หลักสูตรผู้บริหารเทคโนโลยีสารสนเทศระดับสูง

CIO (Chief Information Officer) รุ่นที่ 25

# การบริหารความเสี่ยงด้านไอซีที

# ICT Risk Management

วันที่ 14 มกราคม 2558

ณ ห้องกมลมาส ชั้น 6 โรงแรมเดอะสุโกศล

++ Integrated Risk Management

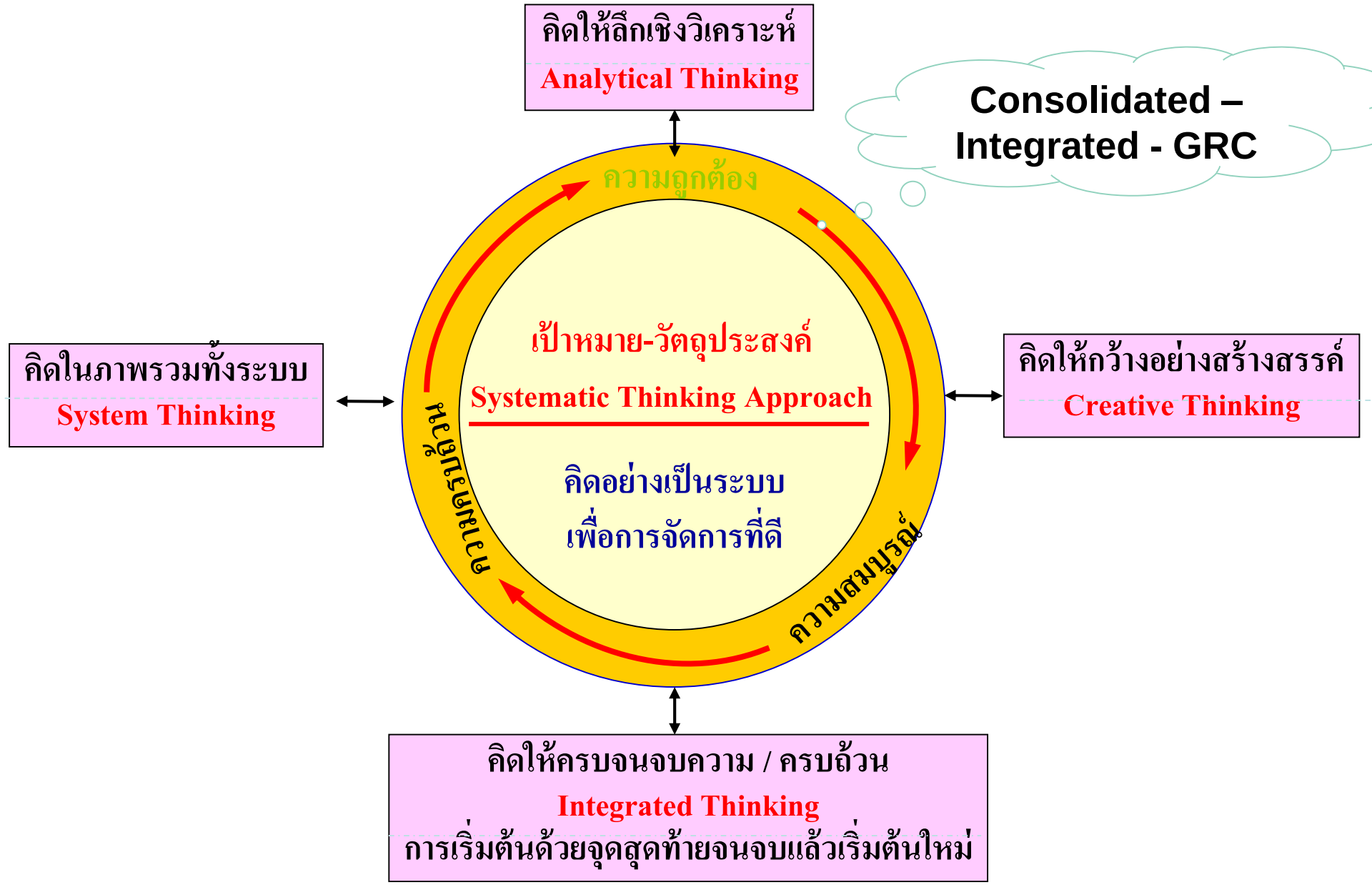
โดย

**นาย เมธา สุวรรณสาร**

CGEIT; CRISC; CRMA; CIA; CPA

www.itgthailand.com

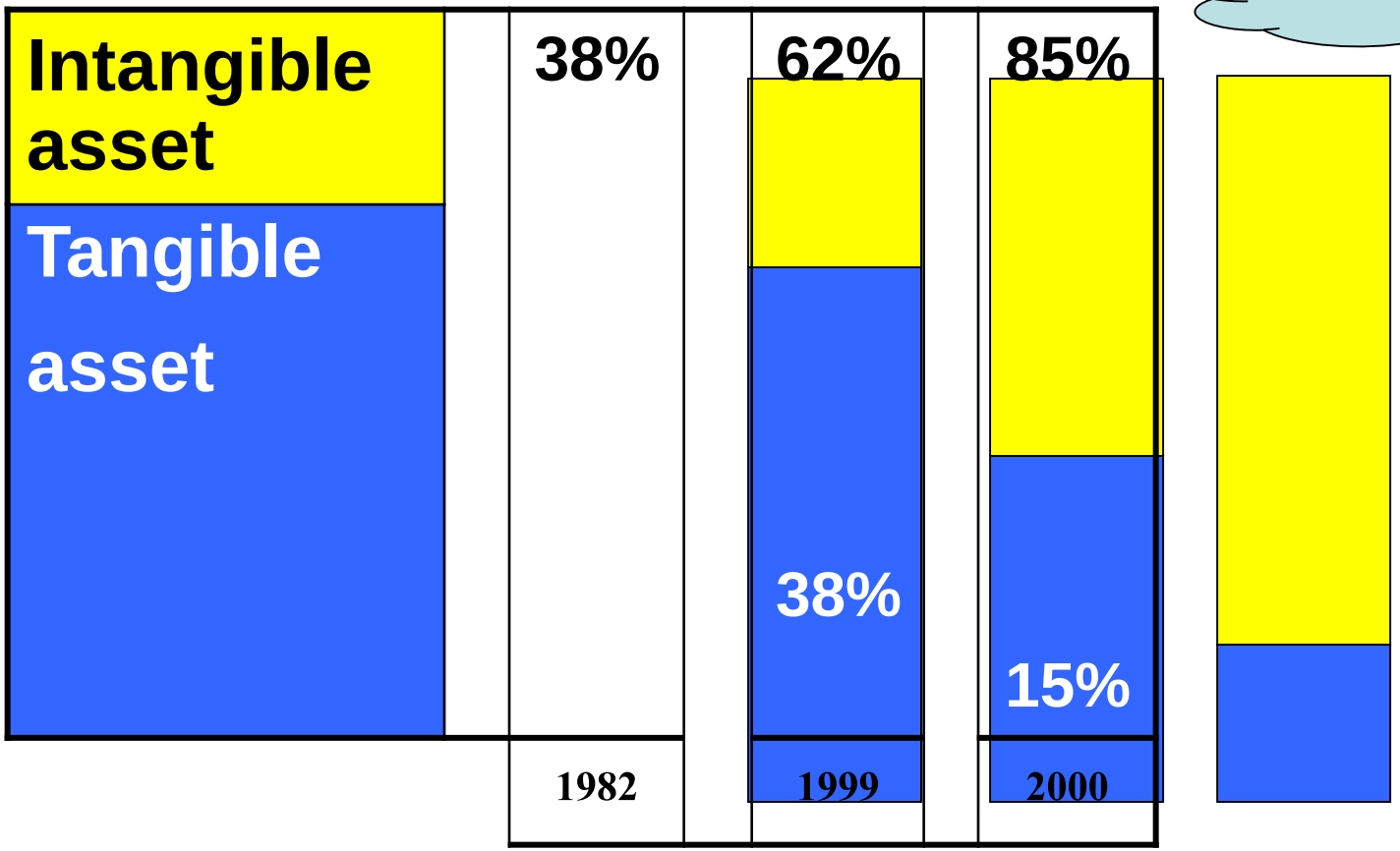
# การบริหารความเสี่ยง กับ ความคิดอย่างเป็นระบบ / IT & Non IT เพื่อการจัดการที่ดี



# Tangible to Intangible asset

## and Value Creation / GRC & ITG Perspective

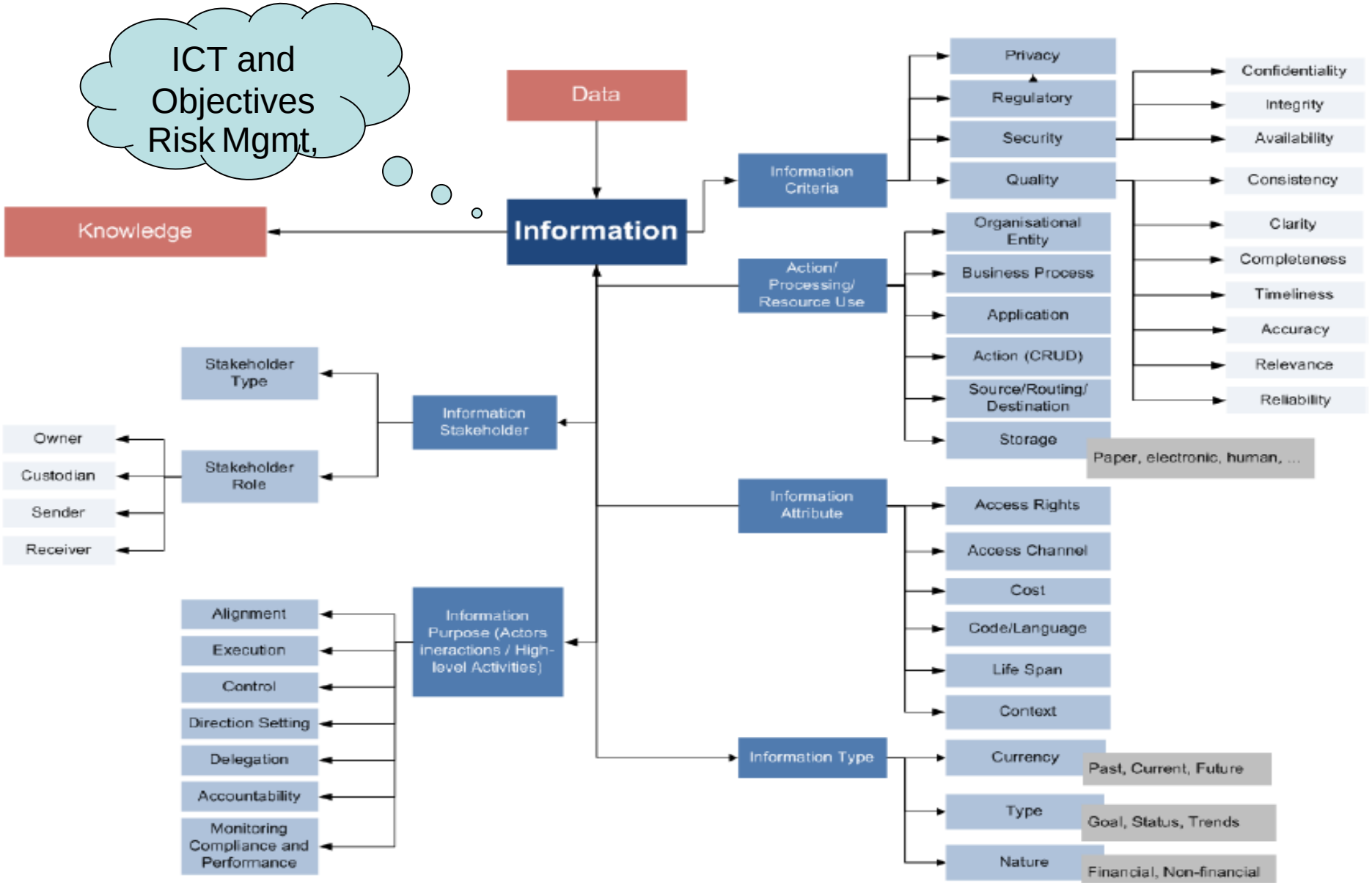
ทบทวน บางมุมมองหากมีเวลา พอนะครับ




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

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

# COBIT 5 Information Reference Model – Starting from Paper Exposure Draft




Source : ISACA

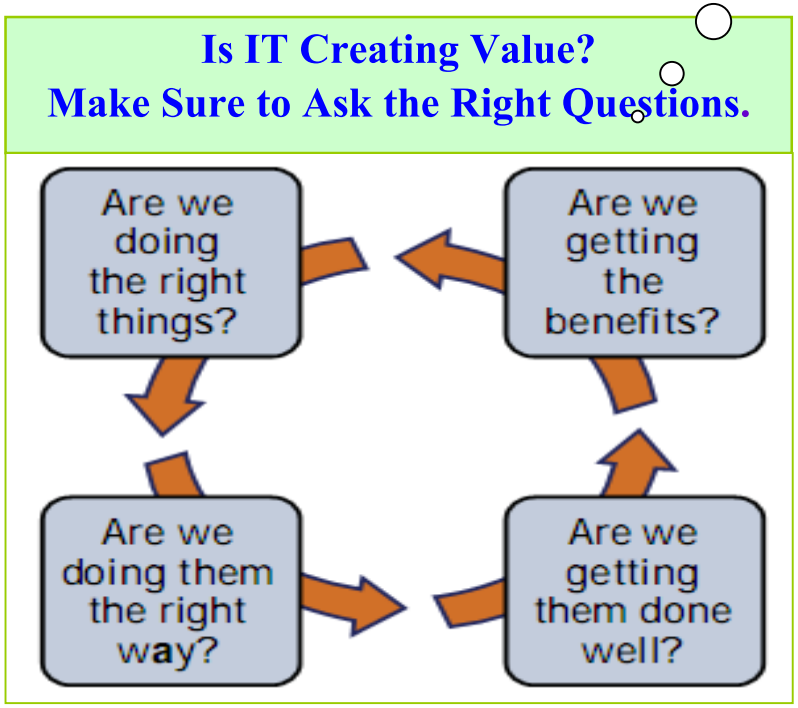
# Unlocking Value & Val IT

## 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?

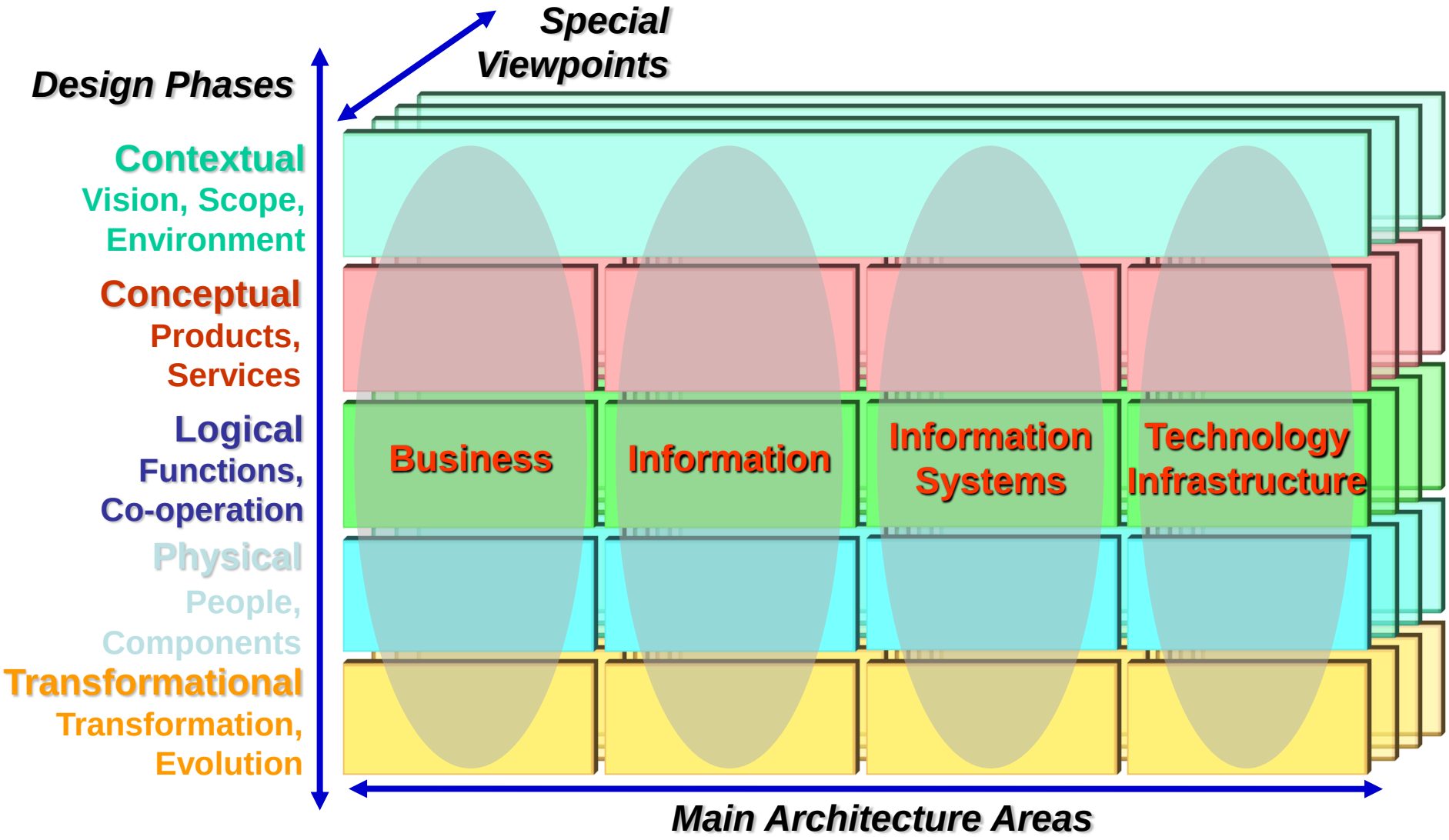
You are here…

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



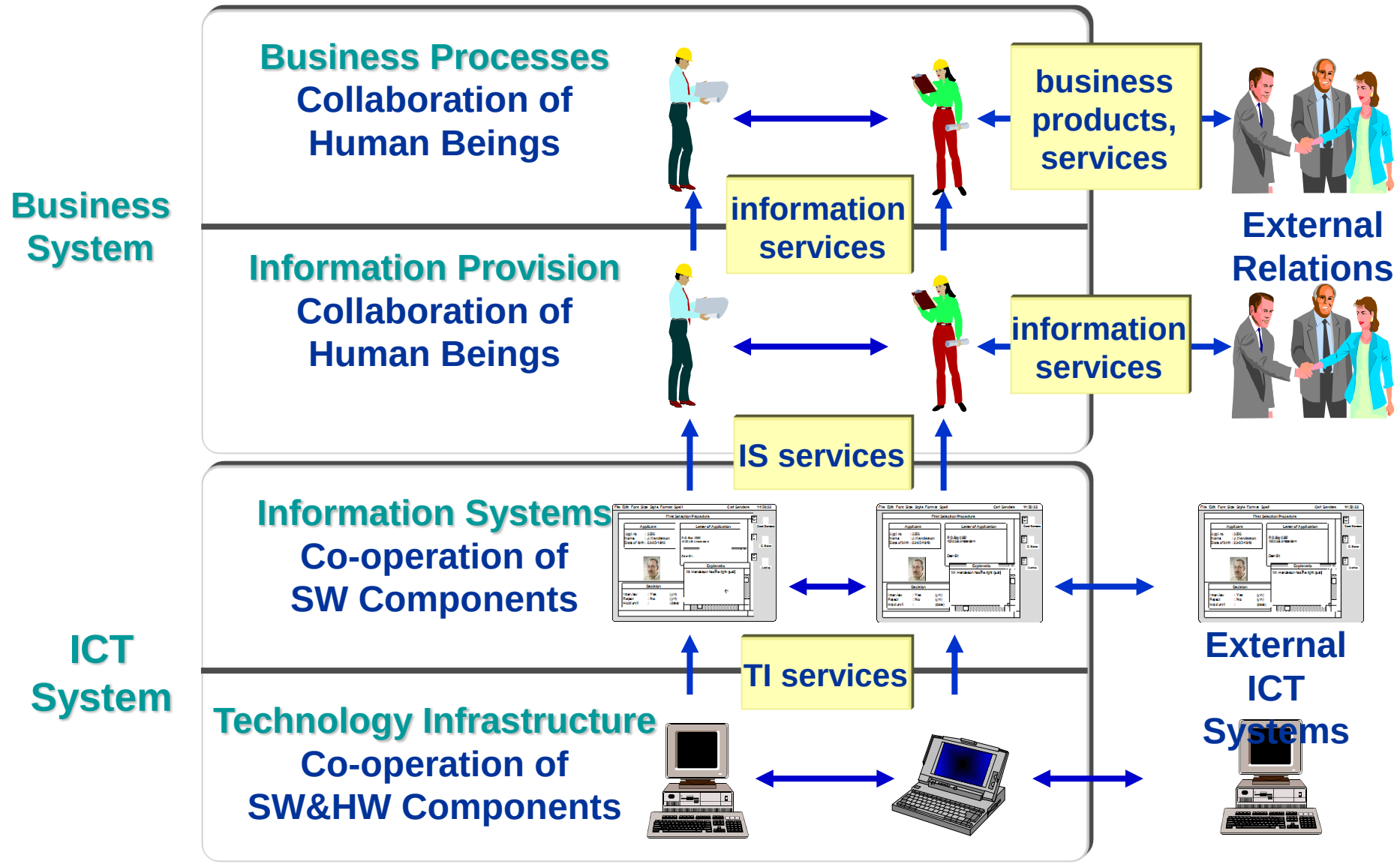

Resource : IT Governance Institute

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



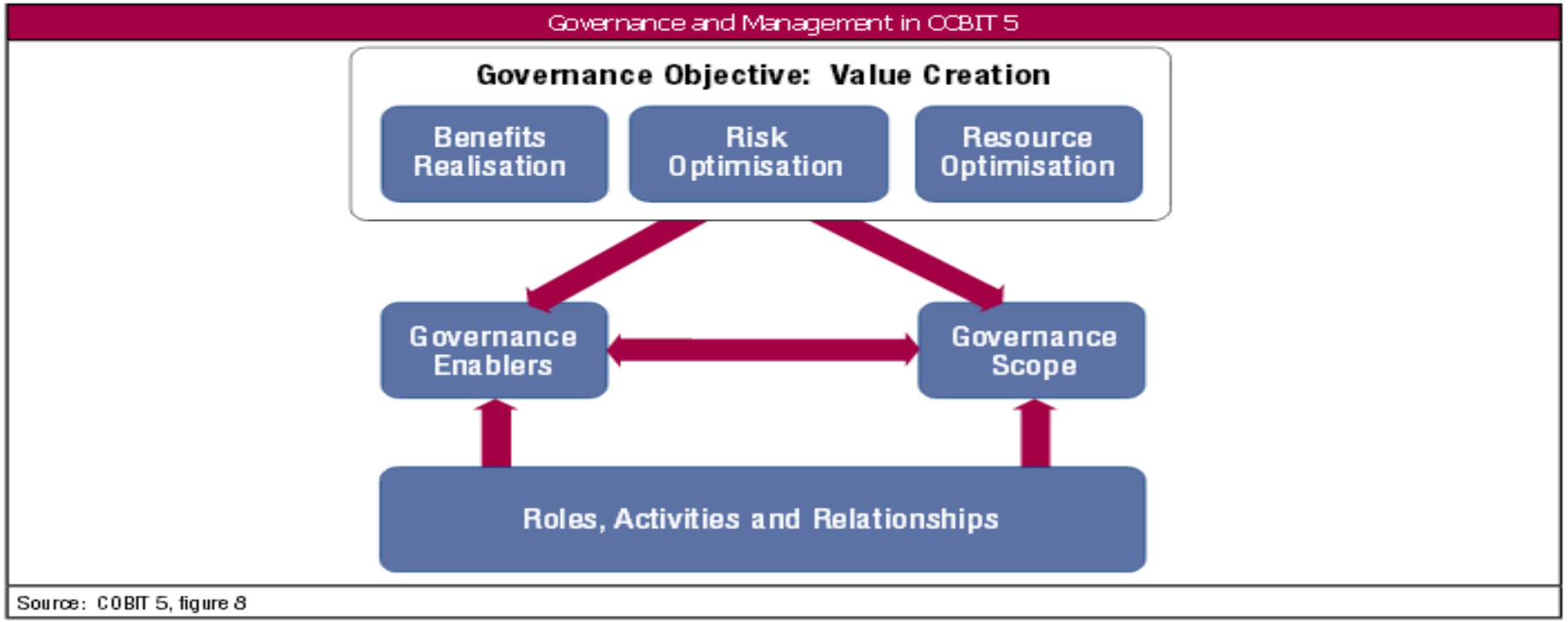

Adopt and Adapt from IAF

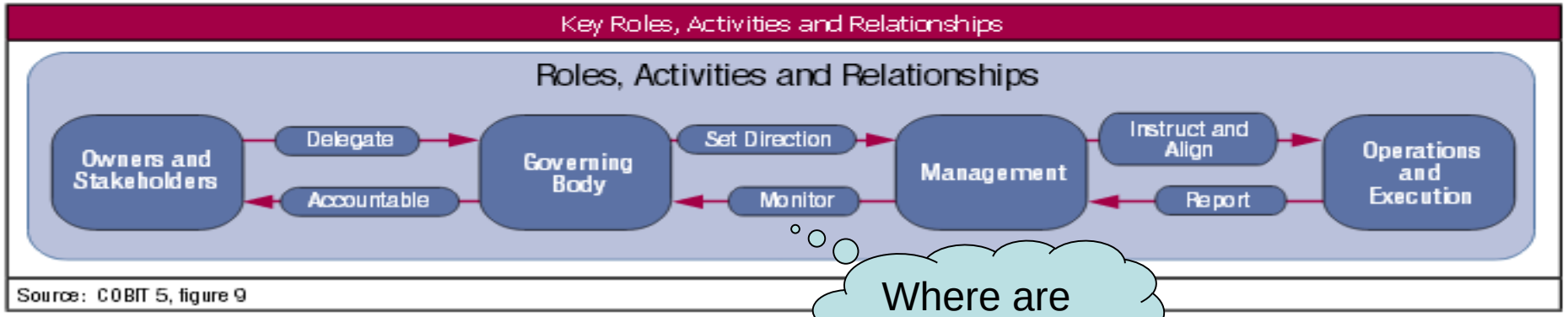
# The ICT enabled Enterprise and control by design




Adopt and Adapt from IAF

# COBIT 5 and Key Roles-Activities- Relationship




Where are you ?

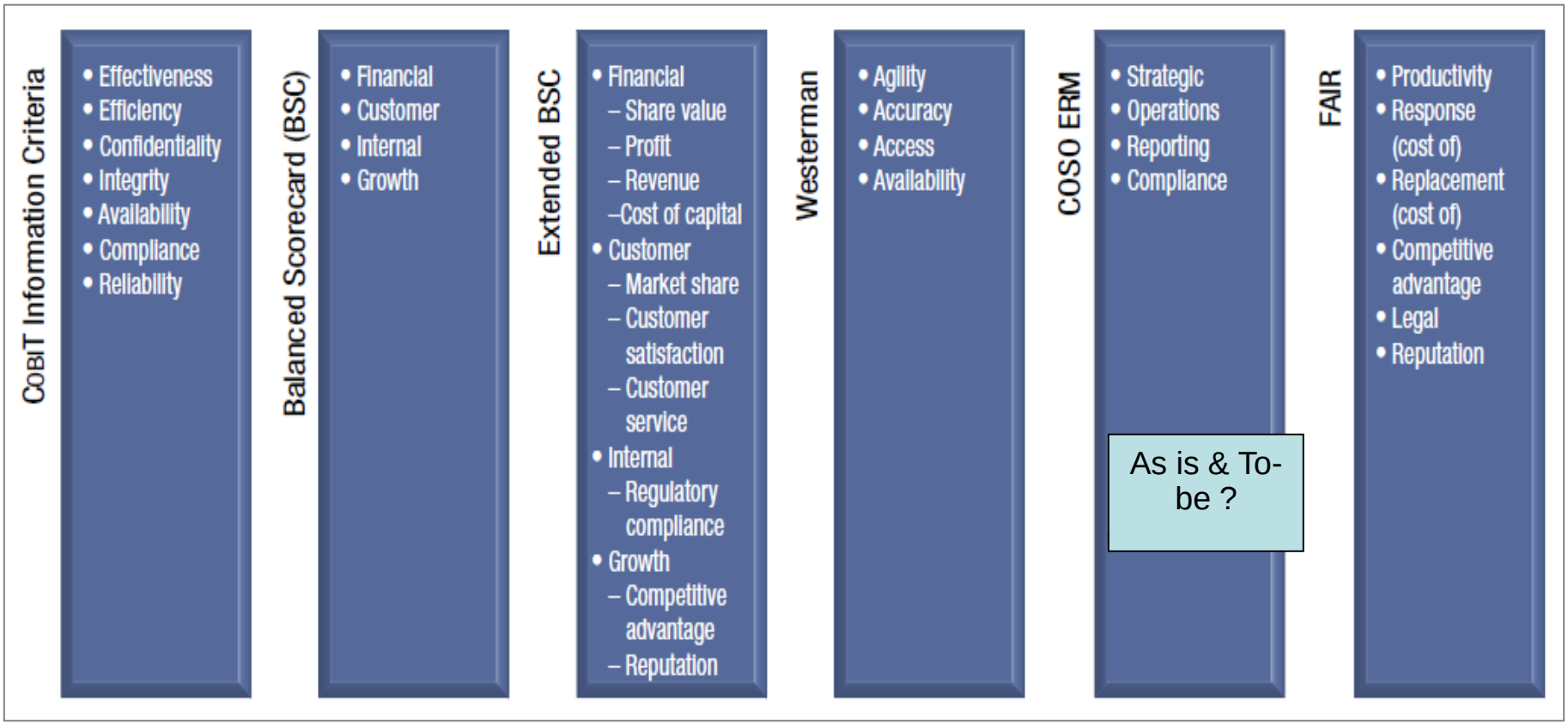
Source : ISACA

# GRC & Risk IT Practitioner Guide

## EXPRESSING AND DESCRIBING RISK

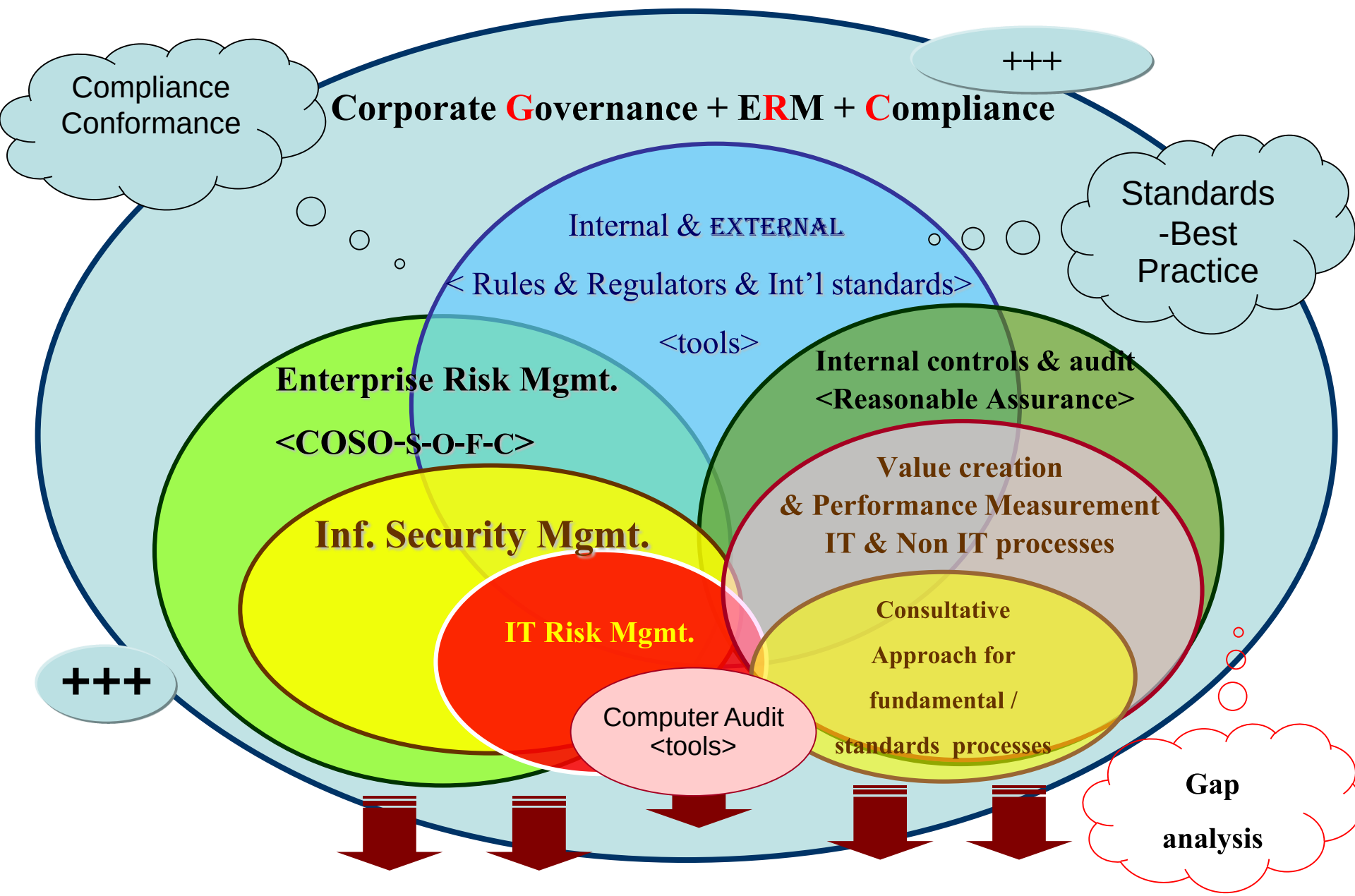
Where Mgmt. & Related Risk –Control-Audit Should be ?

### Expressing IT Risk in Business Terms



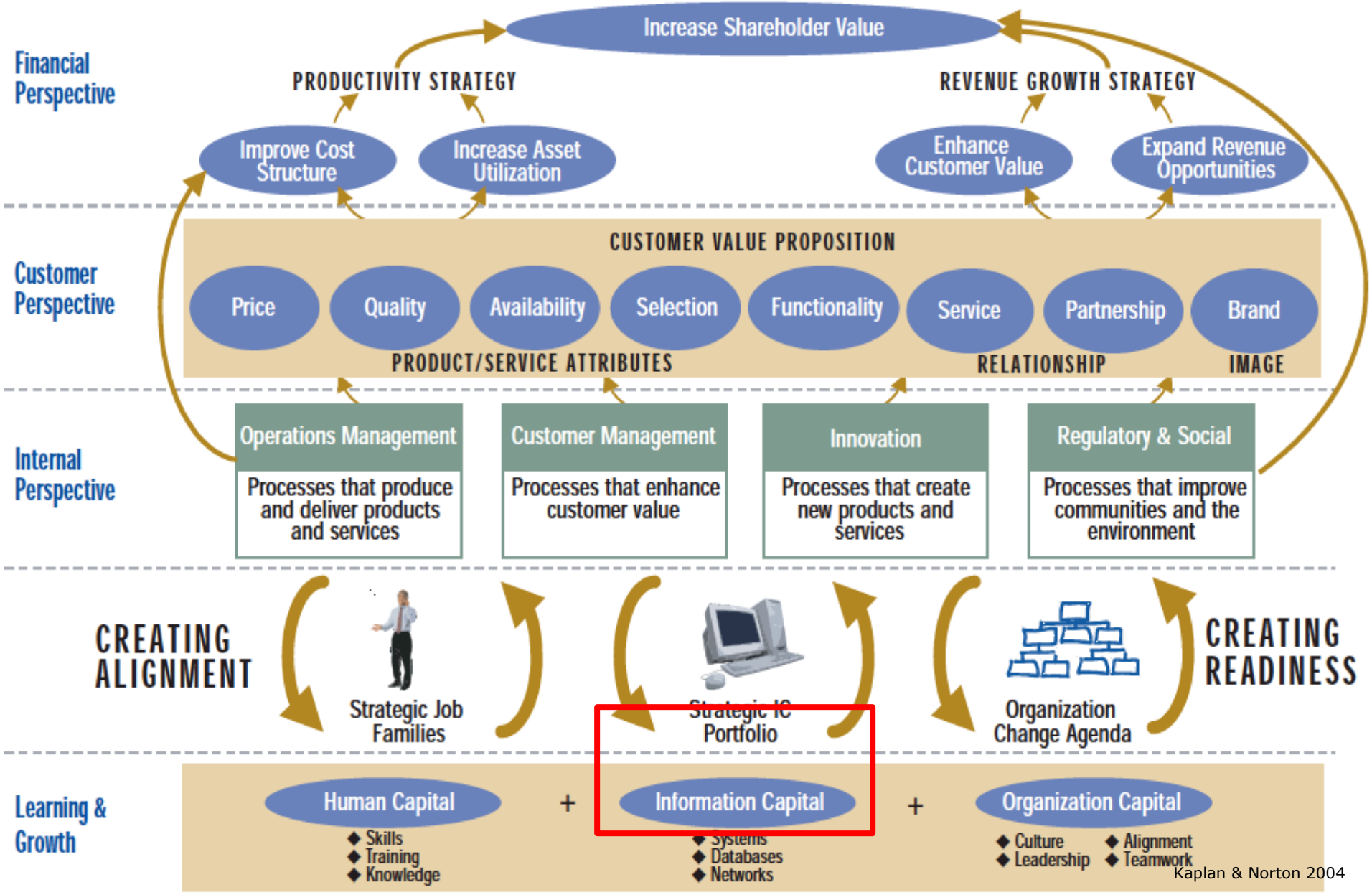

The link between IT risk scenarios and ultimate business impact needs to be established to understand the effects of adverse events. Several techniques and options exist that can help the enterprise to describe IT risk in business terms. The Risk IT framework requires that IT risks be translated/expressed 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



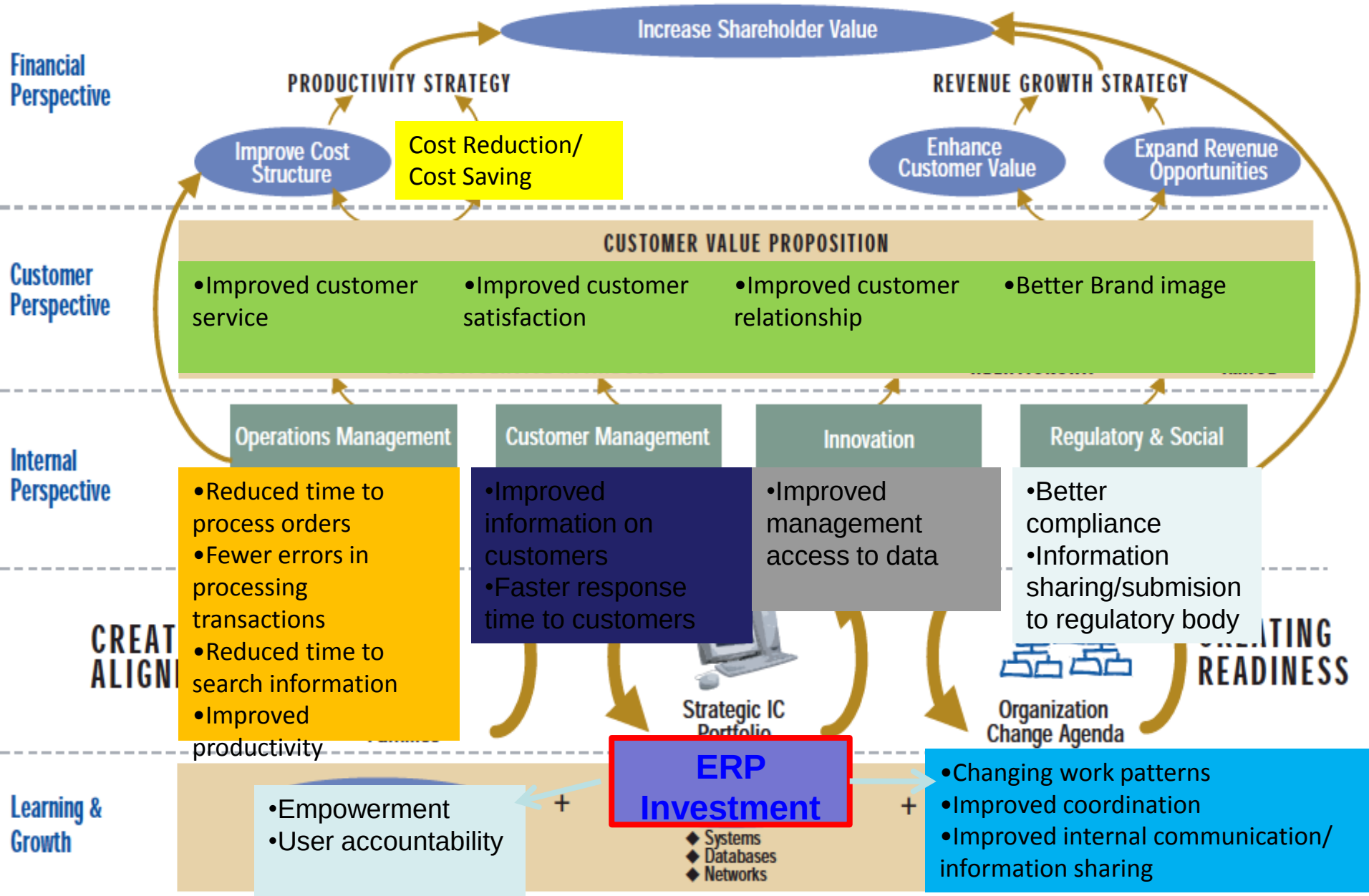

Translating Vision-Mission & Strategy to Balanced Scorecard
for Performance Measurement & Linkages to action for Quality Cycle / P-D-C-A

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




Kaplan & Norton 2004

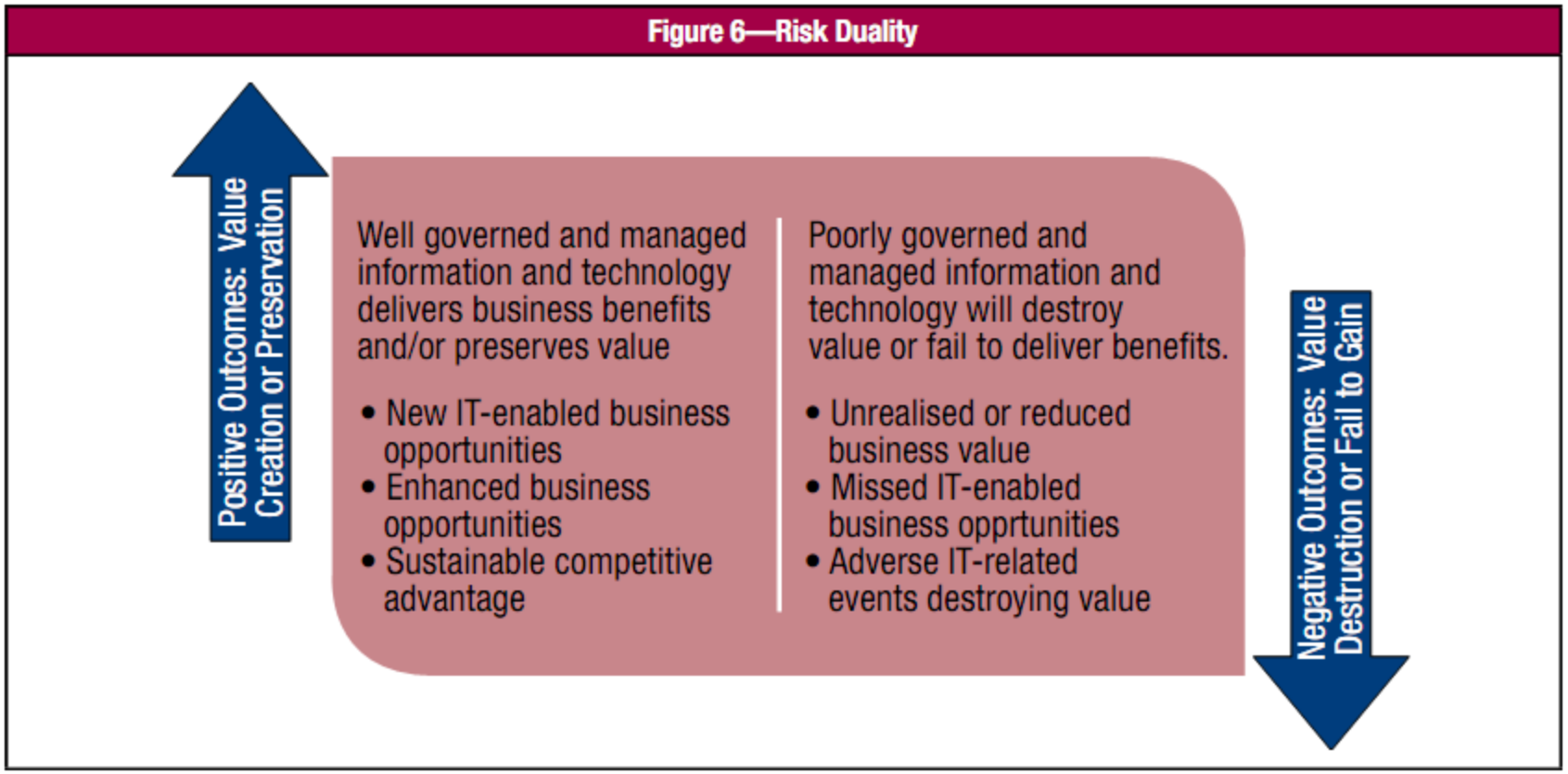
# Sample : Balanced Scorecard & Perspectives Business value of ERP



# IT Governance and IT Management for Value Creation->



**Figure 6—Risk Duality**




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*

# 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.

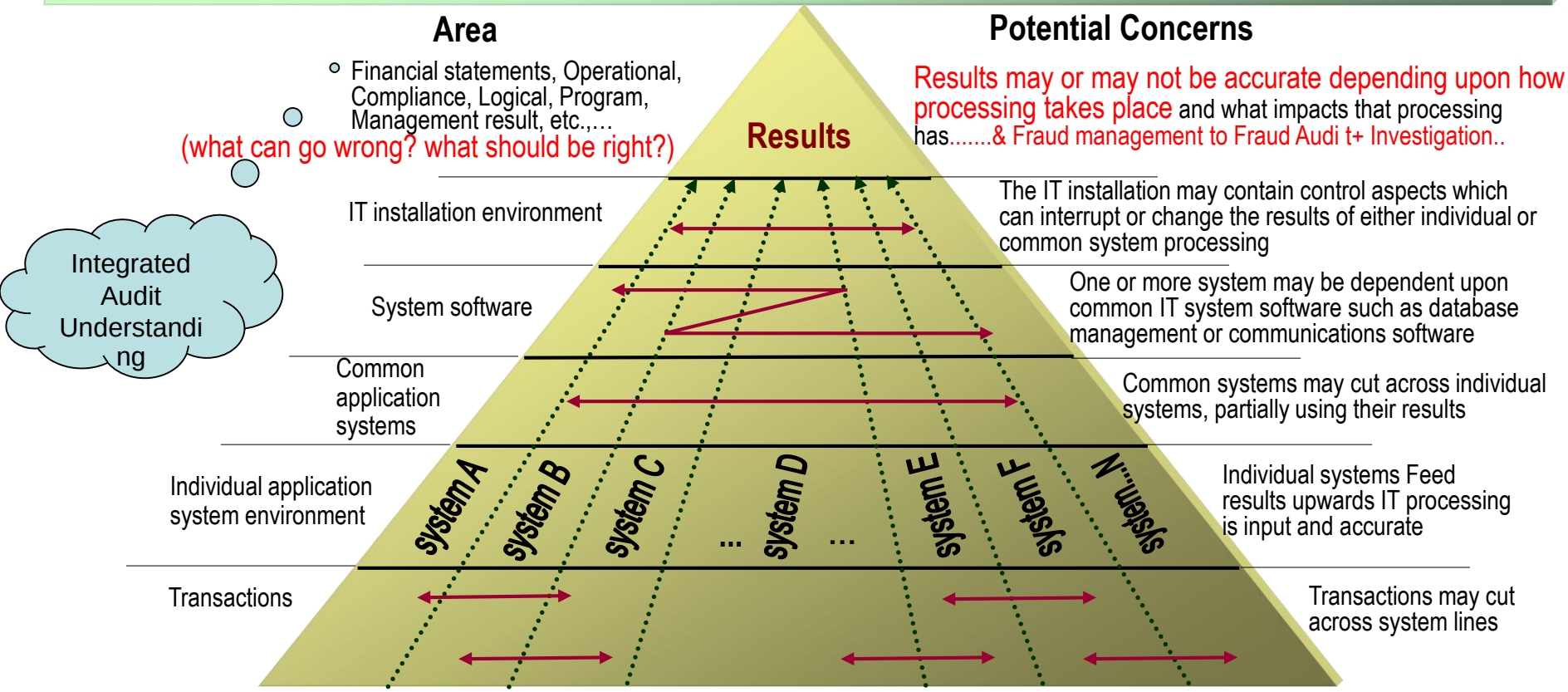
When risk is referenced in *COBIT 5 for Risk*, it is the **current** risk. The concept of inherent risk is rarely used in *COBIT 5 for Risk*. **Figure 7** shows how inherent, current and residual risk interrelate. Theoretically, *COBIT 5 for Risk* focuses on current risk because, in practice, that is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

