CG+ITG+GRC Perspectives

and

COSO - Enterprise Risk Management

Sept 17 2008

โดย : เมธา สุวรรณสาร

Metha Suvanasarn CIA;CPA

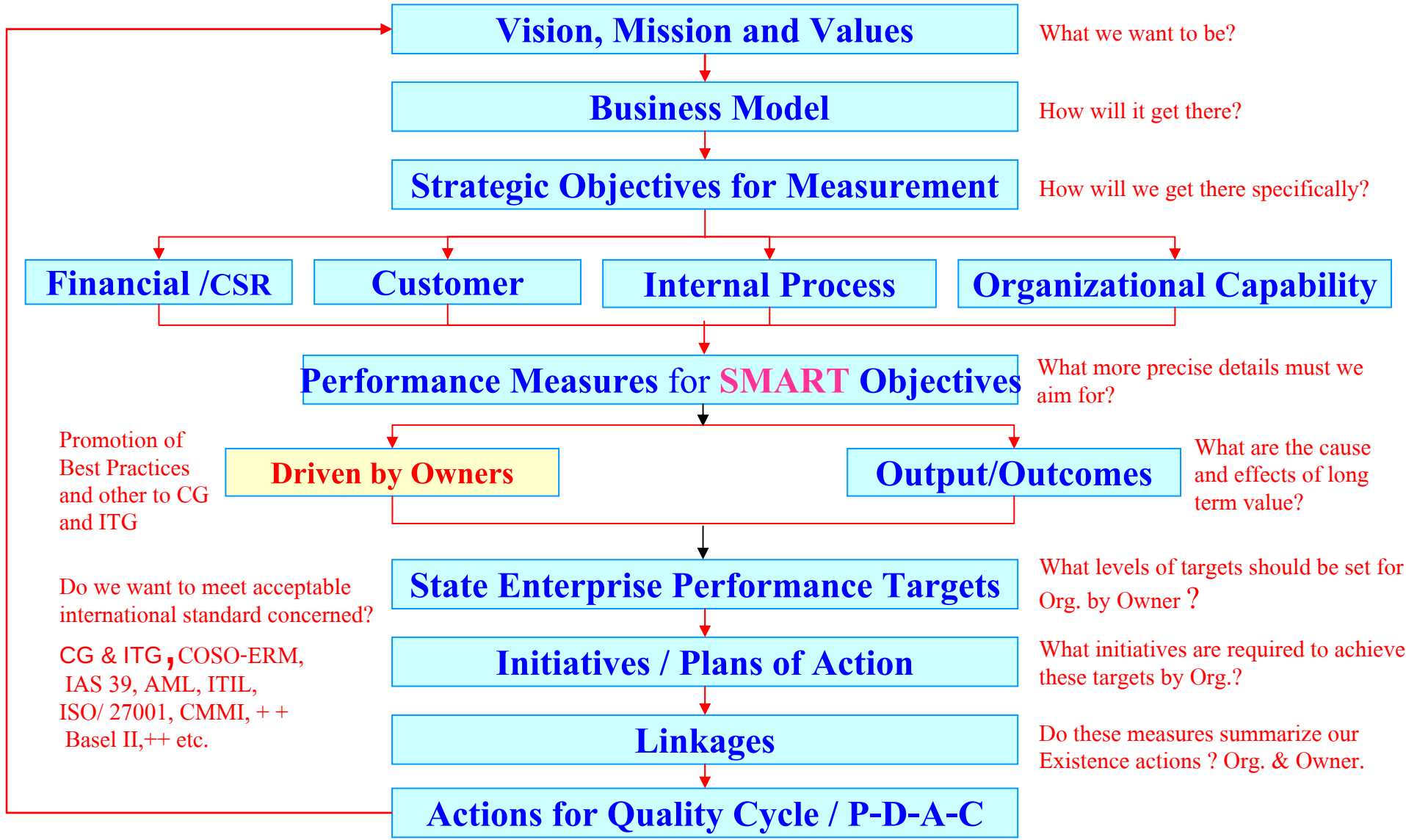
กรอบ CG กับแนวนโยบายของผู้ถือหุ้น (SOD) และกลยุทธ์สู่ Action Plan

หลักธรรมาภิบาล และ
การกำกับดูแลการบริหารจัดการ
ที่มุ่งประสิทธิภาพได้มาตรฐานระดับสากล (World Class)

RESPONSIBILITY มีความเข้าใจและมีจิตความสามารถในการประพฤติปฏิบัติได้ตามหน้าที่และความรับผิดชอบ	**ACCOUNTABILITY** แสดงความยอมรับผิด และรับชอบต่อผลการปฏิบัติหน้าที่	**EQUITABLE TREATMENT** ปฏิบัติต่อผู้มีส่วนได้ส่วนเสียทุกกลุ่ม อย่างเท่าเทียม และเป็นธรรม	**CREATION OF LONG TERM VALUE** แสดงกลยุทธ์และจิตความสามารถ ในการสร้างมูลค่าเพิ่มให้กับกิจการ ในระยะยาว	**TRANSPARENCY** แสดงความโปร่งใสในการดำเนินงาน สามารถอธิบายและตรวจสอบได้	**PROMOTION OF BEST PRACTICES** ส่งเสริมการปฏิบัติอันเป็นเลิศ และการมีจรรยาบรรณที่ดีในการประกอบธุรกิจ	**SOCIAL & ENVIRONMENTAL AWARENESS** มีความสำนึกที่ต้องรับผิดชอบต่อสังคม และสิ่งแวดล้อม
แนวนโยบายผู้ถือหุ้น (Statement of Direction - SOD) ผสมผสานกับหลักการ Balanced Scorecard						
วิสัยทัศน์+พันธกิจ+นโยบาย+กลยุทธ์สู่ Action Plan เพื่อวัดประสิทธิภาพของการบริหารและการจัดการ (ดู Slide ประกอบ)						
การประเมินตนเอง (CSA/CSR) ที่มี KPI ที่ชัดเจน ไม่กำกวม ตรงกับเป้าหมาย โดยใช้มาตรฐานสากลที่เป็นที่ยอมรับทั่วไป (ถ้ามี)						

Translating Vision and Strategy to

Performance Measurement – Drivers & Output/Outcome



ที่มา : ดัดแปลงบางส่วนจาก Hewitt Institute

กรอบการกำกับดูแลกิจการที่ดี CG&ITG และการบริหารเพื่อสร้างคุณค่าเพิ่มกับ Soft Controls

