control

Activity Integration and Alignment Matrix



52

Resource : ISACA

A Business Framework for the Governance and Management of Enterprise IT

COBIT 5 Enterprise Goals / Business BSC

BSC Dimension	Enterprise Goal	Relation to Governance Objectives		
		Benefits Realisation	Risk Optimisation	Resource Optimisation
Financial	1. Stakeholder value of business investments	P		S
	2. Portfolio of competitive products and services	P	P	S
	3. Managed business risk (safeguarding of assets)		P	S
	4. Compliance with external laws and regulations		P	
	5. Financial transparency	P	S	S
Customer	6. Customer-oriented service culture	P		S
	7. Business service continuity and availability		P	
	8. Agile responses to a changing business environment	P		S
	9. Information-based strategic decision making	P	P	P
	10. Optimisation of service delivery costs	P		P
Internal	11. Optimisation of business process functionality	P		P
	12. Optimisation of business process costs	P		P
	13. Managed business change programmes	P	P	S
	14. Operational and staff productivity	P		P
	15. Compliance with internal policies		P	
Learning and Growth	16. Skilled and motivated people	S	P	P
	17. Product and business innovation culture	P		

Performance approaches

Resource : ISACA

STAKEHOLDER NEEDS AND ENTERPRISE GOALS

Mapping COBIT 5 Enterprise Goals to Governance and Management Questions

Criterias Scope & deliverable

STAKEHOLDER NEEDS	1. Stakeholder value of business investments	2. Portfolio of competitive products and services	3. Managed business risk (safeguarding of assets)	4. Compliance with external laws and regulations	5. Financial transparency	6. Customer-oriented service culture	7. Business service continuity and availability	8. Agile responses to a changing business environment	9. Information-based strategic decision making	10. Optimisation of service delivery costs	11. Optimisation of business process functionality	12. Optimisation of business process costs	13. Managed business change programmes	14. Operational and staff productivity	15. Compliance with internal policies	16. Skilled and motivated people	17. Product and business innovation culture
How do I get value from the use of IT? Are end users satisfied with the quality of the IT service?	■	■				■	■						■			■	■
How do I manage performance of IT?		■			■				■	■	■	■		■			
How can I best exploit new technology for new strategic opportunities?	■	■						■					■			■	■
How do I best build and structure my IT department?								■		■	■	■		■	■	■	
How dependent am I on external providers? How well are IT outsourcing agreements being managed? How do I obtain assurance over external providers?			■	■						■							
What are the (control) requirements for information?				■					■						■		
Did I address all IT-related risk?			■				■		■						■		

Resource : ISACA

STAKEHOLDER NEEDS AND ENTERPRISE GOALS

Mapping COBIT 5 Enterprise Goals to Governance and Management Questions (cont.)

Criterias Scope & deliverable

STAKEHOLDER NEEDS	1. Stakeholder value of business investments	2. Portfolio of competitive products and services	3. Managed business risk (safeguarding of assets)	4. Compliance with external laws and regulations	5. Financial transparency	6. Customer-oriented service culture	7. Business service continuity and availability	8. Agile responses to a changing business environment	9. Information-based strategic decision making	10. Optimisation of service delivery costs	11. Optimisation of business process functionality	12. Optimisation of business process costs	13. Managed business change programmes	14. Operational and staff productivity	15. Compliance with internal policies	16. Skilled and motivated people	17. Product and business innovation culture
Am I running an efficient and resilient IT operation?					■		■										
How do I control the cost of IT? How do I use IT resources in the most effective and efficient manner? What are the most effective and efficient sourcing options?										■		■		■			
Do I have enough people for IT? How do I develop and maintain their skills, and how do I manage their performance?										■		■		■			
How do I get assurance over IT?				■											■		
Is the information I am processing well secured?				■			■								■		
How do I improve business agility through a more flexible IT environment?	■							■								■	■

Resource : ISACA

STAKEHOLDER NEEDS AND ENTERPRISE GOALS

Mapping COBIT 5 Enterprise Goals to Governance and Management Questions (cont.)

Criterias Scope & deliverable

STAKEHOLDER NEEDS	1. Stakeholder value of business investments	2. Portfolio of competitive products and services	3. Managed business risk (safeguarding of assets)	4. Compliance with external laws and regulations	5. Financial transparency	6. Customer-oriented service culture	7. Business service continuity and availability	8. Agile responses to a changing business environment	9. Information-based strategic decision making	10. Optimisation of service delivery costs	11. Optimisation of business process functionality	12. Optimisation of business process costs	13. Managed business change programmes	14. Operational and staff productivity	15. Compliance with internal policies	16. Skilled and motivated people	17. Product and business innovation culture
Do IT projects fail to deliver what they promised—and if so, why? Is IT standing in the way of executing the business strategy?	■	■	■					■			■	■	■				
How critical is IT to sustaining the enterprise? What do I do if IT is not available?	■	■					■										
What concrete vital primary business processes are dependent on IT, and what are the requirements of business processes?	■	■									■	■					
What has been the average overrun of the IT operational budgets? How often and how much do IT projects go over budget?					■					■		■		■			

Resource : ISACA

STAKEHOLDER NEEDS AND ENTERPRISE GOALS

Mapping COBIT 5 Enterprise Goals to Governance and Management Questions (cont.)

Criterias Scope & deliverable

STAKEHOLDER NEEDS	1. Stakeholder value of business investments	2. Portfolio of competitive products and services	3. Managed business risk (safeguarding of assets)	4. Compliance with external laws and regulations	5. Financial transparency	6. Customer-oriented service culture	7. Business service continuity and availability	8. Agile responses to a changing business environment	9. Information-based strategic decision making	10. Optimisation of service delivery costs	11. Optimisation of business process functionality	12. Optimisation of business process costs	13. Managed business change programmes	14. Operational and staff productivity	15. Compliance with internal policies	16. Skilled and motivated people	17. Product and business innovation culture
How much of the IT effort goes to fighting fires rather than to enabling business improvements?		■	■									■					
Are sufficient IT resources and infrastructure available to meet required enterprise strategic objectives?		■			■					■		■					
How long does it take to make major IT decisions?	■	■			■			■									
Are the total IT effort and investments transparent?		■		■	■										■		
Does IT support the enterprise in complying with regulations and service levels? How do I know whether I am compliant with all applicable regulations?				■											■		

Resource : ISACA

DETAILED MAPPING ENTERPRISE GOALS — IT-RELATED GOALS

Mapping COBIT 5 Enterprise Goals to IT-related Goals

Criterias Scope & deliverable

		IT-related Goal	Enterprise Goal																
			Stakeholder value of business investments	Portfolio of competitive products and services	Managed business risk (safeguarding of assets)	Compliance with external laws and regulations	Financial transparency	Customer-oriented service culture	Business service continuity and availability	Agile responses to a changing business environment	Information-based strategic decision making	Optimisation of service delivery costs	Optimisation of business process functionality	Optimisation of business process costs	Managed business change programmes	Operational and staff productivity	Compliance with internal policies	Skilled and motivated people	Product and business innovation culture
			1.	2.	3.	4.	5.	6.	7.	8.	9.	10.	11.	12.	13.	14.	15.	16.	17.
			Financial					Customer					Internal					Learning and Growth	
Financial	01	Alignment of IT and business strategy	P	P	S			P	S	P	P	S	P	S	P			S	S
	02	IT compliance and support for business compliance with external laws and regulations			S	P											P		
	03	Commitment of executive management for making IT-related decisions	P	S	S					S	S		S		P			S	S
	04	Managed IT-related business risk			P	S			P	S		P			S		S	S	
	05	Realised benefits from IT-enabled investments and services portfolio	P	P				S		S		S	S	P		S			S
	06	Transparency of IT costs, benefits and risk	S		S		P				S	P		P					
Customer	07	Delivery of IT services in line with business requirements	P	P	S	S		P	S	P	S		P	S	S			S	S
	08	Adequate use of applications, information and technology solutions	S	S	S			S	S		S	S	P	S		P		S	S
Internal	09	IT agility	S	P	S			S		P			P		S	S		S	P
	10	Security of information, processing infrastructure and applications			P	P			P								P		
	11	Optimisation of IT assets, resources and capabilities	P	S						S		P	S	P	S	S			S
	12	Enablement and support of business processes by integrating applications and technology into business processes	S	P	S			S		S		S	P	S	S	S			S
	13	Delivery of programmes delivering benefits, on time, on budget, and meeting requirements and quality standards	P	S	S			S				S		S	P				
	14	Availability of reliable and useful information for decision making	S	S	S	S			P		P		S						
	15	IT compliance with internal policies			S	S											P		
Learning and Growth	16	Competent and motivated business and IT personnel	S	S	P			S		S						P		P	S
	17	Knowledge, expertise and initiatives for business innovation	S	P				S		P	S		S		S			S	P

Resource : ISACA

DETAILED MAPPING ENTERPRISE GOALS — IT-RELATED GOALS

Mapping COBIT 5 Enterprise Goals to IT-related Goals

Criterias Scope & deliverable

		IT-related Goal	Enterprise Goal																
			1. Stakeholder value of business investments	2. Portfolio of competitive products and services	3. Managed business risk (safeguarding of assets)	4. Compliance with external laws and regulations	5. Financial transparency	6. Customer-oriented service culture	7. Business service continuity and availability	8. Agile responses to a changing business environment	9. Information-based strategic decision making	10. Optimisation of service delivery costs	11. Optimisation of business process functionality	12. Optimisation of business process costs	13. Managed business change programmes	14. Operational and staff productivity	15. Compliance with internal policies	16. Skilled and motivated people	17. Product and business innovation culture
			Financial					Customer					Internal					Learning and Growth	
Financial	01	Alignment of IT and business strategy	P	P	S			P	S	P	P	S	P	S	P			S	S
Financial	02	IT compliance and support for business compliance with external laws and regulations			S	P											P		
Financial	03	Commitment of executive management for making IT-related decisions	P	S	S					S	S		S		P			S	S
Financial	04	Managed IT-related business risk			P	S			P	S		P			S		S	S	
Financial	05	Realised benefits from IT-enabled investments and services portfolio	P	P				S		S		S	S	P		S			S
Financial	06	Transparency of IT costs, benefits and risk	S		S		P				S	P		P					
Customer	07	Delivery of IT services in line with business requirements	P	P	S	S		P	S	P	S		P	S	S			S	S
Customer	08	Adequate use of applications, information and technology solutions	S	S	S			S	S		S	S	P	S		P		S	S

Resource : ISACA

DETAILED MAPPING ENTERPRISE GOALS — IT-RELATED GOALS

Mapping COBIT 5 Enterprise Goals to IT-related Goals (Cont.)

Criterias Scope & deliverable

		IT-related Goal	Enterprise Goal: 1. Stakeholder value of business investments	2. Portfolio of competitive products and services	3. Managed business risk (safeguarding of assets)	4. Compliance with external laws and regulations	5. Financial transparency	6. Customer-oriented service culture	7. Business service continuity and availability	8. Agile responses to a changing business environment	9. Information-based strategic decision making	10. Optimisation of service delivery costs	11. Optimisation of business process functionality	12. Optimisation of business process costs	13. Managed business change programmes	14. Operational and staff productivity	15. Compliance with internal policies	16. Skilled and motivated people	17. Product and business innovation culture
			Financial					Customer					Internal					Learning and Growth	
Internal	09	IT agility	S	P	S			S		P			P		S	S		S	P
Internal	10	Security of information, processing infrastructure and applications			P	P			P								P		
Internal	11	Optimisation of IT assets, resources and capabilities	P	S						S		P	S	P	S	S			S
Internal	12	Enablement and support of business processes by integrating applications and technology into business processes	S	P	S			S		S		S	P	S	S	S			S
Internal	13	Delivery of programmes delivering benefits, on time, on budget, and meeting requirements and quality standards	P	S	S			S				S		S	P				
Internal	14	Availability of reliable and useful information for decision making	S	S	S	S			P		P		S						
Internal	15	IT compliance with internal policies			S	S											P		
Learning and Growth	16	Competent and motivated business and IT personnel	S	S	P			S		S						P		P	S
Learning and Growth	17	Knowledge, expertise and initiatives for business innovation	S	P				S		P	S		S		S			S	P

Resour

Risk: a definition

Understanding Risk

- Risk = the effect of uncertainty upon objectives
- Objectives can be whole of organisation, Hospital, Faculty, School, Division, program, etc

Strategic objectives

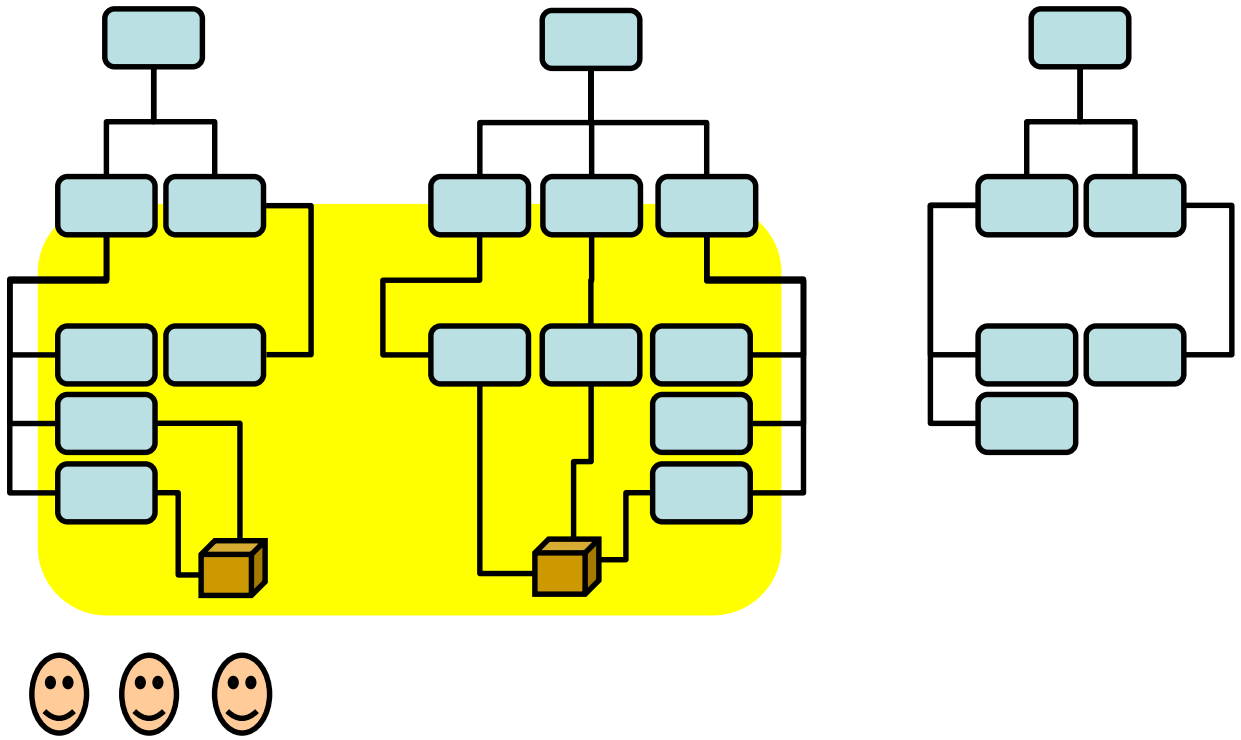
Operational objectives

Process objectives

Project objectives

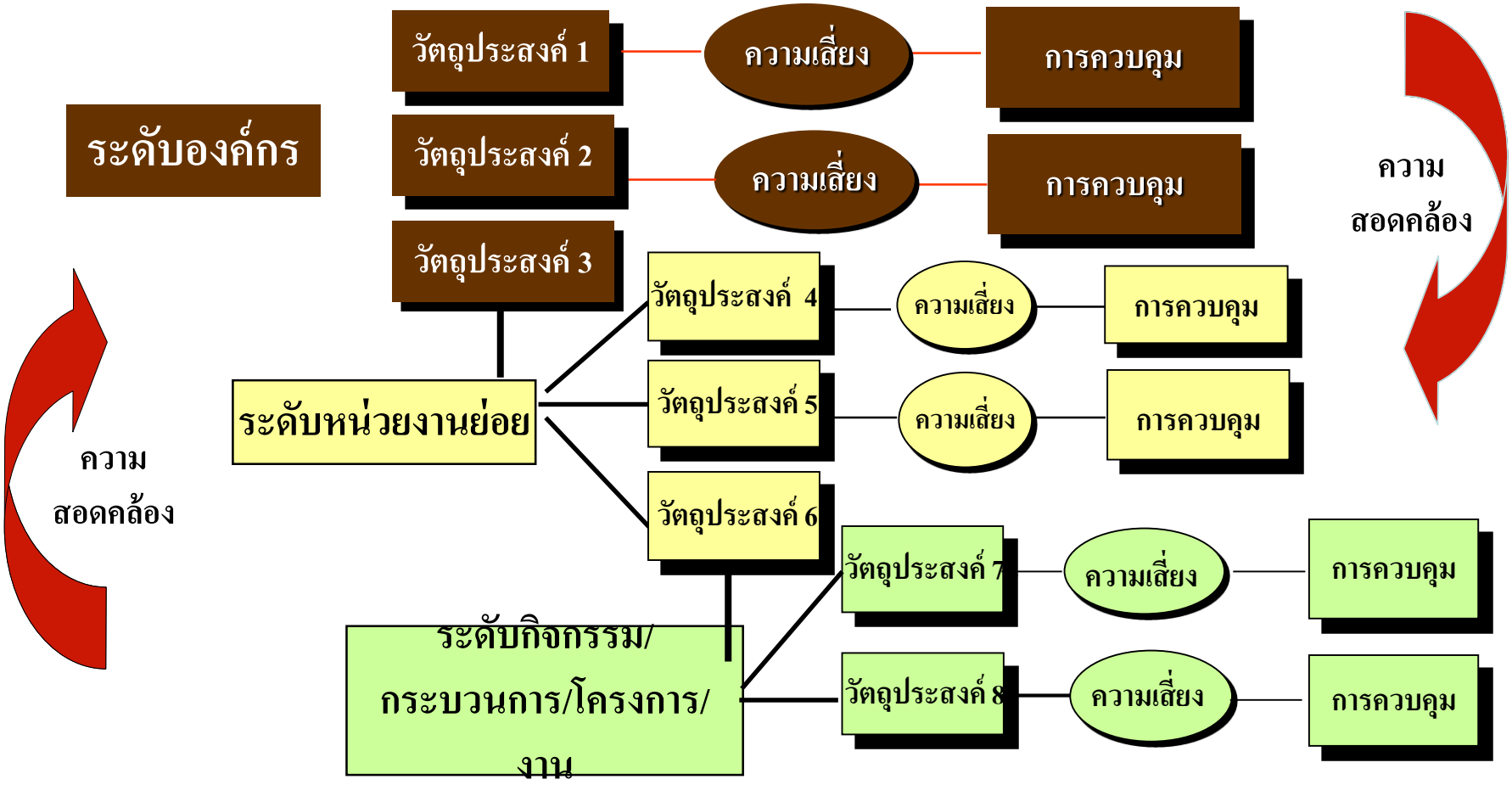
Product objectives

Personal objectives



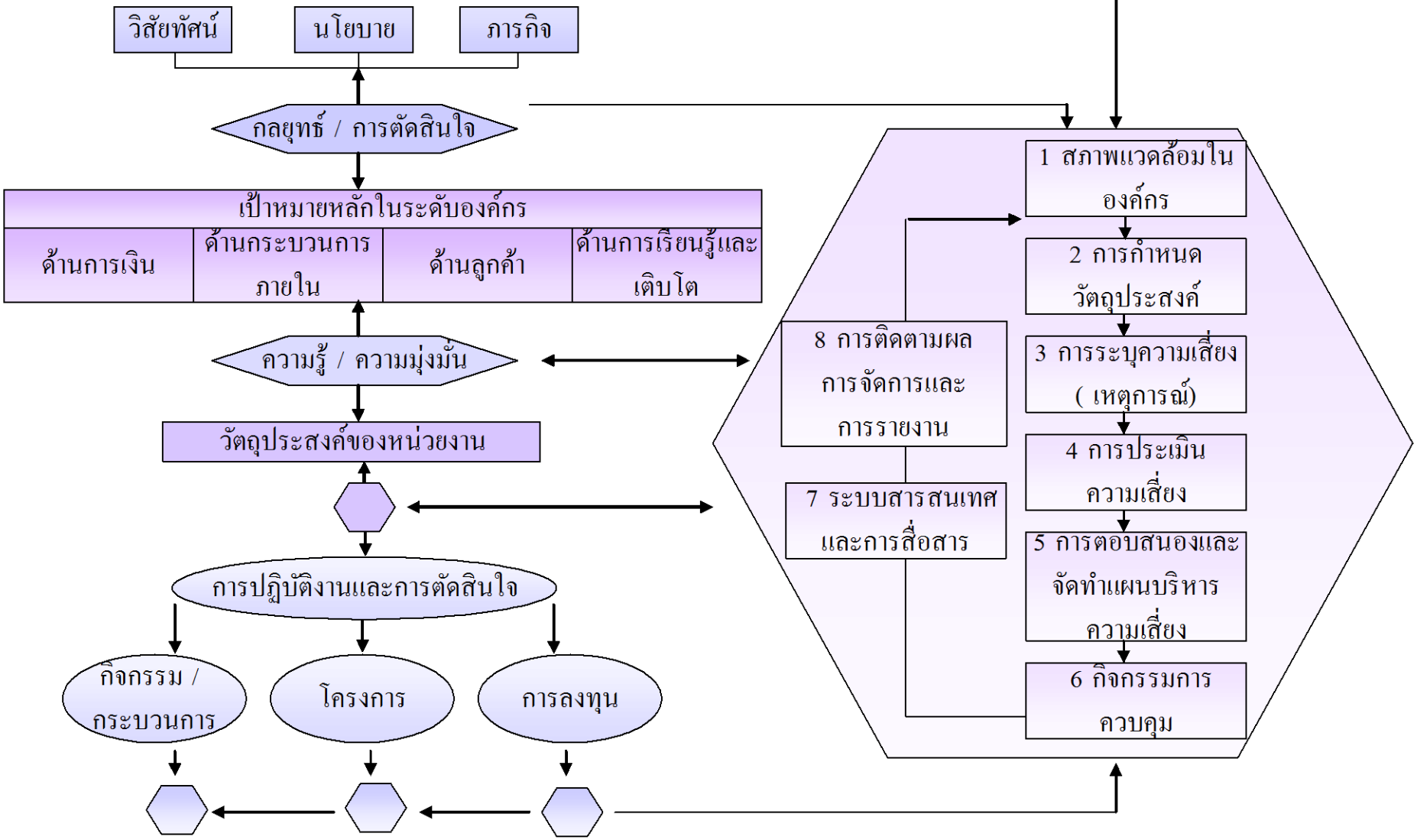
องค์ประกอบของ ERM- Enterprise Risk Management

การกำหนดวัตถุประสงค์ (Objective Setting)



