RISK MANAGEMENT SPECIALIST (RMS)

นักบริหารความเสี่ยงมืออาชีพ

TRISACADEMY
of Management

ISO 31000 & COBIT

ผศ. ดร. พรเทพ อนุสสรนิติสาร

ที่ปรึกษาสถาบันวิทยาการจัดการ ทริส คอร์ปอเรชั่น

22 May 2014

Risk Management Basics

Organizational objectives are influenced by internal and external factors which create uncertainty in achieving those objectives. The effect of this uncertainty is "risk" to the organization's objectives.

Unlike *Risk Elimination* (approach of military and law enforcement) which seeks to remove all risk; *Risk Management* is the coordinated activities to direct and control an organization with regard to risk.

Risk Management allows for multiple risk responses dependent upon evaluation and analysis of risk.

RISK = Negative IMPACT to objectives X LIKELIHOOD of occurrence.

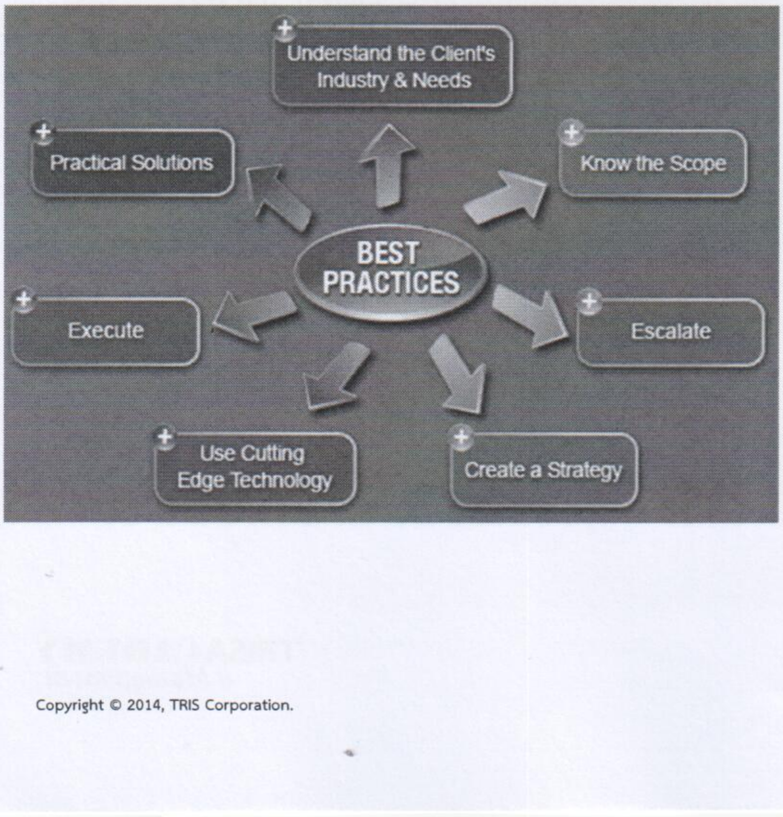
TRISACADEMY
of Management

Basic Responses to Risk

Risk Responses: ลดผลกระทบ

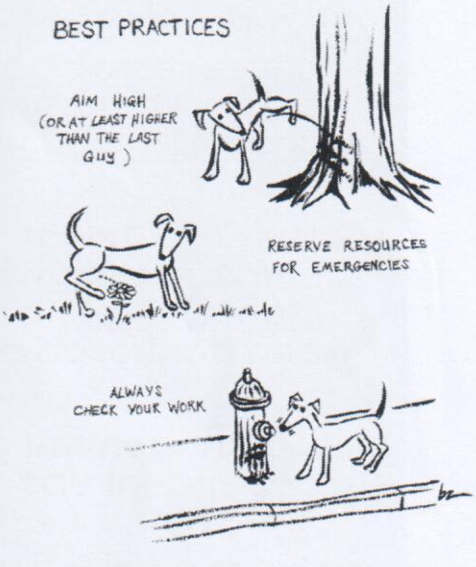
1. **MITIGATE** - corrective action to eliminate or reduce IMPACT or LIKELIHOOD
2. **AVOID** - Cease activity to eliminate risk
3. **TRANSFER** - Shift IMPACT to another entity ที่ปรึกษา, ผู้รับเหมา
4. **ACCEPT** - No corrective action. Document acceptance decision and monitor

Best Practice

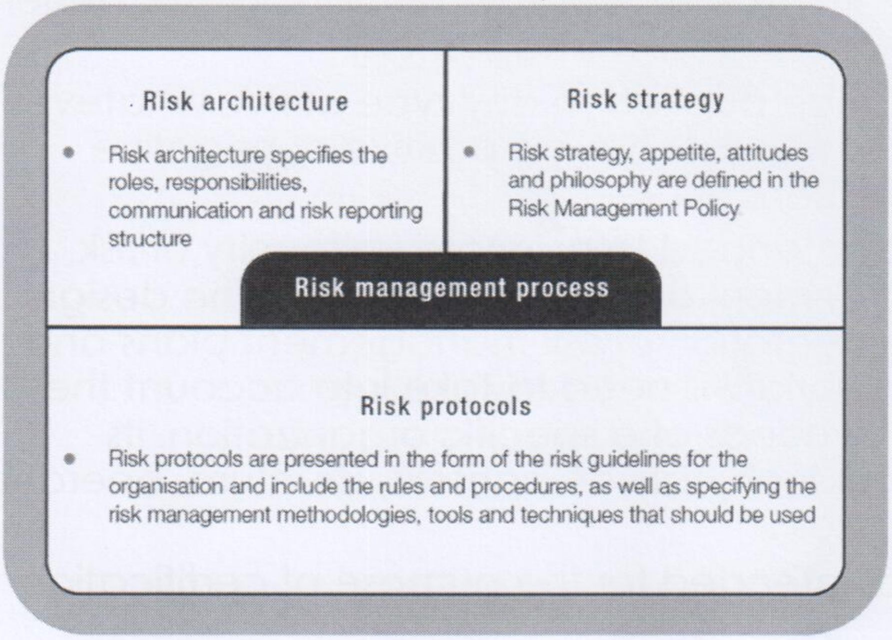


BEST PRACTICES

- Understand the Client's Industry & Needs
- Know the Scope
- Escalate
- Create a Strategy
- Use Cutting Edge Technology
- Execute
- Practical Solutions


BEST PRACTICES
AIM HIGH (OR AT LEAST HIGHER THAN THE LAST GUY)
RESERVE RESOURCES FOR EMERGENCIES
ALWAYS CHECK YOUR WORK

ISO 31000: Framework components



Risk architecture

- Risk architecture specifies the roles, responsibilities, communication and risk reporting structure

Risk strategy

- Risk strategy, appetite, attitudes and philosophy are defined in the Risk Management Policy

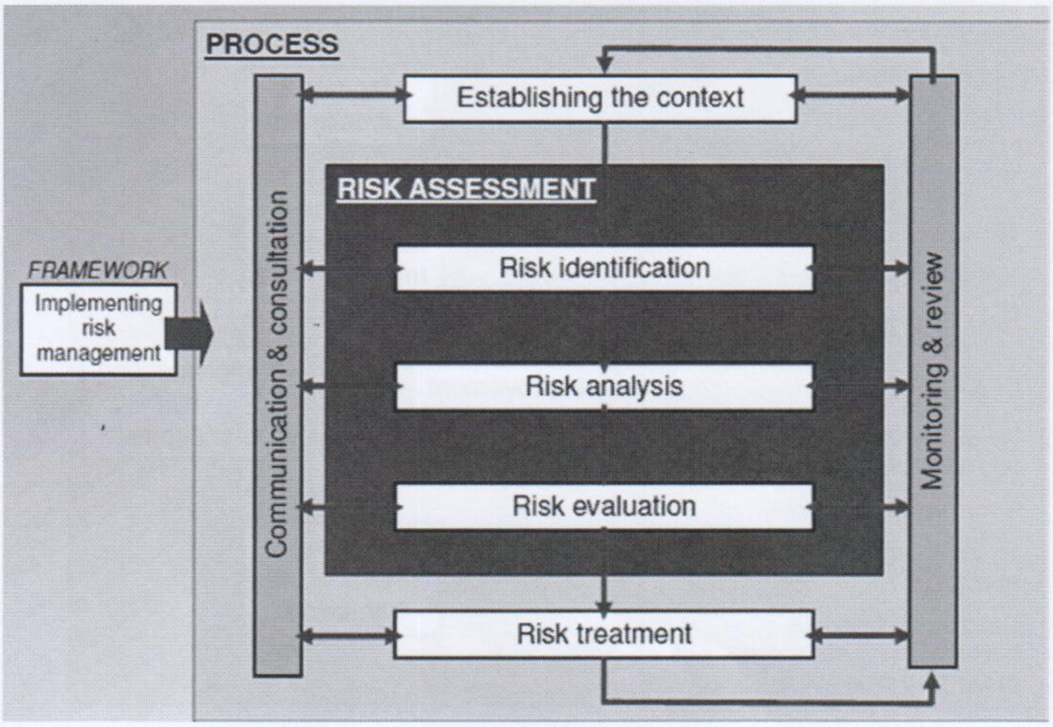
Risk management process

Risk protocols

- Risk protocols are presented in the form of the risk guidelines for the organisation and include the rules and procedures, as well as specifying the risk management methodologies, tools and techniques that should be used

TRIS ACADEMY of Management

ISO 31000: Process



PROCESS

Establishing the context

RISK ASSESSMENT

Risk identification

Risk analysis

Risk evaluation

Risk treatment

Communication & consultation

Monitoring & review

FRAMEWORK

Implementing risk management

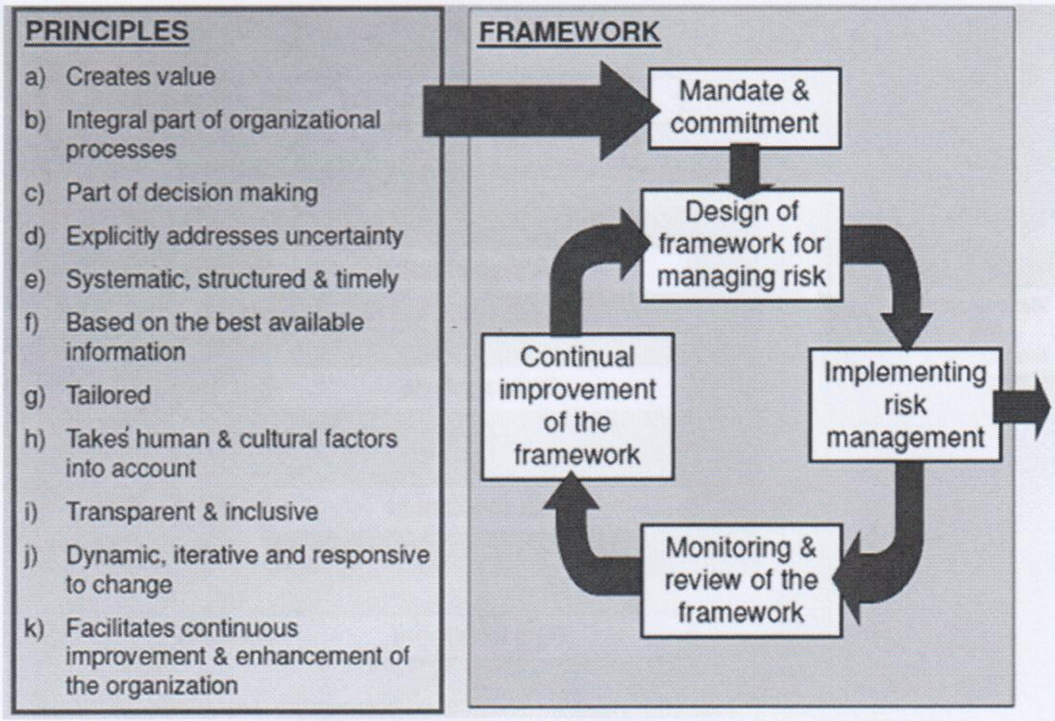
TRIS ACADEMY of Management

ISO 31000: Risk Management – Principles & Guidelines

- Published in 2009, to provide "principles & generic guidelines on risk management"
- "...can be applied to any type of risk, whatever its nature, whether having positive or negative consequences"
- "...not intended to promote uniformity of risk management across organizations. The design and implementation of risk management plans and frameworks will need to take into account the varying needs of a specific organization, its particular objectives, context, structure, operations, processes,.."
- "...not intended for the purpose of certification"

TRISACADEMY *of Management*

ISO 31000: Principles & Framework



PRINCIPLES

a) Creates value
b) Integral part of organizational processes
c) Part of decision making
d) Explicitly addresses uncertainty
e) Systematic, structured & timely
f) Based on the best available information
g) Tailored
h) Takes human & cultural factors into account
i) Transparent & inclusive
j) Dynamic, iterative and responsive to change
k) Facilitates continuous improvement & enhancement of the organization

FRAMEWORK

Mandate & commitment

Design of framework for managing risk

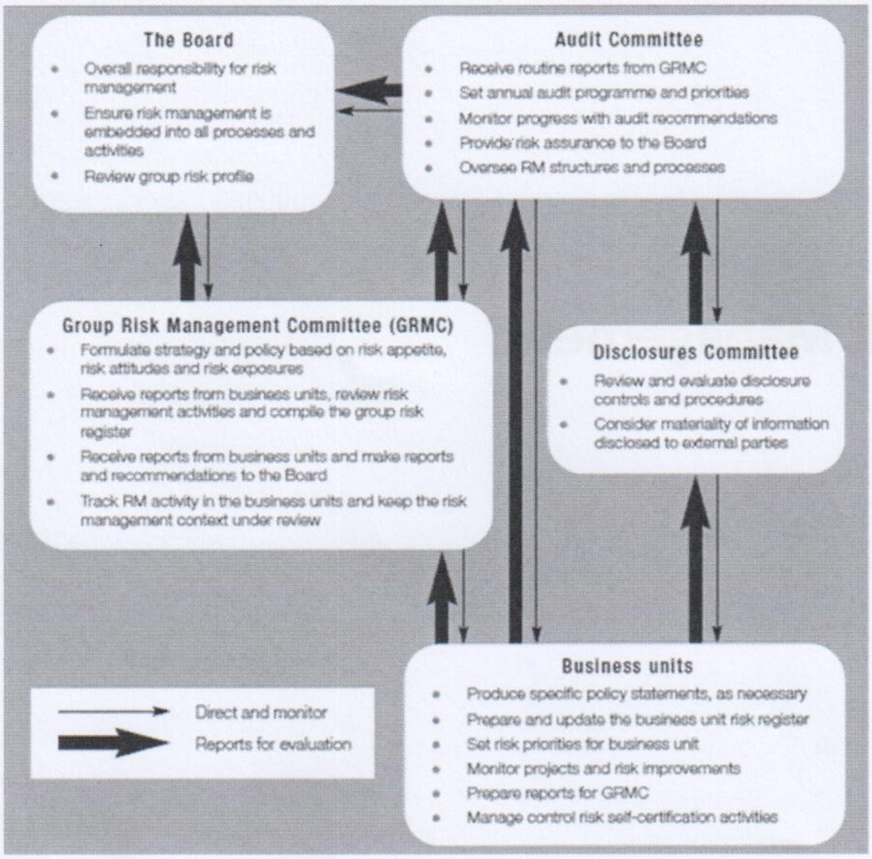
Implementing risk management

Monitoring & review of the framework

Continual improvement of the framework

TRISACADEMY *of Management*

Example: Framework for Public Listed Company



The Board

- Overall responsibility for risk management
- Ensure risk management is embedded into all processes and activities
- Review group risk profile

Audit Committee

- Receive routine reports from GRMC
- Set annual audit programme and priorities
- Monitor progress with audit recommendations
- Provide risk assurance to the Board
- Oversee RM structures and processes

Group Risk Management Committee (GRMC)

- Formulate strategy and policy based on risk appetite, risk attitudes and risk exposures
- Receive reports from business units, review risk management activities and compile the group risk register
- Receive reports from business units and make reports and recommendations to the Board
- Track RM activity in the business units and keep the risk management context under review

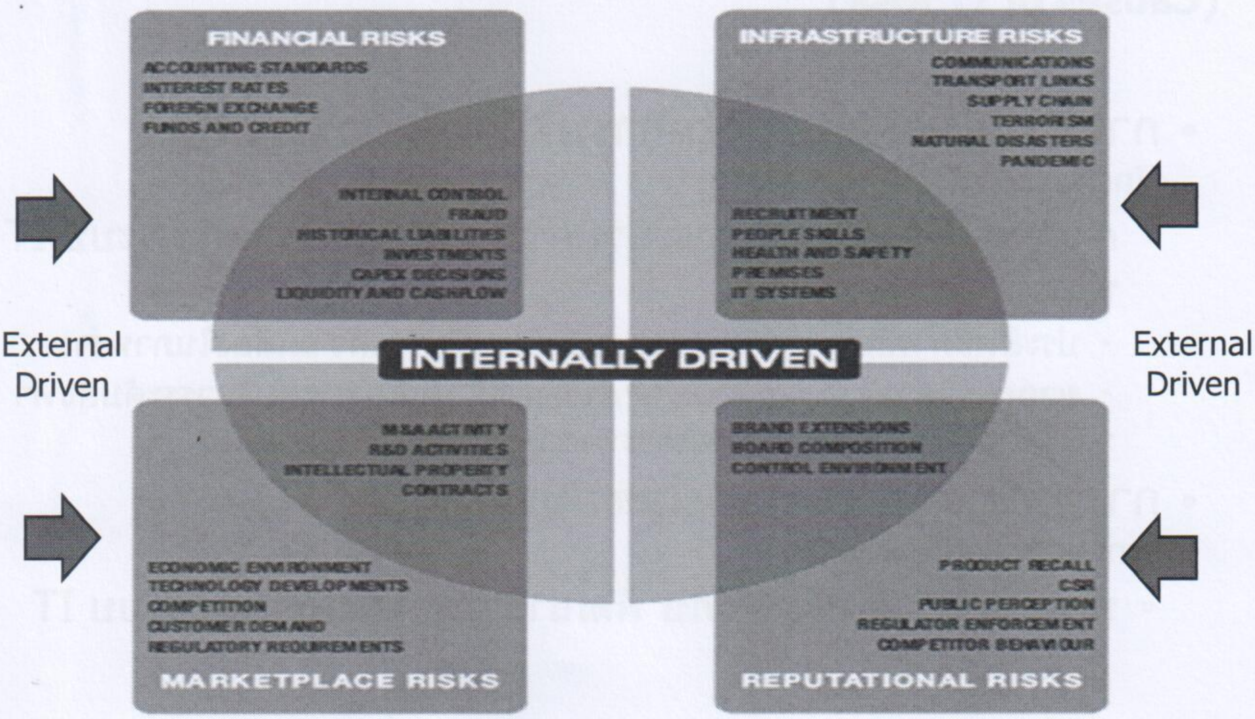
Disclosures Committee

- Review and evaluate disclosure controls and procedures
- Consider materiality of information disclosed to external parties

Business units

- Produce specific policy statements, as necessary
- Prepare and update the business unit risk register
- Set risk priorities for business unit
- Monitor projects and risk improvements
- Prepare reports for GRMC
- Manage control risk self-certification activities

General Risk Classifications



FINANCIAL RISKS

ACCOUNTING STANDARDS
INTEREST RATES
FOREIGN EXCHANGE
FUNDS AND CREDIT

INTERNAL CONTROL
FRAUD
HISTORICAL LIABILITIES
INVESTMENTS
CAPEX DECISIONS
LIQUIDITY AND CASHFLOW

INFRASTRUCTURE RISKS

COMMUNICATIONS
TRANSPORT LINKS
SUPPLY CHAIN
TERRORISM
NATURAL DISASTERS
PANDEMIC

RECRUITMENT
PEOPLE SKILLS
HEALTH AND SAFETY
PREMISES
IT SYSTEMS

INTERNALLY DRIVEN

External Driven

External Driven

M&A ACTIVITY
R&D ACTIVITIES
INTELLECTUAL PROPERTY
CONTRACTS

ECONOMIC ENVIRONMENT
TECHNOLOGY DEVELOPMENTS
COMPETITION
CUSTOMER DEMAND
REGULATORY REQUIREMENTS

MARKETPLACE RISKS

BRAND EXTENSIONS
BOARD COMPOSITION
CONTROL ENVIRONMENT

PRODUCT RECALL
CSR
PUBLIC PERCEPTION
REGULATOR ENFORCEMENT
COMPETITOR BEHAVIOUR

REPUTATIONAL RISKS

TRIS ACADEMY of Management

IT Risk Management

ต้นเหตุของความเสี่ยงด้านระบบ IT (Causes of IT Risk)

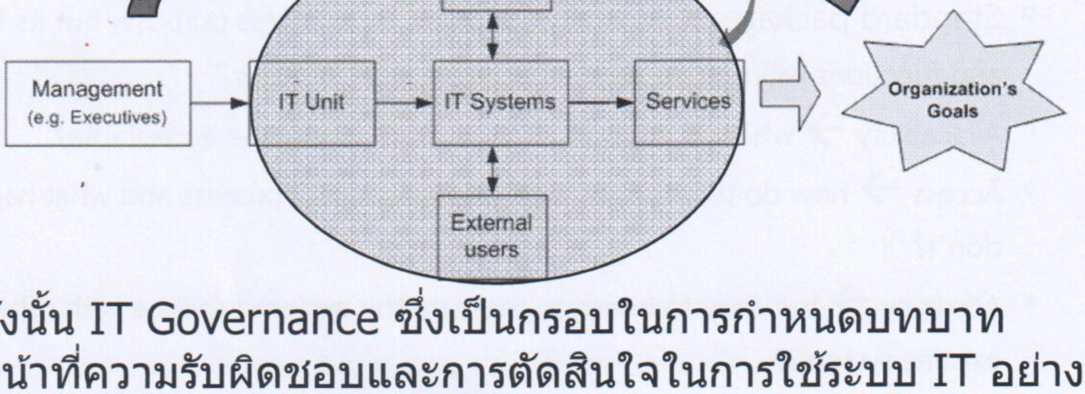
- การขาดประสิทธิภาพในการบริหารจัดการระบบ IT (Ineffective IT Governance)
  - การขาดโครงสร้างและกระบวนการในการบริหารจัดการระบบ IT ทำให้เกิดปัญหา อาทิ
    - ประสิทธิภาพการดำเนินการสูงเฉพาะส่วนที่สร้างความเสี่ยงในภาพรวม
    - ขาดการมีส่วนร่วมจากส่วนต่างๆในองค์กร โดยเฉพาะผู้บริหารระดับสูงทำให้ฝ่าย IT จัดลำดับและผลกระทบของความเสี่ยงไม่ถูกต้อง
- การขยายตัวของความซับซ้อนของระบบ IT (uncontrolled Complexity)
  - พัฒนาการของรถยนต์ กับ พัฒนาการด้านเทคโนโลยีระบบ IT

ต้นเหตุของความเสี่ยงด้านระบบ IT (Causes of IT Risk)

- ความไม่ใส่ใจต่อความเสี่ยงด้าน IT (inattention to risk)
  - ขาดความรู้ความชำนาญ เนื่องจาก การสูญเสียบุคลากรจาก การเกษียณ การลาออก การเลื่อนตำแหน่ง หรือ พึ่งพาผู้เชี่ยวชาญภายนอกมากเกินไป
  - โครงสร้างพื้นฐานของระบบ IT ไม่ดี
  - ความไม่ใส่ใจต่อความเสี่ยงต่างๆของเจ้าหน้าที่
  - การขาดระบบในการเตือนภัยในกิจกรรมหรือกระบวนงานที่มีความเสี่ยง

อุปสรรคของการบริหารความเสี่ยงด้าน IT ระดับองค์กร

- การขาดภาพรวมของการดำเนินการของระบบ IT ที่เชื่อมโยงกับการดำเนินงานและเป้าหมายขององค์กร



- ดังนั้น IT Governance ซึ่งเป็นกรอบในการกำหนดบทบาทหน้าที่ความรับผิดชอบและการตัดสินใจในการใช้ระบบ IT อย่างมีประสิทธิภาพและประสิทธิผล

กรอบการประเมินเหตุความเสี่ยง

- 4A Framework **(MIT Sloan Center for Information Systems Research)**
  1) ความพร้อมใช้ (Availability)
     Keep the system running & recover from interruption
  2) การเข้าถึงระบบ IT (Access)
     Ensure the right people have access they need and wrong people don't!
  3) ความถูกต้อง (Accuracy)
     Provide correct, timely, and complete information
  4) ความว่องไว (Agility)
     Capability to change with managed cost and speed, e.g. new product/service, redesign process etc.