**Figure 7—Interrelationship of Inherent, Current and Residual Risk**

**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 จึงควรพิจารณาในเรื่องมาตรฐานการจัดการตรวจสอบและการบริหารความเสี่ยงในภาพรวมและการพัฒนาบุคคลากรขององค์กรเพิ่มขึ้นอีกมากในเรื่องIT Governance และในเรื่องการตรวจสอบ IT**

# 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

## Organizational Governance Architecture

**Organizational Perspectives & Business Processes**

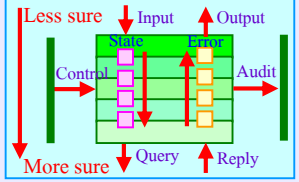
Actuate — Sense

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

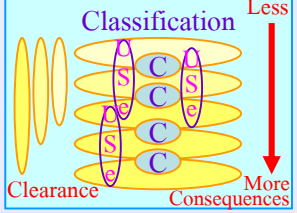
## Control Architecture

- 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

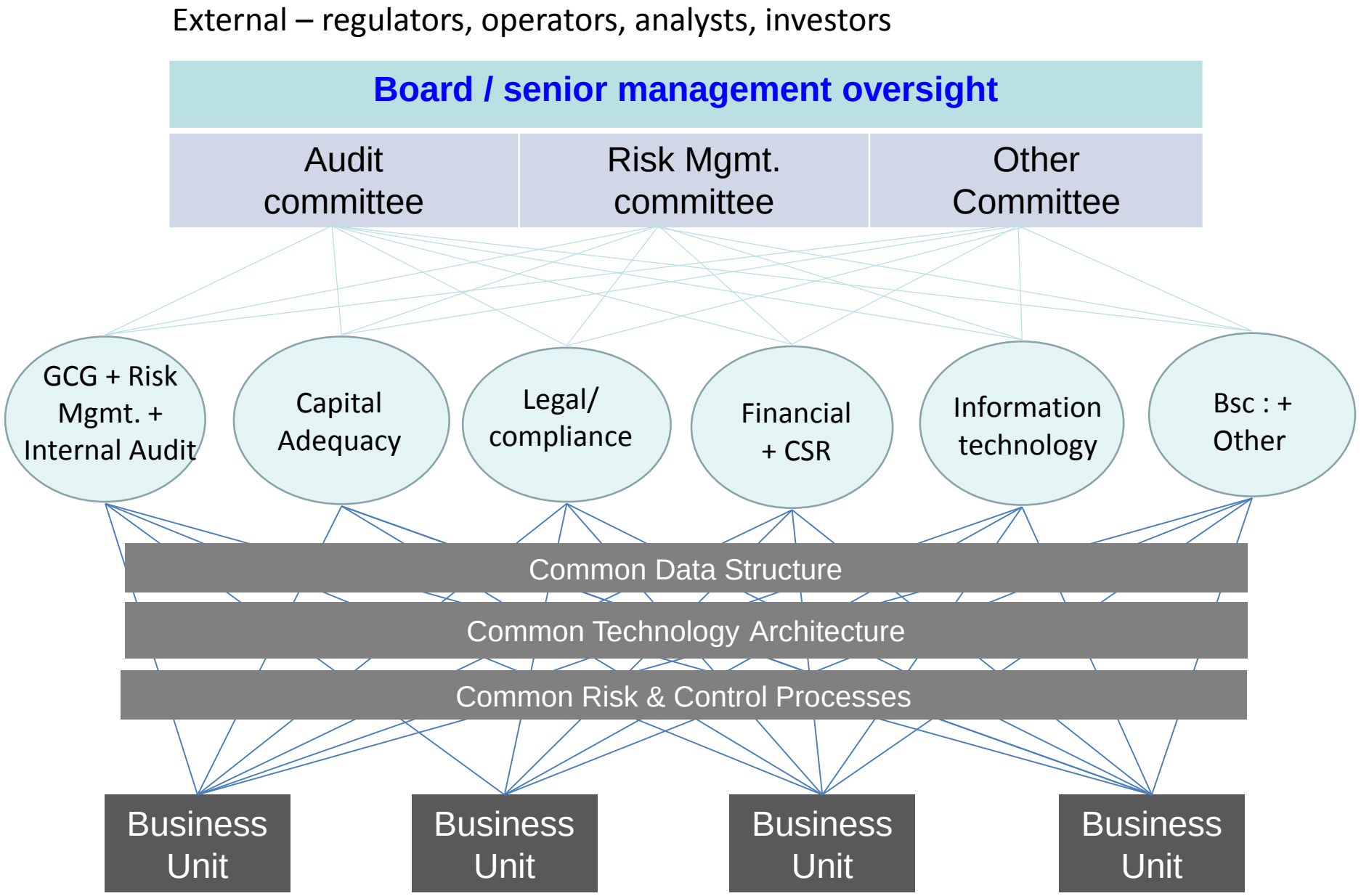
## Objectives

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

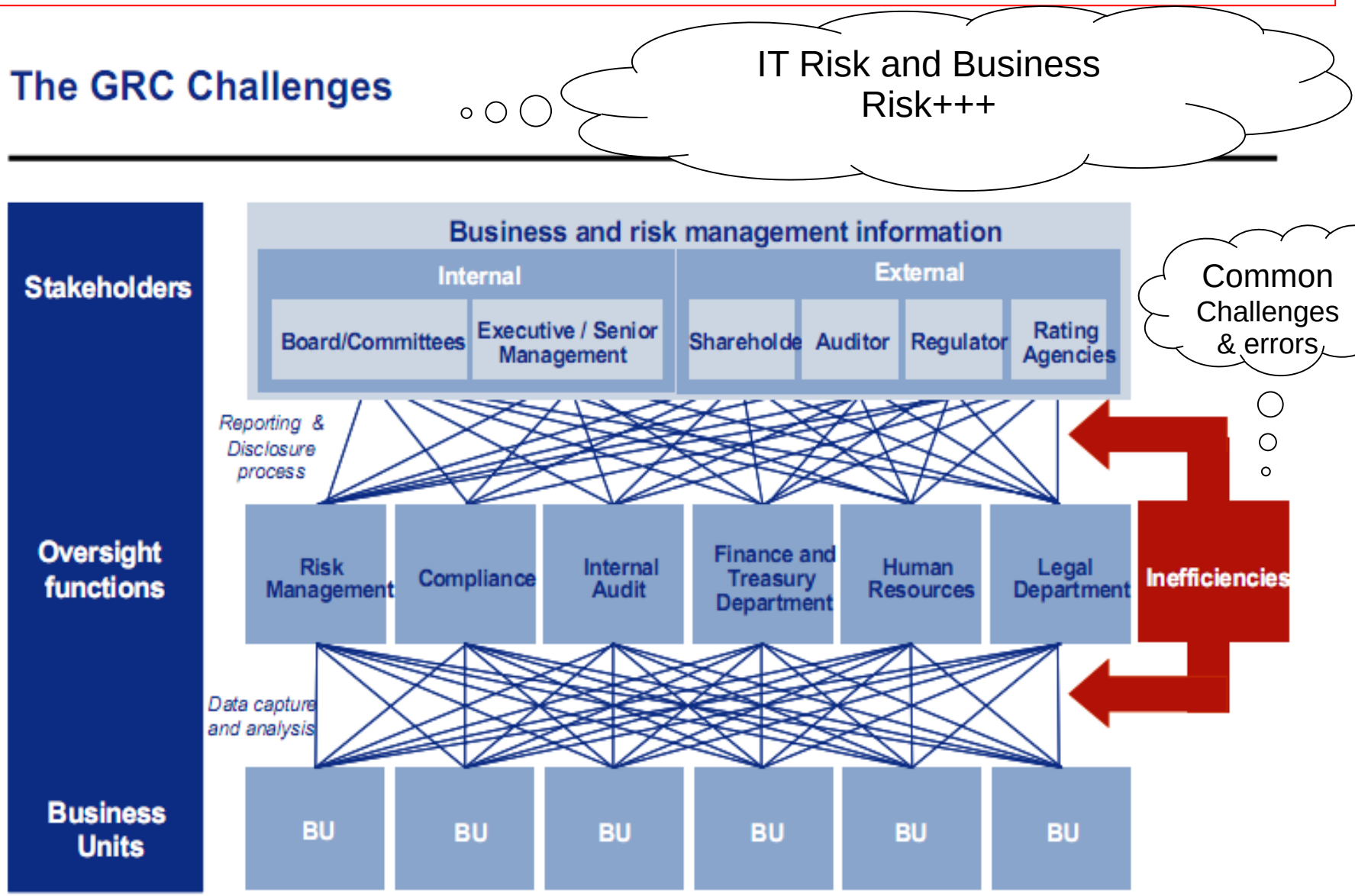
Source : IT Security Governance Guidebook / FRED COHEN

# การโยงใยและความสัมพันธ์ของ
## การกำกับดูแลกิจการที่ดีกับการบริหารความเสี่ยงขององค์กร

# Risk Convergence & Management Model



# A Consolidated-Integrated Single Framework on COSO Model

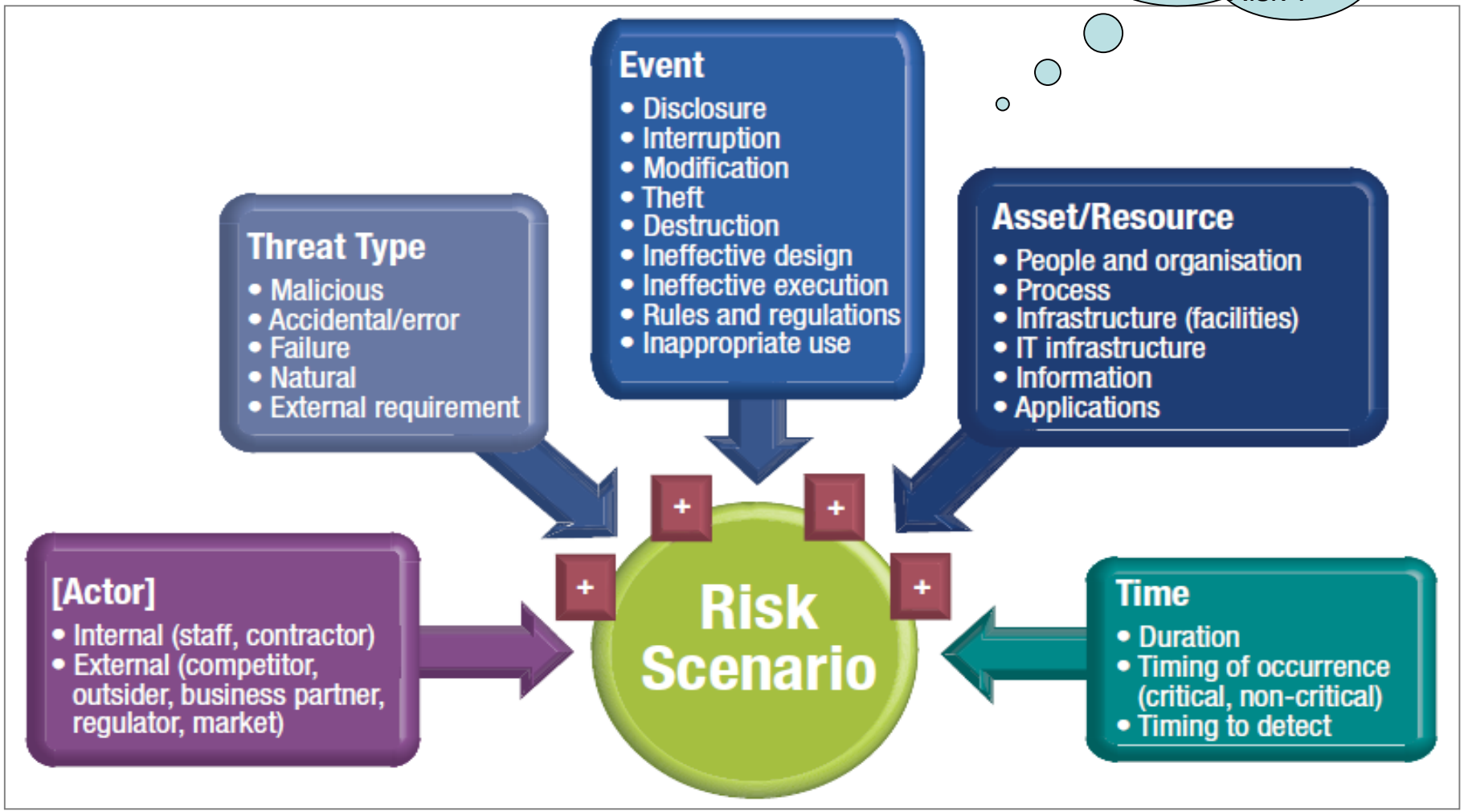



Source: KPMG

# RISK SCENARIOS

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

## IT Risk Scenario Components




Source : ISACA

# Information Security – International Standard (ISO 27001)

GRC and Asset Management

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




Consideration of common errors in identifying objectives –

Identifying a means as an end.

Failing to consider each type & all types of objectives.

Failing to consider the relationships between objectives.

# Without Effective Governance and the Results


Source : Fujitsu

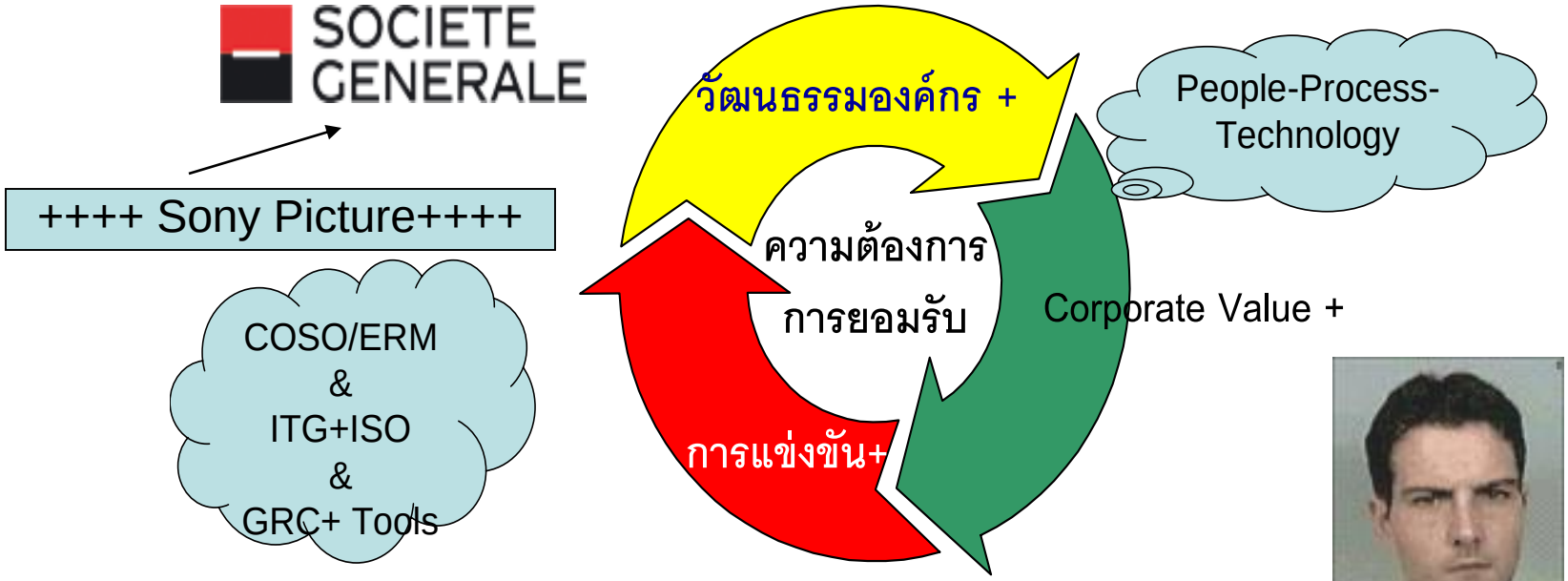
# GRC : Value Creation & Lesson Learned

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

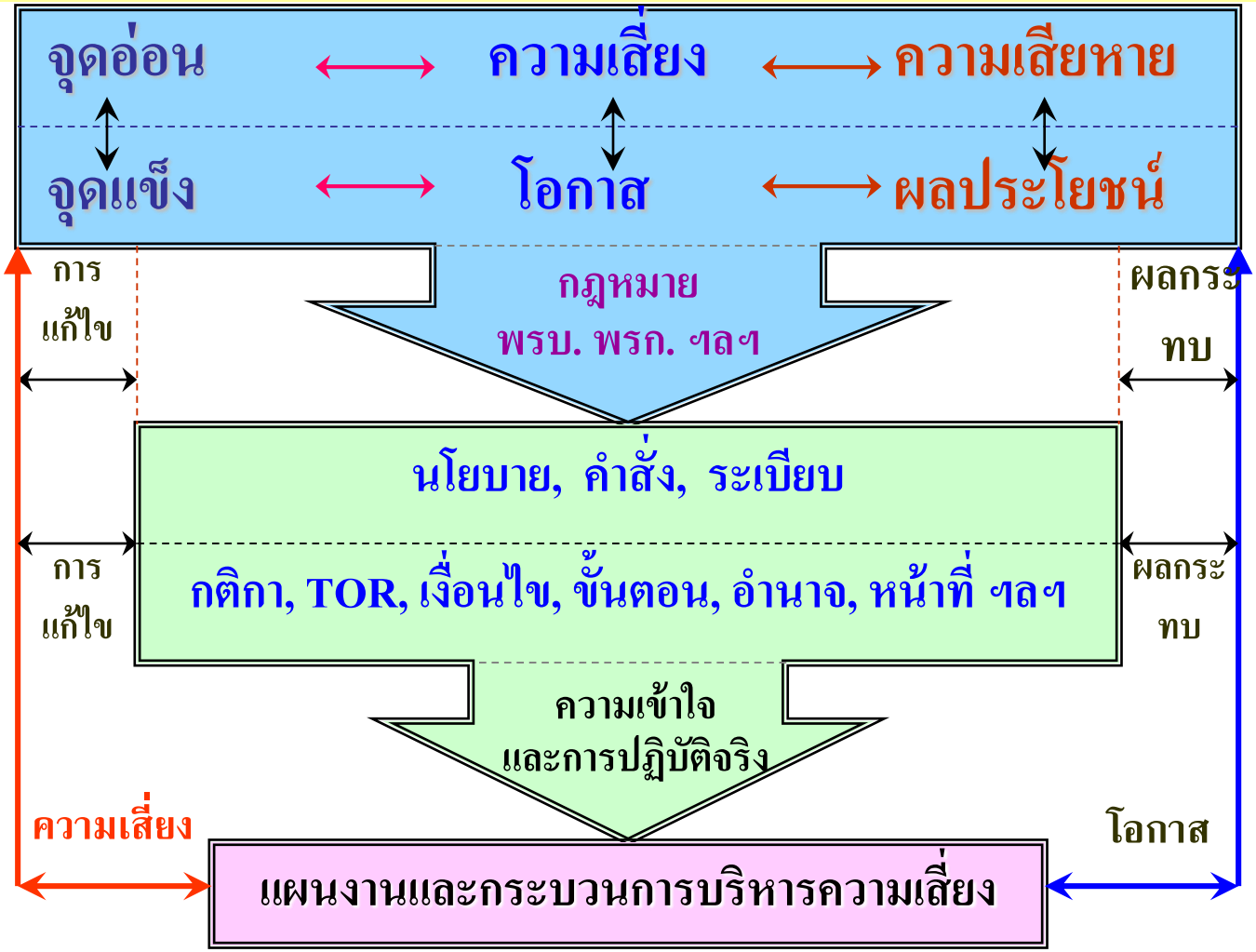
ร่วมกันทบทวน กำหนด นโยบาย กลยุทธ กระบวนการทำงาน++ จากบทเรียนนี้



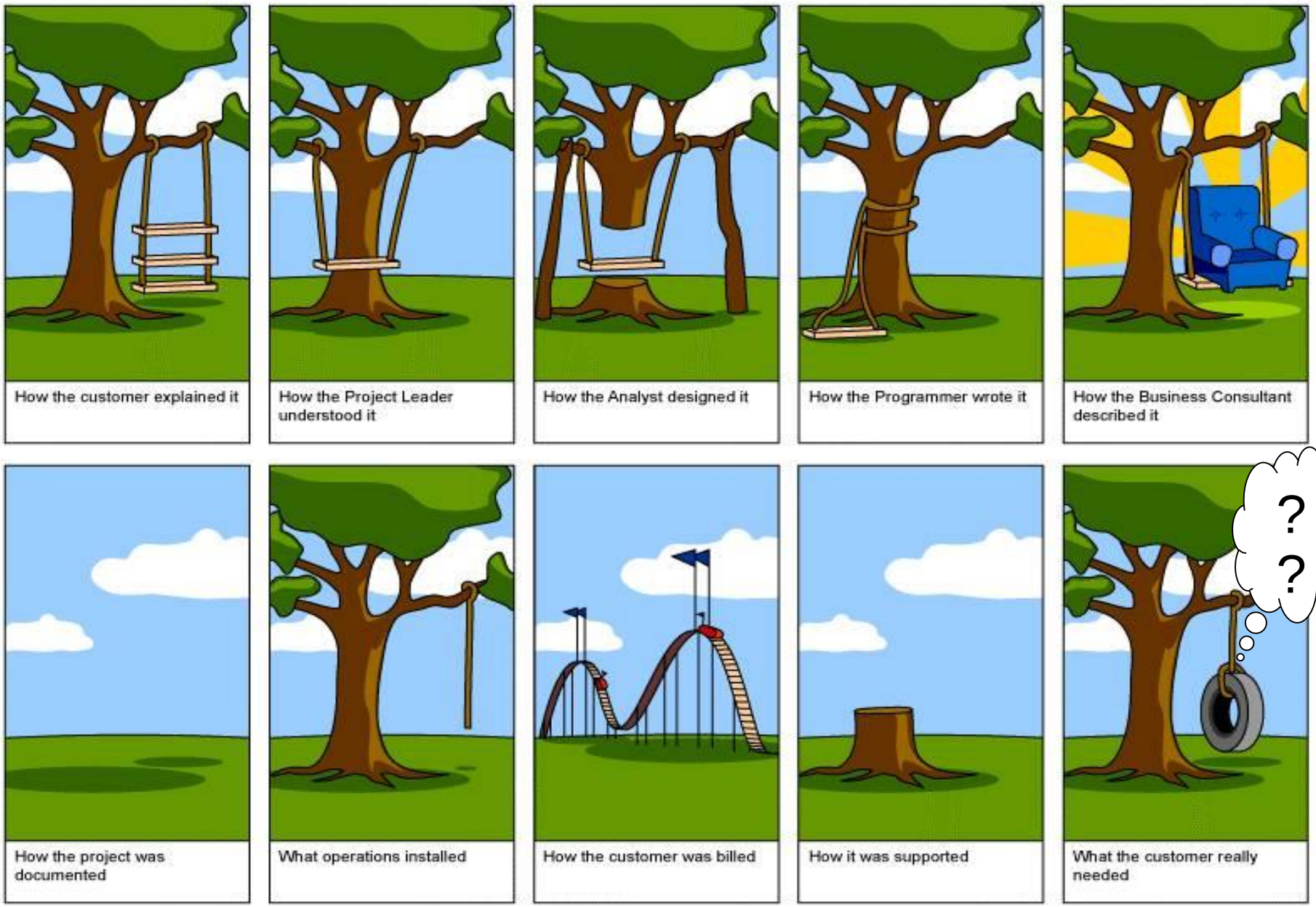
Source: www.itgthailand.com

# X-Ray ความรู้เท่าทันในการบริหารความเสี่ยงและการบริหารแบบบูรณาการ

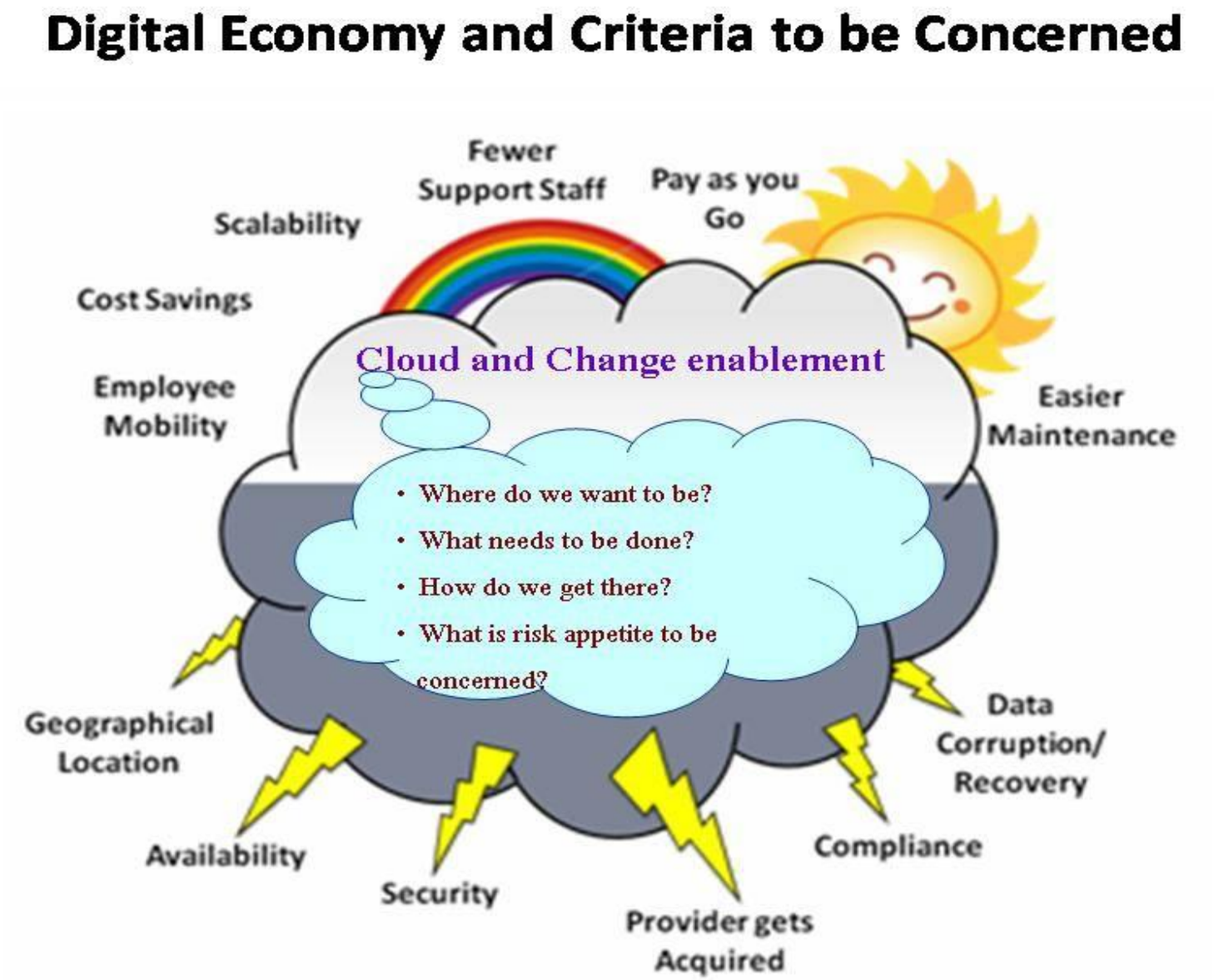
# กับ ICT Risk Mgmt.



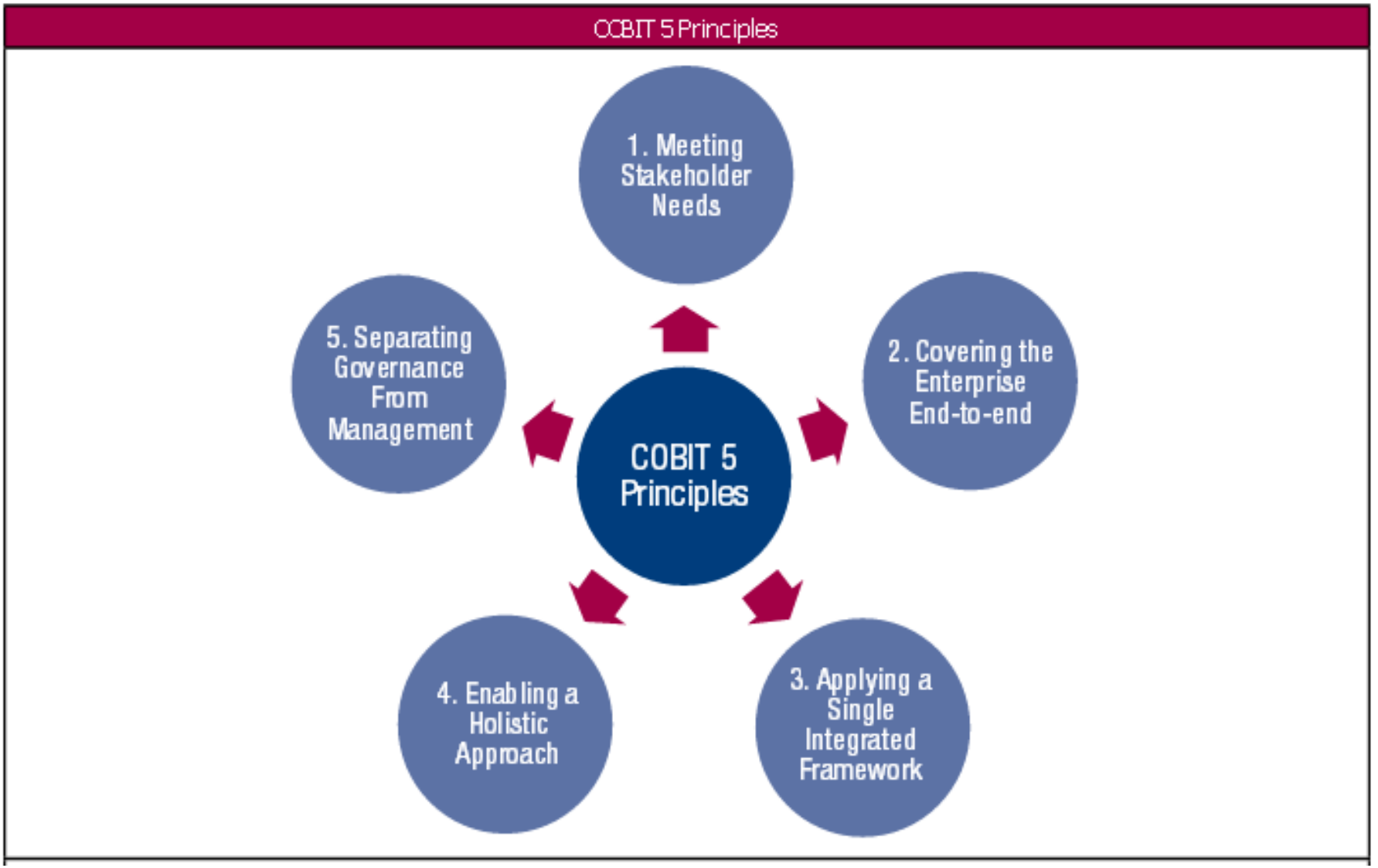

ที่มา: www.itgthailand.com


How the customer explained it
How the Project Leader understood it
How the Analyst designed it
How the Programmer wrote it
How the Business Consultant described it
How the project was documented
What operations installed
How the customer was billed
How it was supported
What the customer really needed
? ?

# การบริหารความเสี่ยงบางมุมมองกับ Digital Economy

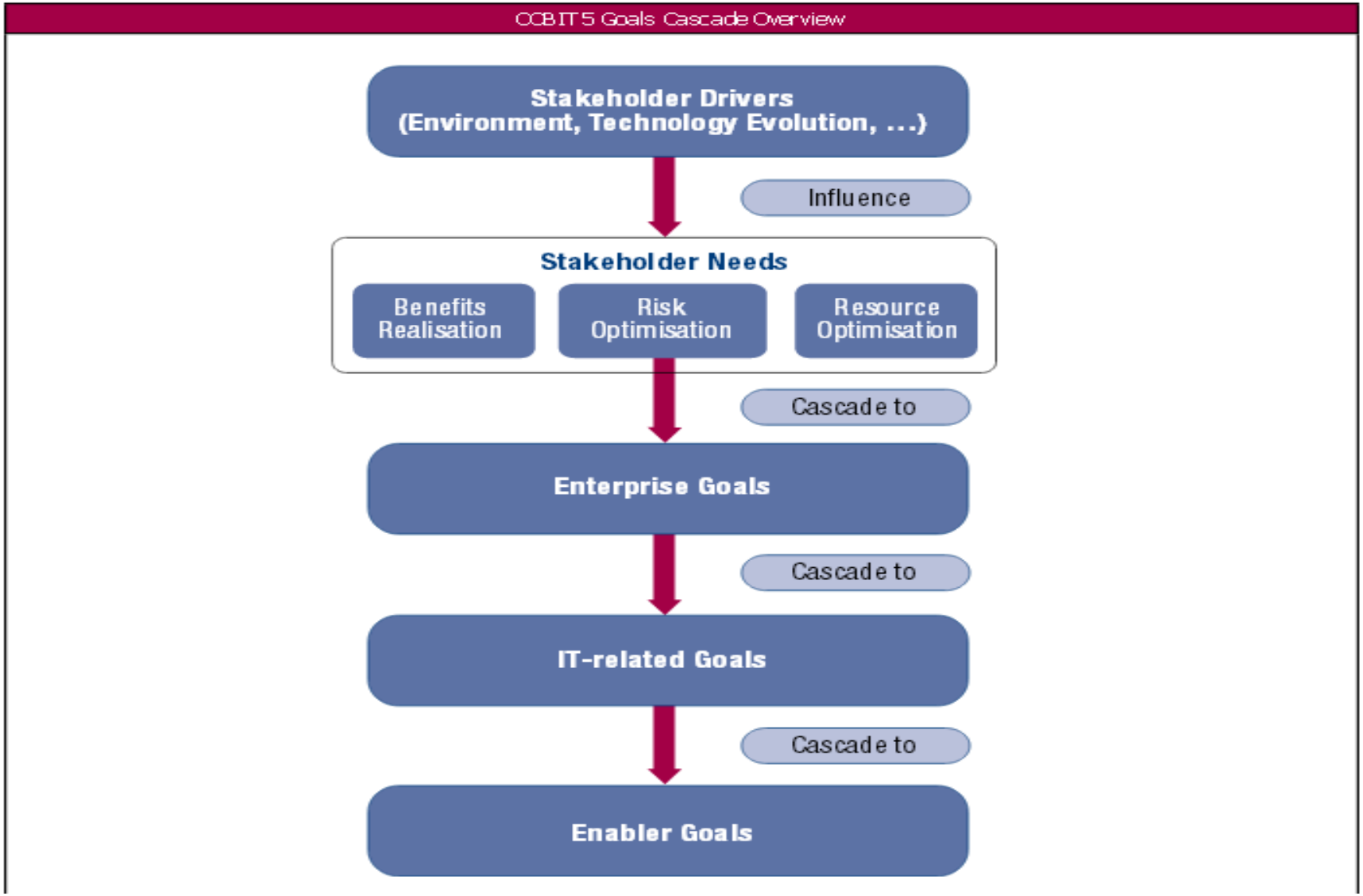


# COBIT 5 for ICT Risk Management




Source : ISACA

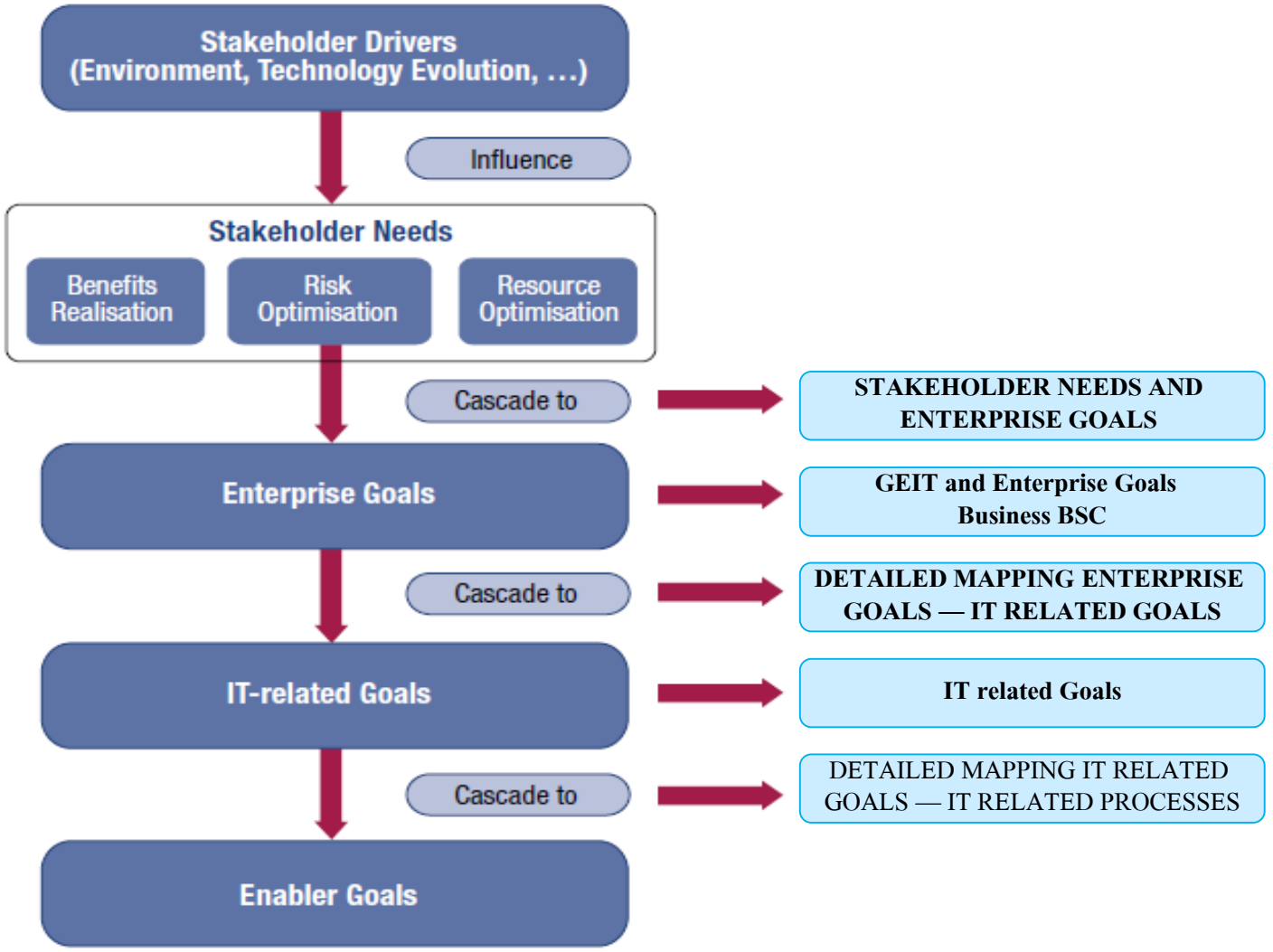
# COBIT 5 for Stakeholder needs




Source : ISACA

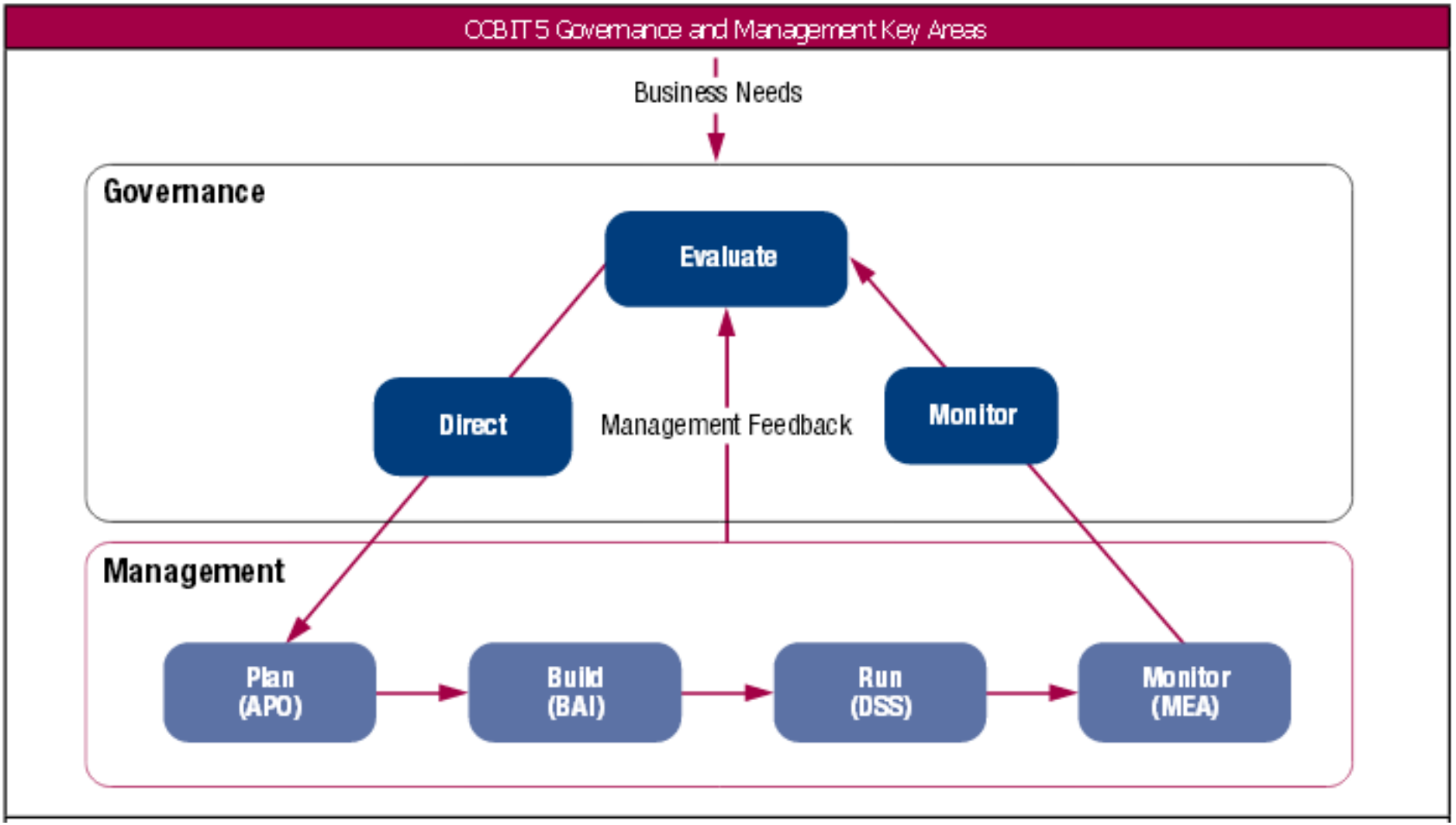
# A Business Framework Perspective for the Governance and Management of Enterprise IT

## Goals Cascade Overview / GEIT – Governance Enterprise of IT




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

# Integrated Single Framework Governance & Management




Source : 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 | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | 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 |

Resource : ISACA

# DETAILED MAPPING ENTERPRISE GOALS — IT-RELATED GOALS

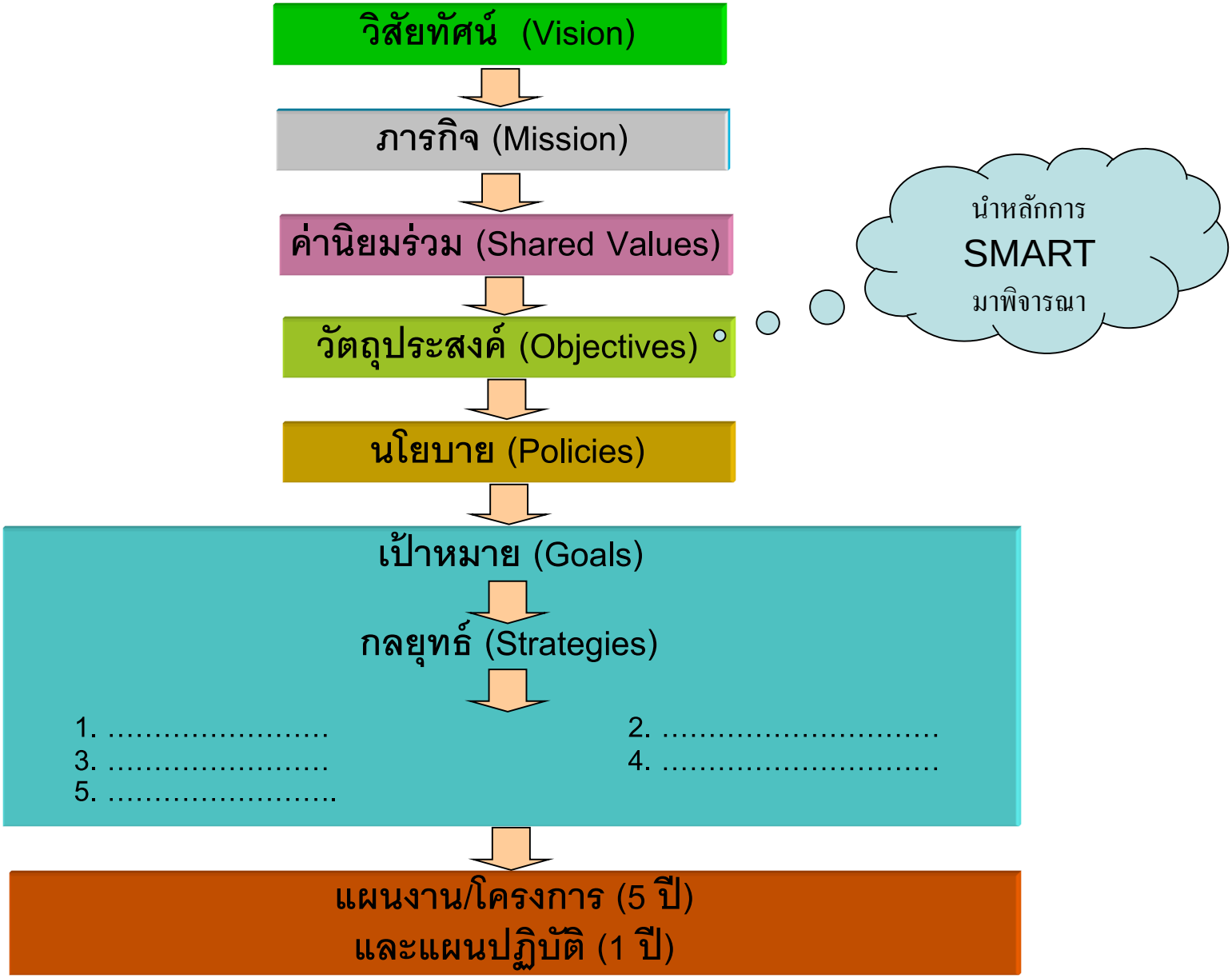
## Mapping COBIT 5 Enterprise Goals to IT-related Goals (Cont.)