แนวทางการบริหารความเสี่ยงแบบบูรณาการขององค์กร

การนำการบริหารความเสี่ยงไปปฏิบัติ



บทบาทหน้าที่ความรับผิดชอบตามโครงสร้าง

ทบทวน Business & ICT Risk

ผู้รับผิดชอบ	ขั้นตอนการดำเนินการ

สื่อสารและสร้างความตระหนักเพื่อให้เกิดการปฏิบัติทั่วทั้งองค์กร

1.คณะกรรมการ

2. คณะกรรมการตรวจสอบ

3.คณะกรรมการบริหารความเสี่ยง

4.ผู้บริหาร

5. คณะทำงานบริหารความเสี่ยง

6. ผู้ประสานงานความเสี่ยงหน่วยงาน

7.ผู้ปฏิบัติงาน

องค์กร

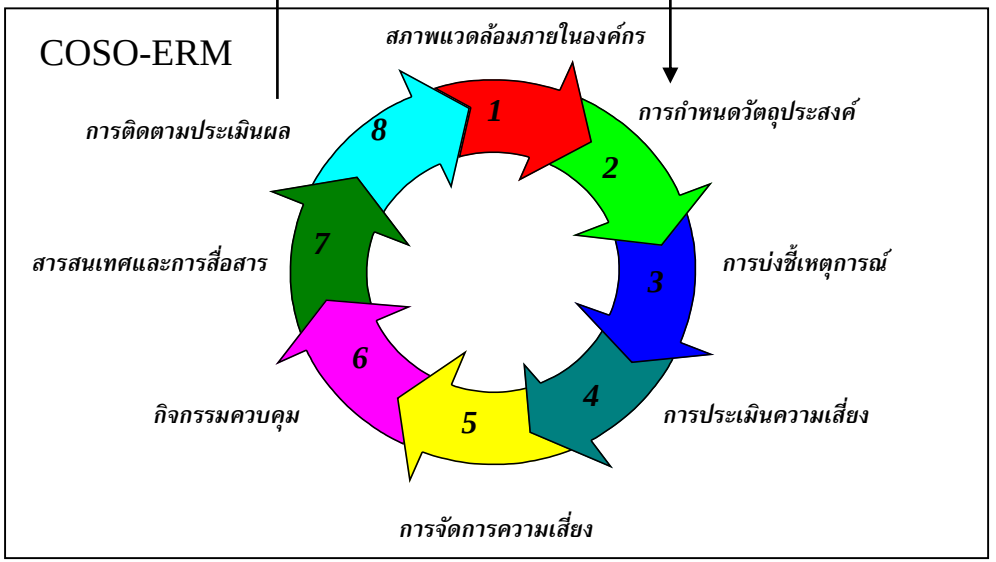
หน่วยงาน

กำหนดนโยบายด้านบริหารความเสี่ยง

อนุมัติแผนปฏิบัติงานประจำปี

กำกับดูแลและติดตามผลการปฏิบัติงานตามนโยบายการบริหารความเสี่ยง

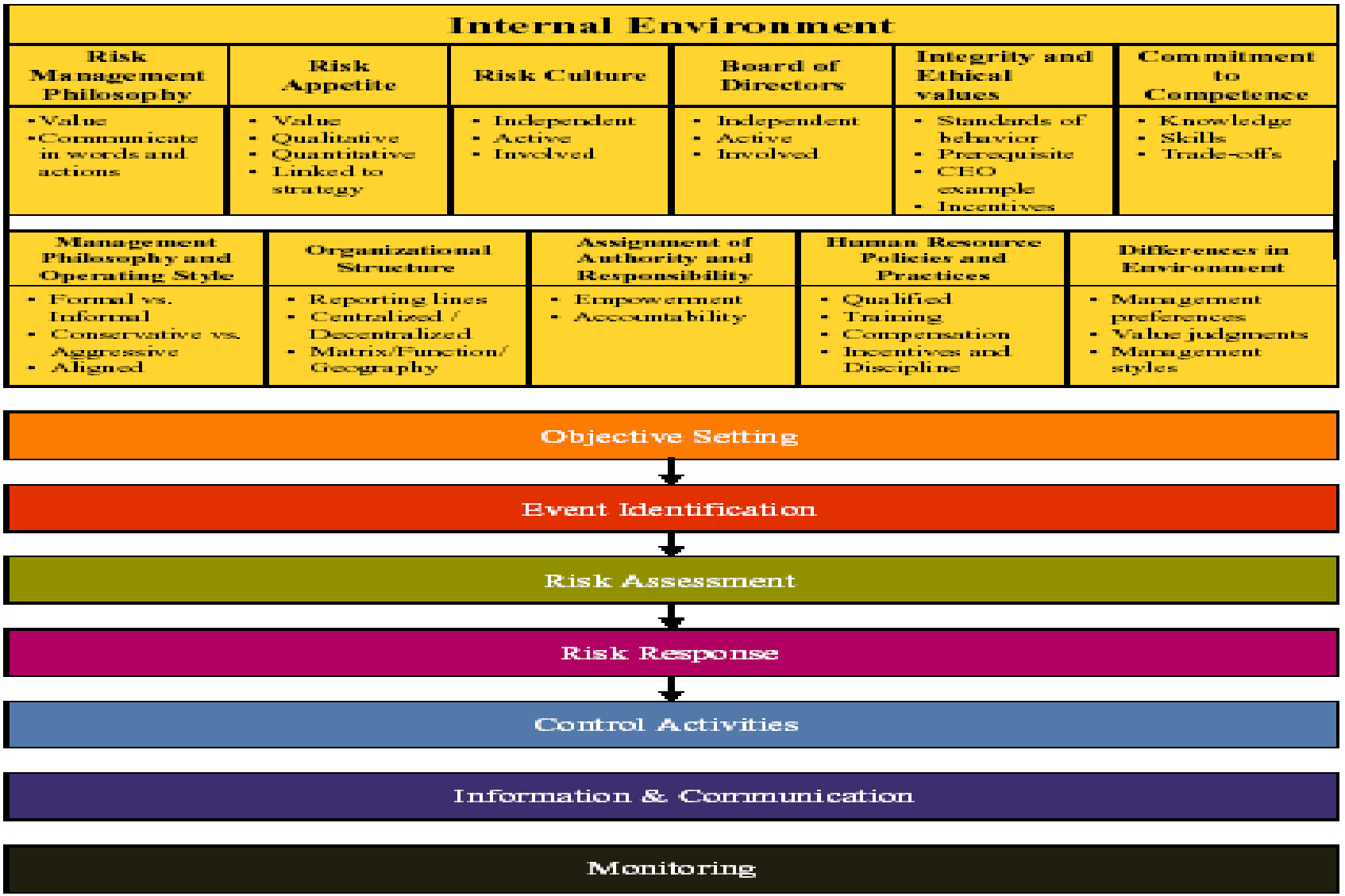
ให้ข้อเสนอแนะเกี่ยวกับนโยบายการบริหารความเสี่ยงโดยรวม กรอบการบริหารความเสี่ยง และแผนปฏิบัติงานประจำปี



กำกับดูแล ติดตามผลการปฏิบัติงานตามนโยบายและแผนการบริหารความเสี่ยง

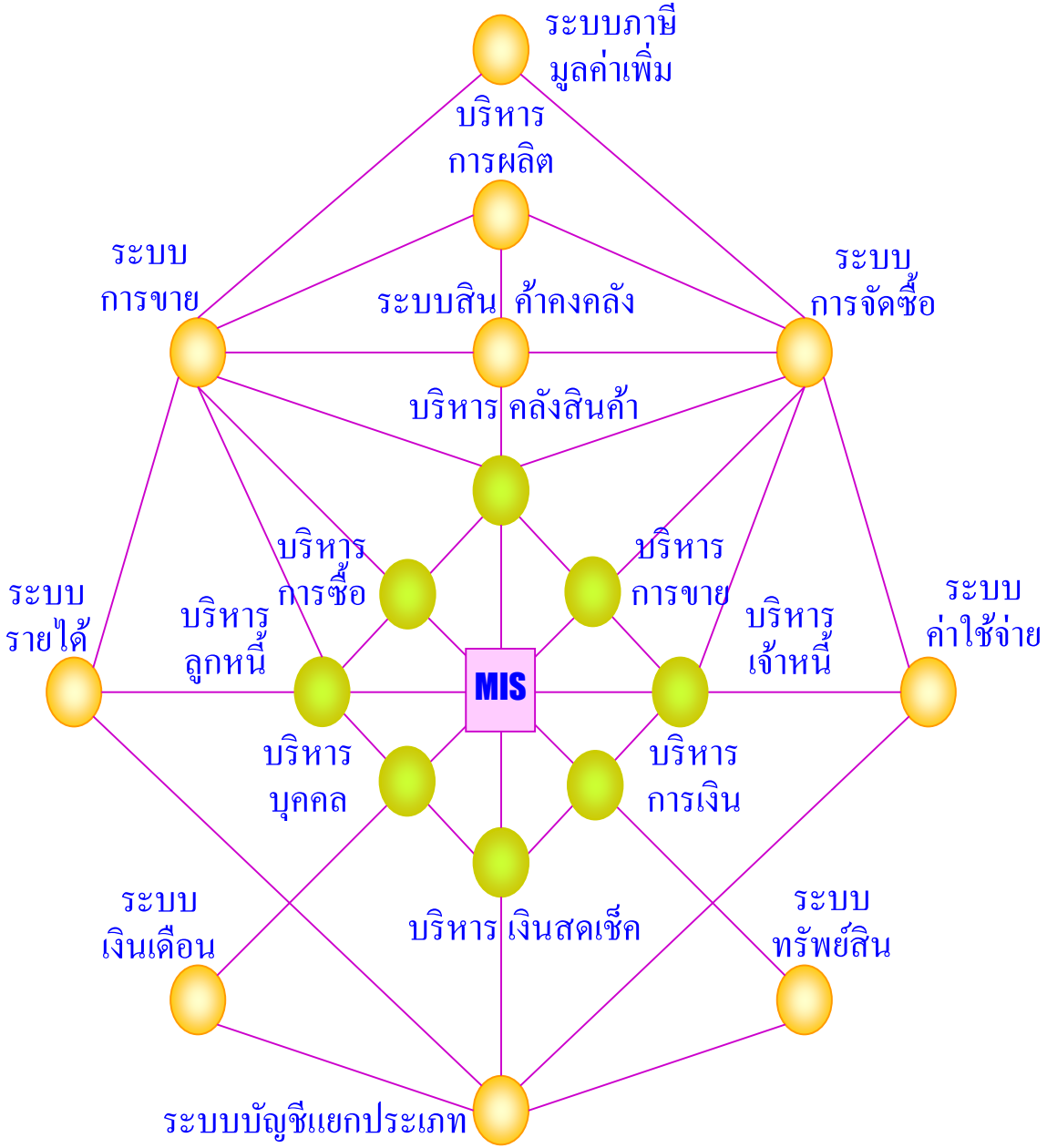
New COSO-ERM Framework

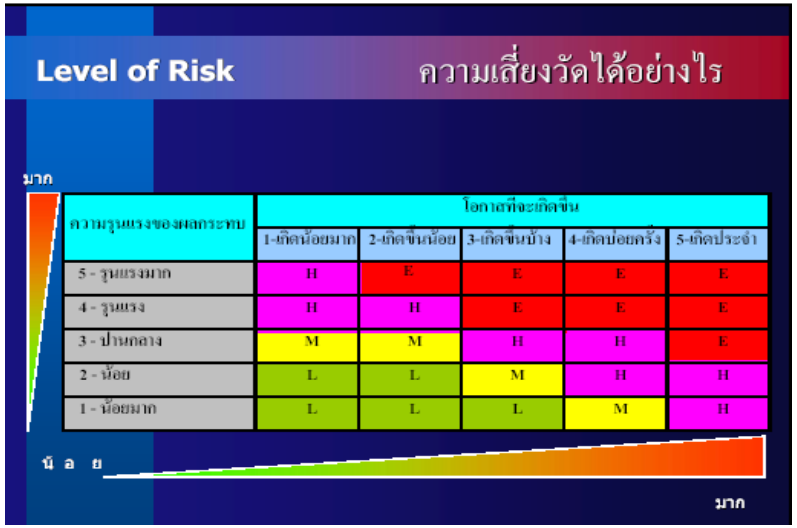
Exhibit 3.1



ที่มา: COSO-ERM

การบริหารจัดการองค์กรแบบบูรณาการกับการตรวจสอบ IT – Non IT



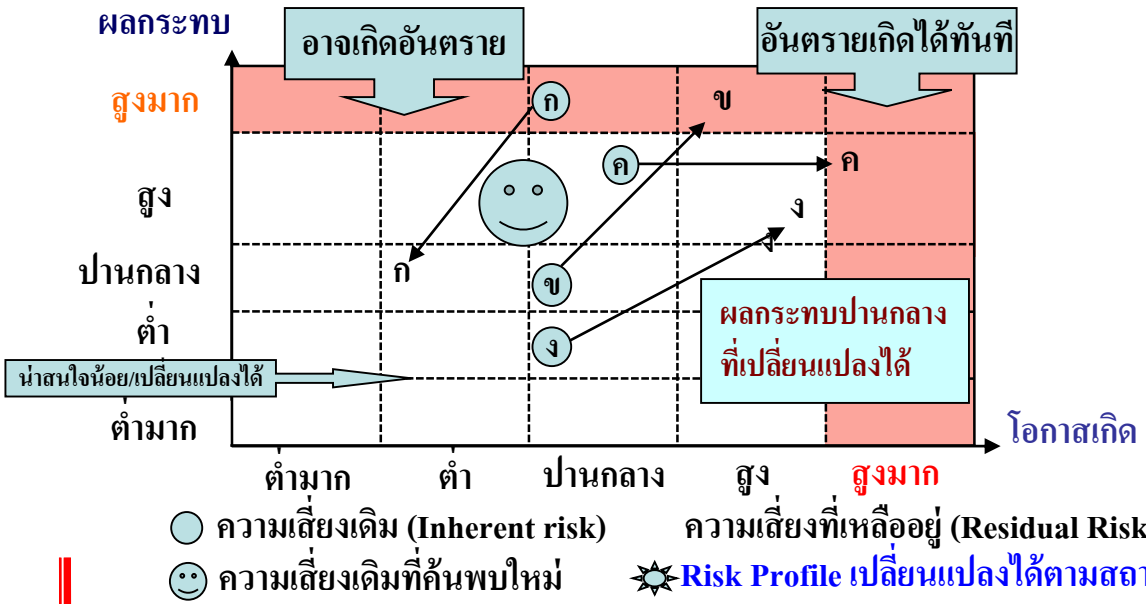


รูปแบบอื่น ๆ ของ Risk Appetite

ข้อสังเกต

- เป็นการยอมรับความเสี่ยงที่เป็นความเห็นของผู้บริหารระดับสูงหรือคณะกรรมการ
- มีการกำหนดเกณฑ์ในการประเมินความเสี่ยงอย่างไร ทั้งในด้านโกาสเกิดและผลกระทบ
- เกณฑ์ในการจัดลำดับความสำคัญดังกล่าวสามารถแสดงถึง Risk Appetite ขององค์กรได้

แผนผัง/โครงร่าง ความเสี่ยง(Risk Profile)



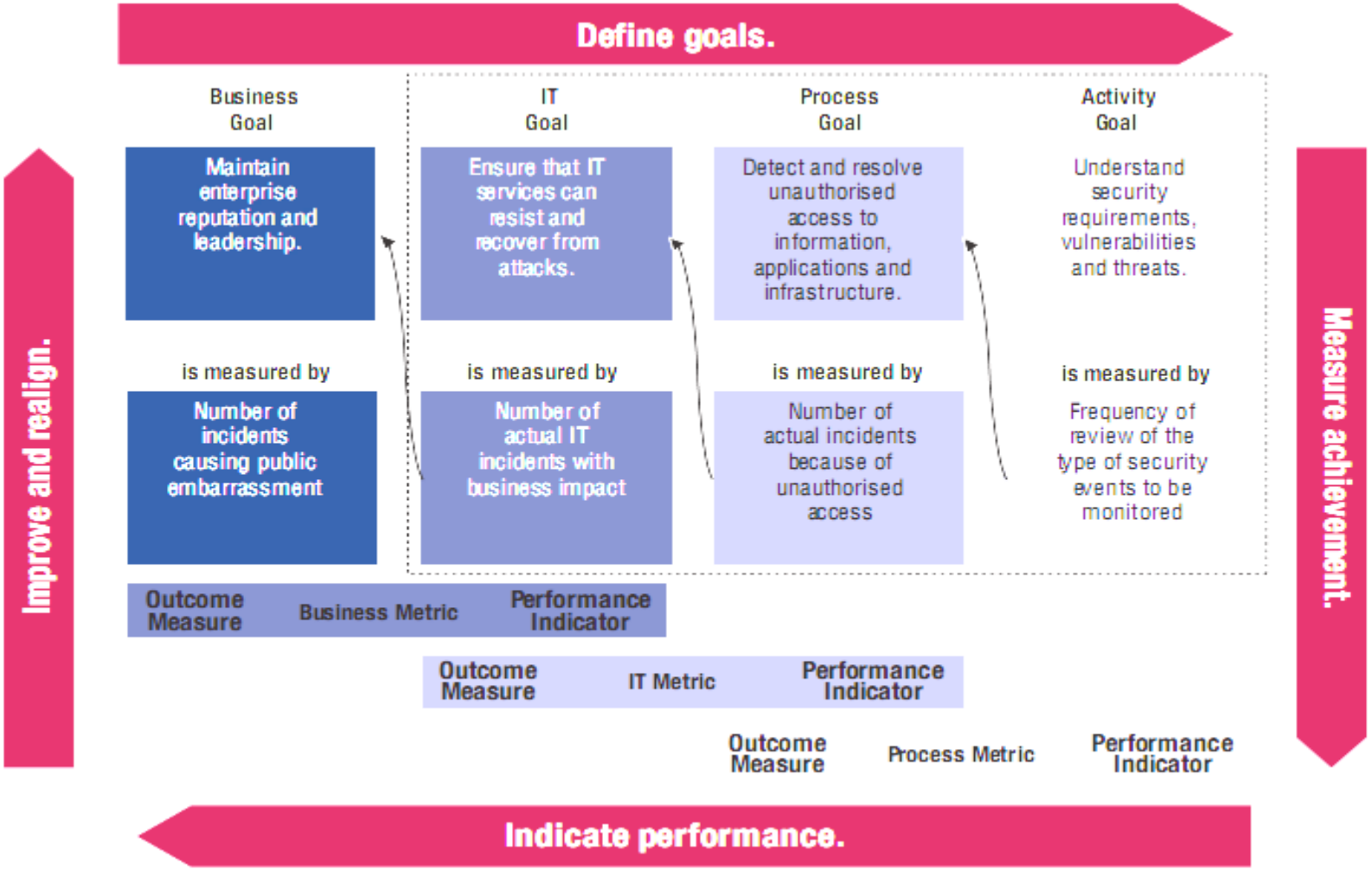
ความเสี่ยงเดิม (Inherent risk)
ความเสี่ยงที่เหลืออยู่ (Residual Risk)
ความเสี่ยงเดิมที่ค้นพบใหม่
Risk Profile เปลี่ยนแปลงได้ตามสถานการณ์

เป้าหมายหลักของการบริหารความเสี่ยง คือ การทำให้องค์กรมั่นใจว่าระดับความเสี่ยงที่องค์กรเผชิญอยู่สอดคล้องกับระดับความเสี่ยงที่องค์กรยอมรับได้ เพื่อให้สามารถบรรลุวัตถุประสงค์

CobiT 4.1 -> COBIT 5

GRC & CobiT Framework

Relationship Amongst Process, Goals and Metrics



Resource : IT Governance Institute


Risk *is a natural part of the business landscape.*
If left unmanaged, the uncertainty can spread like weeds.
If managed effectively, losses can be avoided and benefits obtained.
data leak
opportunity
exposure
challenges
threat
possibility
prospect
GRC Perspectives
IT Risk is Business Risk
RISK IT
BASED ON COBIT®
A set of guiding principles and the first framework to help enterprises identify, govern and effectively manage IT risk.
ISACA®

GRC - COBIT & Risk IT and IT Risk Perspective

What does Risk IT do?

Risk IT:

- Allows an enterprise to customize the components provided in the framework to suit its particular needs
- Provides a common language to help communication and understanding among business, IT, risk and audit management
- Provides an end-to-end, comprehensive view of all risks related to the use of IT and a similarly thorough treatment of risk management, from the tone and culture at the top, to operational issues
- Enables an enterprise to understand and manage all significant IT risk types
- Allows the enterprise to make appropriate risk-aware decisions
- Explains leveraging an investment in an IT internal control system to manage IT-related risk
- Enables integration of IT risk with overall risk and compliance structures within the enterprise
- Provides tangible business benefits

Source : ISACA

GRC- COBIT & Risk IT and IT Risk Perspective

What are the benefits of using Risk IT?

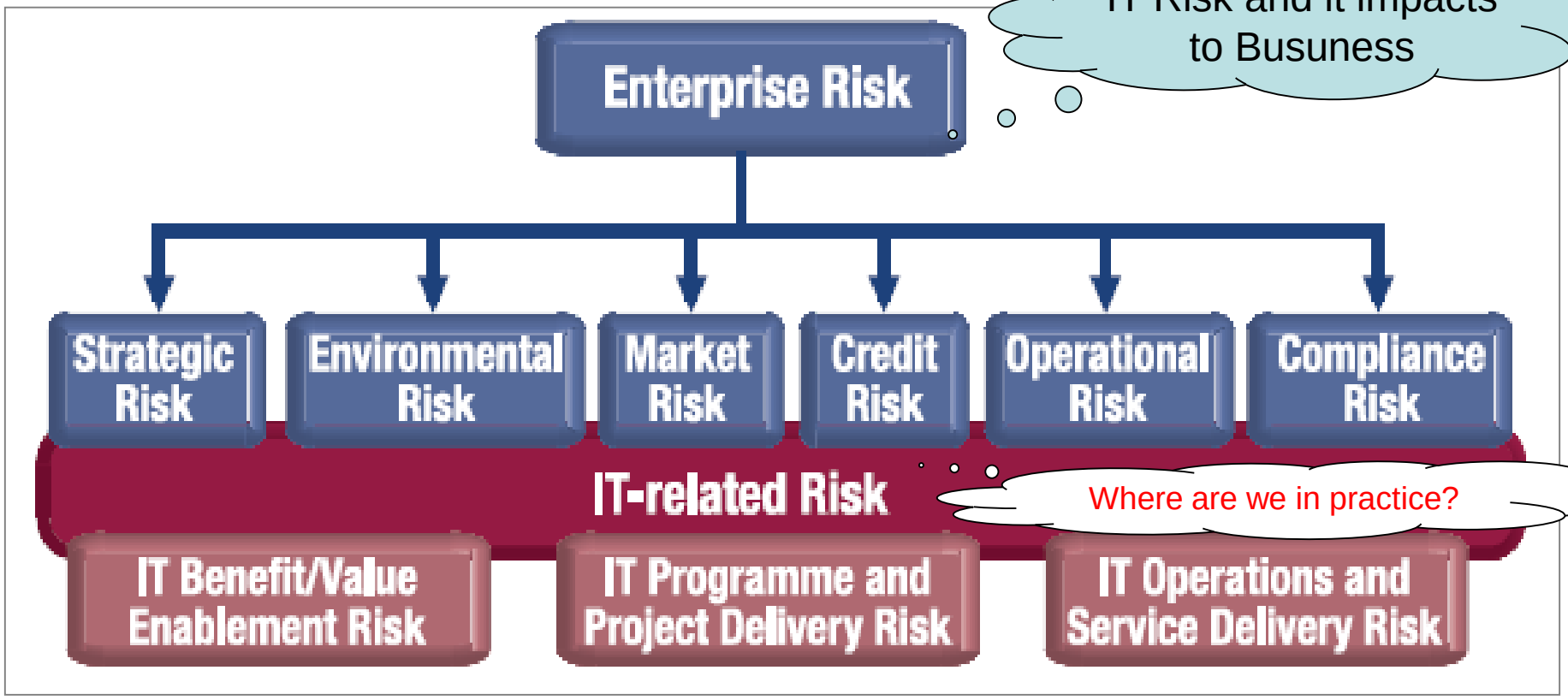
The benefits include:

- Improved communication among business, IT, risk and audit management
- Comprehensive guidance on how to manage IT-related risks
- A complete risk profile to better understand risk, so as to appropriately utilize enterprise resources
- A better understanding of the roles and responsibilities with regard to IT risk management
- Alignment with ERM
- A better view of IT-related risk and its financial implications
- Fewer operational surprises and failures
- Increased information quality
- Greater stakeholder confidence and reduced regulatory concerns
- Innovative applications supporting new business initiatives

Source : ISACA

DEFINING A RISK UNIVERSE AND SCOPING RISK MANAGEMENT

IT Risk in the Risk Hierarchy



Source : ISACA

IT Strategy Committee & IT Steering Committee

	IT STRATEGY COMMITTEE	IT STEERING COMMITTEE
LEVEL	BOARD LEVEL	EXECUTIVE LEVEL

RESPONSIBILITY	• Provides insight and advice to the board on topics such as:
	  • The relevance of developments in IT from a business perspective
	  • The alignment of IT with the business direction
	  • The achievement of strategic IT objectives
	  • The availability of suitable IT resources, skills and infrastructure to meet the strategic objectives
	  • Optimisation of IT costs, including the role and value delivery of external IT sourcing
	  • Risk, return and competitive aspects of IT investments
	  • Progress on major IT projects
	  • The contribution of IT to the business (i.e., delivering the promised business value)
	  • Exposure to IT risks, including compliance risks
	  • Containment of IT risks
	• Provides direction to management relative to IT strategy
		• Decides the overall level of IT spending and how costs will be allocated
		• Aligns and approves the enterprise IT architecture
		• Approves project plans and budgets, setting priorities and milestones
		• Acquires and assigns appropriate resources
		• Ensures projects continuously meet business requirements, including re-evaluation of the business case
		• Monitors project plans for delivery of expected value and desired outcomes, on time and within budget
		• Monitors resource and priority conflict between enterprise divisions and the IT function, and between projects
		• Makes recommendations and requests for changes to strategic plans (priorities, funding, technology approaches, resources, etc.)
		• Communicates strategic goals to project teams
		• Is a major contributor to management's IT governance responsibilities

1.เรามีกรรมการหลายชุด... มีการบูรณาการในการทำงานและแลกเปลี่ยนข้อมูลกันอย่างไร?
2.เรามีหลายหน่วยงาน...มีนโยบายและกลยุทธการบูรณาการอย่างไร?

บทบาทของผู้บริหารและกรรมการมืออาชีพ บางมุมมอง

GRC in COBIT 5 กับการกำกับดูแลที่ไม่ใช่การบริหารจัดการ

- คณะกรรมการมีความรับผิดชอบในการกำกับดูแลกิจการและกำหนดความเสี่ยงที่องค์กรยอมรับได้

- ต้องมีความเป็นผู้นำ มีการตัดสินใจในทางที่จะป้องกันและเพิ่มผลประโยชน์ให้แก่องค์กรอย่างต่อเนื่อง

กรรมการที่เป็นผู้บริหารมีความเข้าใจจริง ๆ หรือไม่ว่า บทบาทของกรรมการที่แท้จริงควรเป็นอย่างไร?

