การบรรยายวิชาการเรื่อง

Tools and Techniques for Enterprise Risk Management (ERM)

เรื่อง “ตัวแบบจำลอง Governance, Risk Management, and Compliance (GRC) เพื่อบริหารความเสี่ยงอย่างมีประสิทธิภาพ”

ผู้บรรยาย ผู้ช่วยศาสตราจารย์สมชาย ศุภธาดา

วันพฤหัสบดีที่ 31 มีนาคม 2554
เวลา 13:15 – 14:45 น.
ห้อง พบ. 301, 302, 307
มหาวิทยาลัยธรรมศาสตร์ ท่าพระจันทร์

จัดโดย ศูนย์วิจัยธุรกิจ
คณะพาณิชยศาสตร์และการบัญชี
มหาวิทยาลัยธรรมศาสตร์

ตัวแบบจำลอง GRC

(Governance Risk Management & Compliance)

เพื่อการบริหารความเสี่ยงอย่างมีประสิทธิภาพ

ผู้ช่วยศาสตราจารย์สมชาย ศุภธาดา

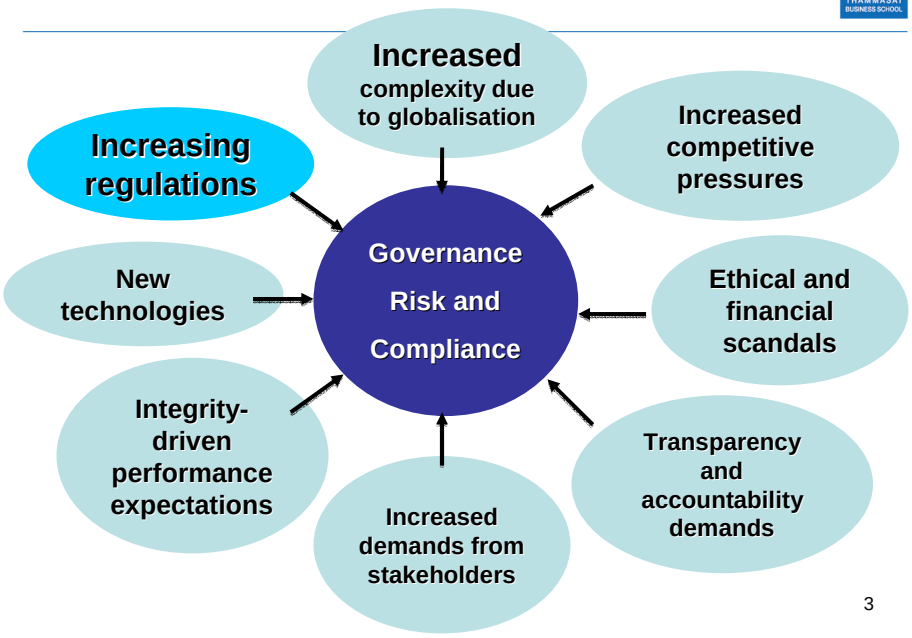
หัวหน้าภาควิชาการบัญชี

คณะพาณิชยศาสตร์และการบัญชี มหาวิทยาลัยธรรมศาสตร์

ความเป็นมาและความจำเป็น

- การบริหารปัจจุบันอยู่ภายใต้ข้อจำกัด และ มีความยากลำบากมากขึ้นจากความต้องการสารสนเทศที่เพิ่มขึ้นของ stakeholders หน่วยงานกำกับดูแล นักวิเคราะห์ และสื่อมวลชน
- การดำเนินงานเพื่อสร้างมูลค่า เป็นกิจกรรมที่**มีความเสี่ยง** **ผลกระทบจากปรากฏการณ์ "เด็ดดอกไม้สะเทือนถึงดวงดาว"** เริ่มรับรู้และรู้สึกกันได้มากยิ่งขึ้น
- การควบรวมกิจการ (M&A) ยิ่งทำให้เกิดเครือข่ายที่เชื่อมโยงและกระทบถึงกันไปหมดในเชิงปฏิกิริยาลูกโซ่
- นอกจากนั้นการกำกับดูแลยิ่งสร้างความซับซ้อนและเพิ่มมิติแห่งความเสี่ยงให้แก่กิจการ
- ***การกำกับดูแลเพื่อการบริหารความเสี่ยงในเชิงธรรมาภิบาล*** ย่อมเป็นประโยชน์ในเชิงประสิทธิภาพการดำเนินการ
- **ฝากให้ดูแล ดูแลให้ถี่ถ้วนรอบด้าน และไม่ฝ่าฝืนกฎนะ**

แรงขับเคลื่อนที่ผลักดันให้เกิด รูปแบบ GRC เชิงบูรณาการ



แรงกดดันที่ทำให้ต้องสนใจ GRC

- **Active compliance with numerous regulations**
- **Better Risk Management**
- **Improve operational management , performance and disciplines**
- **Improve accountability**
- **Align strategies to improve better results**

วิวัฒนาการของ

Governance, Risk & Compliance (GRC)

- **1962 -** Concept of risk management takes hold
- **1992 - COSO audit process**
- **1995 -** Enterprise-wide Risk management
- **2002 - Sarbanes – Oxley**
- **2004 –** COSO ERM
- **2005 - New Federal sentencing guidelines**
- **2008 - Emergence of GRC model**

5

GRC รวมอะไรบ้าง

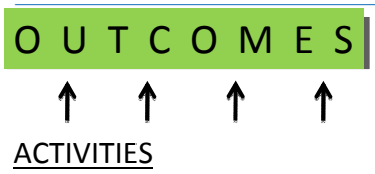
- **Governance**
- **Strategy**
- **Risk Management**
- **Audit**
- **Legal**
- **Supply Chain**
- **Business Continuity**
- **Compliance**
- **Information Technology**
- **Ethics / Corporate Responsibility**
- **Quality**
- **Human capital**

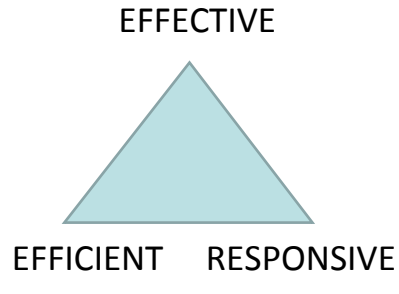
6

ความหมาย

องค์การต้องระบุ ว่า อะไร (WHAT) คือสิ่งที่ต้องการบรรลุ และ จะบรรลุวัตถุประสงค์เหล่านี้อย่างไร **(HOW)** ในขณะที่ต้องจำกัดความเสี่ยง **(RISK)** และอยู่ภายใต้ขอบเขตบางประการ **(BOUNDARIES) ของกฎระเบียบกติกา**

High-Performance





EFFECTIVE

- Design Effectiveness – Is the system is logically designed to meet legal and other defined requirements?
- Operating Effectiveness – Does the system operate as designed?

EFFICIENT

- Financial Efficiency – How much financial capital is required?
- Human Capital Efficiency – What type and level of individual(s) are required?