**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

มุมมองโลกแห่งการเปลี่ยนแปลง กับ โครงสร้างการบริหารขององค์กร โดย พิจารณาถึง **Business Objectives and IT- Related Objectives** กับ **ICT Risk ….**




Source: www.itgthailand.com

# 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**

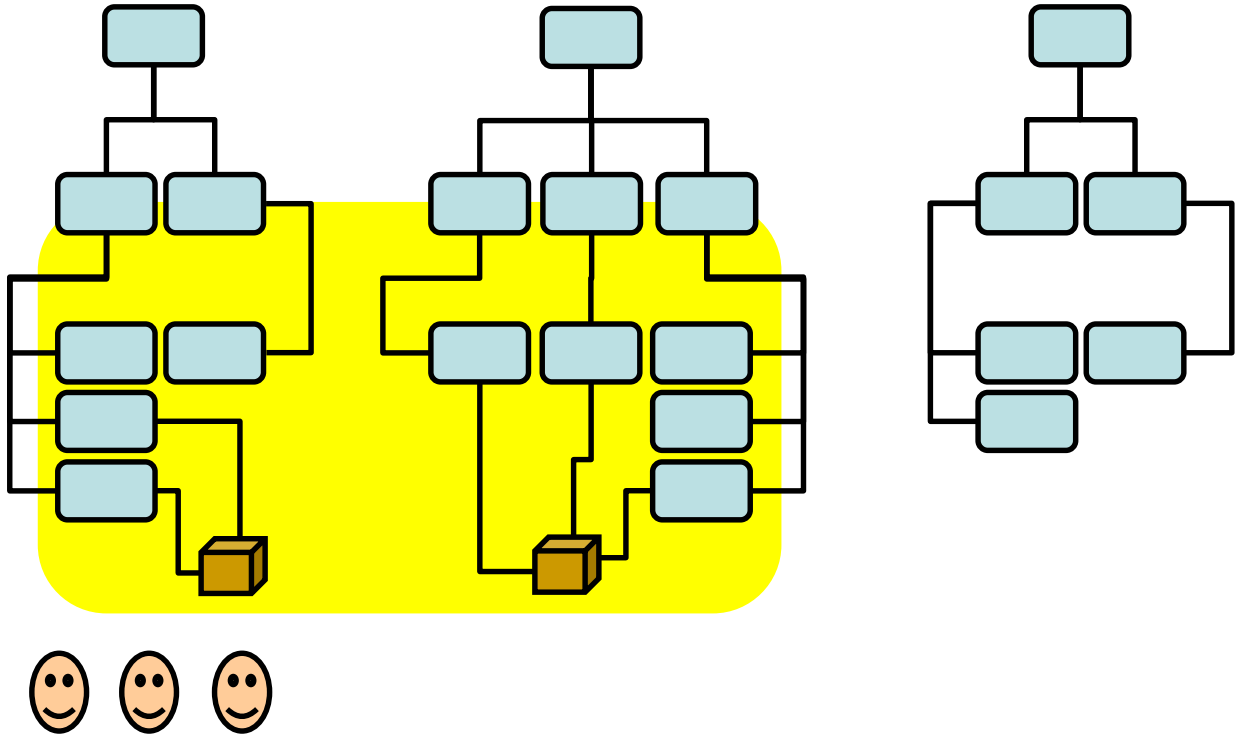
**Operational objectives**

**Process objectives**

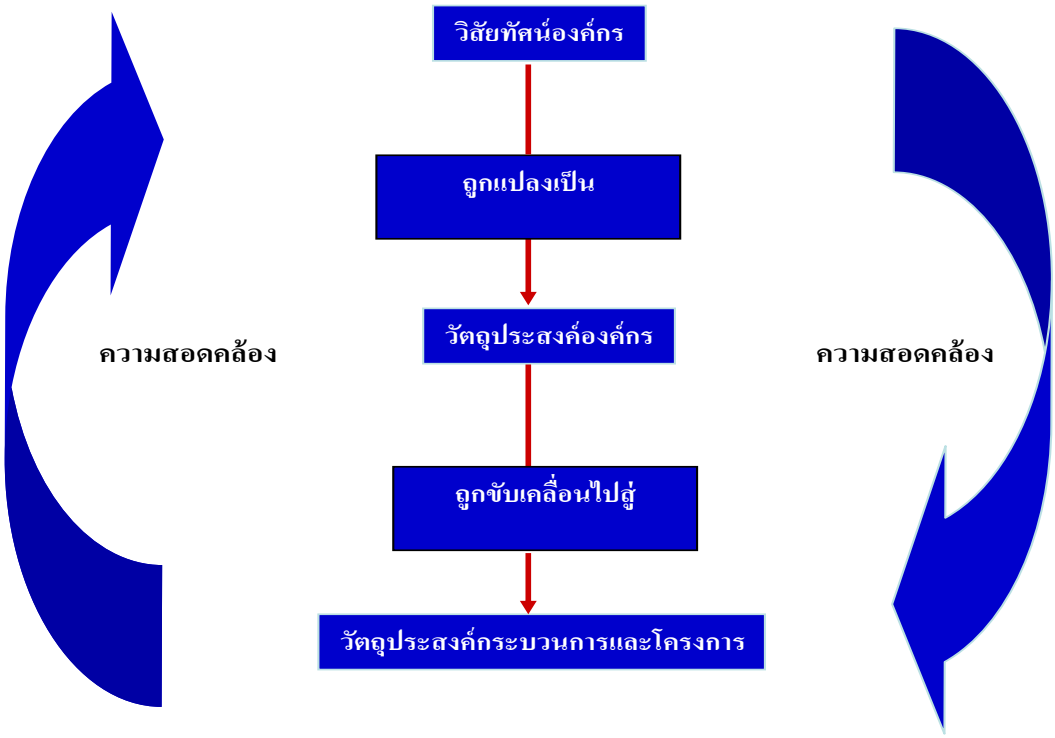
**Project objectives**

**Product objectives**

**Personal objectives**



# การกำหนดวัตถุประสงค์แบบ SMART




วัตถุประสงค์ที่ดีต้อง...

(SMART)

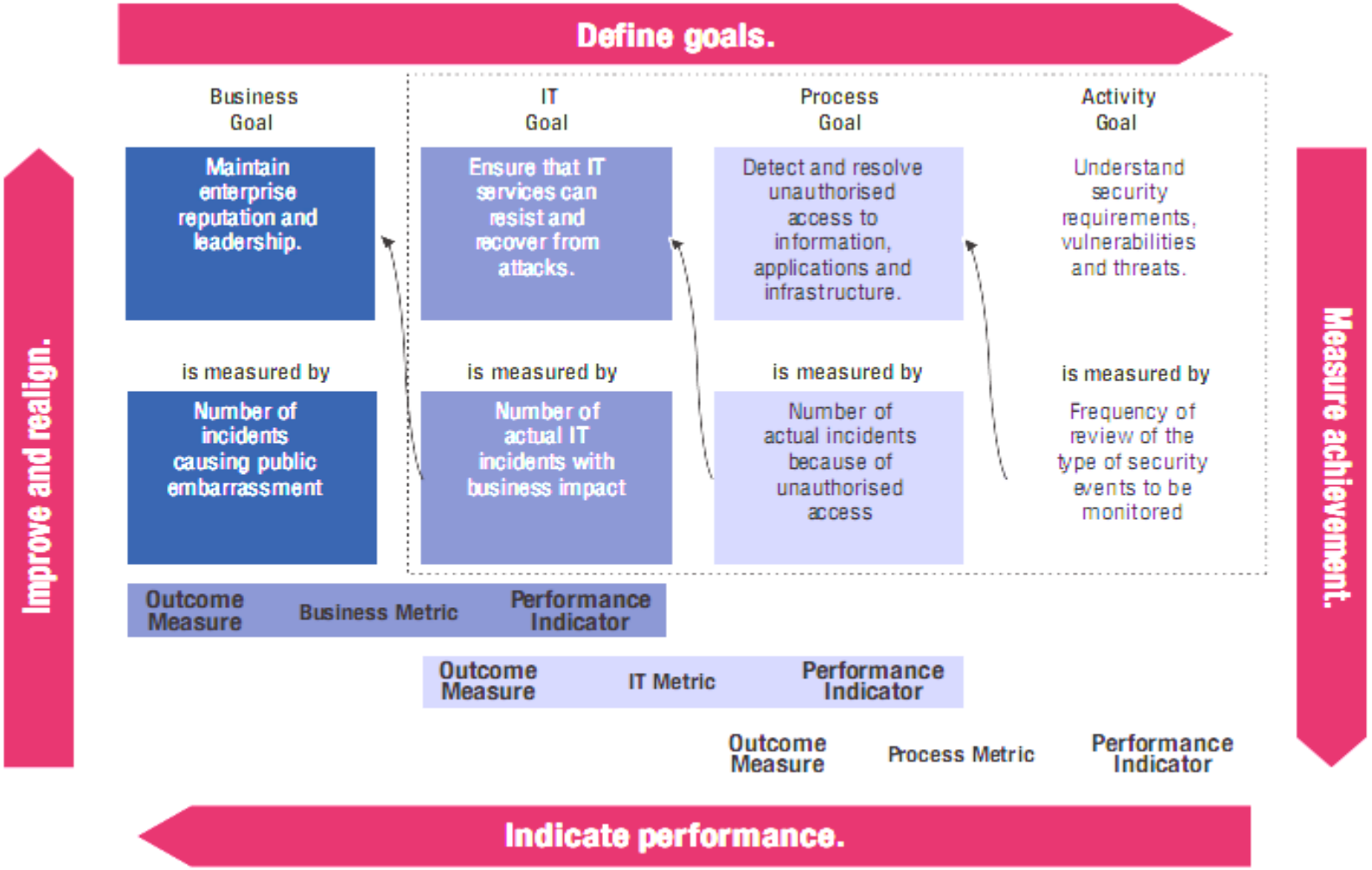
- เฉพาะเจาะจง
- สามารถวัดได้
- สามารถบรรลุผลได้
- เป็นจริงได้
- มีกำหนดเวลา

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

# CobiT 4.1 -> COBIT 5

# GRC & CobiT Framework

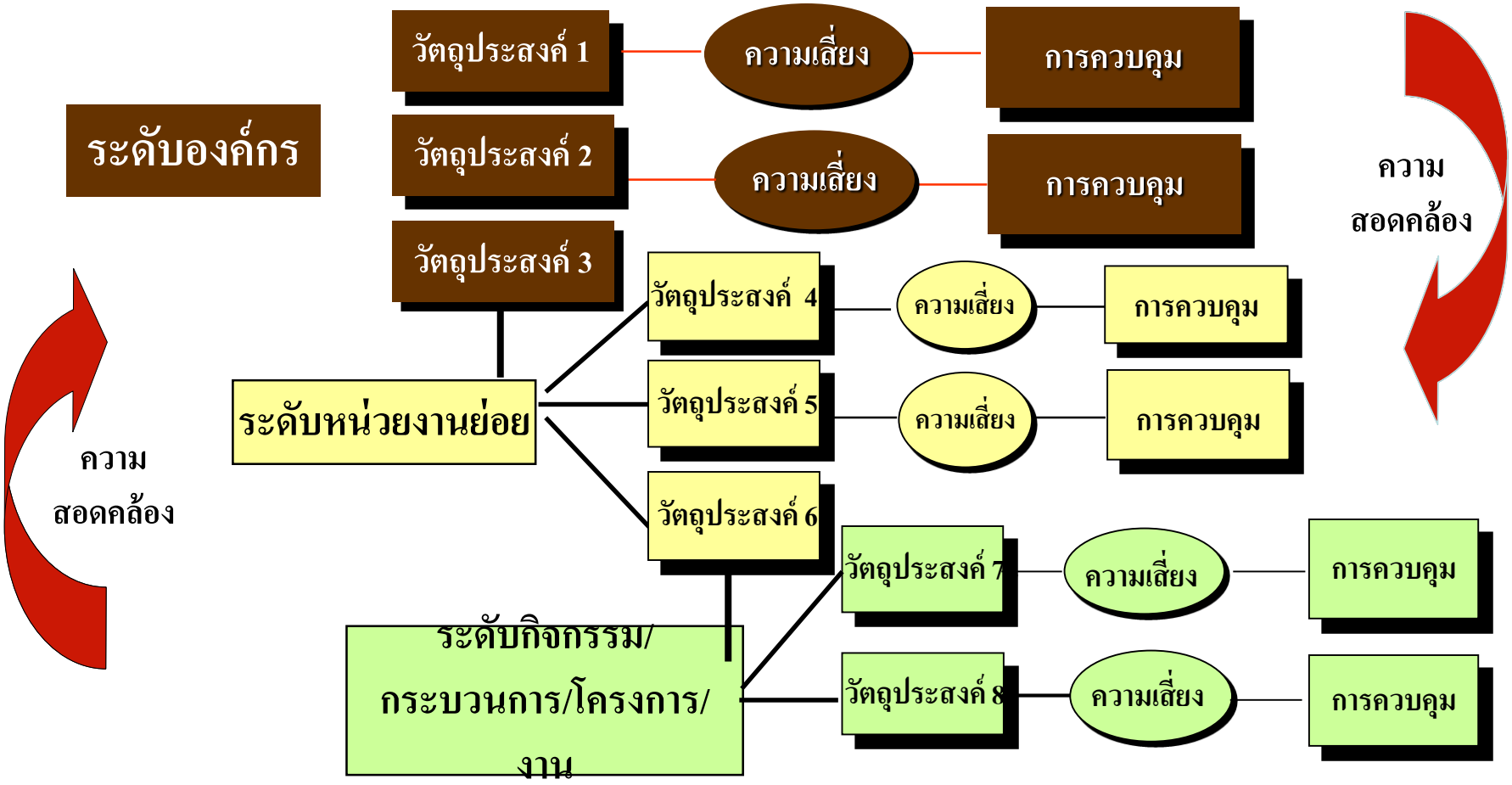
## Relationship Amongst Process, Goals and Metrics



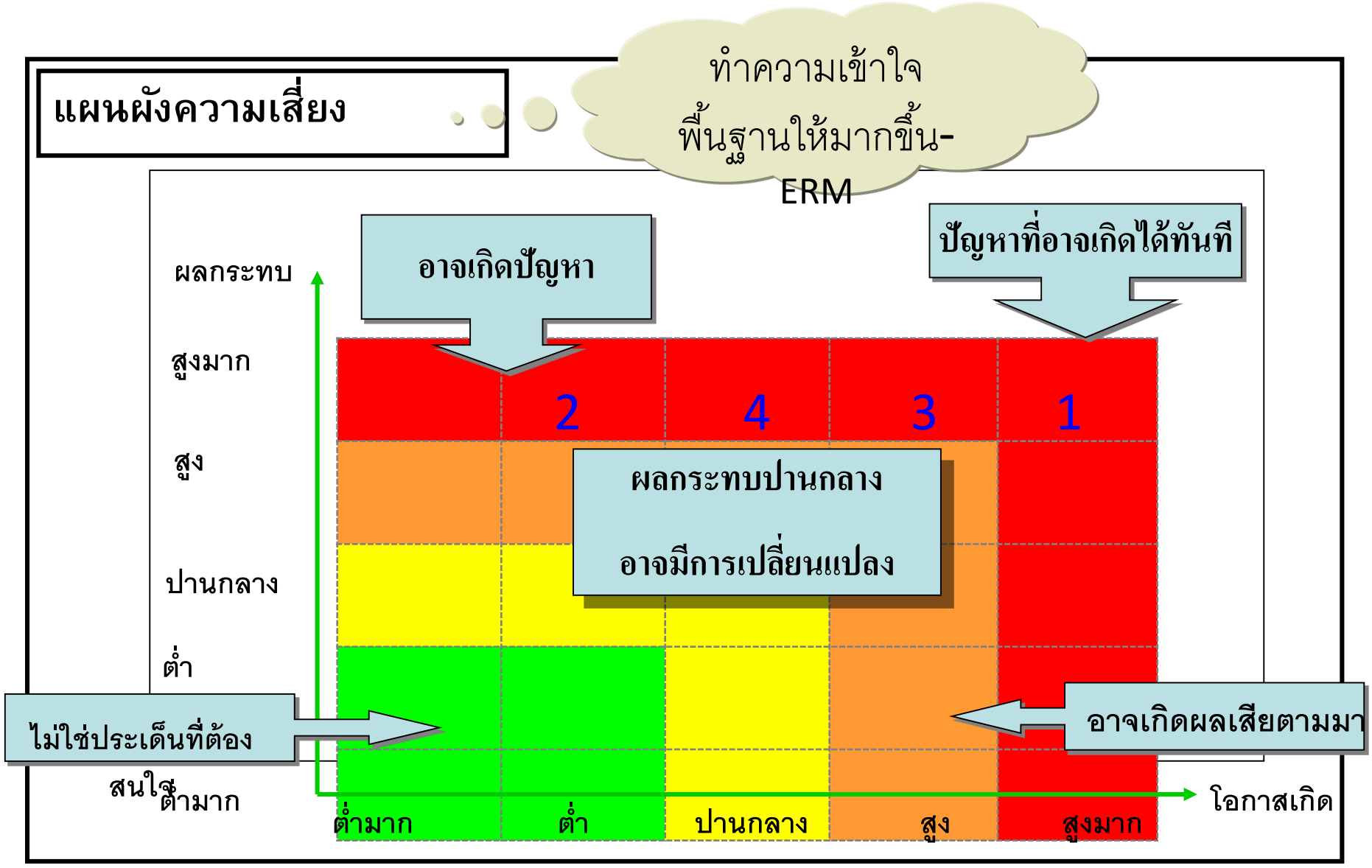

Resource : IT Governance Institute

# องค์ประกอบของ ERM- Enterprise Risk Management

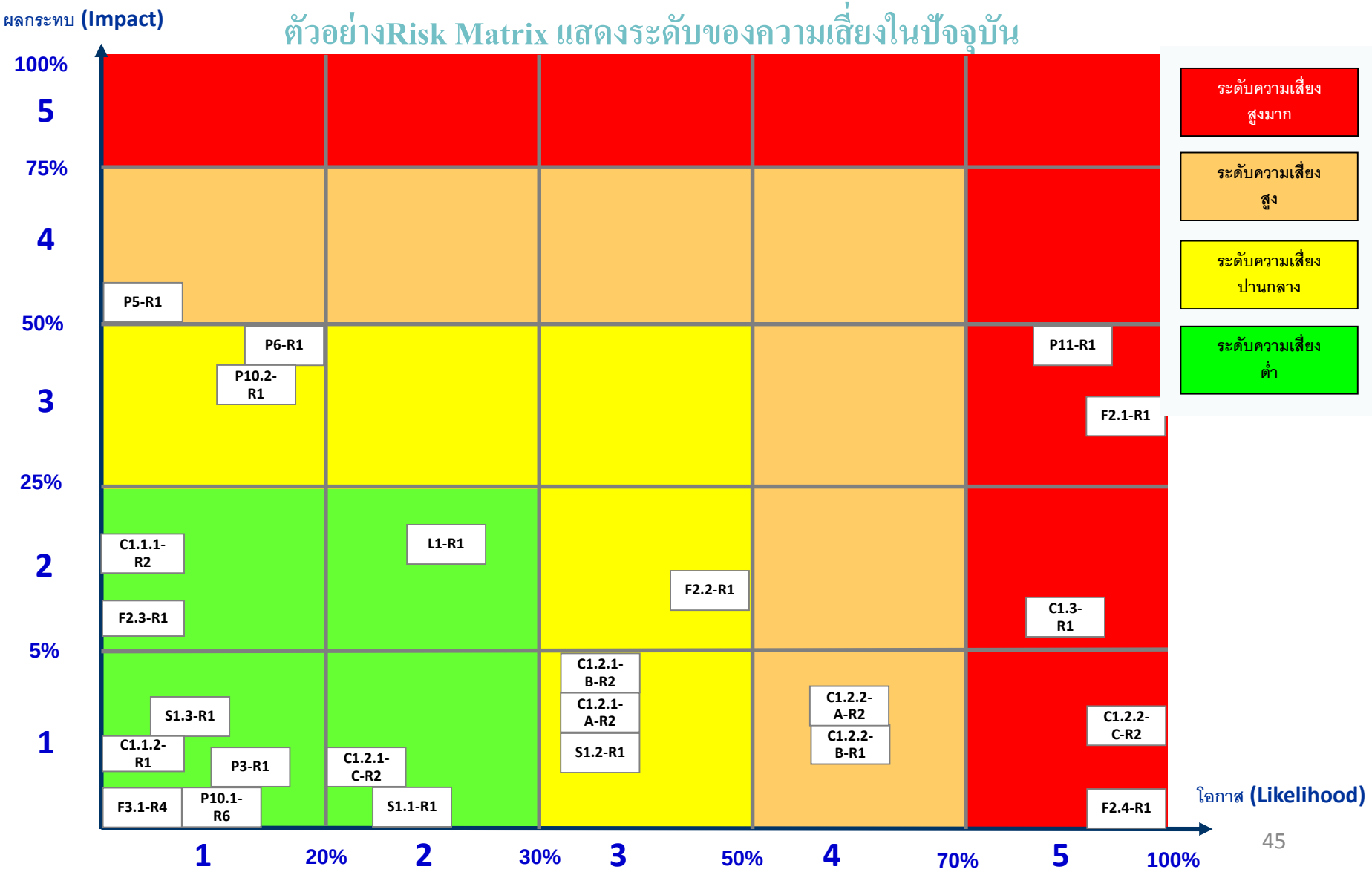
## การกำหนดวัตถุประสงค์ (Objective Setting)



# การติดตามผลและการรายงานการบริหารความเสี่ยง

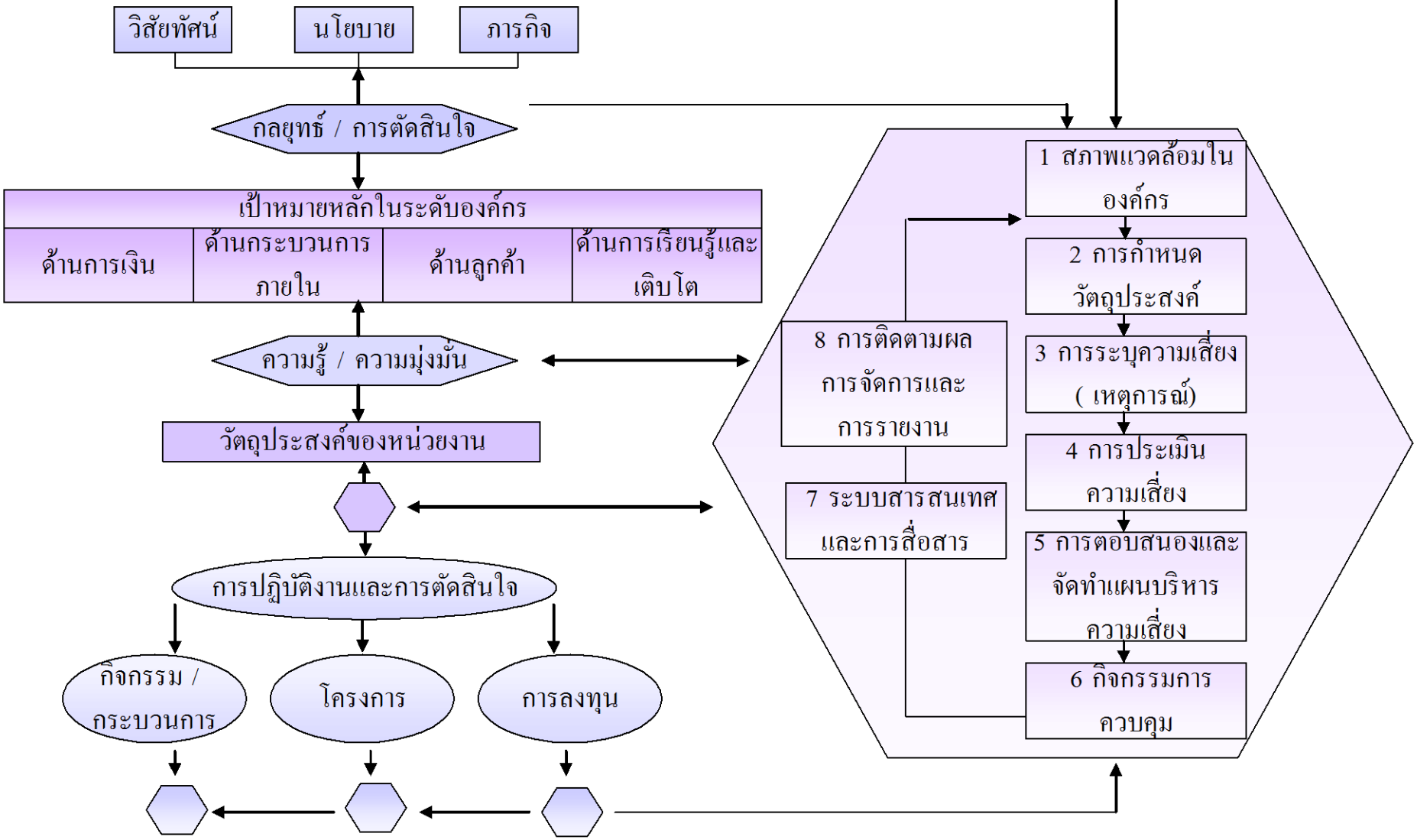


# Integrated GRC in COBIT 5 and Understanding ->Workshop



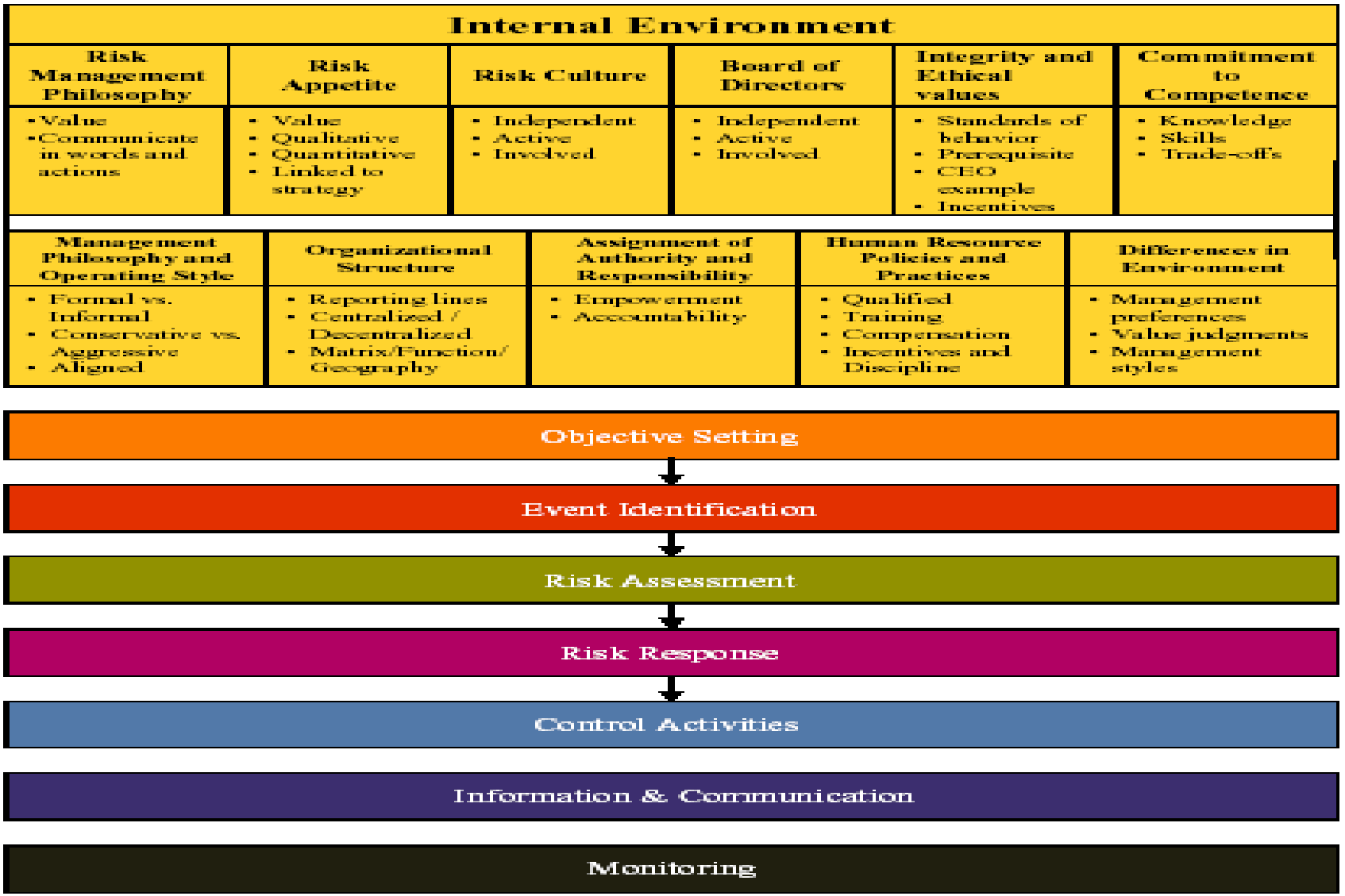
# แนวทางการบริหารความเสี่ยงแบบบูรณาการขององค์กร

## การนำการบริหารความเสี่ยงไปปฏิบัติ



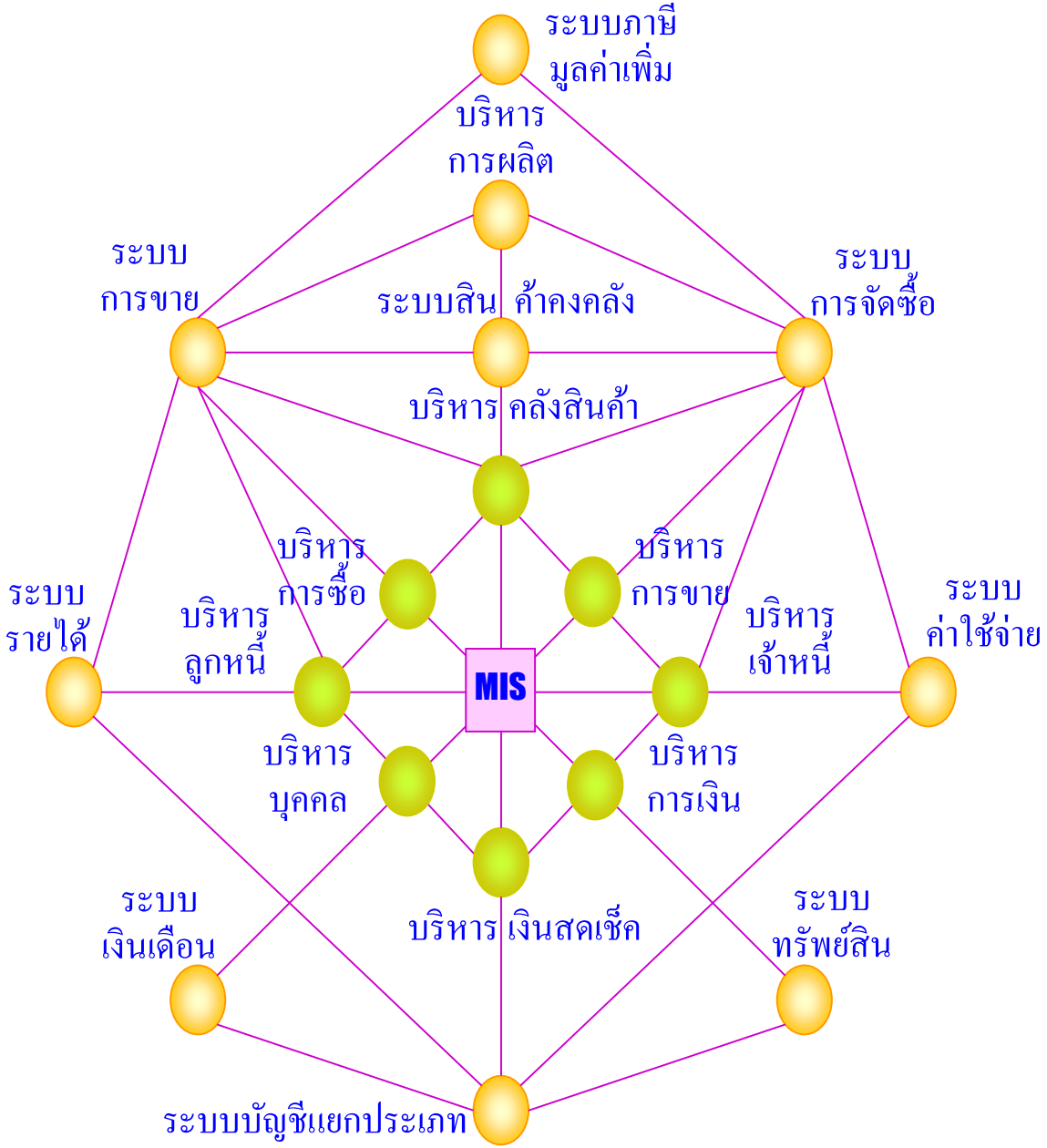
# New COSO-ERM Framework

**Exhibit 3.1**



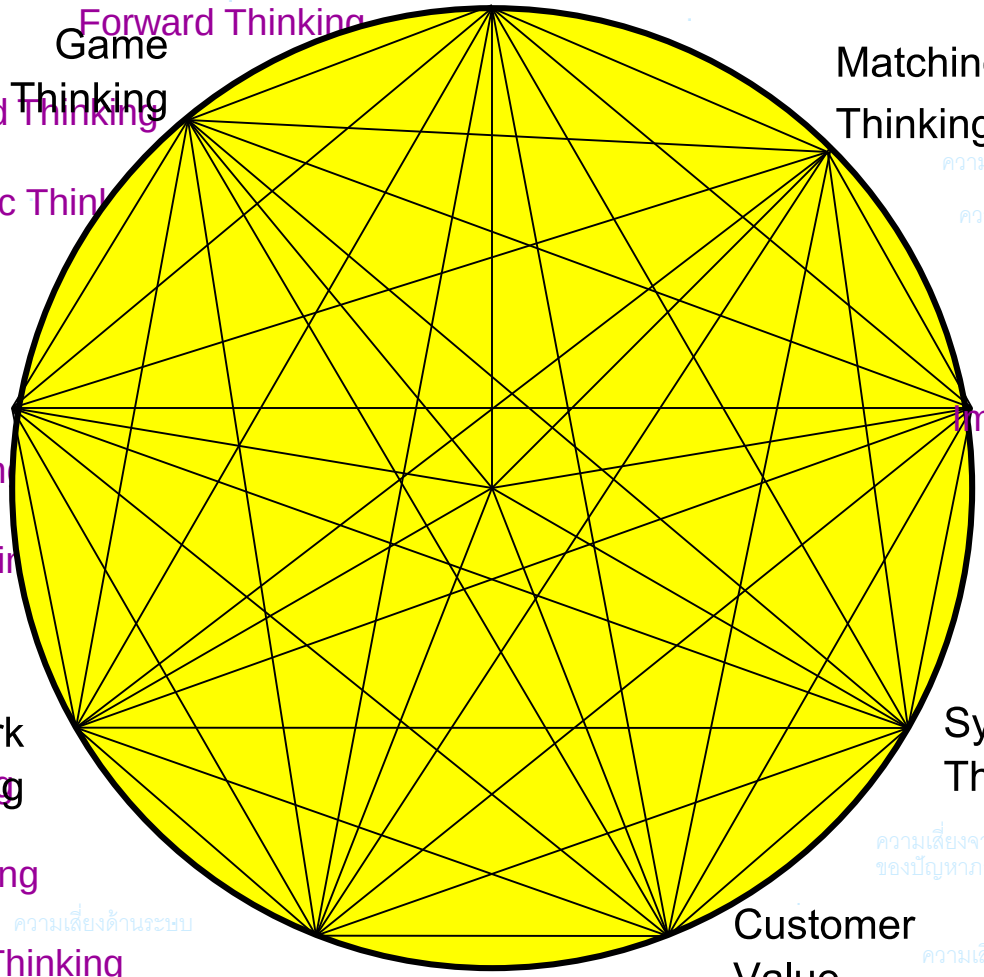

ที่มา: COSO-ERM

# การบริหารจัดการองค์กรแบบบูรณาการกับการตรวจสอบ IT – Non IT



# การบริหารความเสี่ยง
# การเข้าใจความเสี่ยง กับ การบริหารขององค์กร

# STRATEGIC THINKING AND RISK MANAGEMENT

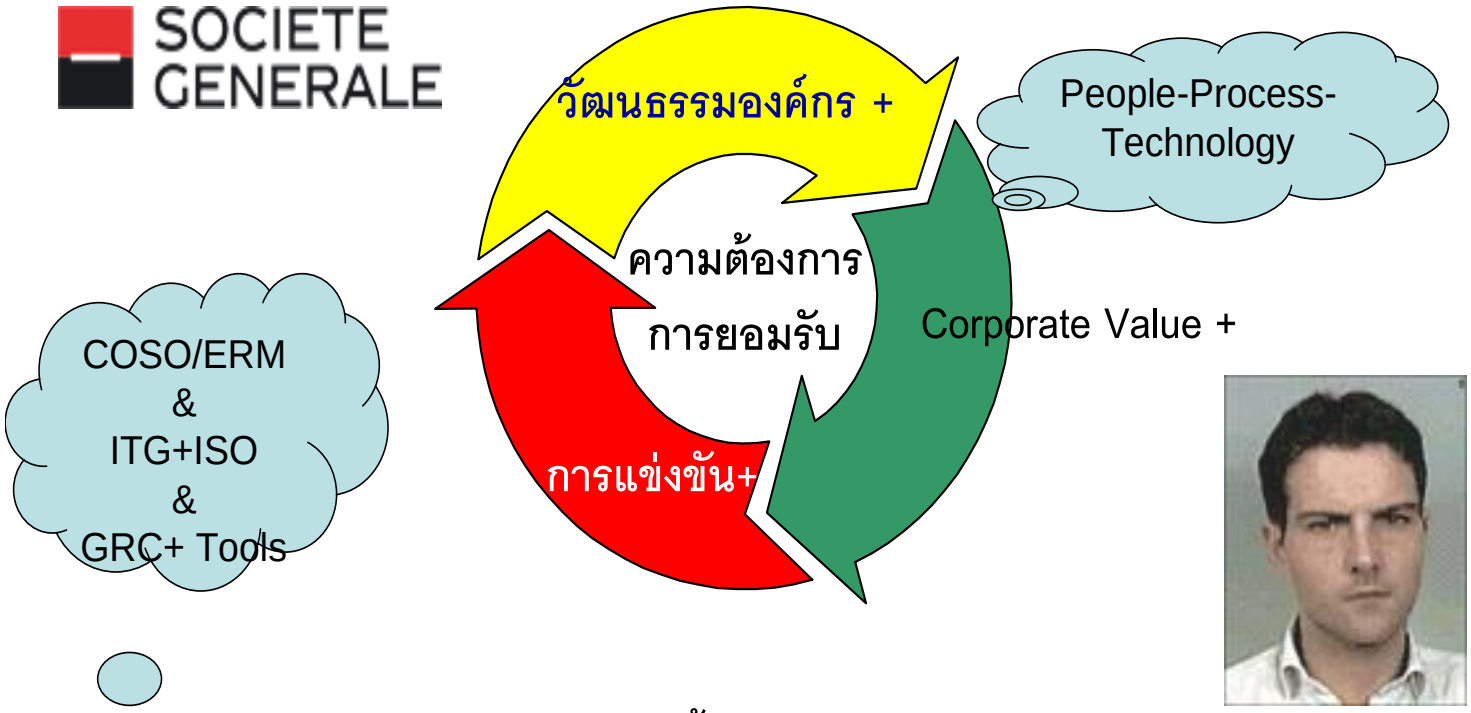


Visionany Thinking
Context Thinking
Forward Thinking
Game Thinking
Weighted Thinking
Dynamic Think
Matching Thinking
Forward Thinking
Weighted Thinking
Context Thinking
Impact Thinking
Bottom Line Thinking
Quantity Thinking
Innovative Thinkin
Grey Thinkin
Planner Thinking
Holistic Thinking
Dynamic Thinking
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

# GRC : Value Creation & Lesson Learned

บทเรียน จากการ ทุจริต 340,000.00 ล้านบาท ทางด้าน IT Risk

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

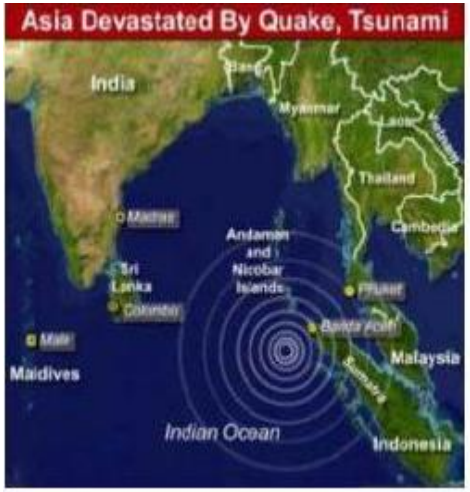


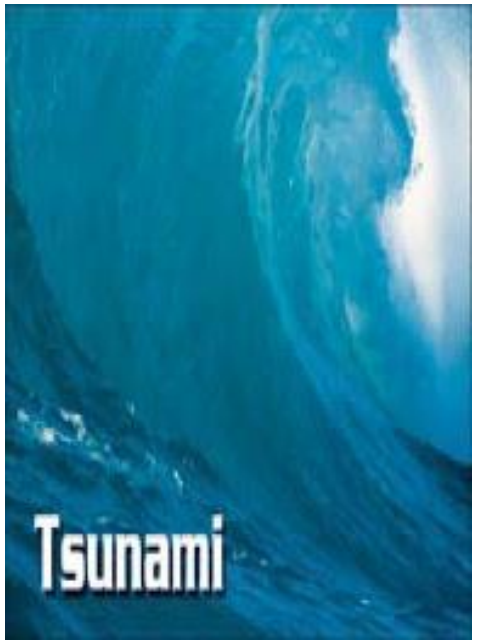



❖ความรู้ ความเข้าใจในกระบวนการ / ขั้นตอน ระบบงาน การตรวจสอบและการควบคุมภายใน + ของนาย Kerviel ผู้บริหาร และ คณะกรรมการต่างๆ

ร่วมกันทบทวน กำหนด นโยบาย กลยุทธ กระบวนการทำงาน++ จากบทเรียนนี้

- **บทเรียนจากความเสี่ยง**




- **ความหมาย และ ทบทวนการบริหารความเสี่ยง - สั้นๆ**

*ความเสี่ยงที่เป็นอันตราย (Hazard)*

เหตุการณ์ในเชิงลบที่หากเกิดขึ้นแล้วอาจเป็นอันตรายหรือสร้างความเสียหายต่อองค์กร

*ความเสียงที่เป็นความไม่แน่นอน (Uncertainty)*

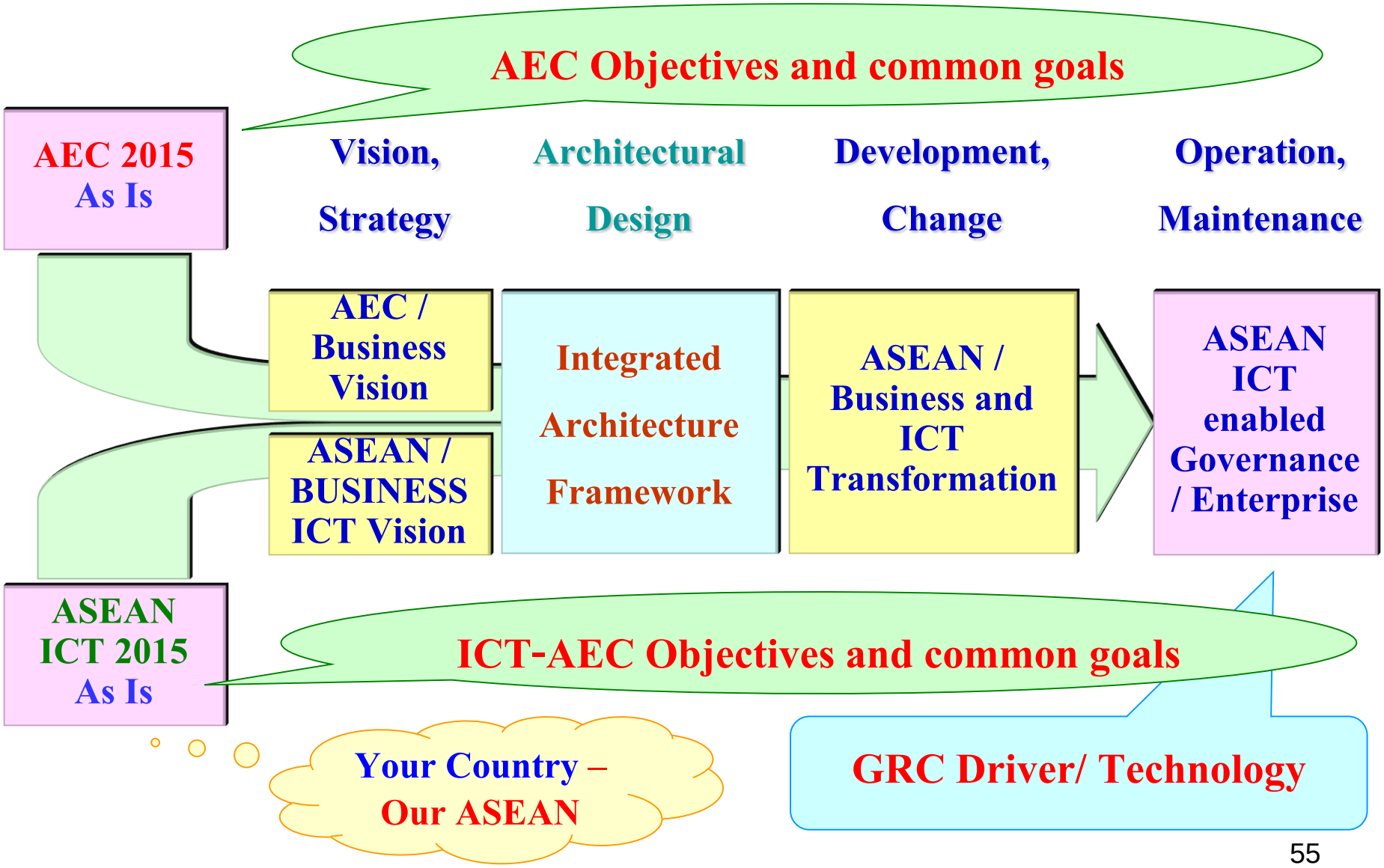
เหตุการณ์ที่ทำให้ผลที่องค์กรได้รับจากเหตุการณ์จริงไม่เป็นไปตามที่คาดการณ์ไว้ อันเนื่องมาจากสาเหตุต่างๆ กัน

*ความเสี่ยงที่เป็นโอกาส (Opportunity)*

เหตุการณ์ที่ทำให้องค์กรเสียโอกาสในการแข่งขัน การดำเนินงานและการเพิ่มมูลค่าของผู้ถือหุ้น