- กรรมการเข้าใจความรับผิดชอบและจุดมุ่งหมายของคณะกรรมการชัดเจนหรือไม่

-กรรมการเข้าใจถ่องแท้หรือไม่ว่า ในฐานะกรรมการควรประพฤติปฏิบัติอย่างไร และหน้าที่ตามกฎหมายมีอะไรบ้าง

- กรรมการเคยศึกษารายละเอียดของหนังสือบริคณห์สนธิและข้อบังคับบริษัทที่ตนเป็นกรรมการอยู่หรือไม่ และทราบหรือไม่ว่าเอกสารเหล่านี้มีไว้เพื่ออะไร

- กรรมการเข้าใจงานต่าง ๆ ที่คณะกรรมการควรแสดงศักยภาพกับงานนั้น ๆ หรือไม่ และทราบหรือไม่ว่าจะเพิ่มพูนศักยภาพนั้น ๆ ได้อย่างไร

- กรรมการสามารถแยกแยะบทบาทของตนในฐานะกรรมการจากบทบาทของผู้บริหารได้หรือไม่

Business Drivers -> + Conformance

กับบทบาทของผู้บริหาร-ผู้ปฏิบัติ

บทบาทของผู้บริหารและกรรมการมืออาชีพ บางมุมมอง

WS – คำถามชวนคุย->ชวนคิด -> เพื่อสร้างคุณค่าเพิ่ม

เกี่ยวกับบทบาทของคณะกรรมการในมุมมองของ GRC in COBIT 5

★ กรรมการมีความเข้าใจชัดเจนหรือไม่ว่าบทบาทการเป็นกรรมการกำหนดให้ “คิดอย่างครอบคลุมและรอบด้าน” ขณะที่บทบาทของการเป็นผู้บริหารเน้น “การลงมือทำให้สำเร็จ” ... จะ Monitoring และ Auditing ที่มีคุณภาพได้อย่างไร

★ ผู้บริหารและกรรมการทุกท่านเข้าใจหน้าที่และความรับผิดชอบทางกฎหมายของตนชัดเจนหรือไม่

★ ผู้บริหารและกรรมการทราบหรือไม่ว่า จุดมุ่งหมายหลักของผู้บริหารและคณะกรรมการคืออะไร

★ ผู้บริหารและกรรมการทราบดีหรือไม่ว่า ต้องปฏิบัติภารกิจอะไรเพื่อบรรลุจุดมุ่งหมายต่าง ๆ ขององค์กร

★ ผู้บริหารและกรรมการตระหนักหรือไม่ว่า คณะกรรมการมีหน้าที่หลัก คือ ทำการตัดสินใจ ซึ่งเป็นบทบาทที่มีความสำคัญอย่างยิ่งในการปกป้องและเพิ่มพูนผลประโยชน์ขององค์กรและผู้ถือหุ้นอย่างต่อเนื่อง ...ส่วนเรื่องอื่นนั้น ให้ถือเป็นการตัดสินใจของฝ่ายบริหาร

★ ท่านและเพื่อนกรรมการตระหนักหรือไม่ว่า ควรทำอย่างไรในกระบวนการตัดสินใจเพื่อทำให้มีโอกาสดีที่สุดในการได้มาซึ่งการตัดสินใจที่ดี ... โดยกระบวนการตัดสินใจดังกล่าว ต้องการการคิดเพื่อพิจารณาทางเลือกและเพื่อประเมินผลลัพธ์ของทางเลือก และตัดสินใจเลือก โดยให้ได้มาซึ่งคุณภาพที่ดีที่สุดใช่หรือไม่

★ มีการกำหนดรายละเอียดเป็นลายลักษณ์อักษรเกี่ยวกับความรับผิดชอบของกรรมการที่เป็นผู้บริหารและกรรมการ ซึ่งมีความแตกต่างกันหรือไม่

★ ผู้บริหารและกรรมการเข้าใจ “Conditioning Tasks” และสามารถทำงานดังกล่าวได้อย่างมีประสิทธิผลหรือไม่

★ ผู้บริหารและกรรมการเข้าใจ “Enterprise Tasks” และสามารถปฏิบัติงานนั้นได้อย่างครอบคลุมหรือไม่

★ ผู้บริหารและกรรมการเข้าใจประเด็นเรื่องการกำกับดูแลกิจการที่อาจส่งผลกระทบต่อองค์กรหรือไม่

บทบาทของผู้บริหารและกรรมการมืออาชีพ บางมุมมอง

การให้ความสำคัญกับกลยุทธ์ และการคาดการณ์ เพื่อการเตรียมพร้อมสำหรับการบริหารความเสี่ยงแบบบูรณาการและการจัดการองค์กรเชิงรุก

การตัดสินใจเกี่ยวกับอนาคตในสิ่งที่จะทำให้ถูกต้องทั้งหมดเป็นเรื่องยาก เป็นความเสี่ยงที่ไม่สามารถประเมินได้ และเป็นเรื่องที่สำคัญที่ผู้บริหารและกรรมการไม่สามารถละเลยได้

ประเด็นคำถามสำคัญ ๆ ที่ผู้บริหารและกรรมการต้องพยายามตอบประเด็นต่าง ๆ เหล่านี้ เพื่อใช้ประกอบแนวทางในการทำงาน และเป็นการเตรียมความพร้อมสำหรับองค์กร

คำถาม + คำแนะนำในมุมมอง GRC

- ☞ องค์กรต้องทำอะไรบ้างเพื่อให้มั่นใจว่าองค์กรยังคงอยู่รอดต่อไปในอนาคต
- ☞ อะไรคือจุดมุ่งหมายขององค์กรทั้งในปัจจุบันและในอนาคต ตามแนวทางของ BSC.
- ☞ องค์กรมีศักยภาพในการดำเนินงานเพียงใด และจะรักษาศักยภาพขององค์กรในสภาพแวดล้อม และ/หรือปัจจัยที่เกี่ยวข้องต่าง ๆ ที่เปลี่ยนแปลงไปได้อย่างไร
- ☞ สาเหตุของการเปลี่ยนแปลงสภาพแวดล้อม และ/หรือปัจจัยต่าง ๆ ที่เกี่ยวข้องนั้นคืออะไร และอะไรคือโอกาสและความเสี่ยงที่อาจเกิดขึ้น ความเสี่ยงและปัญหาที่เกิดขึ้นแล้วมีโอกาสเกิดขึ้นอีกในอนาคตหรือไม่
- ☞ ทรัพยากรบุคคลที่จำเป็นสำหรับการเติบโต ควรจะพัฒนาจากภายในองค์กรหรือสรรหาจากภายนอก

บทบาทของผู้บริหารและกรรมการมืออาชีพ บางมุมมอง

คำถาม + คำแนะ

มุมมอง GRC

WS – คำถามชวนคุย - ชวนคิด - เพื่อสร้างคุณค่าเพิ่ม

เกี่ยวกับการให้ความสำคัญกับกลยุทธ์ และการคาดการณ์ เพื่อการเตรียมพร้อมสำหรับการบริหารความเสี่ยงแบบบูรณาการและการจัดการองค์กร เชิงรุก

★ เป้าหมายหรือวัตถุประสงค์ขององค์กรมีการระบุเป็นลายลักษณ์อักษรที่ชัดเจน เพื่อให้พนักงานทุกคนได้รับทราบหรือไม่

★ ผู้บริหารและกรรมการทุกท่านประพฤติและปฏิบัติ โดยแสดงให้เห็นถึงการยึดถือและแสดงออกถึงค่านิยมขององค์กร ซึ่งเป็นที่รับรู้และเข้าใจกันแล้วหรือไม่ ... และคณะกรรมการรู้สึกพอใจหรือไม่กับการที่ทุกคนในองค์กรปฏิบัติตามค่านิยมขององค์กร

★ การคิดเชิงกลยุทธ์ของผู้บริหารและกรรมการมีความสมดุลระหว่างมุมมองที่มีต่อปัจจัยภายนอกและปัจจัยภายในหรือไม่ ... และความสอดคล้องสมดุลกันระหว่างแนวคิดและการปฏิบัติเป็นอย่างไร

★ ผู้บริหารและกรรมการได้พิจารณาไตร่ตรองทางเลือกเชิงกลยุทธ์ ก่อนนำไปสู่การร่างแผนหรือไม่ และได้มีการทบทวนกลยุทธ์ขององค์กรอย่างสม่ำเสมอตามแนวโน้มที่จะเกิดขึ้นหรือไม่ อย่างไร

★ ผู้บริหารและกรรมการแต่ละท่านได้รับมอบหมาย หรือมีความรับผิดชอบในการติดตาม และให้ข้อมูลกับคณะกรรมการได้ทราบถึงการเปลี่ยนแปลงและแนวโน้มต่าง ๆ ของปัจจัยภายนอกที่เกิดขึ้นในแต่ละด้านหรือไม่

★ คณะกรรมการเป็นผู้ตัดสินใจว่า ควรใช้เป้าหมายใดในการวัดความสำเร็จของแผนกลยุทธ์ ... และเป้าหมายดังกล่าวรวมตัวแปรที่เป็น “นามธรรม” และแนวโน้มต่าง ๆ ตลอดจนตัวแปรที่สามารถวัดเป็นเชิงปริมาณด้วยหรือไม่

★ คณะกรรมการมีความสามารถจริง ๆ ตรงตามบทบาทหน้าที่ที่จะทำงาน เพื่อให้องค์กรประสบความสำเร็จในอนาคตหรือไม่

บทบาทของผู้บริหารและกรรมการมืออาชีพ บางมุมมอง

การสอดส่องดูแล / Monitoring องค์กร โดยผู้บริหารระดับสูงและคณะกรรมการ

บทบาทของประธาน – กรรมการขององค์กร คือ

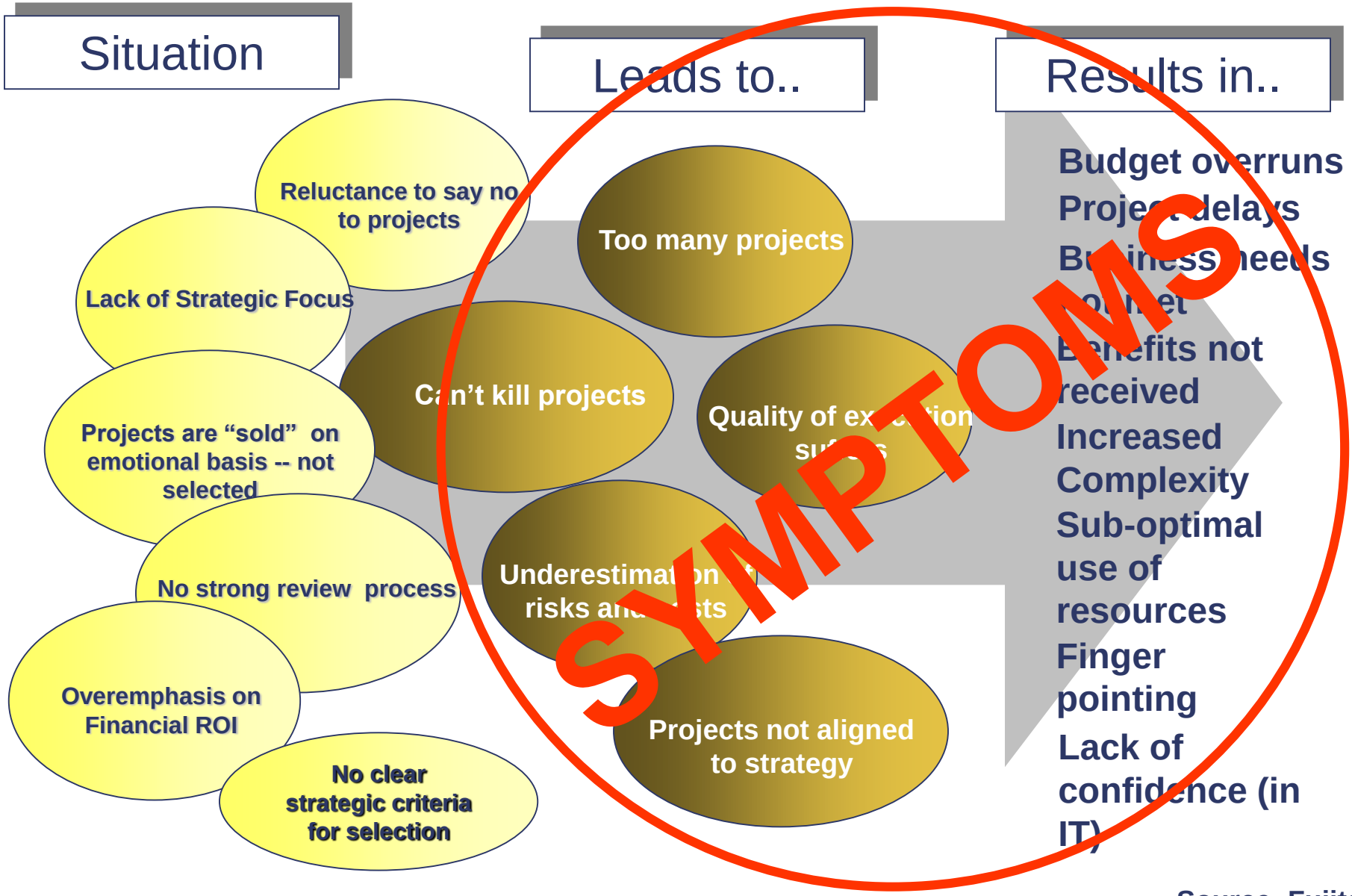
การกำหนดว่าเรื่องใดที่ไม่ต้องนำเสนอให้คณะกรรมการพิจารณา เพื่อให้เกิดความชัดเจนว่าบทบาทใดเป็นหน้าที่ของฝ่ายบริหาร และบทบาทใดควรอยู่ภายในหน้าที่ของคณะกรรมการ

เกณฑ์ที่อาจแนะนำให้กรรมการมีอำนาจในการตัดสินใจคือ

- ☞ ความอยู่รอด ความปลอดภัย มีความรุ่งเรืองมั่งคั่ง และความมีชื่อเสียงขององค์กรในระยะยาว +++
- ☞ นโยบายในการกำกับดูแลภาพพจน์ขององค์กร และแนวทางที่องค์กรจะปฏิบัติต่อผู้อื่น
- ☞ ความสัมพันธ์กับผู้ถือหุ้น หรือหน่วยงานกำกับดูแล ในกรณีที่ไม่มีผู้ถือหุ้น
- ☞ นโยบายที่ครอบคลุมประเด็นการเงินและพันธะสำคัญ ๆ ภาระผูกพันตามกฎหมาย การปฏิบัติตามกฎระเบียบ ความสัมพันธ์กับผู้มีส่วนได้เสียที่เกี่ยวข้อง ความซื่อสัตย์ และประเด็นเกี่ยวกับจริยธรรมอื่น ๆ
- ☞ ประเด็นที่เกี่ยวกับคณะกรรมการและฝ่ายบริหารระดับสูง
- ☞ อำนาจของฝ่ายบริหาร ++++

คำถาม + คำแนะนำใน
มุมมอง GRC /COBIT5

Without Effective Governance



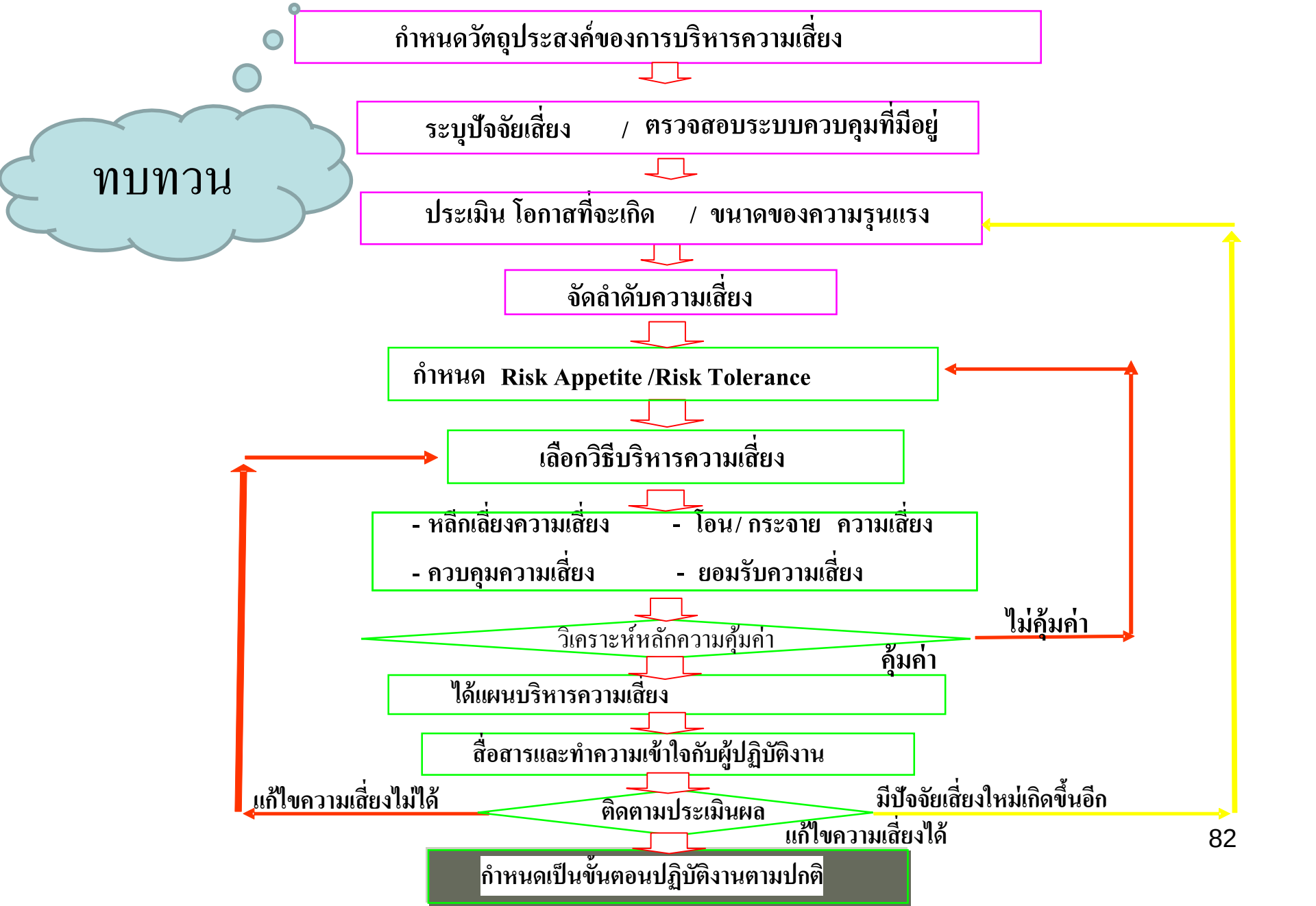
Source: Fujitsu

องค์ประกอบของวัฒนธรรม/จริยธรรม องค์กรกับการสร้างคุณค่าเพิ่มขององค์กร ที่เกี่ยวข้องกับ ITG / COBIT5 บางประการ

Q & A

เกี่ยวกับ Consolidated + Integrated Risk Management + GRC/ COBIT อย่างไร?

Flow Chart การบริหารความเสี่ยงในภาพรวม



กระบวนการบริหารความเสี่ยง 8 ขั้นตอน

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)

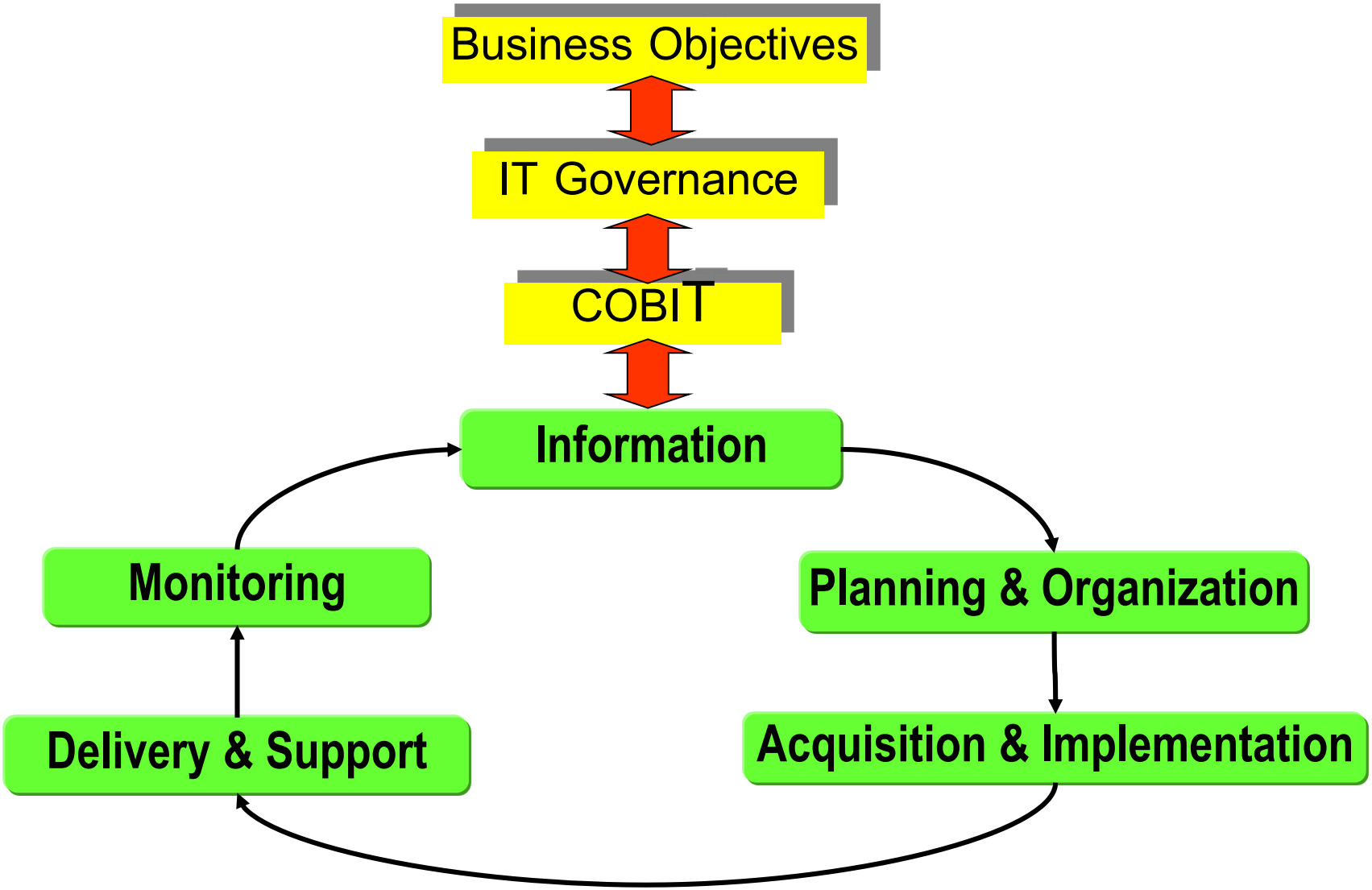
Information – Strategic and Integrated Systems - Communication

↓

8. การติดตามและประเมินผล (Monitoring)

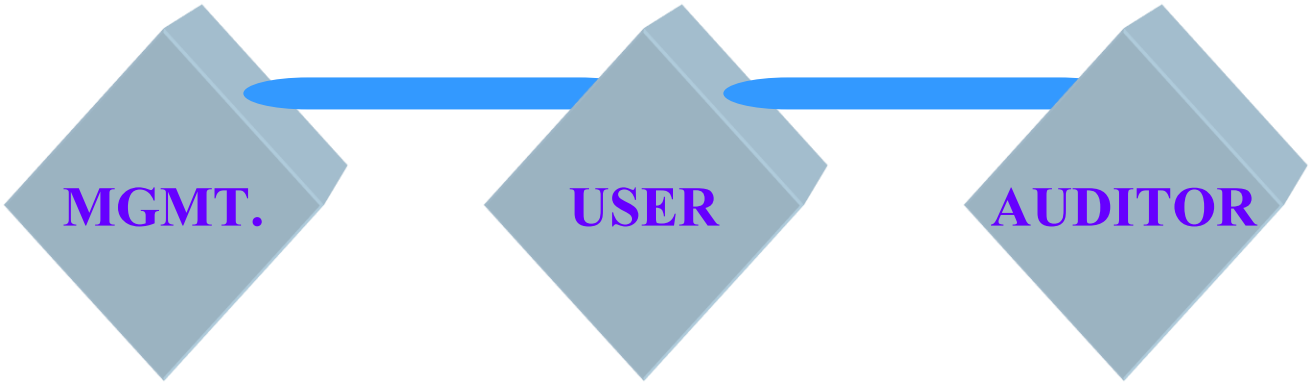
Separate Evaluation – Ongoing Evaluation

IT Governance กับการกำกับดูแลกิจการที่ดี



Change management from COBIT 4 - 4.1 to COBIT5 – GEIT -> Integrated Single Framework