* การพูดคุยกระบวนการไม่ยอมรับ และมีค่าใช้จ่าย

ได้อย่างเสียอย่าง (trade-off)

- Case#1: **ซื้อ** Nonstandard package
  - Nonstandard package -> fit with business objective but does not fit internal technology
  - Standard package -> generally adequate for business purpose, but its features and functions will require some changes in work process
  - Availability → who will support it? How much downtime acceptable?
  - Access → how do to integrate with existing security process and what happens if don't?
  - Accuracy → Is it easy to integrate the data this system produce with other existing systems?
  - Agility → Is it easy to modify this system when business models changes?

(เชื่อมโยง)

ต่อ..Case #1

- ในทางตรงกันข้าม (กับ Standard package)
  - ถ้าจะต้อง Modify กระบวนการให้เข้ากับ Standard package นั้นทำให้กระบวนการสญเสียคุณค่าไปหรือไม่
- คำตอบสุดท้ายอาจจะไม่เปลี่ยนแปลงแต่การที่ทุกๆ ฝ่ายได้แลกเปลี่ยนประเด็นต่างๆทำให้ทราบว่า ระบบ IT จะให้อะไรแล้วจะต้องจ่าย(หรือเสี่ยง)อะไรบ้าง

TRISACADEMY of Management

ได้อย่างเสียอย่าง (trade-off) #2

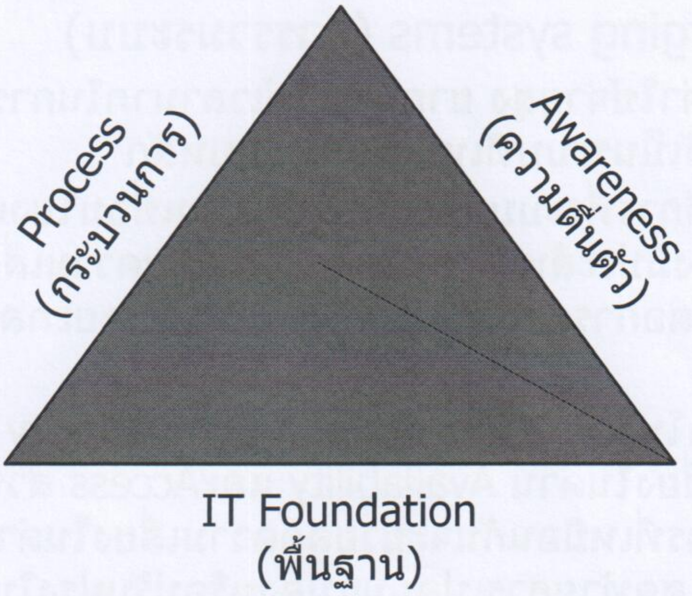
- Case #2: Merging systems (การรวมระบบ)
  - จะต้องใช้ค่าใช้จ่ายสูง ยาก และใช้เวลามากในการแปลงอีกระบบมาให้เป็นระบบที่เหมือนกับระบบหลัก
  - อย่างไรก็ดีการที่ระบบสองระบบสามารถเชื่อมโยงแลกเปลี่ยนข้อมูลอย่างมีประสิทธิภาพจะช่วยลดระดับความเสี่ยงและผลกระทบต่อการดำเนินงานขององค์กรในระยะกลางและระยะยาว,
  - การใช้เทคโนโลยีที่เหมือนกันหรือ Compatibility กันจะช่วยลดความเสี่ยงในด้าน Availability และAccess ส่วนในด้านกระบวนการที่เหมือนกันจะช่วยลดความเสี่ยงในด้าน Accuracy สุดท้ายการเปลี่ยนแปลงหรือปรับปรุงในอนาคตจะทำได้ง่าย (Agility)

TRISACADEMY of Management

ได้อย่างเสียอย่าง (trade-off) #3

- Case #3: Rapid growth vs Control
  - ▫ ในองค์กรที่มีการขยายตัวอย่างรวดเร็ว ส่งผลให้มีกระบวนการทำงานใหม่ๆ เกิดขึ้นมาก และเป็นแรงกดดันให้กับฝ่าย IT ที่จะต้องเร่งรีบพัฒนาระบบให้รองรับกระบวนการใหม่ๆเหล่านี้
  - ▫ องค์กรในลักษณะนี้จะกังวลเรื่องสูญเสียโอกาส (Agility) มากกว่า Access และ Accuracy
  - ▫ เมื่อเวลาผ่านไป หากปราศจากการควบคุมและจัดการกระบวนการที่เหมาะสม จะเป็นการเพิ่มความเสี่ยงในด้านต่างๆมากขึ้นเรือยๆ ทั้ง Access, Accuracy และ นำไปสู่ระบบที่ซับซ้อนยุ่งยากในการปรับปรุงและพัฒนาเพิ่มเติม (Agility)

Where to start IT risk management?



Foundation (พื้นฐาน)

- พื้นฐานของระบบเทคโนโลยีสารสนเทศ ประกอบไปด้วย
  1) ทรัพย์สินด้าน IT เช่น Hardware, software, communication tool etc. → IT Assets
  2) คู่มือและขั้นตอนการดำเนินงาน (Procedures) ในการติดตาม ควบคุม และดูแลระบบ IT
  3) บุคลากรที่เกี่ยวข้อง ในการจัดการพื้นฐานของระบบ IT

  ทั้ง 3 สิ่งทำหน้าที่สนับสนุนและทำให้การดำเนินงานขององค์กรเกิดขึ้นได้
- หลักการ: จะต้องรู้ว่าอะไรเป็นพื้นฐานของระบบ IT และจะต้องมีการจัดการพื้นฐานเหล่านั้นอย่างดี
- แนวคิด: ทำให้โครงสร้างพื้นฐาน**ไม่ซับซ้อน** (Simplification) เพื่อให้ง่ายและจัดการได้อย่างมีประสิทธิภาพ
- การที่ระบบไม่ซับซ้อน → Cost effective risk management

Risk Governance Process

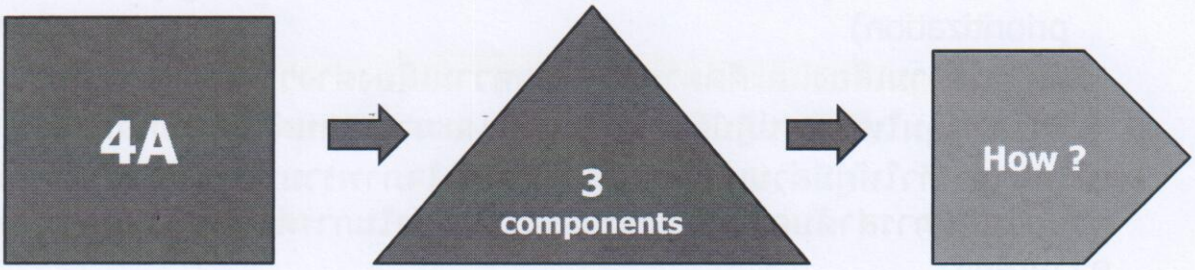
- กระบวนการบริหารจัดการความเสี่ยง (Risk Governance Process) ประกอบไปด้วย
  - การกำหนดนโยบายและมาตรฐาน
  - ชี้บ่งความเสี่ยง (Risk identification) และลำดับความสำคัญ (Risk prioritization)
  - จัดการความเสี่ยงและติดตามแนวโน้มความเสี่ยงต่างๆ
  - การควบคุมให้มีการปฏิบัติตามนโยบายและมาตรฐานด้านความเสี่ยง
- เป้าหมาย: ทำให้ผู้มีส่วนเกี่ยวข้องทั้งหมดเข้าใจภาพรวมของความเสี่ยงด้าน IT ควบคู่ไปกับการลำดับความสำคัญของความเสี่ยงในการดำเนินการจัดการกับความเสี่ยง
- อุปสรรค: ความไม่เข้าใจและตระหนักในผลกระทบของความเสี่ยง
- กระบวนการบริหารจัดการความเสี่ยงที่ไม่มีประสิทธิภาพ อาจจะทำให้การดำเนินการขององค์กรล่าช้าได้

Risk aware culture

- ความตื่นตัวในด้านความเสี่ยง จะเป็นการป้องกับความเสี่ยง (4A) ในระดับบุคคลทั้งในด้านความรับผิดชอบและพฤติกรรม
  - ความเชี่ยวชาญเฉพาะด้านที่เกี่ยวข้องกับความเสี่ยงด้าน IT
  - ความตื่นตัวขององค์กรต่อพฤติกรรมเสี่ยงและผลกระทบที่อาจจะตามมารวมทั้งแนวทางในการหลีกเลี่ยง
  - วัฒนธรรมองค์กรที่ส่งเสริมให้บุคลากรทุกระดับแลกเปลี่ยนความคิดเห็นเกี่ยวกับความเสี่ยงและมีความรับผิดชอบต่อความเสี่ยง

TRIS ACADEMY
of Management

การบริหารจัดการระบบเทคโนโลยีสารสนเทศ (IT Governance)

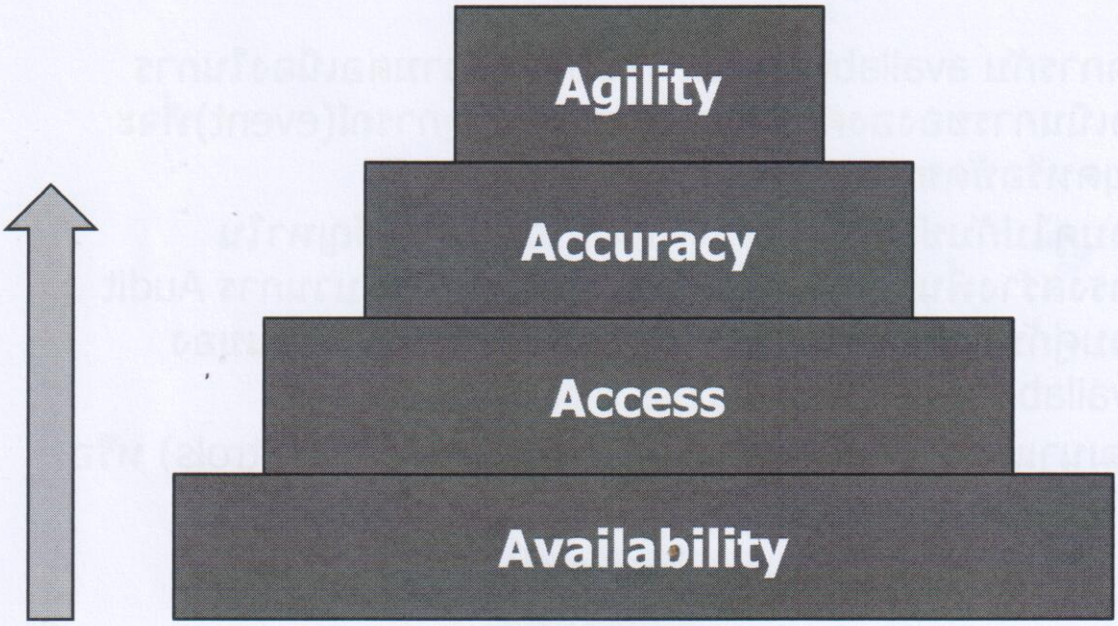


TRIS ACADEMY
of Management

คุณสมบัติของโครงสร้างพื้นฐานที่ดี (Solid Foundation)

- โครงสร้างพื้นฐานที่เป็นมาตรฐานขององค์กร (Standardized infrastructure) โดยจะหลีกเลี่ยงใช้เทคโนโลยีอื่น ถ้าไม่จำเป็น
- ระบบสารสนเทศมีการเชื่อมโยงแลกเปลี่ยนข้อมูลระหว่างกัน (Integrated based applications)
- มีการกำหนดโครงสร้างข้อมูล (Data structure) และบทบาทหน้าที่ของกระบวนการต่างๆ (Process definition) ที่ชัดเจนทั้งองค์กร
- มีกลไกควบคุมการเข้าถึงระบบต่างๆ (Control Access)
- บุคลากรมีความรู้และเข้าใจการทำงานและการดูแลรักษาระบบต่างๆ อย่างทั่วถึง
- มีการปรับปรุงให้มีระบบ IT มีความทันสมัยจาก Patch และ upgrade

IT Risk pyramid



Agility

Accuracy

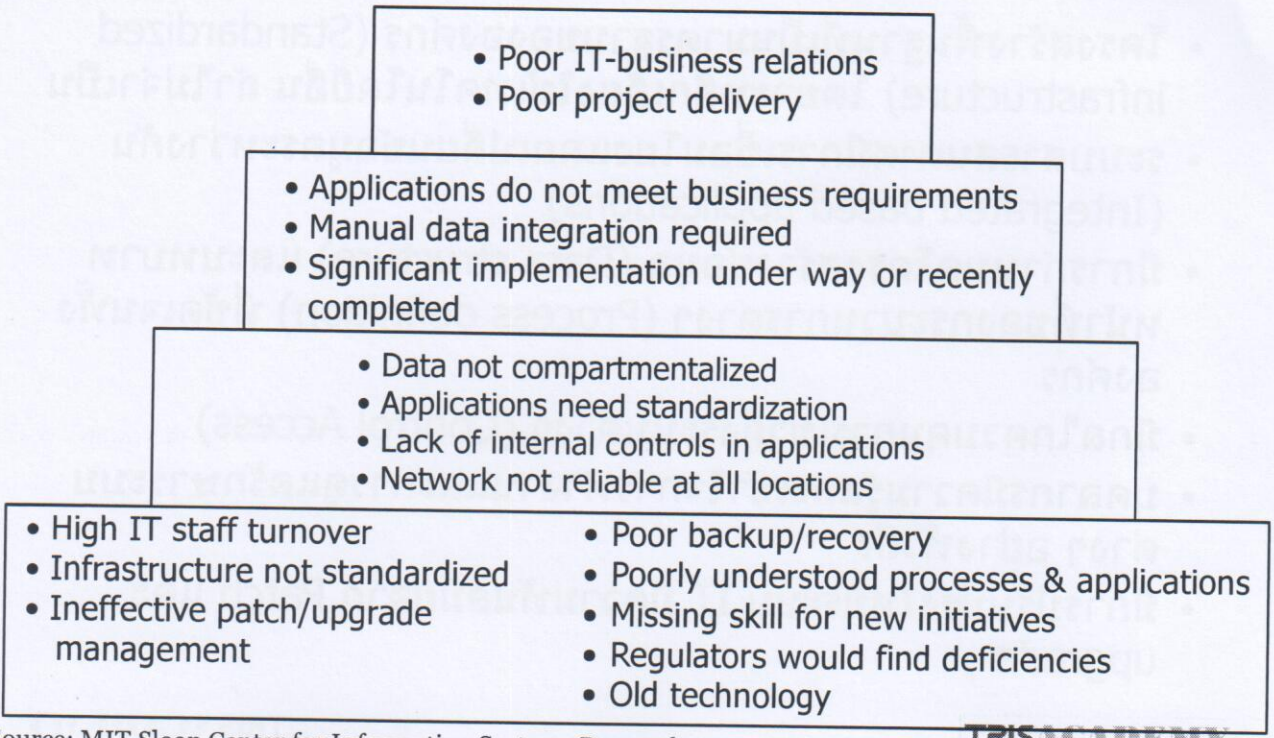
Access

Availability

ปรับปรุง Foundation โดยเริ่มจากฐานปิรามิด

Source: MIT Sloan Center for Information Systems Research

Key IT risk factors and IT risk pyramid



- Poor IT-business relations
- Poor project delivery

- Applications do not meet business requirements
- Manual data integration required
- Significant implementation under way or recently completed

- Data not compartmentalized
- Applications need standardization
- Lack of internal controls in applications
- Network not reliable at all locations

- High IT staff turnover
- Infrastructure not standardized
- Ineffective patch/upgrade management
- Poor backup/recovery
- Poorly understood processes & applications
- Missing skill for new initiatives
- Regulators would find deficiencies
- Old technology

Source: MIT Sloan Center for Information Systems Research

3 ขั้นตอนในการปรับปรุงโครงสร้างพื้นฐาน

1. จัดการกับ availability risk โดยอาศัยความต่อเนื่องในการดำเนินการขององค์กรเป็นหลักหากมีเหตุการณ์(event)ที่จะหยุดหรือขัดขวางการดำเนินงานของระบบ IT
2. ควบคู่ไปกับข้อที่ 1 จะต้องค้นหา(Identify) ปัญหาในโครงสร้างพื้นฐานและรีบแก้ไข โดยอาศัยกระบวนการ Audit ควบคู่กับความรู้ของ IT team โดยเฉพาะในประเด็นของ Availability risk และ Access risk
3. พัฒนาและประยุกต์ใช้แนวทางการควบคุม (IT controls) หรือ IT best practice ในการติดตามสถานะของระบบ IT

Business Continuity Plan

- Business continuity management (BCM) คือความเข้าใจและการลดผลกระทบอันเกิดจากเหตุการณ์ที่ร้ายแรง (Catastrophic events) ที่ส่งผลต่อการดำเนินการที่สำคัญขององค์กร
- BCM เป็นส่วนสำคัญของ Availability risk management
- BCM จะช่วยให้องค์กรเห็นถึงจุดอ่อนและความเสี่ยงของระบบ IT พร้อมไปกับพัฒนาการบริหารความเสี่ยงในระยะยาว
- BCM จะช่วยให้ฝ่ายบริหารและฝ่าย IT ทำงานร่วมกันเข้าใจใน Trade-off ต่างๆได้ดี

Key steps to effective BCM

1. เข้าใจถึงทรัพย์สินด้าน IT และ availability risk
   - วิเคราะห์ผลกระทบ (Impact analysis) เพื่อนำไปจัดลำดับความสำคัญในการจัดสรรทรัพยากรสำหรับกระบวนการที่สำคัญ (critical process)
   - พัฒนารายการทรัพย์สินด้าน IT (inventory of IT) และการเชื่อมโยงกับกระบวนการต่างๆขององค์กร (Business process)
2. จัดทำแผน (BCP)
   - จัดทำแผนการจัดการเหตุการณ์ต่างๆ ที่ประกอบไปด้วย Team และแนวทางการดำเนินการ รวมทั้งวิธีการสื่อสารและแนวทางตอบโต้กับเหตุการณ์ที่เกิดขึ้น
   - กำหนดระดับการให้บริการ และทำแผนการทดสอบ (testing scheme) availability และความต่อเนื่องในการทำงาน

Key steps to effective BCM

3. ดำเนินการ (Implement) และทดสอบแผนที่ได้ทำขึ้น
   - นำเอาประเด็นความต่อเนื่องในการดำเนินการ (Business Continuity) มาสู่วงจรชีวิตของโครงการด้าน IT (IT project life cycle) เพื่อที่จะให้มั่นใจได้ว่ามีการ Recovery ของบุคลากร เทคโนโลยี สถานที่ และกระบวนการการดำเนินการ
   - มีการกำหนดมาตรฐานด้านต่างๆ อาทิ โครงสร้างพื้นฐาน แนวทางการดำเนินงานเพื่อให้ได้ระดับการให้บริการ (Service Level) ที่กำหนดไว้
   - มีการจัดทำระบบแจ้งข่าวสาร (Notification system) ให้กับเจ้าหน้าที่ที่เกี่ยวข้องในเหตุการณ์สำคัญ ตลอดจนฝึกอบรมแนวปฏิบัติอย่างสม่ำเสมอ
   - ทดสอบแผน อย่างน้อยปีละหนึ่งครั้ง ถ้า Comprehensive testing ทำไม่ได้ อย่างน้อยก็ควรทำ walk-through testing เพื่อป้องกันปัญหาอื่นๆที่ขัดขวางแผนงาน

Impact Analysis

- ลำดับแรกในการพัฒนา BCM คือการทำ Business Impact analysis: BIA (ย้ำมุมมองขององค์กร เช่น ชื่อเสียงเป็นต้น) ซึ่งการทำ BIA คือการเปิดโอกาสให้ผู้บริหารระดับสูงได้ประเมินผลกระทบในรายละเอียด

Threat Likelihood	Impact		
	Low (10)	*Medium* (50)	*High* (100)
High (1.0)	Low 10 X 1.0 = 10	Medium 50 X 1.0 = 50	High 100 X 1.0 = 100
Medium (0.5)	Low 10 X 0.5 = 5	Medium 50 X 0.5 = 25	Medium 100 X 0.5 = 50
Low (0.1)	Low 10 X 0.1 = 1	Low 50 X 0.1 = 5	Low 100 X 0.1 = 10

Risk Scale: High (>50 to 100); Medium (>10 to 50); Low (1 to 10)[8]

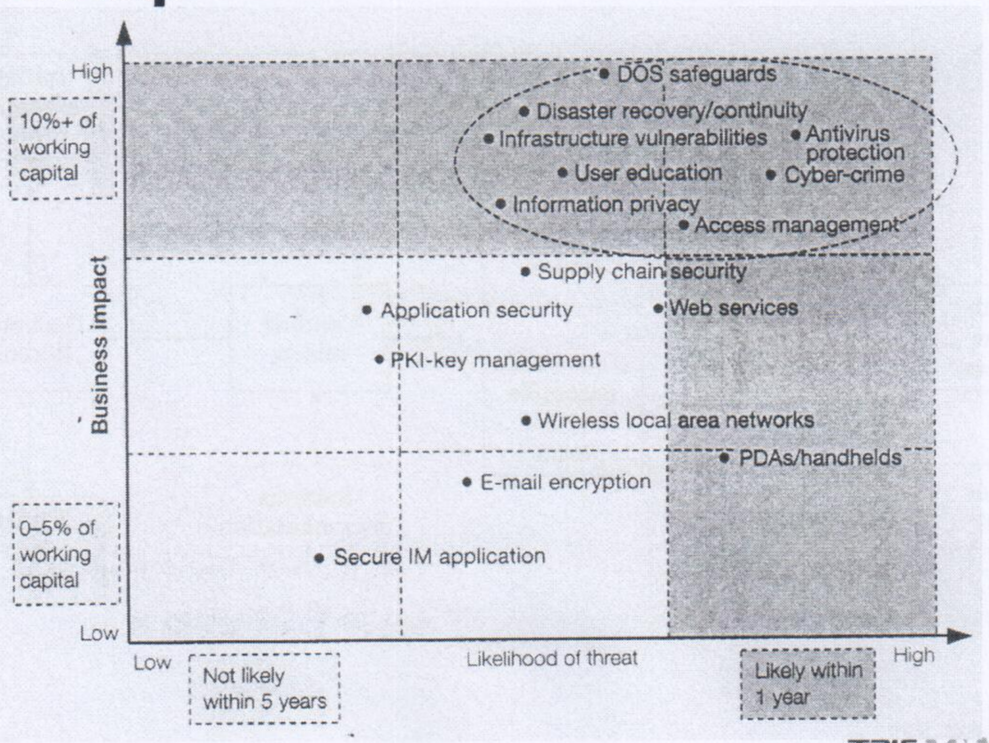
Example of BIA & risk level

Top line of Barnardo's 2004 IT risk register

Risk name	Controls	Weaknesses	Action points	Probability	Impact	Concern	Risk factor
Data loss or compromise of IT systems • Serious Data Protection Act (DPA) leak • Hacking of systems • Unauthorized access	• Audit trail of changes • Strong external defense of IT systems • Password/access controls • Policy on passwords	• Lack of DPA knowledge	• Train/educate in DPA • Increase internal controls (training module to be prepared)	2	5	4	40

Source: Richard Hunter, George Westerman, and Dave Aron, "IT Risk Management: A Little Bit More Is a Whole Lot Better," Research Report (Stamford, CT: Gartner Executive Programs, February 2005).