Tone at the Top

- **ระดับวิสัยทัศน์**

โดยคณะผู้บริหารระดับสูง
หรือคณะกรรมการบริหาร

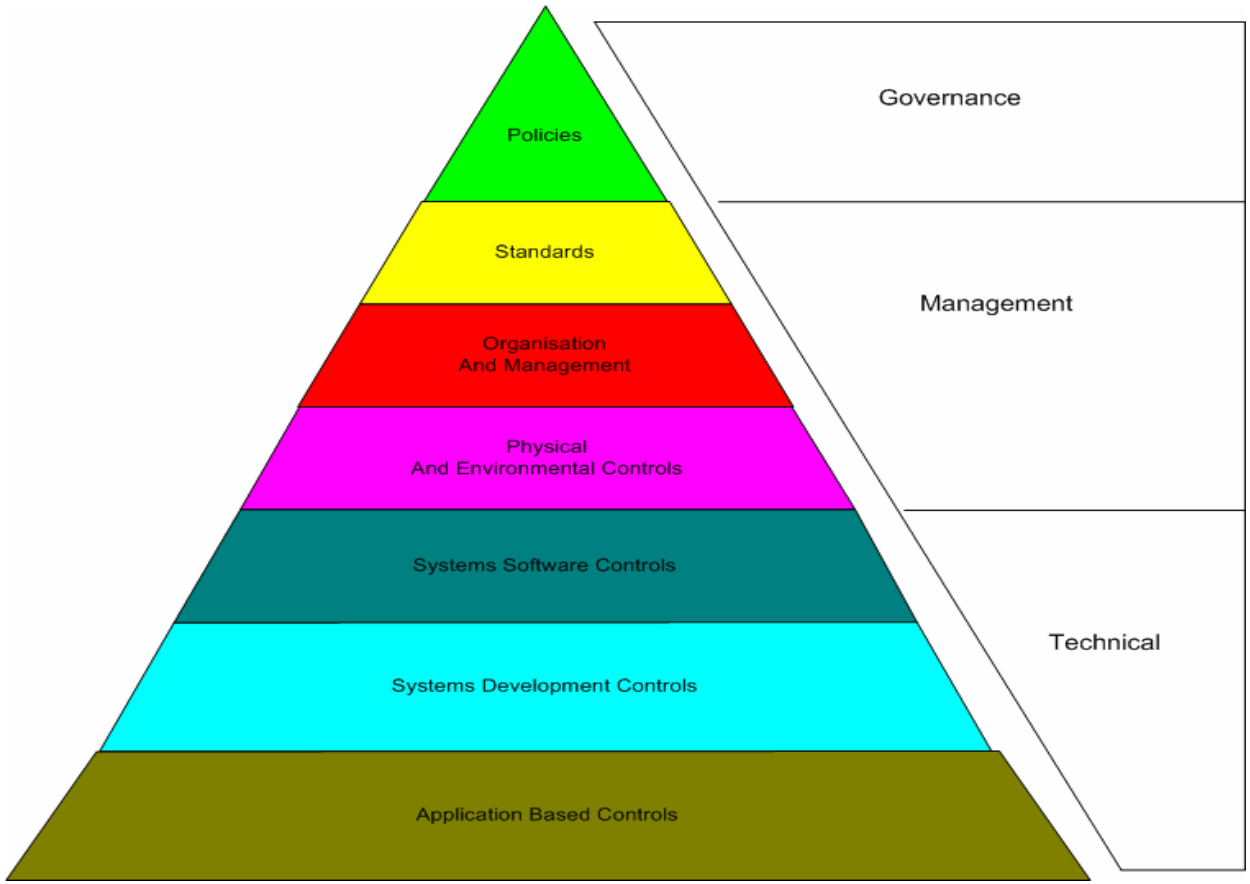
- **ระดับการบริหาร**

โดยผู้อำนวยการ และ
รองผู้อำนวยการ

- **ระดับปฏิบัติการ**

โดยผู้บริหารลงไปถึง
ผู้ปฏิบัติ

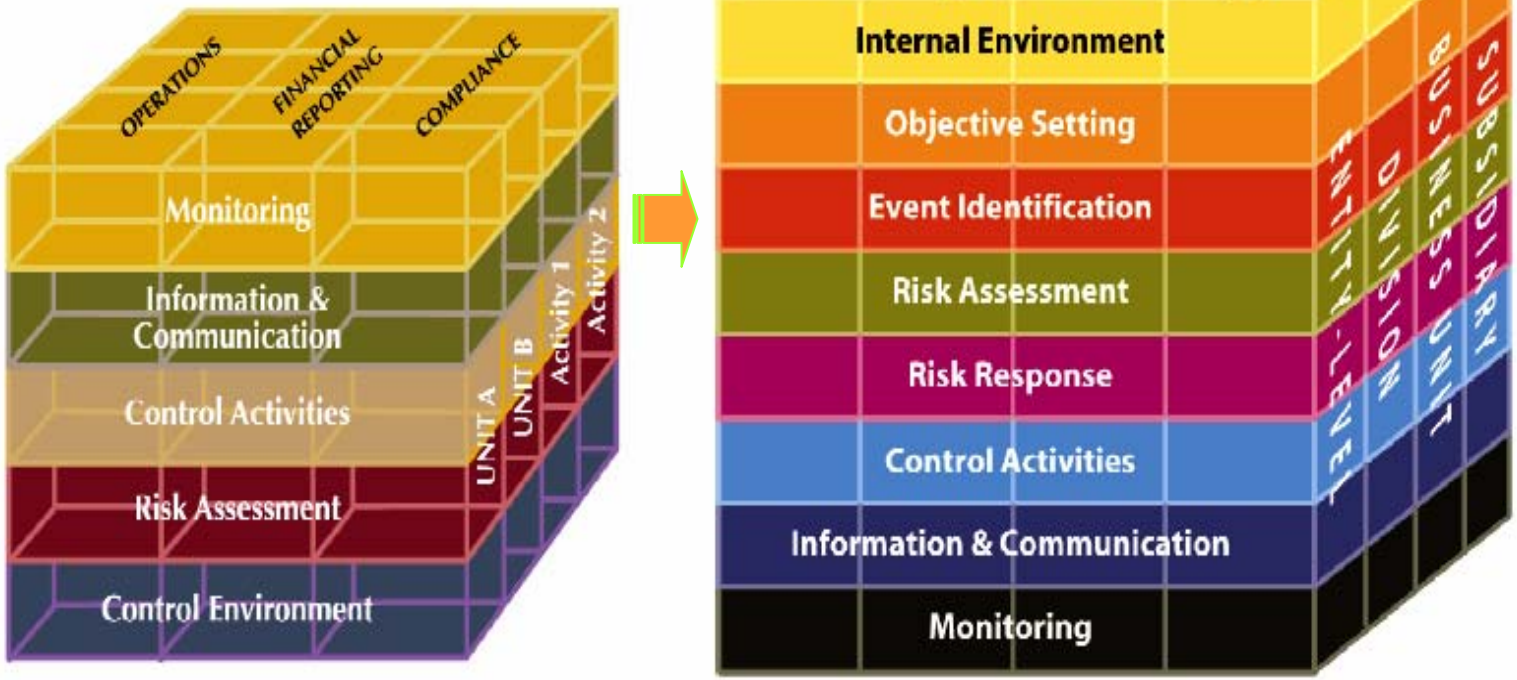
Understanding IT Controls & IT Risk



- A top-down approach used when considering controls to implement and determining areas on which to focus.