54

# ICT Enabled Governance and The Role of ICT



# ICT Risk & Development of Management to Integrated Management

Evolution of Scope

CG – Corporate Governance

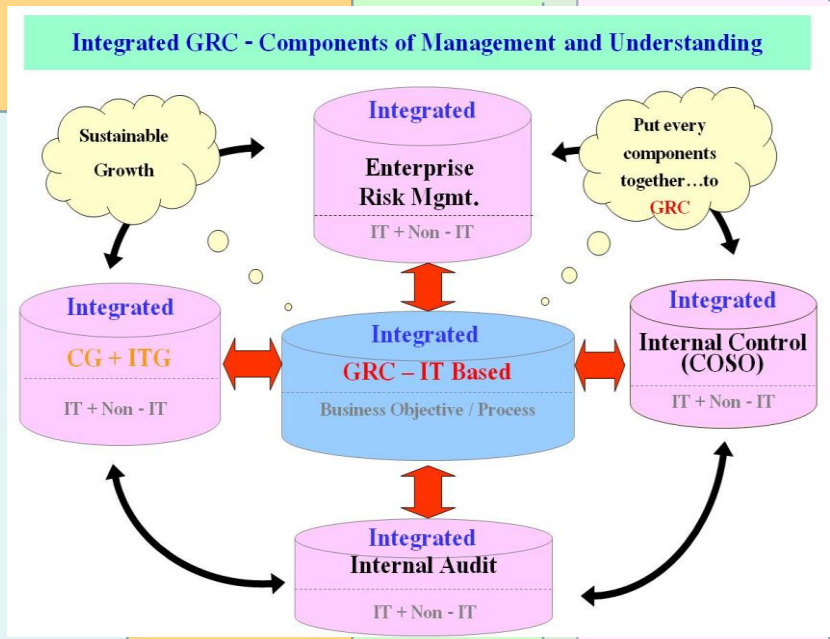
GEIT / Governance of Enterprise IT

IT Governance

Management

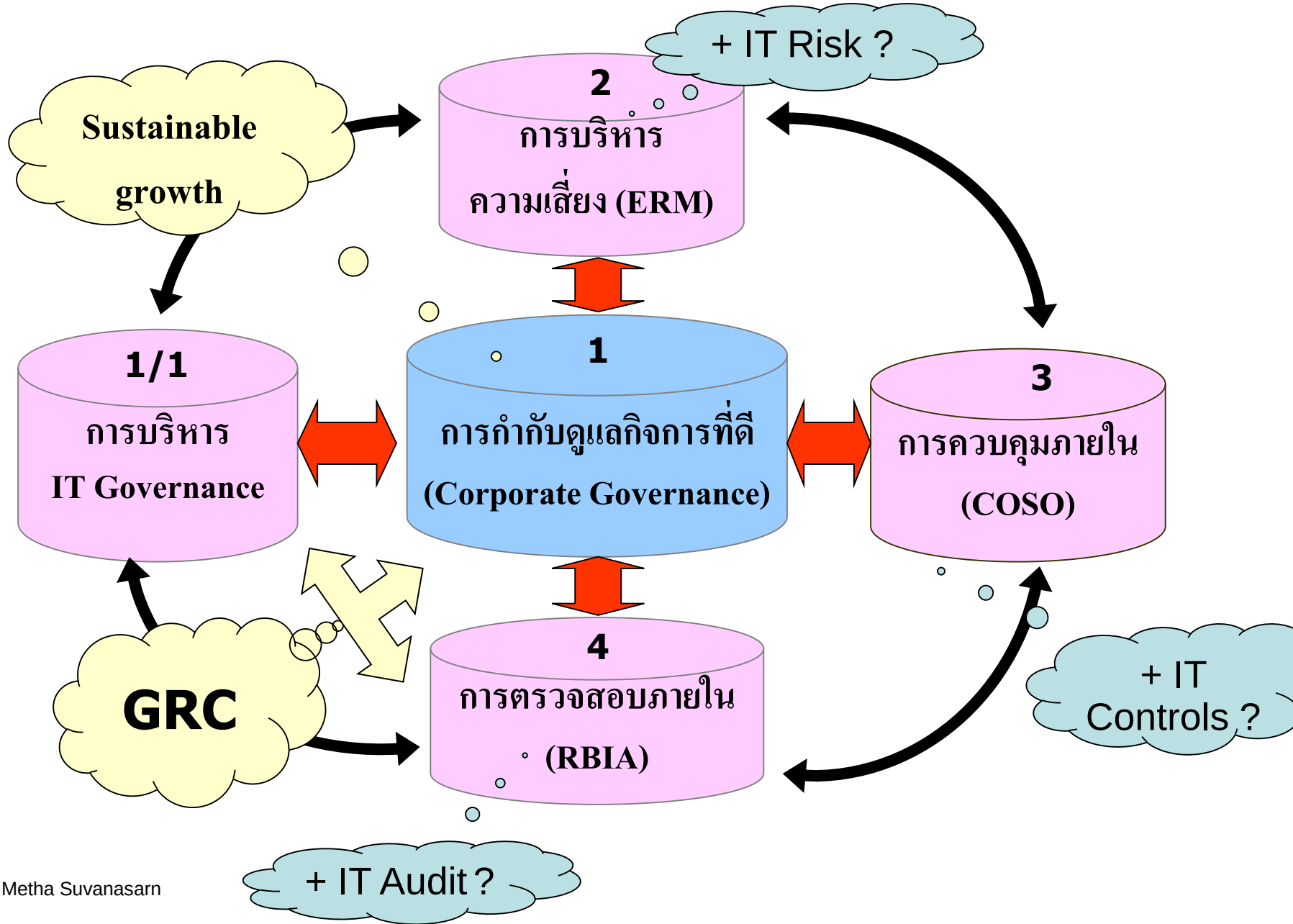
Control

Audit



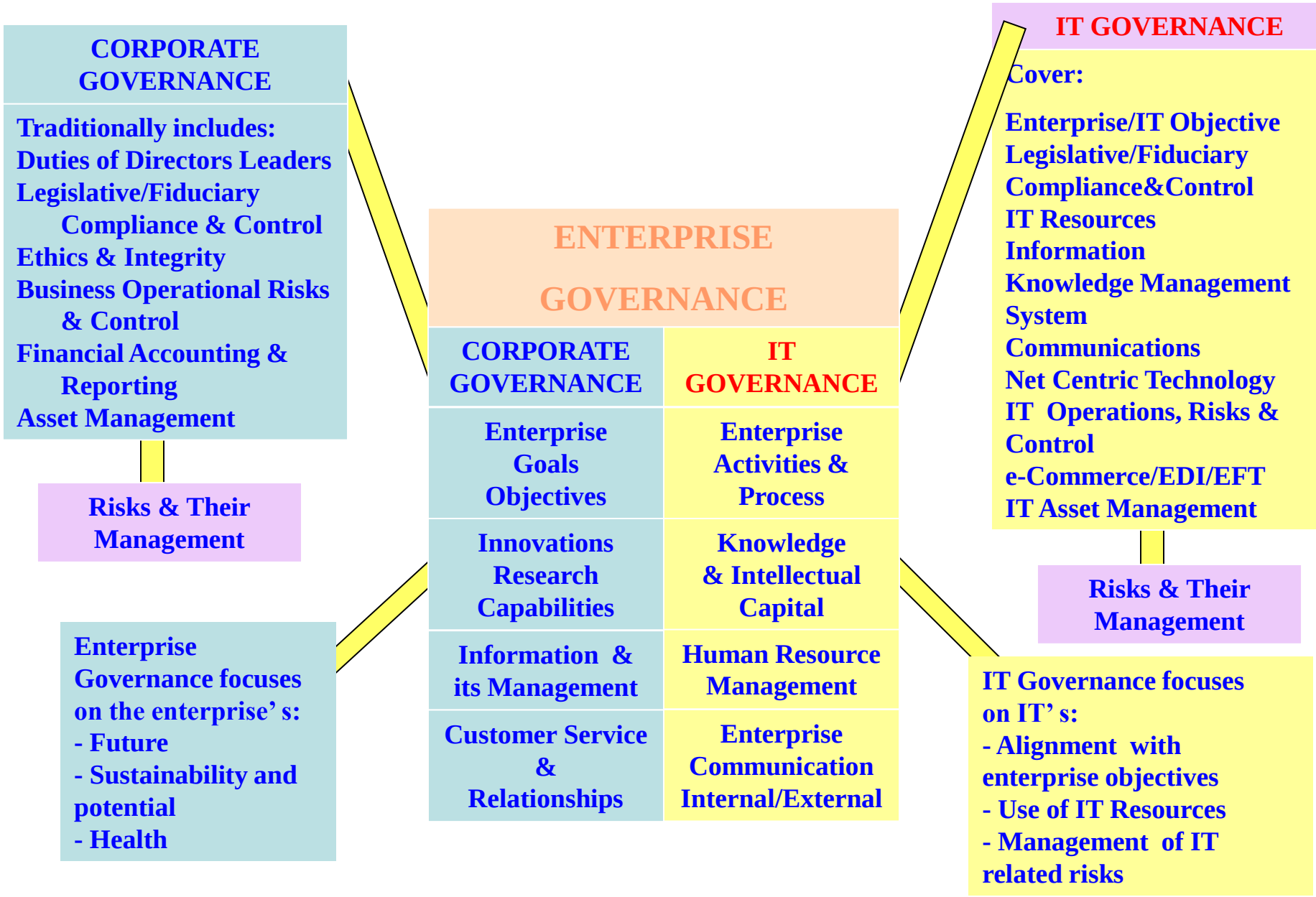

Source : www.itgthailand.com

# Value Creation for Effectiveness & Efficiency of Operations

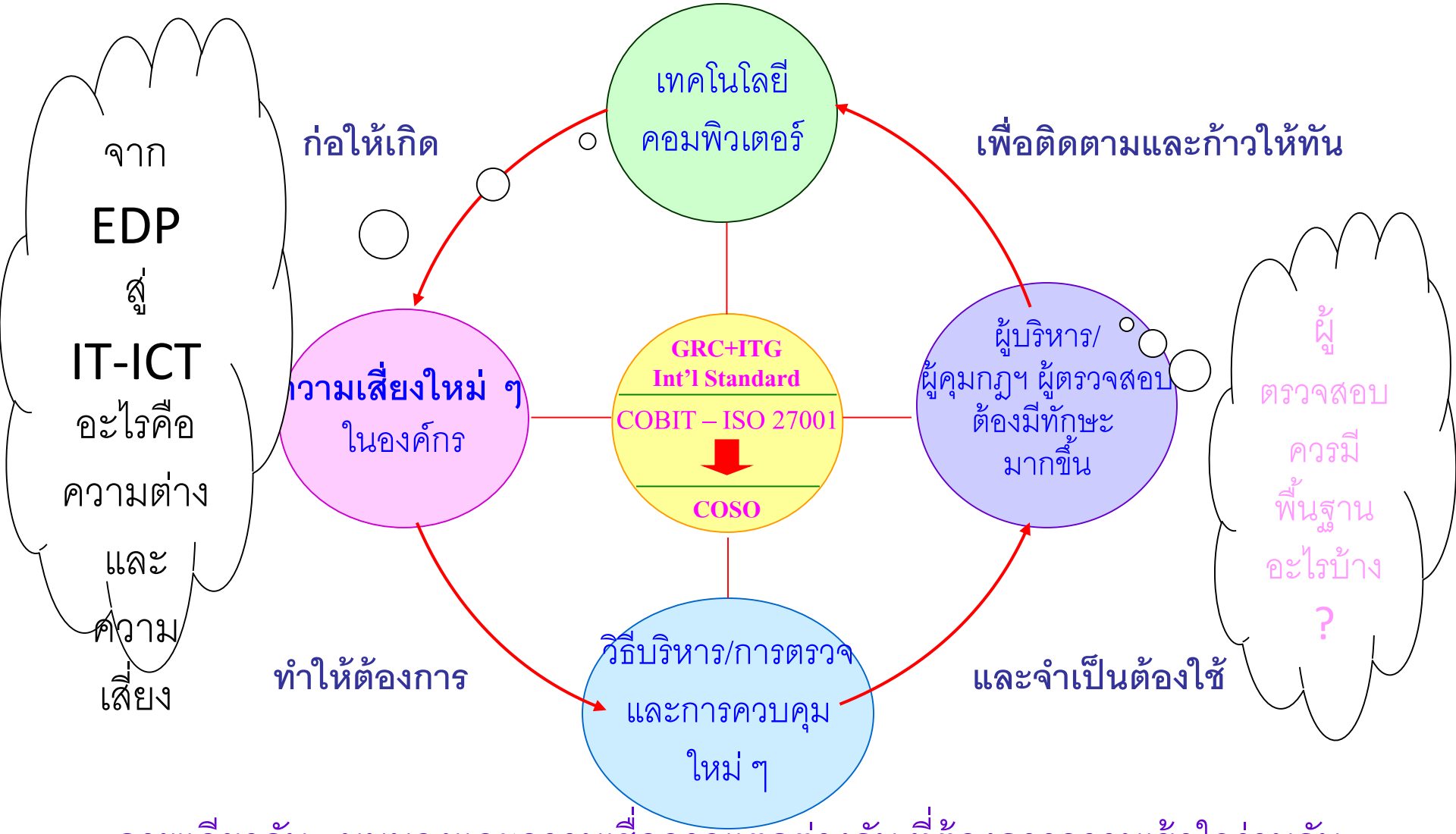



Source : Metha Suvanasarn

# ความสัมพันธ์ของ IT Governance และ Corporate Governance

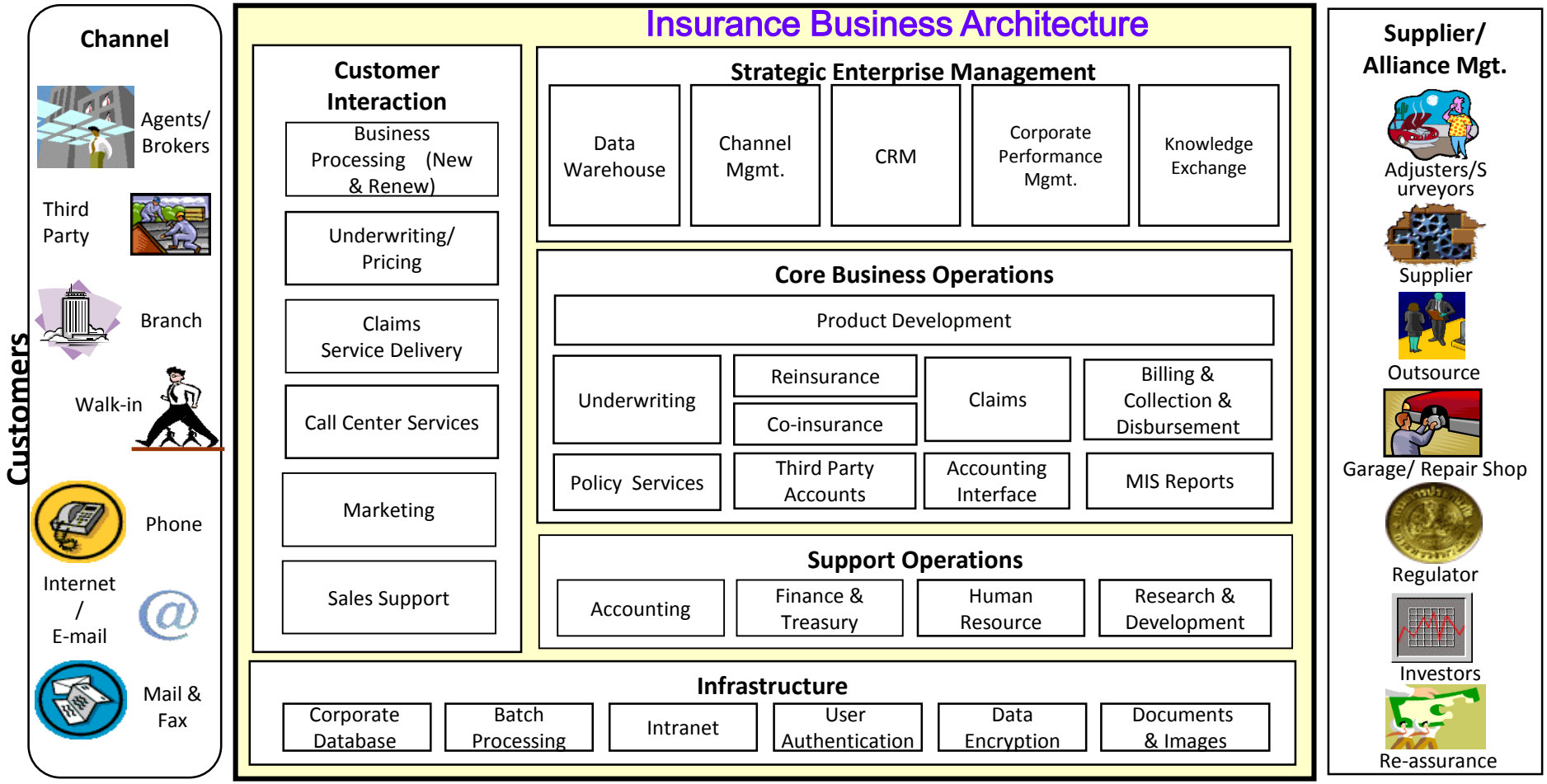


# :การหลอมรวมความเข้าใจในการบริหารมิติต่าง ๆ เพื่อการสร้างคุณค่าเพิ่มให้กับ Stakeh




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

# Insurance Business Architecture or any Org. & Understanding Core Business for P-D-C-A & GRC




จากภาพรวมของระบบงานประกันภัยข้างต้น ผู้ตรวจสอบและผู้บริหารควรเข้าใจถึงผลกระทบต่าง ๆ จาก **Operational Risk, Compliance Risk** และ **Strategic Risk** ที่มีผลกระทบทางการเงินและต่อความถูกต้องของการรายงานทางการเงิน (**Financial Risk**) จากระบบปฏิบัติการที่อาจมีจุดอ่อนทางด้าน **People Risk, Process Risk** และ **Technology Risk** ซึ่งต้องใช้หลักการ **ERM** หรือ **Enterprise Risk Management** ตามหลักการของ **COSO** ที่จะเกี่ยวข้องกับการบริหาร และการวางแผนรวมทั้งการตรวจสอบแบบบูรณาการ ต่อไป

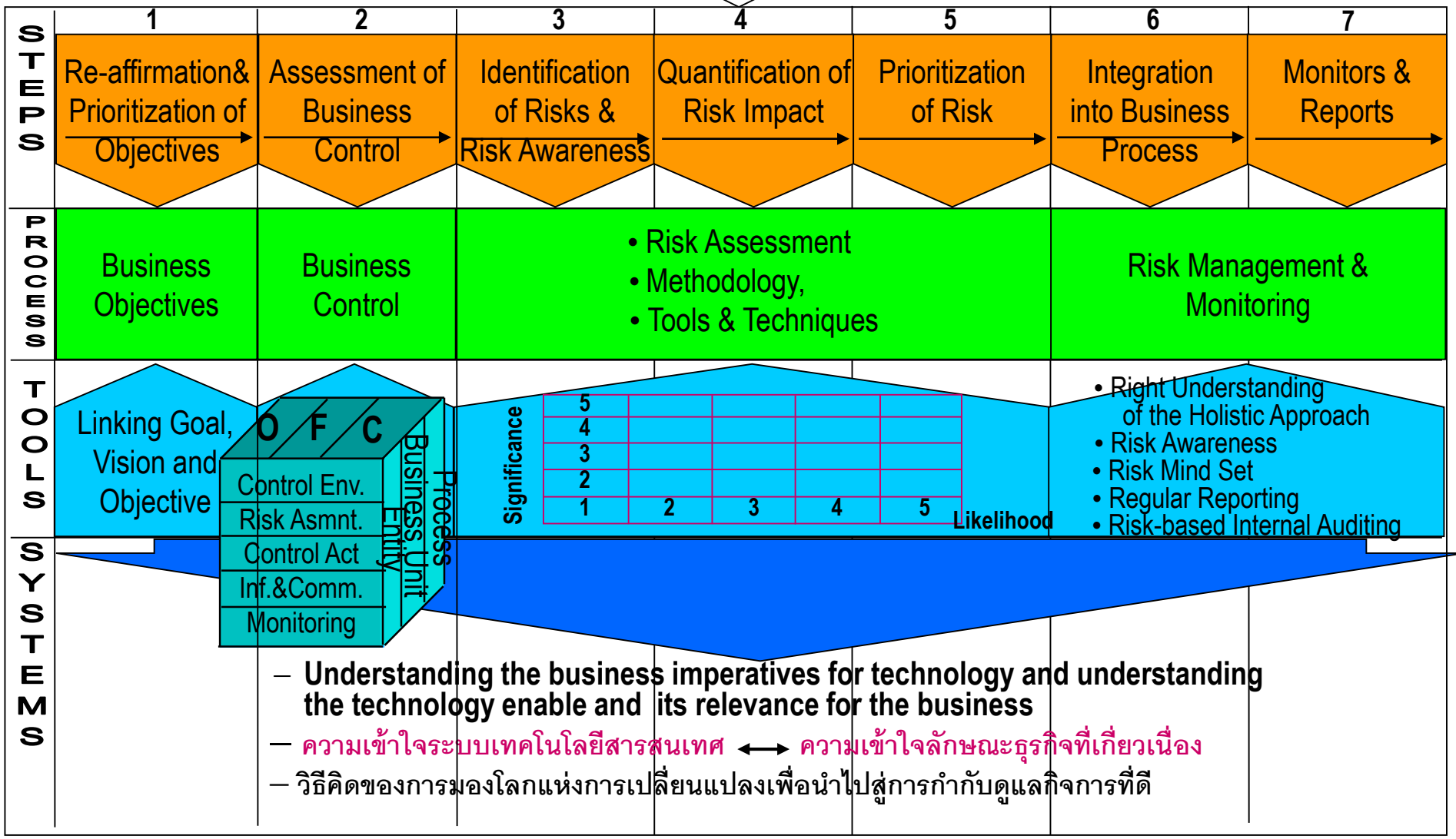
# การกำกับดูแลกิจการที่ดี Governance)

กับ

การตรวจสอบภายใน
(Risk based audit)

องค์รวมของการบริหารความเสี่ยงขององค์กร

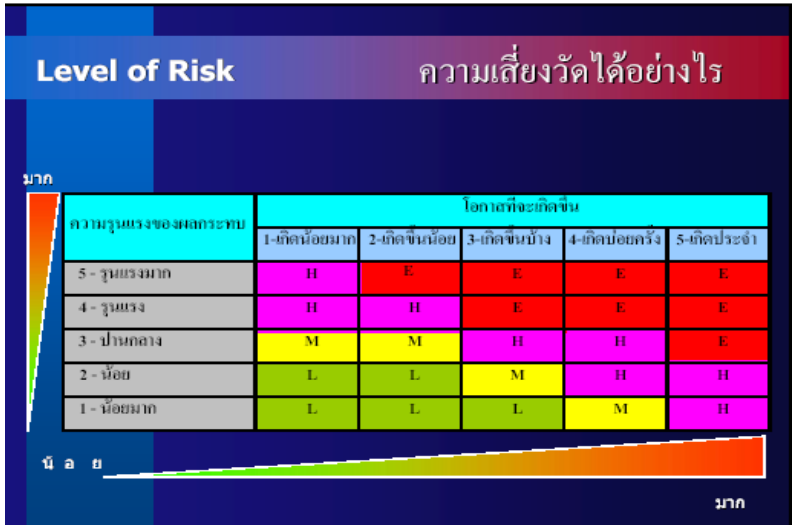
การควบคุมภายใน
(COSO)




– **Understanding the business imperatives for technology and understanding the technology enable and its relevance for the business**

– ความเข้าใจระบบเทคโนโลยีสารสนเทศ ⟷ ความเข้าใจลักษณะธุรกิจที่เกี่ยวเนื่อง

– วิธีคิดของการมองโลกแห่งการเปลี่ยนแปลงเพื่อนำไปสู่การกำกับดูแลกิจการที่ดี

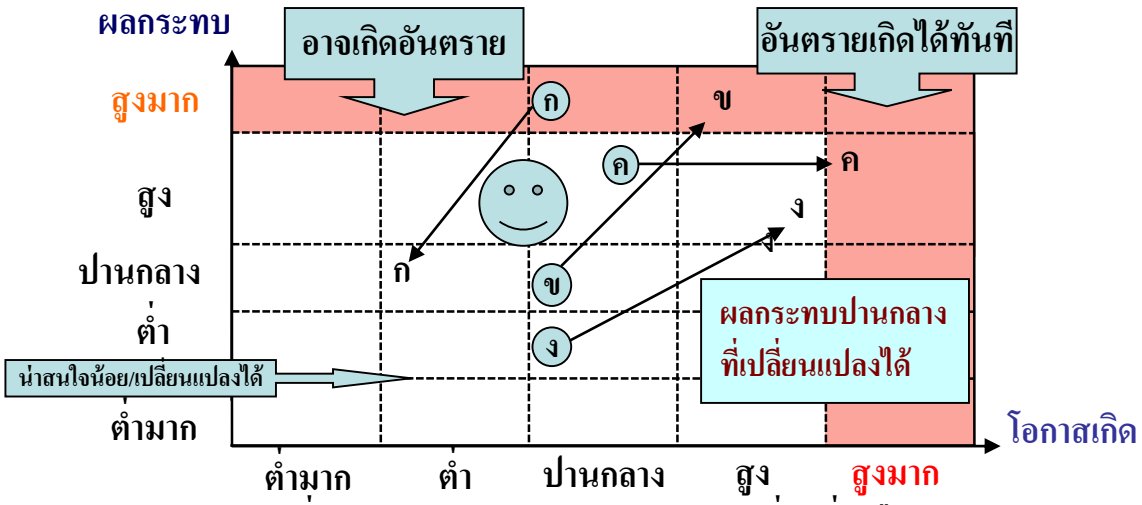



# รูปแบบอื่น ๆ ของ Risk Appetite

## 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


**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 & Risk IT and IT Risk Perspective

Risk IT

BASED ON COBIT®

In business today, risk plays a critical role. Almost every business decision requires executives and managers to balance risk and reward. Effectively managing the business risks is essential to an enterprise's success.

Too often, IT risk (business risk related to the use of IT) is overlooked. Other business risks, such as market risks, credit risks and operational risks have long been integrated into the corporate decision-making processes. IT risk has been relegated to technical specialists outside the boardroom, despite falling under the same 'umbrella' risk category as other business risks: failure to achieve strategic objectives.

Source : ISACA

# GRC & Risk IT and IT Risk Perspective

## What is Risk IT?

**Risk IT is:**

- A framework based on a set of guiding principles for effective governance and management of IT risk
- Part of ISACA's product portfolio on IT governance

Source : 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

# GRC & Risk IT and IT Risk Perspective

## The problem is clear. The solution? Unclear.

## Until now: **Introducing Risk IT**

Risk IT is a framework based on a set of guiding principles for effective management of IT risk.

The Risk IT framework explains IT risk, allows the enterprise to make appropriate risk-aware decisions and will enable users to:

- Integrate the management of IT risk into the overall enterprise risk management (ERM) of the organization
- Make well-informed decisions about the extent of the risk, the risk appetite and the risk tolerance of the enterprise
- Understand how to respond to the risk

Source : ISACA

# GRC & Risk IT and IT Risk Perspective

## Risk IT and CobiT®

The Risk IT framework complements CobiT®, a comprehensive, globally accepted framework for the governance and control of business-driven, IT-based solutions and services. While CobiT supports a set of controls to mitigate IT risk, Risk IT provides a framework for enterprises to identify, govern and manage IT risk. Simply put, CobiT provides the *means* of risk management; Risk IT provides the *ends*. Enterprises who have adopted (or are planning to adopt) CobiT as their IT governance framework can use Risk IT to enhance risk management.

Source : ISACA

# GRC & Risk IT and IT Risk Perspective

## The Risk IT Principles

The Risk IT framework is about IT risk—business risk related to the use of IT. The connection to business is founded in the principles on which the framework is built. Effective enterprise governance and management of IT risk:

- Always connects to business objectives
- Aligns the management of IT-related business risk with overall ERM—if applicable, i.e., if ERM is implemented in the enterprise
- Balances the costs and benefits of managing IT risk
- Promotes fair and open communication of IT risk
- Establishes the right tone from the top while defining and enforcing personal accountability for operating within acceptable and well-defined tolerance levels
- Is a continuous process and part of daily activities

Source : ISACA

# GRC & Risk IT and IT Risk Perspective

## Managing and Understanding IT Risk

To prioritize and manage IT risk, senior executives need a frame of reference and a clear understanding of the IT function and IT risk. However, the enterprise's key stakeholders, including board members and executive management, the very people who should be accountable for risk management within the enterprise, often do not have a full understanding of IT risk.

IT risk is not just a technical issue. While IT subject matter experts help to understand and manage aspects of IT risk, business management is the most important stakeholder. Business managers determine what IT needs to do to support their business; they set the targets for IT and are accountable for managing the associated risks.

In summary, the framework will enable enterprises to understand and manage all significant IT risk types. The Risk IT framework provides an end-to-end, comprehensive view of all risks related to the use of IT, as well as a similar view of risk management. The framework fills the gap between generic risk management frameworks such as COSO ERM and AS/NZS 4360 (soon to be replaced by ISO 31000) and its British equivalent, A Risk Management Standard (ARMS), and detailed (primarily security-related) IT risk management frameworks.

Source : ISACA

# GRC & Risk IT and IT Risk Perspective

## Risk IT Framework

For users of CobiT and Val IT™, this process model will look familiar. Guidance is provided on the key activities within each process, responsibilities for the process, information flows between processes and performance management of each process. The model is divided into three domains—Risk Governance, Risk Evaluation, Risk Response—each containing three processes:

- Risk Governance
  - —Establish and Maintain a Common Risk View
  - —Integrate with ERM
  - —Make Risk-aware Business Decisions
- Risk Evaluation
  - —Collect Data
  - —Analyze Risk
  - —Maintain Risk Profile
- Risk Response
  - —Articulate Risk
  - —Manage Risk
  - —React to Events

Source : ISACA

# GRC & Risk IT and IT Risk Perspective

## Risk IT Practitioner Guide

The *Risk IT Practitioner Guide* is a support document for the Risk IT framework that provides examples of possible techniques to address IT-related risk issues, and more detailed guidance on how to approach the concepts covered in the process model.

Concepts and techniques explored in more detail include:

- Building enterprise-specific scenarios, based on a set of generic IT risk scenarios
- Building a risk map, using techniques to describe the impact and frequency of scenarios
- Building impact criteria with business relevance
- Defining key risk indicators (KRIs)
- Using CobiT and Val IT to mitigate risk; the link between risk and CobiT control objectives and Val IT key management practices

Source : ISACA

# GRC & Risk IT and IT Risk Perspective

## Your Solution to IT Risk

Applying good IT risk management practices as described in Risk IT will provide tangible business benefits, e.g., fewer operational surprises and failures, increased information quality, greater stakeholder confidence and reduced regulatory concerns, innovative applications supporting new business initiatives. The Risk IT framework is part of ISACA's product portfolio on IT governance. Although this document provides a complete and standalone framework, it does include references to CobiT and Val IT. As *The Practitioner Guide*, issued in support of this framework, makes extensive reference to CobiT and Val IT, it is recommended that managers and practitioners acquaint themselves with the major principles and contents of these two frameworks. Like CobiT and Val IT, Risk IT is not a standard, but a flexible framework. This means that enterprises can and should customize the components provided in the framework to suit their particular organizations.

Source : ISACA

# Business Governance of IT and Functional Governance of IT

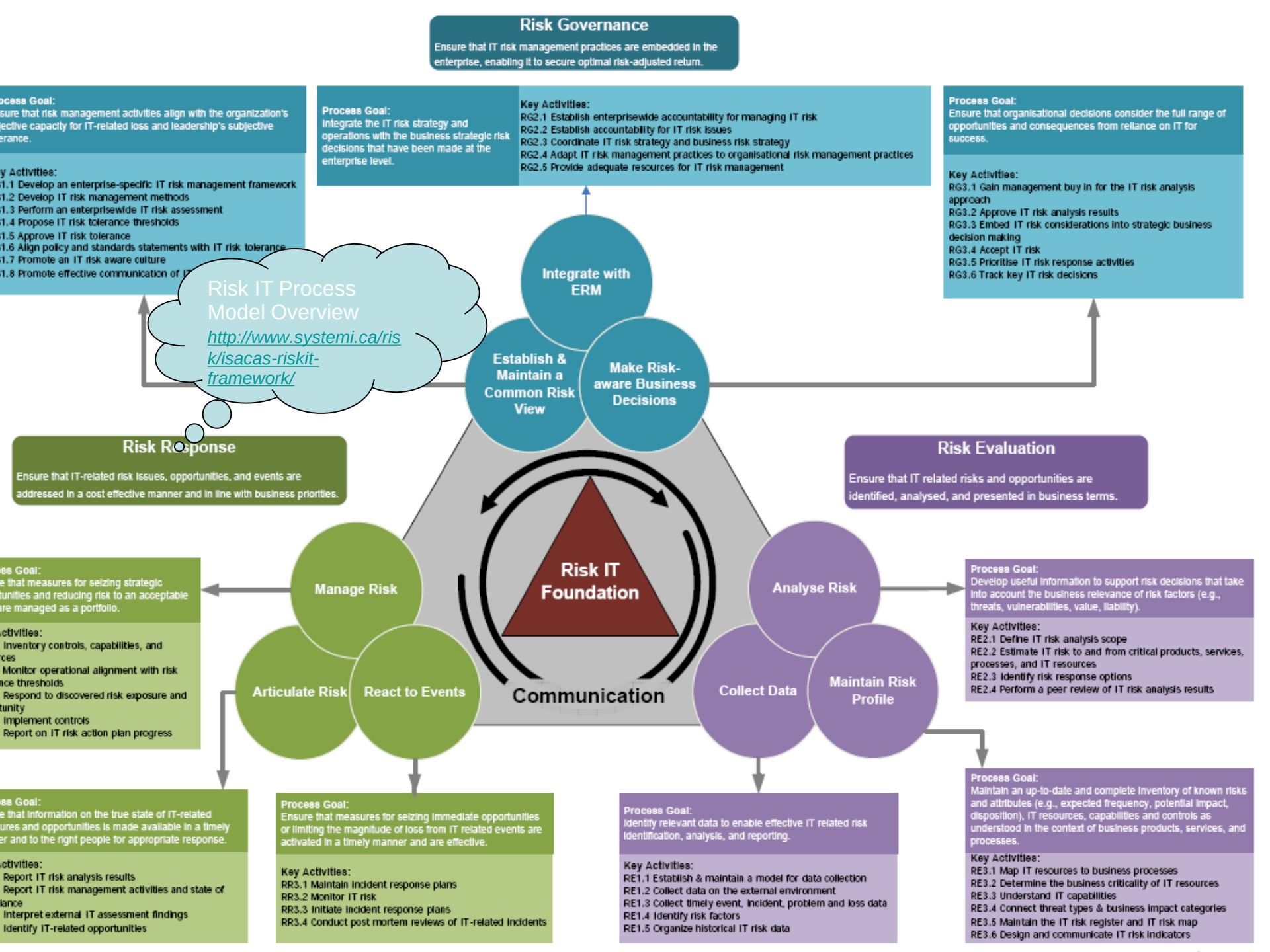
## Business Governance of IT

- Bottom line performance
- Investment in the right thing
- Demand management and prioritisation
- Funding and capital management
- Level of risk
- Balancing the cost, risk and performance equation
- Identifying and delivering benefits

## Functional Governance of IT

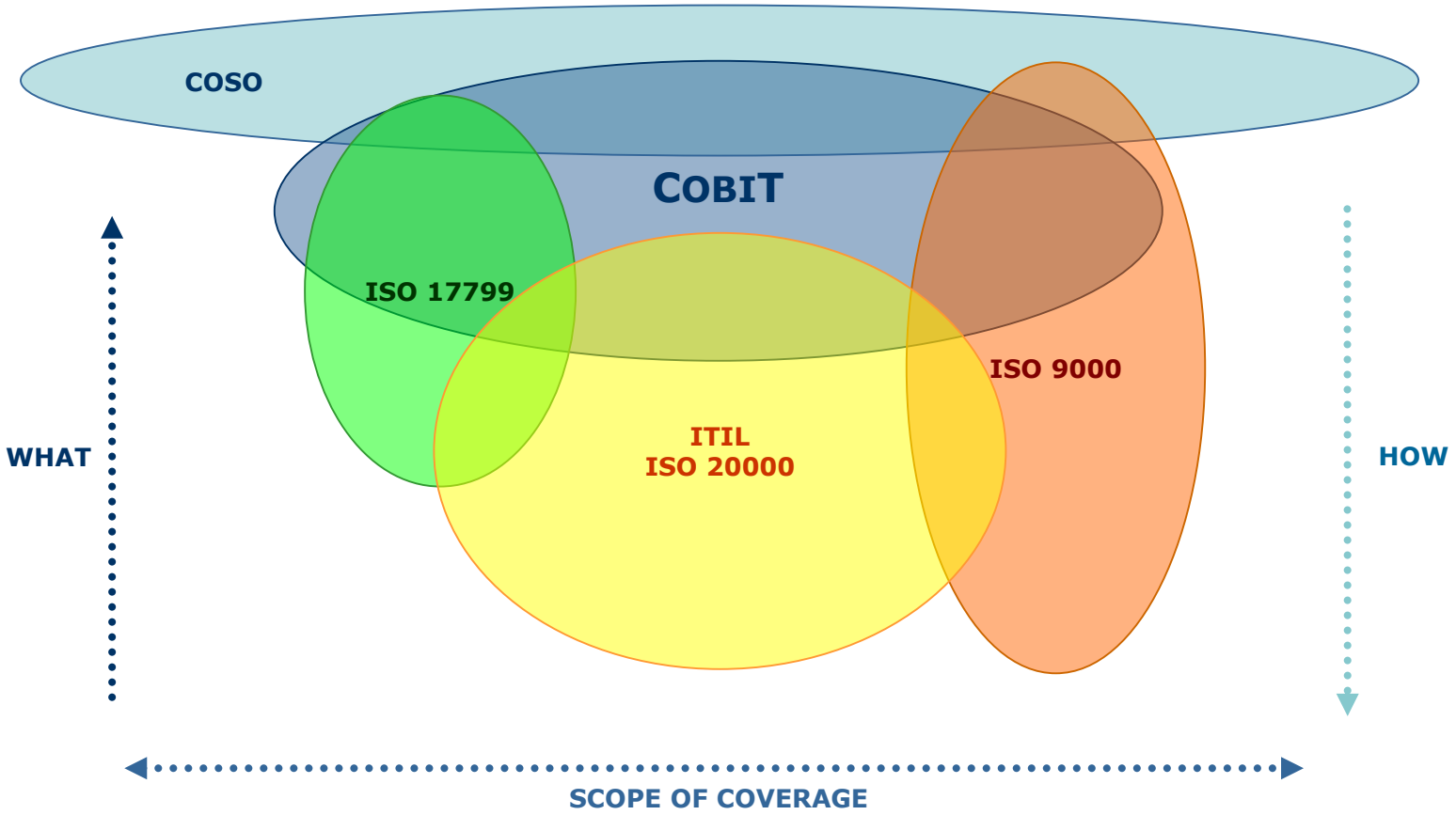
- Compliance
- Doing it the right way
- Supply management and sourcing
- Productivity and unit cost of delivery
- Articulating risk and managing to agreed service levels
- Delivering to estimates
- Standards, repeatable processes, monitoring and control

Source : "Business Governance of IT and IT Governance of IT – a big difference", COBIT Users Convention, Nov 2006 By Chris Gillies


Risk Governance
Ensure that IT risk management practices are embedded in the enterprise, enabling it to secure optimal risk-adjusted return.
Process Goal:
sure that risk management activities align with the organization's
jective capacity for IT-related loss and leadership's subjective
erance.
y Activities:
1.1 Develop an enterprise-specific IT risk management framework
1.2 Develop IT risk management methods
1.3 Perform an enterprisewide IT risk assessment
1.4 Propose IT risk tolerance thresholds
1.5 Approve IT risk tolerance
1.6 Align policy and standards statements with IT risk tolerance
1.7 Promote an IT risk aware culture
1.8 Promote effective communication of I
Process Goal:
Integrate the IT risk strategy and operations with the business strategic risk decisions that have been made at the enterprise level.
Key Activities:
RG2.1 Establish enterprisewide accountability for managing IT risk
RG2.2 Establish accountability for IT risk issues
RG2.3 Coordinate IT risk strategy and business risk strategy
RG2.4 Adapt IT risk management practices to organisational risk management practices
RG2.5 Provide adequate resources for IT risk management
Process Goal:
Ensure that organisational decisions consider the full range of opportunities and consequences from reliance on IT for success.
Key Activities:
RG3.1 Gain management buy in for the IT risk analysis approach
RG3.2 Approve IT risk analysis results
RG3.3 Embed IT risk considerations into strategic business decision making
RG3.4 Accept IT risk
RG3.5 Prioritise IT risk response activities
RG3.6 Track key IT risk decisions
Risk IT Process Model Overview
http://www.systemi.ca/risk/isacas-riskit-framework/
Integrate with ERM
Establish & Maintain a Common Risk View
Make Risk-aware Business Decisions
Risk Response
Ensure that IT-related risk issues, opportunities, and events are addressed in a cost effective manner and in line with business priorities.
Risk Evaluation
Ensure that IT related risks and opportunities are identified, analysed, and presented in business terms.
Risk IT Foundation
Communication
Manage Risk
Articulate Risk
React to Events
Analyse Risk
Collect Data
Maintain Risk Profile
s Goal:
e that measures for seizing strategic
tunities and reducing risk to an acceptable
re managed as a portfolio.
ctivities:
Inventory controls, capabilities, and
ces
Monitor operational alignment with risk
nce thresholds
Respond to discovered risk exposure and
tunity
Implement controls
Report on IT risk action plan progress
s Goal:
e that information on the true state of IT-related
ures and opportunities is made available in a timely
r and to the right people for appropriate response.
ctivities:
Report IT risk analysis results
Report IT risk management activities and state of
iance
Interpret external IT assessment findings
Identify IT-related opportunities
Process Goal:
Ensure that measures for seizing immediate opportunities or limiting the magnitude of loss from IT related events are activated in a timely manner and are effective.
Key Activities:
RR3.1 Maintain incident response plans
RR3.2 Monitor IT risk
RR3.3 Initiate incident response plans
RR3.4 Conduct post mortem reviews of IT-related incidents
Process Goal:
Identify relevant data to enable effective IT related risk identification, analysis, and reporting.
Key Activities:
RE1.1 Establish & maintain a model for data collection
RE1.2 Collect data on the external environment
RE1.3 Collect timely event, incident, problem and loss data
RE1.4 Identify risk factors
RE1.5 Organize historical IT risk data
Process Goal:
Develop useful information to support risk decisions that take into account the business relevance of risk factors (e.g., threats, vulnerabilities, value, liability).
Key Activities:
RE2.1 Define IT risk analysis scope
RE2.2 Estimate IT risk to and from critical products, services, processes, and IT resources
RE2.3 Identify risk response options
RE2.4 Perform a peer review of IT risk analysis results
Process Goal:
Maintain an up-to-date and complete inventory of known risks and attributes (e.g., expected frequency, potential impact, disposition), IT resources, capabilities and controls as understood in the context of business products, services, and processes.
Key Activities:
RE3.1 Map IT resources to business processes
RE3.2 Determine the business criticality of IT resources
RE3.3 Understand IT capabilities
RE3.4 Connect threat types & business impact categories
RE3.5 Maintain the IT risk register and IT risk map
RE3.6 Design and communicate IT risk indicators

# COBIT and Other IT/Infosec Management Standards & Best Practices

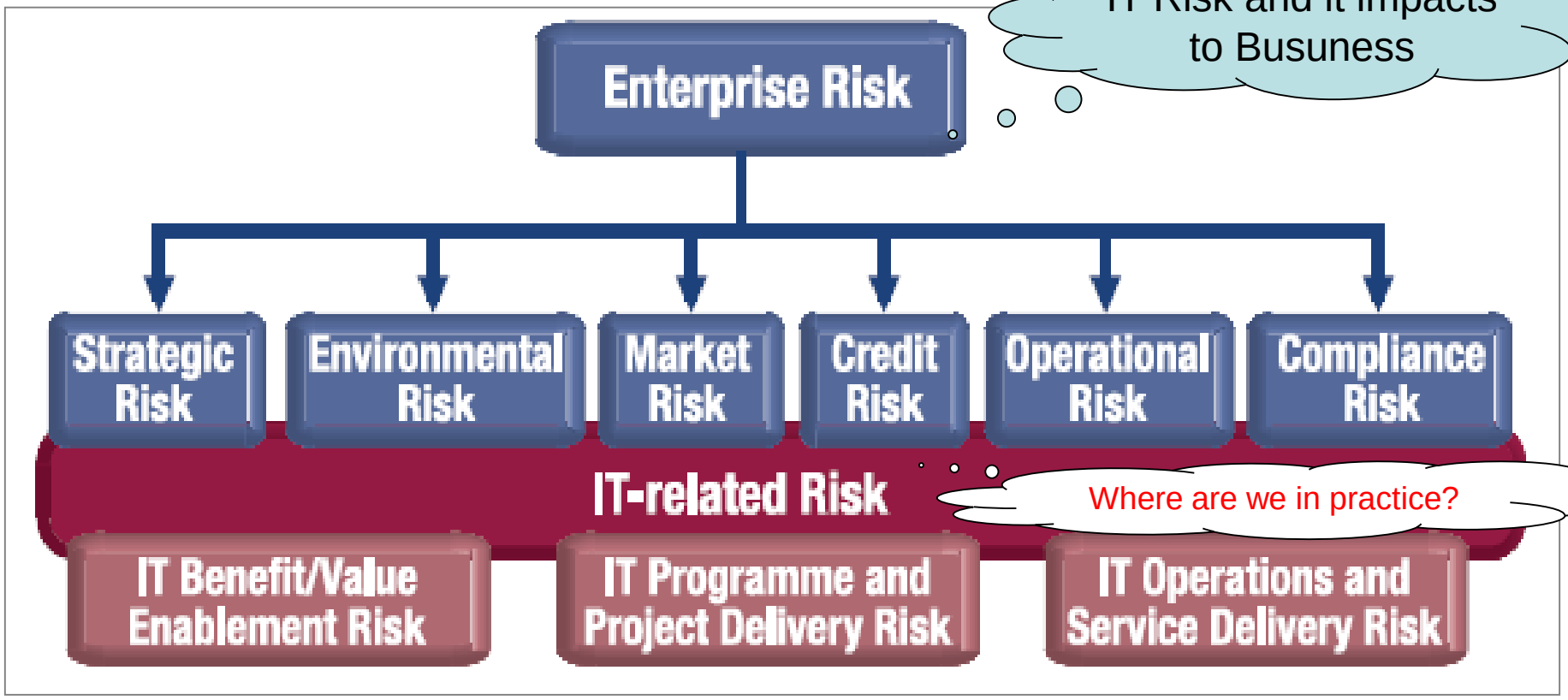
**Organisations will consider and use a variety of IT models, standards and best practices. These must be understood in order to consider how they can be used together, with COBIT acting as the consolidator ('umbrella').**




Source: ITGI

# DEFINING A RISK UNIVERSE AND SCOPING RISK MANAGEMENT

## IT Risk in the Risk Hierarchy




Source : ISACA

# COBIT OVERVIEW

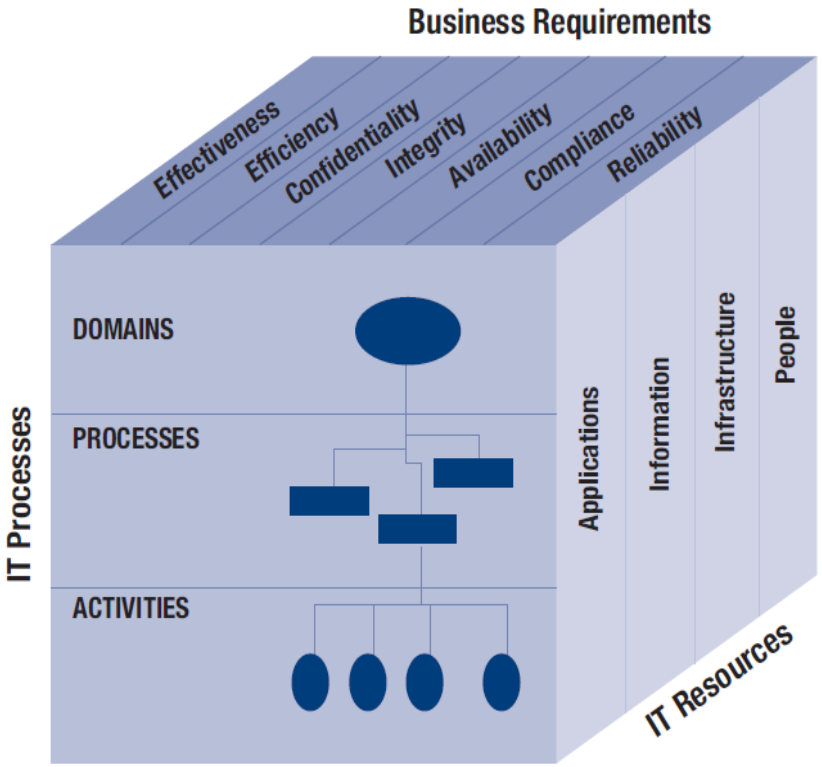
## CobiT Cube

The previously mentioned components (IT processes, information criteria and resources) combine to form a three-dimensional illustration of the IT function. These dimensions, as shown in **figure 5**, represent the CobiT cube.

## IT Governance Using CobiT

By definition, governance of IT and its processes is an ongoing and periodic measurement of deviations from the defined standard and timely and consequent implementation of corrective measures. This approach follows the cybernetic principle, i.e., everyone understands the process of setting the room temperature (standard) for the heating system (process), which will constantly check (compare) ambient room temperature (control information) and will signal (act) the heating system to provide more heat. This model and its principles identify a number of KGIs and KPIs that usually apply to all processes as they deal with what the standard is, who sets it, and who controls or needs to act.