RESPONSIVE

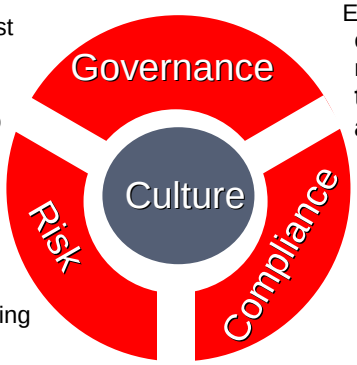
- Cycle Time – How much time does it take?
- Flexibility / Adaptability – Can the system adapt to the changing environment including new requirements and/or new business units?

Governance, Risk, and Compliance (GRC) At-a-Glance

Governance

Set and evaluate performance against objectives

Authorize business strategy & model to achieve objectives



Culture

Establish an organizational climate and individual mindset that promotes **trust, integrity, and accountability**

Risk Management

Identify, assess, and address potential obstacles to achieving objectives

Identify / address violation of mandated and voluntary boundaries

Compliance

Encourage / require compliance with established policies and boundaries

Detect non-compliance and respond accordingly

แนวคิดใหม่ของ Compliance

1.Governance :

การวางนโยบาย ดูแลวัฒนธรรม ดำเนินกระบวนการ จัดขั้นตอนการบริหารจัดการและการกำกับดูแลองค์กรเพื่อตอบสนอง **stakeholders**

2.Risk Management :

การบริหารจัดการความเสี่ยงด้าน [โอกาส **X** ผลกระทบ] ที่จะทำให้การดำเนินงานไม่เป็นไปตามเป้าหมาย วัตถุประสงค์ที่กำหนดไว้

3.Compliance :

การกำกับดูแลให้การปฏิบัติงานเป็นไปตามกฎเกณฑ์ครบถ้วน

แนวคิดใหม่ของ Compliance

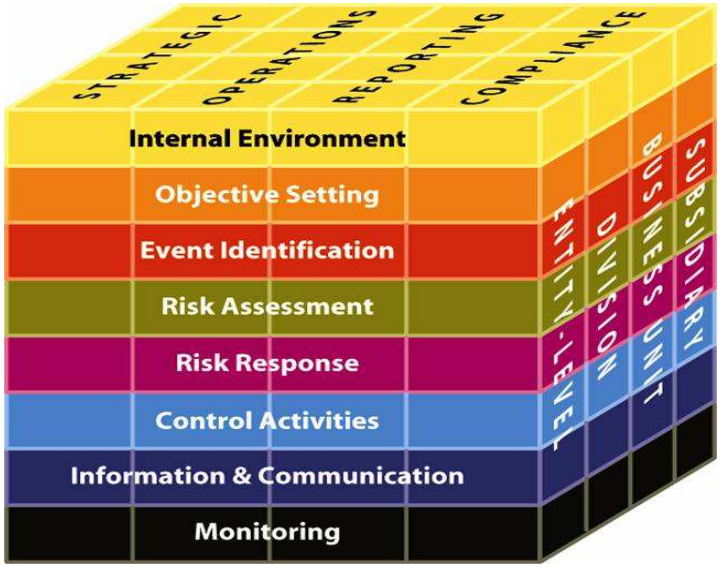
GRC =

กรอบแนวคิด

คณะกรรมการและผู้บริหารต้องจัดให้มีการบริหารการเปลี่ยนแปลง โดยเชื่อมโยงให้มีการจัดการที่ดี (Governance) เข้ากับกระบวนการบริหารความเสี่ยง (COSO – ERM) ทั่วทั้งองค์กร และการควบคุมความเสี่ยงของกิจกรรมต่าง ๆ ในลักษณะเชิงรุก คือ การป้องกันปัญหาที่อาจเกิดขึ้นและกระทบกับการสร้างคุณค่าเพิ่มอย่างมีประสิทธิภาพให้กับองค์กร

Governance	Risk	Compliance
Policy and Procedure Management	Risk assessment	Compliance Management
Document Management	Accident and Incident Management	Fraud
Internal Audit		Continuous Control Monitoring
Training		
BUSINESS PROCESS MANAGEMENT		
REPORTING AND ANALYSIS		

COSO 2 : ERM



	GRC	COSO 2 Model
KEY LINKAGES	*Governance*	**Objective and Risk Appetite**
	Risk management	
	Risk management	**Risk Response and Control Activities**
	Compliance	

องค์ประกอบ GRC และ ผู้ที่มีส่วนเกี่ยวข้อง

1.การกำกับดูแลกิจการ	คณะกรรมการ
2.การกำหนดกลยุทธ์	ฝ่ายจัดการ CEO
3.การบริหารความเสี่ยง	RMC, CRO
4.การตรวจสอบ	CAE , Audit Com. , Audit Firm
5.การกำกับกฎหมาย	ที่ปรึกษา ฝ่ายกฎหมาย
6.การกำกับการปฏิบัติตามกฎเกณฑ์	ที่ปรึกษา CCO CMC

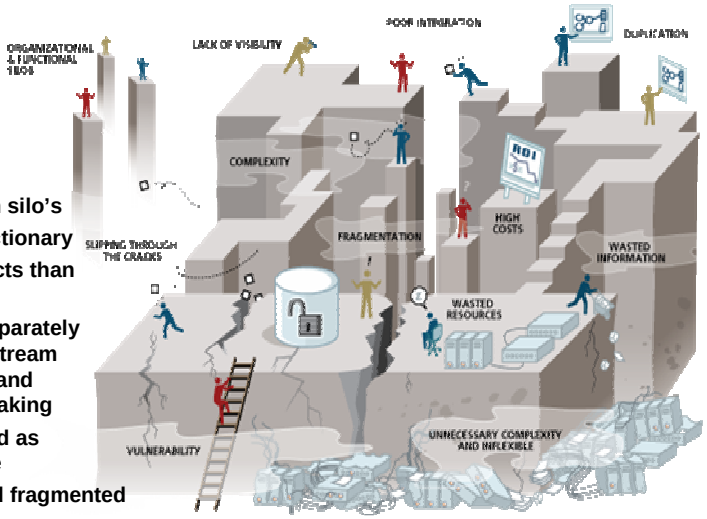
องค์ประกอบ GRC และ ผู้ที่มีส่วนเกี่ยวข้อง

7. IT Governance	CIO, ITCom.
8.ความรับผิดชอบทางสังคม จรรยาบรรณ	C Ethical Officer, CREO
9. การบริหารคุณภาพ	Quality Professionals ทั่วทั้งองค์กร
10 .การกำกับบุคลากร	คณะกรรมการแรงงานสัมพันธ์ ฝ่ายพนักงาน

Transformational Opportunity

Current State

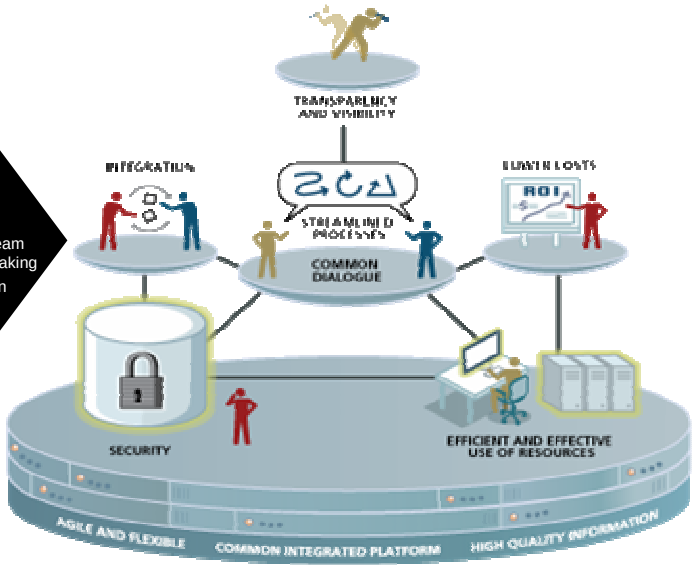
- **Managed in silo's**
- **Mostly reactionary**
- **More projects than programs**
- **Handled separately from mainstream processes and decision-making**
- **People used as middleware**
- **Limited and fragmented use**