Relationship between COSO 1 and COSO 2

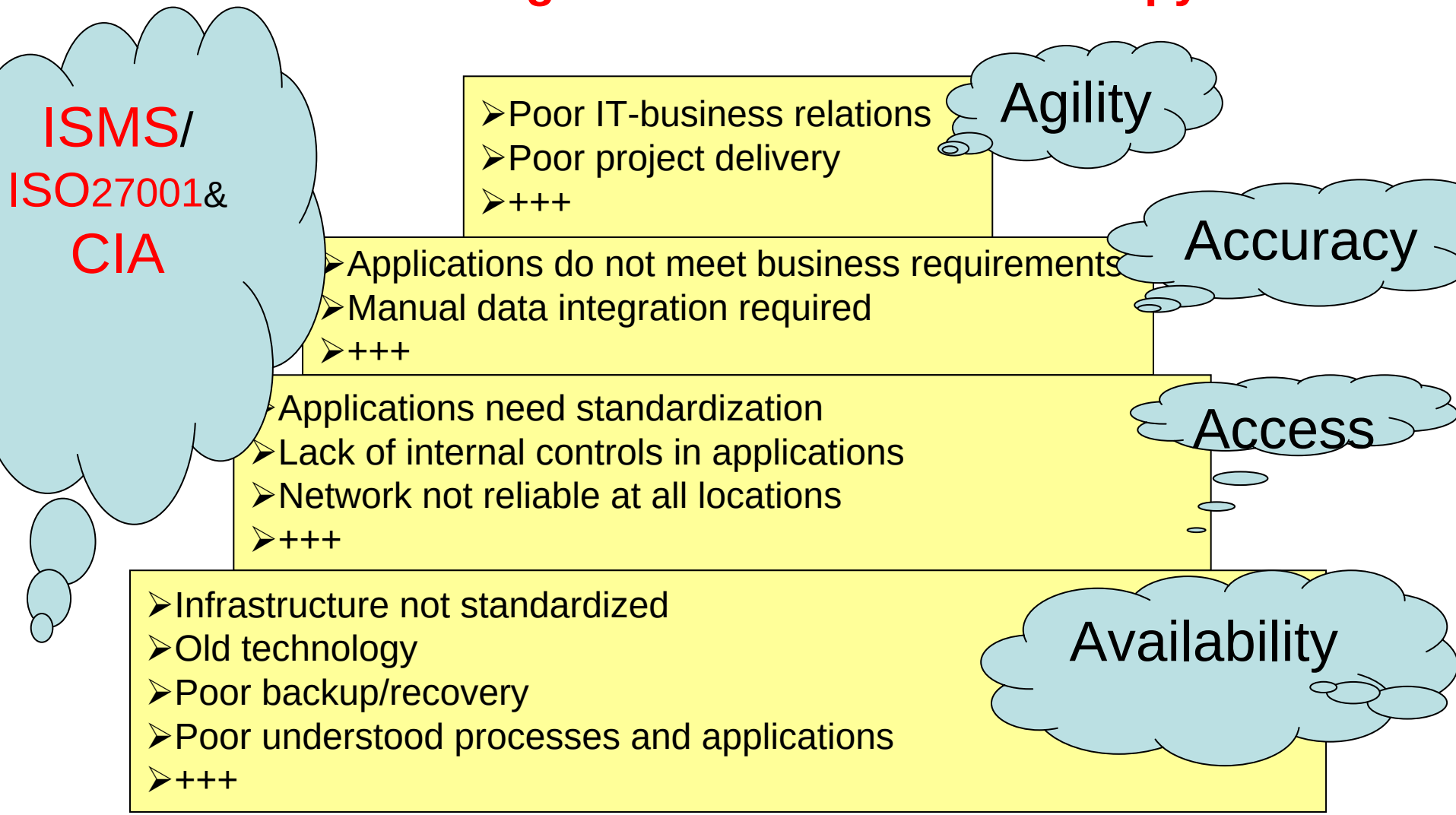
ERM is fully aligned with the COSO Internal Control- Integrated Framework



COSO 1 "Internal Control – Integrated Framework"

COSO 2 "Enterprise Risk Management – Integrated Framework"