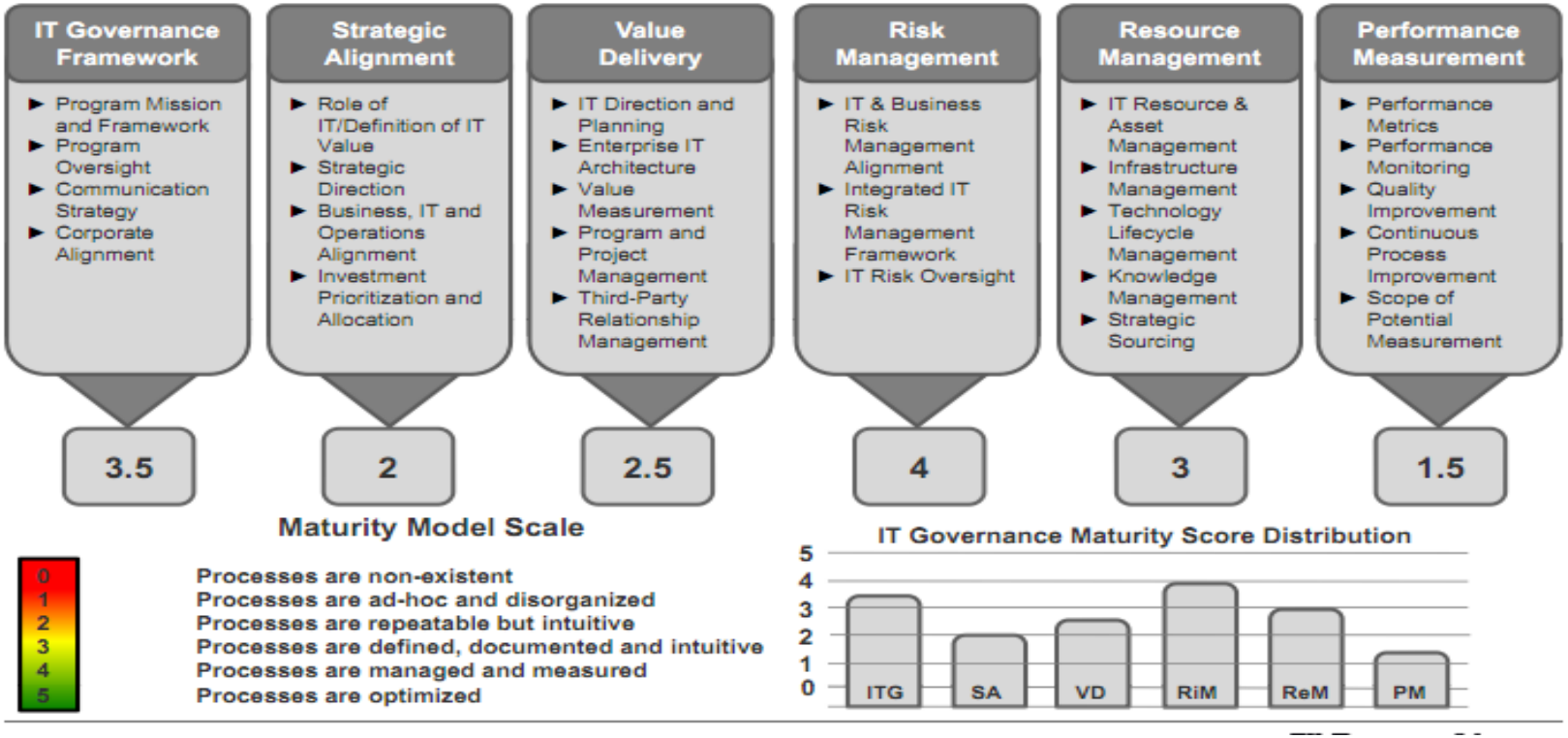
## Top-down Approach




Source : IT Governance Institute

# Controls & Maturity Model & CSA

## Example: IT Governance Maturity Assessment Components




Source : E & Y

# Q & A

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

พระราชกฤษฎีกาว่าด้วยวิธีการแบบปลอดภัยในการทำธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2553 มีผล 180 วันนับจากวันที่ 3 กันยายน 2553++ ท่านพร้อมแล้วหรือยังครับ ? เพราะเกี่ยวข้องกับทุกองค์กร +++ นโยบายความมั่นคงปลอดภัยสารสนเทศฯ +++ โปรดติดตามที่.....

www.itgthailand.com,หรือhttp://www.ratchakitcha.soc.go.th/DATA/PDF/2553/A/053/13.PDF

# บทบาทหน้าที่ความรับผิดชอบตามโครงสร้าง

ทบทวน Business & ICT Risk

| ผู้รับผิดชอบ | ขั้นตอนการดำเนินการ |
|---|---|

สื่อสารและสร้างความตระหนักเพื่อให้เกิดการปฏิบัติทั่วทั้งองค์กร

1.คณะกรรมการ

2. คณะกรรมการตรวจสอบ

3.คณะกรรมการบริหารความเสี่ยง

4.ผู้บริหาร

5. คณะทำงานบริหารความเสี่ยง

6. ผู้ประสานงานความเสี่ยงหน่วยงาน

7.ผู้ปฏิบัติงาน

องค์กร

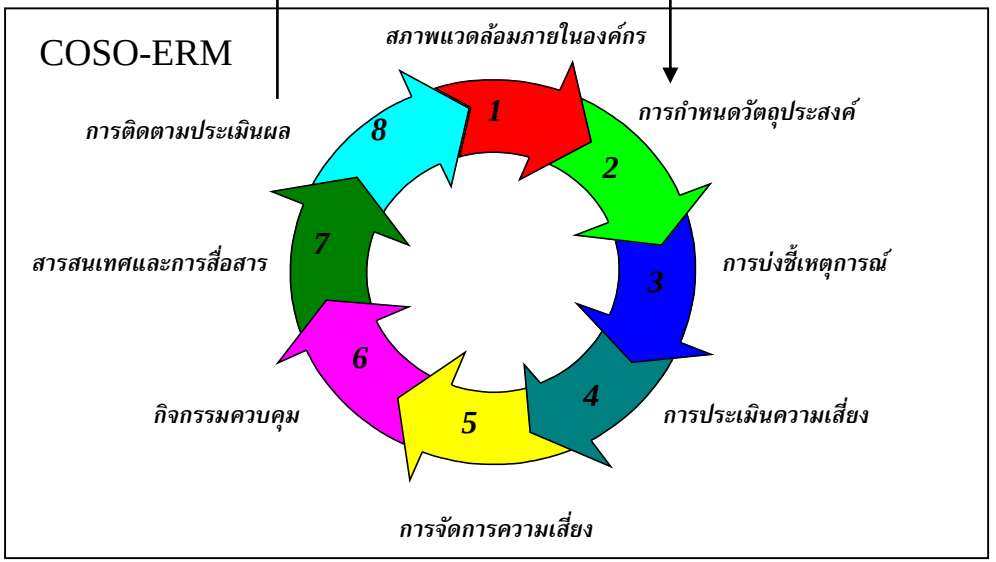
หน่วยงาน

กำหนดนโยบายด้านบริหารความเสี่ยง

อนุมัติแผนปฏิบัติงานประจำปี

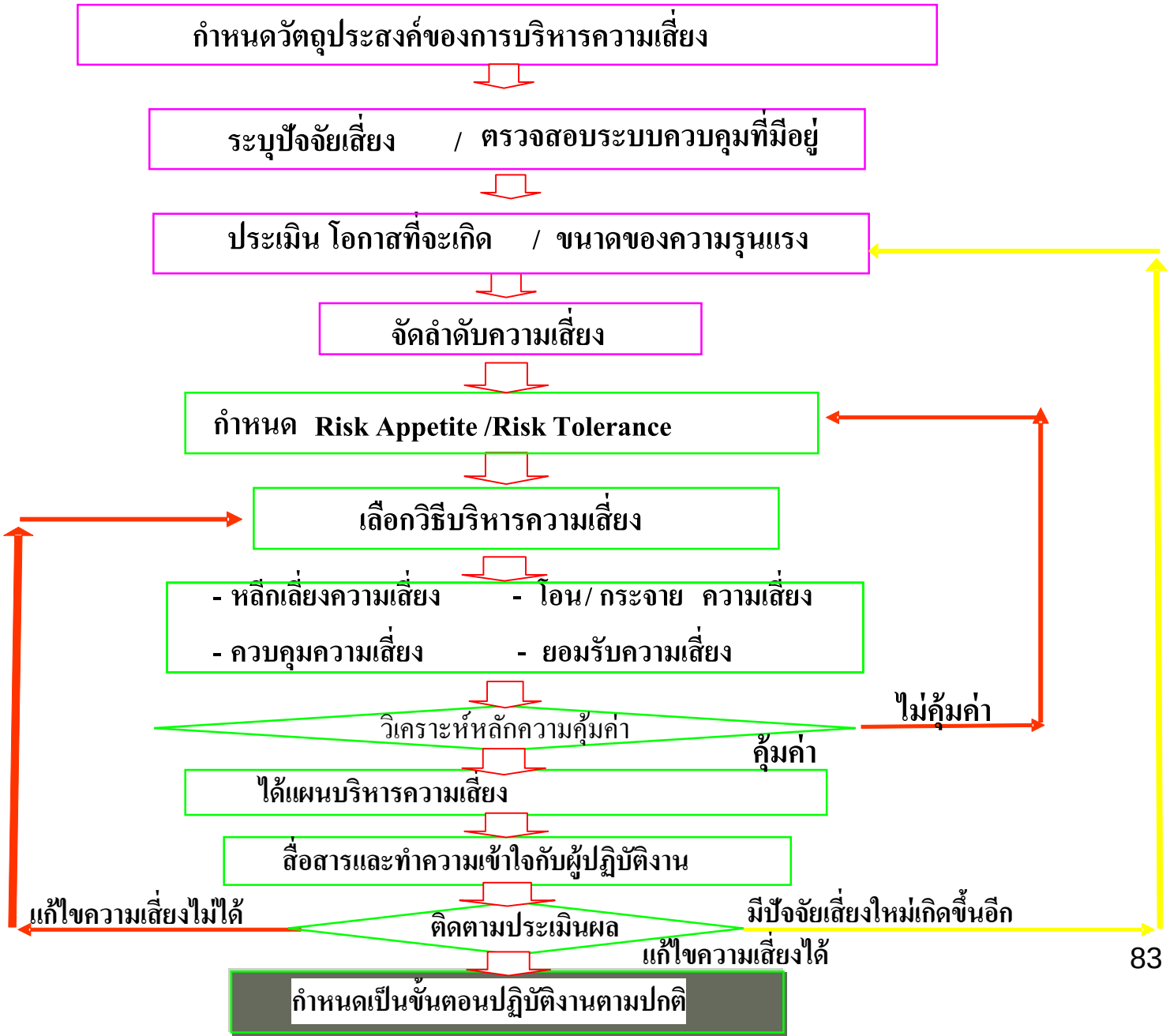
กำกับดูแลและติดตามผลการปฏิบัติงานตามนโยบายการบริหารความเสี่ยง

ให้ข้อเสนอแนะเกี่ยวกับนโยบายการบริหารความเสี่ยงโดยรวม กรอบการบริหารความเสี่ยง และแผนปฏิบัติงานประจำปี




ติดตามผลการปฏิบัติงานตามนโยบายและแผนการบริหารความเสี่ยง

# 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

↓

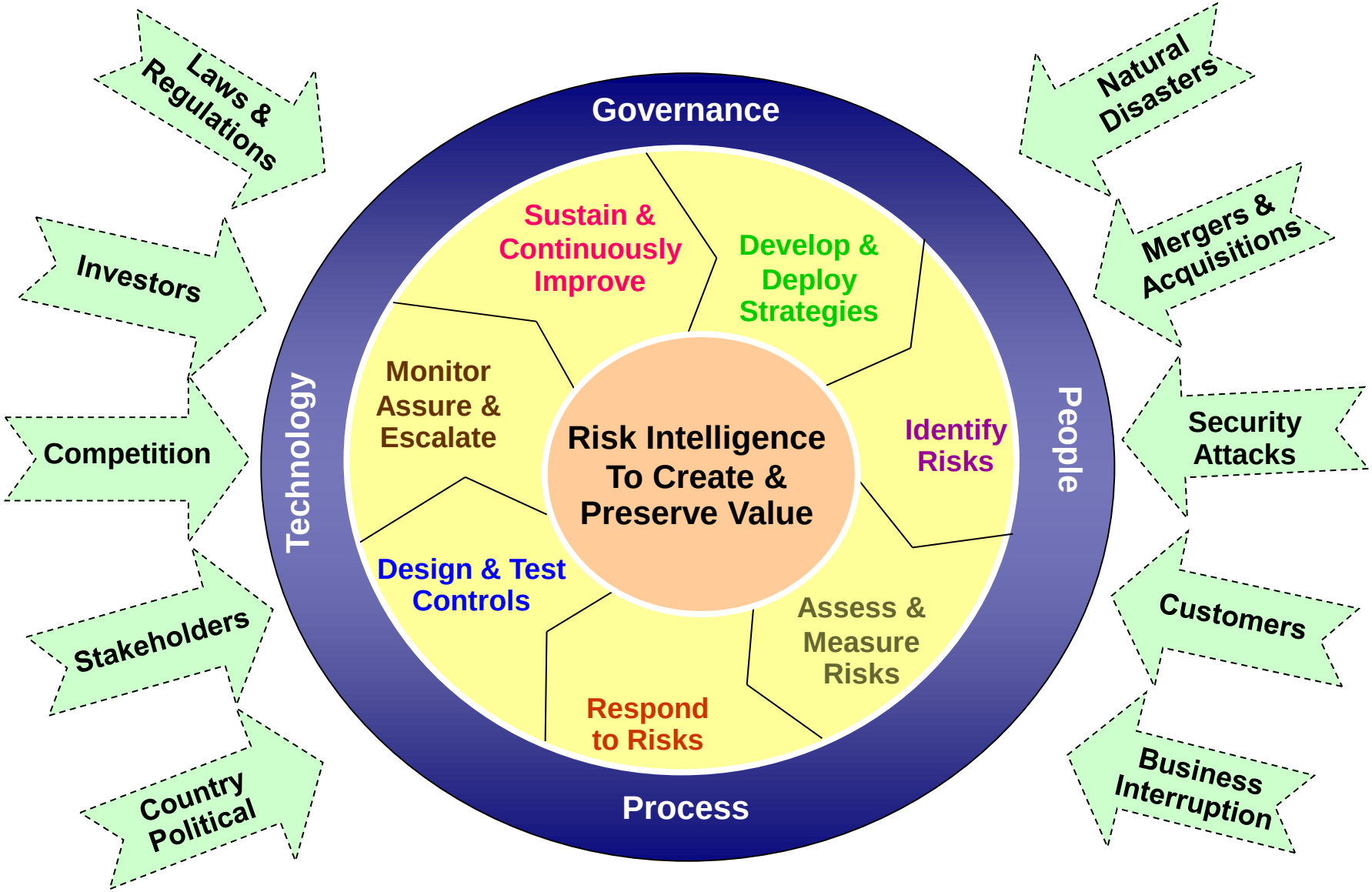
**7. ระบบสารสนเทศและการติดต่อสื่อสาร (Information and Communication)**

Information – Strategic and Integrated Systems - Communication

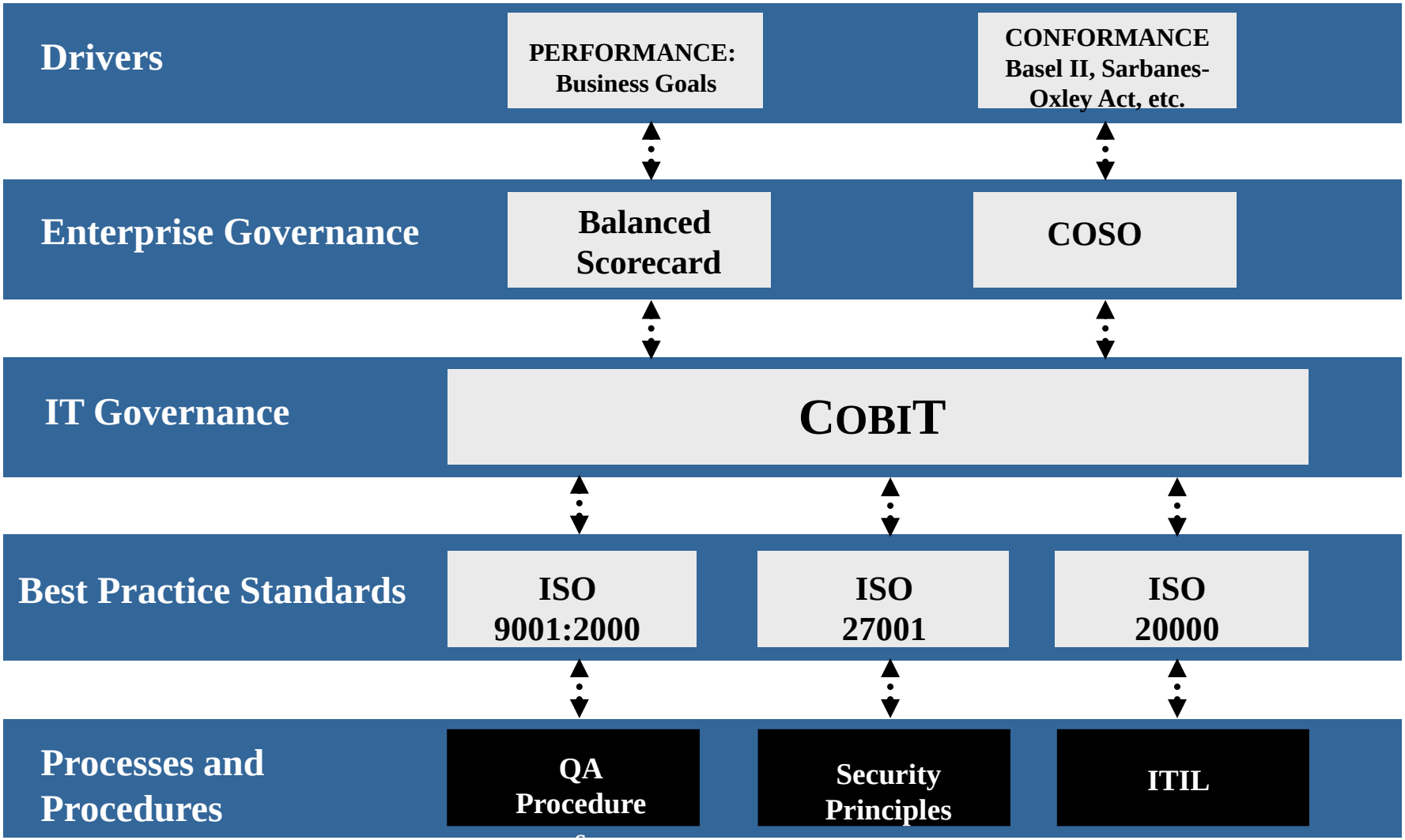
↓

**8. การติดตามและประเมินผล (Monitoring)**

Separate Evaluation – Ongoing Evaluation

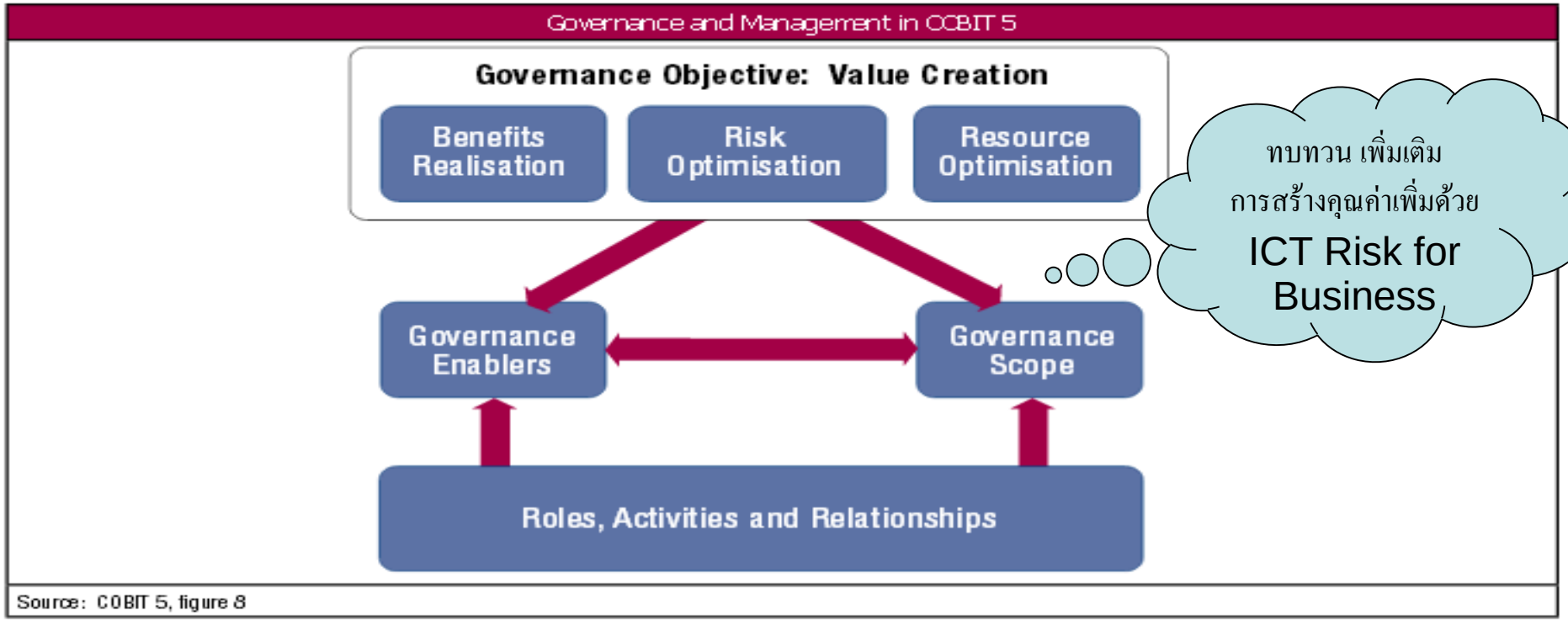

Laws & Regulations
Investors
Competition
Stakeholders
Country Political
Natural Disasters
Mergers & Acquisitions
Security Attacks
Customers
Business Interruption
Governance
Technology
People
Process
Sustain & Continuously Improve
Develop & Deploy Strategies
Identify Risks
Assess & Measure Risks
Respond to Risks
Design & Test Controls
Monitor Assure & Escalate
Risk Intelligence To Create & Preserve Value

# GRC Perspectives & Where Does COBIT Fit?

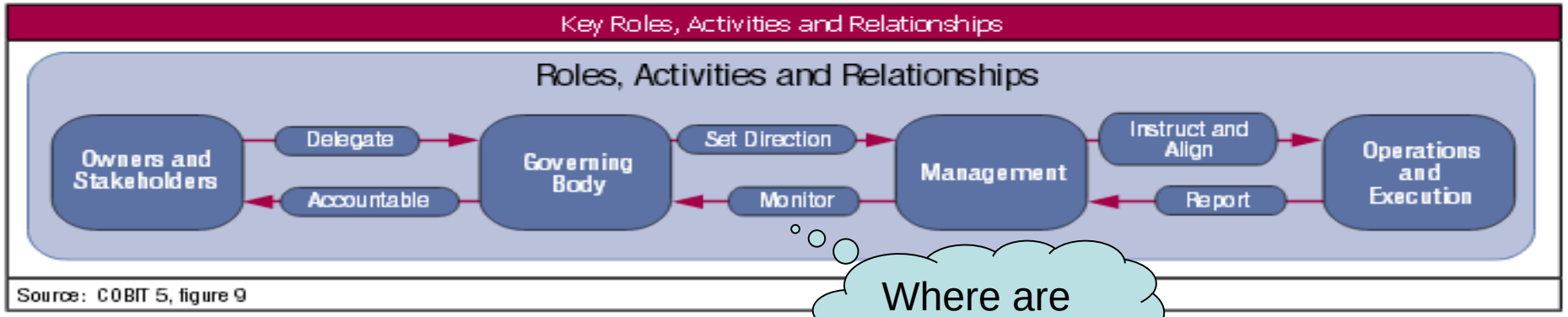



Source: ITGI

# COBIT 5 and Key Roles-Activities- Relationship




ทบทวน เพิ่มเติม
การสร้างคุณค่าเพิ่มด้วย
ICT Risk for Business

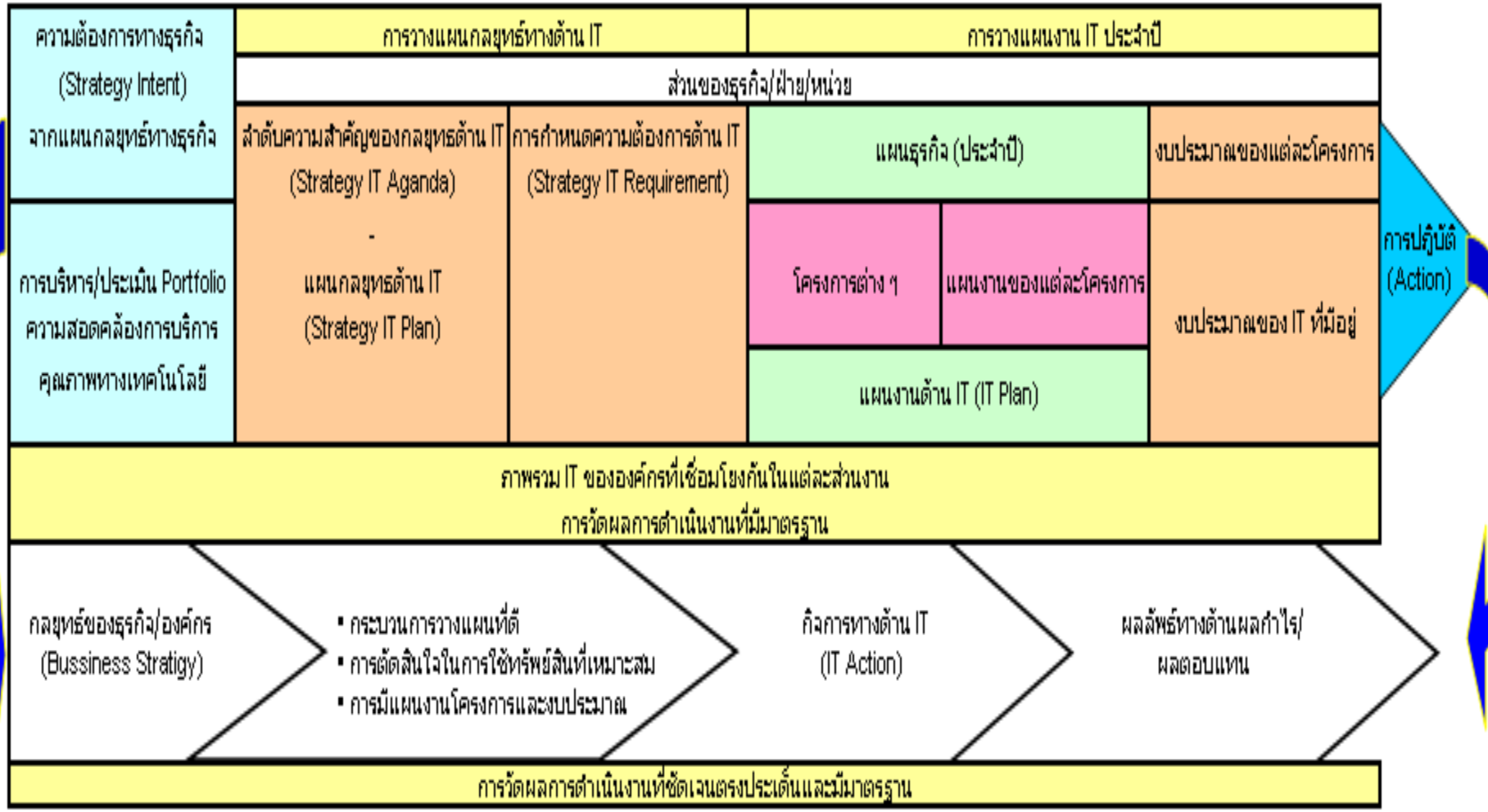



Where are you ?

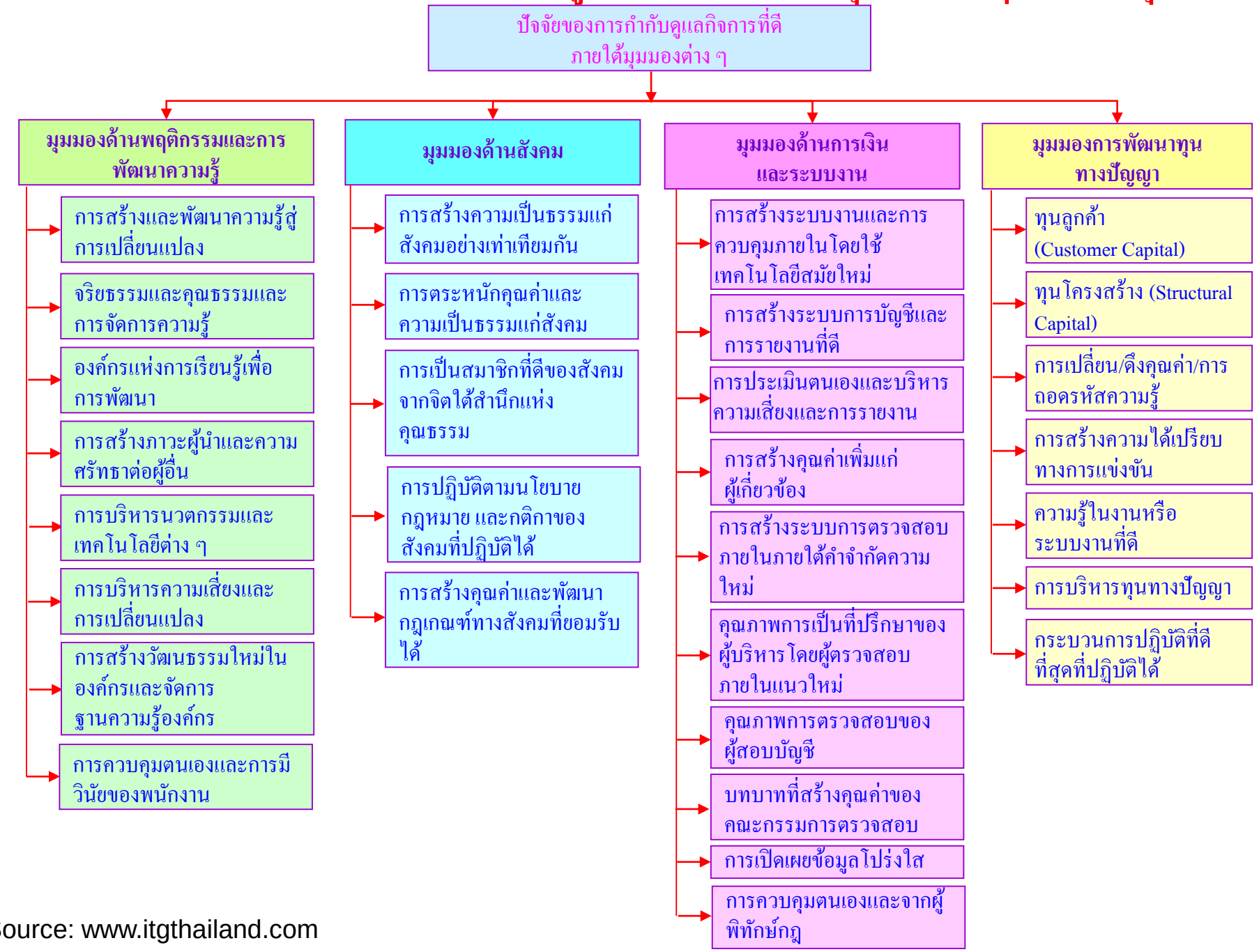
Source : ISACA

# การเชื่อมโยง Value Chain ของกลยุทธ์ (Business Strategy) IT Strategy

## สู่การปฏิบัติ กับ การวัดผลการดำเนินงานขององค์กร- Business Strategy -> Business & IT Related Goals

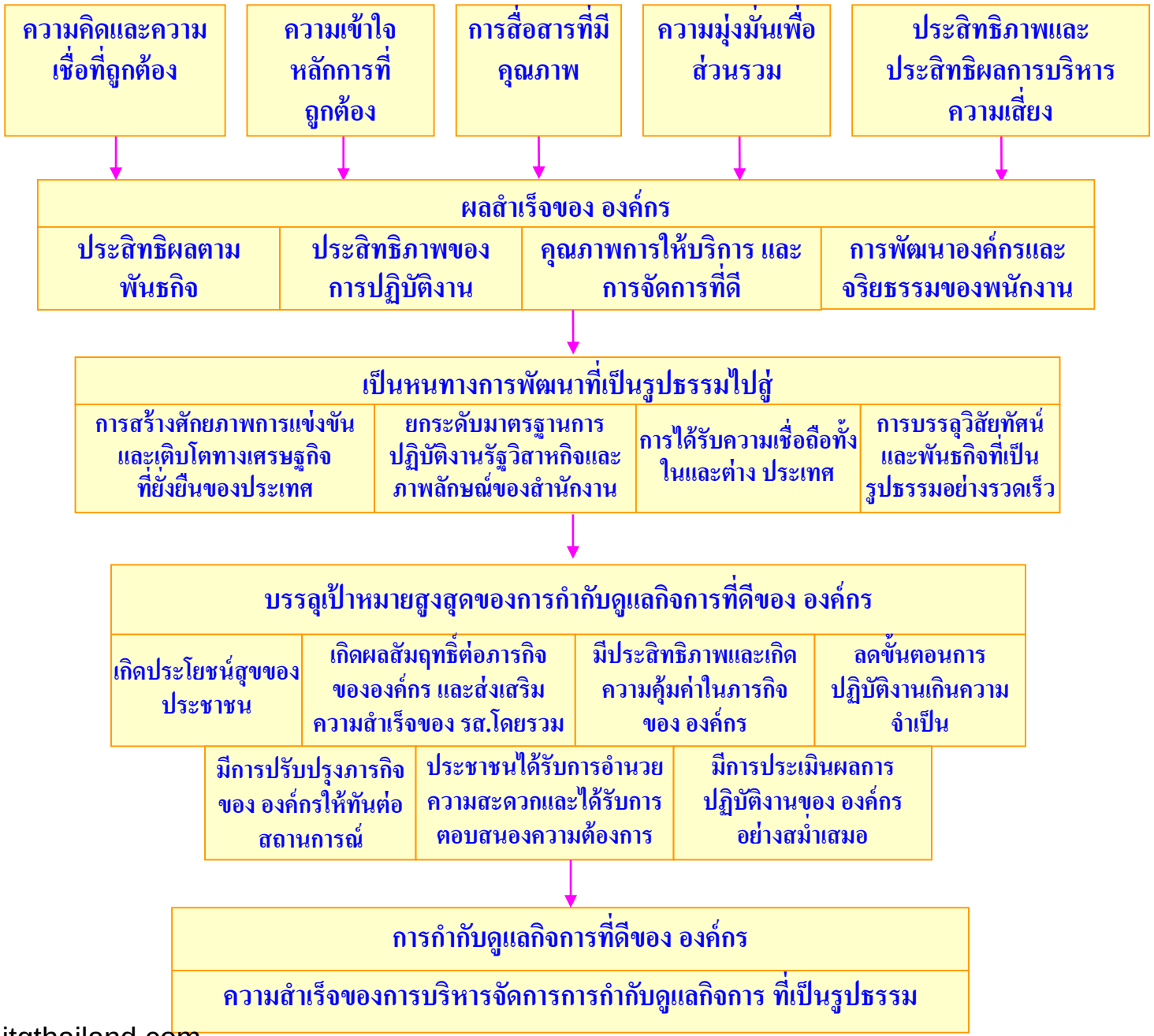


# ปัจจัยและโครงสร้าง/กระบวนการการกำกับดูแลกิจการที่ดี ภายใต้มุมมองต่าง ๆ เพื่อสร้างคุณค่าเพิ่ม



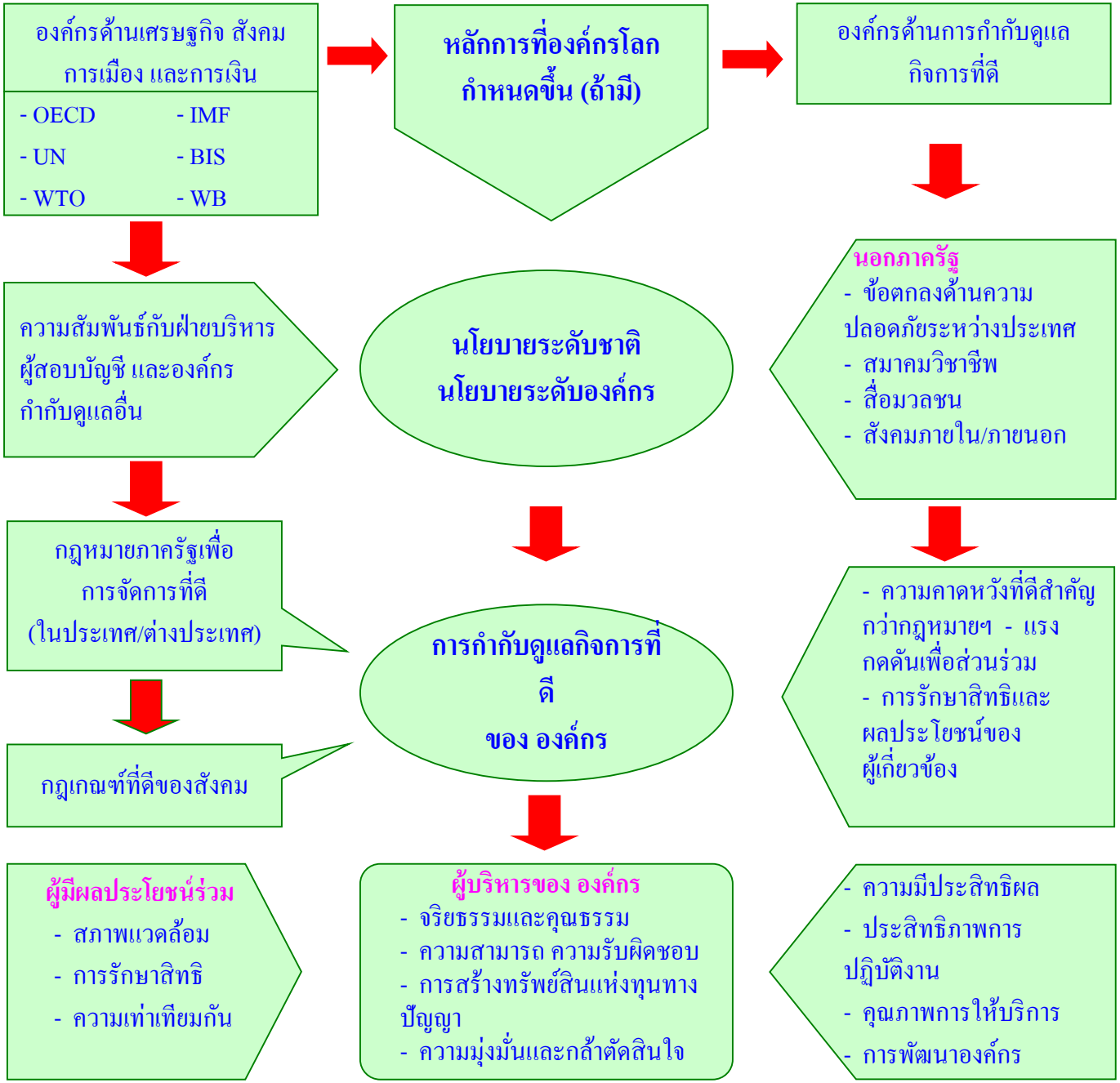

Source: www.itgthailand.com

# กระบวนการสร้างการกำกับดูแลกิจการที่ดีของ องค์กร

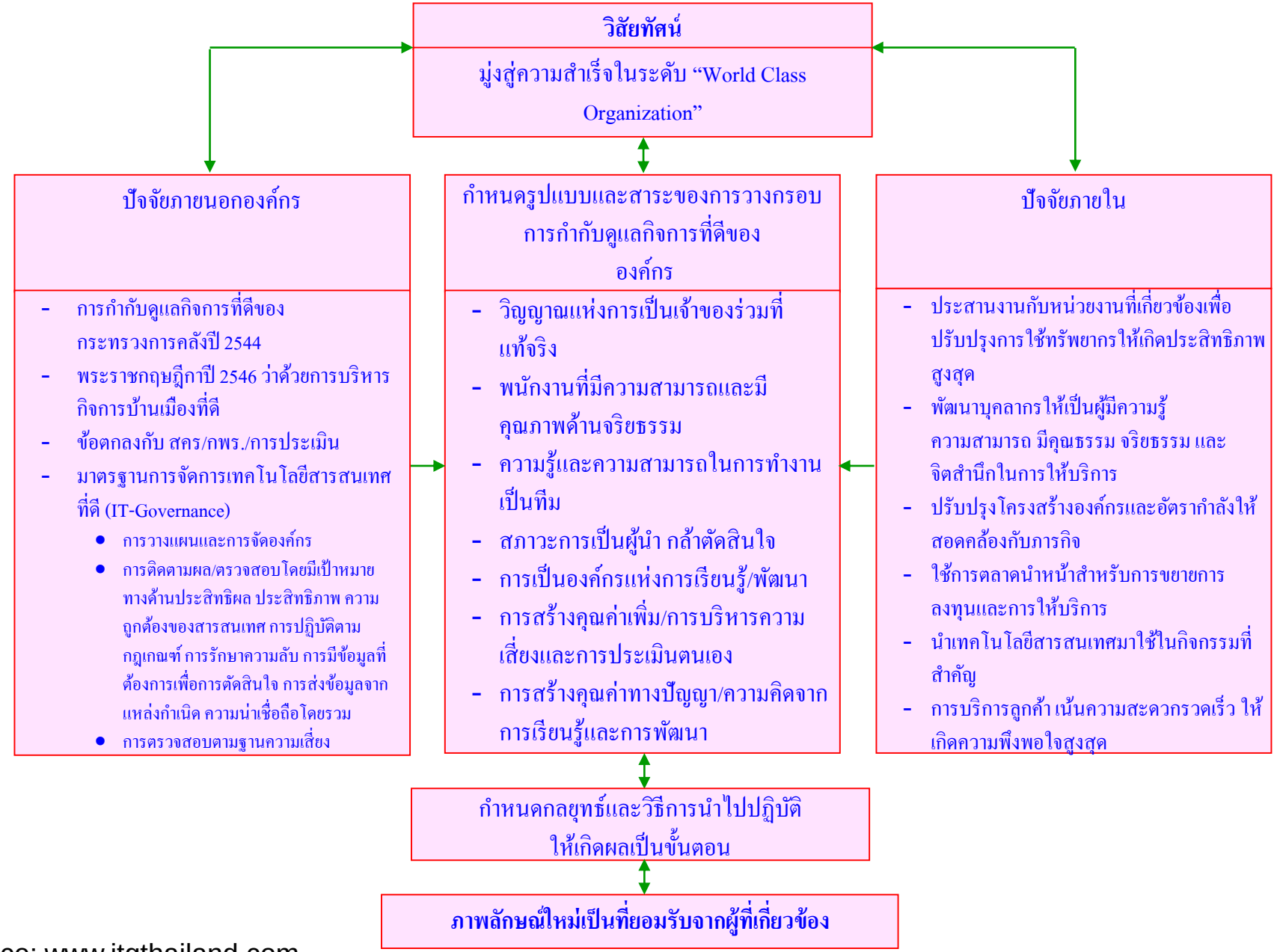



Source: www.itgthailand.com

# สภาพแวดล้อมของการกำกับดูแลกิจการที่ดีของ องค์กร



# องค์รวมของการกำกับดูแลกิจการที่ดีของ องค์กร




Source: www.itgthailand.com

# โครงสร้างกระบวนการและแนวปฏิบัติเกี่ยวกับการบริหารและการจัดการที่ดีของ องค์กร

- คณะกรรมการ (บอร์ด)
- คณะกรรมการชุดต่าง ๆ
- ผู้บริหารระดับสูง

**สังคมโดยรวม**

- รัฐบาล
- ผู้ออกกฎหมาย
- ชุมชน/สื่อมวลชน
- องค์กรวิชาชีพ
- ผู้พิทักษ์กฎระหว่างประเทศ/ในประเทศ

**ผู้บริหารของ องค์กร**

- สร้างแนวทางการกำกับดูแลกิจการที่ดีและการบริหารความเสี่ยง ซึ่งเป็นการบริหารเชิงรุก
- ติดตามประเมินผลการปฏิบัติตามจริยธรรมและการประเมินตนเอง
- กำหนดวิสัยทัศน์เชิงกลยุทธ์
- ตัดสินใจเรื่องที่มีนัยสำคัญ
- กำกับดูแลจากระดับสูงและกำกับระดับหน่วยงาน
- การบริหารการเปลี่ยนแปลง
- สร้างสภาวะการนำ – ผู้นำ

**ผู้มีผลประโยชน์ร่วม**

- ประชาชนในประเทศ
- พนักงาน
- ผู้ผลิต/ผู้ให้บริการ
- หน่วยงานที่เกี่ยวข้องและอื่น ๆ

**ผู้อำนวยการ**

- นำวิสัยทัศน์และกลยุทธ์มาแปลงเป็นแผนหลัก
- กำหนดทิศทางและมาตรการ/บริหาร/ควบคุม เพื่อให้บรรลุเป้าหมาย
- สั่งการ/ควบคุมการปฏิบัติงานของฝ่ายจัดการ
- ให้คุณให้โทษตามหลักเกณฑ์ ระเบียบ ตามคุณค่างาน
- สร้างสภาวะและบรรยากาศในการพัฒนาต่อเนื่อง

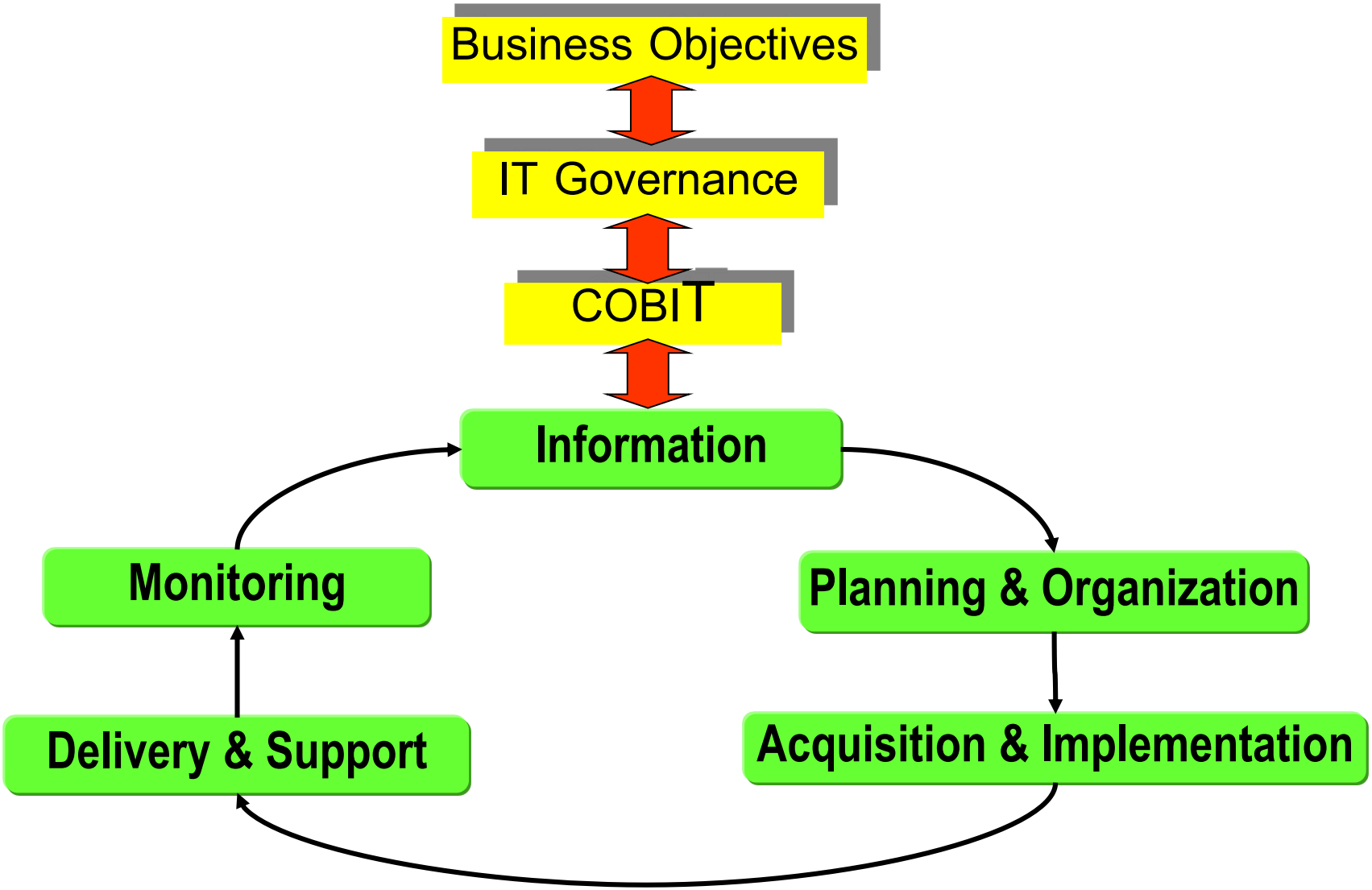
**ผู้บริหาร**

- นำเอาแผนงานหลักมากำหนดแผนปฏิบัติการ
- บริหารให้เกิดประสิทธิภาพและประสิทธิผลในระดับปฏิบัติการตามมิติทั้ง 4
- ควบคุมและสอบทานการบริหารความเสี่ยง
- สร้างความเป็นผู้นำและบริหารการเปลี่ยนแปลง
- จัดให้มีการประเมินตนเองเพื่อการบริหารที่ดี