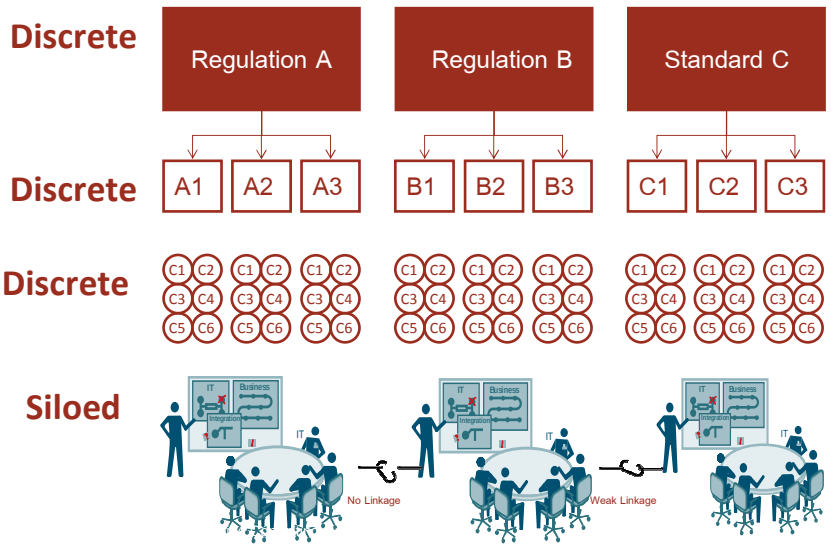
Transformational Opportunity

Future State

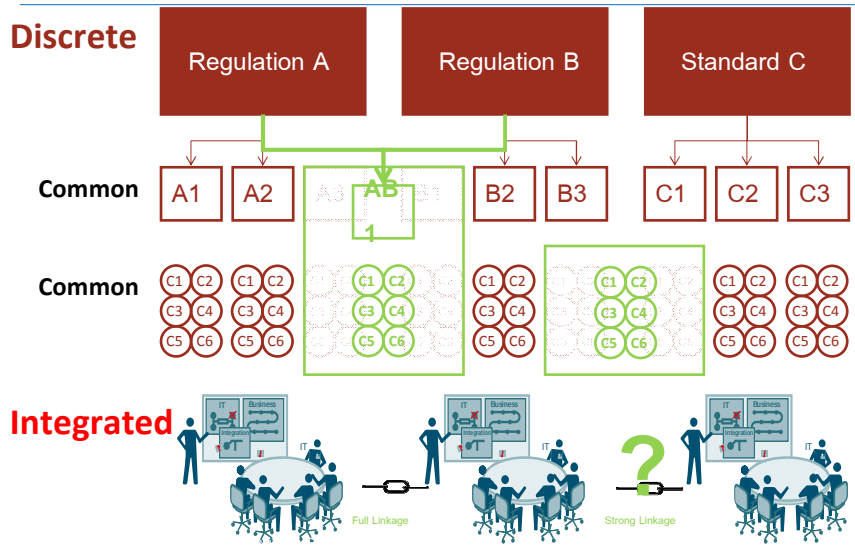
- Enterprise approach
- Integrated GRC
- Program based approach
- Embedded within mainstream processes and decision-making
- Effective use of information technology
- Architected solutions



แทนที่จะทำอย่างนี้

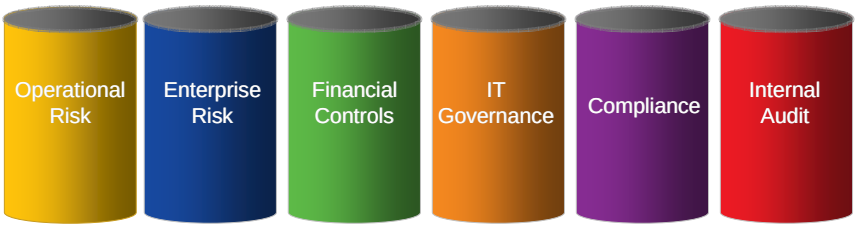


ให้ทำเชิง บูรณาการ แทน



สถานการณ์ปัจจุบัน

- **Major assurance functions currently operate in isolated silos**



- <u>ความท้าทาย</u>
  - **Lack of a common language for risk and control**
  - **No common methodology**
  - **Redundant systems and processes**
  - **Poor visibility and reporting**

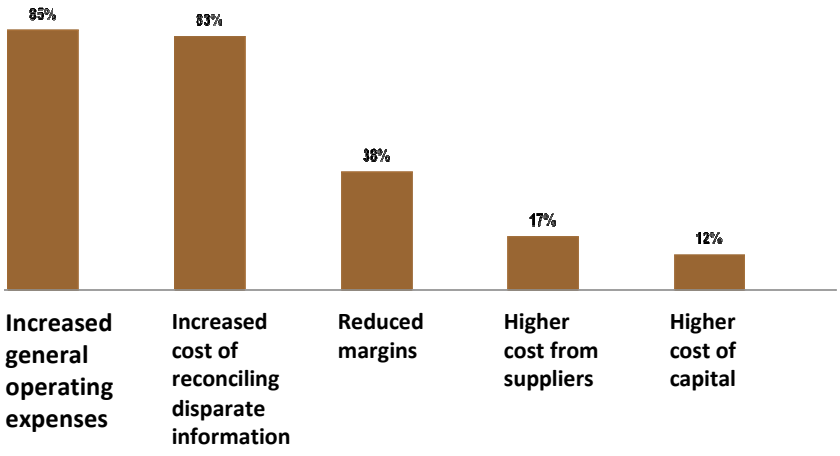
GRC : IT controls and Understanding

- Classification
  - **General controls**
  - **Application controls**
- Classification
  - **Preventive**
  - **Detective**
  - **Corrective**
- Classification
  - **Governance controls**
  - **Management controls**
  - **Technical controls**

ข้อมูลที่เกี่ยวข้องกับ IT GRC สามารถแวะเยี่ยมชมได้ที่

- IT Policy Compliance Group Research Center **(http://www.itpolicycompliance.com/research_reports/)**
- IT GRC Maturity Model Assessment Tool **(http://www.itpolicycompliance.com/interactive-tools/maturity-app.asp)**
- ITPCG Blog (http://itpcg.wordpress.com/)
- Wikipedia: GRC **(http://en.wikipedia.org/wiki/Governance%2C_Risk_Management%2C_and_Compliance)**

Adverse Impact of a Fragmented Approach



Source: 2007 OCEG Benchmark Series: GRC Strategy Study

A PRAGMATIC VIEW OF "GRC"

ไม่ใช่

- A discrete process, technology, or profession
- Organizational department
- A single technology solution
- ERM
- The solution to all audit, risk and compliance problems