IT Risk factors aligned with their tiers in the pyramid

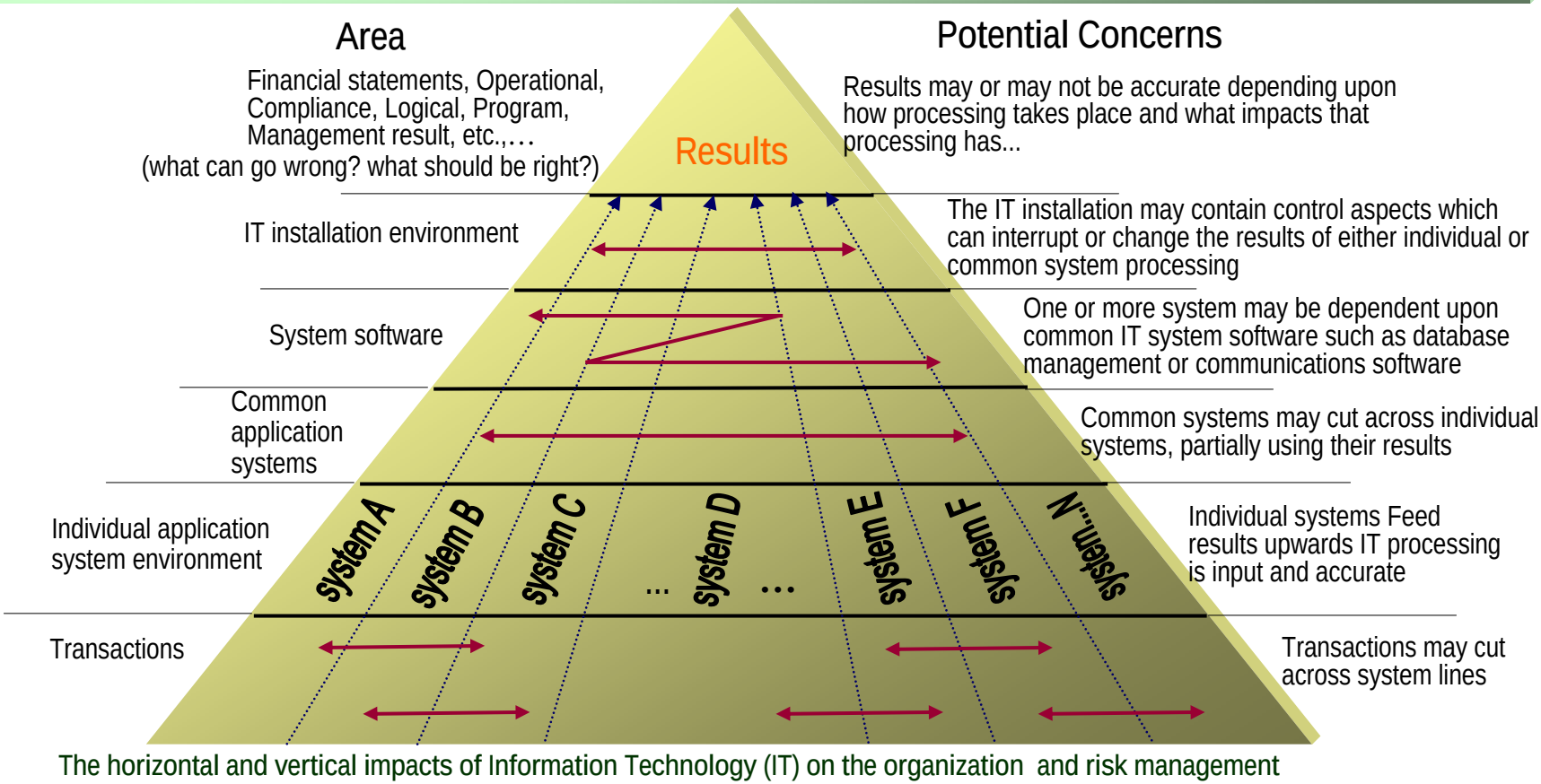


Source: Adopt from IT Risk –turning business threats into competitive advantage by George Westerman & Richard Hunter

IT Governance เป็นส่วนหนึ่งที่สำคัญยิ่งของ Good Corporate Governanceของ องค์กร

Enterprise Risk Mgmt.covering corporate or business support mgmt. ที่เกี่ยวข้องกับความเสี่ยง ในการใช้เทคโนโลยีสารสนเทศ

องค์ประกอบการควบคุมภายในทั้ง 8 และวัตถุประสงค์+การตรวจสอบตามวัตถุประสงค์หลัก ทั้ง 4 ประการของ COSO-ERM

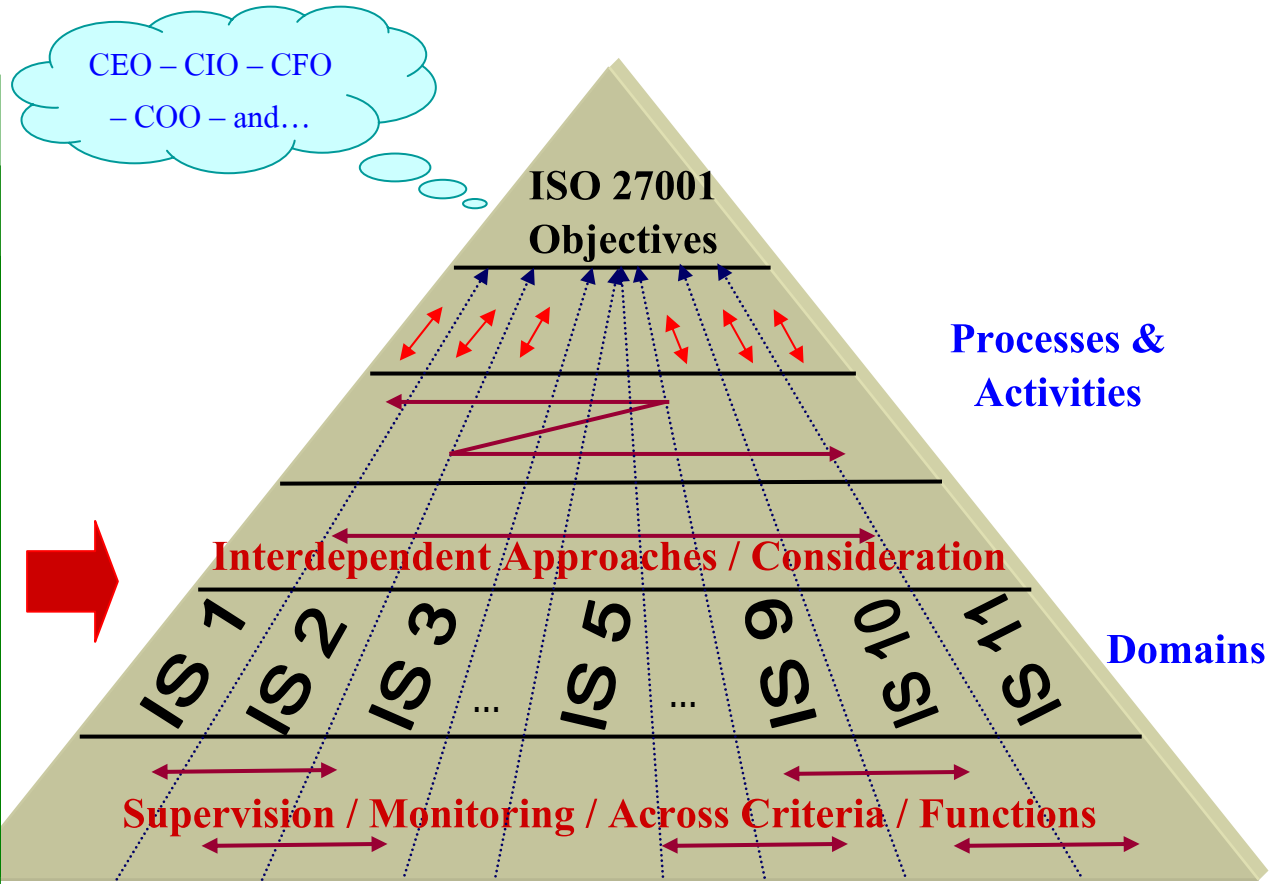


The horizontal and vertical impacts of Information Technology (IT) on the organization and risk management