- งานปฏิบัติการ
- งานสนับสนุน
- การประเมินผลการปฏิบัติงาน
- การพิจารณาระบบผลตอบแทน

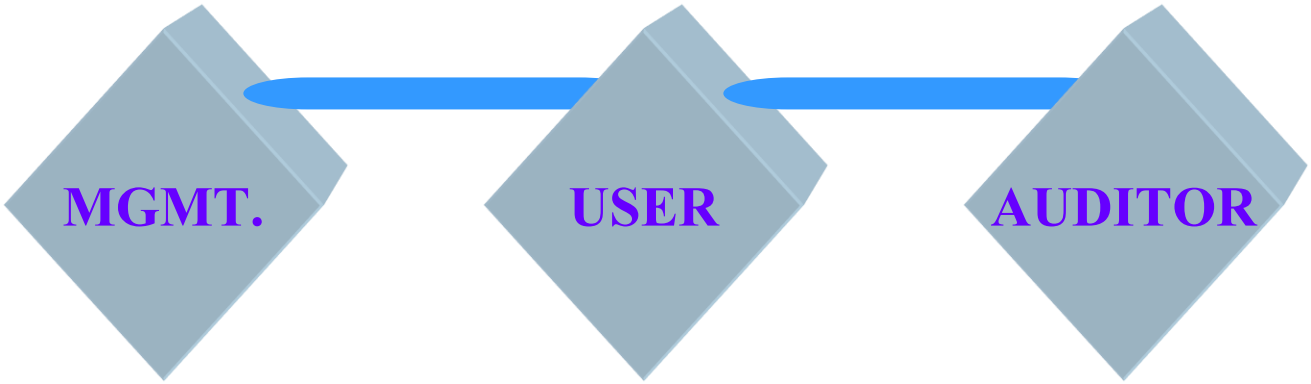
Source: www.itgthailand.com

# IT Governance กับการกำกับดูแลกิจการที่ดี




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

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

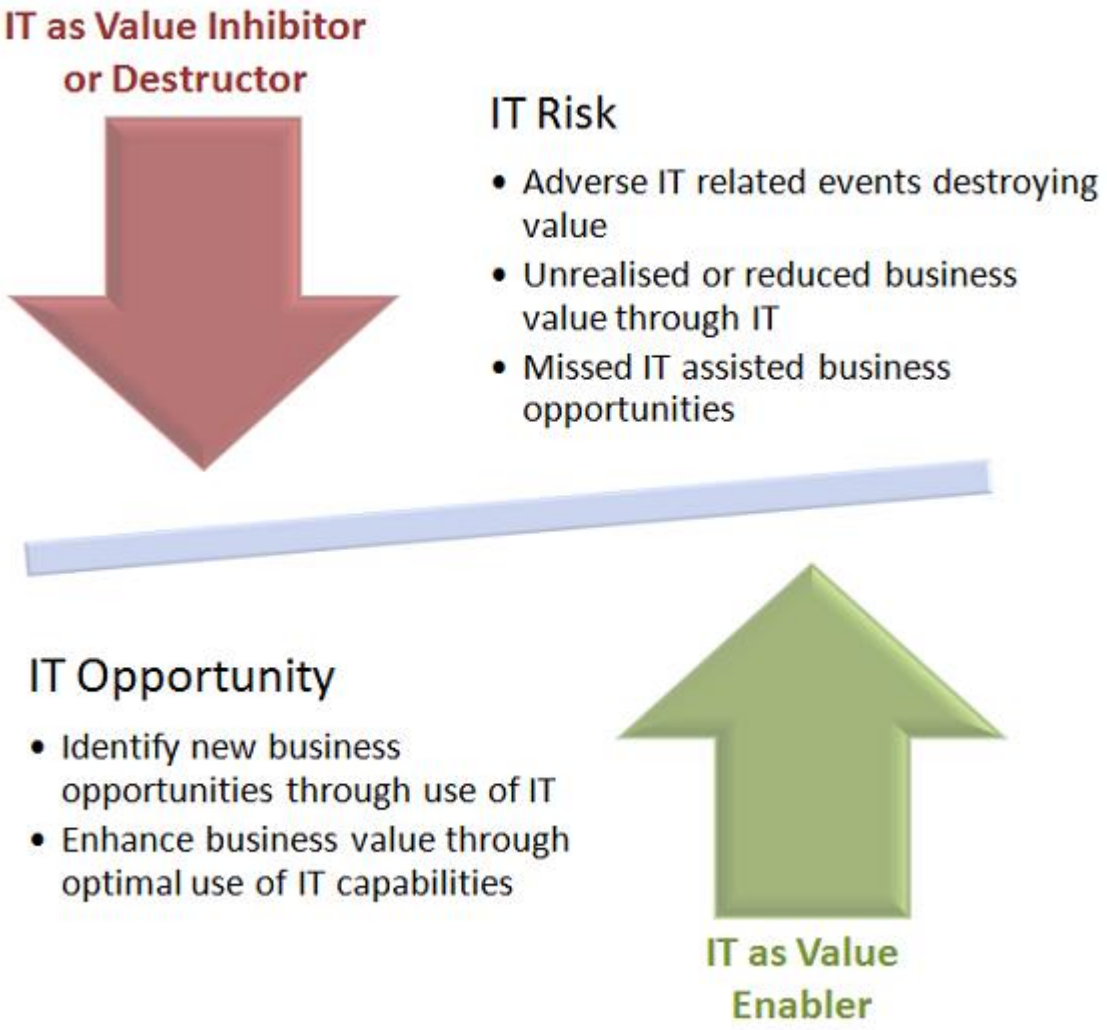



- IT investment decisions
- Balance risk and control investment
- Benchmark existing and future IT environment

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

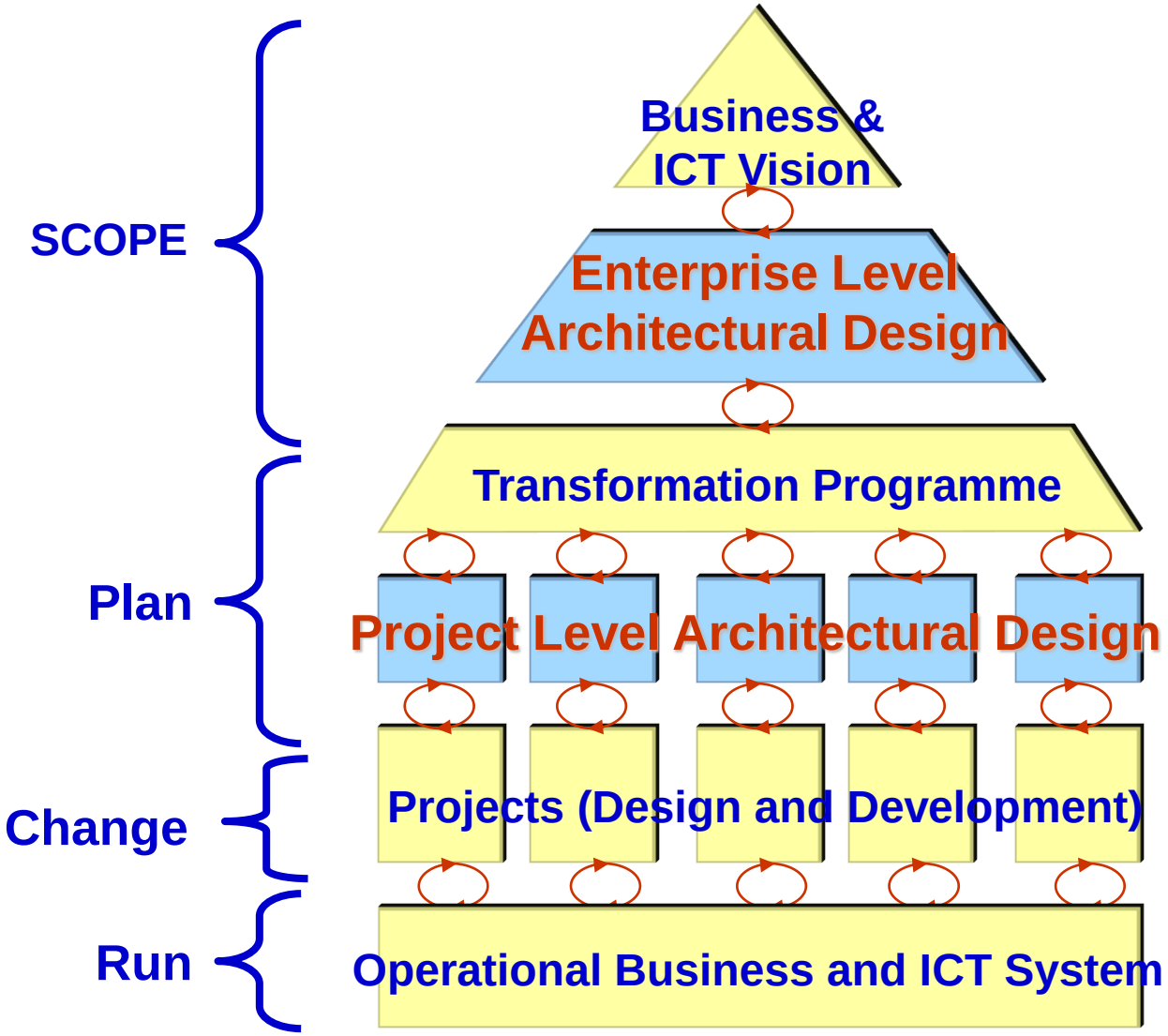
- Substantiate opinions to management on internal controls
- Advise on what minimum controls are necessary

# Risk and Opportunity for GRC -> COBIT5-> Value Creation



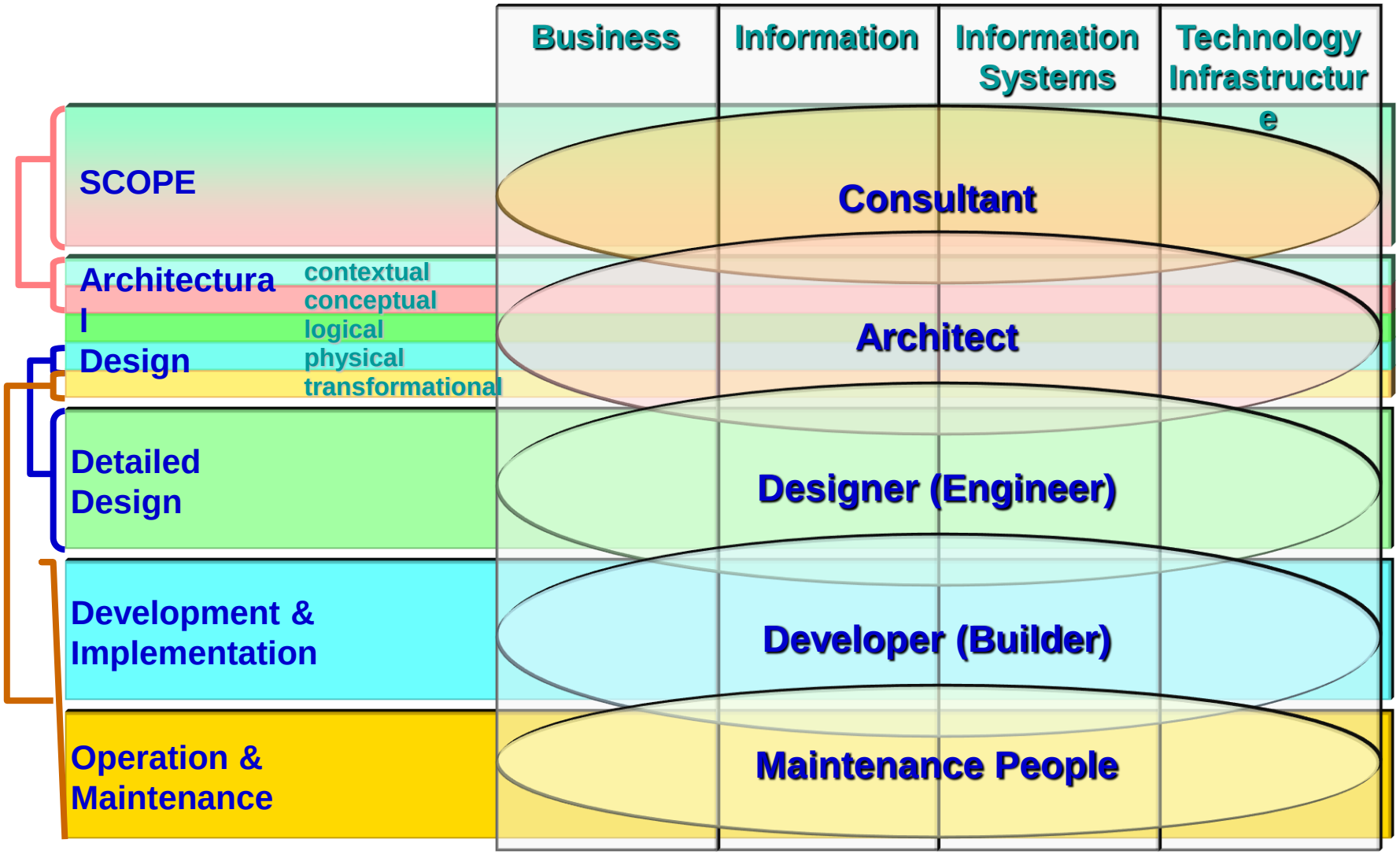

Source : ISACA, Risk IT Framework

# Role of IAF in Business and ICT Transformation



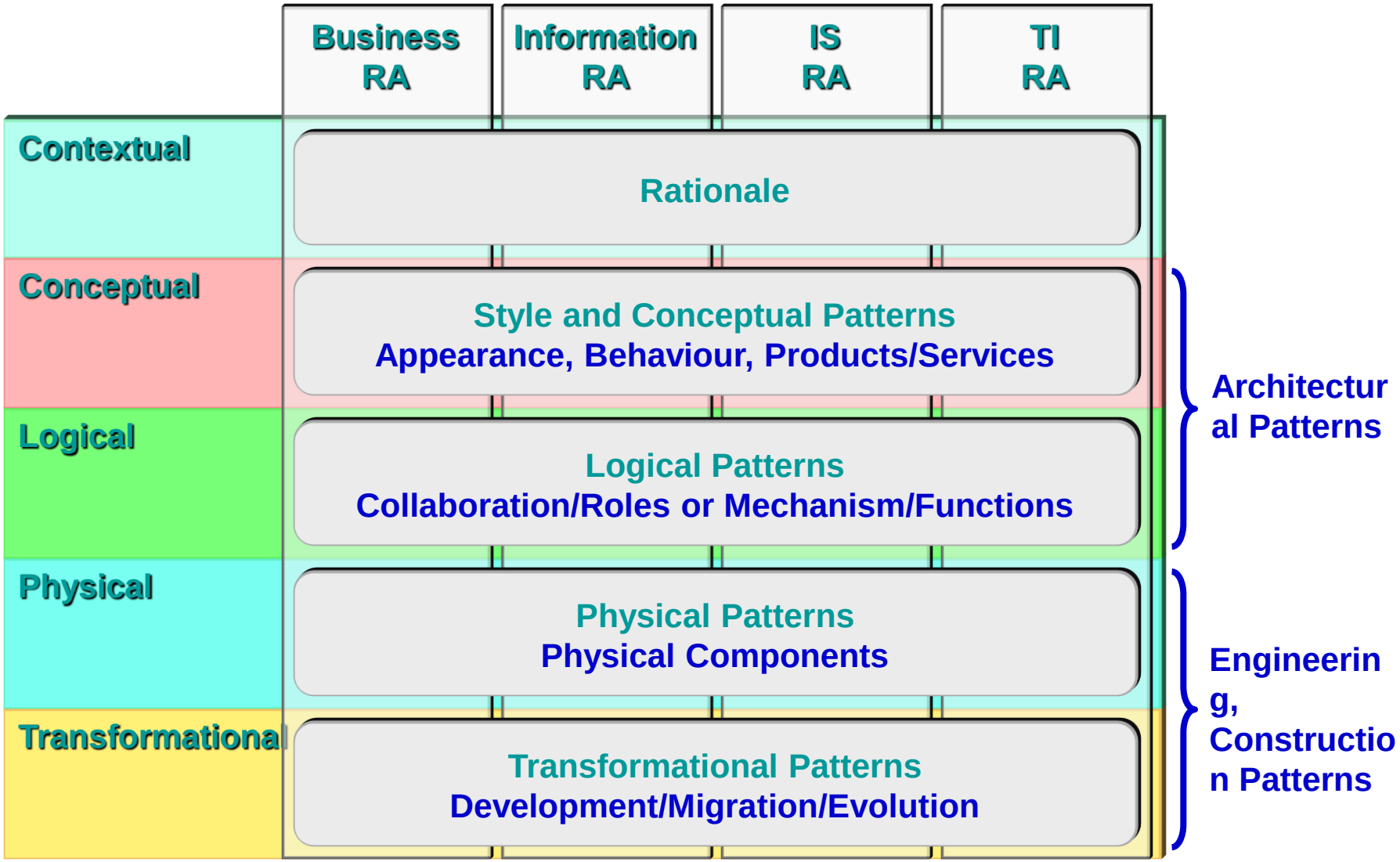

Adopt and Adapt from IAF

# IAF and Professional Roles- ICT Risk



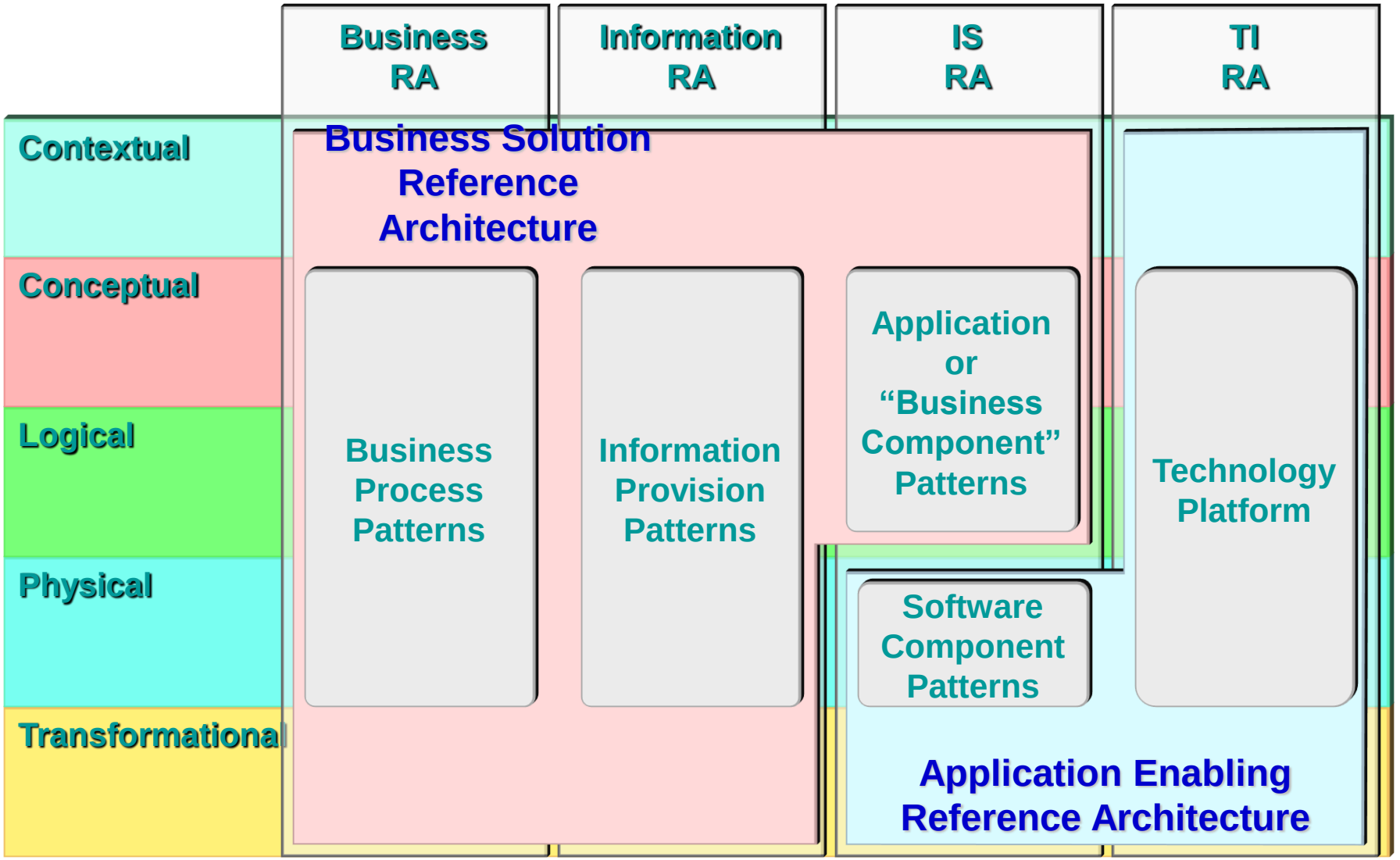

Adopt and Adapt from IAF

# Reference Architectures in IAF (1)



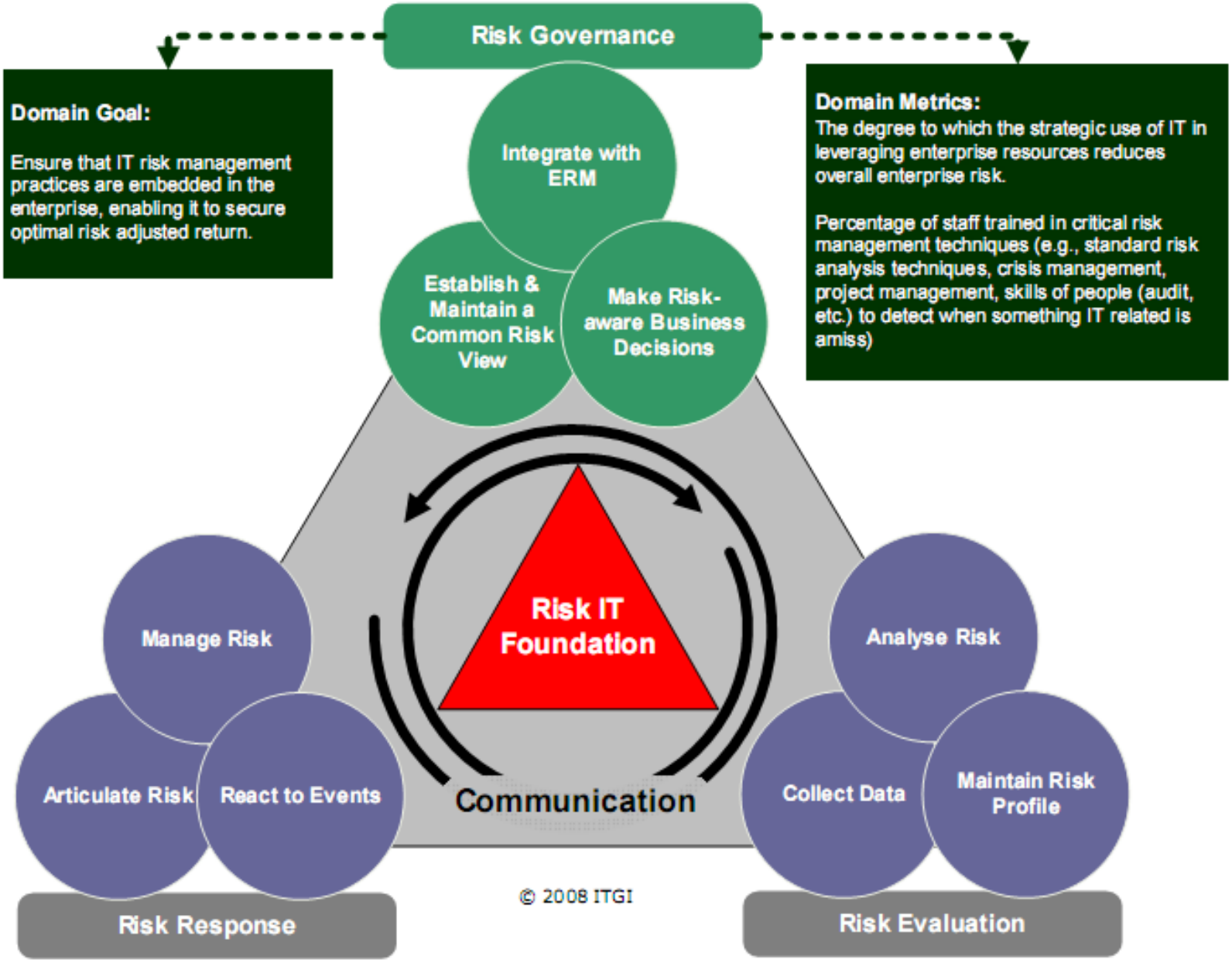

Adopt and Adapt from IAF

# Reference Architectures in IAF (2)




Adopt and Adapt from IAF

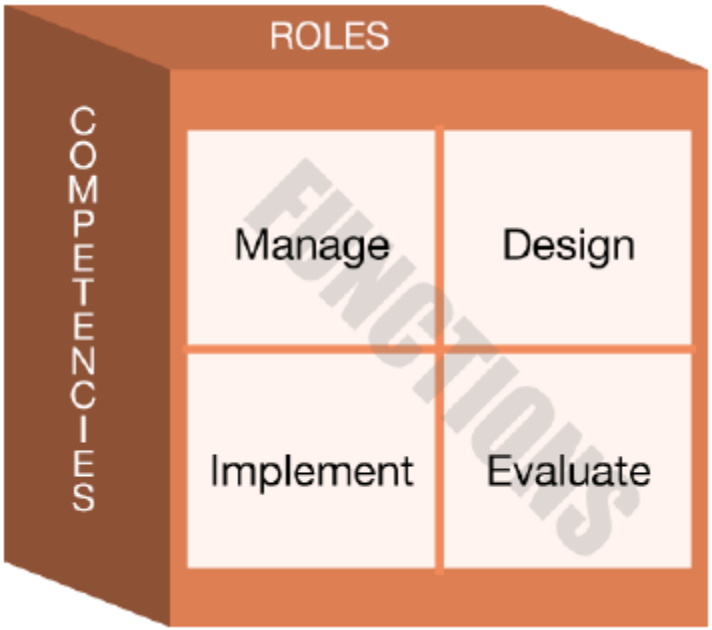
# Risk Governance Domain for Value Creation




Source : ISACA, Risk IT Framework

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

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




Source: EBK-Essential Body of Knowledge

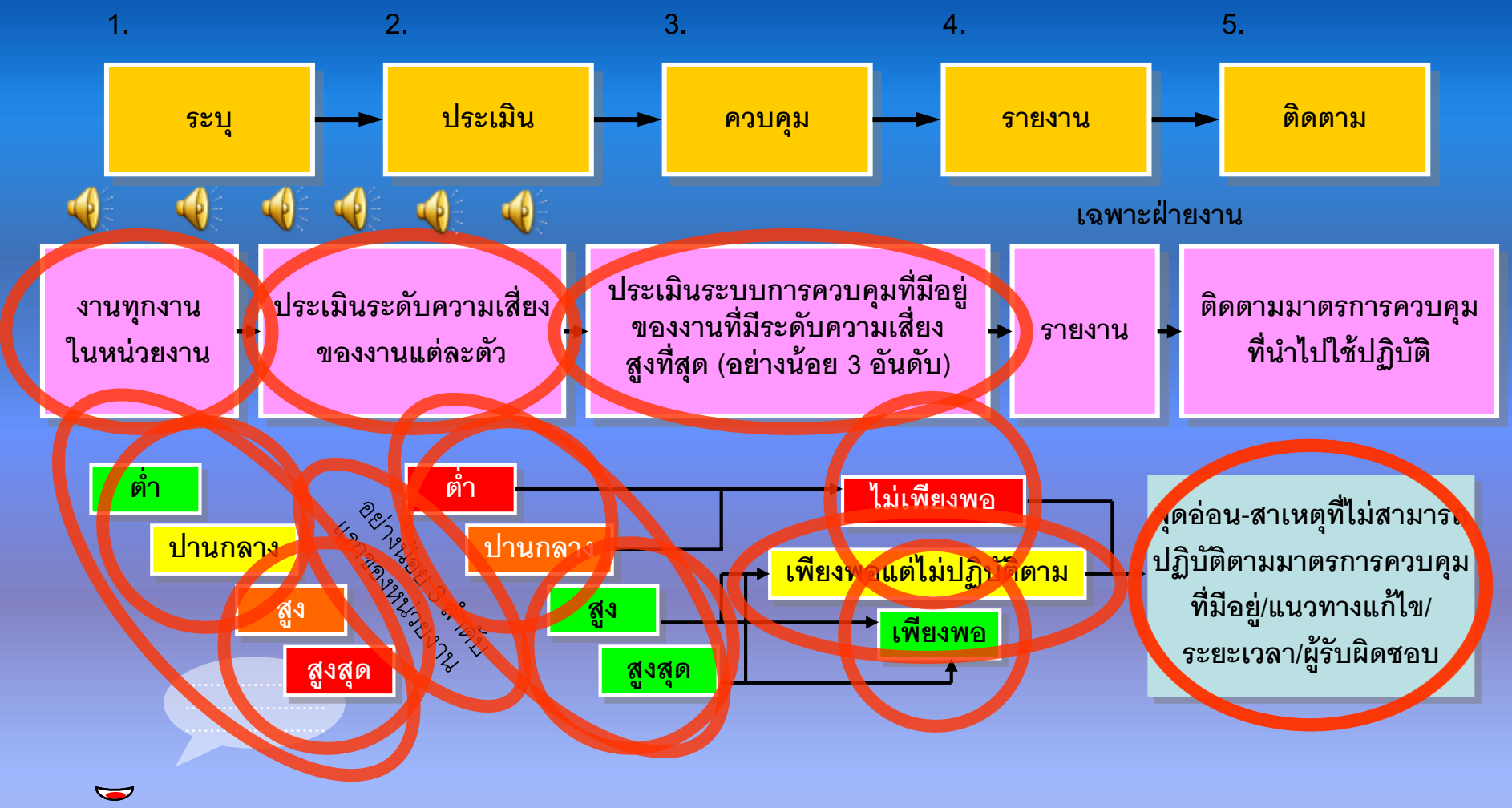
# Competency Areas *(MDIE in each)*

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

# สรุป ขั้นตอนปฏิบัติของการประเมินการควบคุมความเสี่ยงด้วยตนเอง- CSA

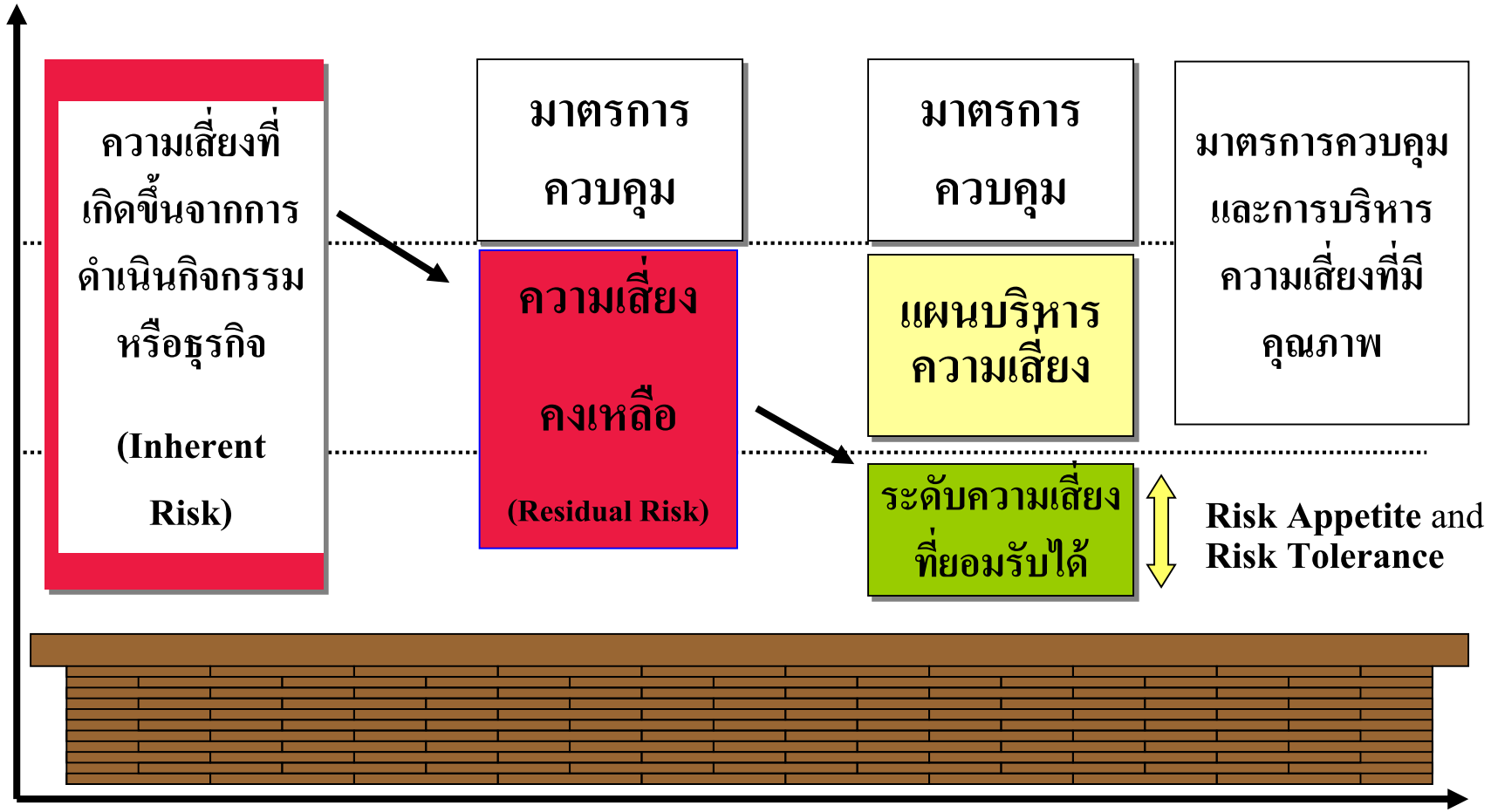
(Operational Risk Self Assessment : ORSA) – มุมมองของ Business Risk & IT-Related Risk



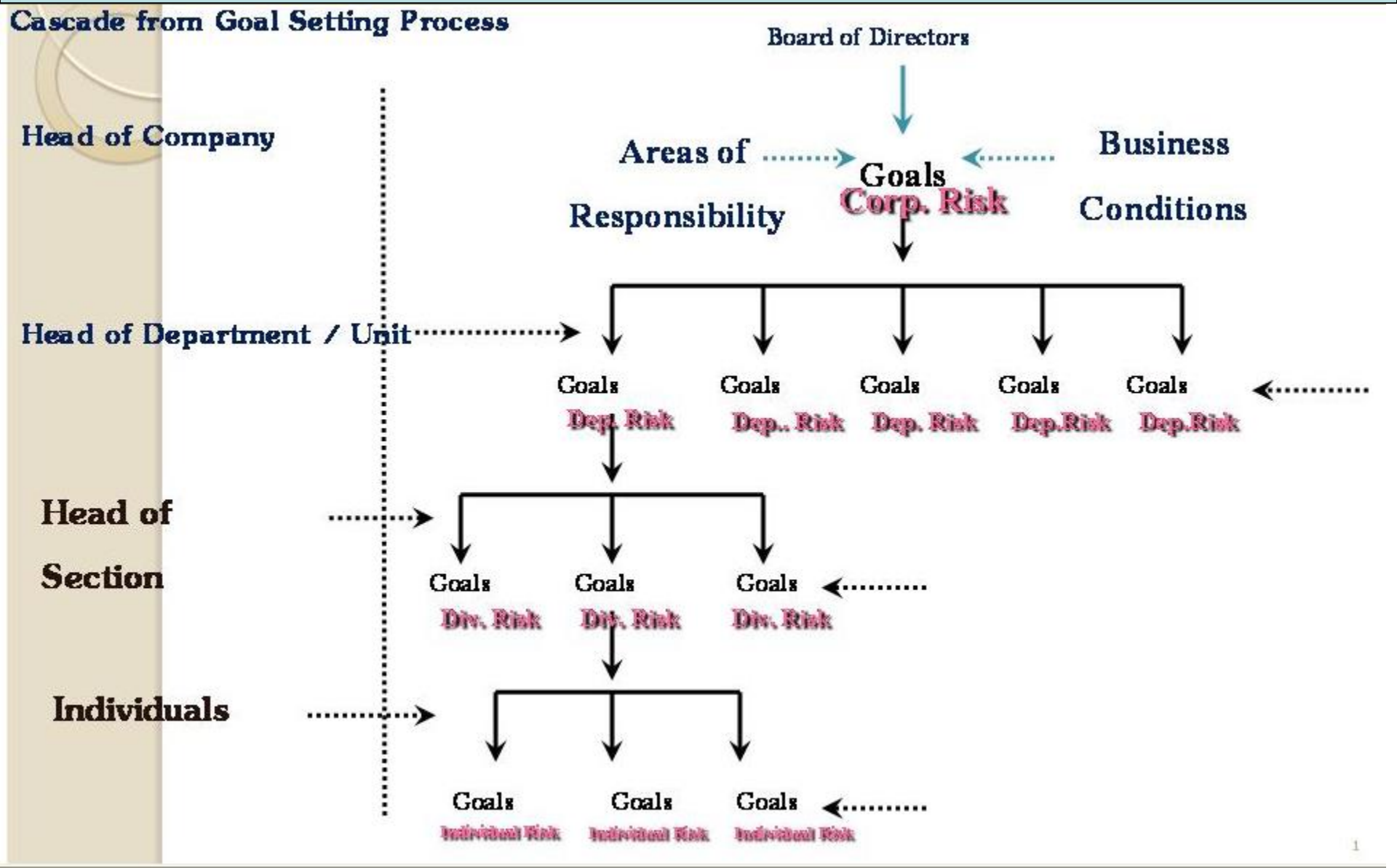

สรุป : ความเข้าใจ การ บริหารความเสี่ยง เบื้องต้น ทางด้าน Business Risk และ การบูรณาการกับ IT Risk