ใช่

- A common discipline to be embraced across silos
- Collaboration between departments
- Purpose built solutions sharing a common framework
- Context for ERM
- Pursuit for improving audit, risk and compliance processes

10 ขั้นตอนในการ implement GRC

1. ประสานงาน coordinate GRC functions
2. ร่วมอภิปรายกับผู้บริหารและคณะกรรมการ
3. ระบุโอกาสแรกเริ่ม identify initial opportunities
4. พัฒนาแผนโครงการแรกเริ่ม
5. ร่างนโยบายความเสี่ยง draft a risk policy
6. เริ่มปฏิบัติการตามแผนโครงการแรกเริ่ม
7. ทบทวน vision และ แผนโครงการ
8. สรุปนโยบายความเสี่ยงของ คณะกรรมการ
9. อนุมัตินโยบายความเสี่ยงและ โครงสร้าง GRC
10. เริ่มปฏิบัติการตามแผนโครงการขั้นสุดท้าย

THE FIVE POINTS OF **GRC COLLABORATION**

1. **Shared context: Organization and process structure**
2. **Common language of risk and control**
3. **Common methodology**
4. **Enterprise-wide reporting**
5. **GRC convergence technology**

1. SHARED CONTEXT & ORGANIZATIONAL STRUCTURE

- **The context must reflect the organization and how value is added – not what is being audited**:
  - The organization and its key components, relationships and capabilities
  - The business processes reflecting how value is added
- All context information is shared. Everyone knows what everyone knows.

Organizational Structure
- o Business unit
- o Legal entity
- o Geographic area
- o Country
- o Product line
- o Service line
- o IT assets

Process Hierarchy
- o Mega process
- o Major Process
- o Process
- o Sub-process

2. COMMON LANGUAGE OF RISK AND CONTROL

… during the 1700's, European naturalists began collecting thousands of specimens of newly discovered species during voyages to Africa, Asia and America. This influx of new species led to the systemization of naming conventions and methodologies for reporting findings. Without standard naming conventions or scientific methodologies, scientists from different disciplines would have no way of sharing discoveries and compiling knowledge.

Charles Darwin

… **during the early 20th century, assurance specialists identified thousands of (SOX and other) risks, controls, issues and action plans …**

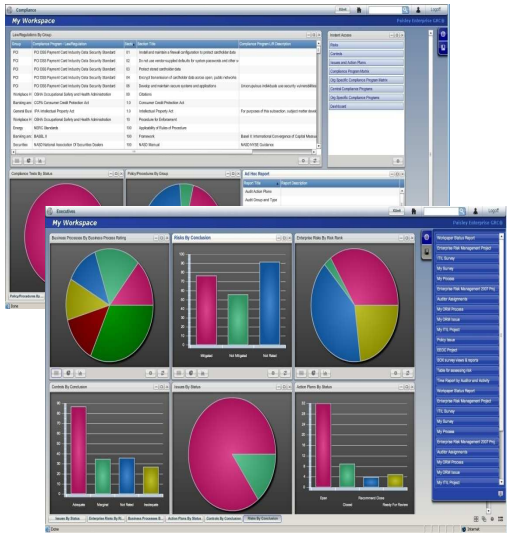
3. COMMON METHODOLOGY

Common methodology exists when silos share each others work and build on it

- Defining, rating and reviewing the risk and control framework of an organization is consistent not only within a particular assessment group but also across groups.
- Assurance groups are not duplicating
- Process owners are not inappropriately burdened by multiple or even conflicting directives from the various assurance groups or their senior management.

4. ENTERPRISE WIDE REPORTING

- Compare trends across the organization over time
- Compare business units at a point in time
- Compare one company to another
- Improve ERM scores by rating agencies – lower costs
- Fewer crises, more stability, higher multiples



5. GRC TECHNOLOGY

- Effectively blend the Compliance function with the various business functions across the organization to create efficiencies by:
  - Knocking down the walls between departments and minimizing cross functional boundaries to reveal that governance-related functions touch all business areas
  - Encouraging business managers to realize a collective responsibility for Compliance requirements

ความคาดหวังของผู้บริหารระดับสูง

- **เป็นเรื่องของทุกคนที่ต้องเข้ามามีส่วนร่วม**
- **การเดินทางของทุกคนด้าน GRC ไม่ใช่เรื่องของปีหรือสองปีแต่เป็นพันธกิจที่จะต้องดำเนินการพัฒนาตนเอง (self improvement) ขึ้นไปเรื่อย ๆ อย่างไม่มีที่สิ้นสุด**