Who Needs IT Governance & Control Models? & Regulators + +



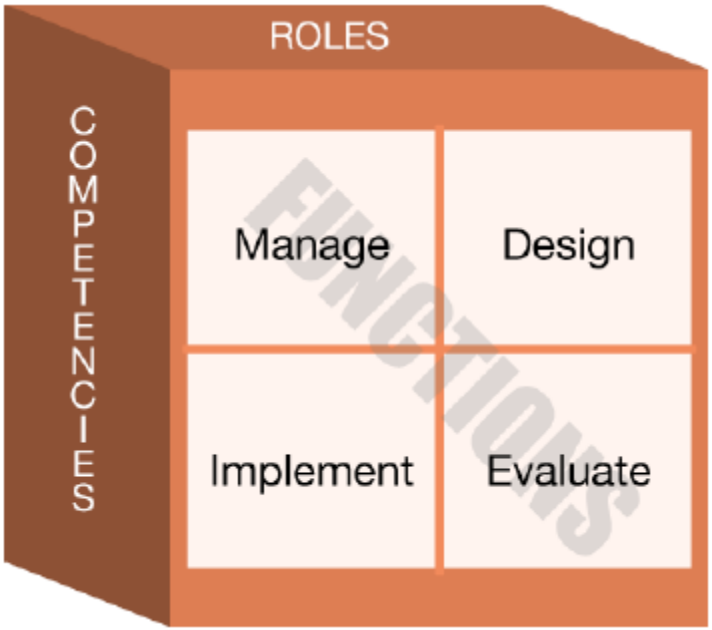
- IT investment decisions
- Balance risk and control investment
- Benchmark existing and future IT environment

Obtain assurance on security and control of products and services they acquire internally or externally

- Substantiate opinions to management on internal controls
- Advise on what minimum controls are necessary

GRC & Functional Perspectives & Competency to drive IT Security + Successful Business

1. Manage
2. Design
3. Implement
4. Evaluate



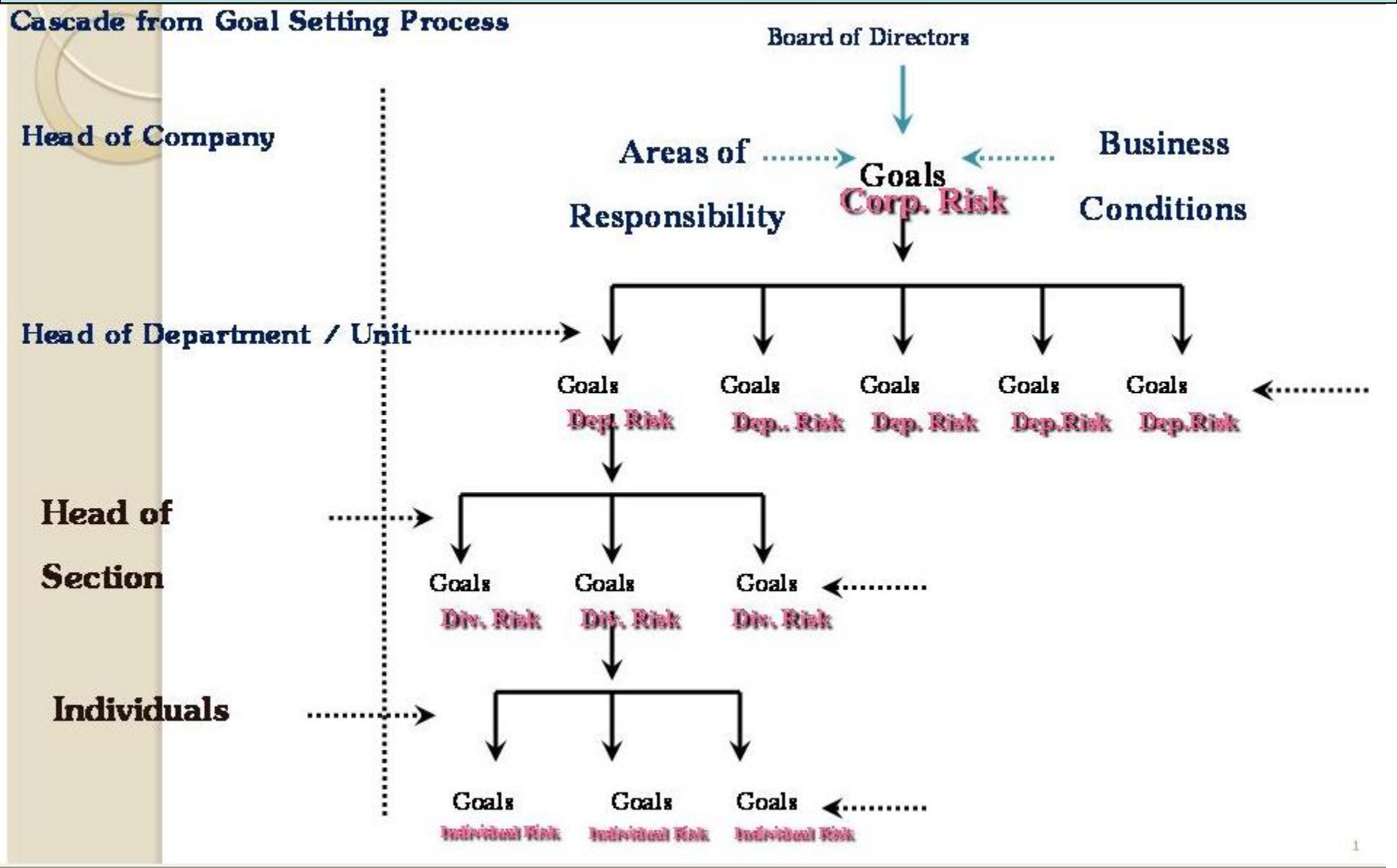
Source: EBK-Essential Body of Knowledge

Competency Areas *(MDIE in each)*

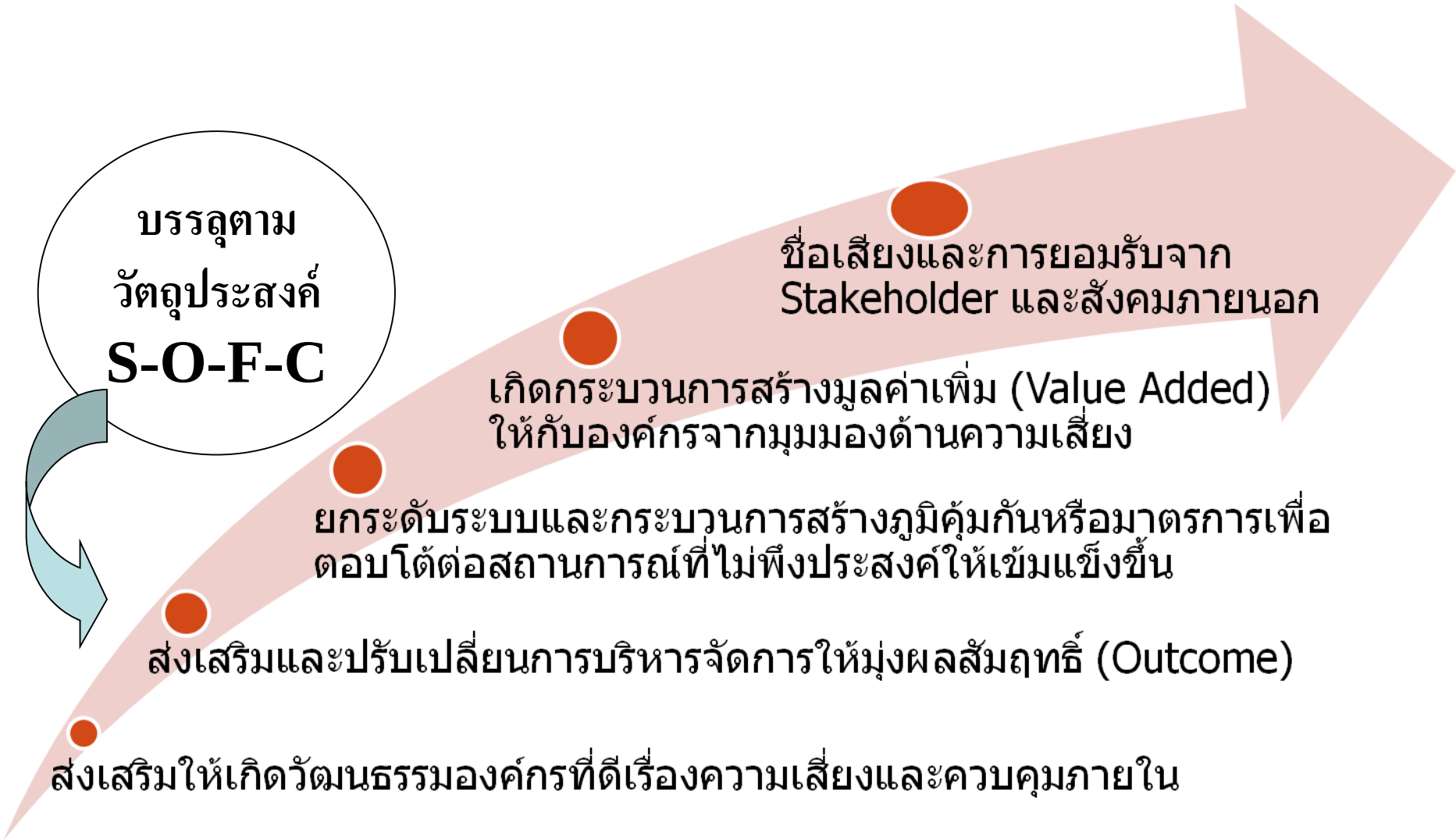
1. Data Security
2. Digital Forensics
3. Enterprise Continuity
4. Incident Management
5. IT Security Training and Awareness
6. IT System Operations and Maintenance
7. Network and Telecommunication Security
8. Personnel Security
9. Physical and Environmental Security
10. Procurement
11. Regulatory and Standards Compliance
12. Security Risk Management
13. Strategic Security Management
14. System and Application Security

Source: EBK

การแตกเป้าหมายหลักขององค์กร ลงมาสู่สายการปฏิบัติงาน เพื่อการบริหารความเสี่ยงทั่วทั้งองค์กร- Integrated Risk Mgmt.

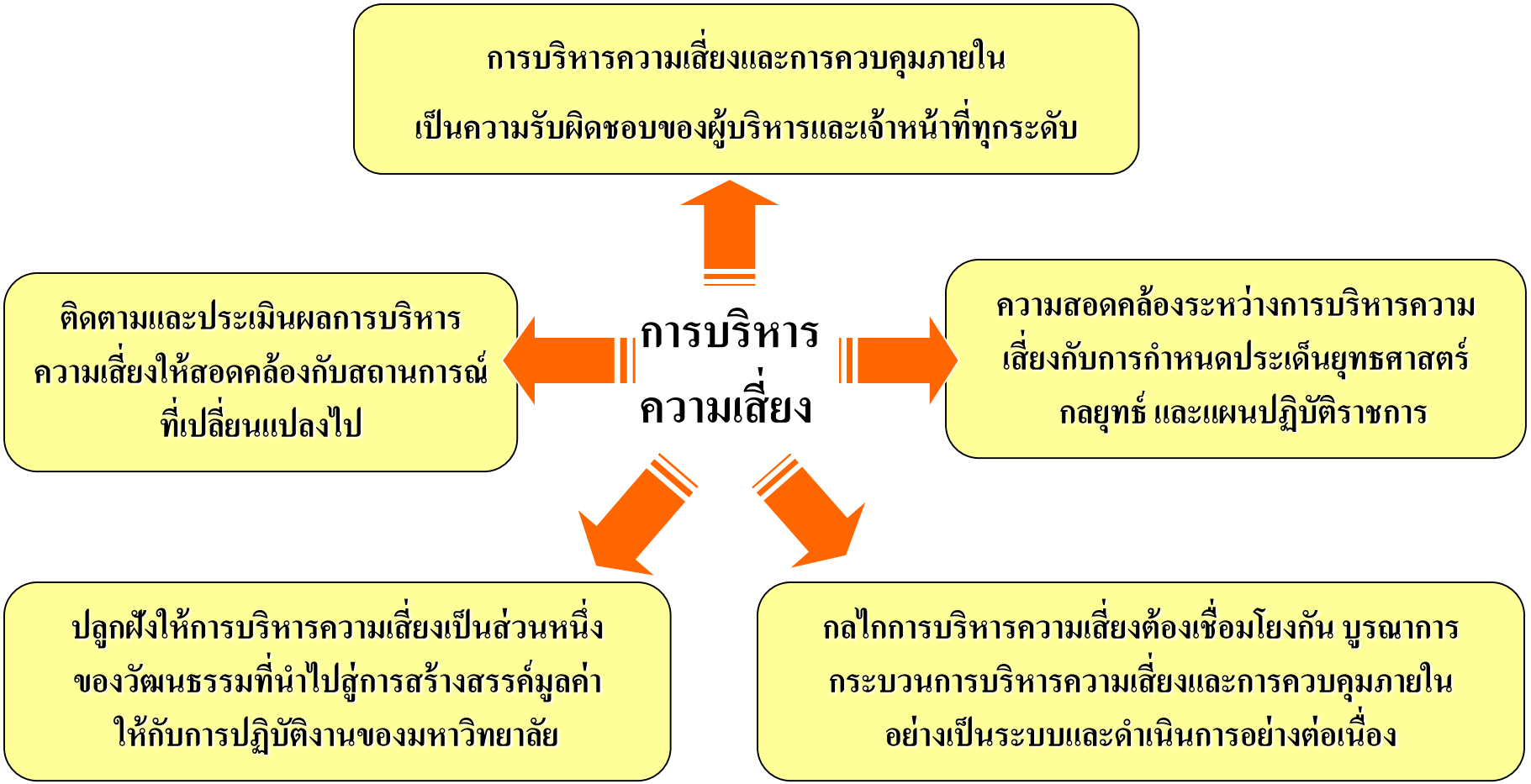


ผลลัพธ์ที่ได้จากการบริหารความเสี่ยง



ERM is a core of GRC…Understanding is very necessary

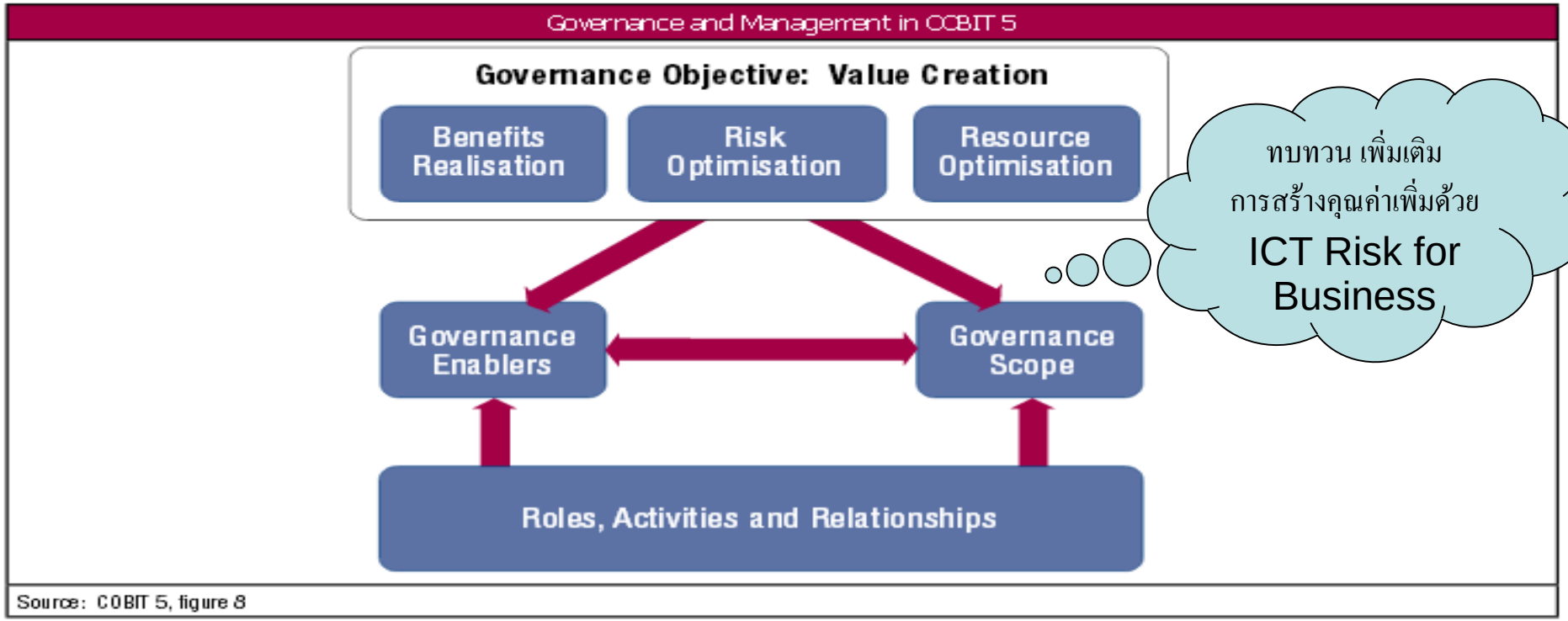
นโยบายการบริหารความเสี่ยง



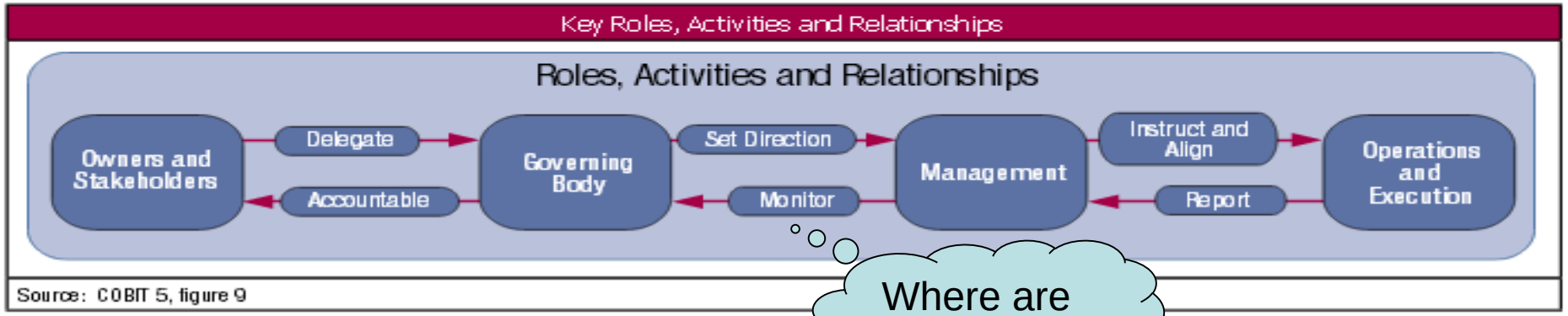
กรอบการประเมินผลการปฏิบัติราชการ

ระดับ	เกณฑ์ระดับความสำเร็จของการนำระบบบริหารความเสี่ยงมาใช้ในกระบวนการบริหารการศึกษา (สกอ.(7.8))
1	มี การแต่งตั้งคณะกรรมการหรือคณะทำงานบริหารความเสี่ยง โดยมีผู้บริหารระดับสูงและตัวแทนที่รับผิดชอบพันธกิจหลักของสถาบันร่วมเป็น คณะกรรมการหรือคณะทำงาน โดยผู้บริหาร ระดับสูงต้องมีบทบาทสำคัญในการกำหนดนโยบายหรือแนวทางในการบริหารความเสี่ยง
2	มี การวิเคราะห์และระบุปัจจัยเสี่ยงที่ส่งผลกระทบหรือสร้างความเสียหายหรือความ ล้มเหลวหรือลดโอกาสที่จะบรรลุเป้าหมายในการบริหารงาน และจัดลำดับความสำคัญของปัจจัยเสี่ยง
3	มี การจัดทำแผนบริหารความเสี่ยง โดยแผนดังกล่าวต้องกำหนดมาตรการหรือแผนปฏิบัติการในการสร้างความรู้ ความเข้าใจให้กับบุคลากรทุกระดับในด้านการบริหารความเสี่ยง และการดำเนินการแก้ไข ลด หรือป้องกันความเสี่ยงที่จะเกิดขึ้นอย่างเป็นรูปธรรม
4	มีการดำเนินการตามแผนบริหารความเสี่ยง
5	มี การสรุปผลการดำเนินงานตามแผนการบริหารความเสี่ยง ตลอดจนมีการกำหนดแนวทางและข้อเสนอแนะในการปรับปรุงแผนบริหารความเสี่ยง โดยได้รับความเห็นชอบจากผู้บริหารสูงสุดของมหาวิทยาลัย

COBIT 5 and Key Roles-Activities- Relationship



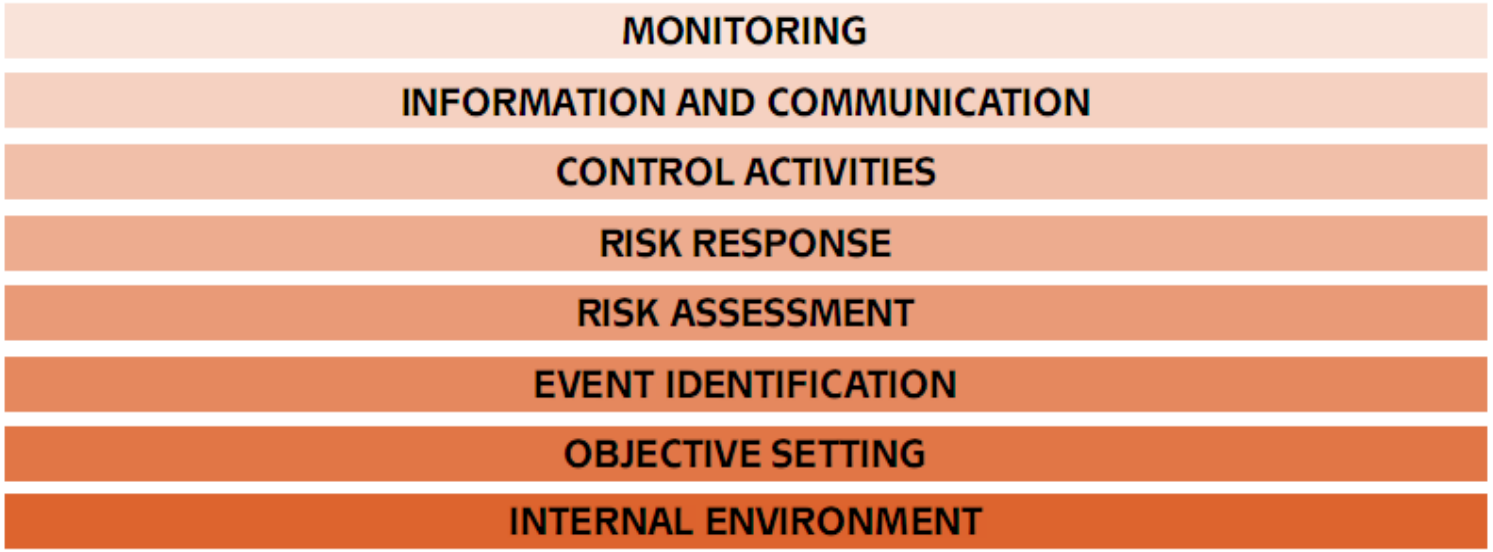
ทบทวน เพิ่มเติม
การสร้างคุณค่าเพิ่มด้วย
ICT Risk for Business



Where are you ?

Source : ISACA

COSO ERM Model for Risk Management and Change Management -> IT-Related Risk



Monitoring

- Monthly performance metrics and change analysis provided to the CIO.
- Audits of change management process conducted by internal auditing.
- Annual control self-assessment (CSA) conducted by business units and the IT department.
- Periodic reports from the change management board provided to senior management.

Information and Communication

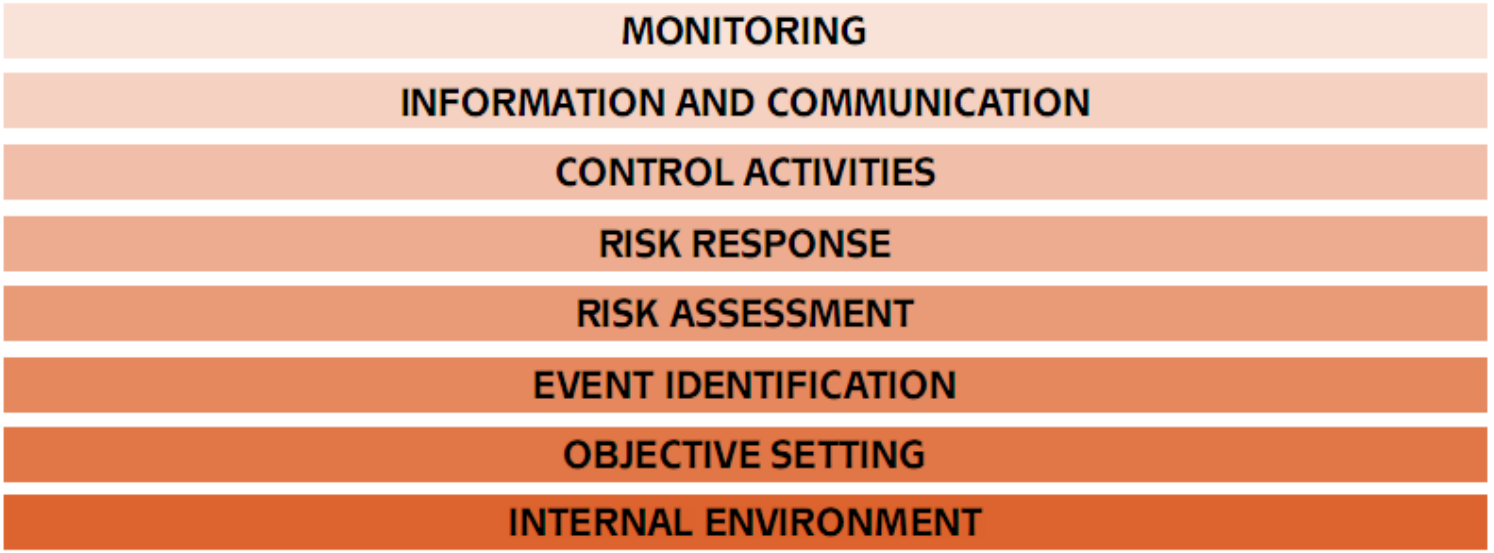
- Periodic messages from senior management that change control is important.
- Service desk issues communicated for resolution and trend analysis.
- Changes in policy communicated to all affected personnel.
- Regular communication of upcoming changes.