: แสดงถึง **Total System Approaches** ของระบบงานในภาพกว้าง ๆ ขององค์กรที่ใช้เทคโนโลยีสารสนเทศซึ่งต้องการความเข้าใจและการประสานงานจากผู้เกี่ยวข้องกับผู้บริหารงานขององค์กรอย่างเข้าใจจริงทั้งทางด้าน **IT , non-IT และITG** โดยรวมและต้องการบริหารความเสี่ยงแบบ **Convergence**ขององค์กรเพิ่มขึ้นอีกมากในเรื่องการกำกับดูแลกิจการที่ดี **(Good Corporate Governance) + IT Governance** ซึ่งองค์กร ควรจะได้พิจารณาในการบริหารแบบบูรณาการที่เกี่ยวข้องกับ **business processes** เพื่อก้าวไปสู่ **Objectives ตามหลัก SMART โดยรวม + +**

Information Security – International Standard (ISO 27001) to IT Audit perspectives

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



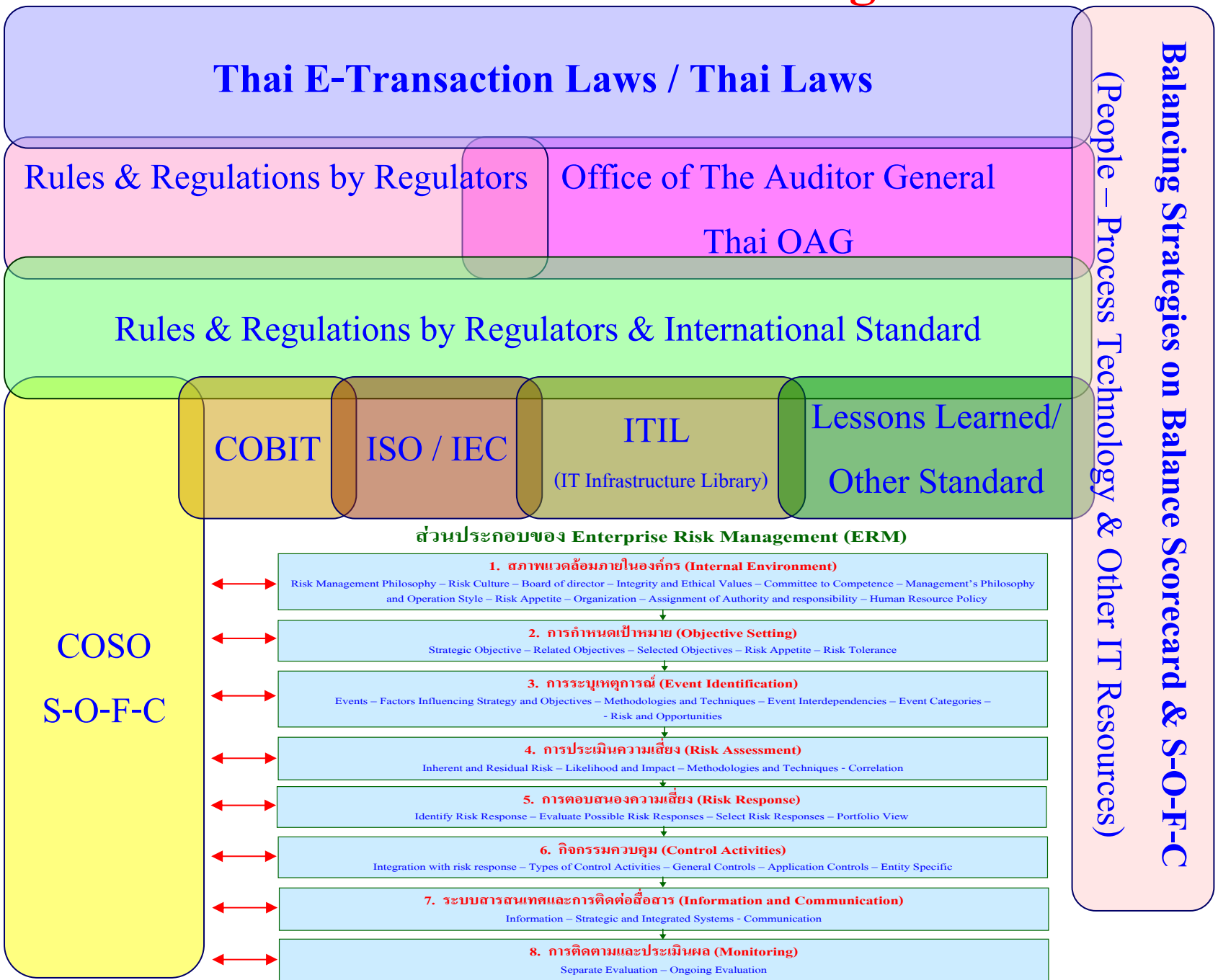
Consideration of common errors in identifying objectives & negative consequences

Identifying a means as an end.

Failing to consider each type & all types of objectives.

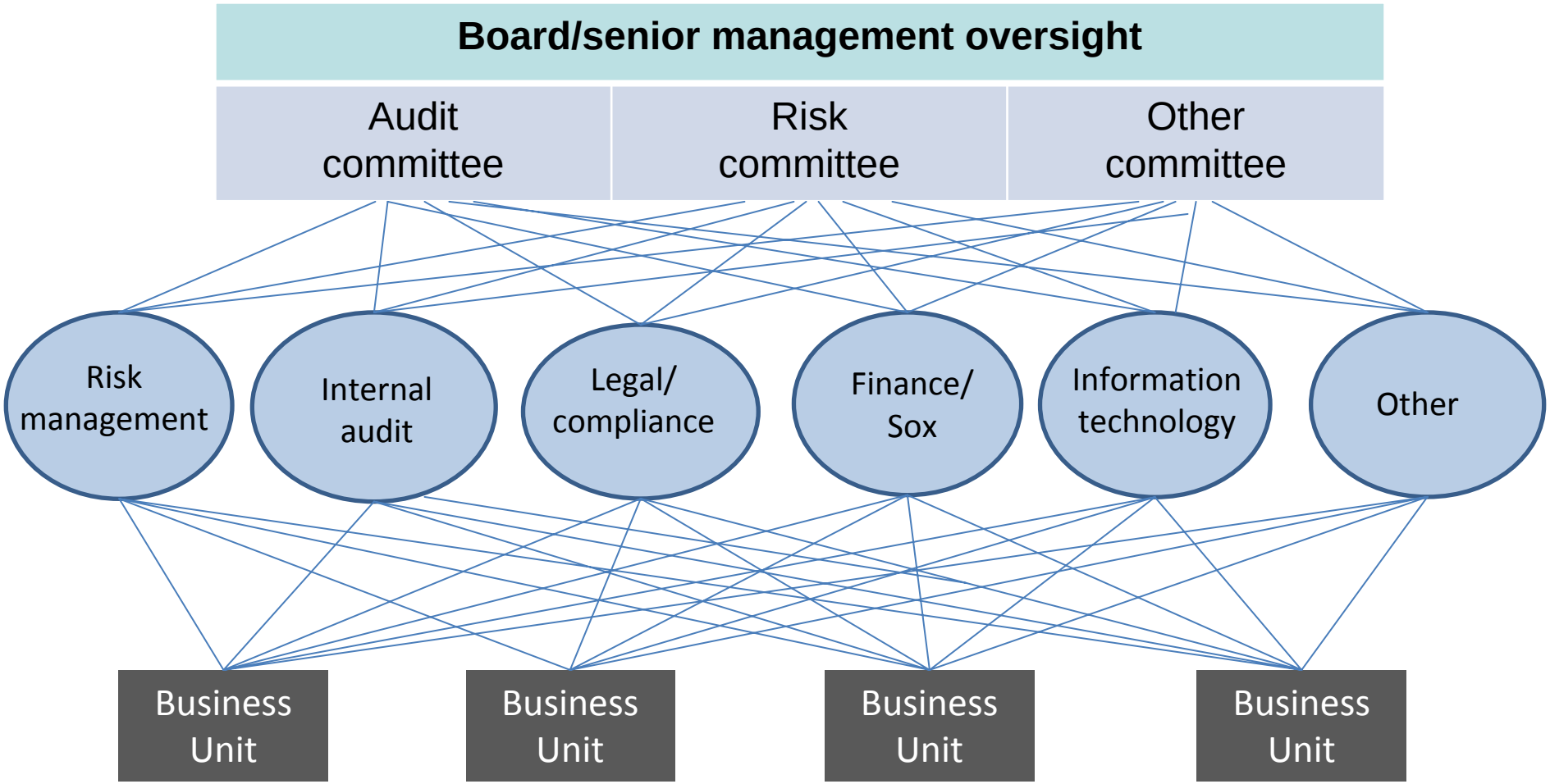
Failing to consider the relationships between objectives.