Risk Map



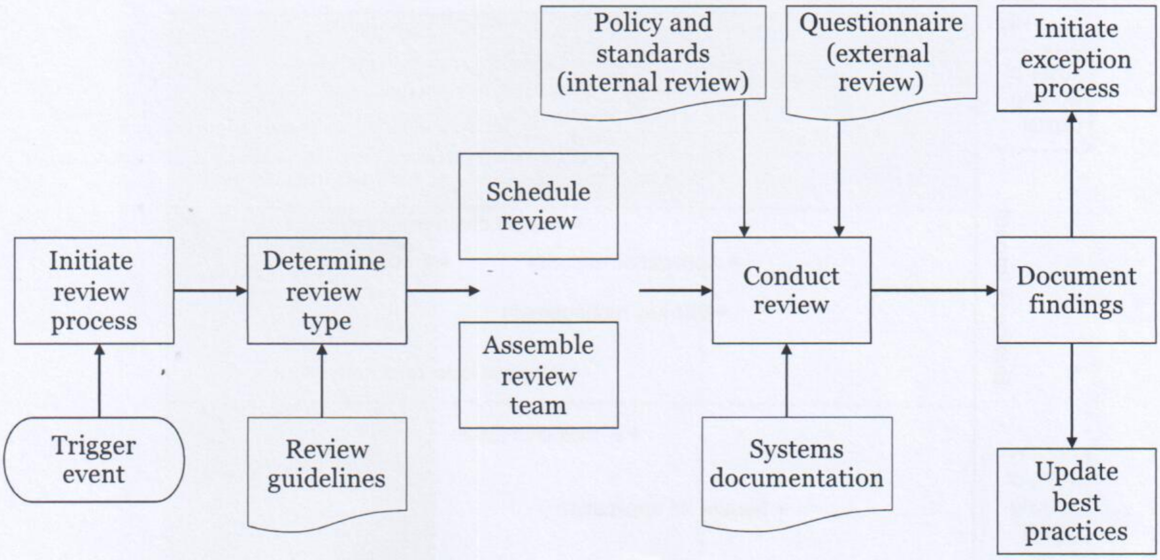
Ex. Risk assessment based on diagnostic scales

Risk impact category	Rating	Weight	Weighted impact score
Service area impacted	8	1	8
Business function criticality	4	1	4
Customer impact	4	3	12
Financial impact	2	3	6
Data sensitivity	2	2	4
TOTAL (risk IMPACT score)			34

Risk likelihood category	Rating	Weight	Weighted likelihood score
Difficulty of exploit	8	3	24
Number of points of entry	2	2	4
Required location	4	1	4
Detection speed	4	1	4
Response planned	4	3	12
TOTAL (risk LIKELIHOOD score)			48

Measurement	Criterion	Rating
High-criticality functions	Business functions could not be down more than 4 hours.	8
Medium-criticality functions	Business functions could be down more than 4 hours but less than 24 hours.	4
Low-criticality functions	Business functions could be down 24 hours or more.	2

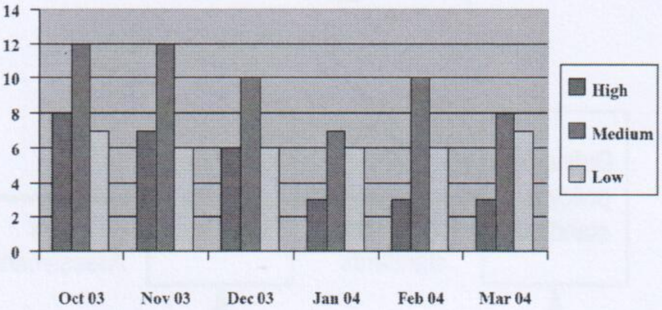
Example: Risk review process



Source : © 2007 Gartner, Inc., and MIT Sloan Center for information Systems Research. Used with permission.

Example: Risk monitoring

Risks by rating		Rating		
# of open issues	Total	High	Medium	Low
Beginning of month	19	3	10	6
New risks	3	1	0	2
Closed risks	4	1	2	1
Improved risk rating	0	0	0	0
Declined risk rating	0	0	0	0
End of month	18	3	8	7



Risk Aging	Risk category	Owner	Total	Months						
				Under 1	1-2	2-3	3-6	6-9	9-12	Over 12
	Architecture	Manager A	2					1	1	
	Financial control	Manager B	2		1			1		
	Human capital	Manager C	1				1			
	Operations	Manager D	6		2			1	3	
	Project mgmt.	Manager E	1		1					
	Security	Manager F	6	2	1			1	2	
	Strategy	Manager G	0							
		Total	**18**	2	5	0	1	4	6	0

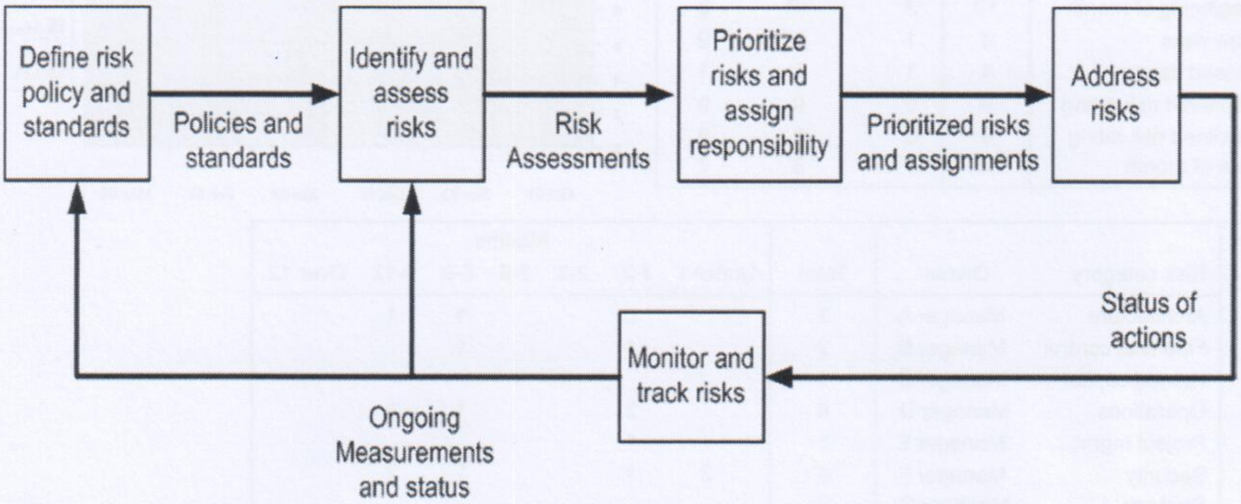
Source : George Westerman and Robert Walpole, "PFPC: Building and IT Risk Management Competency", working paper 352, Center for Information Systems Research, MIT Sloan School of Management, Cambridge, MA. Used with permission.

Note : Managers' names removed to protect confidentiality

Service levels

	Business	Service level	Recommendations
Class 1	Customer- or partner-facing	• 24 × 7 scheduled • 99.9%	Yearly "war gaming" (unannounced full-scale simulated disaster or attack scenario) Full tests every six months after
Class 2	Less critical revenue-producing	• 24 × 6 + 18 hours (6 hours reserved for maintenance window) • 99.5%	"Desktop" tests every six months and full yearly tests after
Class 3	Company back-office functions	• 18 × 7 scheduled • 99%	"Desktop" tests every six months and full yearly tests after
Class 4	Departmental functions	• 24 × 6 + 12 hours (12 hours reserved for maintenance window) • 98%	"Desktop" tests every six months and full yearly tests after

IT risk governance process



Define risk policy and standards

Policies and standards

Identify and assess risks

Risk Assessments

Prioritize risks and assign responsibility

Prioritized risks and assignments

Address risks

Status of actions

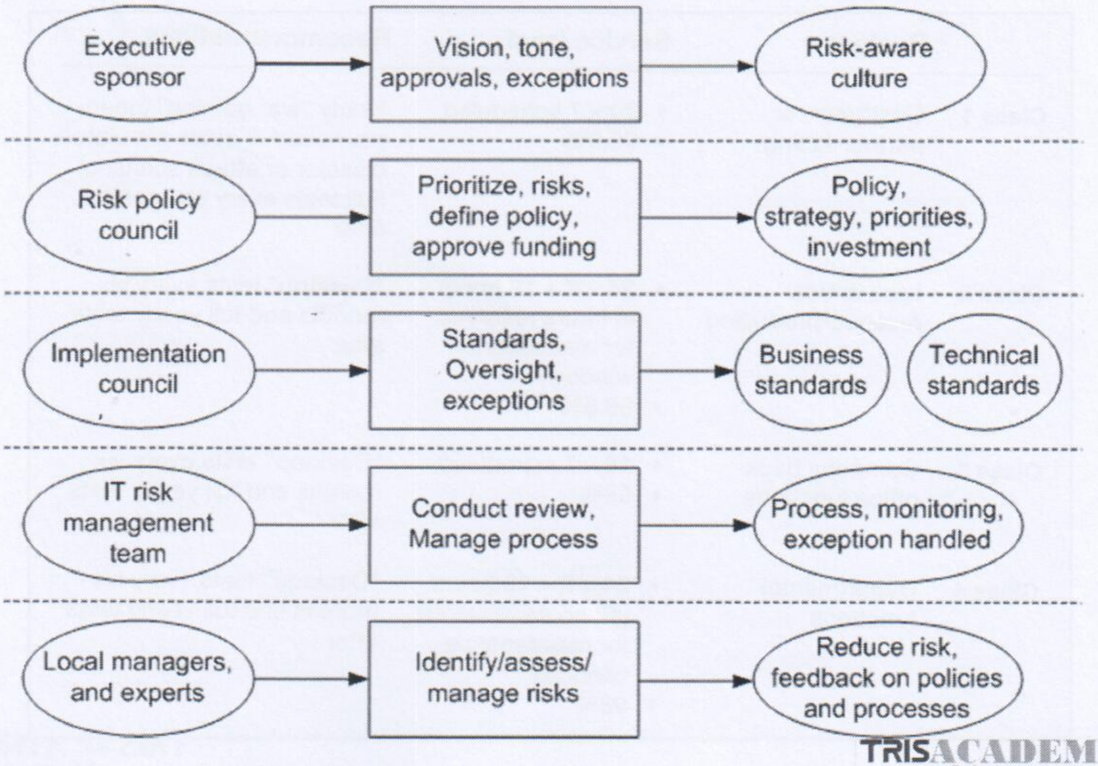
Monitor and track risks

Ongoing Measurements and status

Source: Adapted from Best Practices Council for IT Security Executives Report on IT Security Governance, December 2005, Garther Inc.

TRIS ACADEMY of Management

Organizational structure in IT risk governance process



Executive sponsor → Vision, tone, approvals, exceptions → Risk-aware culture

Risk policy council → Prioritize, risks, define policy, approve funding → Policy, strategy, priorities, investment

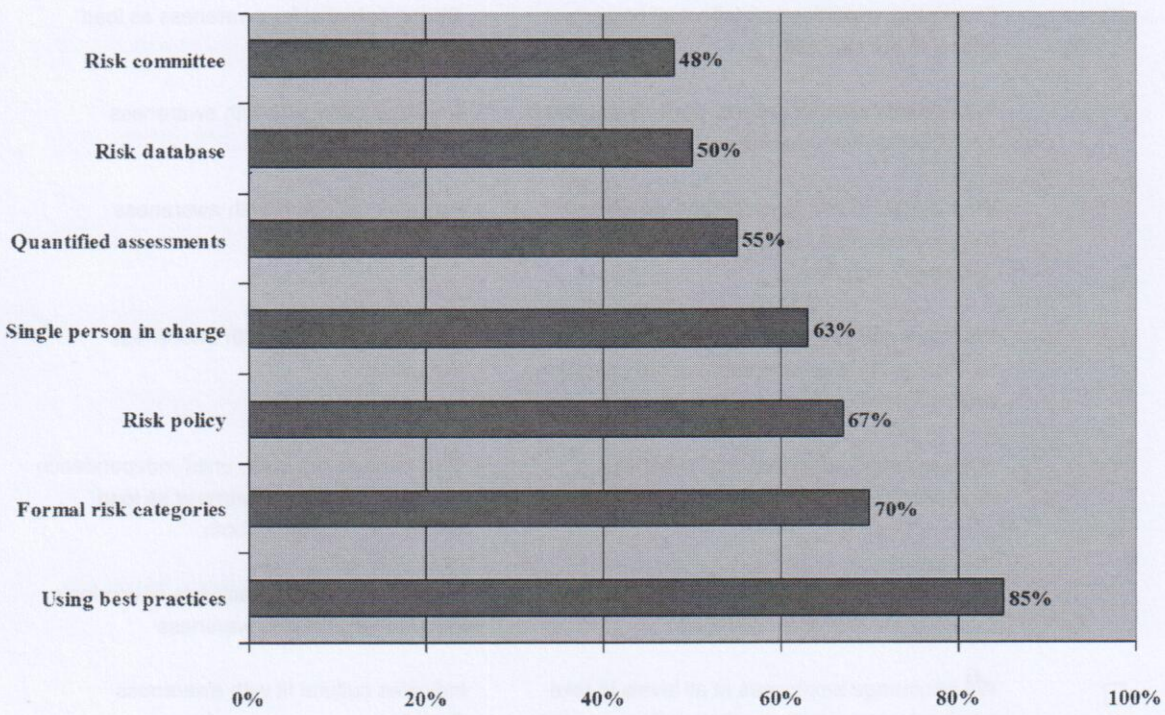
Implementation council → Standards, Oversight, exceptions → Business standards; Technical standards

IT risk management team → Conduct review, Manage process → Process, monitoring, exception handled

Local managers, and experts → Identify/assess/ manage risks → Reduce risk, feedback on policies and processes

TRIS ACADEMY of Management

Survey: Adoption of key practices



Source : © 2007 MIT Sloan Center for information Systems Research. Used with permission.

Note : Bar represent percentage of surveyed organizations stating that they use a practice consistently.

TRIS ACADEMY *of Management*

Risk governance process checklist

Agree? (check)	Characteristic	Reasoning
□	We customarily use committees and task forces to make policy decisions	Indicates cultural fit with governance process
□	We have formal processes for resolving policy exceptions.	Indicates cultural fit with governance process
□	We use audits frequently to validate our processes.	Indicates cultural fit with governance process
□	We actively enforce strong corporate standards and principles for behavior.	Indicates cultural fit with governance process
□	Our core business processes and/or products and services (excluding financial management processes) are subject to regulation.	Often decisive factor for risk governance as lead discipline
□	We have recently been subject to severe regulatory penalties, or our executives have been indicted or fired for ethical lapses.	Usually decisive factor for risk governance as lead discipline
□	Our enterprise revenues (or budget, for a public agency) are greater than $1 billion.	Indicates that resources are sufficient to support risk governance process as lead discipline

Risk-aware culture checklist

Agree? (check)	Characteristic	Reasoning
□	Proprietary expertise or intellectual property is critical to our success.	Strong potential for awareness as lead discipline
□	We cultivate internal experts, such as engineers, and listen to them carefully.	Indicates cultural fit with awareness discipline
□	We think about risk in everything we do and before we commit resources or make a decision to proceed.	Indicates cultural fit with awareness discipline
□	We use a quality management approach such as TQM or Six Sigma to improve our operations and decisions.	Indicates cultural fit with awareness discipline
□	We encourage business units to behave entrepreneurially and look out for themselves.	Emphasis on business units' independence is consistent with awareness as lead discipline, contrary to both
□	Our industry or company ia s target for political or social activists or for criminals.	Focused targeting by activists or criminals requires heightened awareness
□	We encourage employees at all levels to take personal responsibility for their actions and the results of those actions.	Indicates cultural fit with awareness discipline

Source : © 2007 MIT Sloan Center for information Systems Research and Gartner, Inc. Used with permission.

Foundation checklist

Agree? (check)	Characteristic	Reasoning
□	We have a focused and standardized technology base (e.g., one ERP instance worldwide).	Often decisive factor for foundation as lead discipline
□	Our company built or rebuilt its technology base less than 10 years ago.	Strong potential for foundation as lead discipline
□	Our technology base is supported by detailed, up-to-date documentation.	Strong potential for foundation as lead discipline
□	We have an active portfolio management process and maintain an ongoing fund for renewing the installed base.	Strong potential for foundation as lead discipline
□	We have a well-developed architecture that guides most or all of our systems acquisitions and development.	Potential for foundation as lead discipline
□	Controlling costs through standardization of operations is a key company strategy.	Indicates cultural fit with foundation discipline
□	Our enterprise has plans or strategies that will require significantly retooling our technology base.	Retooling of technology base offers "green field" opportunity and strongly favors foundation discipline

Source : © 2007 MIT Sloan Center for information Systems Research and Gartner, Inc. Used with permission.

Foundation IT risk discipline decision factors applied to Shure, Inc.

Agree? (check)	Risk Governance Process
☐	We customarily use committees and task forces to make policy decisions.
☐	We have normal processes for resolving policy exceptions.
☐	We use audits frequently to validate our processes.
☐	We actively enforce strong corporate standards and principles for behavior.
☐	Our core business processes and/or products and services (excluding financial management process) are subject to regulation.
☐	We have recently been subject to severe regulatory penalties, or our executives have been indicted or fired for ethical lapses.
☐	Our enterprise revenues (or budget, for a public agency) are greater than $1 billion.
	Awareness
☒	Proprietary expertise or intellectual property is critical to our success.
☒	We cultivate internal experts, such as engineers, and listen to them carefully.
☒	We think about risk in everything we do and before we commit resources or make a decision to proceed.
☒	We use quality management approach such as TQM or Six Sigma to improve our operations and decisions.
☐	We encourage business units to behave entrepreneurially and look out for themselves.
☐	Our industry or company ia a target for political or social activists or for criminals.
☒	We encourage employees at all levels to take personal responsibility for their actions and the results of those actions.

Foundation IT risk discipline decision factors applied to Shure, Inc.

	Risk Governance Process
☐	We have a focused and standardized technology base (e.g., one ERP instance worldwide).
☒	Our company built or rebuilt its technology base less than 10 years ago.
☐	Our technology base is supported by detailed, up-to-date documentation.
☐	We have an active portfolio management process and maintain an ongoing fund for renewing the installed base.
☒	We have a well-developed architecture that guides most or all of our systems acquisitions and development.
☒	Controlling costs through standardization of operations is a key company strategy.
☐	Our enterprise has plans or strategies that will require significantly retooling our technology base.

Note : Authors' interpretation of the case study information.

ประเภทของการตัดสินใจหลักที่เกี่ยวข้องกับการบริหารจัดการระบบ IT (Major Decision Domain in IT Governance)

- 5 ประเภทกรอบการตัดสินใจหลักที่เกี่ยวข้องกับระบบ IT
  1. ด้านยุทธศาตร์ของระบบ IT (Principles): บทบาทของระบบ IT ที่เกี่ยวข้องกับกลยุทธของององค์กร
  2. ด้านสถาปัตยกรรม IT (Architecture): ทางเลือกด้านเทคนิคที่จะช่วยผลักดันให้องค์กรบรรลุเป้าหมาย
  3. ด้านโครงสร้างพื้นฐานของระบบ IT (Infrastructure): ปัจจัยพื้นฐานที่สะท้อนให้เห็นถึงศักยภาพของระบบ และมักจะถูกออกแบบไว้ล่วงหน้าก่อนที่จะทราบความต้องการที่แท้จริง
  4. ด้านความต้องการในการดำเนินการขององค์กร (Business application needs): รูปแบบของระบบ IT ที่ช่วยสนับสนุนหรือดำเนินการกิจกรรมขององค์กร
  5. ลำดับความสำคัญและการลงทุน (Prioritization and investment): การกำหนดงบประมาณการลงทุนและที่จุดใด
- การตัดสินในรูปแบบต่างๆเกิดได้ในหลายๆจุดไม่ว่าจะเป็น ระดับฝ่าย ระดับแผนก ฯลฯ

TRISACADEMY of Management

การตัดสินใจหลักที่เกี่ยวข้องกับการบริหารจัดการระบบ IT(1)

1. IT Principles
   - ทำอย่างไรถึงสามารถแปลงยุทธศาสตร์ขององค์กรมาเป็นยุทธศาตร์ด้าน IT เพื่อช่วยสนับสนุนการตัดสินใจที่เกี่ยวข้องกับระบบ IT?
   - อะไรเป็นบทบาทของระบบ IT ต่อการดำเนินงานขององค์กร?
   - อะไรคือการดำเนินงานที่น่าพึงพอใจของระบบ IT?
   - จะหาเงินสนับสนุนการลงทุนด้าน IT มาจากไหน?

TRISACADEMY of Management

IT Decision Making (2)

2. IT Architecture

- อะไรคือกระบวนการ/ภาระกิจหลักขององค์กร และมีความเชือมโยงกับระบบ IT อย่างไร
- กระบวนการ/ภาระกิจหลักนี้ต้องใช้ข้อมูลใดเป็นหลักในการดำเนินการ และสามารถบูรณาการข้อมูลเหล่านี้ได้หรือไม่
- เทคโนโลยีอะไรควรมีการกำหนดมาตรฐานการใช้งานทั่วองค์กรและสนับสนุนการมาตรฐานและบูรณาการการดำเนินงาน
- กิจกรรมอะไรที่จะต้องมีการกำหนดมาตรฐานการดำเนินงานเพื่อสนับสนุนการบูรณาการข้อมูล
- ทางเลือกของเทคโนโลยีอะไรที่จะสนับสนุนการดำเนินงานขององค์กรอย่างไร

IT Decision Making (3)

3. IT Infrastructure

- อะไรคือโครงสร้างพื้นฐานหลักในการสนับสนุนให้องค์กรบรรลุเป้าหมายทางยุทธศาสตร์ ?
- โครงสร้างพื้นฐานอะไรควรมีในทุกๆส่วนขององค์กร รวมทั้งคุณภาพการให้บริการระดับใดของระบบที่จำเป็นต้องมี
- การประเมินราคาโครงสร้างพื้นฐานอย่างไร
- แผนในการทำให้โครงสร้างพื้นฐานมีความทันสมัยเสมอ
- โครงสร้างพื้นฐานที่ควรว่าจ้างให้ผู้อื่นดำเนินการแทน (Outsource)

IT Decision Making (4)

4. Business application needs

- เป้าหมาย(ตลาด)และโอกาสของการประยุกต์ใช้ระบบ IT
- ประเมินความสำเร็จในการประยุกต์ใช้ระบบ IT อย่างไร
- ทำอย่างไรให้ระบบสถาปัตยกรรม IT แบบมาตรฐาน สามารถตอบสนองต่อความต้องการในการดำเนินงานขององค์กรได้ และในขณะเดียวกันอะไรคือข้อยกเว้นของการอ้างอิงมาตรฐาน
- ใครคือผู้รับผิดชอบต่อผลการดำเนินงานของโครงการและมีการวางแผนการทำการบริหารการเปลี่ยนแปลงอย่างไรให้ประโยชน์ที่ได้จากระบบ IT มีความยั่งยืน

IT Decision Making (5)

5. Prioritization and investment

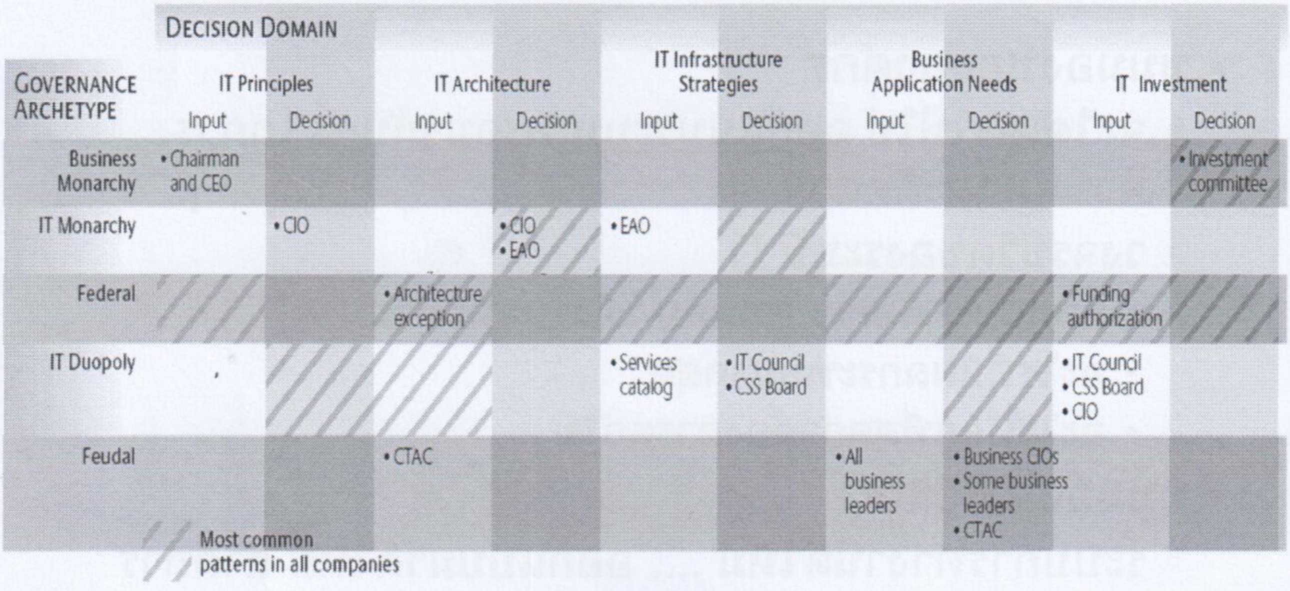
- การเปลี่ยนแปลงหรือปรับปรุงกระบวนการใดมีผลต่อการการดำเนินงานเชิงยุทธศาตร์ขององค์กรที่สุด
- ในระบบ IT หลายๆระบบที่มีอยู่ ระบบใดบ้างที่ยังสามารถสนับสนุนการดำเนินงานเชิงยุทธศาตร์ขององค์กรในปัจจุบัน
- ประโยชน์ที่ได้รับทั้งองค์กรเมื่อเปรียบเทียบกับการลงทุนของฝ่ายหรือแผนก การลงทุนของแต่ละส่วนสะท้อยถึงความสำคัญต่อภาพรวมขององค์กรหรือไม่
- จะประเมินผลการดำเนินงานของระบบ IT ภายหลังติดตั้งเสร็จอย่างไร