# ERM- Enterprise Risk Management

## การประเมินความเสี่ยง (Risk Assessment)

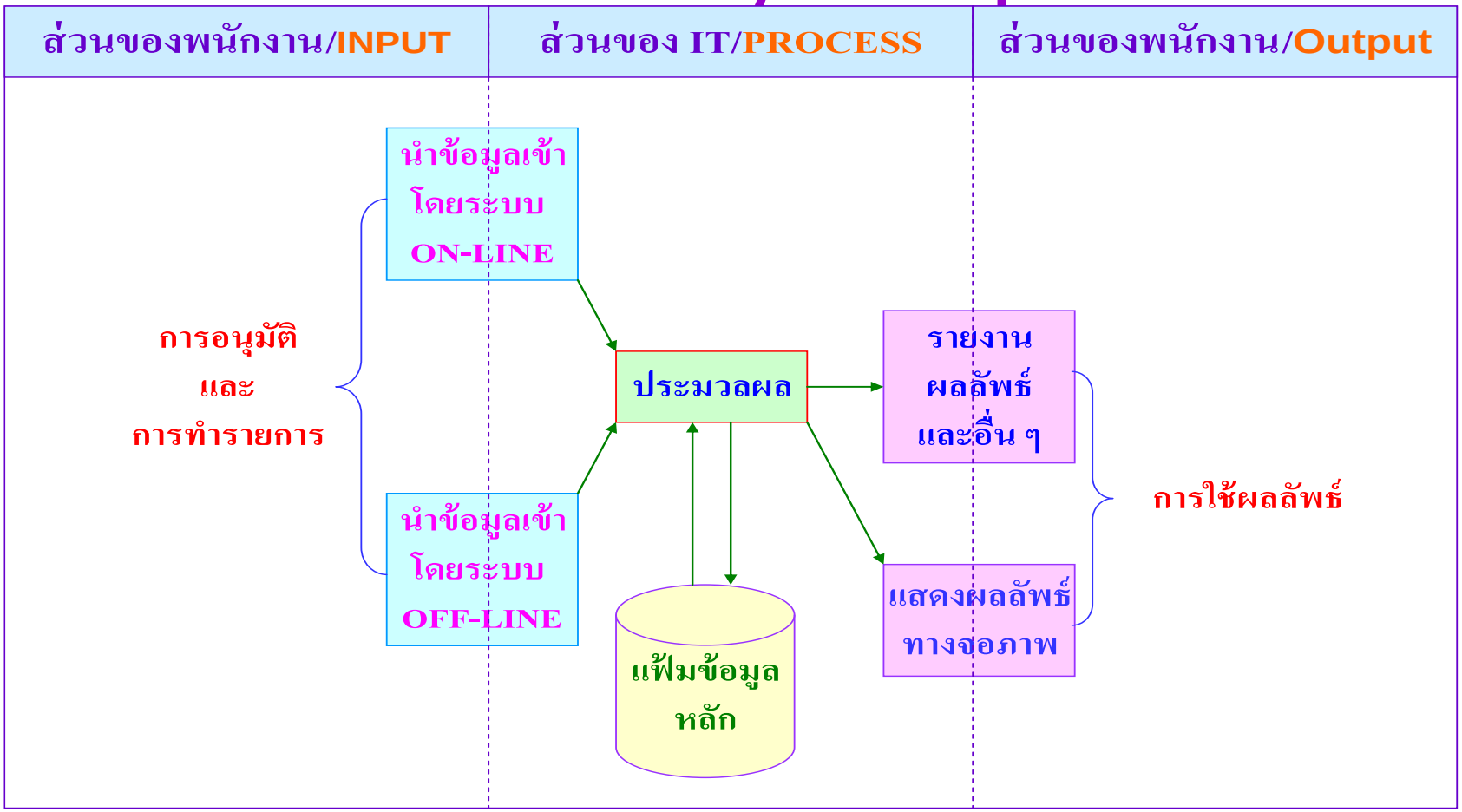


# การแตกเป้าหมายหลักขององค์กร ลงมาสู่สายการปฏิบัติงาน เพื่อการบริหารความเสี่ยงทั่วทั้งองค์กร- Integrated Risk Mgmt.

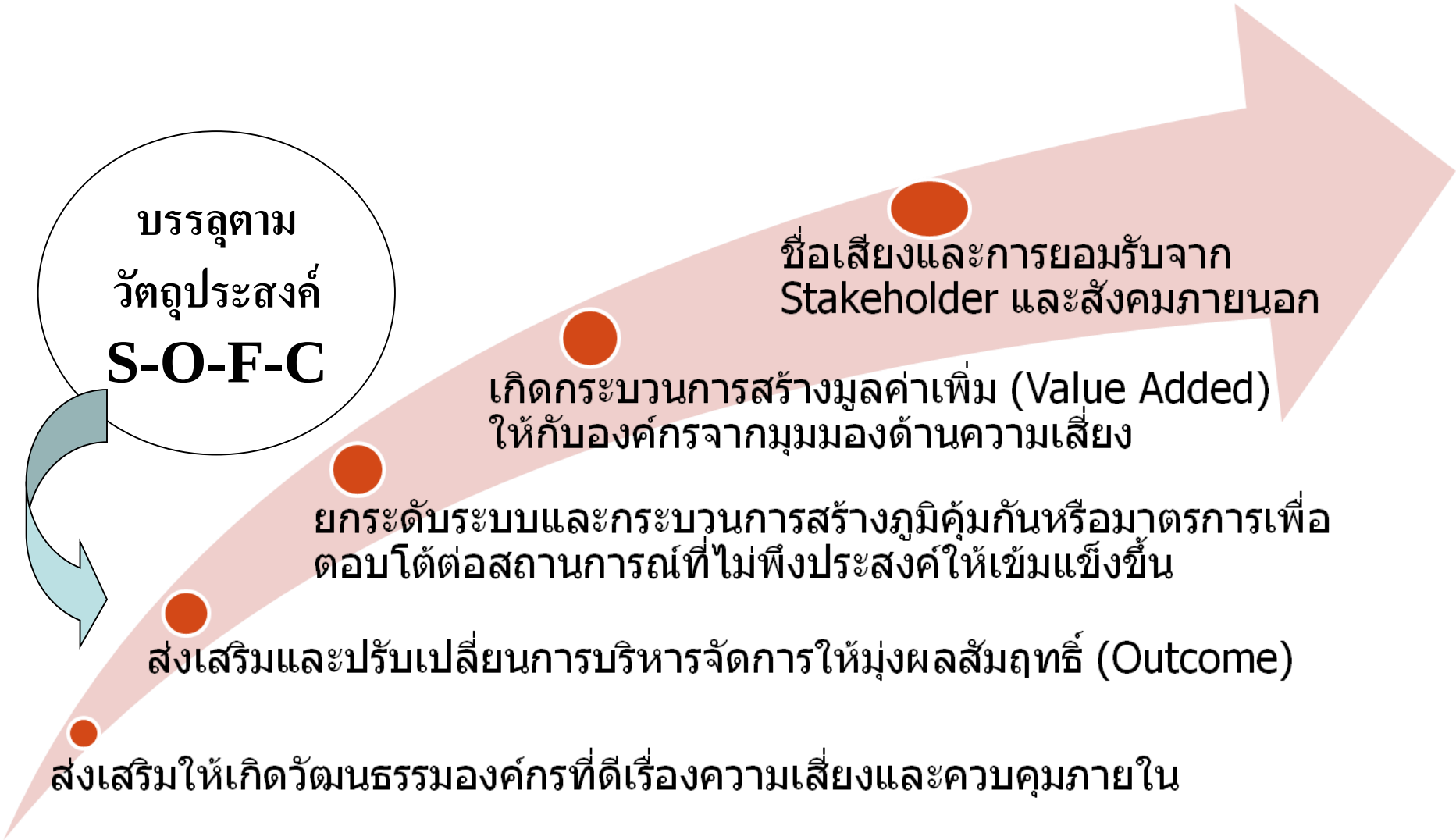


# GRC : Value Creation for Effectiveness & Efficiency of Operations

ส่วนของคอมพิวเตอร์ในระบบงานต่าง ๆ ของทุกองค์กร กับความเสี่ยง

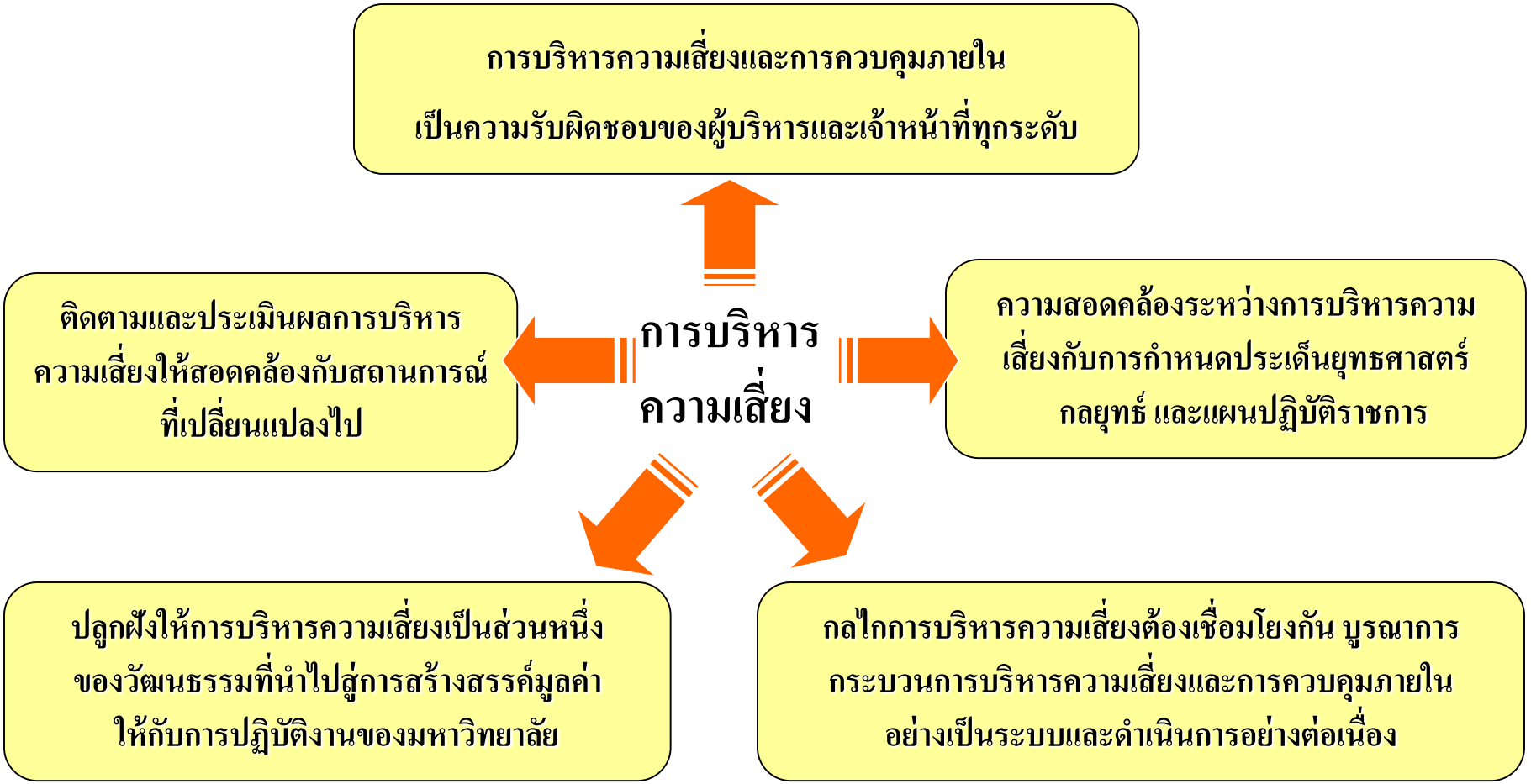


# ผลลัพธ์ที่ได้จากการบริหารความเสี่ยง



ERM is a core of GRC…Understanding is very necessary

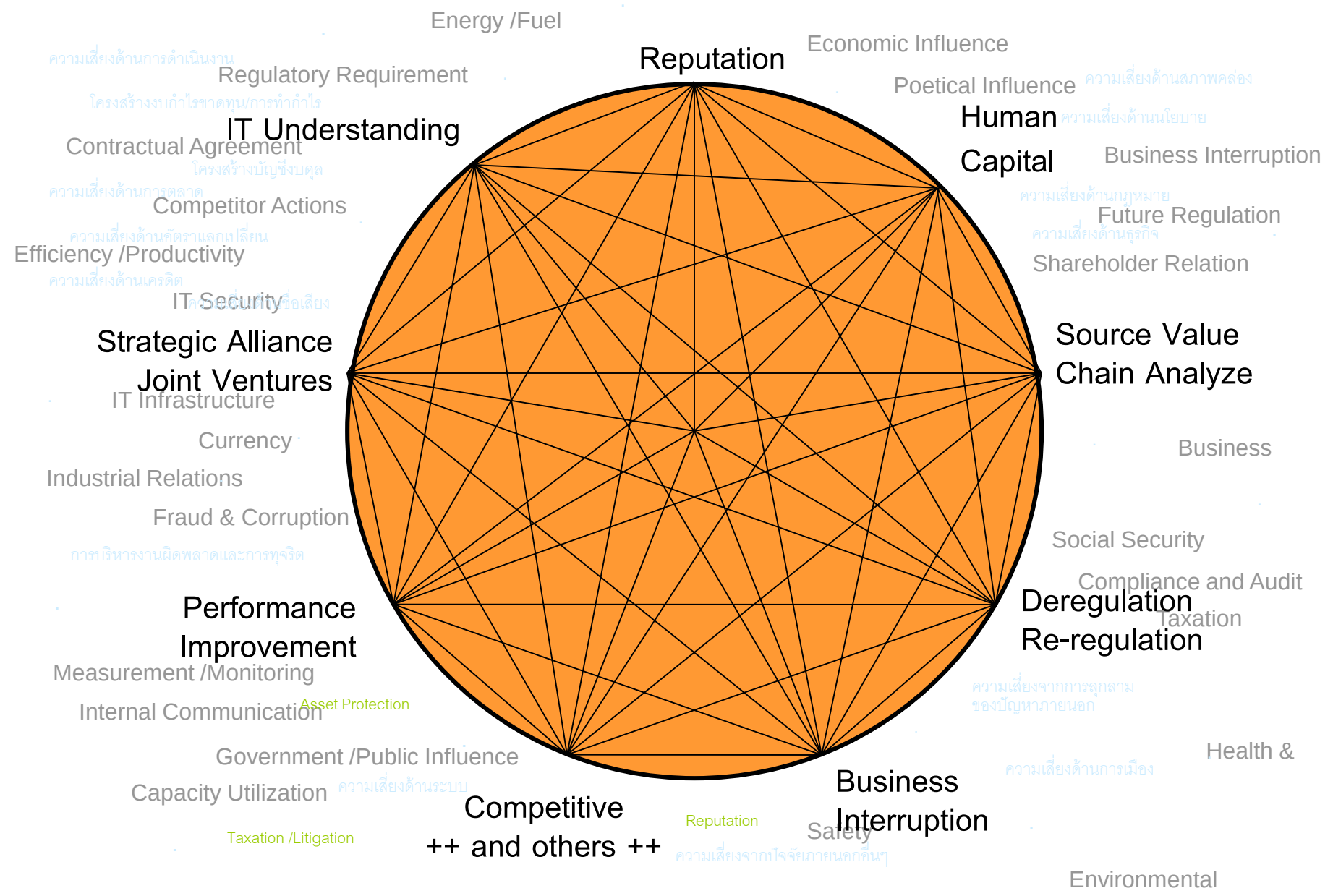
# นโยบายการบริหารความเสี่ยง



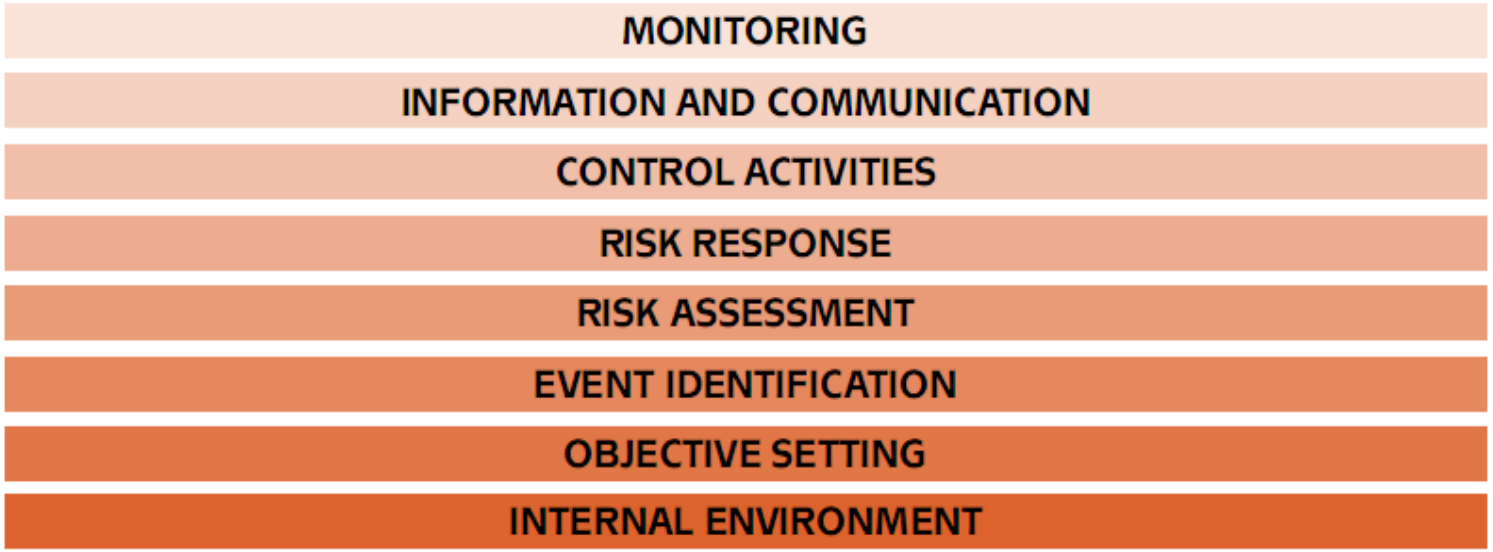
# กรอบการประเมินผลการปฏิบัติราชการ

| 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 |

# ผลกระทบต่อเนื่องของความเสี่ยงประเภทต่างๆ บางมุมมองขององค์กร



# 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**

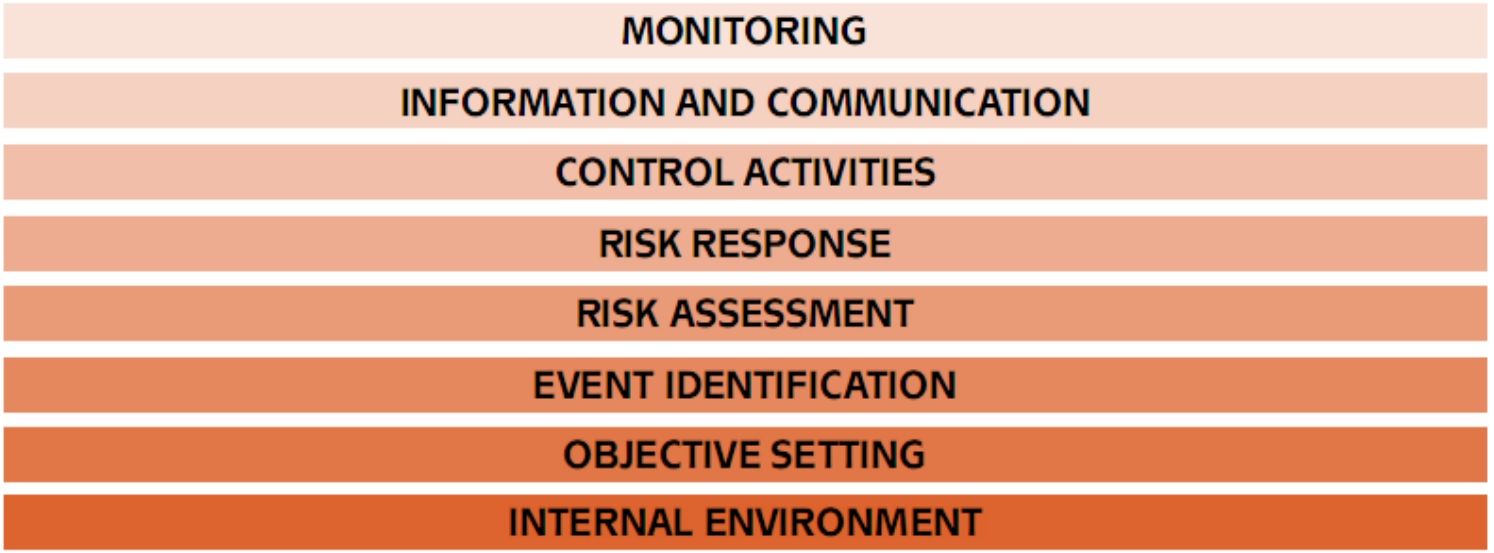
- Periodic messages from senior management that change control is important.
- Service desk issues communicated for resolution and trend analysis.
- Changes in policy communicated to all affected personnel.
- Regular communication of upcoming changes.

**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

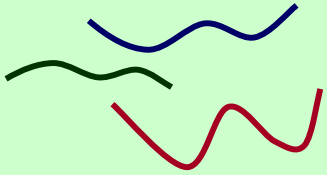
Source : GTAG

# ความเข้มแข็งในการบริหารองค์กรและประเทศแบบบูรณาการ&ICT Risk

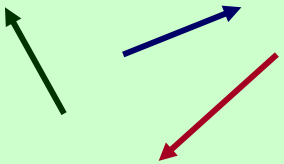
IT-Based & Understanding

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

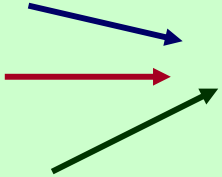
**1** ไม่มีระบบใดเลย
(ขาดความเข้าใจในการบริหารเชิงกลยุทธ์อย่างสิ้นเชิง)



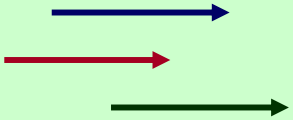
**2** แก้ปัญหาเฉพาะหน้า
(เป็นเรื่อง ๆ เป็นกลุ่ม ๆ)

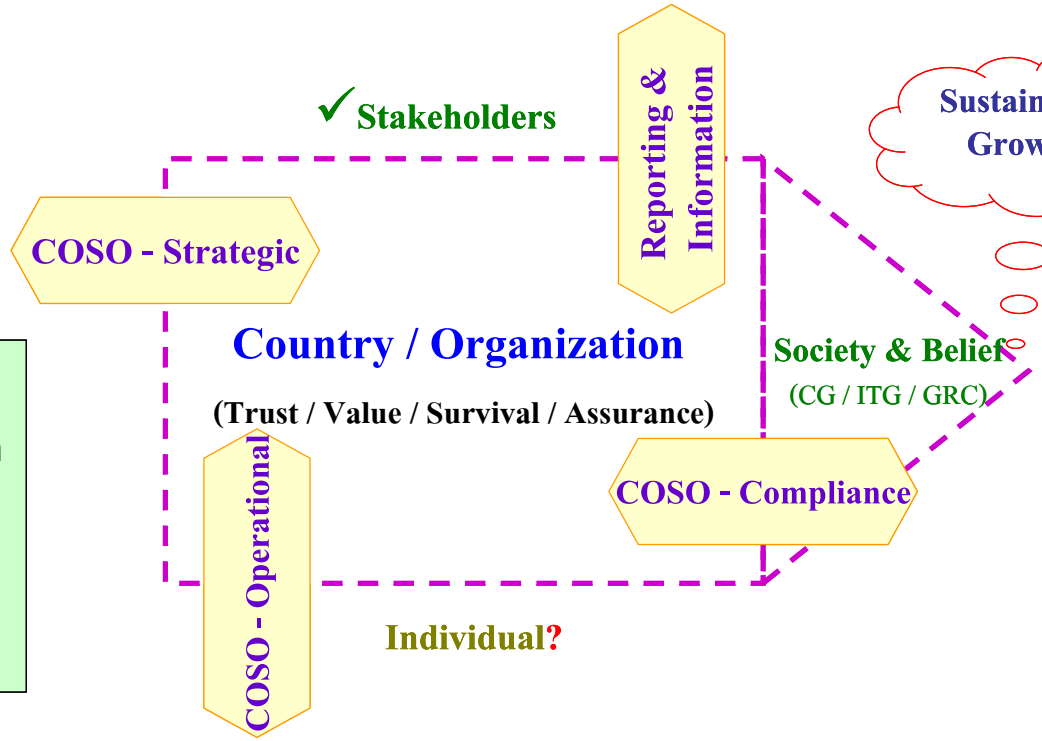


**3** แนวทางเริ่มเป็นระบบ
(เริ่มต้นจากรัฐบาลและองค์กร)

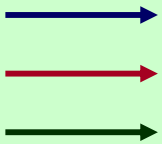


**4** มุ่งเป็นทิศทางเดียวกัน
(โดยกระบวนการเรียนรู้)

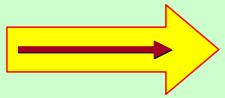




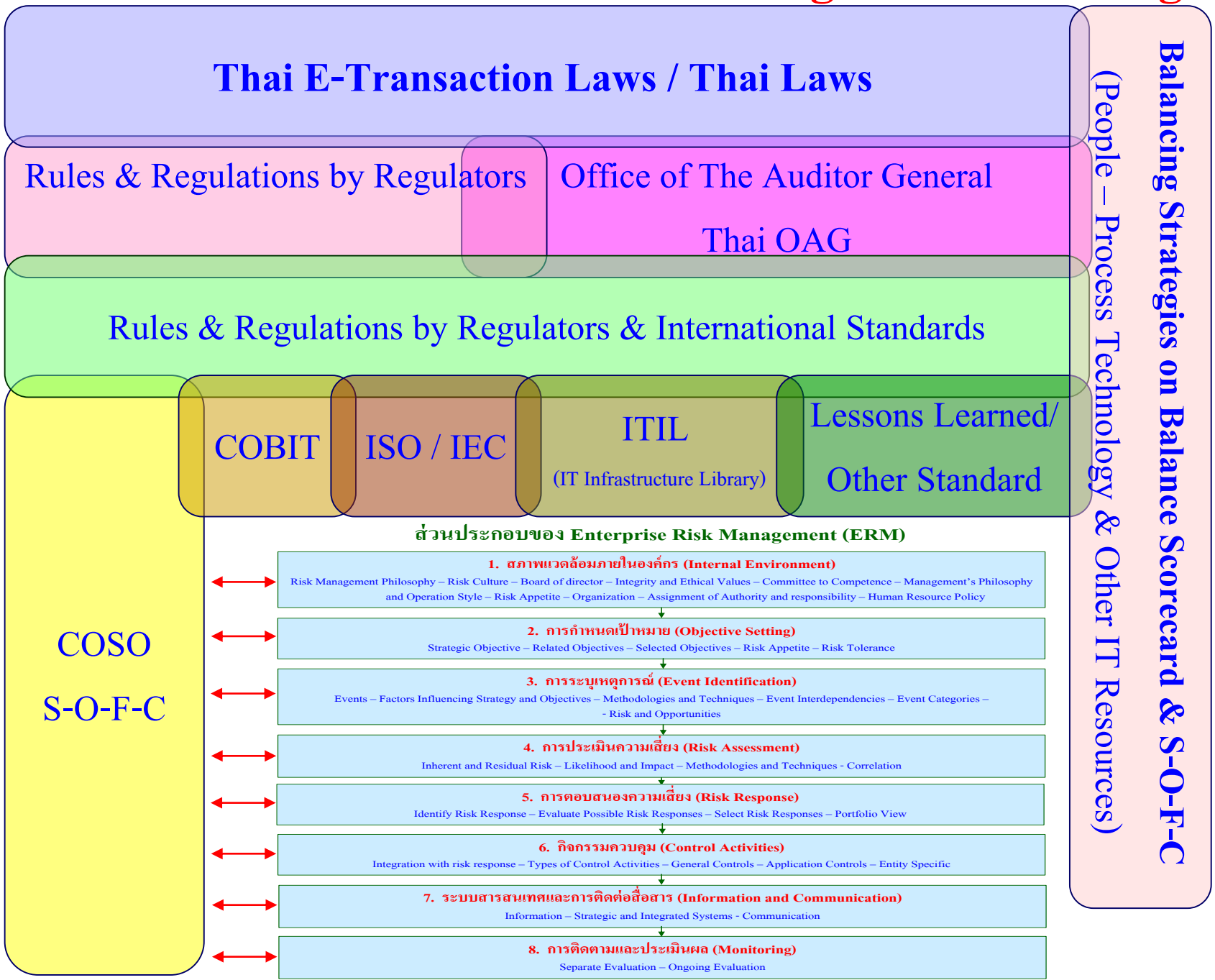

**5** แนวทางบูรณาการ
(สร้างความเชื่อมั่นของ Stakeholder)



**6** บูรณาการเป็นหนึ่งเดียว
(เพื่อการเติบโตอย่างยั่งยืนของประเทศชาติ)

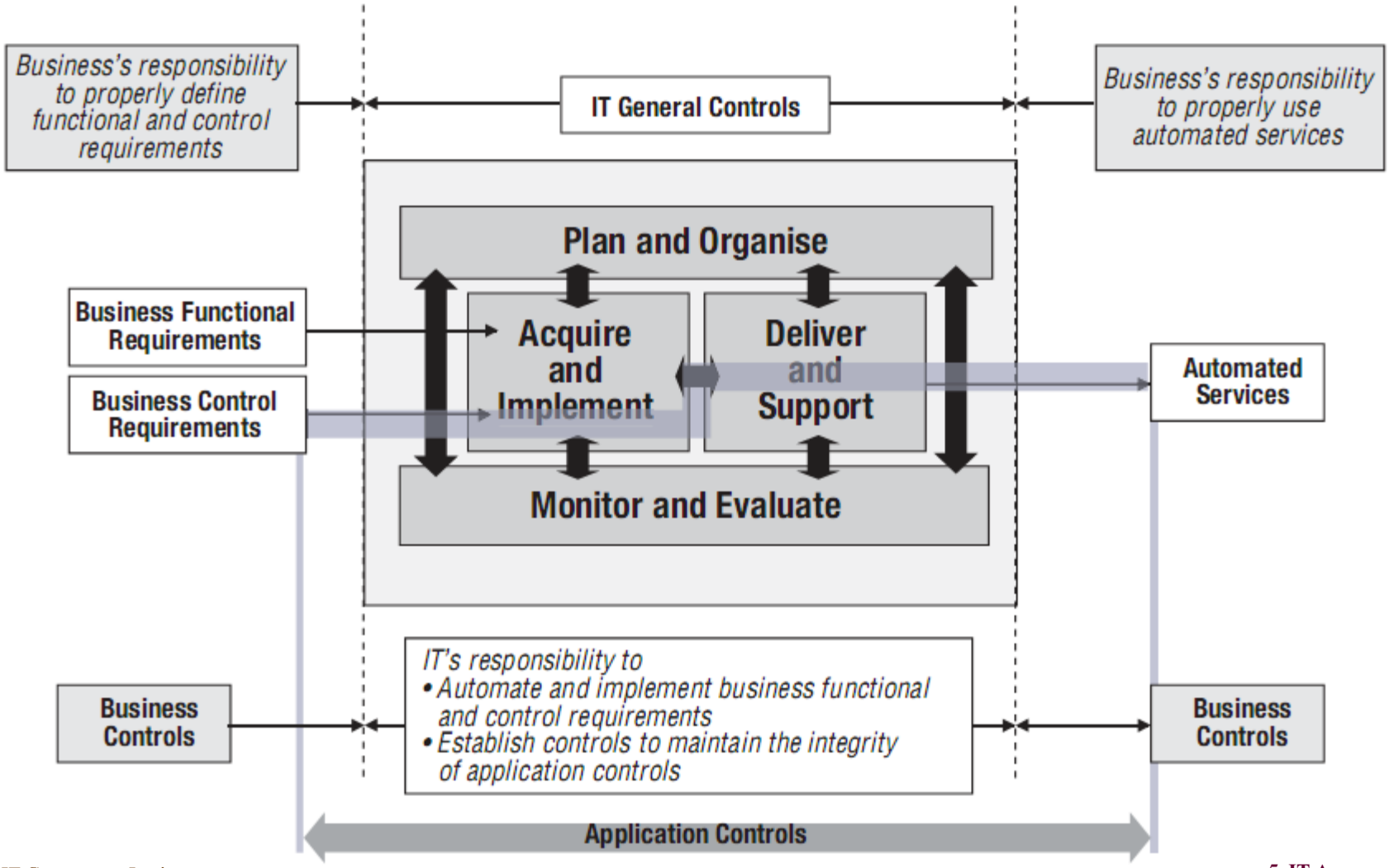


# CG/ITG & GRC Framework + Convergence Risk & Mgmt.



# IT Risk and Application Controls - COBIT-> GRC->>> COBIT5 / GEIT

## IT General Controls and Application Controls




Source : IT Governance Institute

# 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

# ICT Risk & Development of Management to Integrated Management

Evolution of Scope

CG – Corporate Governance

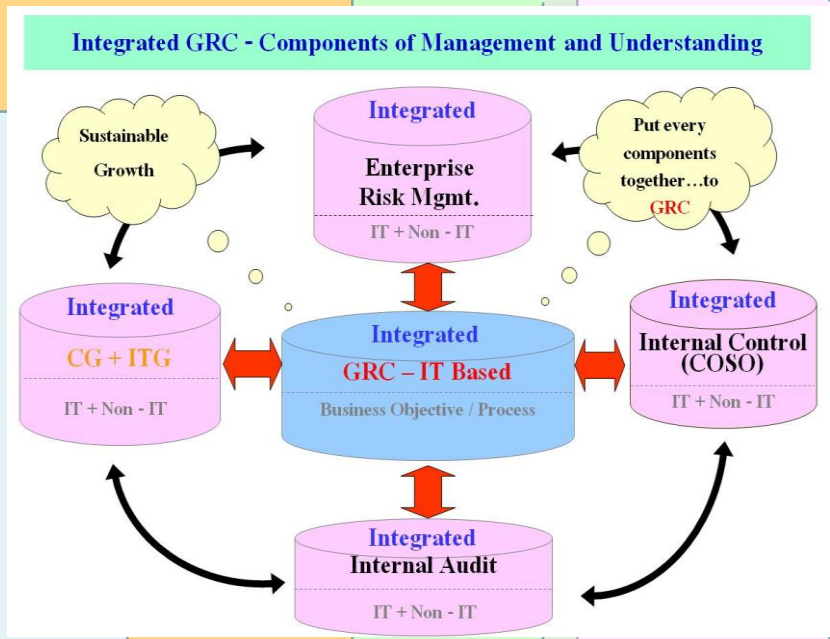
GEIT / Governance of Enterprise IT

IT Governance

Management

Control

Audit

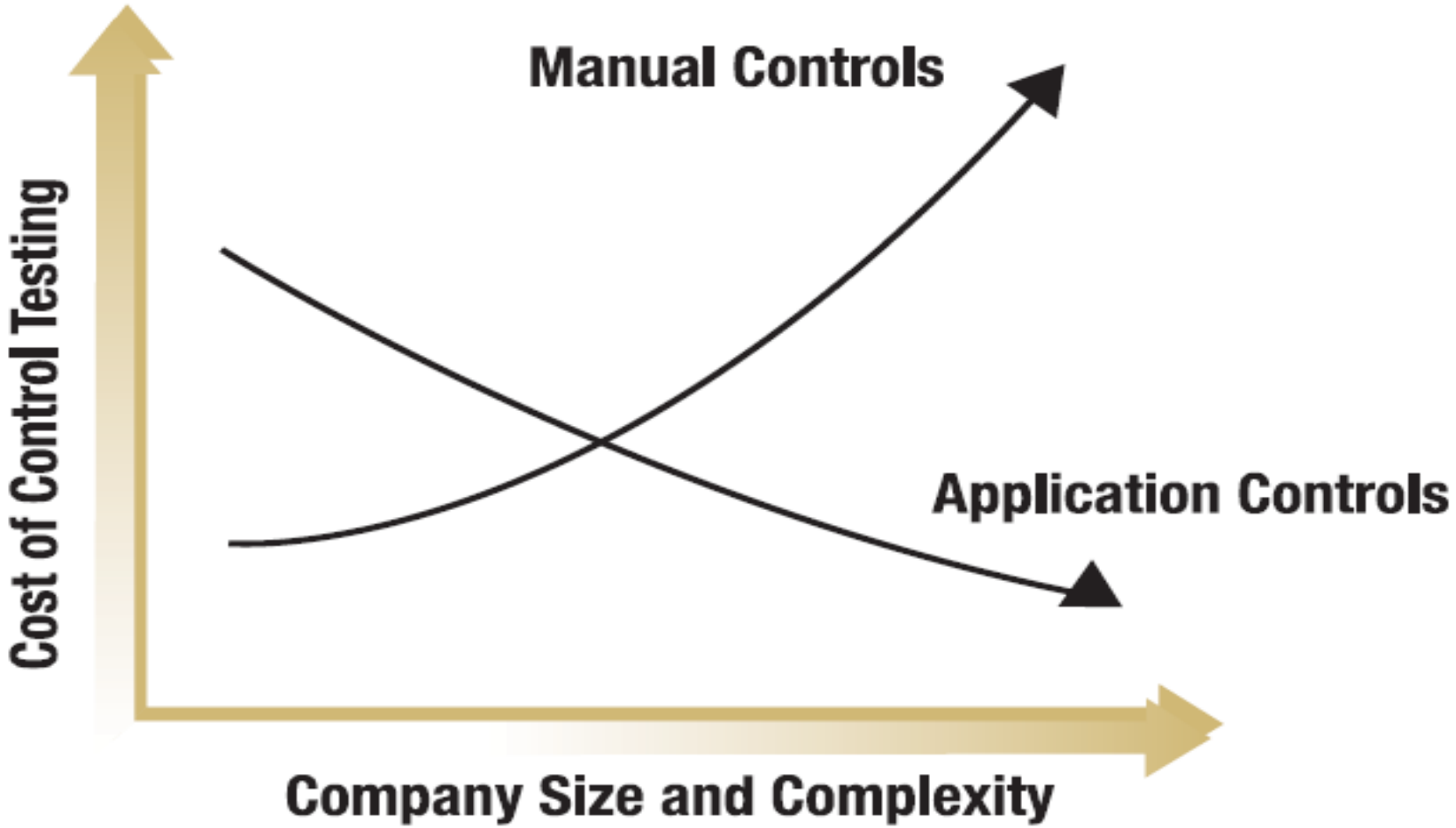



Source : www.itgthailand.com

# Application Controls

## The Business Case for Application Controls

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



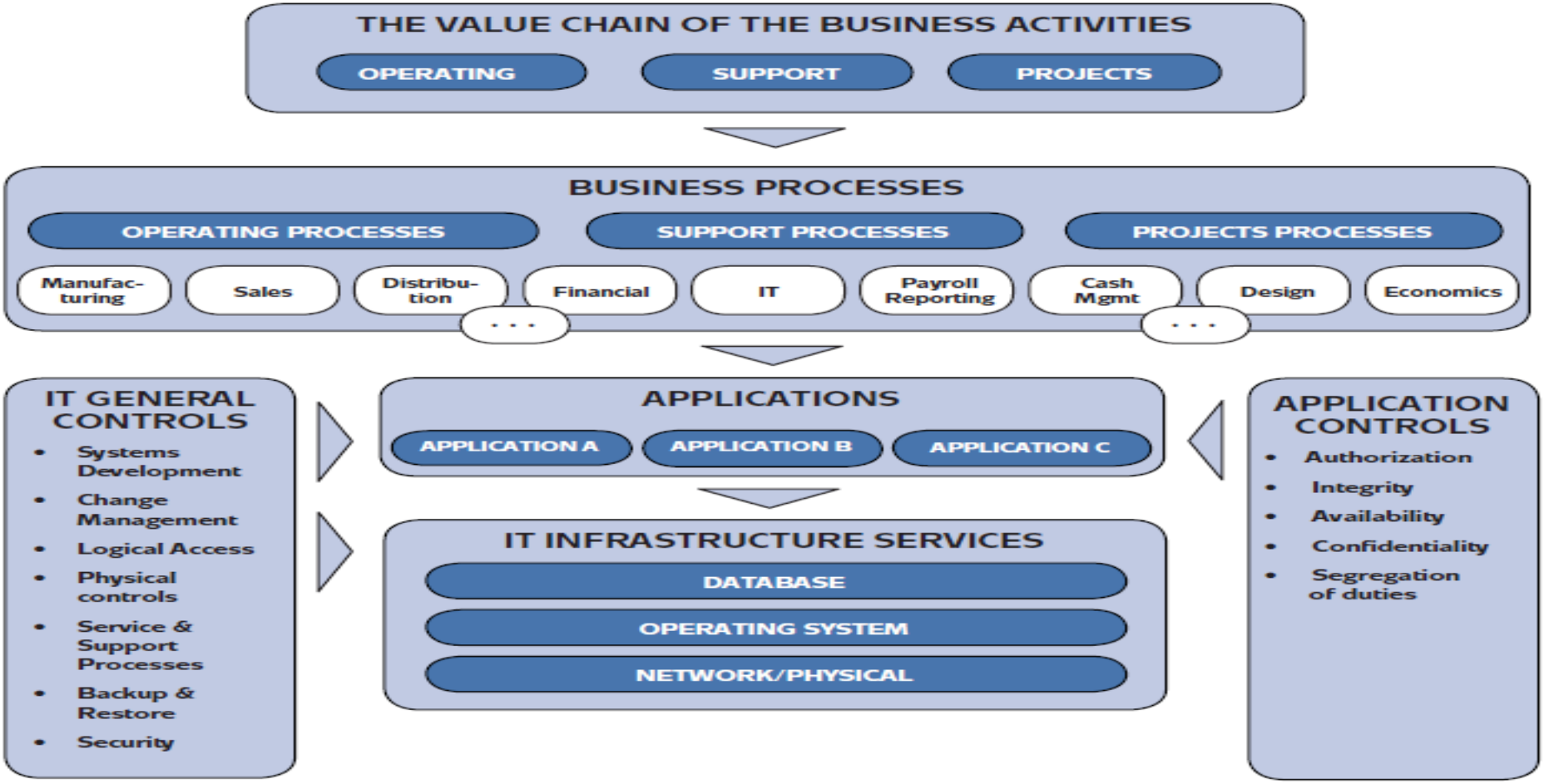

Source : IT Governance Institute

# GRC & Developing the IT Audit Plan

## Understanding the Business & Risk IT + IT Risk

### IT Environment Factors & Management

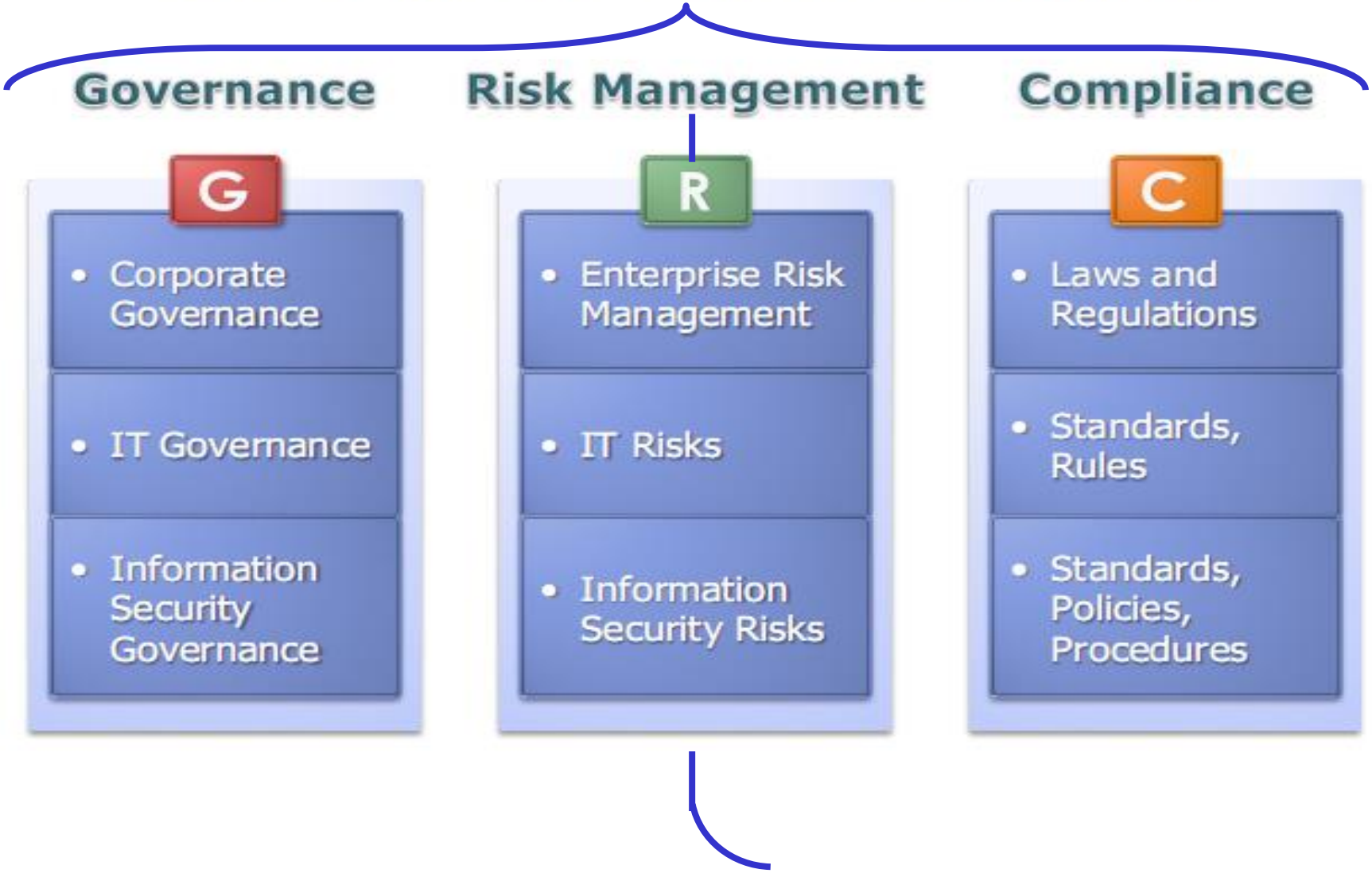
**Understanding the IT environment in a business context**




Source: The Institute of Internal Auditors

# GRC & SINGLE UMBRELLA MANGEMENT & AUDIT

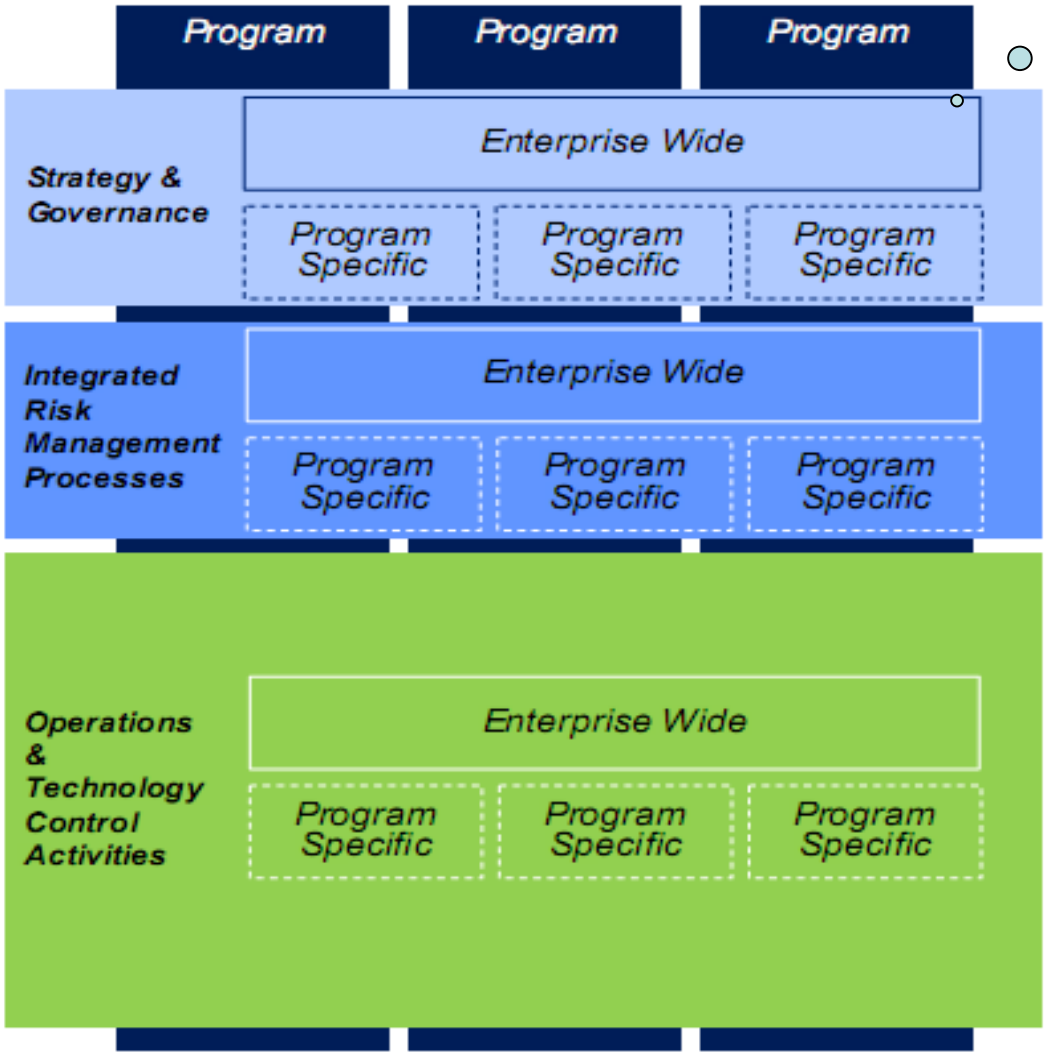
RBIA – Integrated Audit



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

CSA & GRC

## Re-engineered GRC Framework




**GRC**

**CORPORATE RISK STRATEGY**

*Establishes Governance & Enterprise Risk Strategy*

**INTEGRATED RISK MANAGEMENT PROCESSES**

*Establishes Common Risk Management Processes, Common Data Architecture, and Common Technology Architecture*

**OPERATIONS**

*Establishes Controls for the Different Operational Processes*

| FINANCE | SECURITY | REGULATORY | HR | OTHER ••• | PRIVACY | CAP MARKETS | SUPPLY CHAIN |
|---|---|---|---|---|---|---|---|

APPLICATION

| DATABASE | OPERATING SYSTEM | NETWORK |
|---|---|---|

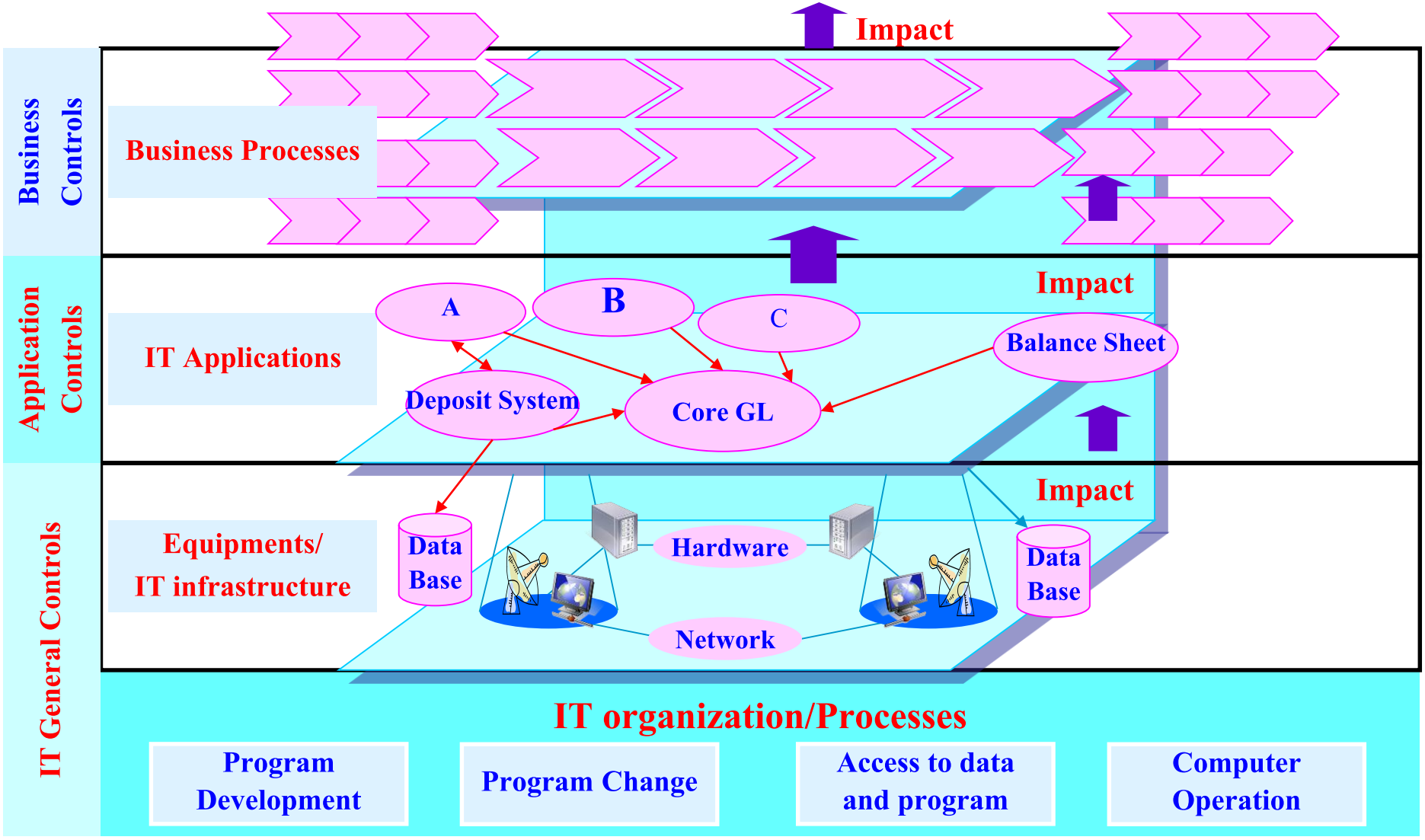
FACILITY

# Audit assurance for AC & C –Levels ?

CSA by Yourself

## Management and audit approach

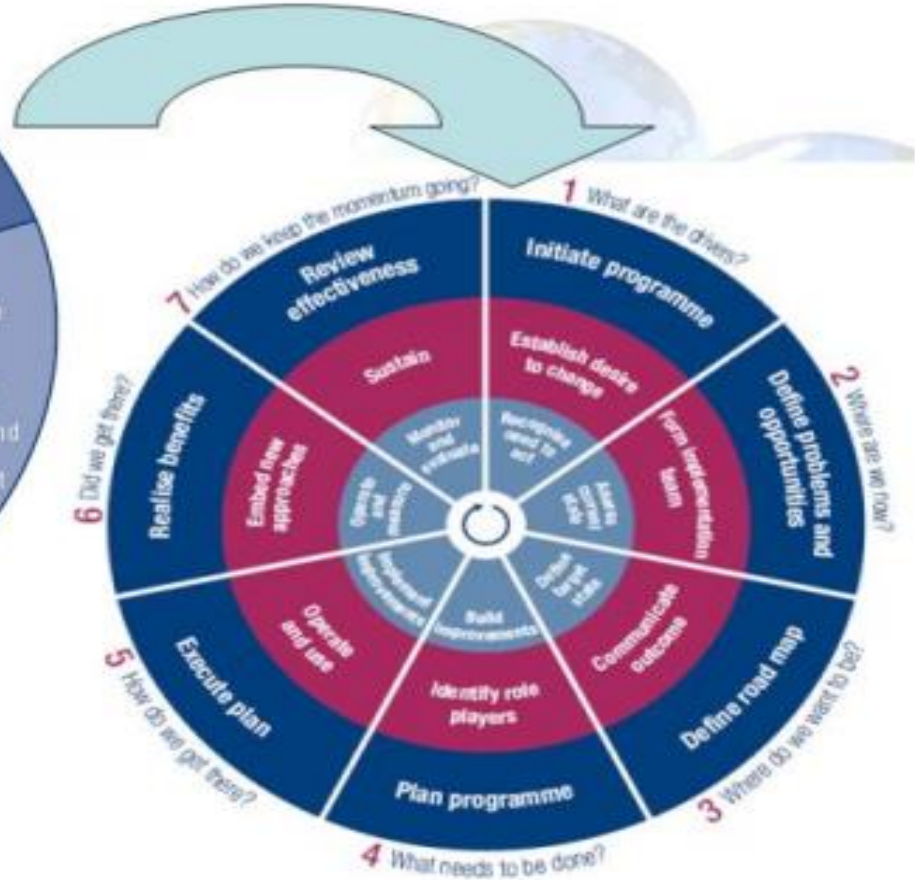
## Financial Statements & Reports & Actions



# PRACTICAL GRC

## Implementing and Continually Improving ITG


"The New Life Cycle Model"