IT Governance & GRC + Risk Convergence Framework

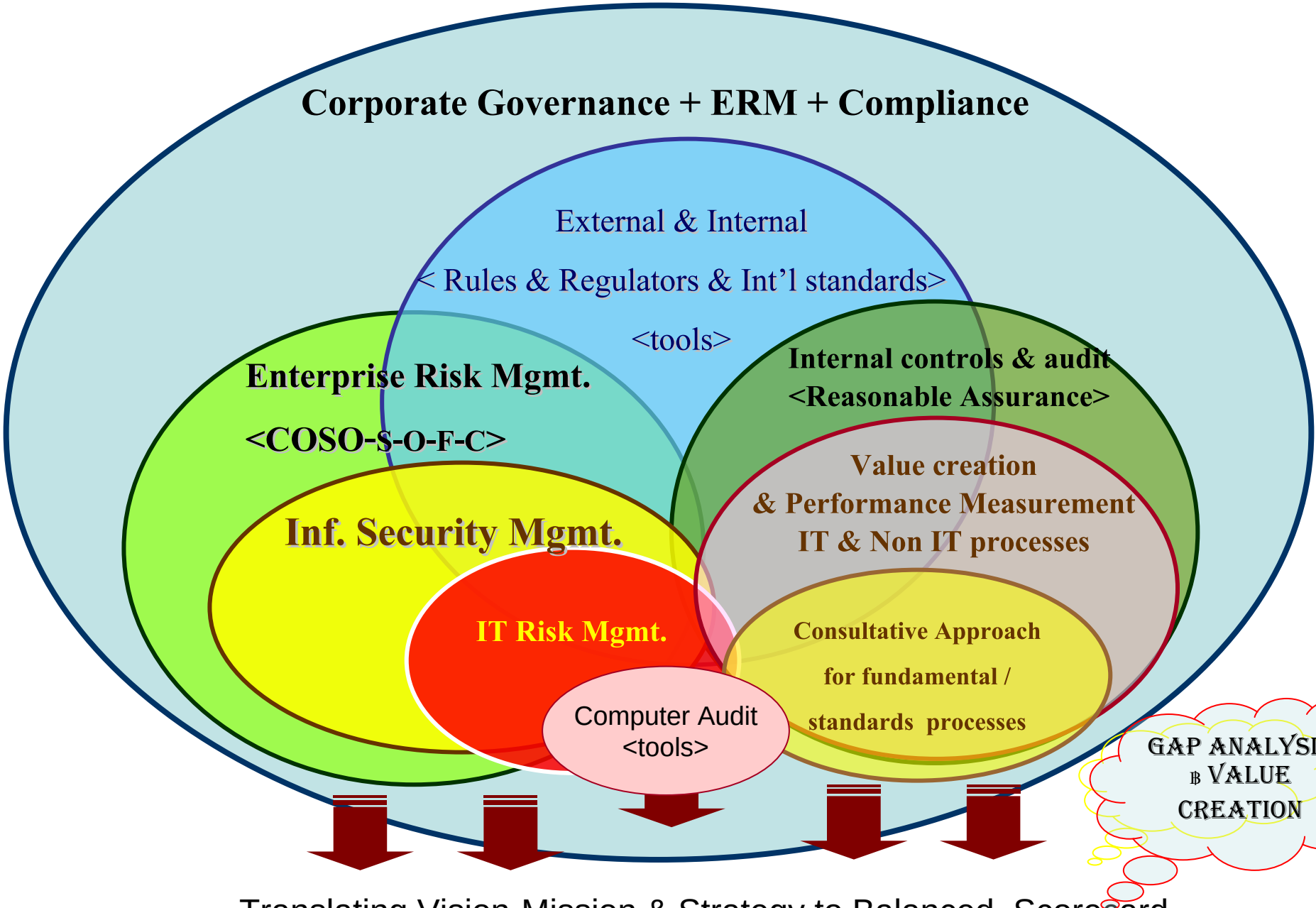


Focus of convergence is on bringing together the myriad governance & control processes across the institution

External – regulators, analysts, investors, stakeholders



Source : Ernst & Young



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

IT Governance / GRC / Compliance & ORCA Understanding

Level 0 – Laws & Regulations

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

Level 2 – Internal Control Framework – IT Governance/ISO

(Enterprise Wide-What to do/ Check list)

Level 3 – IT Best Practices, Standard and Lessons Learned

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

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

(People – Process Technology & Other IT Resources)

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

❖ **Objectives**

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

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

are things and organization wants to accomplish.