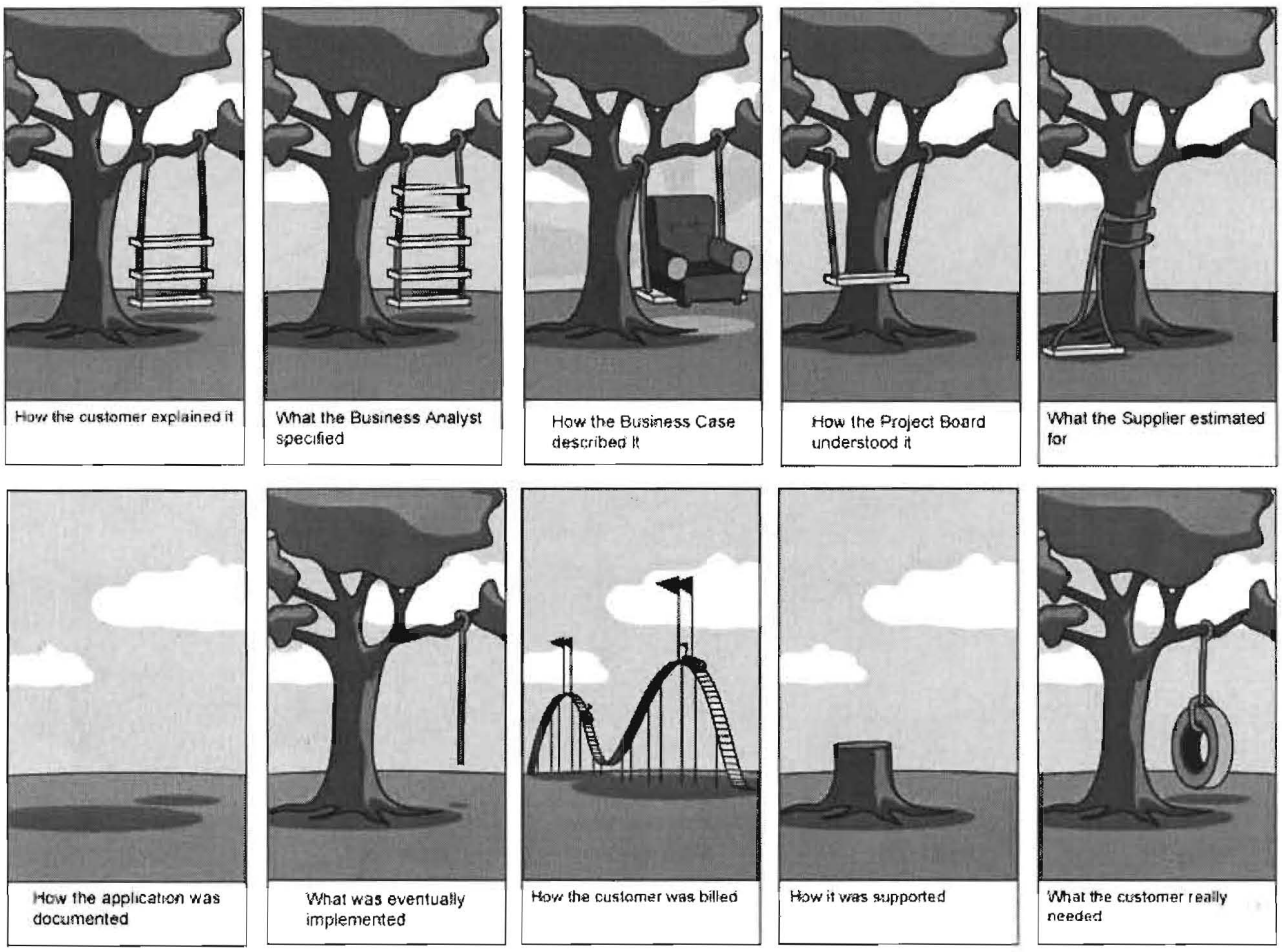
ความคาดหวังของผู้บริหารระดับสูง

- **ต้องลงทุนด้านโครงสร้างพื้นฐานและระบบงานเป็นเงินจำนวนมาก** ซึ่งในหลายองค์กรมองว่าเงินลงทุนเพื่อซื้อการยอมรับว่าองค์กรมี **GRC** ค่อนข้างแพง และมีภาระต้องบำรุงรักษาและบริหารจัดการสารสนเทศที่เป็นผลลัพธ์ของกระบวนการ **GRC** อีกมากมายรวมทั้งเสียสละเวลากับการนี้ไปมาก **จึงต้องการความคุ้มค่าของการลงทุนดังกล่าวด้วย และทุกคนต้องเลิกมองกระบวนการของ GRC ว่าเป็นเรื่องเฉพาะกิจหรือเฉพาะกาล**
- **เป็นความท้าทายของ CRO หรือ CIO หรือคณะกรรมการตรวจสอบแล้วแต่ว่าใครจะได้รับการมอบหมายความรับผิดชอบ**

ฝากท้าย

- **หลายคนคิดที่จะเปลี่ยนโลก แต่ไม่ค่อยมีใครคิดที่จะเปลี่ยนแปลงตัวเอง** (ลีโอ ตอล์สตอย)
- สำหรับ GRC ต้องการคิด
  - **ให้ลึกเชิงวิเคราะห์** Analytical
  - **ให้กว้างอย่างสร้างสรรค์** Creative
  - **ในภาพรวมทั้งระบบ** Systematic
  - **ให้ครบจนจบความ** Integrative

[เอกสารส่วนที่ 1 >>> รูป แผนภูมิ ภาพ ประกอบ GRC Model]



Fraud on the Rise

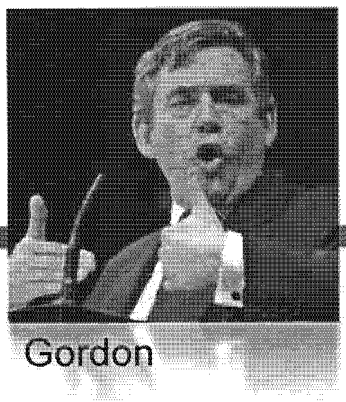
Societe Generale lost €6.3B as Jerome Kerviel went rogue

B. Ramalinga Raju reveals falsifying $1B Corp. account

Siemens agrees to pay $1.3B in bribery settlement

Fannie Mae IT contractor indicted for planting malware

Call for Increased Regulatory Scrutiny



AMERICAS

- HIPAA
- FDA CFR 21 Part 11
- OMB Circular A-123
- SEC and DoD Records Retention
- USA PATRIOT Act
- Gramm-Leach-Bliley Act
- Federal Sentencing Guidelines
- Foreign Corrupt Practices Act
- Market Instruments 52 (Canada)

EMEA

- EU Privacy Directives
- UK Companies Law
- Restriction of Hazardous Substances (ROHS/WEE)

GLOBAL

- International Accounting Standards
- Basel II (Global Banking)
- OECD Guidelines on Corporate Governance

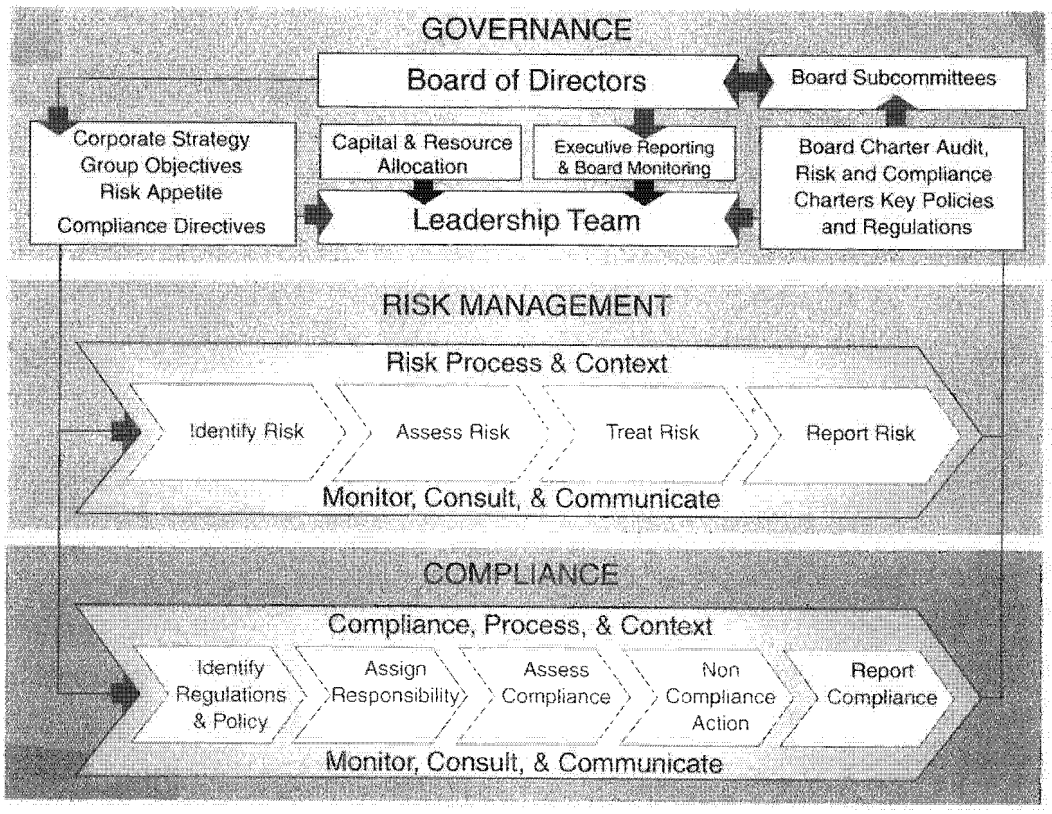
APAC

- J-SOX, C-SOX, K-S0X, C49
- CLERP 9: Audit Reform and Corporate Disclosure Act (Australia)
- Stock Exchange of Thailand Code on Corporate Governance