ลักษณะโครงสร้างการตัดสินใจในการจัดการระบบ IT (Decision structures in IT governance)

- Archetypal ~ Decision structure
- เราควรรู้ว่าใครคือคนตัดสินใจและเป็นผู้รับผิดชอบ (Accountability) ในการตัดสินใจนั้น
- 6 Archetypes (Centralized vs Decentralized)
  - Business Monarchy: เป็นระบบรวมศูนย์ที่สุด คือ CEO หรือ CIO ตัดสินใจโดยลำพัง
  - IT Monarchy: การตัดสินใจโดยผู้เกี่ยวข้องด้าน IT เท่านั้น
  - Federal: การตัดสินใจในรูปแบบคณะกรรมการที่มีหลายๆฝ่ายรวมทั้งแผนก IT ด้วย
  - IT Duopoly: การตัดสินใจร่วมกันสองส่วน ซึ่งมักจะเป็น IT dept. กับหัวหน้าหน่วยงานที่ใช้ระบบ
  - Feudal system: Process/business unit leader ตัดสินใจเอง
  - Anarchy: each individual/small group pursue his,her or their own IT agenda

TRISACADEMY of Management

ภูมิทัศน์การตัดสินใจ (Decision Landscape)



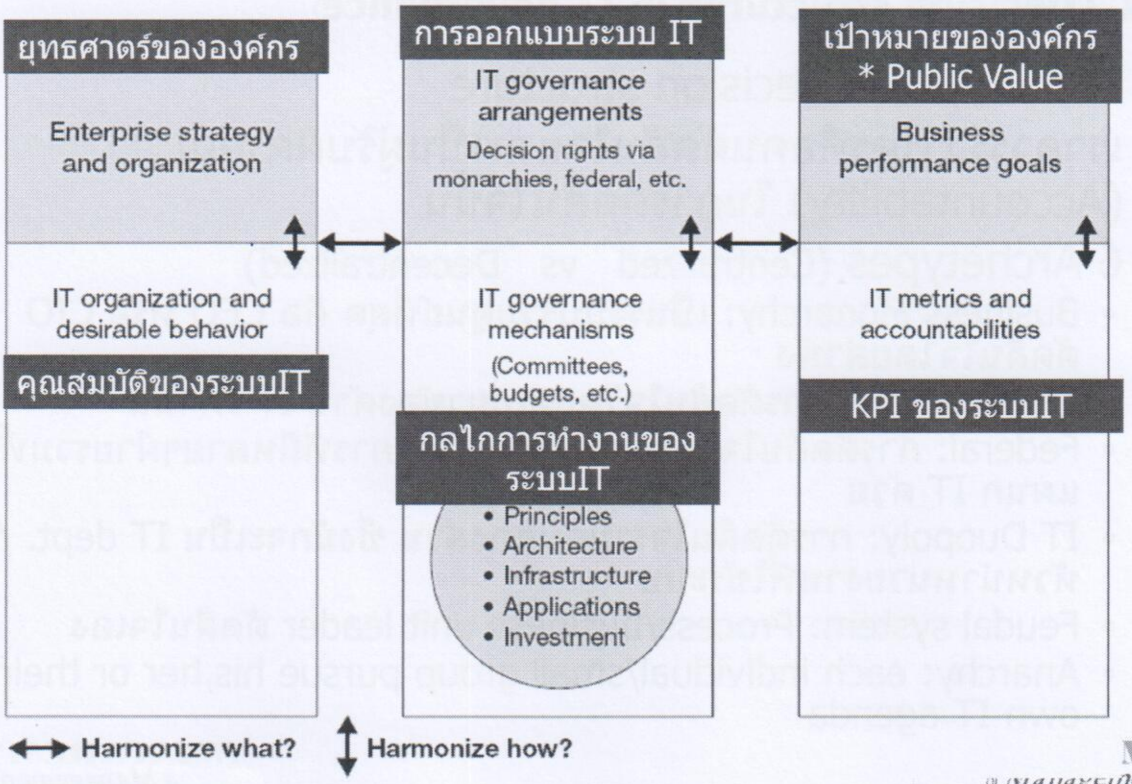
	DECISION DOMAIN									
GOVERNANCE ARCHETYPE	IT Principles		IT Architecture		IT Infrastructure Strategies		Business Application Needs		IT Investment	
	Input	Decision	Input	Decision	Input	Decision	Input	Decision	Input	Decision
Business Monarchy	• Chairman and CEO									▨ • Investment committee
IT Monarchy		• CIO		▨ • CIO • EAO	• EAO	▨				
Federal	▨		• Architecture exception		▨	▨	▨	▨	• Funding authorization	▨
IT Duopoly		▨	▨		• Services catalog	• IT Council • CSS Board		▨	• IT Council • CSS Board • CIO	
Feudal			• CTAC				• All business leaders	• Business CIOs • Some business leaders • CTAC		

▨ Most common patterns in all companies

รู้ไปทำไม ??

TRISACADEMY of Management

แนวคิด (Conceptual framework)



ยุทธศาสตร์ขององค์กร

Enterprise strategy and organization

IT organization and desirable behavior

คุณสมบัติของระบบIT

การออกแบบระบบ IT

IT governance arrangements

Decision rights via monarchies, federal, etc.

IT governance mechanisms

(Committees, budgets, etc.)

กลไกการทำงานของระบบIT

- Principles
- Architecture
- Infrastructure
- Applications
- Investment

เป้าหมายขององค์กร

* Public Value

Business performance goals

IT metrics and accountabilities

KPI ของระบบIT

↔ Harmonize what?

↕ Harmonize how?

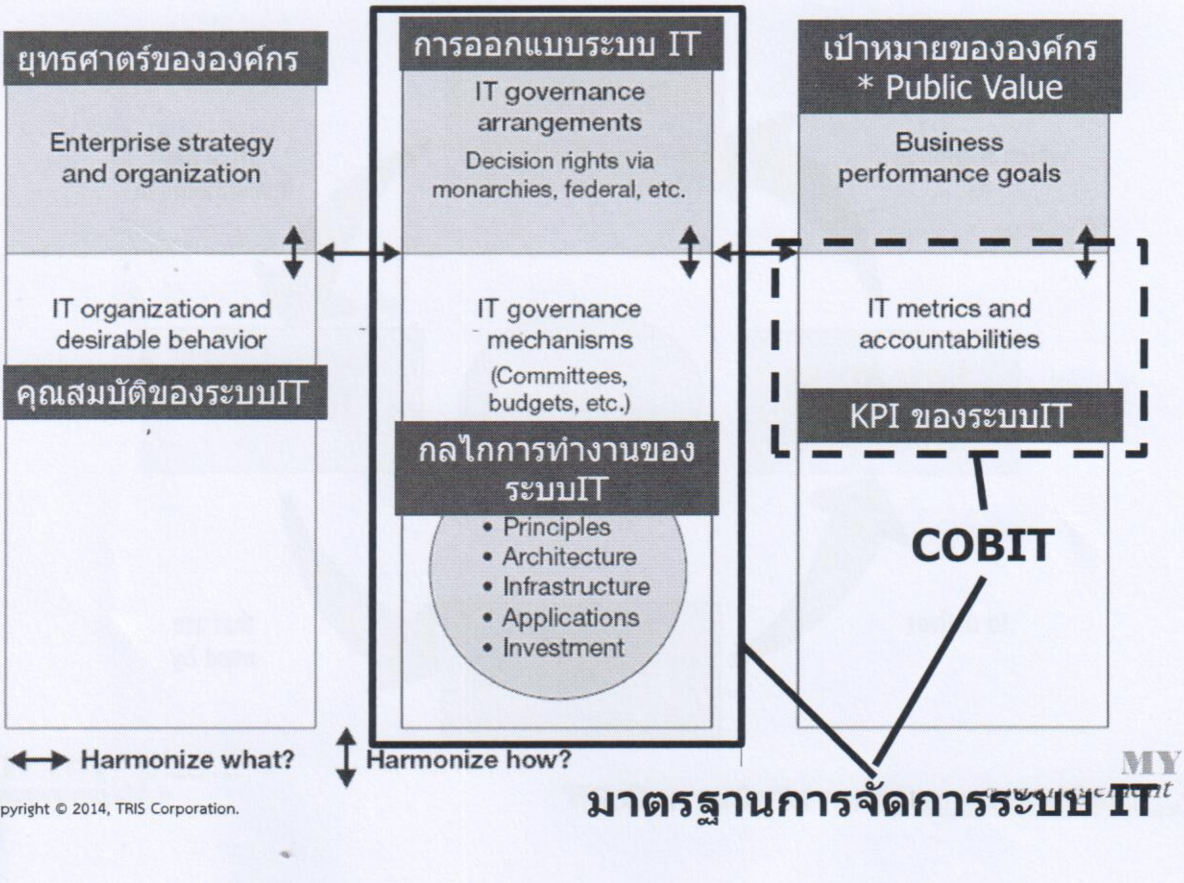
รู้ไปทำไมนี่ แนวคิด

- มุมมองขององค์กร
  - จะได้เอาไปใช้ ออกแบบระบบ พร้อมๆกับกลไกการควบคุมและติดตาม
  - วงจรชีวิตของระบบ IT
    - ออกแบบ พัฒนา ทดสอบ ใช้งานจริง ปรับปรุง
    - อะไรที่มีผลกระทบมากสุด
    - อะไรที่ถูกที่สุดถ้าต้องการแก้ไข
- มุมมอง Auditor
  - ระบบการทำงานดีไหม .... ออกแบบมาดีไหม ถ้าดีการเชื่อมโยงจะมี

มาตรฐานการบริหารจัดการระบบ ICT

- เป็น Best Practices
- เอาไปใช้ประโยชน์อย่างไร ?
  - ▫ ตัวอย่างของการดำเนินการให้ได้ IT Good Governance
  - ▫ ตอบคำถามที่ว่าทำอย่างไร
- มุมมองขององค์กร
  - ▫ ช่วยในการออกแบบ และกำหนดกลไกการดำเนินการ
- มุมมองของ Auditor
  - ▫ ตรวจสอบว่าองค์ประกอบสำคัญๆ มีไหม
  - ▫ แนะนำได้ว่าจะต้องทำอย่างไร ต้องมีอะไร

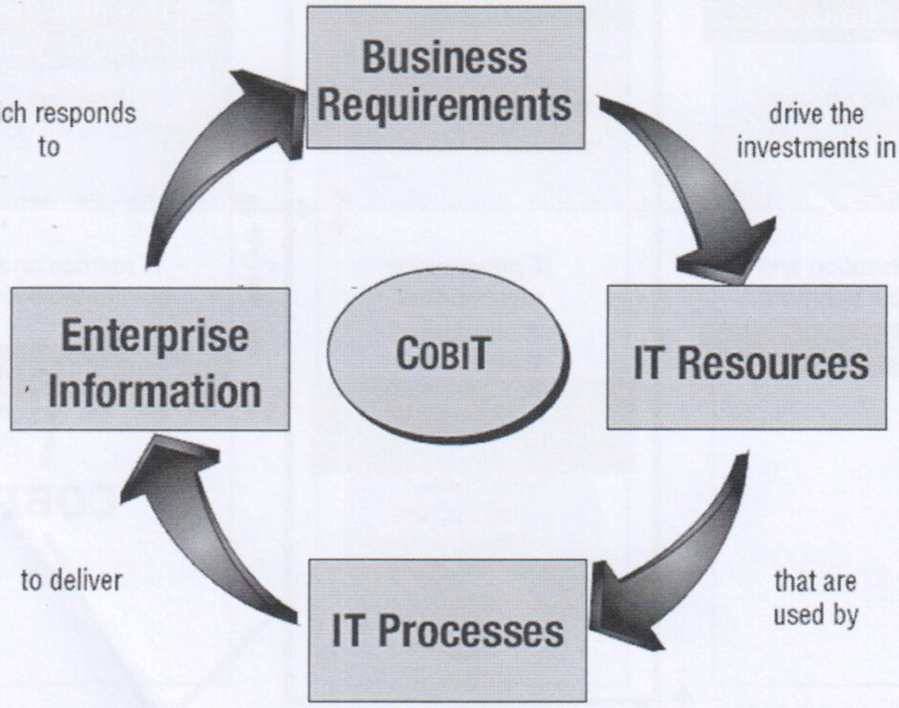
แนวคิด (Conceptual framework)



COBIT

- IT Governance according to COBIT
- COBIT 4.1 & 5

วงจรการออกแบบระบบ IT ของ COBIT



อ้างอิงกรอบมาตรฐานการดำเนินงาน CoBiT

What is COBIT?

Control Objective for Information and related Technologies (COBIT)

- Making a link to the business requirements
- Provide good practices across a domain and process framework
- strongly focused on control and less on execution
- help optimize IT-enabled investments, ensure service delivery
- provide a measure against which to judge when things do go wrong

TRISACADEMY of Management

COBIT & Related Frameworks/Standards

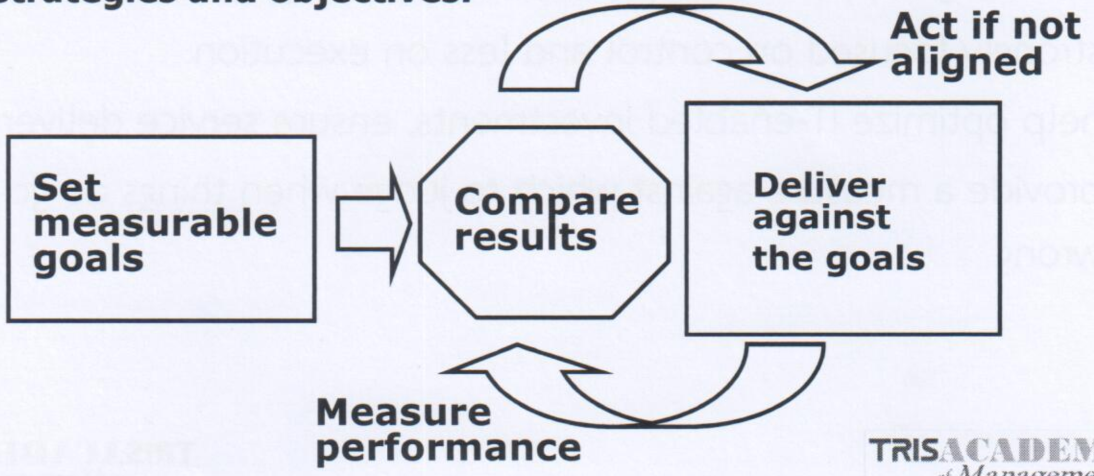
Organizations find it convenient to use COBIT because COBIT relates to other frameworks/standards, such as ITIL, ISO 17799, CMM, and COSO.

ITIL	ISO 17799	CMM	COSO
The IT Infrastructure Library is a collection of best practices in IT service management. It is focused on the "how" of IT or service and its processes and the central role of the user.	The Code of Practice for Information Security Management is an international standard based on BS 7799-1. It is presented as the best practice for implementing information security management.	The scheme for certification of the software quality management system to improve the effectiveness of the quality management system and targets customers, suppliers and assurance professionals	The COSO Framework is an effective standard and an accepted framework for establishing internal controls and determining their effectiveness.

TRISACADEMY of Management

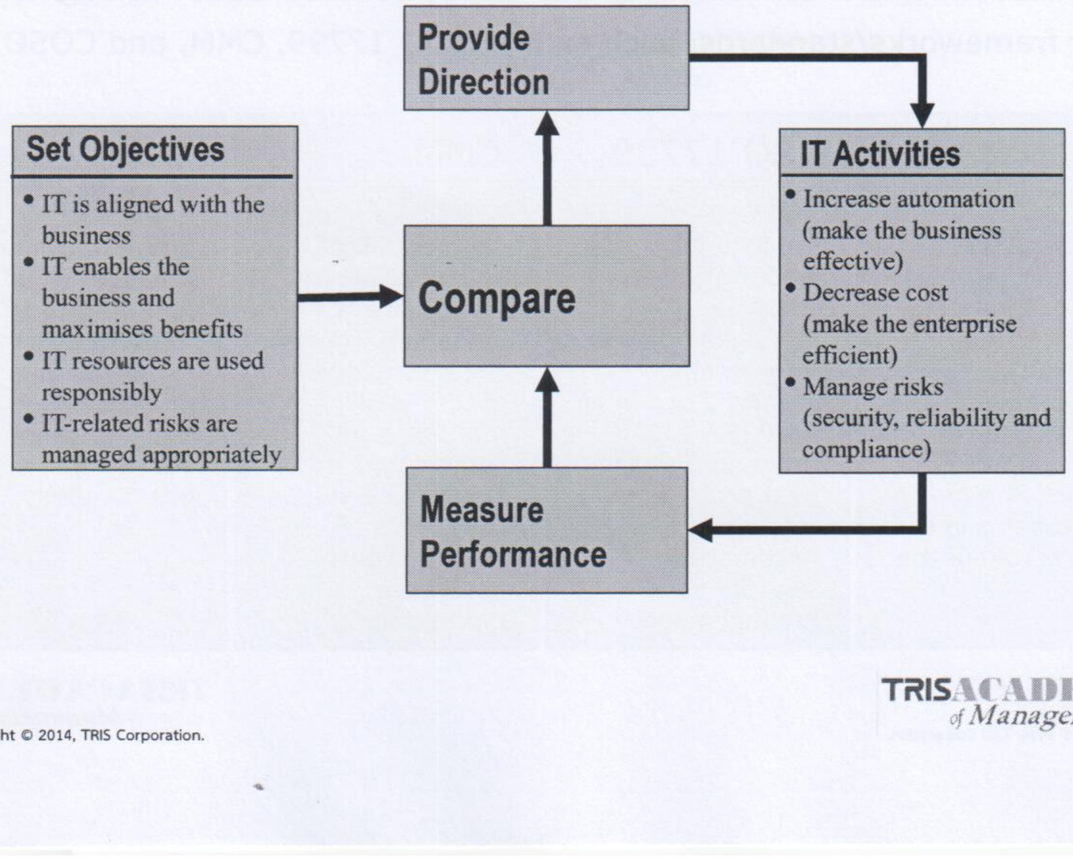
Definition

- **IT governance, like other governance subjects, is the responsibility of executives and shareholders (represented by the board of directors). It consists of the leadership and organizational structures and processes that ensure that the organization's IT sustains and extends the organization's strategies and objectives.**



TRISACADEMY *of Management*

IT Governance Framework



Set Objectives

- IT is aligned with the business
- IT enables the business and maximises benefits
- IT resources are used responsibly
- IT-related risks are managed appropriately

IT Activities

- Increase automation (make the business effective)
- Decrease cost (make the enterprise efficient)
- Manage risks (security, reliability and compliance)

TRISACADEMY *of Management*

Who does COBIT serve?

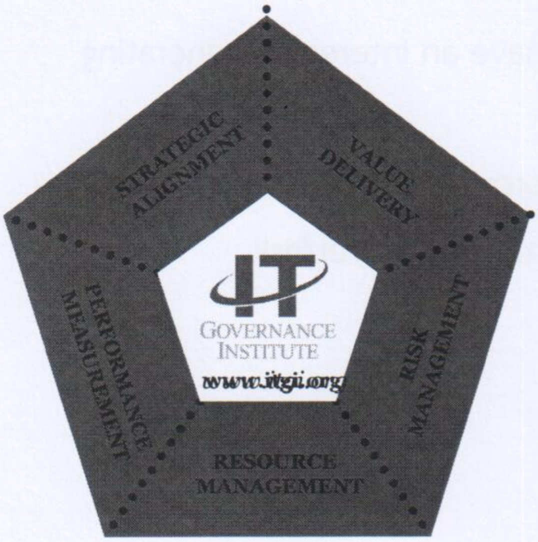
- Stakeholders within the enterprise who have an interest in generating value from IT investments
- Internal and external stakeholders who provide the IT services
- Internal and external stakeholders who have a control/risk responsibility

Stakeholder Value and Business Objectives

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		

Source: COBIT® 5, figure 5. © 2012 ISACA® All rights reserved.

Governance Fundamental

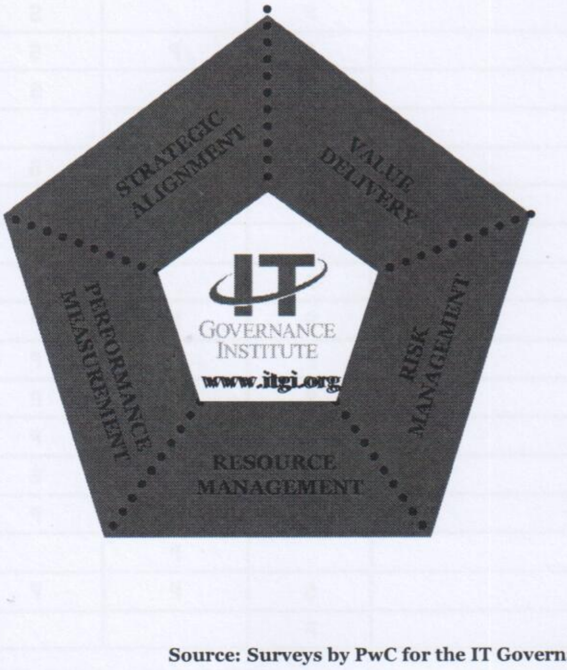


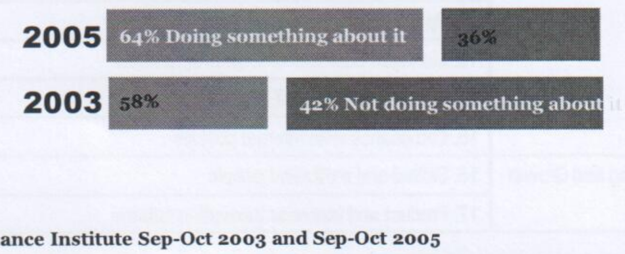
Enterprise governance is a set of responsibilities and practices exercised by the board and executive management with the goal of:

- Providing **strategic direction**
- Ensuring that **objectives** are achieved
- Ascertaining that **risks** are managed appropriately
- Verifying that the **enterprise's resources** are used responsibly

IT governance is:

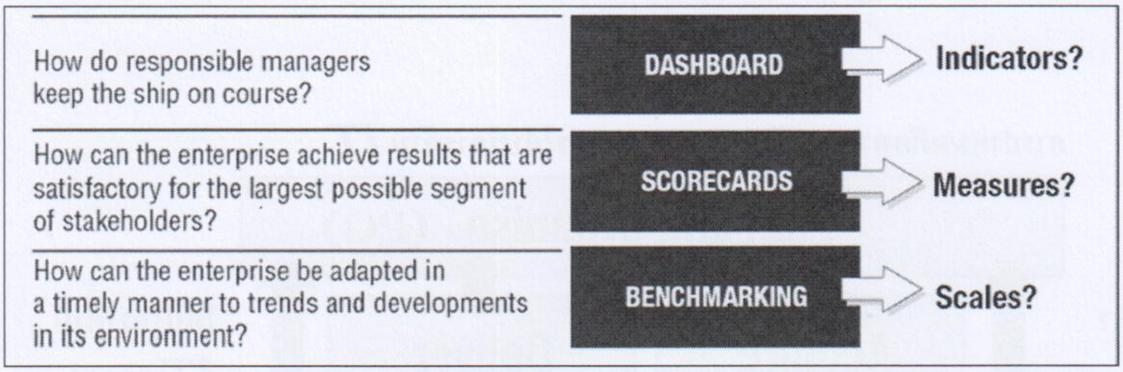
- The responsibility of the board of directors and executive management
- An **integral part** of enterprise governance, consisting of the leadership, organisational structures and processes that ensure that the **enterprise's IT sustains and extends the organisation's strategies and objectives**





Source: Surveys by PwC for the IT Governance Institute Sep-Oct 2003 and Sep-Oct 2005

Design to provide direction



How do responsible managers keep the ship on course? — DASHBOARD → Indicators?

How can the enterprise achieve results that are satisfactory for the largest possible segment of stakeholders? — SCORECARDS → Measures?