Control Activities

- Common process in place and documented.
- Effective change control committee structure.
- Change control log used.
- Segregation of duties between developers and technical staff maintained.
- Automated controls to enforce process of promoting changes into production.
- Automated process to return production environment to pre-change state.
- Approved configurations documented.
- Clear delegation of authority documented.
- Approvals for changes documented.
- Automated system and data backups and ability to restore from approved environment.

Source : GTAG

COSO ERM Model for Risk Management and Change Management -> IT-Related Risk



Risk Assessment

- Firm's strategic and process-level risk assessments consider risks associated with out-of-process (unintended or unauthorized) changes.
- Risks due to change well understood by IT personnel.
- Thorough risk assessment of all proposed changes performed.
- Business continuity planning in place.
- Internal audit assessment performed.
- Business insurance needs assessment performed.
- Risk factors assessed to determine classification of the change and level of testing and approval.

Objective Setting and Event Identification

- Management establishes business objectives and strategies.
- Management establishes objectives for change management; identifies what events could prevent successful achievement of business objectives and adherence to change process.

Internal Environment

- Senior management demonstrates that change management is important.
- Presence of an effective culture of change management.
- No tolerance for out-of-process changes; waiver process in place.
- Documentation exists (policies, procedures, process for managing changes in applications, databases, operating systems, and all other IT assets).
- Process training for all affected personnel provided.
- Defined roles and responsibilities enforced.
- Service level aggreements (SLAs) and contracts with vendors in place that define process and performance standards.
- Company-level standards and guidelines for the change process in place.

Source : GTAG

COSO ERM กับข้อควรคำนึงถึงการบริหารการเปลี่ยนแปลงที่เกี่ยวข้องกับสารสนเทศขององค์กร

การเฝ้าติดตามประเมิน (Monitoring)

- มาตรวัดผลการดำเนินรายเดือน รวมทั้งข้อมูลการวิเคราะห์การเปลี่ยนแปลง นำเสนอหัวหน้าเจ้าหน้าที่สารสนเทศ(CIO)
- สอบทานกระบวนการ การบริหารการเปลี่ยนแปลงโดยผู้ตรวจสอบภายใน
- ดำเนินการประเมินการควบคุมด้วยตนเอง (Control Self Assessment - CSA) โดยหน่วยงานเจ้าของธุรกิจและฝ่ายเทคโนโลยีสารสนเทศอย่างต่อเนื่องทุกปี
- นำเสนอรายงาน การบริหารการเปลี่ยนแปลงต่อผู้บริหารระดับสูงจากคณะกรรมการ การบริหารการเปลี่ยนแปลงเป็นระยะ

สารสนเทศและการสื่อสาร (Information and communication)

- มีสาส์นเป็นระยะจากผู้บริหารระดับสูงเกี่ยวกับความสำคัญของการควบคุมการเปลี่ยนแปลง
- มีการสื่อสารเกี่ยวกับผลการดำเนินการและการวิเคราะห์แนวโน้ม จากเจ้าหน้าที่ผู้ให้บริการ
- มีการสื่อสารเกี่ยวกับการเปลี่ยนแปลงนโยบายให้กับผู้เกี่ยวข้องทุกท่าน
- มีการสื่อสารเป็นประจำ ถึงมีการเปลี่ยนแปลงที่จะดำเนินการ

Source : GTAG

COSO ERM กับข้อควรคำนึงถึงการบริหารการเปลี่ยนแปลงที่เกี่ยวข้องกับสารสนเทศขององค์กร

กิจกรรมการควบคุม (Control activities)

- มีกระบวนการบริหารการเปลี่ยนแปลงที่ใช้ร่วมกันในองค์กร รวมทั้งมีการจัดทำเป็นเอกสาร
- มีโครงสร้างคณะกรรมการควบคุมการเปลี่ยนแปลงที่มีประสิทธิผล
- มีการบันทึกหลักฐาน (log) การควบคุมการเปลี่ยนแปลง
- มีการแบ่งแยกหน้าที่ระหว่างผู้พัฒนาระบบงานและเจ้าหน้าที่บำรุงรักษาระบบงาน
- มีกระบวนการ ขั้นตอนแบบอัตโนมัติ ในการควบคุมการนำผลจากการเปลี่ยนแปลงไปใช้กับระบบงานจริง
- มีกระบวนการ ขั้นตอนแบบอัตโนมัติ เพื่อรองรับการปรับระบบงานจริงเข้าสู่สภาพแวดล้อมก่อนการเปลี่ยนแปลง

กิจกรรมการควบคุม (Control activities)(ต่อ)

มีการนำเสนอวัฒนธรรมในการบริหารการเปลี่ยนแปลงที่มีประสิทธิผลและมีการดำเนินการตามกระบวนการบริหารการเปลี่ยนแปลง

- ไม่ยอมรับการออกนอกกระบวนการของการเปลี่ยนแปลง หรือการข้ามกระบวนการ
- มีการจัดทำเอกสารเป็นลายลักษณ์อักษร (นโยบาย ขั้นตอนการดำเนินงาน กระบวนการบริหารการเปลี่ยนแปลงที่เกี่ยวกับระบบงาน ฐานข้อมูล ระบบปฏิบัติการ และสินทรัพย์ทางเทคโนโลยีสารสนเทศ)
- มีการอบรมการดำเนินงานตามกระบวนการแก่ผู้เกี่ยวข้องทั้งหมด

Source : GTAG

COSO ERM กับข้อควรคำนึงถึงการบริหารการเปลี่ยนแปลงที่เกี่ยวข้องกับสารสนเทศขององค์กร

กิจกรรมการควบคุม (Control activities) (ต่อ)

- มีการบังคับใช้บทบาทและหน้าที่รับผิดชอบที่กำหนดไว้
- มีการจัดทำข้อตกลงการให้บริการ (Service level agreements - SLAs) กับบริษัทผู้ขาย โดยมีการกำหนดมาตรฐานกระบวนการและการดำเนินงาน
- มีการกำหนดแนวปฏิบัติและแนวปฏิบัติระดับบริษัทสำหรับกระบวนการเปลี่ยนแปลง
    - มีเอกสารอนุมัติการปรับตั้งค่า พารามิดตอร์ (configurations)
- มีเอกสารการกระจายอำนาจที่ชัดเจน
- มีเอกสารอนุมัติการเปลี่ยนแปลง
- มีระบบอัตโนมัติ ระบบสำรองข้อมูลและความสามารถในการนำกลับคืน (restore) จากสภาพแวดล้อมที่ได้รับอนุมัติ

Source : GTAG

COSO ERM กับข้อควรคำนึงถึงการบริหารการเปลี่ยนแปลงที่เกี่ยวข้องกับสารสนเทศขององค์กร

การประเมินความเสี่ยง (Risk assessment)

- การประเมินความเสี่ยงทางกลยุทธ์และระดับกระบวนการขององค์กรมีการพิจารณาความเสี่ยงที่เกี่ยวข้องกับการบริหารการเปลี่ยนแปลงที่ไม่ดำเนินการตามกระบวนการ (ไม่มีการกำหนดแผนหรือ ไม่ได้รับการอนุมัติ)
- เจ้าหน้าที่เทคโนโลยีสารสนเทศมีความรู้และความเข้าใจในความเสี่ยงที่จากการเปลี่ยนแปลงเป็นอย่างดี
- มีการประเมินความเสี่ยงครอบคลุมการเปลี่ยนแปลงทุกเหตุการณ์
- มีการจัดทำแผนงานเพื่อความต่อเนื่องทางธุรกิจ (Business continutity planning)

การประเมินความเสี่ยง (Risk assessment) (ต่อ)

- มีการประเมินการตรวจสอบภายใน
- มีการประเมินความจำเป็นในการประกันภัย
- มีการประเมินปัจจัยเสี่ยงเพื่อระบุประเภทของการเปลี่ยนแปลงและระดับของการทดสอบ รวมทั้งการอนุมัติ

Source : GTAG

COSO ERM กับข้อควรคำนึงถึงการบริหารการเปลี่ยนแปลงที่เกี่ยวข้องกับสารสนเทศขององค์กร

การกำหนดวัตถุประสงค์และการระบุเหตุการณ์

(Objective seting and event identification)

- ฝ่ายจัดการกำหนดวัตถุประสงค์ และกลยุทธ์ของธุรกิจ
- ฝ่ายจัดการกำหนดวัตุประสงค์ของการบริหารการเปลี่ยนแปลง ระบุเหตุการณ์ที่ทำให้ไม่สามารถดำเนินการได้ตามวัตถุประสงค์ทางธุรกิจที่กำหนดและกระบวนการเปลี่ยนแปลง

สภาพแวดล้อมภายใน (Internal environment)

- ผู้บริหารระดับสูงให้ความสำคัญกับการบริหารการเปลี่ยนแปลง

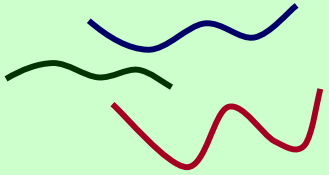
Source : GTAG

ความเข้มแข็งในการบริหารองค์กรและประเทศแบบบูรณาการ&ICT Risk

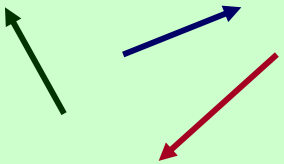
IT-Based & Understanding

GRC / Governance – Risk Mgmt. – Compliance & Integrity Management

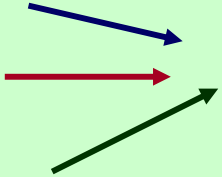
1 ไม่มีระบบใดเลย
(ขาดความเข้าใจในการบริหารเชิงกลยุทธ์อย่างสิ้นเชิง)



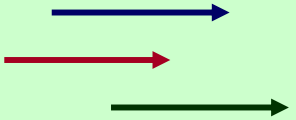
2 แก้ปัญหาเฉพาะหน้า
(เป็นเรื่อง ๆ เป็นกลุ่ม ๆ)

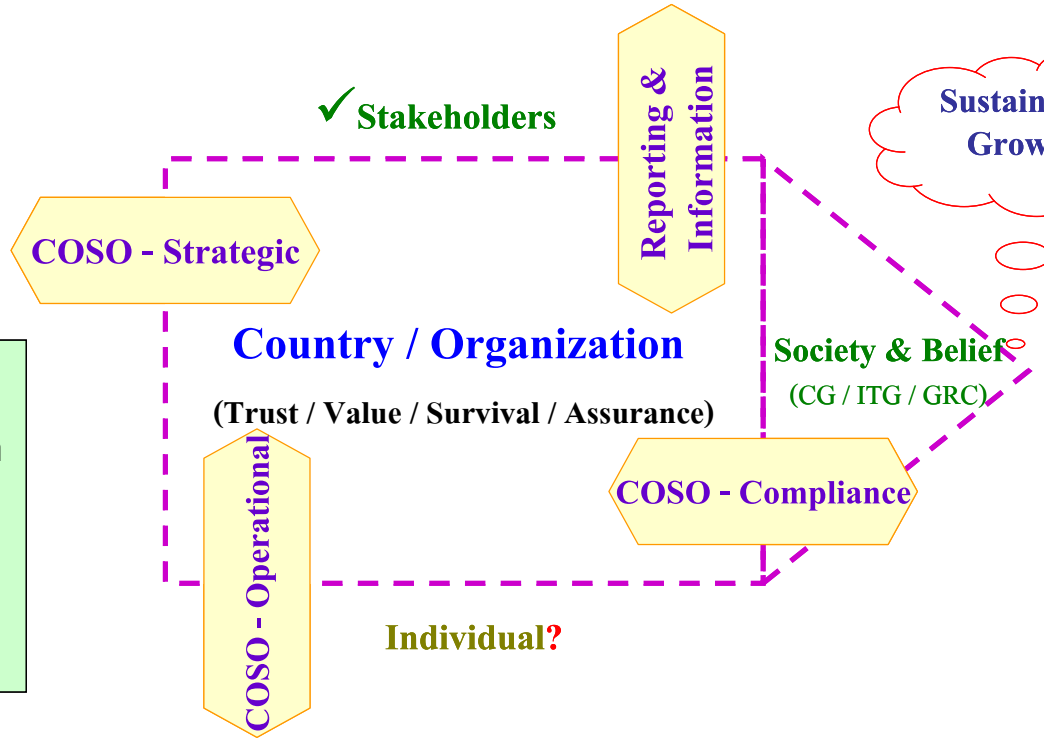


3 แนวทางเริ่มเป็นระบบ
(เริ่มต้นจากรัฐบาลและองค์กร)

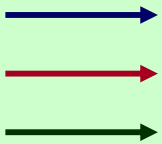


4 มุ่งเป็นทิศทางเดียวกัน
(โดยกระบวนการเรียนรู้)

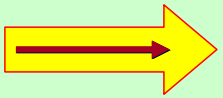




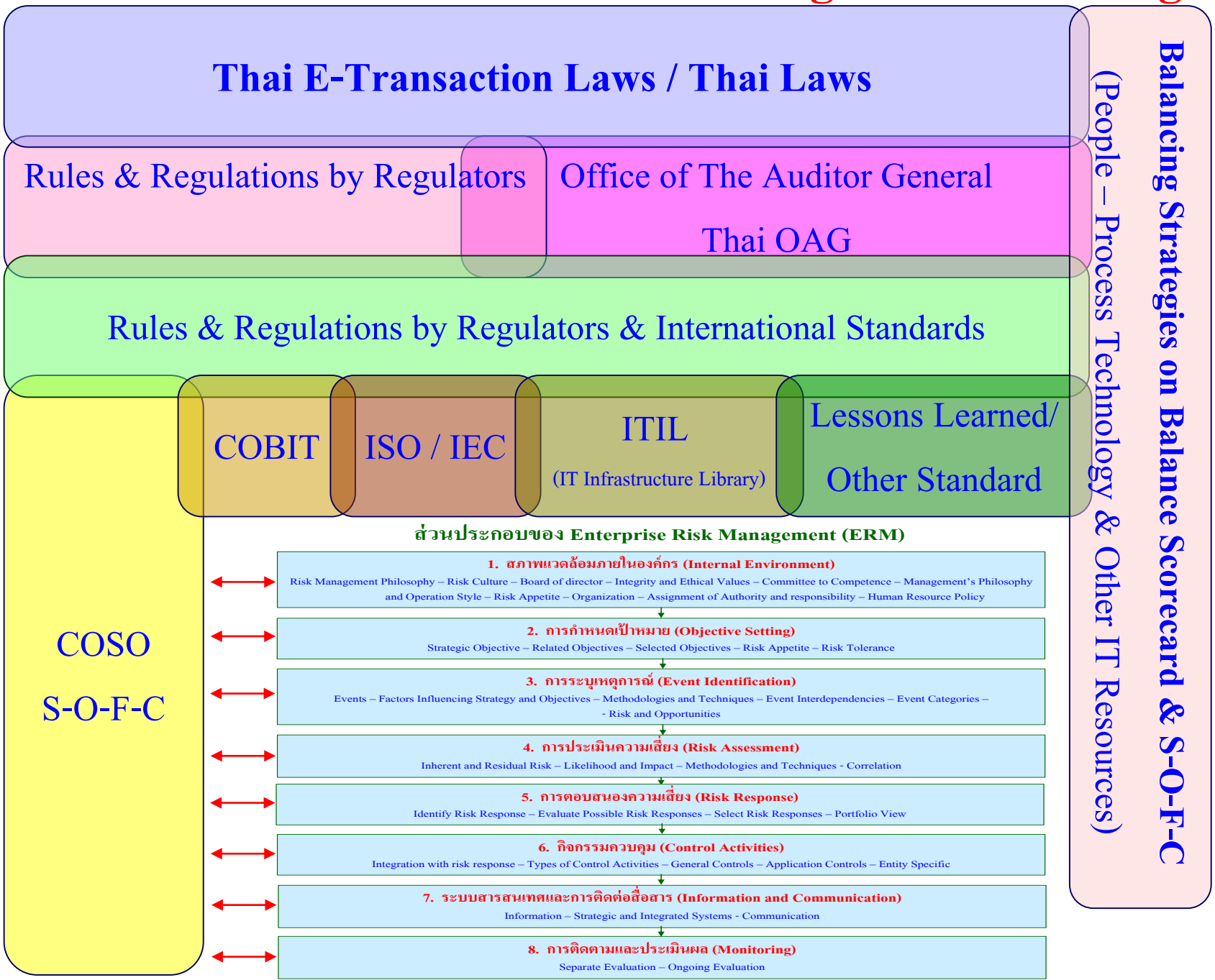
5 แนวทางบูรณาการ
(สร้างความเชื่อมั่นของ Stakeholder)



6 บูรณาการเป็นหนึ่งเดียว
(เพื่อการเติบโตอย่างยั่งยืนของประเทศชาติ)



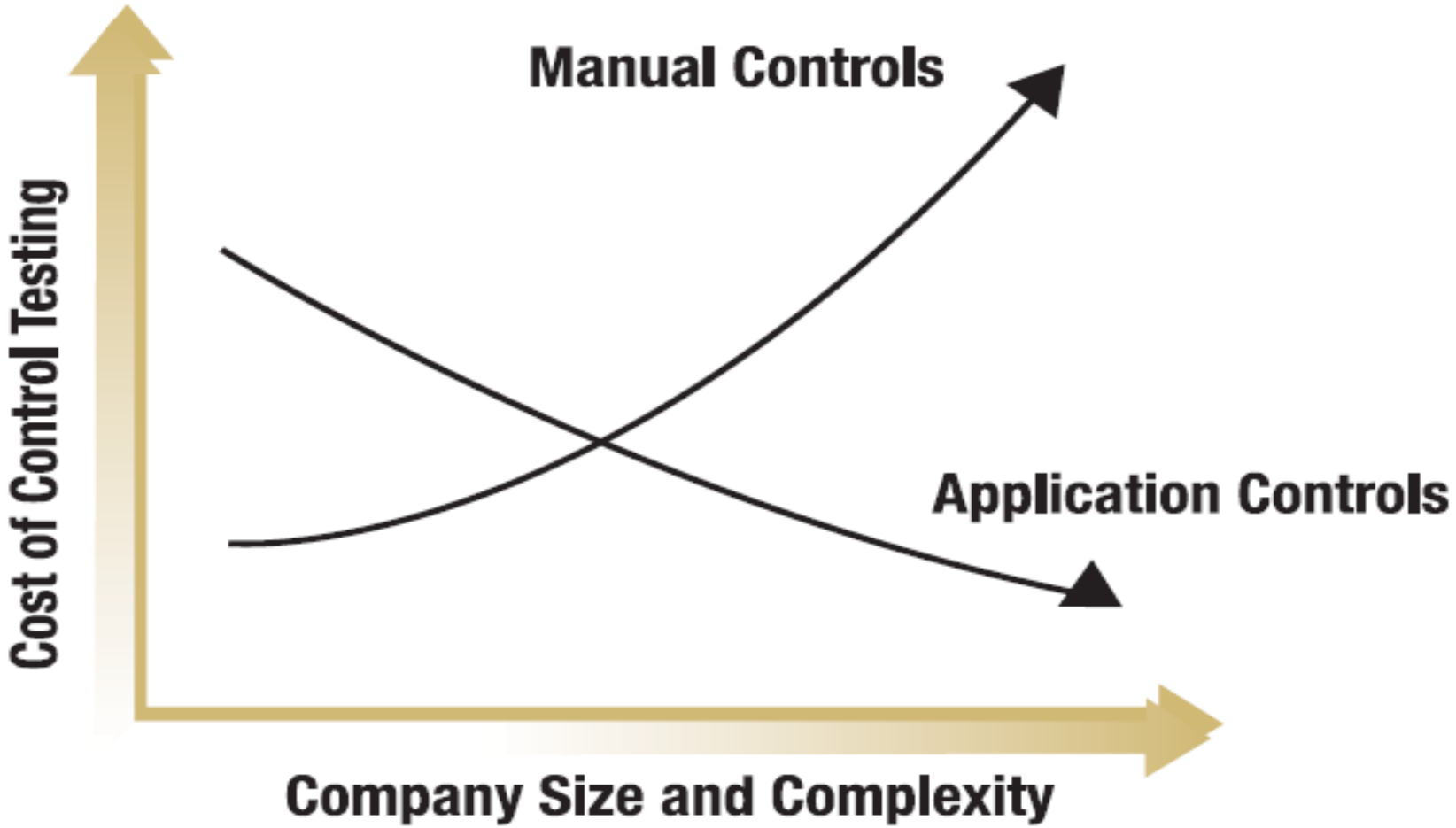
CG/ITG & GRC Framework + Convergence Risk & Mgmt.