# 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

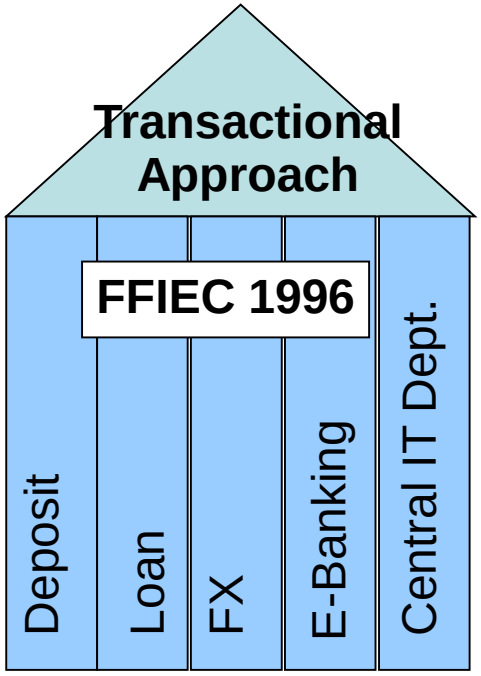
Source: The Institute of Internal Auditors

# เปรียบเทียบการตรวจสอบแนวทางเดิมกับแนวทางใหม่ที่ได้ผลมาก

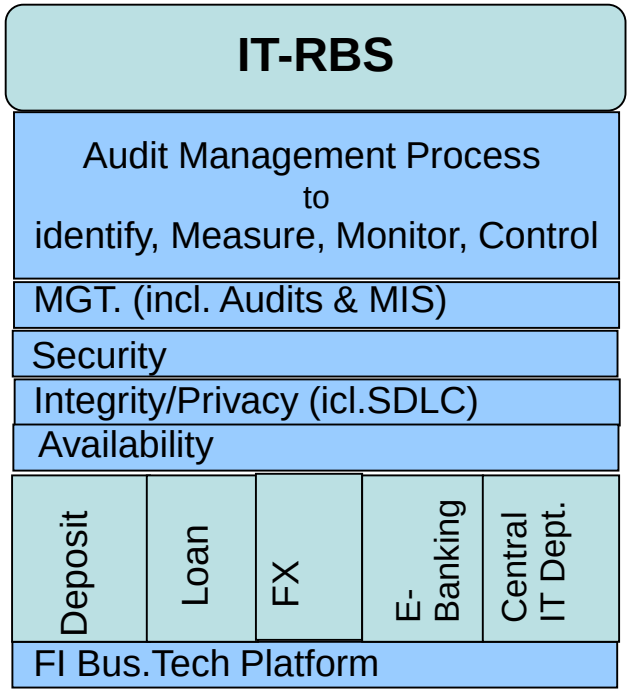
IT Audit &
Non-IT Audit

**SR98-9 IT Risks**

แนวการตรวจสอบ
ข้ามสายงาน-ยุค
ปัจจุบัน

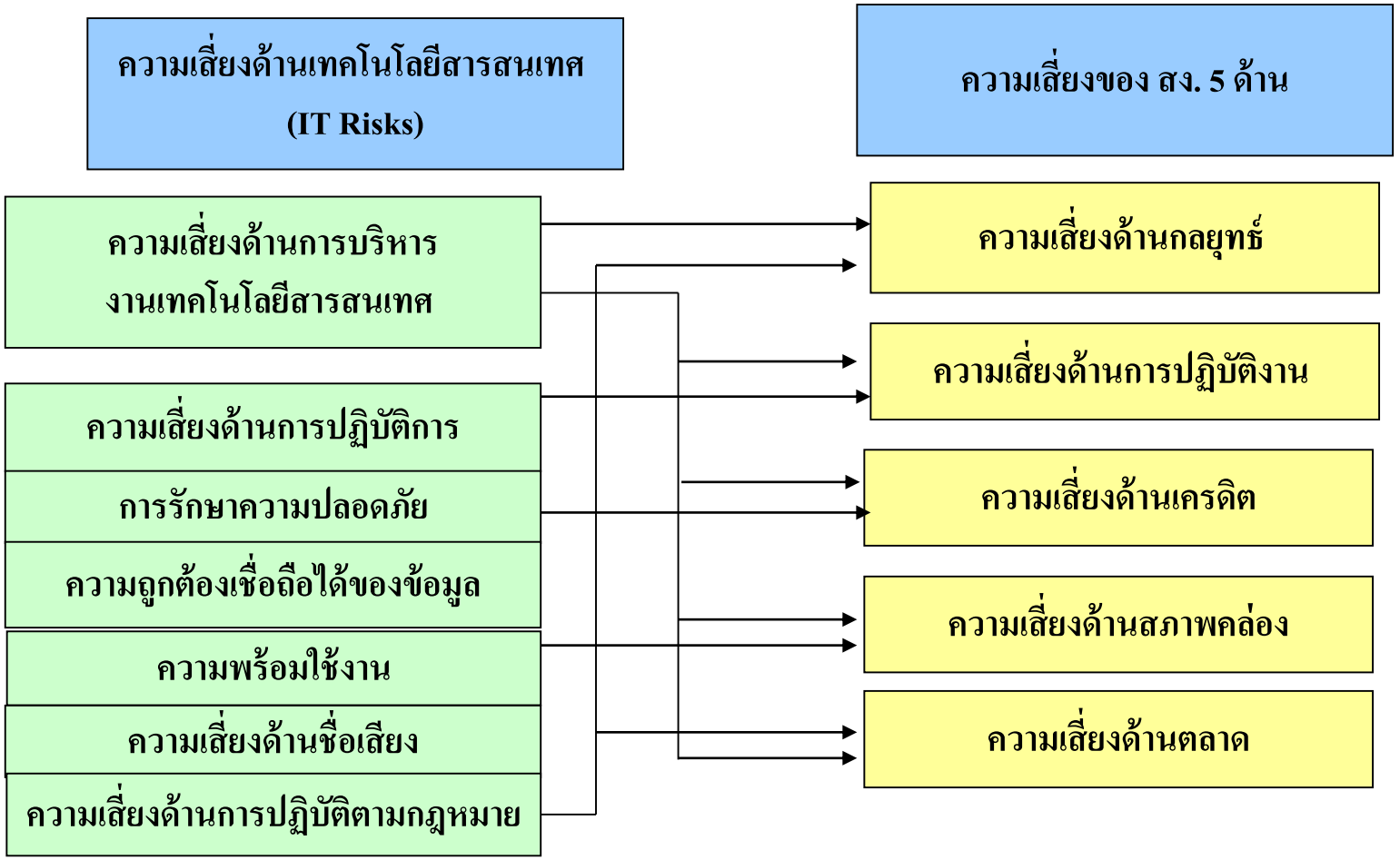



**Operational Risk Management**



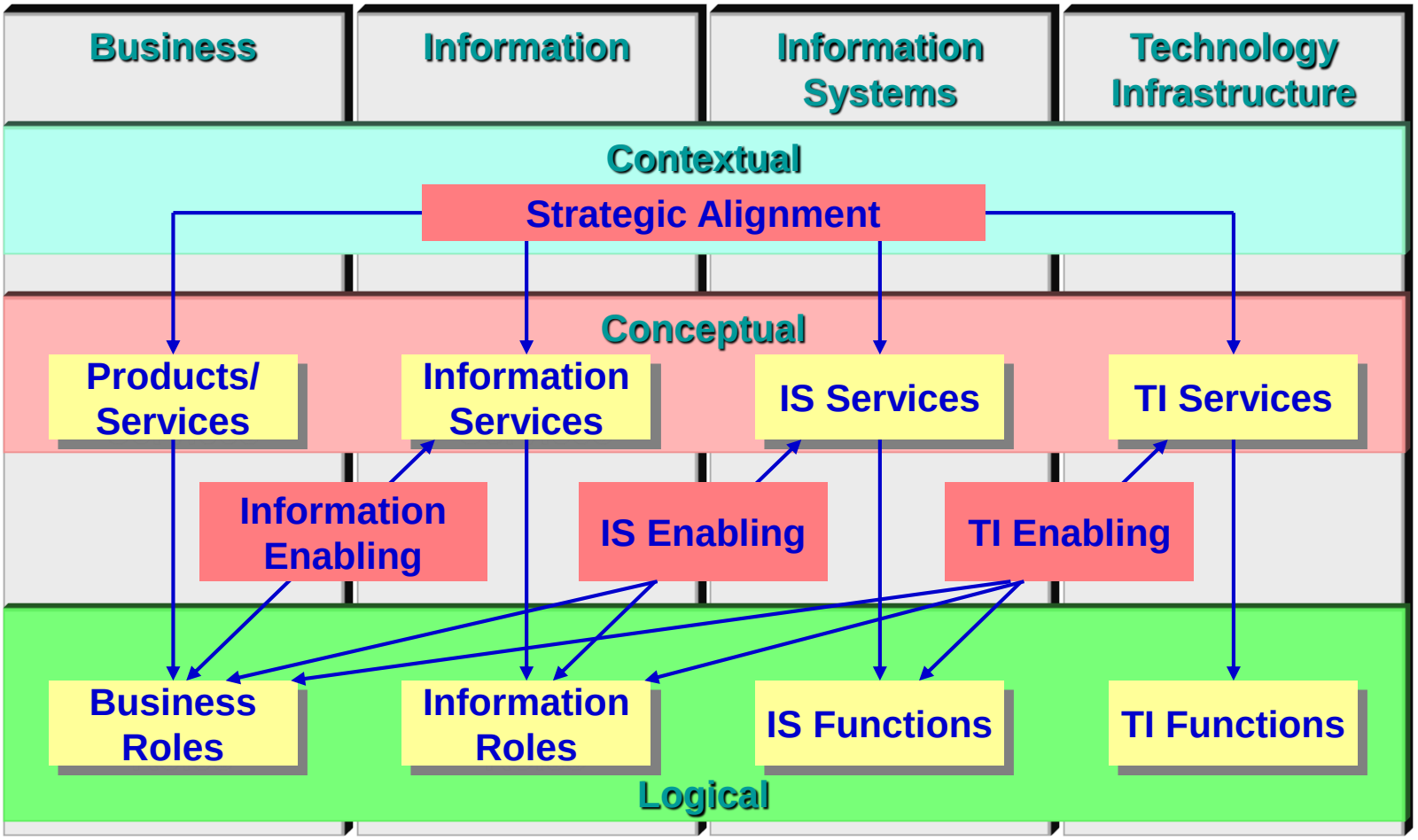

Integrated Audit

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



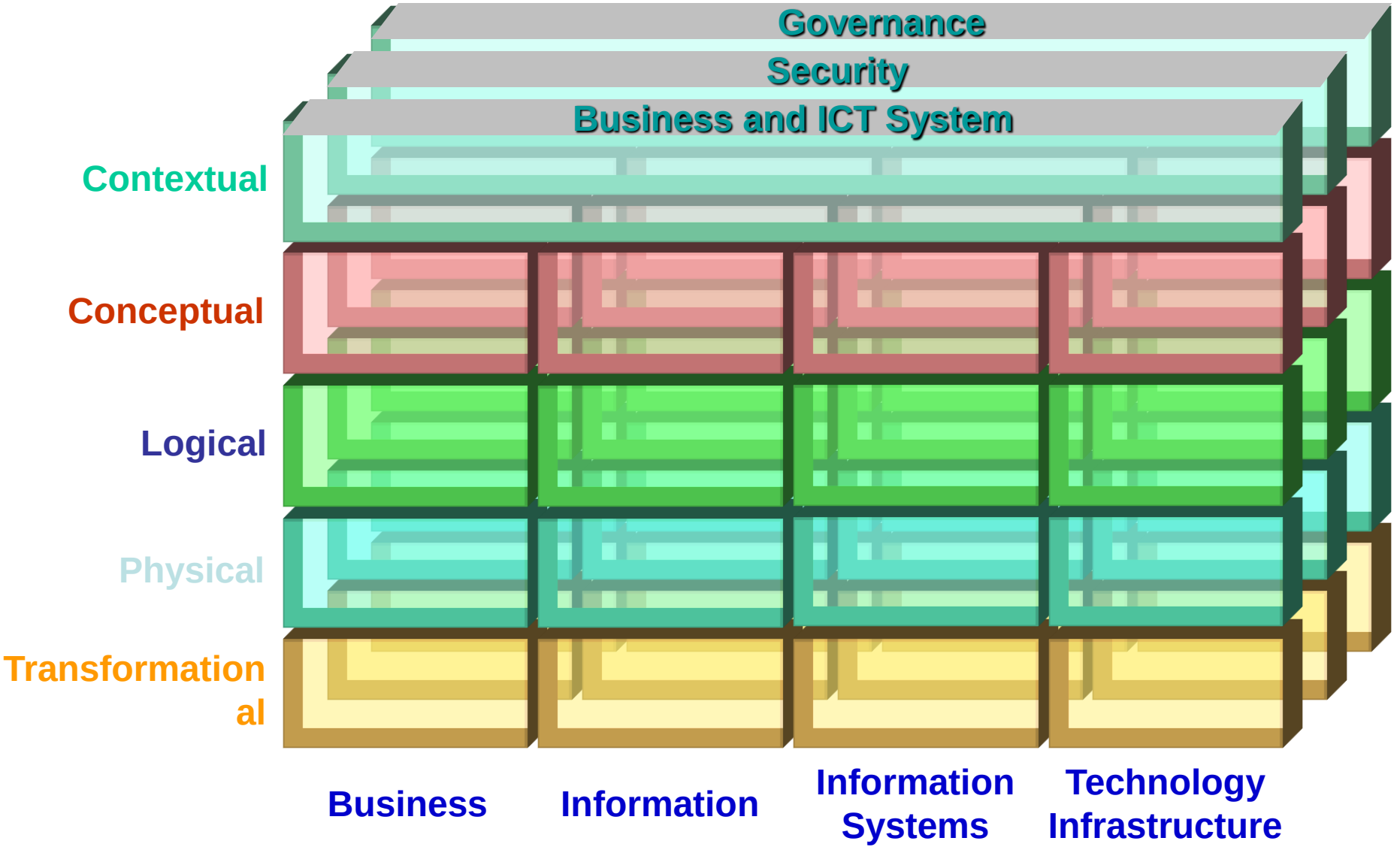

ที่มา : ธนาคารแห่งประเทศไทย เพื่อนำมาประยุกต์ใช้ในการวางแผนและการตรวจสอบภายในขององค์กร

# Strategic Alignment between Main Architecture Areas




Adopt and Adapt from IAF

# Special Viewpoints in IAF and Management




Adopt and Adapt from IAF

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"

# GRC : Governance-Risk Management - Compliance

## การบูรณาการระหว่าง Governance - Risk management - Compliance (GRC)

## กับบทบาทของคณะกรรมการและผู้บริหาร

Integrated Audit / Management

**บทบาทของคณะกรรมการ**

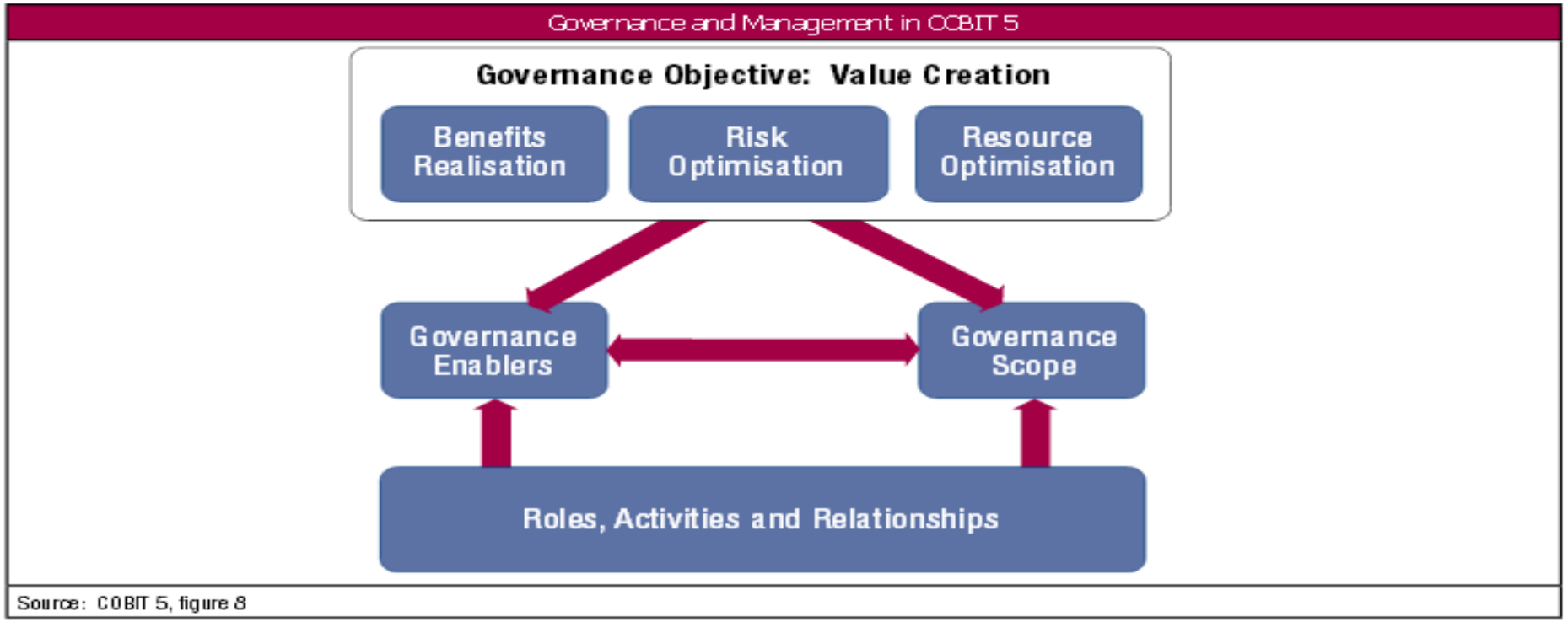
1. มีการกำหนดนโยบายด้าน GRC
2. มีการร่วมกำหนดกลยุทธ์ขององค์กรและนโยบายในการปฏิบัติงาน ติดตามดูแลการปฏิบัติหน้าที่ของฝ่ายบริหารให้เป็นไปตามกลยุทธ์และนโยบายที่กำหนดไว้
3. มีการกำหนดอำนาจหน้าที่ของคณะกรรมการที่เกี่ยวข้องกับ GRC
4. มีการกำหนดนโยบายและกลยุทธ์ในการบริหารจัดการความเสี่ยงอย่างชัดเจน เป็นลายลักษณ์อักษร มีประสิทธิภาพ และเหมาะสมกับสภาพแวดล้อมในการดำเนินธุรกิจ
5. มีการสร้างกระบวนการเพื่อให้เกิดความมั่นใจได้ถึงการที่ รส. ได้มีการวิเคราะห์ถึงเหตุการณ์ที่จะทำให้ปัจจัยที่เป็นความเสี่ยงได้เกิดขึ้น
6. มีการสร้างกระบวนการเพื่อให้เกิดความมั่นใจได้ถึงการที่ รส. ได้กำหนดมาตรการในการติดตามเหตุการณ์ที่เป็นสาเหตุของปัจจัยความเสี่ยง รวมทั้งมาตรการในการลดความเสี่ยงเหล่านั้น
7. มีการสร้างกระบวนการเพื่อให้เกิดความมั่นใจได้ถึงการที่ รส. ได้แจ้งให้พนักงานทุกคนที่เกี่ยวข้องรับทราบ และปฏิบัติตามมาตรการบริหารความเสี่ยงที่กำหนดไว้
8. มีการสร้างกระบวนการเพื่อให้เกิดความมั่นใจได้ถึงการที่ รส. มีการติดตามการปฏิบัติตามแผนการบริหารความเสี่ยงที่กำหนดไว้
9. มีการสร้างกระบวนการเพื่อให้เกิดความมั่นใจได้ถึงการที่ รส. ได้มีกระบวนการระบุปัจจัยเสี่ยงที่เกี่ยงที่เกี่ยวข้องกับการที่จะทำให้องค์กรไม่บรรลุเป้าหมายในด้าน GRC
10. ดูแลการบริหารความเสี่ยงขององค์กร โดยรับรู้ถึงระดับความมีประสิทธิผลของการบริหารความเสี่ยงที่ฝ่ายบริหารได้จัดให้มีขึ้นในองค์กร ตระหนักและให้ความเห็นชอบกับระดับความเสี่ยงที่ยอมรับได้ขององค์กร สอบทานความเสี่ยงในภาพรวมขององค์กรและพิจารณาเปรียบเทียบกับระดับความเสี่ยงที่องค์กรยอมรับได้

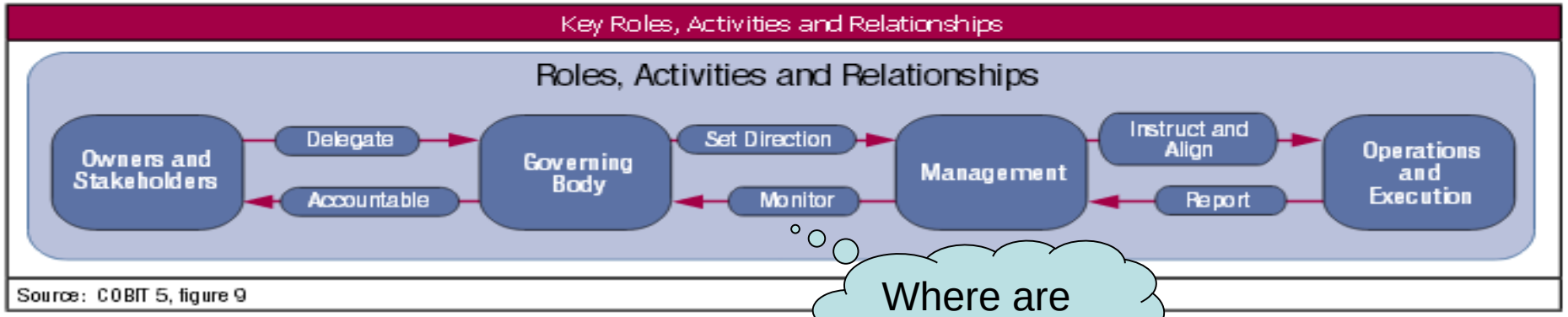
**ระดับ C-Level**

11. รส. มีการกำหนดคณะทำงานที่รับผิดชอบดำเนินงานในด้าน GRC โดยมีผู้บริหารสูงสุดเป็นประธานคณะทำงาน และมีแผนงานที่ชัดเจนในการดำเนินการด้าน GRC รวมถึงนำเสนอคณะกรรมการเพื่อพิจารณา
12. รส. มีการประเมินอย่างสม่ำเสมอถึงการประกอบธุรกิจขององค์กรว่ามีปัจจัยในบ้างที่เป็นปัจจัยความเสี่ยงทั้งที่มาจากภายนอกและภายใน ซึ่งอาจมีผลกระทบต่อการดำเนินธุรกิจอย่างมีนัยสำคัญ
13. รส. ต้องมีการระบุปัจจัยเสี่ยงและกระบวนการในการบริหารความเสี่ยงในด้าน Compliance ให้ครบถ้วน
14. รส. ต้องมีการเปิดเผยข้อมูลสำคัญๆ อย่างครบถ้วน ถูกต้อง เพียงพอ และทันต่อเหตุการณ์

ที่มา : สคร.- ก.คลัง

# COBIT 5 and Key Roles-Activities- Relationship




Where are you ?

Source : ISACA

หลักสูตรผู้บริหารเทคโนโลยีสารสนเทศระดับสูง

CIO (Chief Information Officer) รุ่นที่ 25

# การบริหารความเสี่ยงด้านไอซีที

# ICT Risk Management

วันที่ 14 มกราคม 2558

ณ ห้องกมลมาส ชั้น 6 โรงแรมเดอะสุโกศล

++ Integrated Risk Management

โดย

**นาย เมธา สุวรรณสาร**

CGEIT; CRISC; CRMA; CIA; CPA

www.itgthailand.com

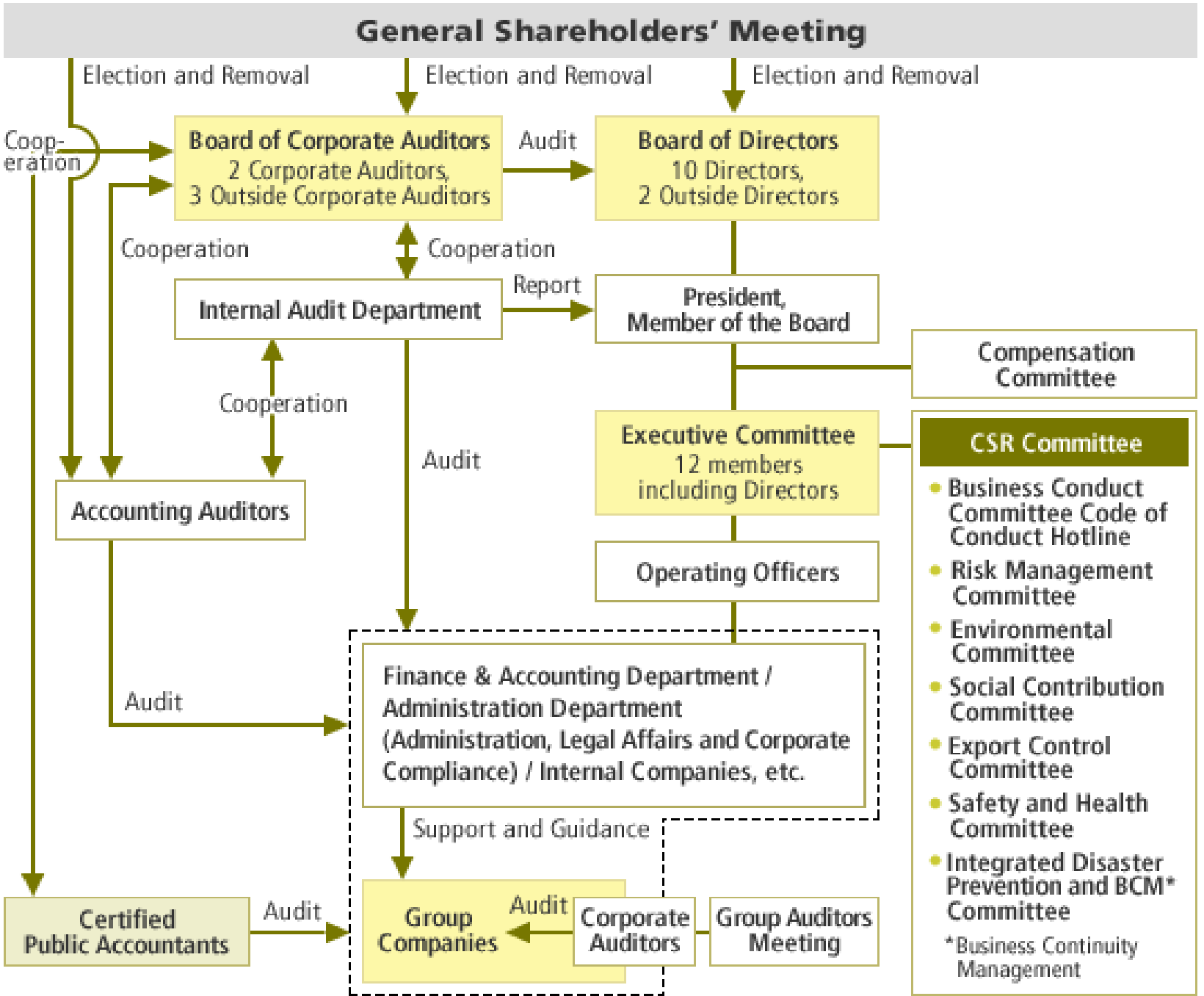
# Q & A

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

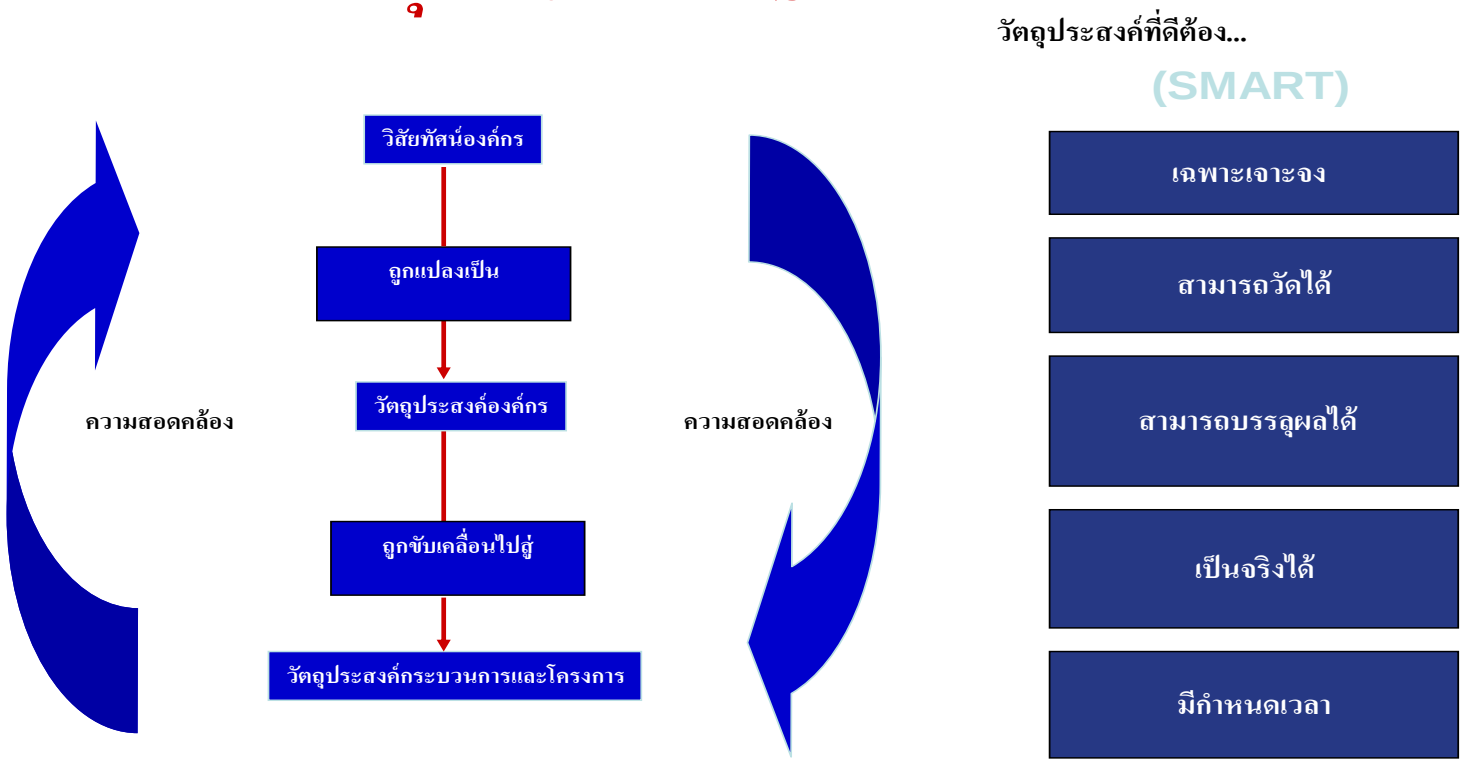
พระราชกฤษฎีกาว่าด้วยวิธีการแบบปลอดภัยในการทำธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2553 มีผล 180 วันนับจากวันที่ 3 กันยายน 2553 ท่านพร้อมแล้วหรือยังครับ ? เพราะเกี่ยวข้องกับทุกองค์กร +++ นโยบายความมั่นคงปลอดภัยสารสนเทศฯ +++ โปรดติดตามที่.....

www.itgthailand.com,หรือhttp://www.ratchakitcha.soc.go.th/DATA/PDF/2553/A/053/13.PDF

## Corporate Governance Organization (as of June 30, 2010)



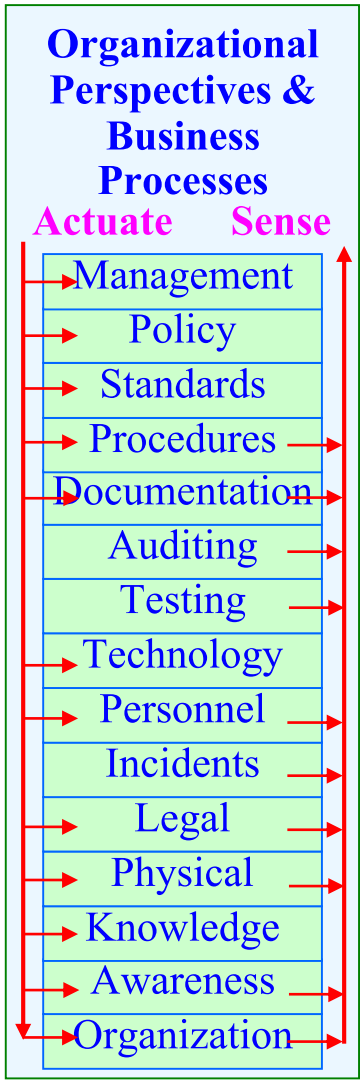
# การกำหนดวัตถุประสงค์แบบ SMART




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

# IT Security Governance

## Organizational Perspectives




### Management
People
Budgets
Effects
Senses
Controls
Planning
Strategy
Tactics
Coordination
Politics

### Policy
Governance
Align w/value
Power
Feedback
Budget
Appeals
Acceptable use
Obey laws

### Standards
GAISP
ISO17799
CMM-SEC
COBIT
COSO
ITIL
NSTSSI
Technical

### Procedures
Situation
Process
Actions
Logging
Escalation
Flow Control
Closure
Feedback

### Documentation
Situations
Requirements
Formats/Copies
Tracking
Marking
Storage
Use/Disposal

### Auditing
Internal
External
Period
Standard
Coverage

### Testing
Fault models
Coverage
Regression
Periodic
Change
Blind
Planned

### Technology
Attacks
Defenses
Mainframes
Midrange
Servers
Clients
Firewalls
Networks
Telephony
Backbone
Cabling
Hosts
External links
OS's
Configurations
Applications

### Personnel
Life cycles
Knowledge
Awareness
Background
Trustworthiness
History
Capabilities
Intents
Modus operandi
Roles
Changes
Clearances
Need to know
IdM interface

### Incidents
Detection
Response
Adaption
OODA loops

### Legal
Regulatory
Civil
Criminal
Notice
Contracts
Liability
Jurisdiction
Investigatory
Chain of Custody
Evidential
Forensics

### Physical
Time
Location
Path
Properties
A-graph
Entry
Egress
Emergency
Hardening
Locking
Mantraps
Surveillance
Response time
Force on force
OODA loops

### Knowledge
Education
Experience
Training
Degrees

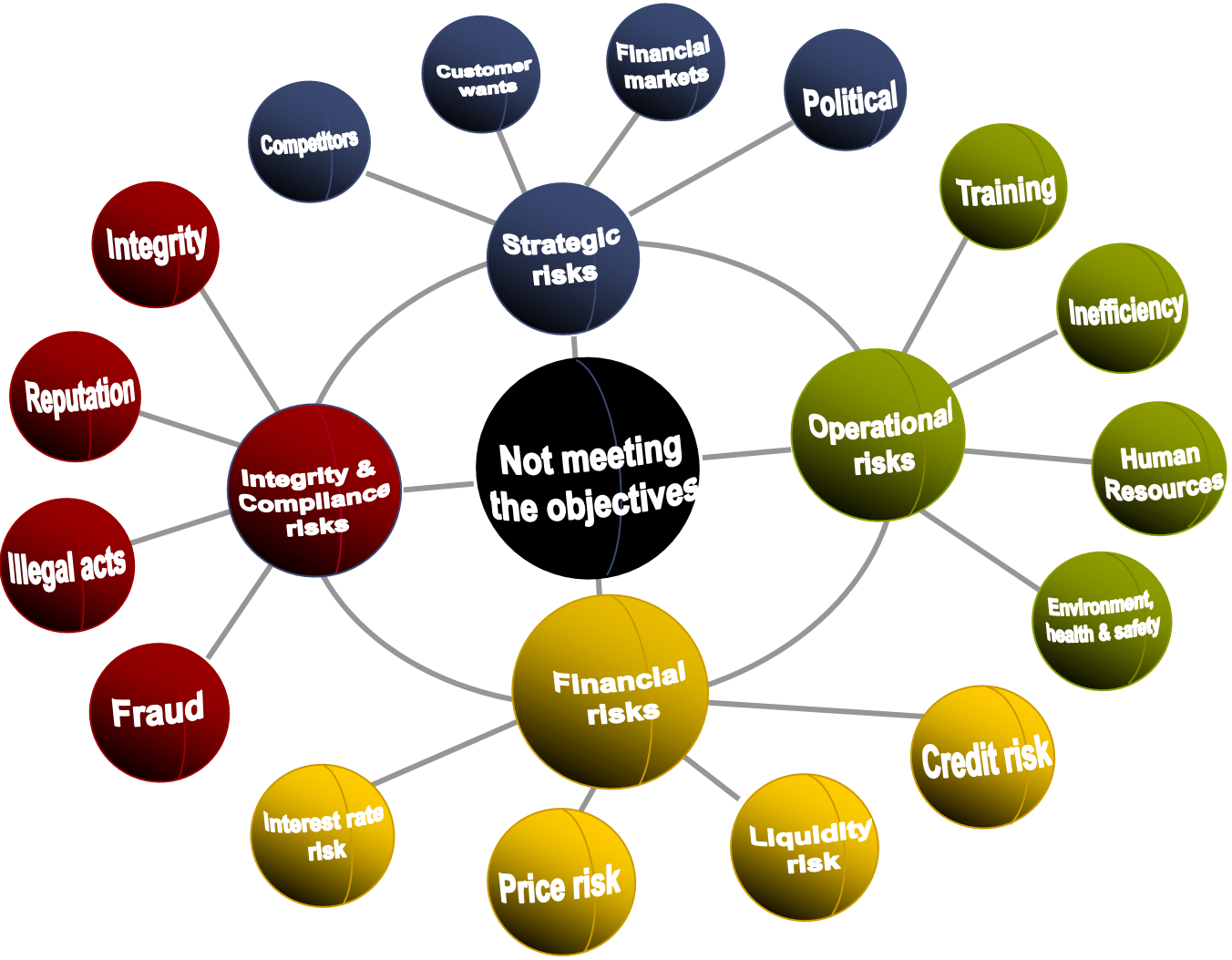
### Awareness
Document review
Initial briefings
Day-to-day
Dept. meetings
Computer-based
Video-based
Groups
Lectures
Games
Posters/banners
Badging & carding
Stand-downs
Memos
emails
Award programs
Social pressure
Covert

### Organization
Structure
Rewards
Punishments
Communication



Source : IT Security Governance Guidebook / FRED COHEN

# Typical risk factors



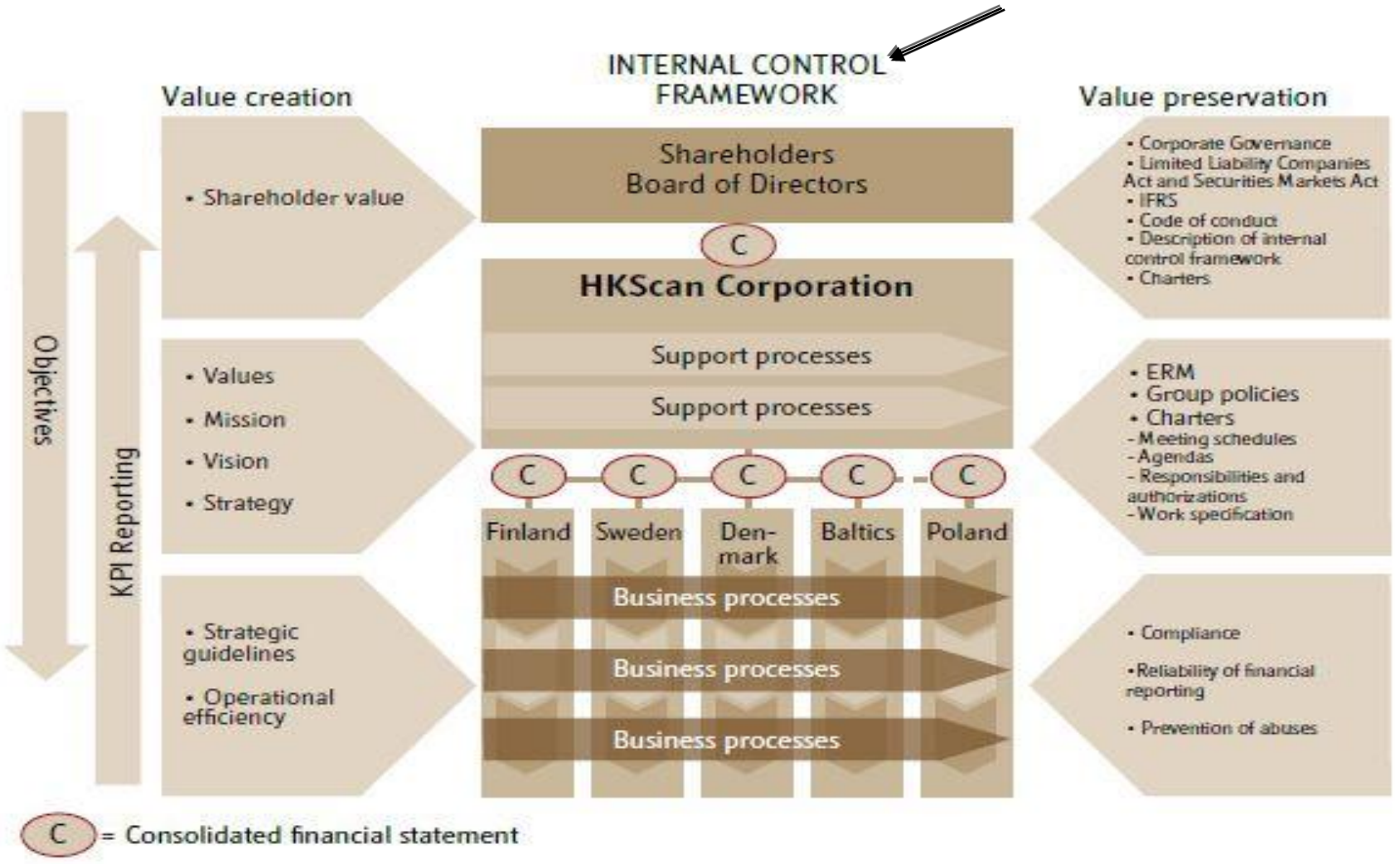

A typical breakdown of risks into categories might include:

- S : Strategic Risk
- O : Operational Risk
- F: Financial Risk
- C: Compliance Risk

and be derived from internal and external conditions


150

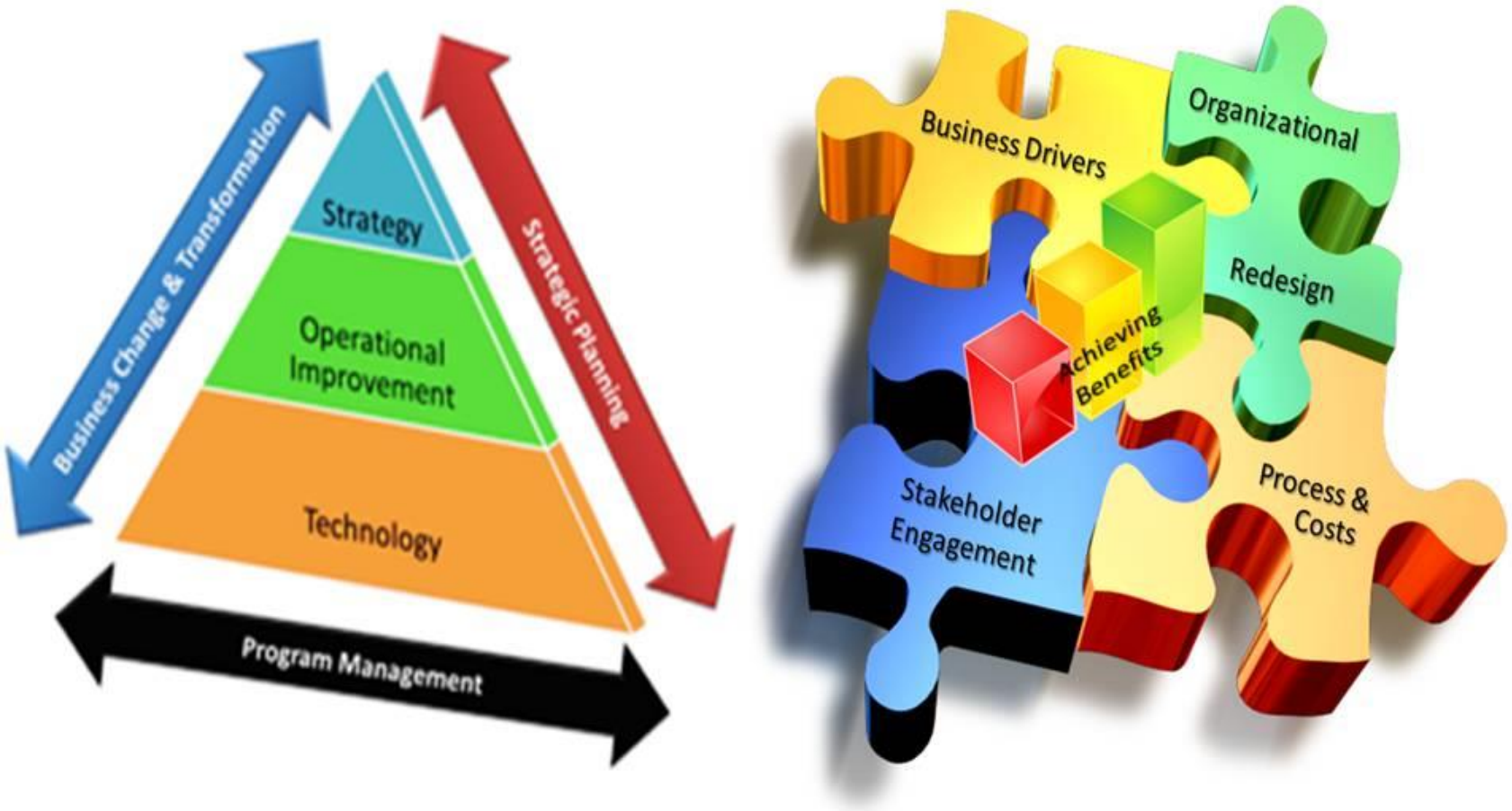
# GRC – Integrated Management / monitoring and Control




Source:The internal **control framework** contains elements originating in the **COSO** …hkscan.com

# การบริหารความเสี่ยงบางมุมมองกับ Digital Economy

## Integrated Management Perspective- Approach to Digital Economy




Adopt and Adapted from http://www.arrayconsultancy.com/businesstransformation.html

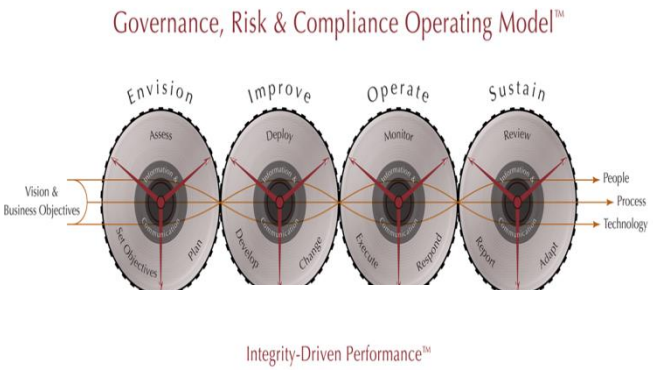
# GRC - Governance; Risk Mgmt; Compliance

## Enterprise Model & Integrity-Driven Performance

Governance, Risk & Compliance

Operating Model™

Enterprise vision and objectives




Integrity-Driven Performance™

Achievement of Enterprise vision and objectives

**I**nput **P**rocess **O**utput

Adopt from: A New Strategy for Success Through Integrated Governance, Risk and Compliance Management---- PWC

# ความเสี่ยงกับการจัดการที่ดี

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

# สุภาษิตและคติที่น่าสนใจ

เมื่อลมเปลี่ยนทิศ
บางคนสร้างกำแพง
บางคนสร้างกังหันลม

(สุภาษิตจีน)

เราเปลี่ยนทิศทางลม
ไม่ได้
แต่เราปรับใบเรือได้

(มหาตมะ คานธี-อินเดีย)

**Change before we are forced to change**

(Jack Welch-US)


Thank you