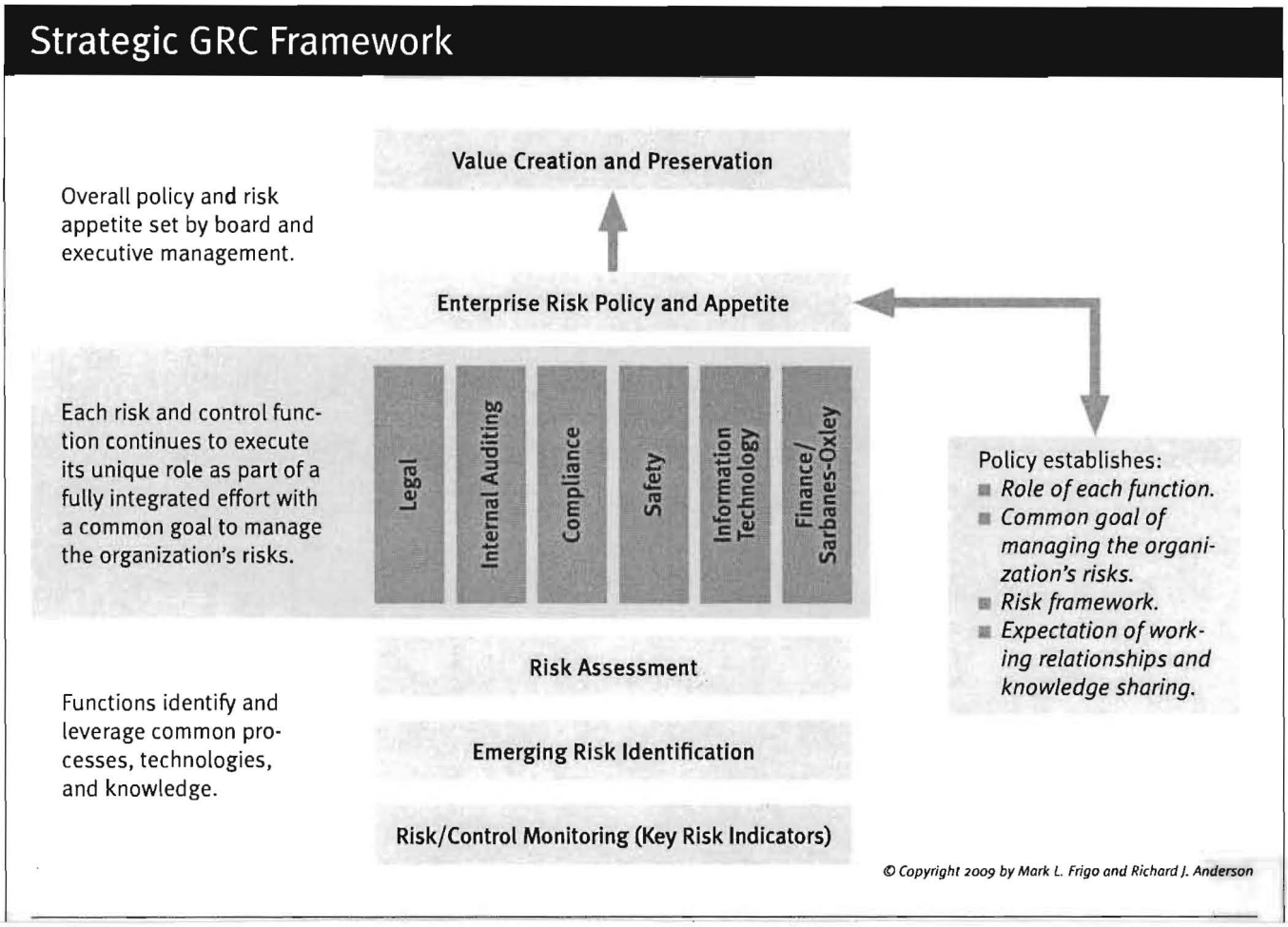
But first, a brief explanation of terms:

- **Governance**
  Running a business based on clear and understandably formulated business objectives and instructions. Important conditions are legal compliance and completeness. Governance thus extends across all business sectors and levels, which is why we speak of horizontal and vertical governance.
- **Risk Management**
  The sum of all measures for dealing with known and unknown internal and external risks. This includes the establishment of early warning systems to identify risks as well as measures to eliminate potential risks and to deal with occurred risks.
- **Compliance**

  Refers to the fulfillment, correspondence or conformity with state laws and with rules and specifications, with principles (ethical and moral) and procedures as well as with standards (e.g. ISO) and conventions that are clearly defined. The compliance can be fulfilled either by means of coercion (e.g. by law) and/or voluntarily (e.g. adherence to standards).