Application Controls

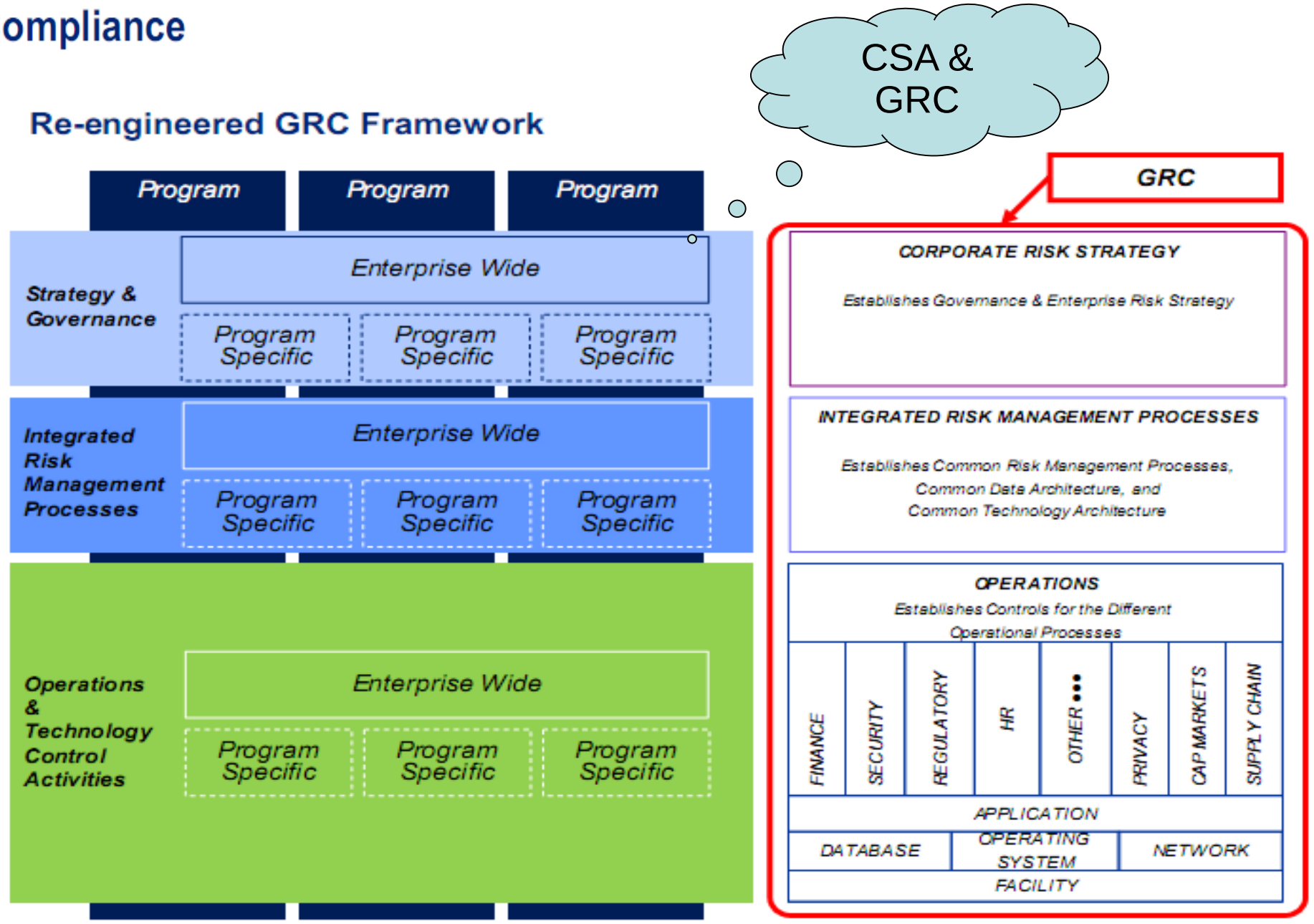
The Business Case for Application Controls

Effect of Size and Complexity on Effort to Document and Test Controls



Source : IT Governance Institute

Complexity Is Driving Organizations to Rethink How They Manage Risk And Compliance



HOW COBITCOMPONENTS SUPPORT IT ASSURANCE ACTIVITIES

Introduction- Sample for better Understanding to Enterprise Governance -> Value Creation

Linking IT Assurance Activities and COBIT Components

IT Assurance Activities	CobiT Components															
	Control Objectives	*CobiT Control Practices*	Value and Risk Statements	Maturity Model	Maturity Model Attributes	RACI (Key Activities and Responsibilities)	Goals and Outcome Measures	Performance Drivers	Management Awareness Tool	Information Criteria	Process List	*Board Briefing on IT Governance, 2nd Edition*	IT Risk and Control Diagnostics	*CobiT Quickstart*	CobiT Online—Searching and Browsing	CobiT Online—Benchmarking	*IT Control Objectives for Sarbanes-Oxley, 2nd Edition*
Perform a quick risk assessment.			✔	✔		✔	✔	✔	✔				✔	✔	✔		
Assess threat, vulnerability and business impact.			✔			✔	✔	✔							✔		✔
Diagnose operational and project risk.			✔			✔	✔	✔	✔				✔		✔		
Plan risk-based assurance initiatives.	✔		✔	✔		✔	✔	✔	✔			✔	✔		✔	✔	✔
Identify critical IT processes based on value drivers.				✔	✔	✔	✔		✔	✔	✔	✔	✔		✔	✔	
Assess process maturity.				✔	✔	✔	✔		✔		✔	✔			✔	✔	
Scope and plan assurance initiatives.						✔	✔			✔	✔		✔		✔		✔
Select the control objectives for critical processes.						✔	✔			✔	✔				✔		✔
Customise control objectives.	✔	✔			✔	✔	✔	✔							✔		✔
Build a detailed assurance programme.	✔	✔		✔		✔	✔						✔		✔		✔
Test and evaluate controls.	✔	✔	✔		✔	✔	✔								✔		✔
Substantiate risk.	✔	✔	✔			✔	✔	✔	✔	✔	✔				✔	✔	✔
Report assurance conclusions.	✔	✔	✔	✔		✔	✔	✔	✔	✔	✔				✔	✔	✔
Self-assess process maturity.	✔	✔		✔		✔	✔	✔	✔				✔		✔		
Self-assess controls.	✔	✔				✔	✔						✔	✔	✔	✔	

Source : IT Governance Institute

INFORMATION TECHNOLOGY RISK AND CONTROLS

Linking IT Controls with The COSO Internal Control Framework

Top 10 Technology Risk Issues as Identified by The IIA Advanced Technology Committee

1. Legislation and Regulatory Compliance
2. Threat / Vulnerability Management (Application exploits, DDOS, IM, SPAM, Viruses, Trojans, worms…)
3. Privacy (including identity protection)
4. Continuous Monitoring / Auditing / Assurance
5. Wireless Security
6. Intrusion Protection (including firewalls, monitoring, analysis, reaction…)
7. IT Outsourcing (including offshore)
8. Enterprise Security Metrics (dashboards, scorecards, analytics…)
9. Identity Management
10. Acquisitions & Divestitures – impacts on systems management

The Institute of Internal Auditors, Advanced Technology Committee Meeting, Dec. 2005.

Source : The Institute of Internal Auditors - IIA

Linking IT Controls with The COSO Internal Control Framework

General Control Activities Versus Application Control Activities

General IT control activities span all IT systems and are put in place to ensure the integrity, reliability, and accuracy of the application systems. Typical general control activities include:

- Systems development standards.
- Information security policies and procedures.
- Backup and recovery standards.
- Service level agreements with vendors.
- Network monitoring procedures and practices.
- Program coding standards.
- Computer hardware architecture and product standards.
- Hardware and software installation, configuration, and testing standards.

Source : The Institute of Internal Auditors - IIA

INFORMATION TECHNOLOGY RISK AND CONTROLS

Linking IT Controls with The COSO Internal Control Framework

COSO Model for Technology Controls

Monitoring

- Monthly metrics from technology performance.
- Technology cost and control performance analysis.
- Periodic technology management assessments.
- Internal audit of technology enterprise.
- Internal audit of high risk areas.

Information and Communication

- Periodic Corporate communications (Intranet, e-mail, meetings, mailings).
- Ongoing technology awareness of best practices.
- IT performance survey.
- IT and security training.
- Help desk ongoing issue resolution.

Source : The Institute of Internal Auditors - IIA

INFORMATION TECHNOLOGY RISK AND CONTROLS

Linking IT Controls with The COSO Internal Control Framework

COSO Model for Technology Controls (con.)

Control Activities

- Review board for change management.
- Comparison of technology initiatives to plan and return on investment.
- Documentation and approval of IT plans and systems architecture.
- Compliance with information and physical security standards.
- Adherence to business continuity risk assessment.
- Technology standards compliance enforcement.

Source : The Institute of Internal Auditors - IIA

INFORMATION TECHNOLOGY RISK AND CONTROLS

Linking IT Controls with The COSO Internal Control Framework

COSO Model for Technology Controls (con.)

Risk Assessment

- IT risks included in overall corporate risk assessment.
- IT integrated into business risk assessments.
- Differentiate IT controls for high risk business areas/functions.
- IT internal audit assessment.
- IT insurance assessment.

Control Environment

- Tone at the top – IT and security controls considered important.
- Overall technology policy and information security policy.
- Corporate Technology Governance Committee.
- Technology Architecture and Standards Committee.
- Full representation of all business units.

Source : The Institute of Internal Auditors - IIA

INFORMATION TECHNOLOGY RISK AND CONTROLS

Linking IT Controls with The COSO Internal Control Framework

Application Control Activities

Application Control Activities pertain to individual application systems.

- The primary mission of any information systems function is to run applications for the benefit of systems users.
- Application system integrity is critical to operational success.
- A set of control activities needs to be in place to ensure that the system processes and logic perform according to specifications each time the system is run.
- The level of resources spent on integrity control activities needs to be evaluated in light of the risk associated with the application and data.
- To ensure overall system integrity, a combination of input, processing, and output control activities in necessary.
- The better the combination of these control activities, the higher the reliability of the overall system of internal controls.

Source : The Institute of Internal Auditors - IIA

INFORMATION TECHNOLOGY RISK AND CONTROLS

The Four Principles

1. The only IT infrastructure elements (e.g., databases, operating system, networks) relevant to information technology general controls (ITGC) assessment are those that support financially significant applications and data.
2. The IT Processes primarily relevant to ITGC assessment are those that directly impact the integrity of financially significant applications and data, such as:
   - Change management and systems development.
   - Operations management.
   - Security management.
3. Implications to the reliability of financially significant applications and data, including controls, are based upon the achievement of failure of IT process objectives, not the design and operating effectiveness of the individual controls with those processes.
4. The basis for identifying key controls in the three IT processes is based on:
   - Inherent risk of not achieving the IT processes objectives.
   - IT process risk objectives.

Source : The Institute of Internal Auditors - IIA

Information Technology Controls and COSO-ERM to GRC

COSO Model for Technology Controls

Monitoring:

- Monthly metrics from technology performance
- Technology cost and control performance analysis
- Periodic technology management assessments
- Internal audit of technology enterprise
- Internal audit of high risk areas

Control Activities:

- Review board for change management
- Comparison of technology initiatives to plan and return on investment
- Documentation and approval of IT plans and systems architecture
- Compliance with information and physical security standards
- Adherence to business continuity risk assessment
- Technology standards compliance enforcement

Information and Communication:

- Periodic corporate communications (intranet, e-mail, meetings, mailings)
- Ongoing technology awareness of best practices
- IT performance survey
- IT and security training
- Help desk ongoing issue resolution

Risk Assessment:

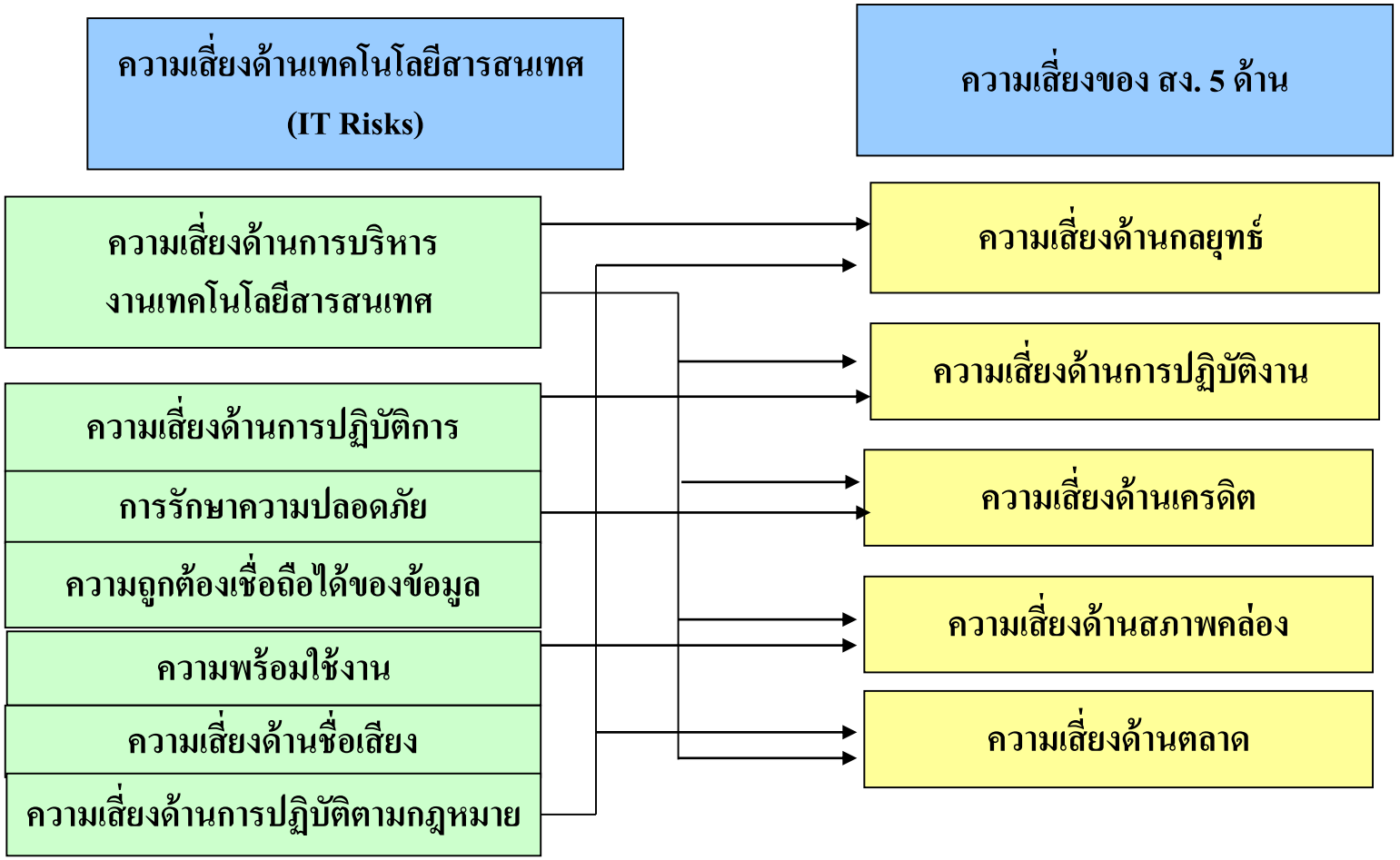
- IT risks included in overall corporate risk assessment
- IT integrated into business risk assessments
- Differentiate IT controls for high risk business areas/functions
- IT Internal audit assessment
- IT Insurance assessment

Control Environment:

- Tone from the top – IT and security controls considered Important
- Overall technology policy and Information security policy
- Corporate Technology Governance Committee
- Technology Architecture and Standards Committee
- Full representation of all business units

Source: The Institute of Internal Auditors

IT Risks VS Risk-based Examination and Supervision/Audit Approaches for FIs



ที่มา : ธนาคารแห่งประเทศไทย เพื่อนำมาประยุกต์ใช้ในการวางแผนและการตรวจสอบภายในขององค์กร

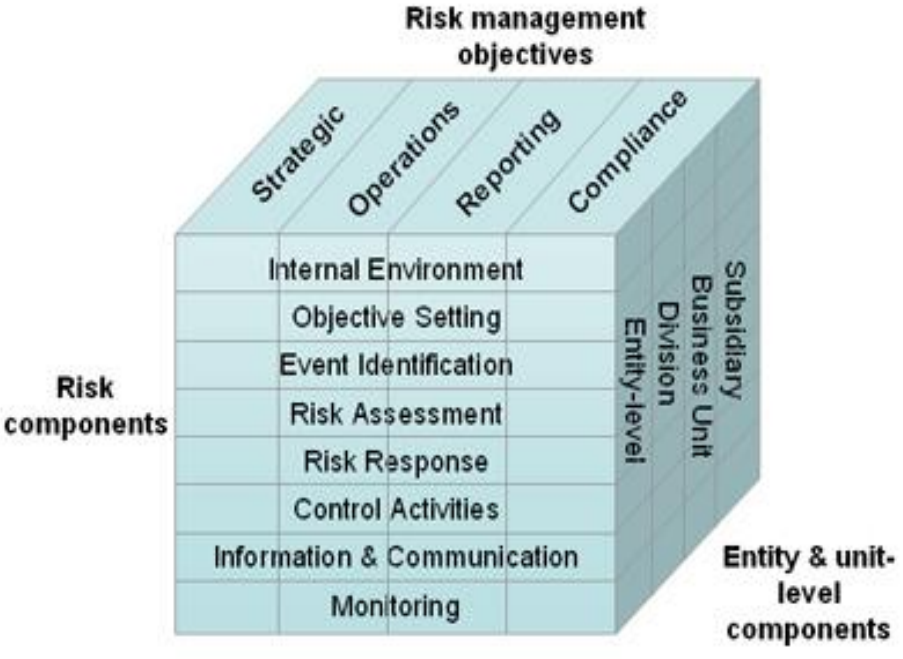
ทำเพียงบางข้อได้หรือไม่ ?

ก้าวสู่ GRC-COBIT5 ได้อย่างไร ?

Business Risk จาก IT Risk อยู่ที่ใด? ใครรับผิดชอบ ?

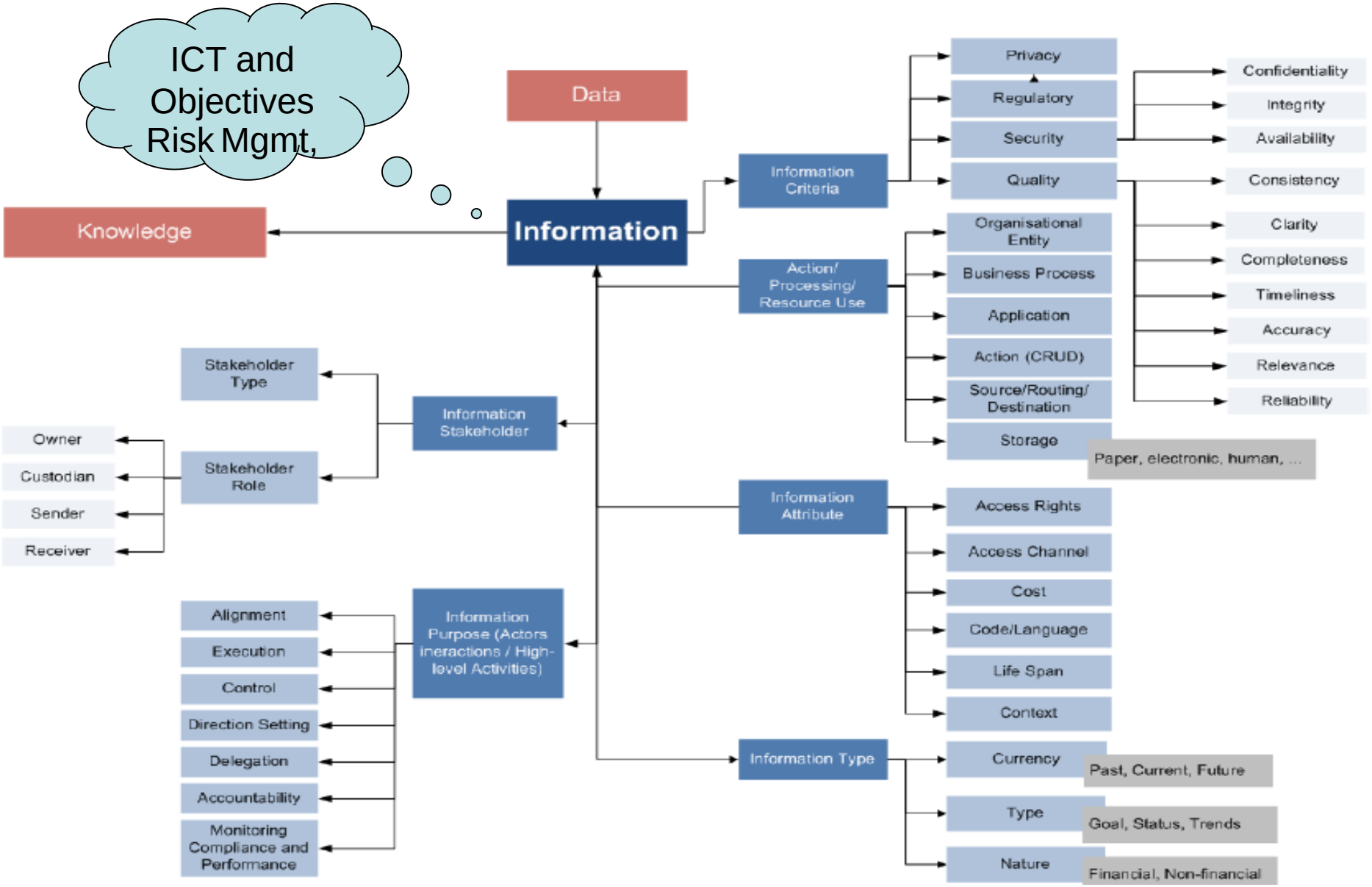
COSO 2 (2004) : Enterprise Risk Management - Integrated Framework

COSO 1 "Internal Control – Integrated Framework"



COSO 2 "Enterprise Risk Management – Integrated Framework"

COBIT 5 Information Reference Model – Starting from Paper Exposure Draft



Source : ISACA

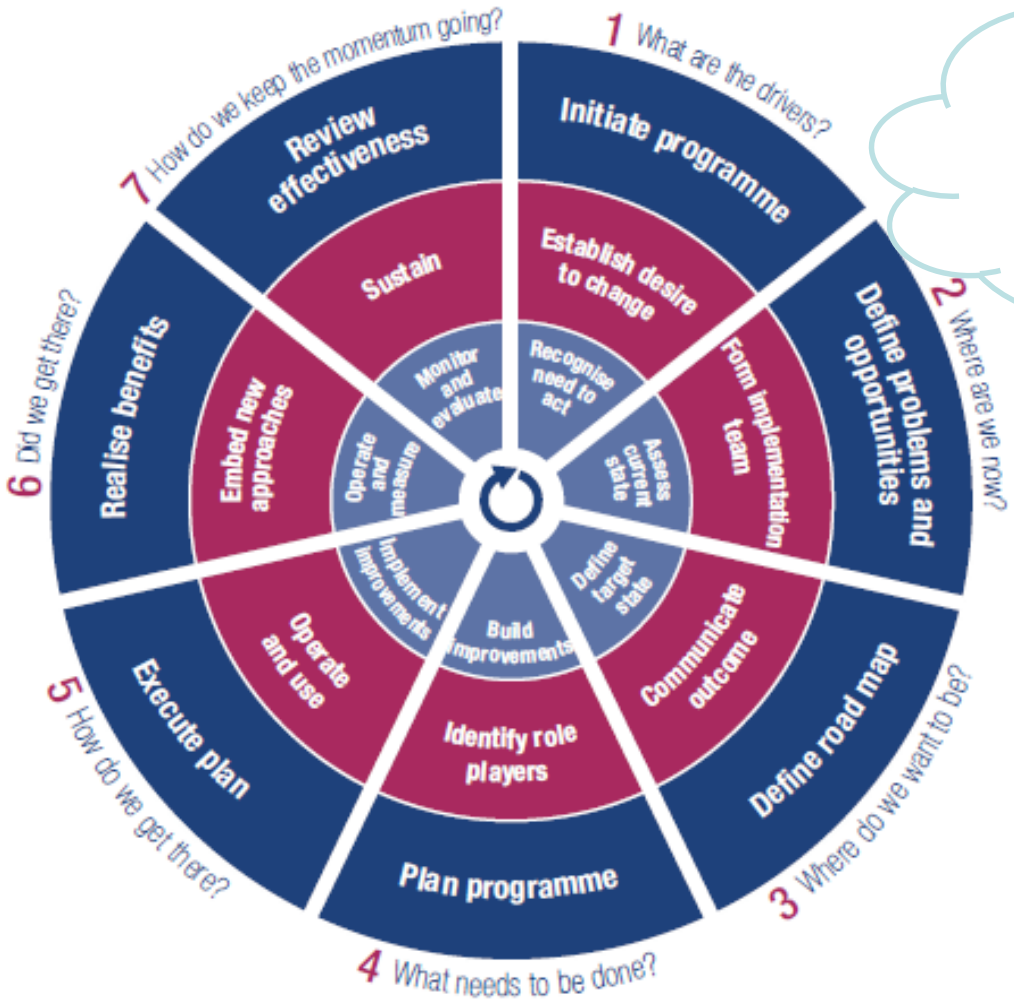
PRACTICAL COBIT 5

Implementing and Continually Improving ITG

"The New Life Cycle Model"

A Business Framework for the Governance and Management of Enterprise IT

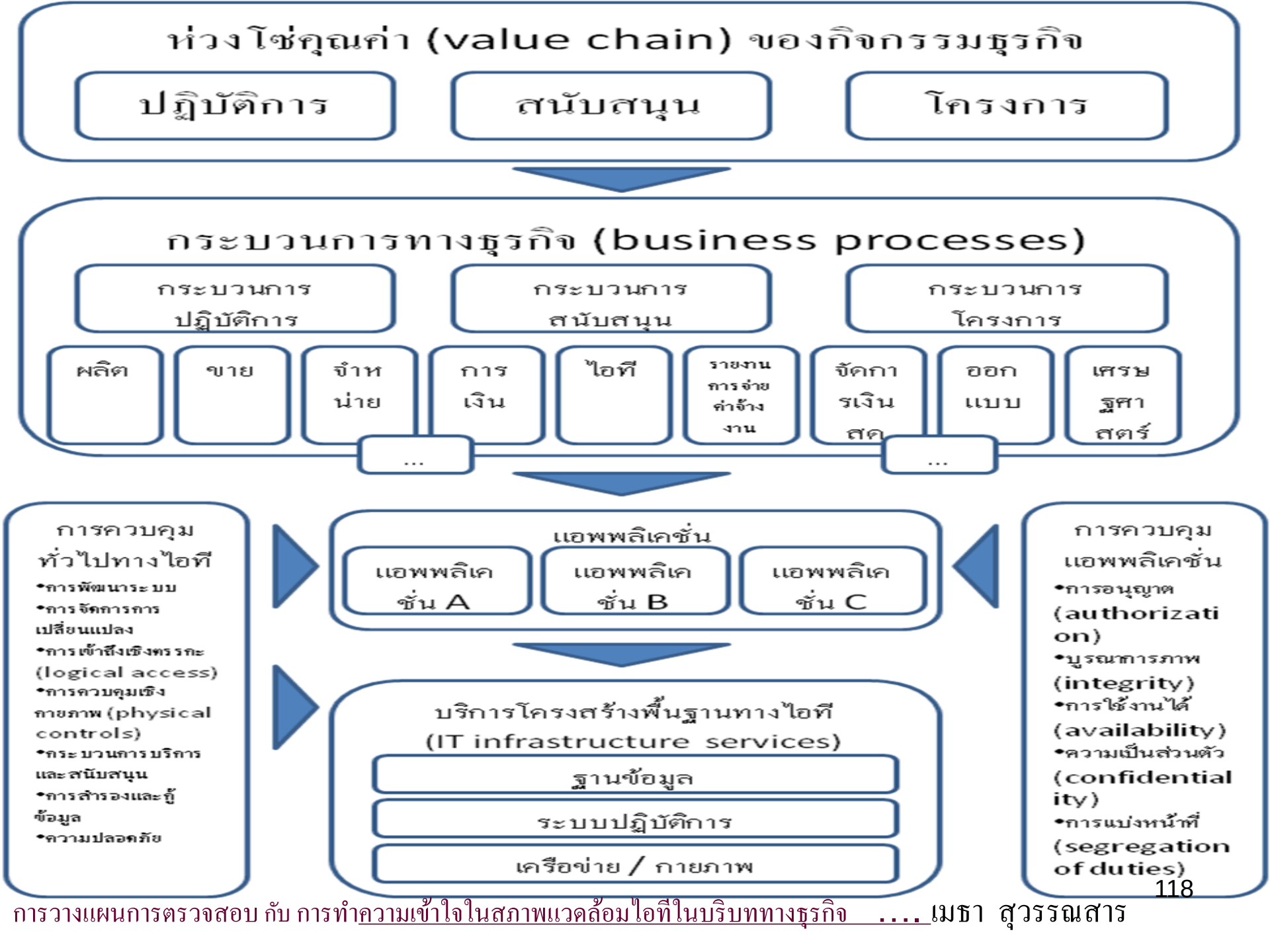
COBIT 5 and The Seven Phases of the Implementation Life Cycle