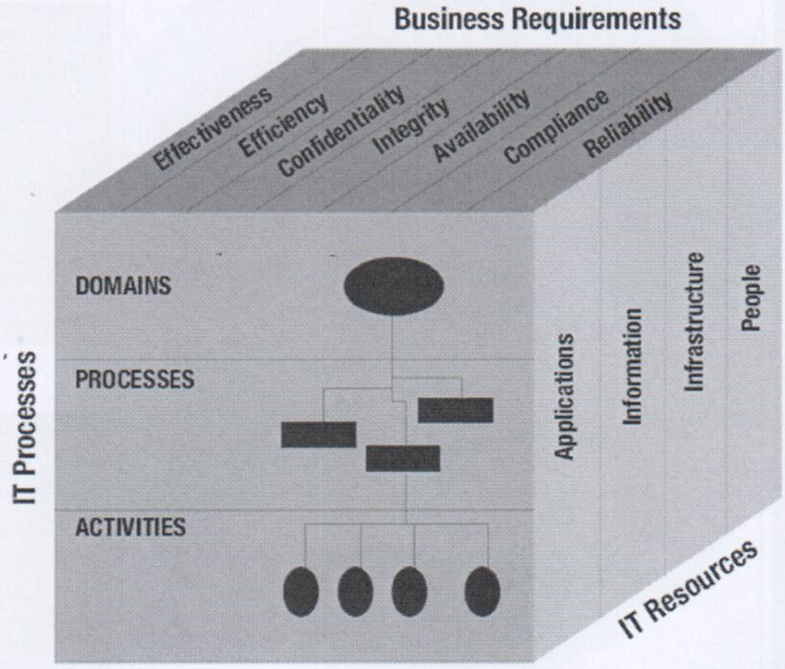
How can the enterprise be adapted in a timely manner to trends and developments in its environment? — BENCHMARKING → Scales?

An answer to these requirements of determining and monitoring the appropriate IT control and performance level is COBIT's definition of:

- **Benchmarking** of IT process performance and capability, expressed as maturity models, derived from the Software Engineering Institute's Capability Maturity Model (CMM)
- **Goals and metrics** of the IT processes to define and measure their outcome and performance based on the principles of Robert Kaplan and David Norton's balanced business scorecard
- **Activity goals** for getting these processes under control, based on COBIT's control objectives

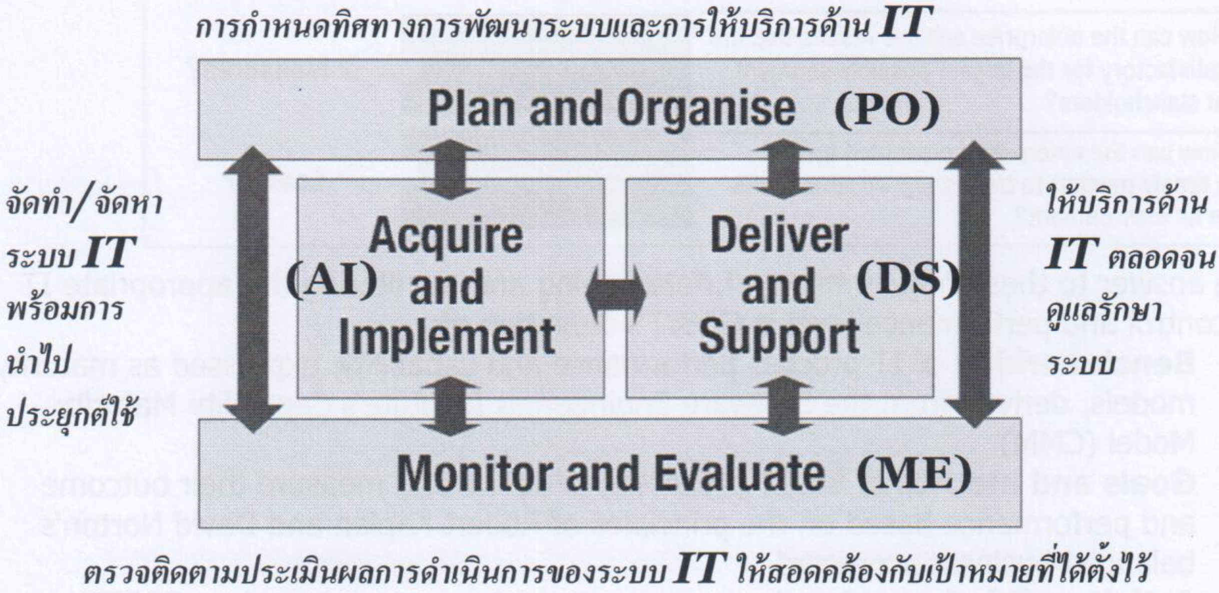
TRISACADEMY *of Management*

กรอบการวิเคราะห์องค์ประกอบของระบบ IT



TRISACADEMY *of Management*

ตัวอย่าง มาตรฐานการจัดการและพัฒนาระบบ IT



การกำหนดทิศทางการพัฒนาระบบและการให้บริการด้าน *IT*

Plan and Organise (PO)

จัดทำ/ จัดหาระบบ *IT* พร้อมการนำไปประยุกต์ใช้

(AI) Acquire and Implement

Deliver and Support (DS)

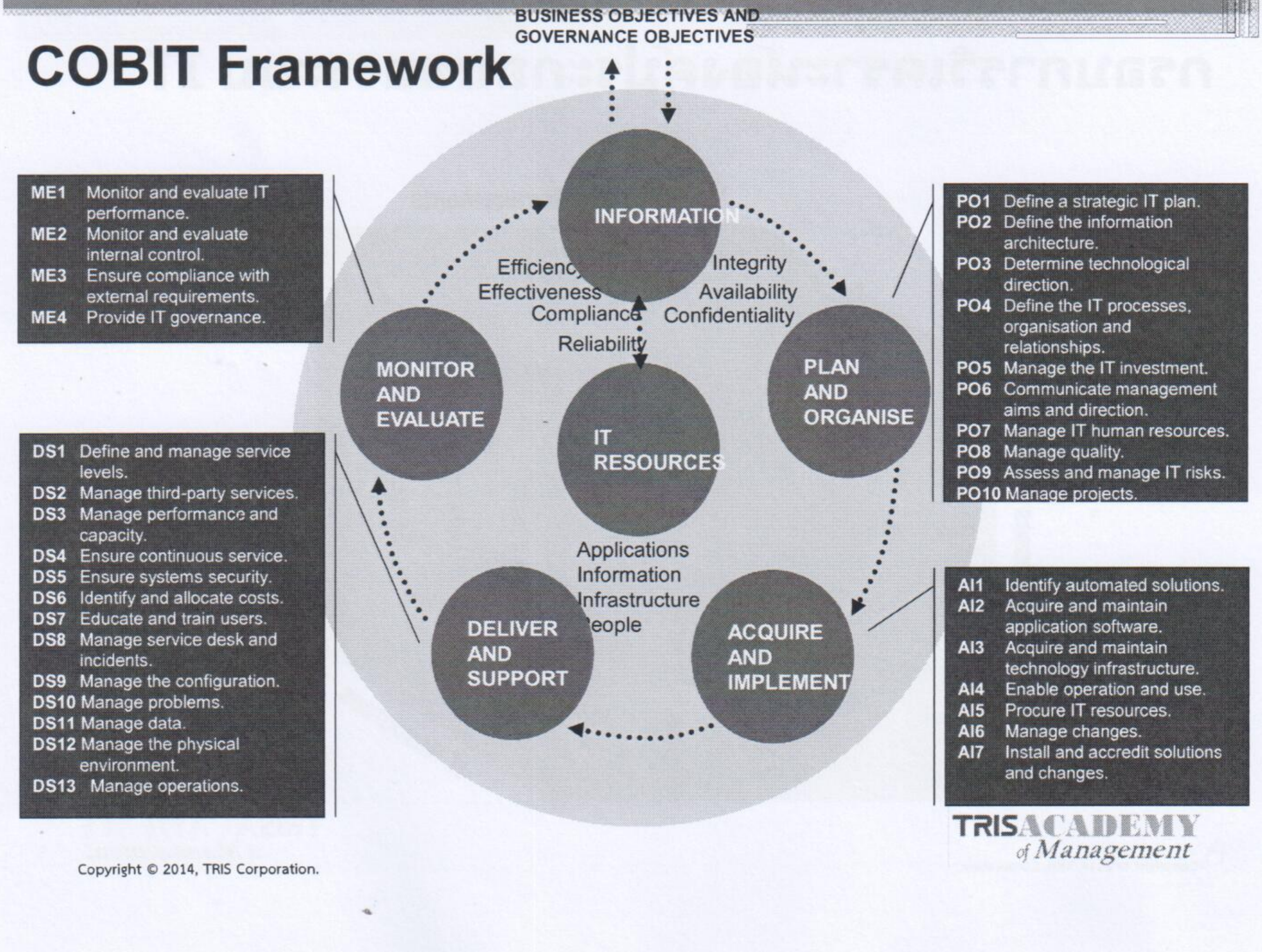
ให้บริการด้าน *IT* ตลอดจนดูแลรักษาระบบ

Monitor and Evaluate (ME)

ตรวจติดตามประเมินผลการดำเนินการของระบบ *IT* ให้สอดคล้องกับเป้าหมายที่ได้ตั้งไว้

TRIS ACADEMY of Management

COBIT Framework



ME1	Monitor and evaluate IT performance.
ME2	Monitor and evaluate internal control.
ME3	Ensure compliance with external requirements.
ME4	Provide IT governance.

PO1	Define a strategic IT plan.
PO2	Define the information architecture.
PO3	Determine technological direction.
PO4	Define the IT processes, organisation and relationships.
PO5	Manage the IT investment.
PO6	Communicate management aims and direction.
PO7	Manage IT human resources.
PO8	Manage quality.
PO9	Assess and manage IT risks.
PO10	Manage projects.

DS1	Define and manage service levels.
DS2	Manage third-party services.
DS3	Manage performance and capacity.
DS4	Ensure continuous service.
DS5	Ensure systems security.
DS6	Identify and allocate costs.
DS7	Educate and train users.
DS8	Manage service desk and incidents.
DS9	Manage the configuration.
DS10	Manage problems.
DS11	Manage data.
DS12	Manage the physical environment.
DS13	Manage operations.

AI1	Identify automated solutions.
AI2	Acquire and maintain application software.
AI3	Acquire and maintain technology infrastructure.
AI4	Enable operation and use.
AI5	Procure IT resources.
AI6	Manage changes.
AI7	Install and accredit solutions and changes.

TRIS ACADEMY of Management

PLAN AND ORGANIZE (PO)

PO1 Define a strategic IT plan.
PO2 Define the information architecture.
PO3 Determine technological direction.
PO4 Define the IT processes, organisation and relationships.
PO5 Manage the IT investment.
PO6 Communicate management aims and direction.
PO7 Manage IT human resources.
PO8 Manage quality.
PO9 Assess and manage IT risks.
PO10 Manage projects.

TRISACADEMY
of Management

ACQUIRE AND IMPLEMENT (AI)

AI1 Identify automated solutions.
AI2 Acquire and maintain application software.
AI3 Acquire and maintain technology infrastructure.
AI4 Enable operation and use.
AI5 Procure IT resources.
AI6 Manage changes.
AI7 Install and accredit solutions and changes.

TRISACADEMY
of Management

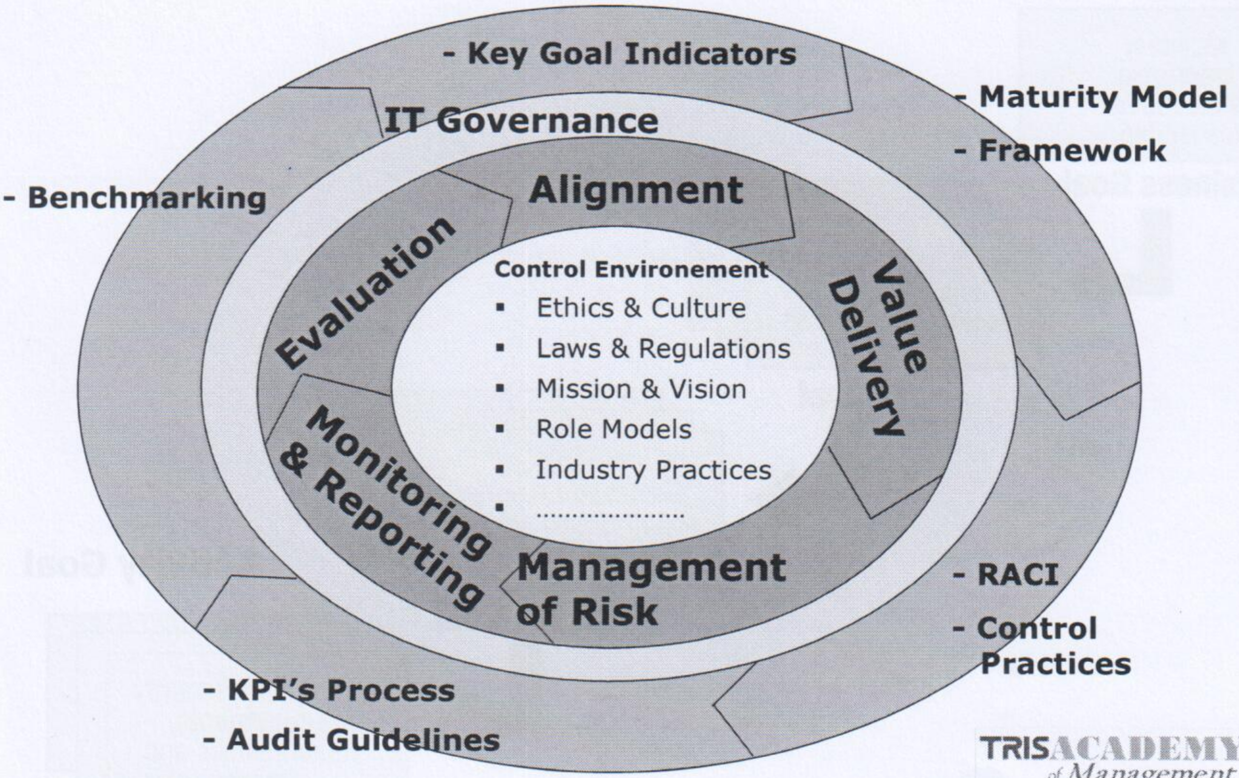
DELIVER AND SUPPORT (DS)

DS1 Define and manage service levels.
DS2 Manage third-party services.
DS3 Manage performance and capacity.
DS4 Ensure continuous service.
DS5 Ensure systems security.
DS6 Identify and allocate costs.
DS7 Educate and train users.
DS8 Manage service desk and incidents.
DS9 Manage the configuration.
DS10 Manage problems.
DS11 Manage data.
DS12 Manage the physical environment.
DS13 Manage operations.

MONITOR AND EVALUATE (ME)

ME1 Monitor and evaluate IT performance.
ME2 Monitor and evaluate internal control.
ME3 Ensure compliance with external requirements.
ME4 Provide IT governance.

CobiT Implementation



- Key Goal Indicators

- Maturity Model
- Framework

- Benchmarking

IT Governance

Alignment

Value Delivery

Management of Risk

Monitoring & Reporting

Evaluation

Control Environement

- Ethics & Culture
- Laws & Regulations
- Mission & Vision
- Role Models
- Industry Practices
- ………………….

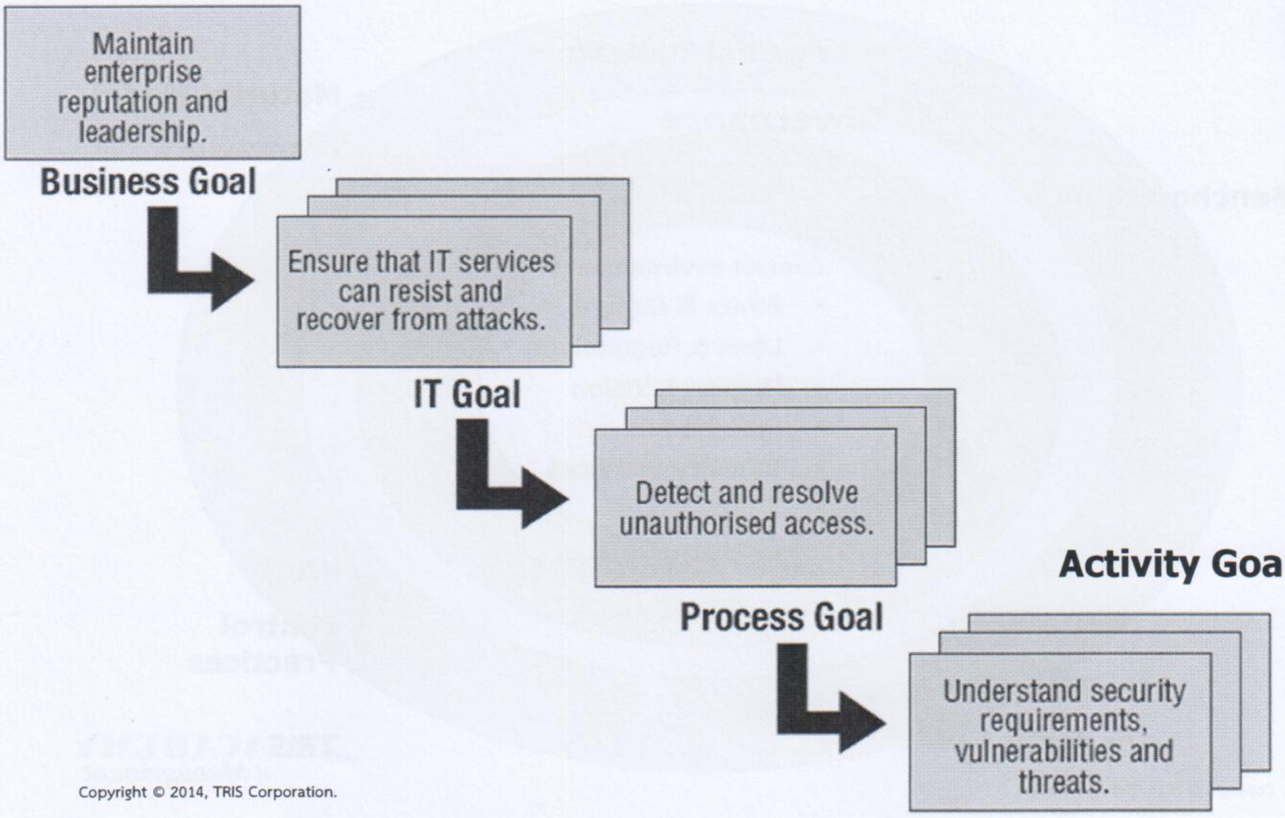
- RACI
- Control Practices

- KPI's Process
- Audit Guidelines

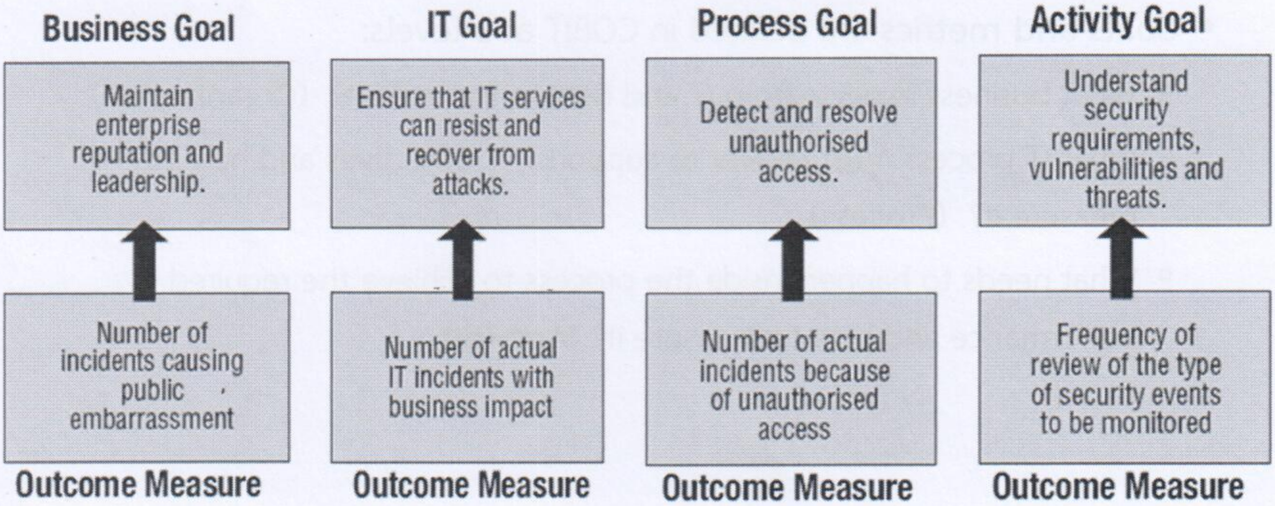
Performance measurement

- **Goals and metrics** are defined in COBIT at 3 levels:
  - What business expects from IT and how to measure it? **(Organization)**
  - What IT process must deliver to support IT's objectives and how to measure it? **(Process)**
  - What needs to happen inside the process to achieve the required performance and how to measure it? **(Activity)**

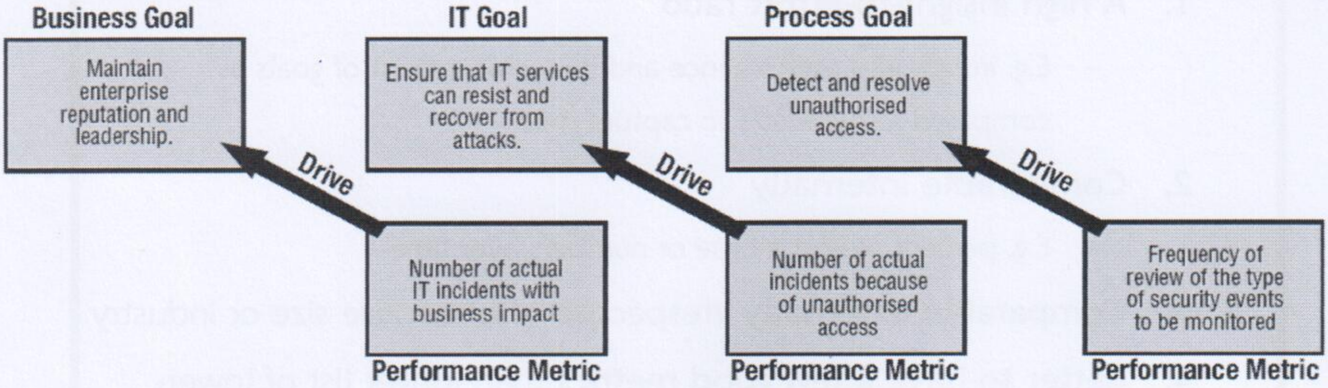
Example of goal relationships


Maintain enterprise reputation and leadership.
Business Goal
Ensure that IT services can resist and recover from attacks.
IT Goal
Detect and resolve unauthorised access.
Process Goal
Activity Goal
Understand security requirements, vulnerabilities and threats.