❖ **Risks**

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

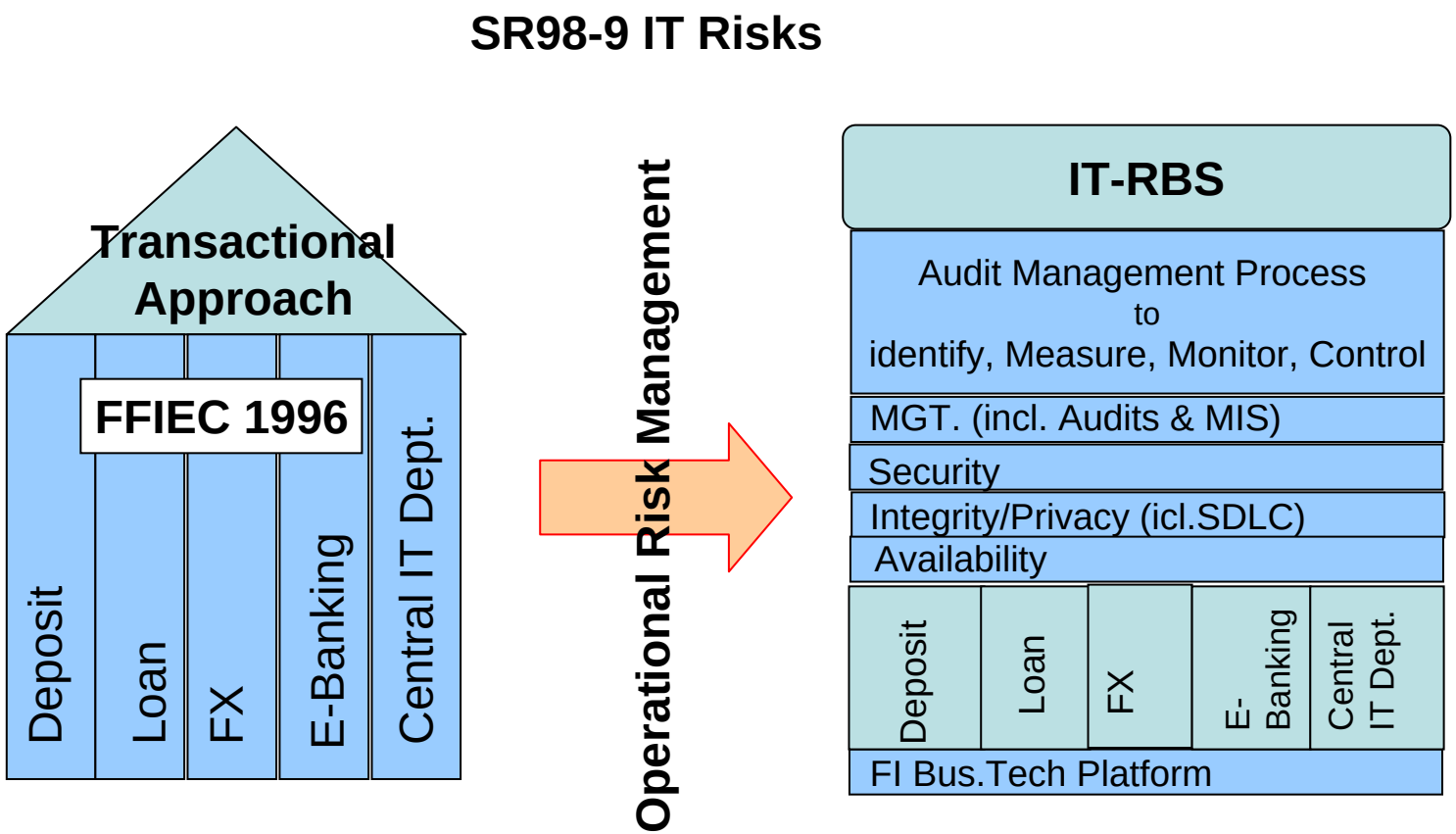
are things that might prevent accomplishing and objective.

❖ **Control**

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

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

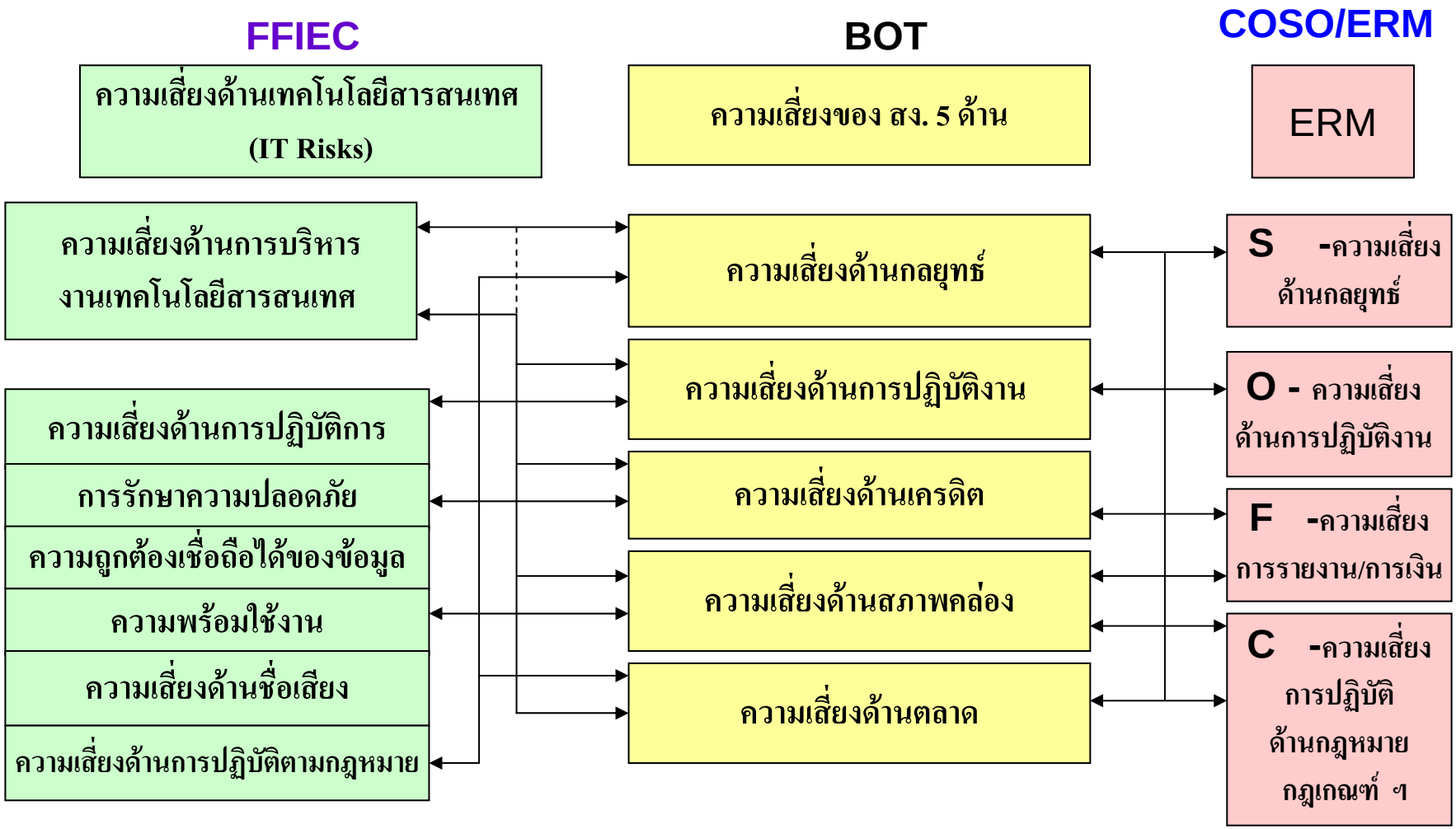
เปรียบเทียบการตรวจสอบแนวทางเดิมกับแนวทางใหม่ กับ มุมมองของ ITG&GRC เพื่อสร้างคุณค่าเพิ่มในการตรวจสอบ ให้กับ Stakeholders