How to improve your Business / Please mention…++

- **Programme management** (outer ring)
- **Change enablement** (middle ring)
- **Continual improvement life cycle** (inner ring)

Resource : ISACA

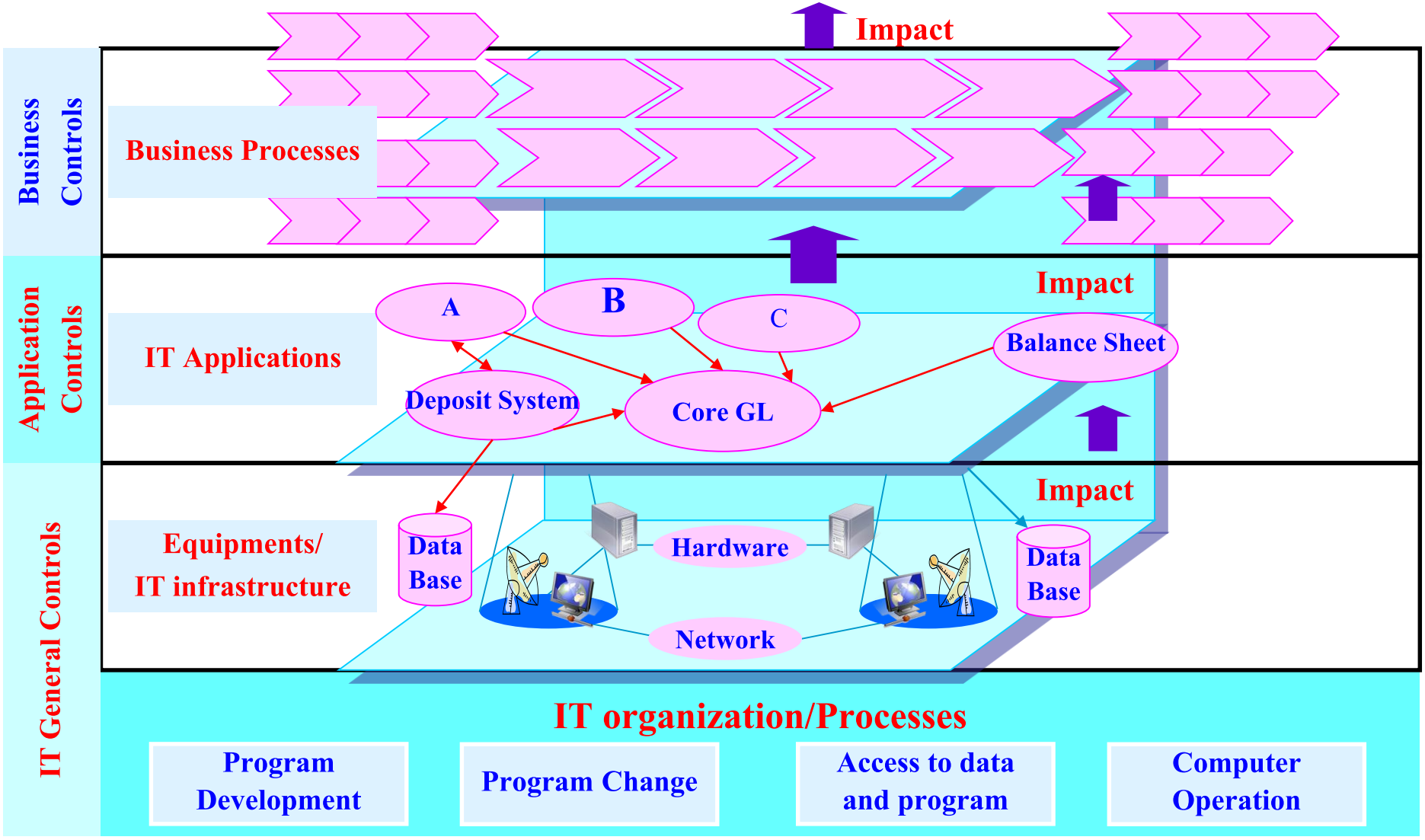

ห่วงโซ่คุณค่า (value chain) ของกิจกรรมธุรกิจ
ปฏิบัติการ
สนับสนุน
โครงการ
กระบวนการทางธุรกิจ (business processes)
กระบวนการ ปฏิบัติการ
กระบวนการ สนับสนุน
กระบวนการ โครงการ
ผลิต
ขาย
จำหน่าย
การเงิน
ไอที
รายงานการจ่ายค่าจ้างงาน
จัดการเงินสด
ออกแบบ
เศรษฐศาสตร์
...
...
การควบคุมทั่วไปทางไอที
•การพัฒนาระบบ
•การจัดการการเปลี่ยนแปลง
•การเข้าถึงเชิงตรรกะ (logical access)
•การควบคุมเชิงกายภาพ (physical controls)
•กระบวนการบริการและสนับสนุน
•การสำรองและกู้ข้อมูล
•ความปลอดภัย
แอพพลิเคชั่น
แอพพลิเคชั่น A
แอพพลิเคชั่น B
แอพพลิเคชั่น C
บริการโครงสร้างพื้นฐานทางไอที (IT infrastructure services)
ฐานข้อมูล
ระบบปฏิบัติการ
เครือข่าย / กายภาพ
การควบคุมแอพพลิเคชั่น
•การอนุญาต (authorization)
•บูรณภาพ (integrity)
•การใช้งานได้ (availability)
•ความเป็นส่วนตัว (confidentiality)
•การแบ่งหน้าที่ (segregation of duties)

Audit assurance for AC & C –Levels ?

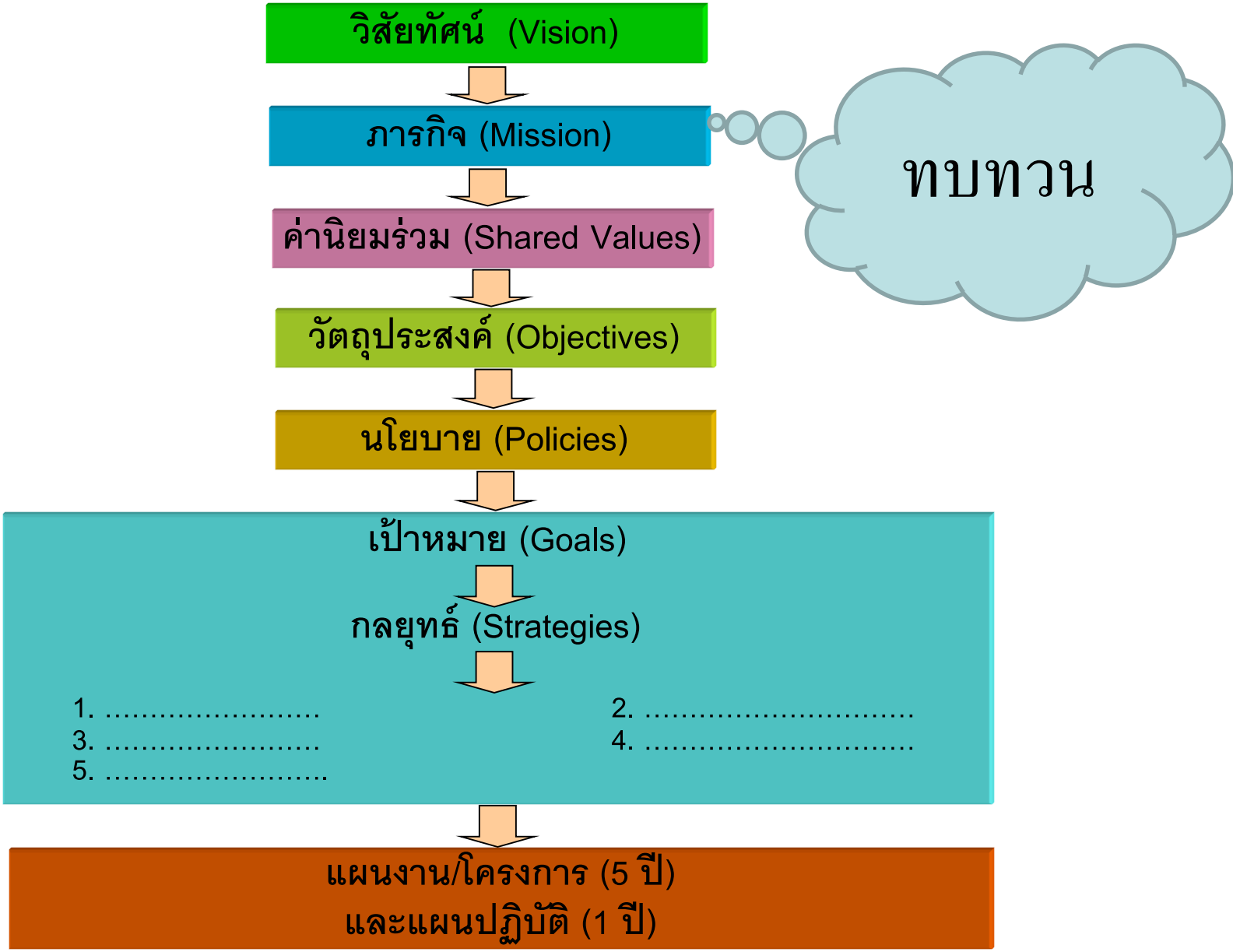
CSA by Yourself

Management and audit approach

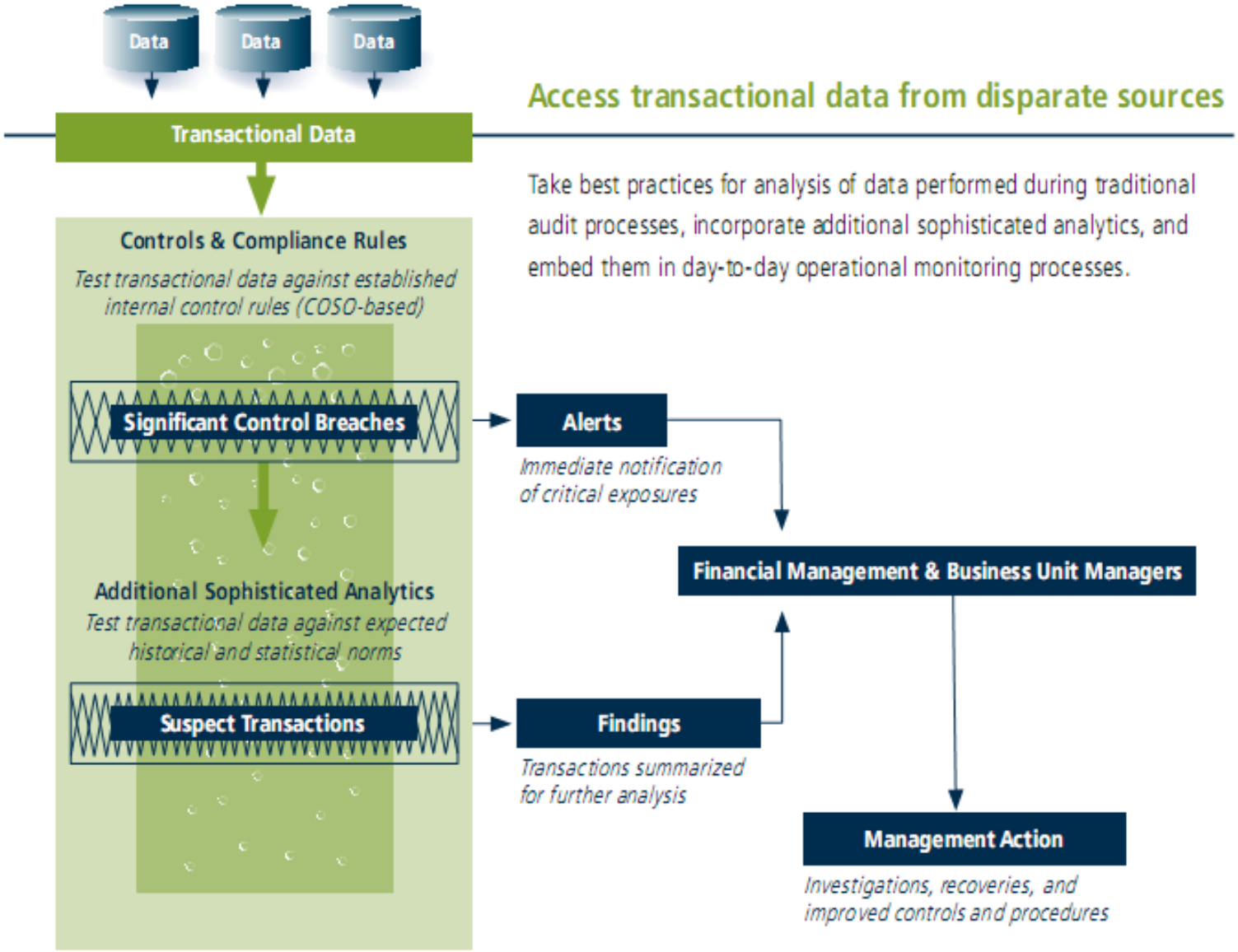
Financial Statements & Reports & Actions



มุมมองโลกแห่งการเปลี่ยนแปลง กับ โครงสร้างแผนบริหารขององค์กร



การติดตามความเสี่ยง และการควบคุมความเสี่ยง/ การบริหาร แบบต่อเนื่อง



Source : GTAG

CIO16 2014 AnnualConference

CIO16 Association of Thailand

Enterprise Business & Transformation

COBIT 5

THE IN DEPTH LOOK INTO GOVERNANCE FRAMEWORK

6 October 2014

By

Mr. Metha Suvanasarn

Vice President, Thailand Information Security Association (TISA)

www.itgthailand.com

COBIT 5

The In Depth Look Into Governance Framework

กระบวนการสำหรับการบริหารจัดการไอทีระดับองค์กร – ด้านการกำกับ/บอร์ด

- มั่นใจในการกำหนดกรอบการดำเนินงานการกำกับดูแล และการบำรุงรักษา
- มั่นใจในการส่งมอบผลประโยชน์
- มั่นใจในความเสี่ยงที่เหมาะสม
- มั่นใจในการใช้ทรัพยากรให้ได้ประโยชน์สูงสุด
- มั่นใจในความโปร่งใสต่อผู้มีส่วนได้เสีย

COBIT 5

The In Depth Look Into Governance Framework

กระบวนการสำหรับการบริหารจัดการไอทีระดับองค์กร - ด้านการบริหารจัดการ

จัดวางแนว จัดทำแผน และจัดระบบ

ความสัมพันธ์ระหว่างเป้าหมายระดับองค์กรใน COBIT 5 กับเป้าหมายที่เกี่ยวข้องกับไอที

เป้าหมายที่เกี่ยวข้องกับไอที			เป้าหมายระดับองค์กร																
			คุณค่าจากการลงทุนในธุรกิจของผู้มีส่วนได้เสีย	กลุ่มของผลิตภัณฑ์และบริการที่มีความสามารถในการแข่งขัน	ความเสี่ยงทางธุรกิจที่ได้รับการจัดการ (การปกป้องคุ้มครองทรัพย์สิน)	การปฏิบัติตามกฎหมายและกฎระเบียบข้อบังคับต่างๆจากภายนอก	ความโปร่งใสทางการเงิน	วัฒนธรรมที่เน้นการบริการลูกค้า	บริการของธุรกิจที่มีความต่อเนื่องและความพร้อมให้บริการ	การตอบสนองอย่างฉับไวต่อการเปลี่ยนแปลงในสภาพแวดล้อมทางธุรกิจ	การตัดสินใจเชิงกลยุทธ์บนพื้นฐานของสารสนเทศ	ต้นทุนในการส่งมอบบริการที่ให้ประโยชน์สูงสุด	หน้าที่งานในกระบวนการทางธุรกิจที่ให้ประโยชน์สูงสุด	ต้นทุนของกระบวนการทางธุรกิจที่ให้ประโยชน์สูงสุด	โครงการเพื่อการเปลี่ยนแปลงทางธุรกิจที่เป็นการบริหารจัดการ	การปฏิบัติงานและบุคลากรที่มีประสิทธิภาพ	การปฏิบัติตามนโยบายภายในองค์กร	บุคลากรที่มีทักษะและแรงจูงใจ	วัฒนธรรมที่ส่งเสริมนวัตกรรมสำหรับผลิตภัณฑ์และการดำเนินธุรกิจ
			1.	2.	3.	4.	5.	6.	7.	8.	9.	10.	11.	12.	13.	14.	15.	16.	17.
			ด้านการเงิน					ด้านลูกค้า					ด้านกระบวนการภายใน					ด้านการเรียนรู้และเติบโต	
ด้านการเงิน	01	กลยุทธ์ด้านไอทีสอดคล้องไปในแนวทางเดียวกันกับกลยุทธ์ด้านธุรกิจ	P	P	S			P	S	P	P	S	P	S	P			S	S
	02	ไอทีเอื้ออำนวยและสนับสนุนให้ธุรกิจสามารถปฏิบัติตามกฎหมายและกฎระเบียบข้อบังคับของหน่วยงานภายนอก			S	P											P		
	03	ผู้บริหารระดับสูงให้คำมั่นในการตัดสินใจต่างๆ ที่เกี่ยวข้องกับไอที	P	S	S					S	S		S		P			S	S
	04	ความเสี่ยงของธุรกิจที่เกี่ยวข้องกับไอทีสามารถบริหารจัดการได้			P	S			P	S		P			S		S	S	
	05	ประโยชน์ที่ได้รับจริงจากกลุ่มของการลงทุนและการให้บริการในด้านต่างๆ ที่มีไอทีเป็นปัจจัยเอื้อ	P	P				S		S		S	S	P		S			S
	06	ต้นทุน ประโยชน์ และความเสี่ยงทางด้านไอทีที่มีความโปร่งใส	S		S		P				S	P		P					

COBIT 5

The In Depth Look Into Governance Framework

กระบวนการสำหรับการบริหารจัดการไอทีระดับองค์กร - ด้านการบริหารจัดการ

จัดวางแนว จัดทำแผน และจัดระบบ

ความสัมพันธ์ระหว่างเป้าหมายระดับองค์กรใน COBIT 5 กับเป้าหมายที่เกี่ยวข้องกับไอที

			เป้าหมายระดับองค์กร																
			คุณค่าจากการลงทุนในธุรกิจของผู้มีส่วนได้เสีย	กลุ่มของผลิตภัณฑ์และบริการที่มีความสามารถในการแข่งขัน	ความเสี่ยงทางธุรกิจที่ได้รับการจัดการ (การปกป้องคุ้มครองทรัพย์สิน)	การปฏิบัติตามกฎหมายและกฎระเบียบข้อบังคับจากภายนอก	ความโปร่งใสทางการเงิน	วัฒนธรรมที่เน้นการบริการลูกค้า	บริการของธุรกิจมีความต่อเนื่องและความพร้อมให้บริการ	การตอบสนองอย่างฉับไวต่อการเปลี่ยนแปลงในสภาพแวดล้อมทางธุรกิจ	การตัดสินใจเชิงกลยุทธ์บนพื้นฐานของสารสนเทศ	ต้นทุนในการส่งมอบบริการที่ให้ประโยชน์สูงสุด	หน่วยงานในกระบวนการทางธุรกิจที่ให้ประโยชน์สูงสุด	ต้นทุนของกระบวนการทางธุรกิจที่ให้ประโยชน์สูงสุด	ชุดโครงการเพื่อการเปลี่ยนแปลงทางธุรกิจที่ได้รับการบริหารจัดการ	การปฏิบัติงานและบุคลากรที่มีประสิทธิภาพ	การปฏิบัติตามนโยบายภายในองค์กร	บุคลากรที่มีทักษะและแรงจูงใจ	วัฒนธรรมที่ส่งเสริมนวัตกรรมสำหรับผลิตภัณฑ์และการดำเนินธุรกิจ
			1.	2.	3.	4.	5.	6.	7.	8.	9.	10.	11.	12.	13.	14.	15.	16.	17.
เป้าหมายที่เกี่ยวข้องกับไอที			ด้านการเงิน					ด้านลูกค้า					ด้านกระบวนการภายใน					ด้านการเรียนรู้และเติบโต	
ด้านลูกค้า	07	การส่งมอบบริการด้านไอทีเป็นไปตามความต้องการของธุรกิจ	P	P	S	S		P	S	P	S		P	S	S			S	S
	08	การใช้ระบบงาน สารสนเทศ และเทคโนโลยีอย่างเหมาะสม	S	S	S			S	S		S	S	P	S		P		S	S

COBIT 5

The In Depth Look Into Governance Framework

กระบวนการสำหรับการบริหารจัดการไอทีระดับองค์กร - ด้านการบริหารจัดการ

จัดวางแนว จัดทำแผน และจัดระบบ

ความสัมพันธ์ระหว่างเป้าหมายระดับองค์กรใน COBIT 5 กับเป้าหมายที่เกี่ยวข้องกับไอที

			เป้าหมายระดับองค์กร																	
			คุณค่าจากการลงทุนในธุรกิจของผู้มีส่วนได้เสีย	พอร์ตผลิตภัณฑ์และบริการที่มีความสามารถในการแข่งขัน	ความเสี่ยงทางธุรกิจที่เกิดจากการจัดการ (การปกป้องสินทรัพย์)	การปฏิบัติตามกฎหมายและข้อบังคับภายนอก	ความโปร่งใสทางการเงิน	วัฒนธรรมที่เน้นการบริการลูกค้า	บริการของธุรกิจที่มีความต่อเนื่องและความพร้อมให้บริการ	การตอบสนองอย่างรวดเร็วต่อการเปลี่ยนแปลงในสภาพแวดล้อมทางธุรกิจ	การตัดสินใจเชิงกลยุทธ์บนพื้นฐานของสารสนเทศ	ต้นทุนในการส่งมอบบริการที่ให้ประโยชน์สูงสุด	หน้าที่งานในกระบวนการทางธุรกิจที่ให้ประโยชน์สูงสุด	ต้นทุนของกระบวนการทางธุรกิจที่ให้ประโยชน์สูงสุด	ชุดโครงการที่การเปลี่ยนแปลงทางธุรกิจที่สัมพันธ์กับการบริหารจัดการ	การปฏิบัติงานและบุคลากรที่มีประสิทธิภาพ	การปฏิบัติตามนโยบายภายในองค์กร	ทุนของบุคลากรที่มีทักษะและแรงจูงใจ	วัฒนธรรมที่ส่งเสริมนวัตกรรมสำหรับผลิตภัณฑ์และการดำเนินธุรกิจ
ด้านกระบวนการภายใน	09	ความคล่องตัวทางด้านไอที	S	P	S			S		P			P		S	S		S	P
	10	ความมั่นคงปลอดภัยของสารสนเทศ โครงสร้างพื้นฐานในการประมวลผล และระบบงาน			P	P			P								P		
	11	การใช้สินทรัพย์ ทรัพยากร และสมรรถนะทางด้านไอทีให้ได้ประโยชน์สูงสุด	P	S						S		P	S	P	S	S			S
	12	การเอื้ออำนวยและสนับสนุนการทำงานของกระบวนการทางธุรกิจโดยบูรณาการระบบงานและเทคโนโลยีเข้าไปใช้ในกระบวนการทางธุรกิจ	S	P	S			S		S		S	P	S	S	S			S
	13	การส่งมอบชุดโครงการต่างๆ ก่อให้เกิดประโยชน์ ตรงเวลา ตามงบประมาณที่ตั้งไว้ และตามความต้องการและมาตรฐานด้านคุณภาพ	P	S	S			S				S		S	P				
	14	ความพร้อมใช้ของสารสนเทศที่เชื่อถือได้และมีประโยชน์ในการตัดสินใจ	S	S	S	S			P		P		S							
	15	ไอทีที่ปฏิบัติตามนโยบายภายในขององค์กร			S	S											P		