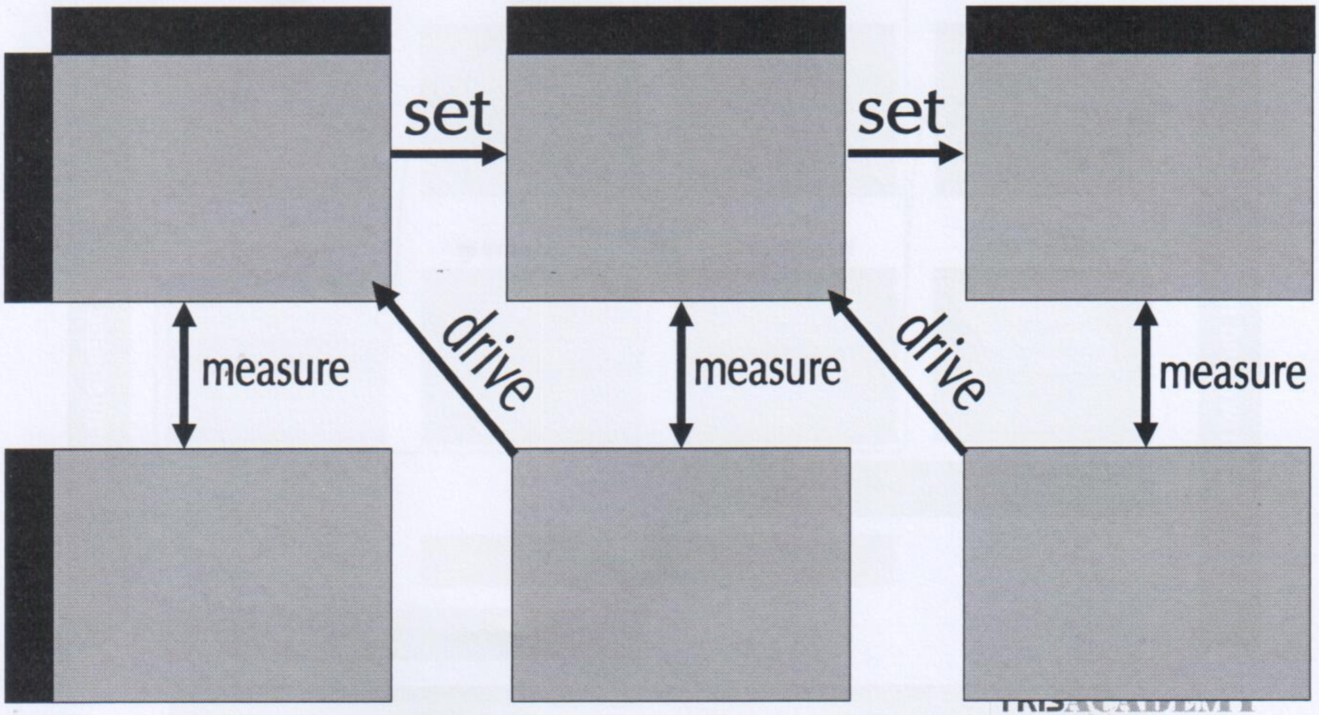
Example of outcome measures


Business Goal
IT Goal
Process Goal
Activity Goal
Maintain enterprise reputation and leadership.
Ensure that IT services can resist and recover from attacks.
Detect and resolve unauthorised access.
Understand security requirements, vulnerabilities and threats.
Number of incidents causing public embarrassment
Number of actual IT incidents with business impact
Number of actual incidents because of unauthorised access
Frequency of review of the type of security events to be monitored
Outcome Measure
Outcome Measure
Outcome Measure
Outcome Measure

Performance drivers


Business Goal
Maintain enterprise reputation and leadership.
IT Goal
Ensure that IT services can resist and recover from attacks.
Process Goal
Detect and resolve unauthorised access.
Drive
Drive
Drive
Number of actual IT incidents with business impact
Performance Metric
Number of actual incidents because of unauthorised access
Performance Metric
Frequency of review of the type of security events to be monitored
Performance Metric

Goal & Metrics in COBIT



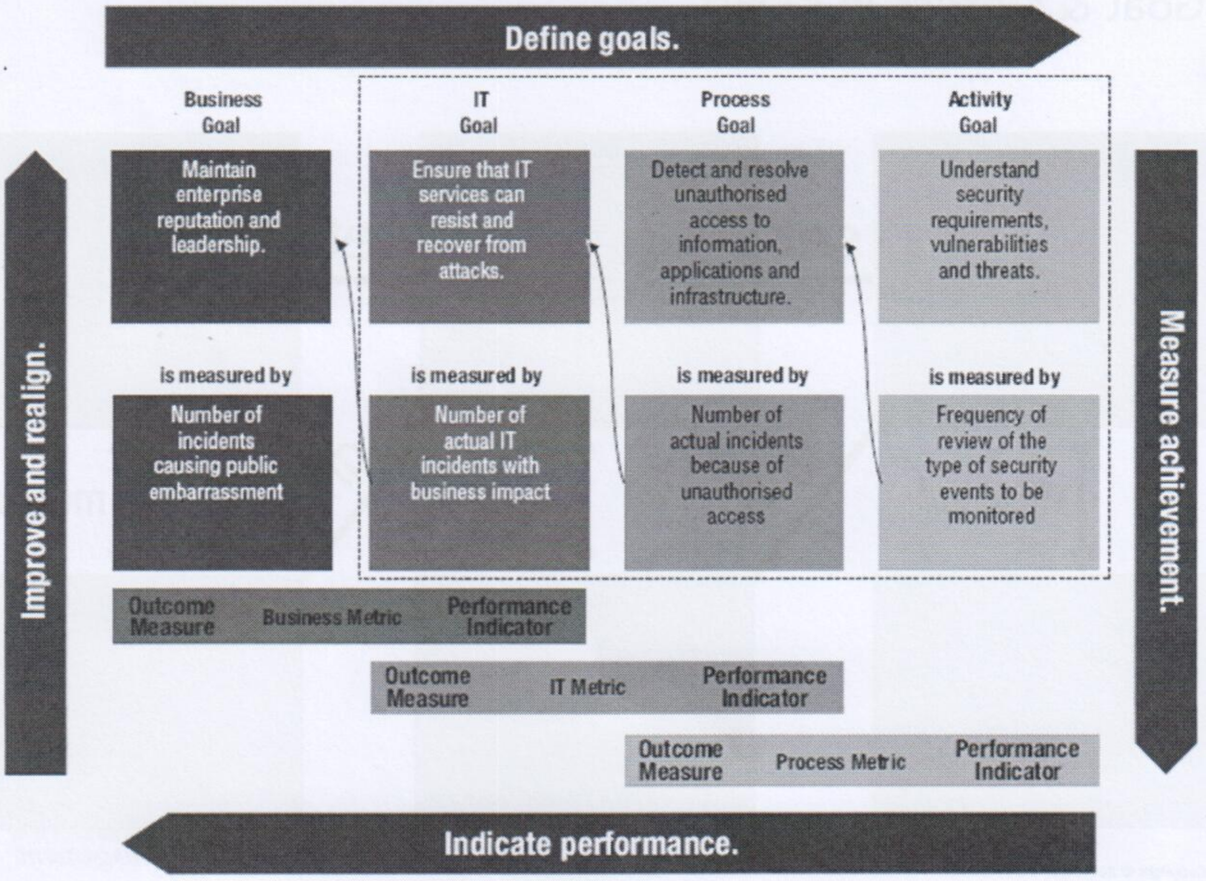
COBIT's Metrics

The metrics are developed based on the following characteristics:

1. **A high insight-to-effort ratio**
   - E.g. insight into performance and the achievement of goals as compared to the effort to capture them
2. **Comparable internally**
   - E.g. percent against a base or numbers over time
3. **Comparable externally** irrespective of enterprise size or industry
4. **Better to have a few good metrics** than longer list of lower-quality metrics
5. **Easy to measures**, not to be confused with target

TRIS ACADEMY of Management

Relationship among process, goals, and metrics



Define goals.

Business Goal	IT Goal	Process Goal	Activity Goal
Maintain enterprise reputation and leadership.	Ensure that IT services can resist and recover from attacks.	Detect and resolve unauthorised access to information, applications and infrastructure.	Understand security requirements, vulnerabilities and threats.
is measured by	is measured by	is measured by	is measured by
Number of incidents causing public embarrassment	Number of actual IT incidents with business impact	Number of actual incidents because of unauthorised access	Frequency of review of the type of security events to be monitored

Outcome Measure — Business Metric — Performance Indicator

Outcome Measure — IT Metric — Performance Indicator

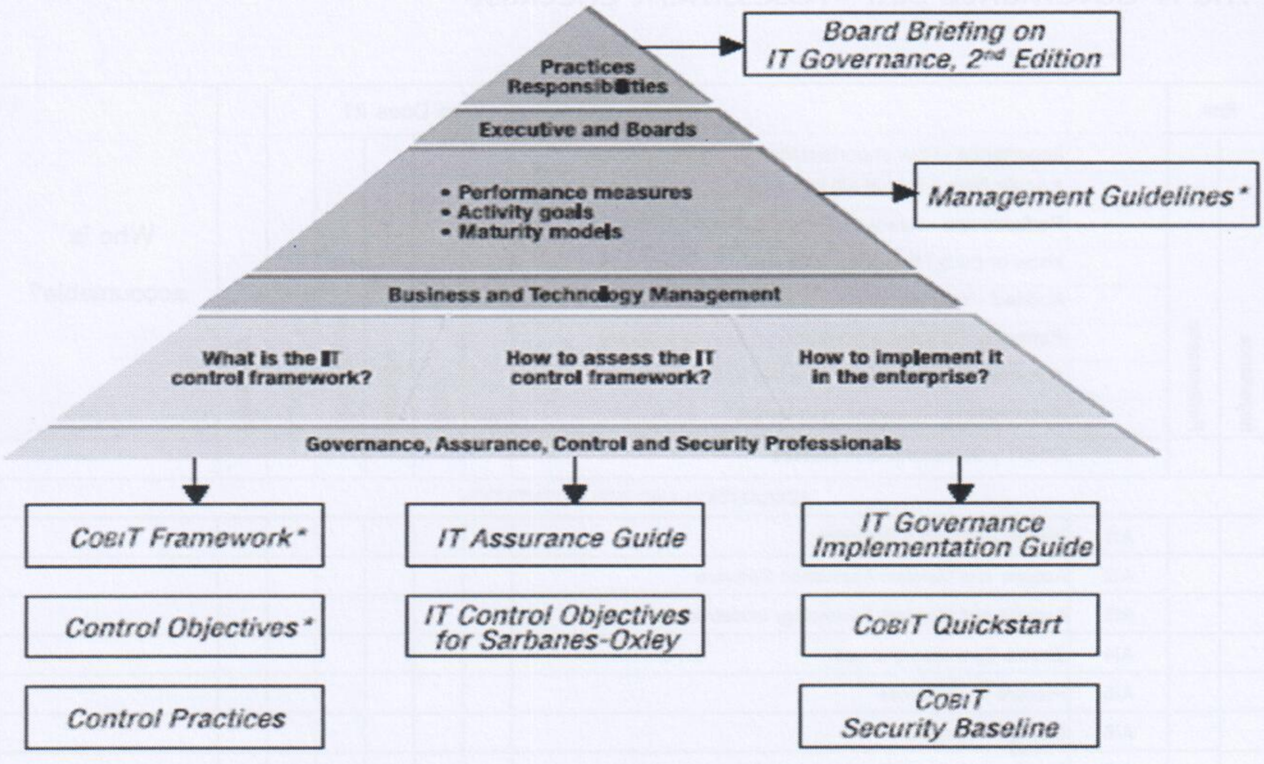
Outcome Measure — Process Metric — Performance Indicator

Improve and realign.

Measure achievement.

Indicate performance.

Figure 3—COBIT Products


Practices
Responsibilities
Board Briefing on IT Governance, 2nd Edition
Executive and Boards
• Performance measures
• Activity goals
• Maturity models
Management Guidelines*
Business and Technology Management
What is the IT control framework?
How to assess the IT control framework?
How to implement it in the enterprise?
Governance, Assurance, Control and Security Professionals
COBIT Framework*
IT Assurance Guide
IT Governance Implementation Guide
Control Objectives*
IT Control Objectives for Sarbanes-Oxley
COBIT Quickstart
Control Practices
COBIT Security Baseline

* Now integrated into COBIT 4.0

The IT Governance Self - Assessment Checklist

Risk				Who Does It?						
Importance	Performance		**Importance** - How important for the organization on a scale from 1 (not at all) to 5 (very) **Performance** - how well it is done, from 1 (don't know or badly) to 5 (very well) **Audited** - Yes, Nor or? **Formality** - is there a contract, an SLA or a clearly documente procedure? (Yes, No or ?) **Accountable** - Name or "don't know" COBIT's Domains and Processes	IT	Other	Outside	Don't Know	Audited	Formality	Who is accountable?
			PLANNING AND ORGANIZATION							
		PO1	Define a Strategic IT Plan							
		PO2	Define the Information Architecture							
		PO3	Determine the Technological Direction							
		PO4	Define the IT Processes, Organization and Relationships							
		PO5	Manage the IT Investment							
		PO6	Communicate Management aims and Direction							
		PO7	Manage IT Human Resources							
		PO8	Manage Quality							
		PO9	Assess and Manage IT Risks							
		PO10	Manage Projects							
		PO11	Manage Quality							

The IT Governance Self - Assessment Checklist

Risk			Importance - How important for the organization on' a scale from 1 (not at all) to 5 (very) Performance - how well it is done, from 1 (don't know or badly) to 5 (very well) Audited - Yes, Nor or? Formality - is there a contract, an SLA or a clearly documente procedure? (Yes, No or ?) Accountable - Name or "don't know"	Who Does It?						Who is accountable?
Importance	Performance		COBIT's Domains and Processes	IT	Other	Outside	Don't Know	Audited	Formality	
			ACQUISITION AND IMPLEMENTATION							
		AI1	Identify Automated Solutions							
		AI2	Acquire and Maintain Application Software							
		AI3	Acquire and Maintain Technology infrastructure							
		AI4	Enable Operation and use.							
		AI5	Procure IT resources							
		AI6	Manage Changes.							
		AI7	Install and Accredit Soultions and Changes							

TRISACADEMY
of Management

The IT Governance Self - Assessment Checklist

Risk			Importance - How important for the organization on a scale from 1 (not at all) to 5 (very) Performance - how well it is done, from 1 (don't know or badly) to 5 (very well) Audited - Yes, Nor or? Formality - is there a contract, an SLA or a clearly documente procedure? (Yes, No or ?) Accountable - Name or "don't know"	Who Does It?						Who is accountable?
Importance	Performance		COBIT's Domains and Processes	IT	Other	Outside	Don't Know	Audited	Formality	
			DELIVERY AND SUPPORT							
		DS1	Define and Manage Service Levels							
		DS2	Manage Third - party Services							
		DS3 '	Manage Performance and Capacity							
		DS4	Ensure Continuous Service							
		DS5	Ensure Systems Security							
		DS6	Identify and Allocate Costs							
		DS7	Educate and Train Users							
		DS8	Manage Service desk and Incidents							
		DS9	Manage the Configuration							
		DS10	Manage Problems							
		DS11	Manage Data							
		DS12	Manage the Physical Environment							
		DS13	Manage Operations							

MY
nent

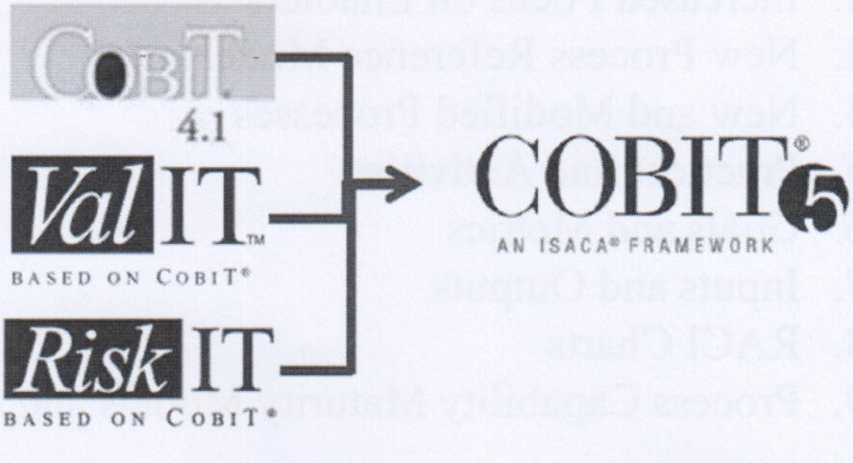
The COBIT 5 Framework

- Simply stated, COBIT 5 helps enterprises create optimal value from IT by maintaining a balance between realising benefits and optimising risk levels and resource use.
- COBIT 5 enables information and related technology to be governed and managed in a holistic manner for the entire enterprise, taking in the full end-to-end business and functional areas of responsibility, considering the IT-related interests of internal and external stakeholders.
- The COBIT 5 (5) principles and (7) enablers are generic and useful for enterprises of all sizes, whether commercial, not-for-profit or in the public sector.

TRIS ACADEMY of Management

Why COBIT 5?

COBIT 5 has clarified management level processes and integrated COBIT 4.1, Val IT and Risk IT content into one process reference model

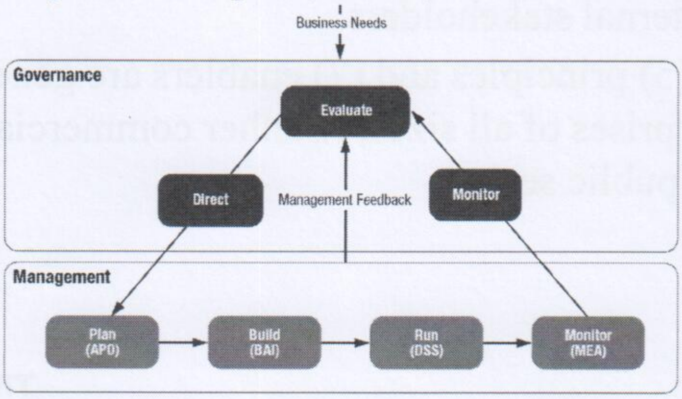


TRIS ACADEMY of Management

COBIT 5 Revised Framework

The COBIT 5 process reference model subdivides the IT-related practices and activities of the enterprise into two main areas—governance and management—with management further divided into domains of processes:

- The GOVERNANCE domain contains five governance processes; within each process, evaluate, direct and monitor (EDM) practices are defined.
- The four MANAGEMENT domains are in line with the responsibility areas of plan, build, run and monitor (PBRM)

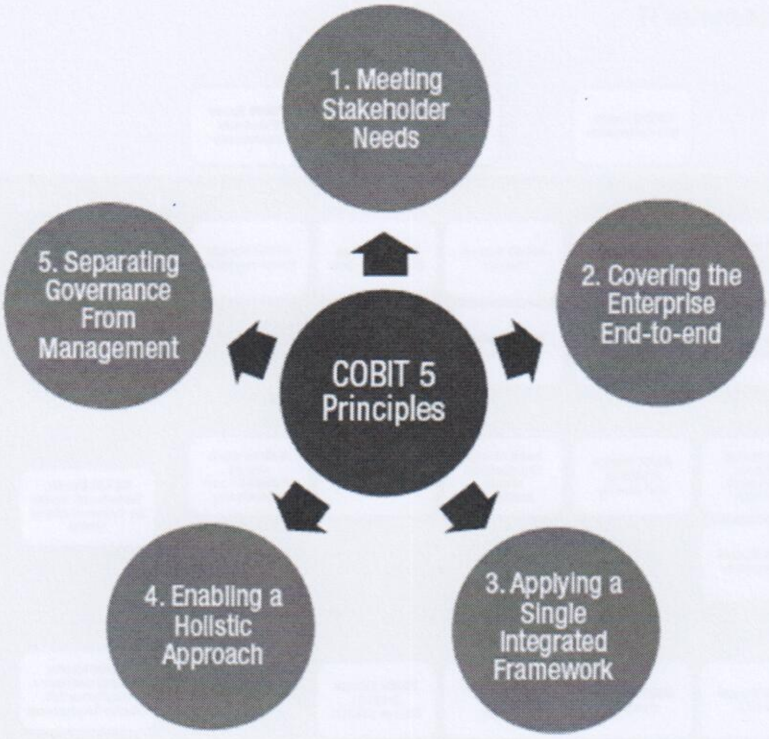


Source: COBIT® 5, figure 15. © 2012 ISACA® All rights reserved.

Areas of Change

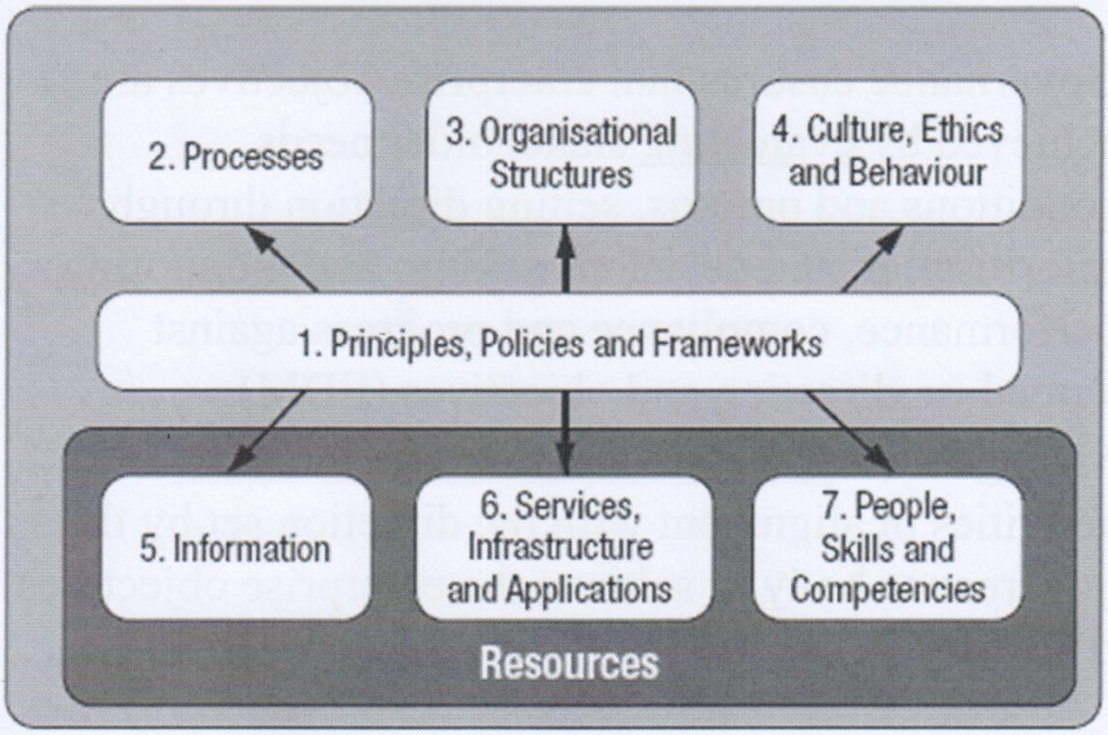
- The following slides summarise the major changes in COBIT 5 content and how they may impact GEIT implementation/improvement:
  1. New GEIT Principles
  2. Increased Focus on Enablers
  3. New Process Reference Model
  4. New and Modified Processes
  5. Practices and Activities
  6. Goals and Metrics
  7. Inputs and Outputs
  8. RACI Charts
  9. Process Capability Maturity Models and Assessments

COBIT 5 Principles


1. Meeting Stakeholder Needs
2. Covering the Enterprise End-to-end
3. Applying a Single Integrated Framework
4. Enabling a Holistic Approach
5. Separating Governance From Management
COBIT 5 Principles

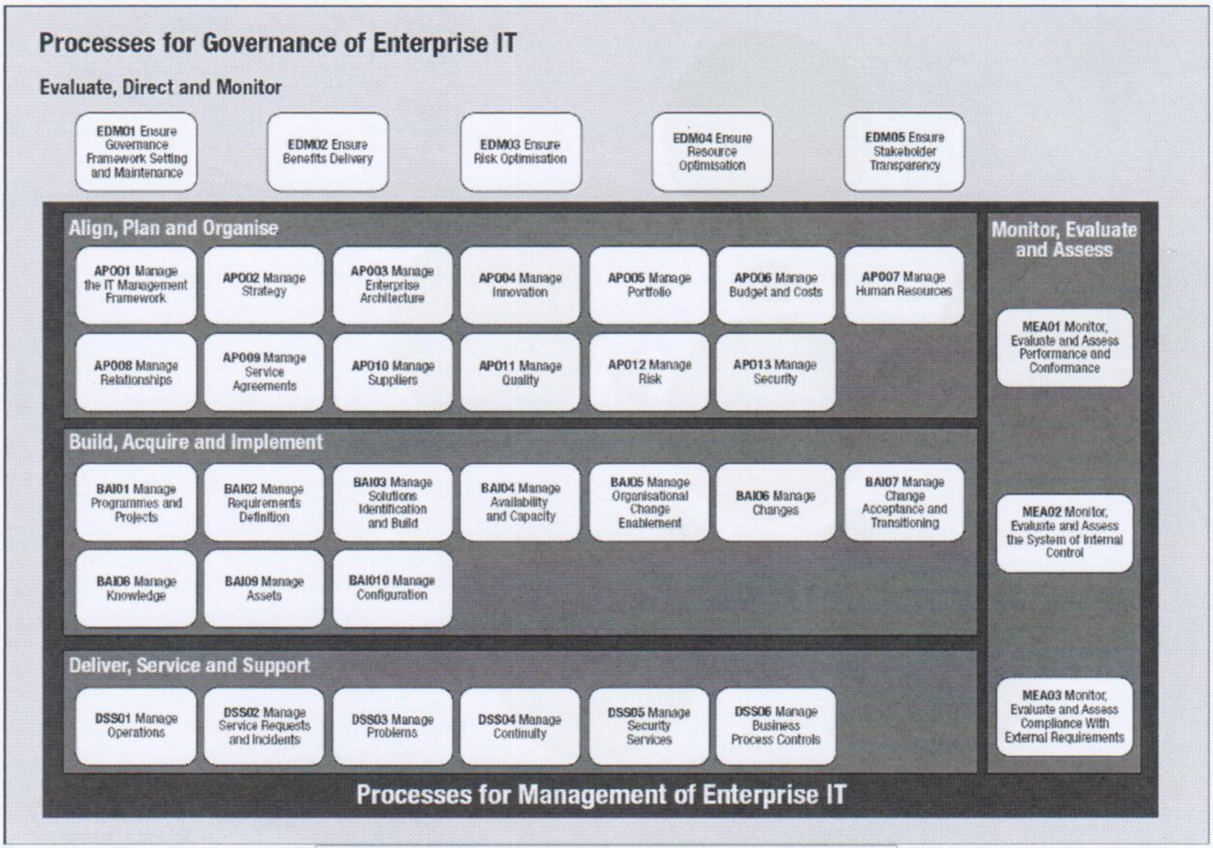
Source: COBIT® 5, figure 2. © 2012 ISACA® All rights reserved.

COBIT 5 Enablers


2. Processes
3. Organisational Structures
4. Culture, Ethics and Behaviour
1. Principles, Policies and Frameworks
5. Information
6. Services, Infrastructure and Applications
7. People, Skills and Competencies
Resources

Source: COBIT® 5, figure 12. © 2012 ISACA® All rights reserved.