ที่มา : ธนาคารแห่งประเทศไทย

IT Risks VS Risk-based Audit and Supervision/Audit

Approaches for IT Governance / GRC

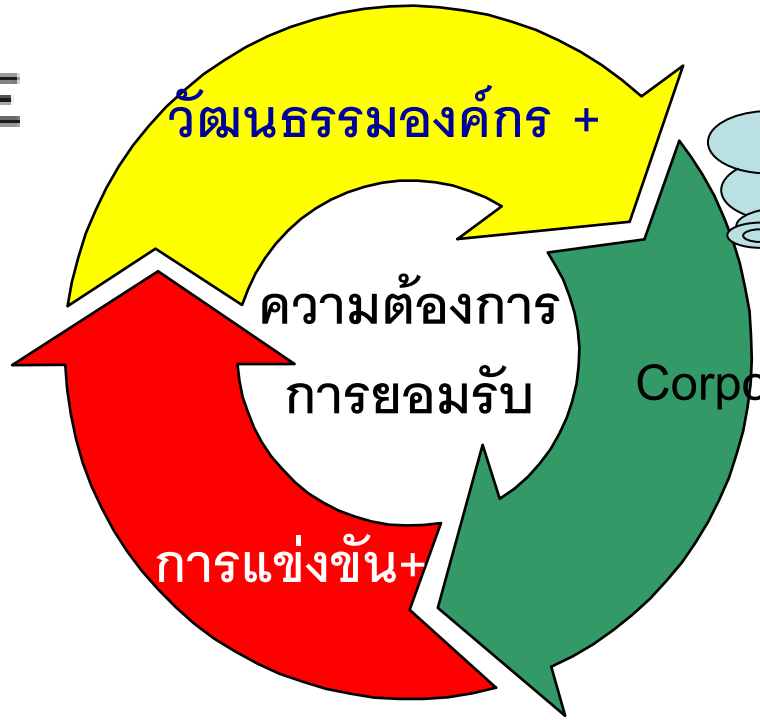


ที่มา : ปรับปรุง/ดัดแปลง จากธนาคารแห่งประเทศไทย

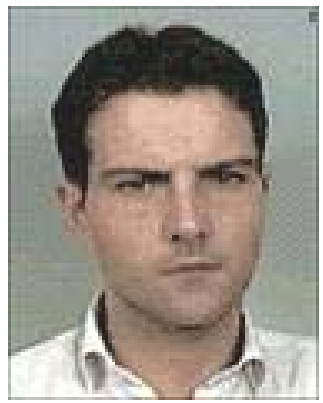
บทเรียน จากการ ทุจริต 240,000.00 ล้านบาท[us$7000ล้าน] ทางด้าน IT Risk

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

SOCIETE GENERALE



COSO/ERM
&
ITG+ISO
&
GRC+ Tools



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

ร่วมกันทบทวน กำหนด นโยบาย กลยุทธ กระบวนการทำงาน++ จากบทเรียนนี้

++ปัญหาสถาบันการเงินกับ GRC .ใน US ล่าสุด++

Changing the Internal Auditor's Paradigm

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

ที่มา : IIA Institute


การกำกับดูแลกิจการที่ดี
เพื่อการเติบโตอย่างยั่งยืนขององค์กร/รัฐวิสาหกิจ
มิติที่1 ความมั่นคงทางการเงิน&CSR
มิติที่3 กระบวนการภายใน / Business Processes
ความมั่นคงขององค์กร ที่มาจากการบริหารความเสี่ยงและการควบคุมภายใน/การตรวจสอบแบบ Cross Functional
มิติที่2 ความพึงพอใจของลูกค้า
มิติที่4 การเรียนรู้และการพัฒนา
ความเสี่ยงของ สง. 5 ด้าน
COSO-ERM
ความเสี่ยงด้านเทคโนโลยีสารสนเทศ (IT Risks)/Principle-based
ความเสี่ยงด้านกลยุทธ์
ความเสี่ยงด้านการปฏิบัติงาน
ความเสี่ยงด้านเครดิต
ความเสี่ยงด้านสภาพคล่อง
ความเสี่ยงด้านตลาด
S -ความเสี่ยงด้านกลยุทธ์
O - ความเสี่ยงด้านการปฏิบัติงาน
F -ความเสี่ยงการรายงาน/การเงิน
C -ความเสี่ยงการปฏิบัติด้านกฎหมาย กฎเกณฑ์ ฯ
ความเสี่ยงด้านการบริหารงานเทคโนโลยีสารสนเทศ
ความเสี่ยงด้านการปฏิบัติการ
การรักษาความปลอดภัย
ความถูกต้องเชื่อถือได้ของข้อมูล
ความพร้อมใช้งาน
ความเสี่ยงด้านชื่อเสียง
ความเสี่ยงด้านการปฏิบัติตามกฎหมาย
Vision & Mission ขององค์กร
แผนงานและโครงการต่าง ๆตาม SMART
KSF & KPI
การควบคุมภายในและการตรวจสอบ
การปรับปรุงและการรายงานผล
Responsibility
Accountability
Equitable Treatment
Creation of Long Term Value
Social and Environmental Awareness
Promotion of Best Practices
Transparency
บรรษัทภิบาล (CG) เป็นแก่นแท้ของการเติบโตอย่างยั่งยืนของทุกองค์กร

Q & A

การกำหนด Statement Of Direction หรือ **ทิศทางการบริหาร ของ ผู้กำกับกฎเกณฑ์ กับ องค์กรที่เกี่ยวข้อง**