A sample governance, risk, and compliance operating model



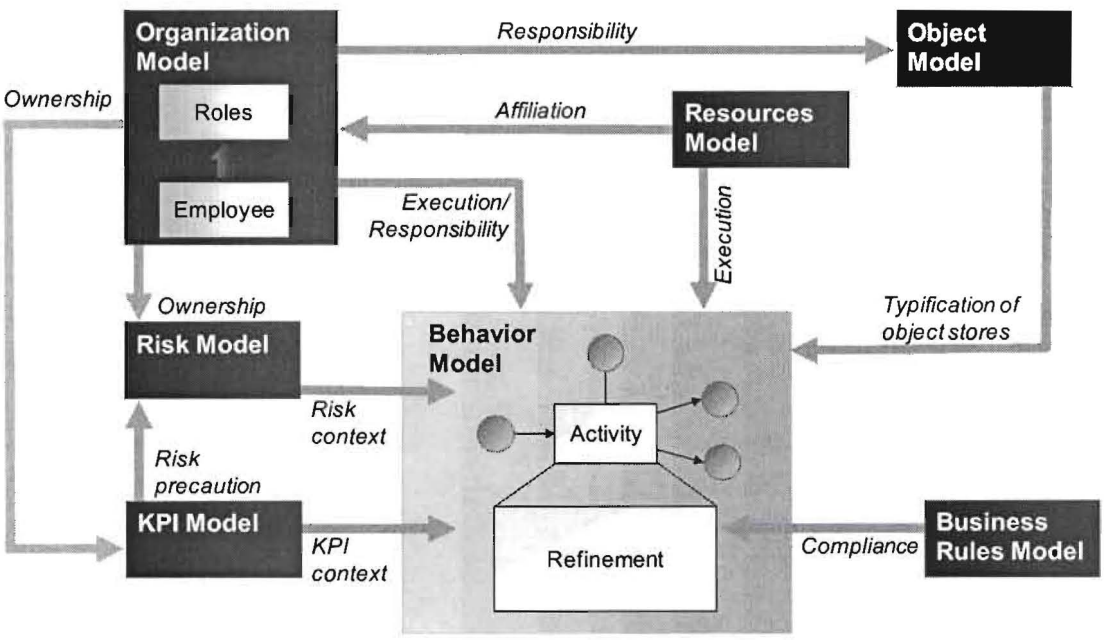
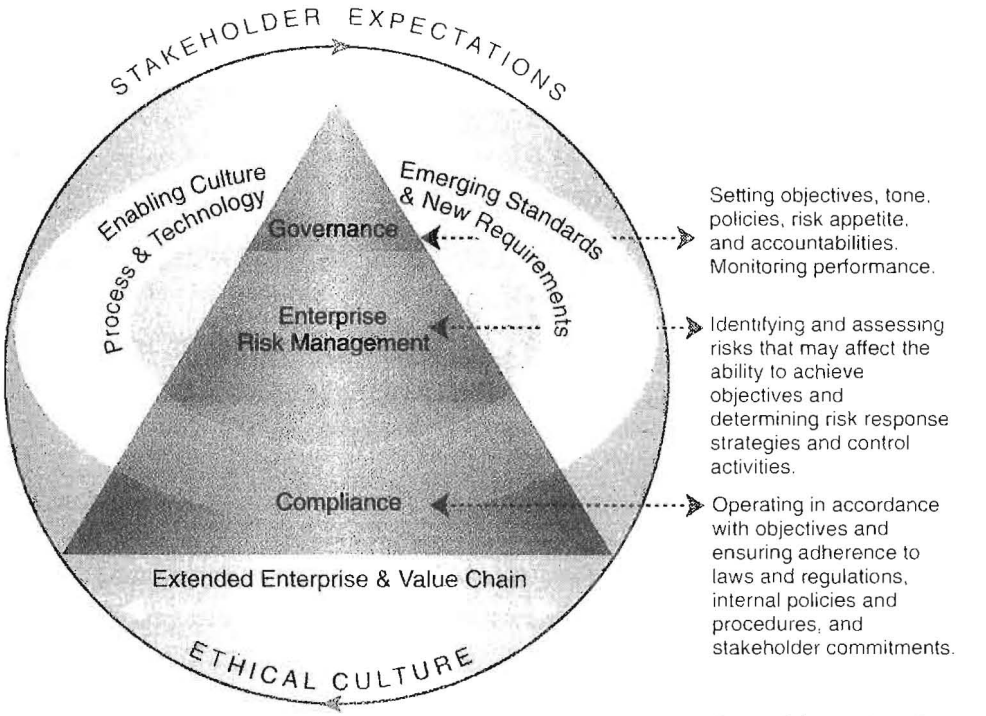
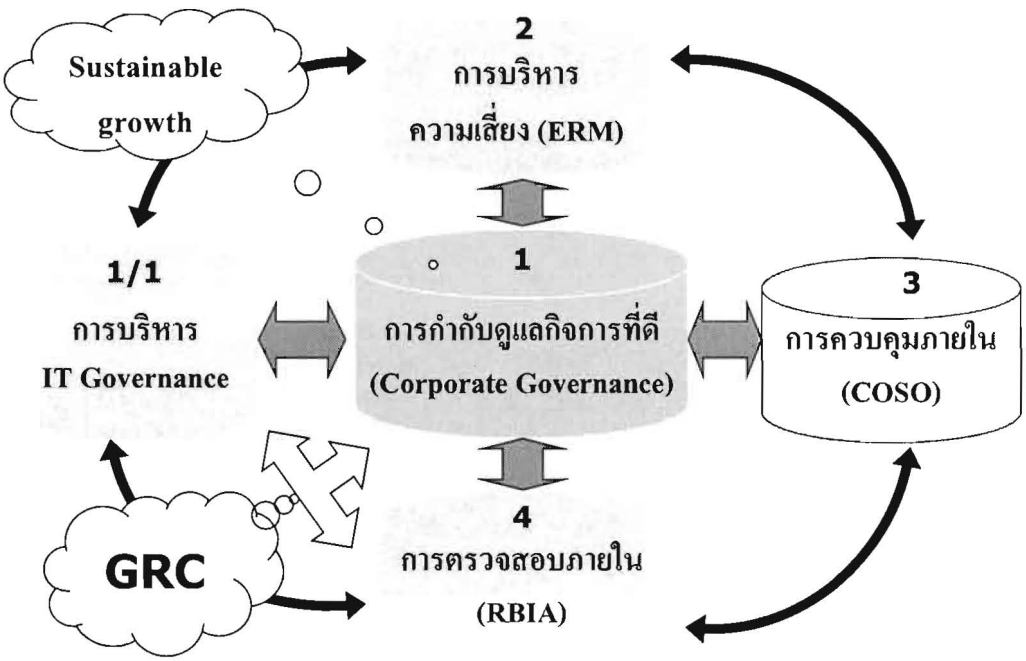


Figure. 1: Integrated business model without "information islands"