New Process Reference Model



Processes for Governance of Enterprise IT

Evaluate, Direct and Monitor

EDM01 Ensure Governance Framework Setting and Maintenance

EDM02 Ensure Benefits Delivery

EDM03 Ensure Risk Optimisation

EDM04 Ensure Resource Optimisation

EDM05 Ensure Stakeholder Transparency

Align, Plan and Organise

APO01 Manage the IT Management Framework

APO02 Manage Strategy

APO03 Manage Enterprise Architecture

APO04 Manage Innovation

APO05 Manage Portfolio

APO06 Manage Budget and Costs

APO07 Manage Human Resources

APO08 Manage Relationships

APO09 Manage Service Agreements

APO10 Manage Suppliers

APO11 Manage Quality

APO12 Manage Risk

APO13 Manage Security

Monitor, Evaluate and Assess

MEA01 Monitor, Evaluate and Assess Performance and Conformance

MEA02 Monitor, Evaluate and Assess the System of Internal Control

MEA03 Monitor, Evaluate and Assess Compliance With External Requirements

Build, Acquire and Implement

BAI01 Manage Programmes and Projects

BAI02 Manage Requirements Definition

BAI03 Manage Solutions Identification and Build

BAI04 Manage Availability and Capacity

BAI05 Manage Organisational Change Enablement

BAI06 Manage Changes

BAI07 Manage Change Acceptance and Transitioning

BAI08 Manage Knowledge

BAI09 Manage Assets

BAI010 Manage Configuration

Deliver, Service and Support

DSS01 Manage Operations

DSS02 Manage Service Requests and Incidents

DSS03 Manage Problems

DSS04 Manage Continuity

DSS05 Manage Security Services

DSS06 Manage Business Process Controls

Processes for Management of Enterprise IT

Source: COBIT® 5, figure 16. © 2012 ISACA® All rights reserved.

Governance and Management

- Governance ensures that enterprise objectives are achieved by evaluating stakeholder needs, conditions and options; setting direction through prioritisation and decision making; and monitoring performance, compliance and progress against agreed-on direction and objectives (EDM).
- Management plans, builds, runs and monitors activities in alignment with the direction set by the governance body to achieve the enterprise objectives (PBRM).

In Summary ...

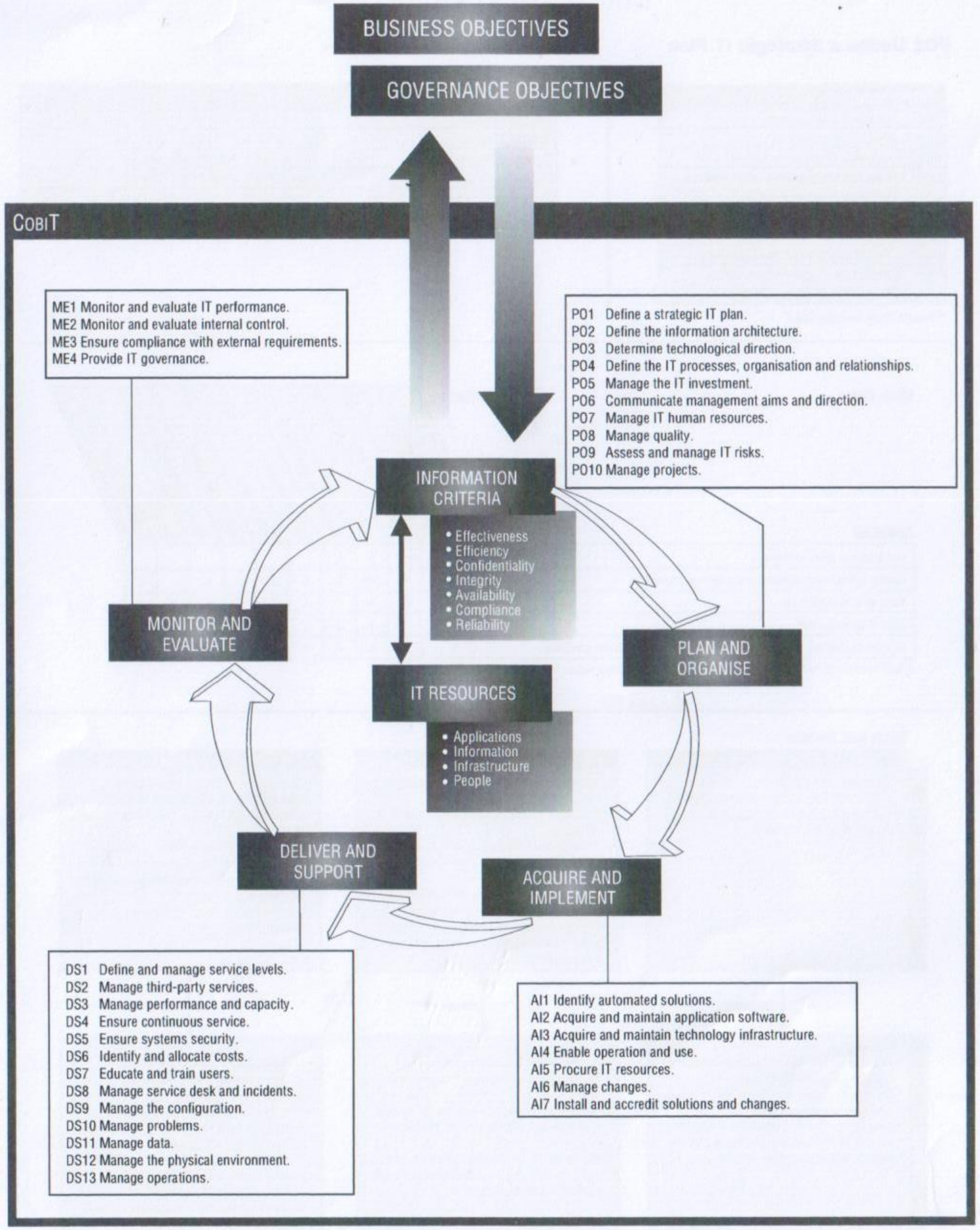
COBIT 5 brings together the five principles that allow the enterprise to build an effective governance and management framework based on a holistic set of seven enablers that optimises information and technology investment and use for the benefit of stakeholders.

TRIS ACADEMY of Management

Q & A

Thank You

สถาบันวิทยาการจัดการ
TRIS Academy of Management
บริษัท ทริส คอร์ปอเรชั่น จำกัด
อาคารสีลมคอมเพล็กซ์ ชั้น 24
เลขที่ 191 ถนนสีลม แขวงสีลม เขตบางรัก กรุงเทพฯ 10150
โทรศัพท์ 0 2231 3011 ต่อ318 โทรสาร 0 2231 3680
e-Mail : trisacademy@tris.co.th
www.trisacademy.com



ME1 Monitor and evaluate IT performance.
ME2 Monitor and evaluate internal control.
ME3 Ensure compliance with external requirements.
ME4 Provide IT governance.

PO1 Define a strategic IT plan.
PO2 Define the information architecture.
PO3 Determine technological direction.
PO4 Define the IT processes, organisation and relationships.
PO5 Manage the IT investment.
PO6 Communicate management aims and direction.
PO7 Manage IT human resources.
PO8 Manage quality.
PO9 Assess and manage IT risks.
PO10 Manage projects.

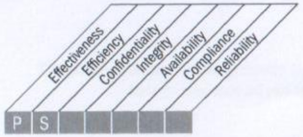
DS1 Define and manage service levels.
DS2 Manage third-party services.
DS3 Manage performance and capacity.
DS4 Ensure continuous service.
DS5 Ensure systems security.
DS6 Identify and allocate costs.
DS7 Educate and train users.
DS8 Manage service desk and incidents.
DS9 Manage the configuration.
DS10 Manage problems.
DS11 Manage data.
DS12 Manage the physical environment.
DS13 Manage operations.

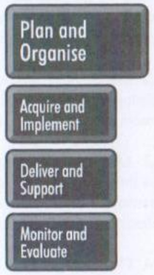
AI1 Identify automated solutions.
AI2 Acquire and maintain application software.
AI3 Acquire and maintain technology infrastructure.
AI4 Enable operation and use.
AI5 Procure IT resources.
AI6 Manage changes.
AI7 Install and accredit solutions and changes.

Process Description

PO1 Define a Strategic IT Plan

IT strategic planning is required to manage and direct all IT resources in line with the business strategy and priorities. The IT function and business stakeholders are responsible for ensuring that optimal value is realised from project and service portfolios. The strategic plan improves key stakeholders' understanding of IT opportunities and limitations, assesses current performance, identifies capacity and human resource requirements, and clarifies the level of investment required. The business strategy and priorities are to be reflected in portfolios and executed by the IT tactical plan(s), which specifies concise objectives, action plans and tasks that are understood and accepted by both business and IT.





Control over the IT process of

Define a strategic IT plan

that satisfies the business requirement for IT of

sustaining or extending the business strategy and governance requirements whilst being transparent about benefits, costs and risks

by focusing on

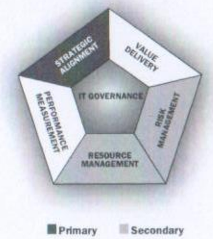
incorporating IT and business management in the translation of business requirements into service offerings, and the development of strategies to deliver these services in a transparent and effective manner

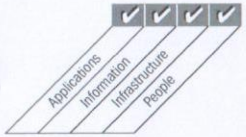
is achieved by

- Engaging with business and senior management in aligning IT strategic planning with current and future business needs
- Understanding current IT capabilities
- Providing for a prioritisation scheme for the business objectives that quantifies the business requirements

and is measured by

- Percent of IT objectives in the IT strategic plan that support the strategic business plan
- Percent of IT projects in the IT project portfolio that can be directly traced back to the IT tactical plans
- Delay between updates of IT strategic plan and updates of IT tactical plans





Control Objectives

PO1 Define a Strategic IT Plan

PO1.1 IT Value Management
Work with the business to ensure that the enterprise portfolio of IT-enabled investments contains programmes that have solid business cases. Recognise that there are mandatory, sustaining and discretionary investments that differ in complexity and degree of freedom in allocating funds. IT processes should provide effective and efficient delivery of the IT components of programmes and early warning of any deviations from plan, including cost, schedule or functionality, that might impact the expected outcomes of the programmes. IT services should be executed against equitable and enforceable service level agreements (SLAs). Accountability for achieving the benefits and controlling the costs should be clearly assigned and monitored. Establish fair, transparent, repeatable and comparable evaluation of business cases, including financial worth, the risk of not delivering a capability and the risk of not realising the expected benefits.

PO1.2 Business-IT Alignment
Establish processes of bi-directional education and reciprocal involvement in strategic planning to achieve business and IT alignment and integration. Mediate between business and IT imperatives so priorities can be mutually agreed.

PO1.3 Assessment of Current Capability and Performance
Assess the current capability and performance of solution and service delivery to establish a baseline against which future requirements can be compared. Define performance in terms of IT's contribution to business objectives, functionality, stability, complexity, costs, strengths and weaknesses.

PO1.4 IT Strategic Plan
Create a strategic plan that defines, in co-operation with relevant stakeholders, how IT goals will contribute to the enterprise's strategic objectives and related costs and risks. It should include how IT will support IT-enabled investment programmes, IT services and IT assets. IT should define how the objectives will be met, the measurements to be used and the procedures to obtain formal sign-off from the stakeholders. The IT strategic plan should cover investment/operational budget, funding sources, sourcing strategy, acquisition strategy, and legal and regulatory requirements. The strategic plan should be sufficiently detailed to allow for the definition of tactical IT plans.

PO1.5 IT Tactical Plans
Create a portfolio of tactical IT plans that are derived from the IT strategic plan. The tactical plans should address IT-enabled programme investments, IT services and IT assets. The tactical plans should describe required IT initiatives, resource requirements, and how the use of resources and achievement of benefits will be monitored and managed. The tactical plans should be sufficiently detailed to allow the definition of project plans. Actively manage the set of tactical IT plans and initiatives through analysis of project and service portfolios.

PO1.6 IT Portfolio Management
Actively manage with the business the portfolio of IT-enabled investment programmes required to achieve specific strategic business objectives by identifying, defining, evaluating, prioritising, selecting, initiating, managing and controlling programmes. This should include clarifying desired business outcomes, ensuring that programme objectives support achievement of the outcomes, understanding the full scope of effort required to achieve the outcomes, assigning clear accountability with supporting measures, defining projects within the programme, allocating resources and funding, delegating authority, and commissioning required projects at programme launch.

Management Guidelines

PO1 Define a Strategic IT Plan

From	Inputs
PO5	Cost-benefits reports
PO9	Risk assessment
PO10	Updated IT project portfolio
DS1	New/updated service requirements; updated IT service portfolio
*	Business strategy and priorities
*	Programme portfolio
ME1	Performance input to IT planning
ME4	Report on IT governance status; enterprise strategic direction for IT

* Inputs from outside CobiT

Outputs	To					
Strategic IT plan	PO2...PO6	PO8	PO9	AI1	DS1	
Tactical IT plans	PO2...PO6	PO9	AI1	DS1		
IT project portfolio	PO5	PO6	PO10	AI6		
IT service portfolio	PO5	PO6	PO9	DS1		
IT sourcing strategy	DS2					
IT acquisition strategy	AI5					

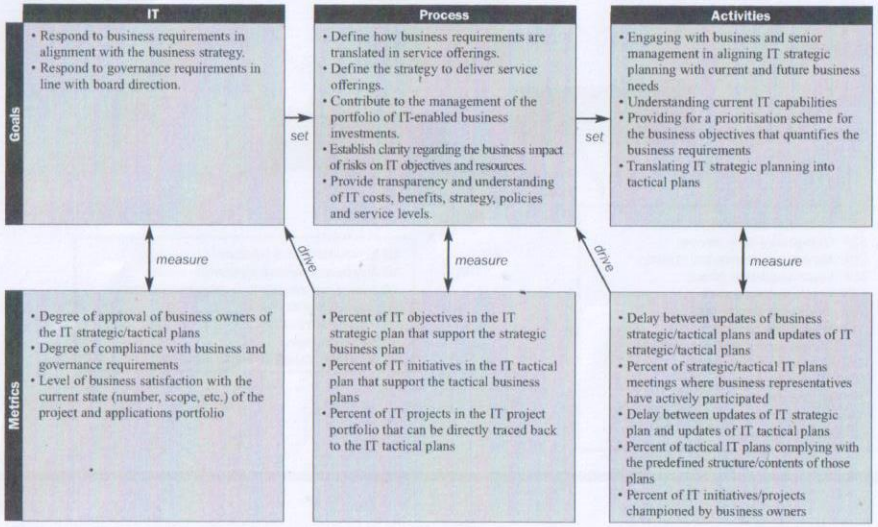
RACI Chart

Activities	Functions: CEO	CFO	Business Executive	CIO	Business Process Owner	Head Operations	Chief Architect	Head Development	Head IT Administration	PMO	Compliance, Audit, Risk and Security
Link business goals to IT goals.	C	I	A/R	R	C						
Identify critical dependencies and current performance.	C	C	R	A/R	C	C	C	C	C		C
Build an IT strategic plan.	A	C	C	R	I	C	C	C	C	I	C
Build IT tactical plans.	C	I		A	C	C	C	C	C	R	I
Analyse programme portfolios and manage project and service portfolios.	C	I	I	A	R	R	C	R	C	C	I

A **RACI** chart identifies who is **R**esponsible, **A**ccountable, **C**onsulted and/or **I**nformed.

รับผิด

Goals and Metrics



IT – Goals:
- Respond to business requirements in alignment with the business strategy.
- Respond to governance requirements in line with board direction.

Process – Goals:
- Define how business requirements are translated in service offerings.
- Define the strategy to deliver service offerings.
- Contribute to the management of the portfolio of IT-enabled business investments.
- Establish clarity regarding the business impact of risks on IT objectives and resources.
- Provide transparency and understanding of IT costs, benefits, strategy, policies and service levels.

Activities – Goals:
- Engaging with business and senior management in aligning IT strategic planning with current and future business needs
- Understanding current IT capabilities
- Providing for a prioritisation scheme for the business objectives that quantifies the business requirements
- Translating IT strategic planning into tactical plans

IT – Metrics:
- Degree of approval of business owners of the IT strategic/tactical plans
- Degree of compliance with business and governance requirements
- Level of business satisfaction with the current state (number, scope, etc.) of the project and applications portfolio

Process – Metrics:
- Percent of IT objectives in the IT strategic plan that support the strategic business plan
- Percent of IT initiatives in the IT tactical plan that support the tactical business plans
- Percent of IT projects in the IT project portfolio that can be directly traced back to the IT tactical plans

Activities – Metrics:
- Delay between updates of business strategic/tactical plans and updates of IT strategic/tactical plans
- Percent of strategic/tactical IT plans meetings where business representatives have actively participated
- Delay between updates of IT strategic plan and updates of IT tactical plans
- Percent of tactical IT plans complying with the predefined structure/contents of those plans
- Percent of IT initiatives/projects championed by business owners

Maturity Model

PO1 Define a Strategic IT Plan

Management of the process of *Define a strategic IT plan* that satisfies the business requirement for IT of *sustaining or extending the business strategy and governance requirements whilst being transparent about benefits, costs and risks* is:

0 Non-existent when
IT strategic planning is not performed. There is no management awareness that IT strategic planning is needed to support business goals.

1 Initial/*Ad Hoc* when
The need for IT strategic planning is known by IT management. IT planning is performed on an as-needed basis in response to a specific business requirement. IT strategic planning is occasionally discussed at IT management meetings. The alignment of business requirements, applications and technology takes place reactively rather than by an organisationwide strategy. The strategic risk position is identified informally on a project-by-project basis.

2 Repeatable but Intuitive when
IT strategic planning is shared with business management on an as-needed basis. Updating of the IT plans occurs in response to requests by management. Strategic decisions are driven on a project-by-project basis without consistency with an overall organisation strategy. The risks and user benefits of major strategic decisions are recognised in an intuitive way.

3 Defined when
A policy defines when and how to perform IT strategic planning. IT strategic planning follows a structured approach that is documented and known to all staff. The IT planning process is reasonably sound and ensures that appropriate planning is likely to be performed. However, discretion is given to individual managers with respect to implementation of the process, and there are no procedures to examine the process. The overall IT strategy includes a consistent definition of risks that the organisation is willing to take as an innovator or follower. The IT financial, technical and human resources strategies increasingly influence the acquisition of new products and technologies. IT strategic planning is discussed at business management meetings.

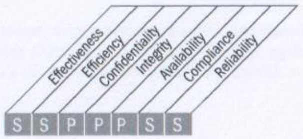
4 Managed and Measurable when
IT strategic planning is standard practice and exceptions would be noticed by management. IT strategic planning is a defined management function with senior-level responsibilities. Management is able to monitor the IT strategic planning process, make informed decisions based on it and measure its effectiveness. Both short-range and long-range IT planning occurs and is cascaded down into the organisation, with updates done as needed. The IT strategy and organisationwide strategy are increasingly becoming more co-ordinated by addressing business processes and value-added capabilities and leveraging the use of applications and technologies through business process re-engineering. There is a well-defined process for determining the usage of internal and external resources required in system development and operations.

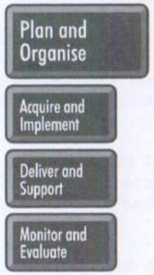
5 Optimised when
IT strategic planning is a documented, living process; is continuously considered in business goal setting; and results in discernible business value through investments in IT. Risk and value-added considerations are continuously updated in the IT strategic planning process. Realistic long-range IT plans are developed and constantly updated to reflect changing technology and business-related developments. Benchmarking against well-understood and reliable industry norms takes place and is integrated with the strategy formulation process. The strategic plan includes how new technology developments can drive the creation of new business capabilities and improve the competitive advantage of the organisation.

Process Description

PO9 Assess and Manage IT Risks

A risk management framework is created and maintained. The framework documents a common and agreed-upon level of IT risks, mitigation strategies and residual risks. Any potential impact on the goals of the organisation caused by an unplanned event is identified, analysed and assessed. Risk mitigation strategies are adopted to minimise residual risk to an accepted level. The result of the assessment is understandable to the stakeholders and expressed in financial terms, to enable stakeholders to align risk to an acceptable level of tolerance.





Control over the IT process of

Assess and manage IT risks

that satisfies the business requirement for IT of

analysing and communicating IT risks and their potential impact on business processes and goals

by focusing on

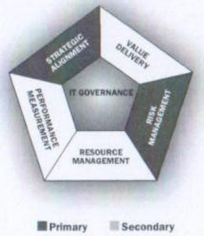
development of a risk management framework that is integrated in business and operational risk management frameworks, risk assessment, risk mitigation and communication of residual risk

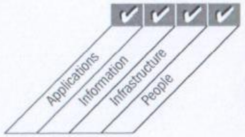
is achieved by

- Ensuring that risk management is fully embedded in management processes, internally and externally, and consistently applied
- Performing risk assessments
- Recommending and communicating risk remediation action plans

and is measured by

- Percent of critical IT objectives covered by risk assessment
- Percent of identified critical IT risks with action plans developed
- Percent of risk management action plans approved for implementation





Control Objectives

PO9 Assess and Manage IT Risks

PO9.1 IT Risk Management Framework
Establish an IT risk management framework that is aligned to the organisation's (enterprise's) risk management framework.

PO9.2 Establishment of Risk Context
Establish the context in which the risk assessment framework is applied to ensure appropriate outcomes. This should include determining the internal and external context of each risk assessment, the goal of the assessment, and the criteria against which risks are evaluated.

PO9.3 Event Identification
Identify events (an important realistic threat that exploits a significant applicable vulnerability) with a potential negative impact on the goals or operations of the enterprise, including business, regulatory, legal, technology, trading partner, human resources and operational aspects. Determine the nature of the impact and maintain this information. Record and maintain relevant risks in a risk registry.

PO9.4 Risk Assessment
Assess on a recurrent basis the likelihood and impact of all identified risks, using qualitative and quantitative methods. The likelihood and impact associated with inherent and residual risk should be determined individually, by category and on a portfolio basis.

PO9.5 Risk Response
Develop and maintain a risk response process designed to ensure that cost-effective controls mitigate exposure to risks on a continuing basis. The risk response process should identify risk strategies such as avoidance, reduction, sharing or acceptance; determine associated responsibilities; and consider risk tolerance levels.

PO9.6 Maintenance and Monitoring of a Risk Action Plan
Prioritise and plan the control activities at all levels to implement the risk responses identified as necessary, including identification of costs, benefits and responsibility for execution. Obtain approval for recommended actions and acceptance of any residual risks, and ensure that committed actions are owned by the affected process owner(s). Monitor execution of the plans, and report on any deviations to senior management.

Management Guidelines

PO9 Assess and Manage IT Risks

From	Inputs
PO1	Strategic and tactical IT plans, IT service portfolio
PO10	Project risk management plan
DS2	Supplier risks
DS4	Contingency test results
DS5	Security threats and vulnerabilities
ME1	Historical risk trends and events
ME4	Enterprise appetite for IT risks

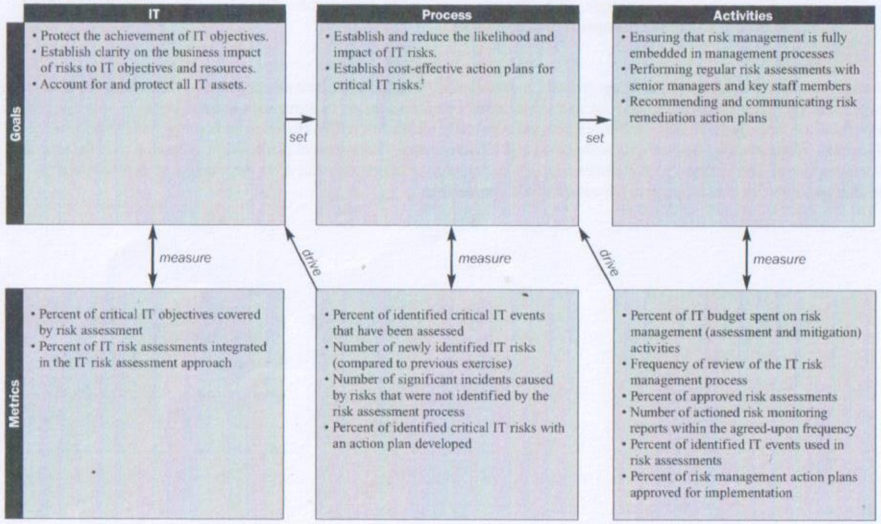
Outputs	To						
Risk assessment	PO1	DS4	DS5	DS12	ME4		
Risk reporting	ME4						
IT-related risk management guidelines	PO6						
IT-related risk remedial action plans	PO4	AI6					

RACI Chart

Activities	CEO	CFO	Business Executive	CIO	Business Senior Mangement	Head Operations	Chief Architect	Head Development	Head IT Administration	PMO	Compliance, Audit, Risk and Security
Determine risk management alignment (e.g., assess risk).	A	R/A	C	C	R/A	I					I
Understand relevant strategic business objectives.		C	C	R/A	C	C					I
Understand relevant business process objectives.				C	C	R/A					I
Identify internal IT objectives, and establish risk context.					R/A		C	C	C		I
Identify events associated with objectives (some events are business-oriented [business is A]; some are IT-oriented [IT is A, business is C]).	I			A/C	A	R	R	R	R		C
Assess risk associated with events.				A/C	A	R	R	R	R		C
Evaluate and select risk responses.	I	I	A	A/C	A	R	R	R	R		C
Prioritise and plan control activities.	C	C	A	A	R	R	C	C	C		C
Approve and ensure funding for risk action plans.		A	A		R	I	I	I	I		I
Maintain and monitor a risk action plan.	A	C	I	R	R	C	C	C	C	C	R

A **RACI** chart identifies who is **R**esponsible, **A**ccountable, **C**onsulted and/or **I**nformed.