COBIT 5

The In Depth Look Into Governance Framework

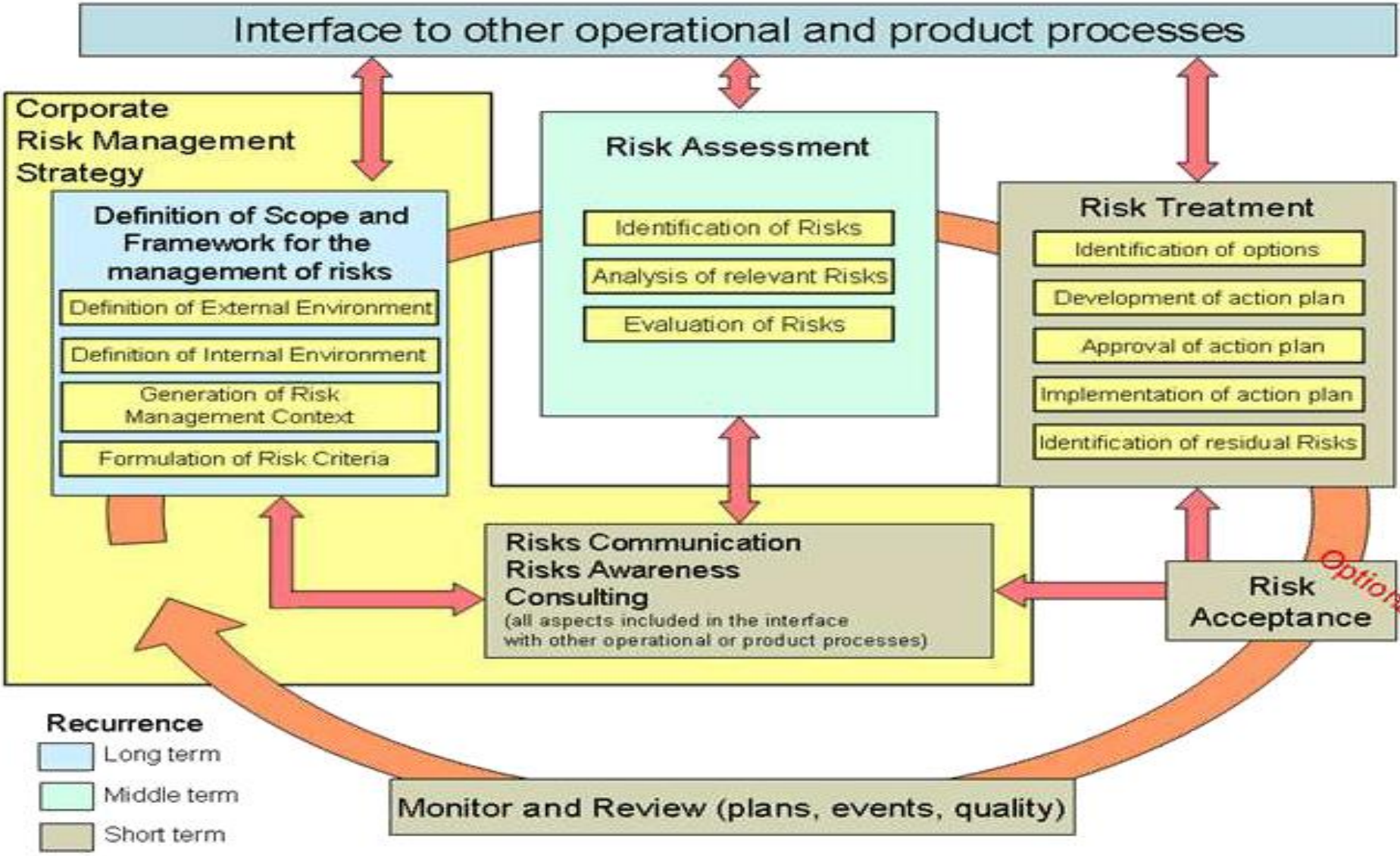
กระบวนการสำหรับการบริหารจัดการไอทีระดับองค์กร - ด้านการบริหารจัดการ

จัดวางแนว จัดทำแผน และจัดระบบ

ความสัมพันธ์ระหว่างเป้าหมายระดับองค์กรใน COBIT 5 กับเป้าหมายที่เกี่ยวข้องกับไอที

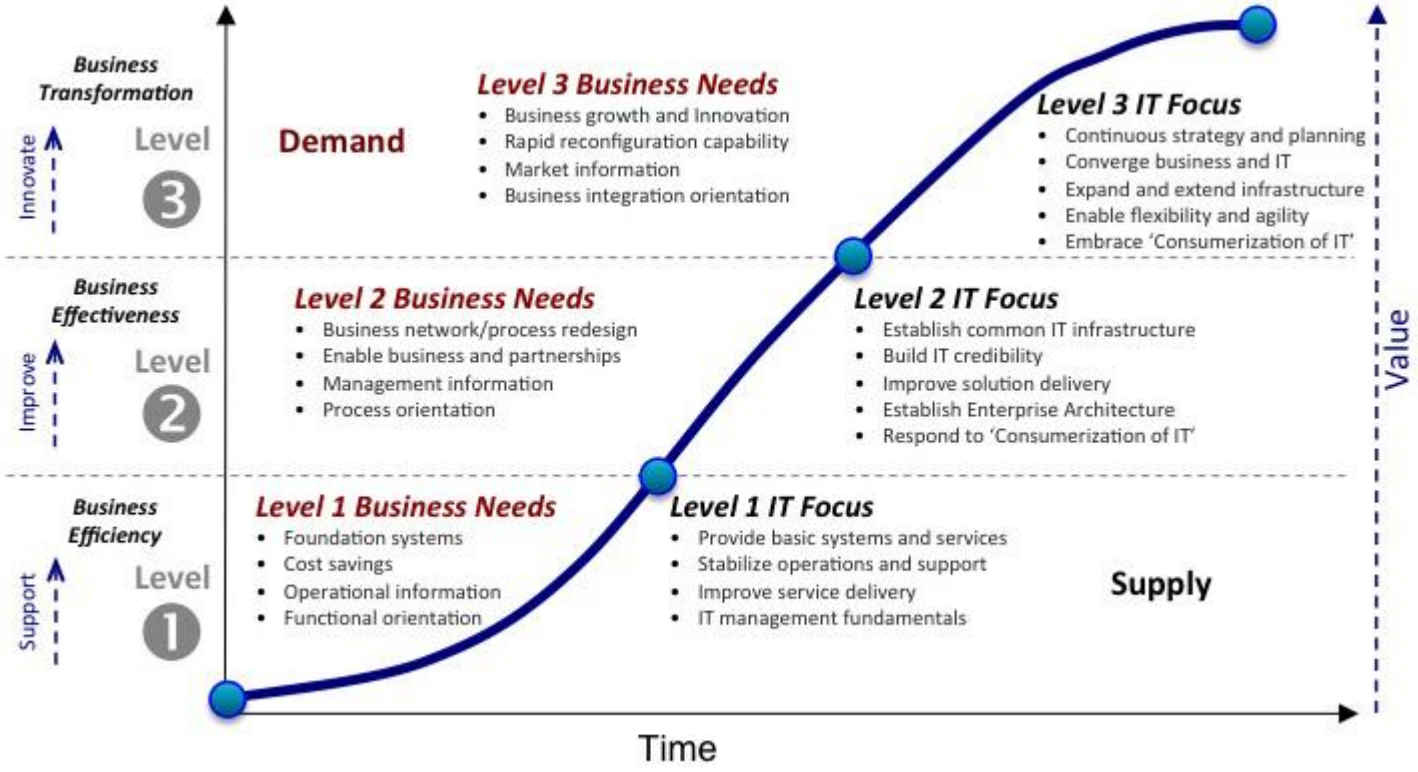
			เป้าหมายระดับองค์กร																
			คุณค่าจากการลงทุนในธุรกิจของผู้มีส่วนได้เสีย	กลุ่มของผลิตภัณฑ์และบริการที่มีความสามารถในการแข่งขัน	ความเสี่ยงทางธุรกิจที่ได้รับการจัดการ (การปกป้องคุ้มครองทรัพย์สิน)	การปฏิบัติตามกฎหมายและกฎระเบียบข้อบังคับจากภายนอก	ความโปร่งใสทางการเงิน	วัฒนธรรมที่เน้นการบริการลูกค้า	บริการของธุรกิจมีความต่อเนื่องและความพร้อมให้บริการ	การตอบสนองอย่างฉับไวต่อการเปลี่ยนแปลงในสภาพแวดล้อมทางธุรกิจ	การตัดสินใจเชิงกลยุทธ์บนพื้นฐานของสารสนเทศ	ต้นทุนในการส่งมอบบริการที่ให้ประโยชน์สูงสุด	หน่วยงานในกระบวนการทางธุรกิจที่ให้ประโยชน์สูงสุด	ต้นทุนของกระบวนการทางธุรกิจที่ให้ประโยชน์สูงสุด	บุคโครงการเพื่อการเปลี่ยนแปลงทางธุรกิจที่ได้รับการบริหารจัดการ	การปฏิบัติงานและบุคลากรที่มีประสิทธิภาพ	การปฏิบัติตามนโยบายภายในองค์กร	บุคลากรที่มีทักษะและแรงจูงใจ	วัฒนธรรมที่ส่งเสริมนวัตกรรมสำหรับผลิตภัณฑ์และการดำเนินธุรกิจ
			1.	2.	3.	4.	5.	6.	7.	8.	9.	10.	11.	12.	13.	14.	15.	16.	17.
เป้าหมายที่เกี่ยวข้องกับไอที			ด้านการเงิน					ด้านลูกค้า					ด้านกระบวนการภายใน					ด้านการเรียนรู้และเติบโต	
ด้านการเรียนรู้และเติบโต	16	บุคลากรทั้งทางด้านไอทีและด้านธุรกิจที่มีความสามารถและมีแรงจูงใจ	S	S	P			S		S						P		P	S
	17	ความรู้ ความเชี่ยวชาญ และการริเริ่มดำเนินการเพื่อนวัตกรรมทางธุรกิจ	S	P				S		P	S		S		S			S	P

The Risk Management Process



From Wikipedia **IT risk management** The Risk Management Process, according to ISO Standard

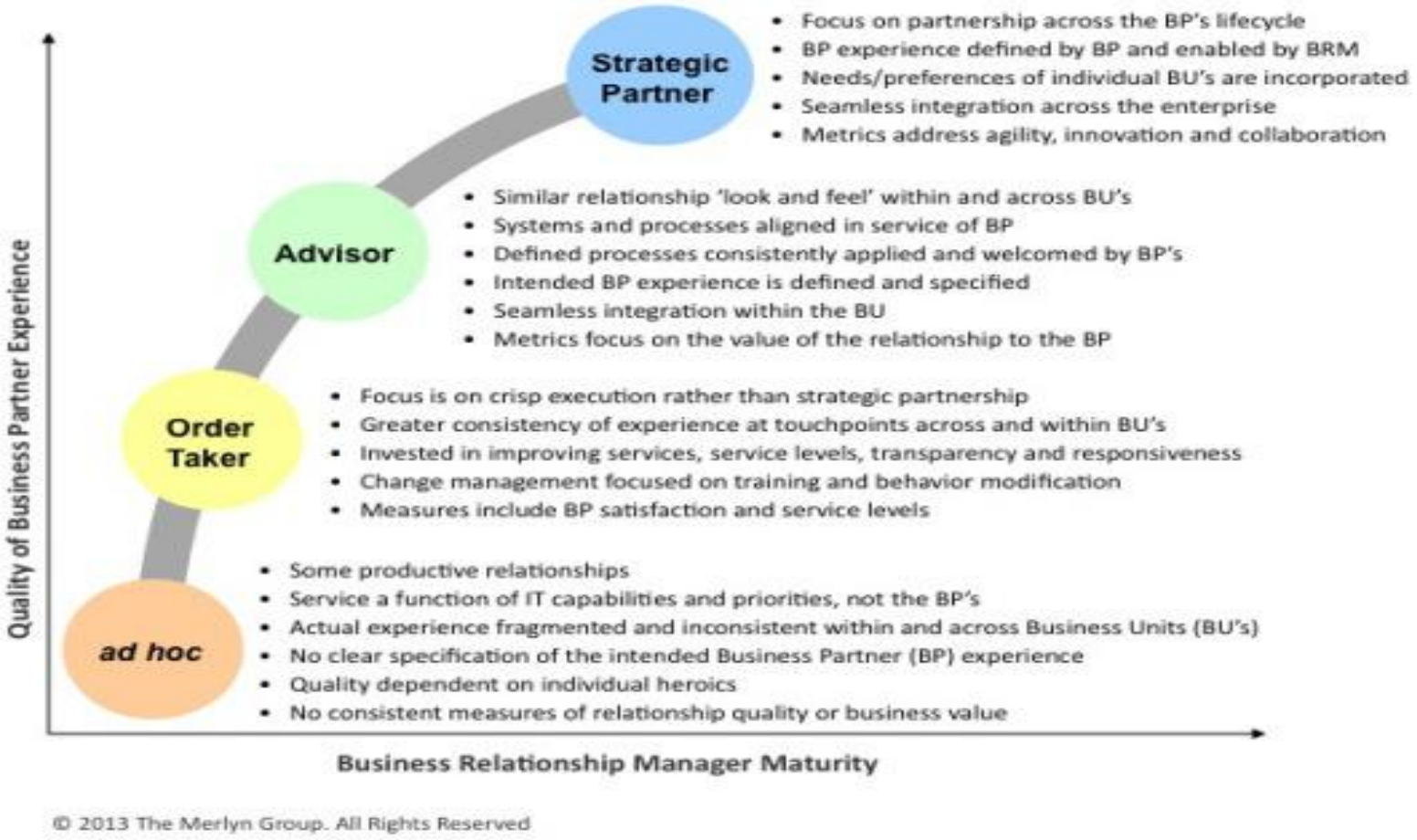
COBIT 5
The In Depth Look onto Governance Framework



http://vaughanmerlyn.com/tag/business-it-maturity/

COBIT 5

The In Depth Look onto Governance Framework



http://vaughanmerlyn.com/tag/business-it-maturity/

COBIT 5

The In Depth Look onto Governance Framework

Typical Competencies Required of the BRM

:Drives Value Realization

:Understands Business Environment

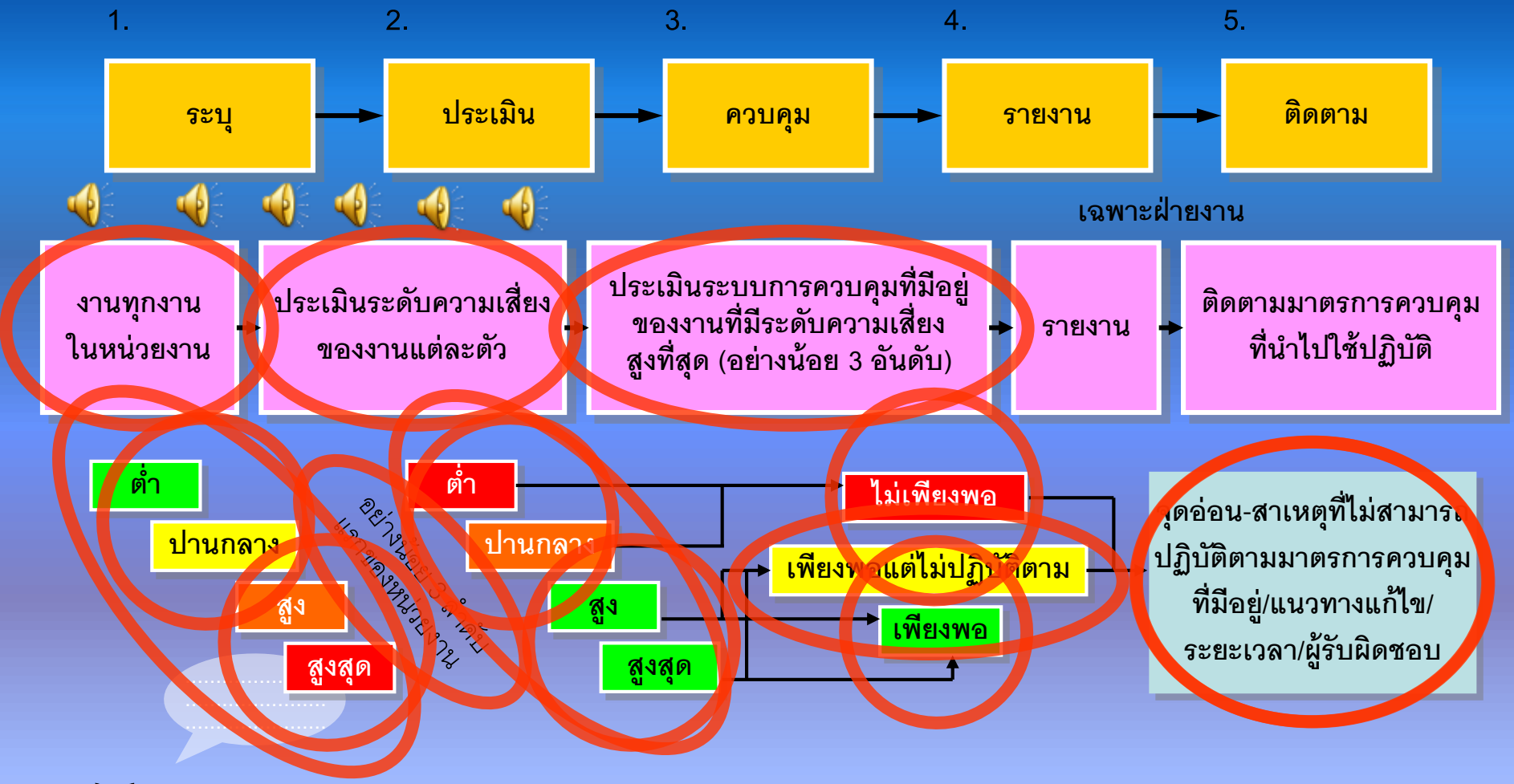
:Aligns IT with the Business

First, let me say that some readers will fume at the subheading. "IT and the Business are one and the same!" they shout. While this may reflect a laudable perspective (and one that will gradually materialize as IT-business convergence takes place) it is rarely, if ever, the case today.

Unless your business *is* information technology, then "business" is where profits are generated, and IT organizations work in support of that

สรุป ขั้นตอนปฏิบัติของการประเมินการควบคุมความเสี่ยงด้วยตนเอง- CSA

(Operational Risk Self Assessment : ORSA) – มุมมองของ Business Risk & IT-Related Risk



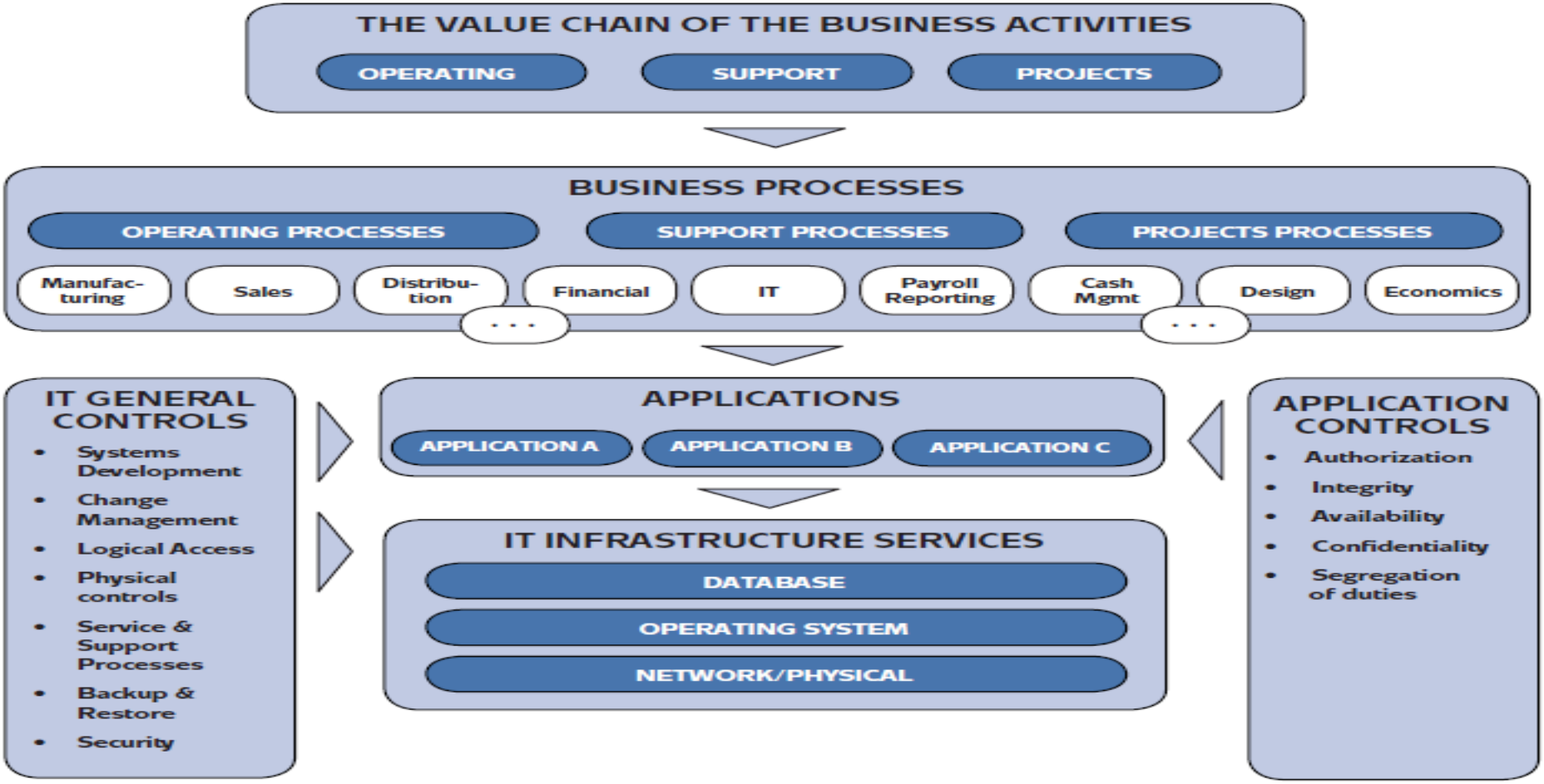
สรุป : ความเข้าใจ การ บริหารความเสี่ยง เบื้องต้น ทางด้าน Business Risk และ การบูรณาการกับ IT Risk

GRC & Developing the IT Audit Plan

Understanding the Business & Risk IT + IT Risk

IT Environment Factors & Management

Understanding the IT environment in a business context



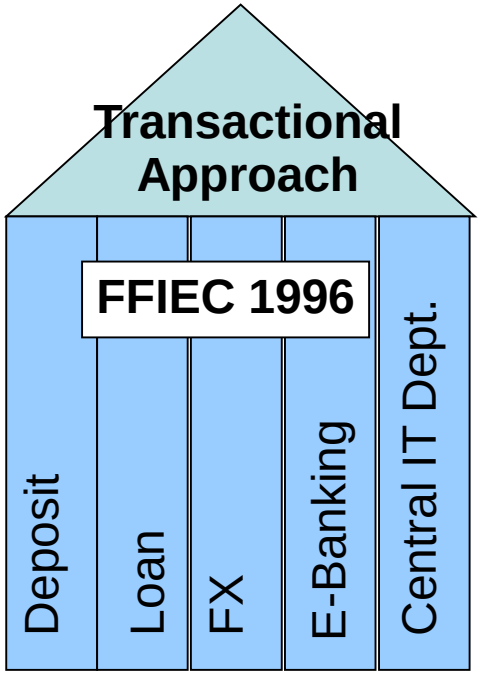
Source: The Institute of Internal Auditors

เปรียบเทียบการตรวจสอบแนวทางเดิมกับแนวทางใหม่ที่ได้ผลมาก

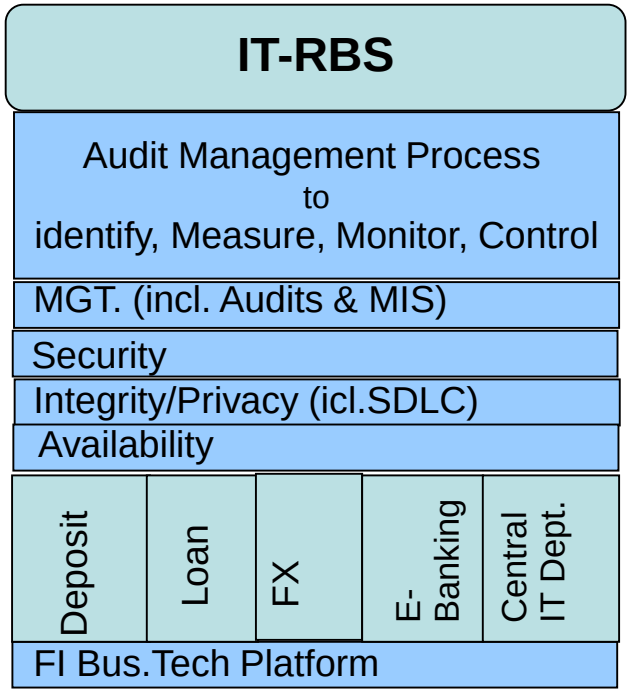
IT Audit &
Non-IT Audit

SR98-9 IT Risks

แนวการตรวจสอบ
ข้ามสายงาน-ยุค
ปัจจุบัน



Operational Risk Management



Integrated Audit

ความเสี่ยงกับการจัดการที่ดี

ต้องรอบรู้	ความเสี่ยง	สารพัด
ต้องเร่งรัด	จัดการ	ความเสียหาย
ก่อนจะเกิด	หลายแบบ	ให้แยบคาย
ทุ่มใจกาย	สุดชีวิต	พิชิตงาน

Q & A

เกี่ยวกับ Consolidated + Integrated Risk Management **->GRC->GEIT** และ การสร้างคุณค่าเพิ่มได้อย่างไร?


Thank you