Integrating governance, risk, and compliance



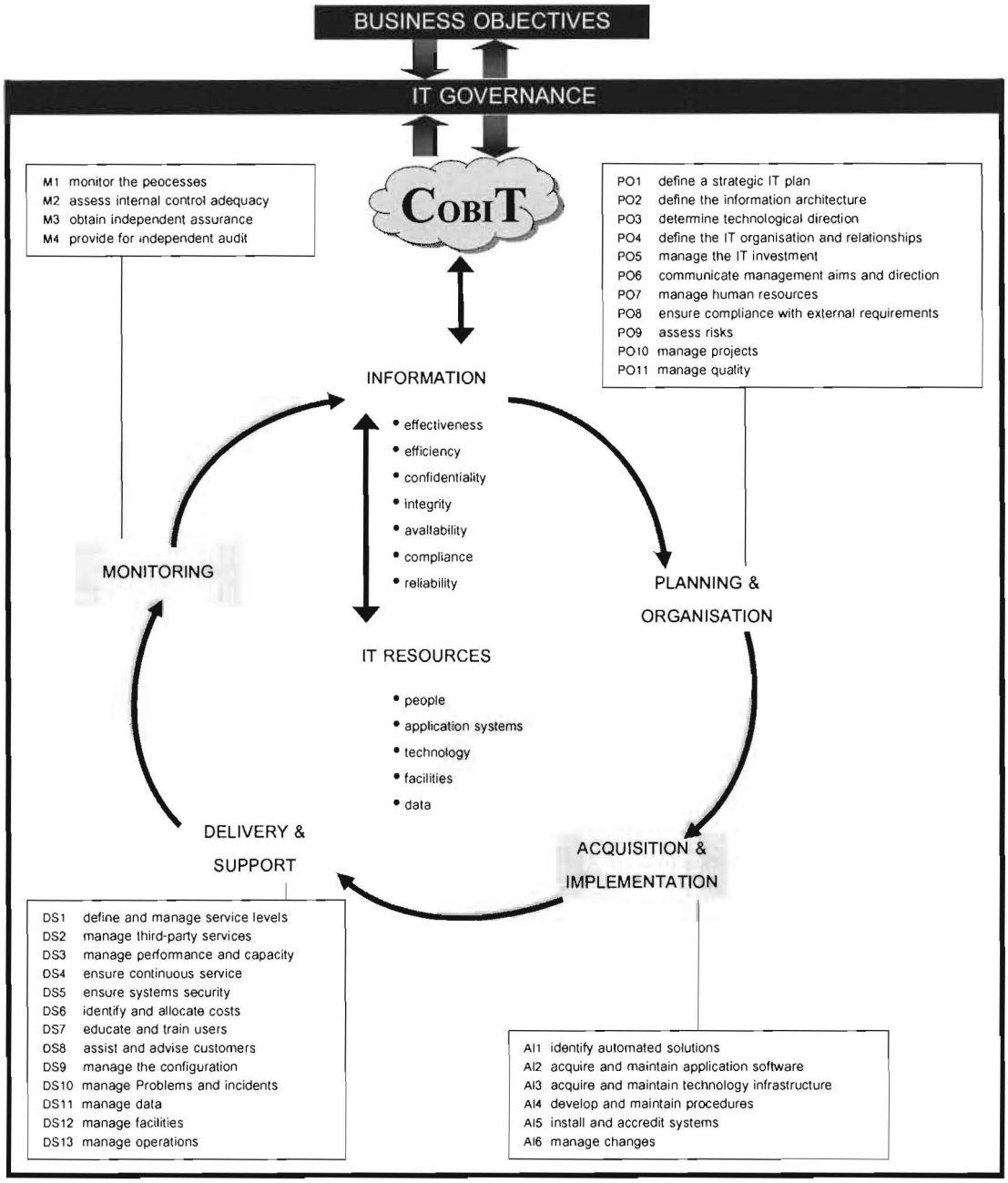
COBIT

มาตรฐาน COBIT เป็นทั้งแนวคิดและแนวทางการปฏิบัติ (Framework) เพื่อการควบคุมภายในที่ดีด้านเทคโนโลยีสำหรับองค์กรต่างๆ ที่จะใช้อ้างอิงถึงแนวทางการปฏิบัติที่ดี (Best Practice) ซึ่งสามารถนำไปปรับใช้ได้ในทุกองค์กรสำหรับกิจกรรมที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ โดยโครงสร้างของมาตรฐาน COBIT ได้ออกแบบอยู่บนพื้นฐานของกระบวนการทางธุรกิจ Business Process สามารถแบ่งได้เป็น 4 กระบวนการหลัก (Domain) ได้แก่

- การวางแผนและการจัดการองค์กร (PO : Planning and Organization)
- การจัดหาและติดตั้ง (AI : Acquisition and Implementation)
- การส่งมอบและบำรุงรักษา (DS : Delivery and Support)
- การติดตามผล (M : Monitoring)

ในแต่ละกระบวนการหลักข้างต้น มาตรฐาน COBIT แสดงวัตถุประสงค์ของการควบคุมหลัก (High-level Control Objectives) รวมถึง 34 หัวข้อ และในแต่ละหัวข้อจะประกอบด้วยวัตถุประสงค์ของการควบคุมย่อยลงไปอีกขั้นหนึ่ง (Detailed Control Objectives) รวมถึง 318 หัวข้อย่อย พร้อมทั้งแนวทางการตรวจสอบ (Audit Guidelines) สำหรับแต่ละหัวข้ออีกด้วย

กรอบมาตรฐาน COBIT



ที่มา : www.isaca.org, www.itgi.org

ITIL

แสดงส่วนประกอบของ ITIL

มาตรฐาน ITIL นั้น เป็นมาตรฐานด้านความปลอดภัยจากประเทศอังกฤษ มีวัตถุประสงค์ในการสร้าง Best Practices สำหรับกระบวนการของ IT Service Delivery และ Support แต่ไม่ได้เป็นการกำหนด Framework ของการควบคุมในแนวกว้าง ITIL นั้นจะมุ่งไปทางการเสนอวิธีการในการปฏิบัติ แต่มีขอบเขตงานเพียงแค่ IT service Management และมีความลึกในรายละเอียดของกระบวนการทำงาน ซึ่งมีวัตถุประสงค์ที่จะให้ทางฝ่ายระบบสารสนเทศ และ Service Management เป็นผู้นำไปใช้ ซึ่งได้จัดแบ่งกระบวนการเทคโนโลยีสารสนเทศ ดังนี้

- *Security Management* เป็นการบริหาร IT โดยการสร้างข้อกำหนด ตรวจสอบผล และควบคุมรักษาความปลอดภัยของระบบด้านข้อมูล และบริการขององค์กรเมื่อมีผู้เกี่ยวข้องเข้าสู่ระบบเทคโนโลยีสารสนเทศ
- *Change Management* คือ การบริหารการเปลี่ยนแปลงเพื่อก่อให้เกิดความเชื่อมั่นใน IT ขององค์กร ซึ่งมีการใช้วิธีการปฏิบัติและกระบวนการที่มีมาตรฐานเพื่อที่จะจัดการกับการเปลี่ยนแปลงของสภาพแวดล้อมของระบบบน Production เพื่อที่จะลดผลกระทบจากปัญหาเนื่องจากการเปลี่ยนแปลงเพื่อพัฒนาคุณภาพของบริการ

- *Release Management* เป็นการบริหารกระบวนการนำระบบออกให้ผู้ใช้สามารถใช้ระบบงานต่างๆ ได้ โดยเริ่มต้นจากการวางแผนเพื่อนำระบบออกใช้ เตรียมเอกสารของระบบเผยแพร่ และการจัดอบรมให้แก่ลูกค้า เพื่อให้เกิดความมั่นใจในระบบเทคโนโลยีสารสนเทศที่พัฒนาขึ้น
- *Incident Management* หรือเรียกว่า Help Desk หรือ Service Desk เป็นกระบวนการแก้ไขระบบให้สามารถกลับมาใช้งานได้ปกติ ซึ่งจะแก้ไขก็ต่อเมื่อมีการแจ้งปัญหาจากลูกค้า หรือผู้ใช้งาน โดย IT จะต้องจัดการแก้ไขปัญหาที่เกิดขึ้นดังกล่าวให้เสร็จสิ้นเร็วที่สุด เพื่อให้กระทบกับผู้เกี่ยวข้องน้อยที่สุด
- *Problem Management* เป็นบริหาร IT โดยการคิดเชิงรุก (Proactive) เพื่อลดปัญหาของระบบที่เกิดจากการแจ้งของผู้ใช้งาน มุ่งเน้นการวิเคราะห์ไปที่ต้นเหตุของปัญหา รวมถึงการควบคุมความผิดพลาดที่อาจเกิดขึ้นในอนาคต ซึ่งมักจะเป็นการดำเนินการระยะยาว
- *Service-Level Management* คือการบริหารการให้บริการระบบเทคโนโลยีสารสนเทศอย่างเหมาะสม และเป็นไปตามความต้องการของลูกค้า หรือผู้ที่มีส่วนเกี่ยวข้องในระบบด้านต่างๆ โดย IT สามารถให้คำมั่นในการดำเนินงานเพื่อการบริการที่มีศักยภาพแก่ลูกค้าได้
- *Availability Management* เป็นการบริหารระบบเทคโนโลยีสารสนเทศ เพื่อแสดงเปอร์เซ็นต์ความถูกต้องของข้อมูลจากระบบต่างๆ ที่องค์กรบริการแก่ลูกค้า โดยเจ้าหน้าที่เทคโนโลยีสารสนเทศมีหน้าที่ในการกำหนดลักษณะการใช้งาน ตรวจสอบการเข้าสู่ระบบของลูกค้าและควบคุมการบริการให้เกิดประสิทธิภาพสูงสุดแก่ลูกค้า
- *Configuration Management* เป็นกระบวนการของการวางแผนเพื่อรองรับการบริหารการเปลี่ยนแปลง ซึ่งจะเป็นการกำหนด ควบคุม และตรวจสอบความถูกต้องของ Configuration Item หรือ CI ให้มีความทันสมัยและถูกต้องอยู่เสมอ