Goals and Metrics



Goals

IT
- Protect the achievement of IT objectives.
- Establish clarity on the business impact of risks to IT objectives and resources.
- Account for and protect all IT assets.

Process
- Establish and reduce the likelihood and impact of IT risks.
- Establish cost-effective action plans for critical IT risks.[†]

Activities
- Ensuring that risk management is fully embedded in management processes
- Performing regular risk assessments with senior managers and key staff members
- Recommending and communicating risk remediation action plans

Metrics

- Percent of critical IT objectives covered by risk assessment
- Percent of IT risk assessments integrated in the IT risk assessment approach

- Percent of identified critical IT events that have been assessed
- Number of newly identified IT risks (compared to previous exercise)
- Number of significant incidents caused by risks that were not identified by the risk assessment process
- Percent of identified critical IT risks with an action plan developed

- Percent of IT budget spent on risk management (assessment and mitigation) activities
- Frequency of review of the IT risk management process
- Percent of approved risk assessments
- Number of actioned risk monitoring reports within the agreed-upon frequency
- Percent of identified IT events used in risk assessments
- Percent of risk management action plans approved for implementation

Maturity Model

PO9 Assess and Manage IT Risks

Management of the process of *Assess and manage IT risks* that satisfies the business requirement for IT of *analysing and communicating IT risks and their potential impact on business processes and goals* is:

0 Non-existent when
Risk assessment for processes and business decisions does not occur. The organisation does not consider the business impacts associated with security vulnerabilities and development project uncertainties. Risk management is not identified as relevant to acquiring IT solutions and delivering IT services.

1 Initial/*Ad Hoc* when
IT risks are considered in an *ad hoc* manner. Informal assessments of project risk take place as determined by each project. Risk assessments are sometimes identified in a project plan but are rarely assigned to specific managers. Specific IT-related risks, such as security, availability and integrity, are occasionally considered on a project-by-project basis. IT-related risks affecting day-to-day operations are seldom discussed at management meetings. Where risks have been considered, mitigation is inconsistent. There is an emerging understanding that IT risks are important and need to be considered.

2 Repeatable but Intuitive when
A developing risk assessment approach exists and is implemented at the discretion of the project managers. The risk management is usually at a high level and is typically applied only to major projects or in response to problems. Risk mitigation processes are starting to be implemented where risks are identified.

3 Defined when
An organisationwide risk management policy defines when and how to conduct risk assessments. Risk management follows a defined process that is documented. Risk management training is available to all staff members. Decisions to follow the risk management process and receive training are left to the individual's discretion. The methodology for the assessment of risk is convincing and sound and ensures that key risks to the business are identified. A process to mitigate key risks is usually instituted once the risks are identified. Job descriptions consider risk management responsibilities.

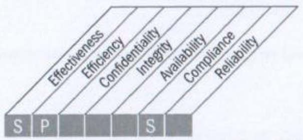
4 Managed and Measurable when
The assessment and management of risk are standard procedures. Exceptions to the risk management process are reported to IT management. IT risk management is a senior management-level responsibility. Risk is assessed and mitigated at the individual project level and also regularly with regard to the overall IT operation. Management is advised on changes in the business and IT environment that could significantly affect the IT-related risk scenarios. Management is able to monitor the risk position and make informed decisions regarding the exposure it is willing to accept. All identified risks have a nominated owner, and senior management and IT management determine the levels of risk that the organisation will tolerate. IT management develops standard measures for assessing risk and defining risk/return ratios. Management budgets for an operational risk management project to reassess risks on a regular basis. A risk management database is established, and part of the risk management processes is beginning to be automated. IT management considers risk mitigation strategies.

5 Optimised when
Risk management develops to the stage where a structured, organisationwide process is enforced and well managed. Good practices are applied across the entire organisation. The capture, analysis and reporting of risk management data are highly automated. Guidance is drawn from leaders in the field, and the IT organisation takes part in peer groups to exchange experiences. Risk management is truly integrated into all business and IT operations, is well accepted and extensively involves the users of IT services. Management detects and acts when major IT operational and investment decisions are made without consideration of the risk management plan. Management continually assesses risk mitigation strategies.

Process Description

AI5 Procure IT Resources

IT resources, including people, hardware, software and services, need to be procured. This requires the definition and enforcement of procurement procedures, the selection of vendors, the setup of contractual arrangements, and the acquisition itself. Doing so ensures that the organisation has all required IT resources in a timely and cost-effective manner.



Control over the IT process of

Procure IT resources

that satisfies the business requirement for IT of

improving IT's cost-efficiency and its contribution to business profitability

by focusing on

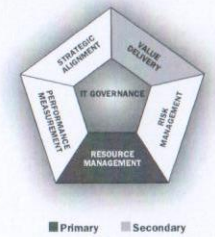
acquiring and maintaining IT skills that respond to the delivery strategy, an integrated and standardised IT infrastructure, and reducing IT procurement risk

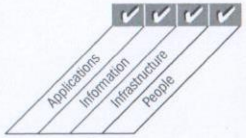
is achieved by

- Obtaining professional legal and contractual advice
- Defining procurement procedures and standards
- Procuring requested hardware, software and services in line with defined procedures

and is measured by

- Number of disputes related to procurement contracts
- Amount of reduction of the purchasing cost
- Percent of key stakeholders satisfied with suppliers





Control Objectives

AI5 Procure IT Resources

AI5.1 Procurement Control
Develop and follow a set of procedures and standards that is consistent with the business organisation's overall procurement process and acquisition strategy to acquire IT-related infrastructure, facilities, hardware, software and services needed by the business.

AI5.2 Supplier Contract Management
Set up a procedure for establishing, modifying and terminating contracts for all suppliers. The procedure should cover, at a minimum, legal, financial, organisational, documentary, performance, security, intellectual property, and termination responsibilities and liabilities (including penalty clauses). All contracts and contract changes should be reviewed by legal advisors.

AI5.3 Supplier Selection
Select suppliers according to a fair and formal practice to ensure a viable best fit based on specified requirements. Requirements should be optimised with input from potential suppliers.

AI5.4 IT Resources Acquisition
Protect and enforce the organisation's interests in all acquisition contractual agreements, including the rights and obligations of all parties in the contractual terms for the acquisition of software, development resources, infrastructure and services.

Management Guidelines

AI5 Procure IT Resources

From	Inputs
PO1	IT acquisition strategy
PO8	Acquisition standards
PO10	Project management guidelines and detailed project plans
AI1	Business requirement feasibility study
AI2-3	Procurement decisions
DS2	Supplier catalogue

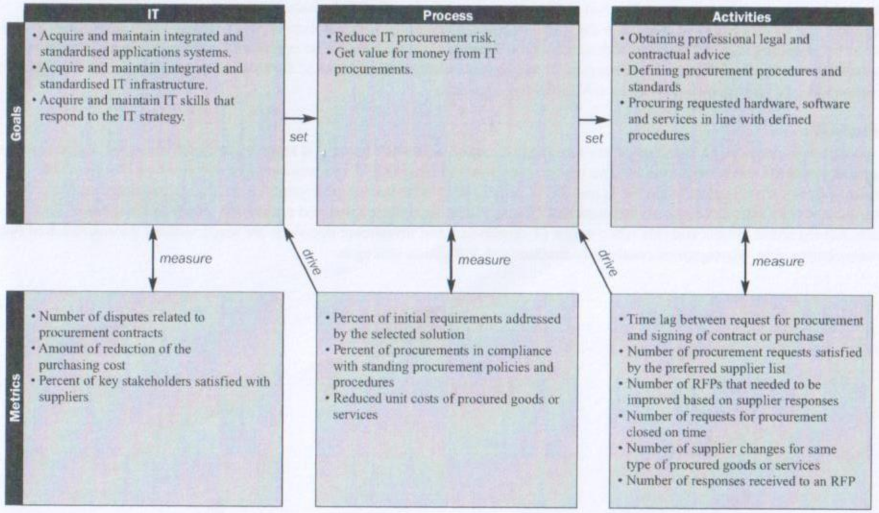
Outputs	To						
Third-party relationship management requirements	DS2						
Procured items	AI7						
Contractual arrangements	DS2						

RACI Chart

Activities	CEO	CFO	Business Executive	CIO	Business Process Owner	Head Operations	Chief Architect	Head Development	Head IT Administration	PMO	Compliance, Audit, Risk and Security
Develop IT procurement policies and procedures aligned with procurement policies at the corporate level.	I	C		A		I	I	I	R		C
Establish/maintain a list of accredited suppliers.									A/R		
Evaluate and select suppliers through a request for proposal (RFP) process.	C	C		A		R		R	R	R	C
Develop contracts that protect the organisation's interests.	R	C		A		R		R	R		C
Procure in compliance with established procedures.				A		R		R	R		C

A **RACI** chart identifies who is **R**esponsible, **A**ccountable, **C**onsulted and/or **I**nformed.

Goals and Metrics



IT (Goals)
- Acquire and maintain integrated and standardised applications systems.
- Acquire and maintain integrated and standardised IT infrastructure.
- Acquire and maintain IT skills that respond to the IT strategy.

Process (Goals)
- Reduce IT procurement risk.
- Get value for money from IT procurements.

Activities (Goals)
- Obtaining professional legal and contractual advice
- Defining procurement procedures and standards
- Procuring requested hardware, software and services in line with defined procedures

IT (Metrics)
- Number of disputes related to procurement contracts
- Amount of reduction of the purchasing cost
- Percent of key stakeholders satisfied with suppliers

Process (Metrics)
- Percent of initial requirements addressed by the selected solution
- Percent of procurements in compliance with standing procurement policies and procedures
- Reduced unit costs of procured goods or services

Activities (Metrics)
- Time lag between request for procurement and signing of contract or purchase
- Number of procurement requests satisfied by the preferred supplier list
- Number of RFPs that needed to be improved based on supplier responses
- Number of requests for procurement closed on time
- Number of supplier changes for same type of procured goods or services
- Number of responses received to an RFP

Maturity Model

AI5 Procure IT Resources

Management of the process of *Procure IT resources* that satisfies the business requirement for IT of *improving IT's cost-efficiency and its contribution to business profitability* is:

0 Non-existent when
There is no defined IT resource procurement process in place. The organisation does not recognise the need for clear procurement polices and procedures to ensure that all IT resources are available in a timely and cost-efficient manner.

1 Initial/*Ad Hoc* when
The organisation recognises the need to have documented policies and procedures that link IT acquisition to the business organisation's overall procurement process. Contracts for the acquisition of IT resources are developed and managed by project managers and other individuals exercising their professional judgement rather than as a result of formal procedures and policies. There is only an *ad hoc* relationship between corporate acquisition and contract management processes and IT. Contracts for acquisition are managed at the conclusion of projects rather than on a continuous basis.

2 Repeatable but Intuitive when
There is organisational awareness of the need to have basic policies and procedures for IT acquisition. Policies and procedures are partially integrated with the business organisation's overall procurement process. Procurement processes are mostly utilised for large and highly visible projects. Responsibilities and accountabilities for IT procurement and contract management are determined by the individual contract manager's experience. The importance of supplier management and relationship management is recognised; however, it is addressed based on individual initiative. Contract processes are mostly utilised by large or highly visible projects.

3 Defined when
Management institutes policies and procedures for IT acquisition. Policies and procedures are guided by the business organisation's overall procurement process. IT acquisition is largely integrated with overall business procurement systems. IT standards for the acquisition of IT resources exist. Suppliers of IT resources are integrated into the organisation's project management mechanisms from a contract management perspective. IT management communicates the need for appropriate acquisitions and contract management throughout the IT function.

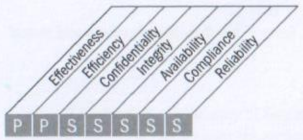
4 Managed and Measurable when
IT acquisition is fully integrated with overall business procurement systems. IT standards for the acquisition of IT resources are used for all procurements. Measurements on contract and procurement management are taken relevant to the business cases for IT acquisition. Reporting on IT acquisition activity that supports business objectives is available. Management is usually aware of exceptions to the policies and procedures for IT acquisition. Strategic management of relationships is developing. IT management enforces the use of the acquisition and contract management process for all acquisitions by reviewing performance measurement.

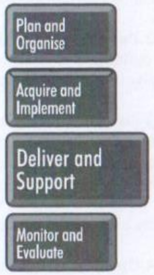
5 Optimised when
Management institutes resources' procurement thorough processes for IT acquisition. Management enforces compliance with policies and procedures for IT acquisition. Measurements on contract and procurement management are taken that are relevant to the business cases for IT acquisitions. Good relationships are established over time with most suppliers and partners, and the quality of relationships is measured and monitored. Relationships are managed strategically. IT standards, policies and procedures for the acquisition of IT resources are managed strategically and respond to measurement of the process. IT management communicates the strategic importance of appropriate acquisition and contract management throughout the IT function.

Process Description

DS1 Define and Manage Service Levels

Effective communication between IT management and business customers regarding services required is enabled by a documented definition of and agreement on IT services and service levels. This process also includes monitoring and timely reporting to stakeholders on the accomplishment of service levels. This process enables alignment between IT services and the related business requirements.





Control over the IT process of

Define and manage service levels

that satisfies the business requirement for IT of

ensuring the alignment of key IT services with the business strategy

by focusing on

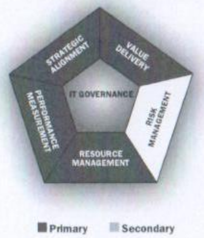
identifying service requirements, agreeing on service levels and monitoring the achievement of service levels

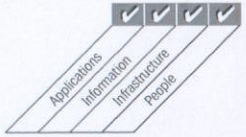
is achieved by

- Formalising internal and external agreements in line with requirements and delivery capabilities
- Reporting on service level achievements (reports and meetings)
- Identifying and communicating new and updated service requirements to strategic planning

and is measured by

- Percent of business stakeholders satisfied that service delivery meets agreed-upon levels
- Number of delivered services not in the catalogue
- Number of formal SLA review meetings with business customers per year





Control Objectives

DS1 Define and Manage Service Levels

DS1.1 Service Level Management Framework
Define a framework that provides a formalised service level management process between the customer and service provider. The framework should maintain continuous alignment with business requirements and priorities and facilitate common understanding between the customer and provider(s). The framework should include processes for creating service requirements, service definitions, SLAs, OLAs and funding sources. These attributes should be organised in a service catalogue. The framework should define the organisational structure for service level management, covering the roles, tasks and responsibilities of internal and external service providers and customers.

DS1.2 Definition of Services
Base definitions of IT services on service characteristics and business requirements. Ensure that they are organised and stored centrally via the implementation of a service catalogue portfolio approach.

DS1.3 Service Level Agreements
Define and agree to SLAs for all critical IT services based on customer requirements and IT capabilities. This should cover customer commitments; service support requirements; quantitative and qualitative metrics for measuring the service signed off on by the stakeholders; funding and commercial arrangements, if applicable; and roles and responsibilities, including oversight of the SLA. Consider items such as availability, reliability, performance, capacity for growth, levels of support, continuity planning, security and demand constraints.

DS1.4 Operating Level Agreements
Define OLAs that explain how the services will be technically delivered to support the SLA(s) in an optimal manner. The OLAs should specify the technical processes in terms meaningful to the provider and may support several SLAs.

DS1.5 Monitoring and Reporting of Service Level Achievements
Continuously monitor specified service level performance criteria. Reports on achievement of service levels should be provided in a format that is meaningful to the stakeholders. The monitoring statistics should be analysed and acted upon to identify negative and positive trends for individual services as well as for services overall.

DS1.6 Review of Service Level Agreements and Contracts
Regularly review SLAs and underpinning contracts (UCs) with internal and external service providers to ensure that they are effective and up to date and that changes in requirements have been taken into account.

Management Guidelines

DS1 Define and Manage Service Levels

From	Inputs
PO1	Strategic and tactical IT plans, IT service portfolio
PO2	Assigned data classifications
PO5	Updated IT service portfolio
AI2	Initial planned SLAs
AI3	Initial planned OLAs
DS4	Disaster service requirements, including roles and responsibilities
ME1	Performance input to IT planning

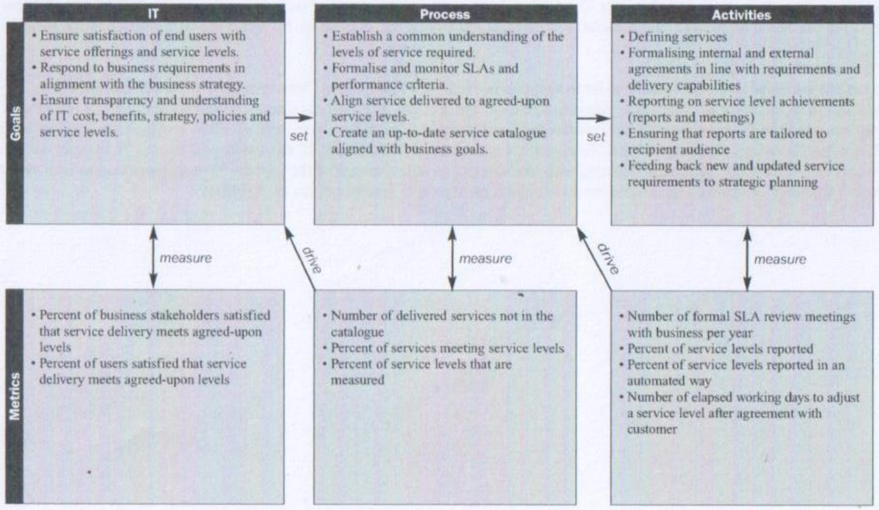
Outputs	To						
Contract review report	DS2						
Process performance reports	ME1						
New/updated service requirements	PO1						
SLAs	AI1	DS2	DS3	DS4	DS6	DS8	DS13
OLAs	DS4	DS5	DS6	DS7	DS8	DS11	DS13
Updated IT service portfolio	PO1						

RACI Chart

Activities \ Functions	CEO	CFO	Business Executive	CIO	Business Process Owner	Head Operations	Chief Architect	Head Development	Head IT Administration	PMO	Compliance, Audit, Risk and Security	Service Manager
Create a framework for defining IT services.			C	A	C	C	I	C	C	I	C	R
Build an IT service catalogue.			I	A	C	C	I	C	C	I	I	R
Define SLAs for critical IT services.		I	I	C	C	R	I	R	R	C	C	A/R
Define OLAs for meeting SLAs.				I	C	R	I	R	R	C	C	A/R
Monitor and report end-to-end service level performance.				I	I	R		I	I		I	A/R
Review SLAs and UCs.		I		I	C	R		R	R		C	A/R
Review and update IT service catalogue.			I	A	C	C	I	C	C	I	I	R
Create service improvement plan.			I	A	I	R	I	R	C	C	I	R

A **RACI** chart identifies who is **R**esponsible, **A**ccountable, **C**onsulted and/or **I**nformed.

Goals and Metrics



IT – Goals:
- Ensure satisfaction of end users with service offerings and service levels.
- Respond to business requirements in alignment with the business strategy.
- Ensure transparency and understanding of IT cost, benefits, strategy, policies and service levels.

Process – Goals:
- Establish a common understanding of the levels of service required.
- Formalise and monitor SLAs and performance criteria.
- Align service delivered to agreed-upon service levels.
- Create an up-to-date service catalogue aligned with business goals.

Activities – Goals:
- Defining services
- Formalising internal and external agreements in line with requirements and delivery capabilities
- Reporting on service level achievements (reports and meetings)
- Ensuring that reports are tailored to recipient audience
- Feeding back new and updated service requirements to strategic planning

IT – Metrics:
- Percent of business stakeholders satisfied that service delivery meets agreed-upon levels
- Percent of users satisfied that service delivery meets agreed-upon levels

Process – Metrics:
- Number of delivered services not in the catalogue
- Percent of services meeting service levels
- Percent of service levels that are measured

Activities – Metrics:
- Number of formal SLA review meetings with business per year
- Percent of service levels reported
- Percent of service levels reported in an automated way
- Number of elapsed working days to adjust a service level after agreement with customer

Maturity Model

DS1 Define and Manage Service Levels

Management of the process of *Define and manage service levels* that satisfies the business requirement for IT of *ensuring the alignment of key IT services with the business strategy* is:

0 Non-existent when
Management has not recognised the need for a process for defining service levels. Accountabilities and responsibilities for monitoring them are not assigned.

1 Initial/*Ad Hoc* when
There is awareness of the need to manage service levels, but the process is informal and reactive. The responsibility and accountability for defining and managing services are not defined. If performance measurements exist, they are qualitative only with imprecisely defined goals. Reporting is informal, infrequent and inconsistent.

2 Repeatable but Intuitive when
There are agreed-upon service levels, but they are informal and not reviewed. Service level reporting is incomplete and may be irrelevant or misleading for customers. Service level reporting is dependent on the skills and initiative of individual managers. A service level co-ordinator is appointed with defined responsibilities, but limited authority. If a process for compliance to SLAs exists, it is voluntary and not enforced.

3 Defined when
Responsibilities are well defined, but with discretionary authority. The SLA development process is in place with checkpoints for reassessing service levels and customer satisfaction. Services and service levels are defined, documented and agreed-upon using a standard process. Service level shortfalls are identified, but procedures on how to resolve shortfalls are informal. There is a clear linkage between expected service level achievement and the funding provided. Service levels are agreed to, but they may not address business needs.

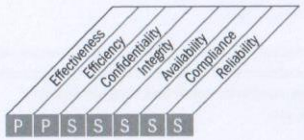
4 Managed and Measurable when
Service levels are increasingly defined in the system requirements definition phase and incorporated into the design of the application and operational environments. Customer satisfaction is routinely measured and assessed. Performance measures reflect customer needs, rather than IT goals. The measures for assessing service levels are becoming standardised and reflect industry norms. The criteria for defining service levels are based on business criticality and include availability, reliability, performance, growth capacity, user support, continuity planning and security considerations. Root cause analysis is routinely performed when service levels are not met. The reporting process for monitoring service levels is becoming increasingly automated. Operational and financial risks associated with not meeting agreed-upon service levels are defined and clearly understood. A formal system of measurement is instituted and maintained.

5 Optimised when
Service levels are continuously re-evaluated to ensure alignment of IT and business objectives, whilst taking advantage of technology, including the cost-benefit ratio. All service level management processes are subject to continuous improvement. Customer satisfaction levels are continuously monitored and managed. Expected service levels reflect strategic goals of business units and are evaluated against industry norms. IT management has the resources and accountability needed to meet service level targets, and compensation is structured to provide incentives for meeting these targets. Senior management monitors performance metrics as part of a continuous improvement process.

Process Description

DS2 Manage Third-party Services

The need to assure that services provided by third parties (suppliers, vendors and partners) meet business requirements requires an effective third-party management process. This process is accomplished by clearly defining the roles, responsibilities and expectations in third-party agreements as well as reviewing and monitoring such agreements for effectiveness and compliance. Effective management of third-party services minimises the business risk associated with non-performing suppliers.



Plan and Organise
Acquire and Implement
Deliver and Support
Monitor and Evaluate

Control over the IT process of

Manage third-party services

that satisfies the business requirement for IT of

providing satisfactory third-party services whilst being transparent about benefits, costs and risks

by focusing on

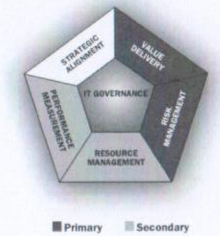
establishing relationships and bilateral responsibilities with qualified third-party service providers and monitoring the service delivery to verify and ensure adherence to agreements

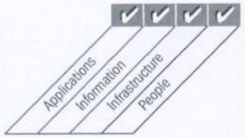
is achieved by

- Identifying and categorising supplier services
- Identifying and mitigating supplier risk
- Monitoring and measuring supplier performance

and is measured by

- Number of user complaints due to contracted services
- Percent of major suppliers meeting clearly defined requirements and service levels
- Percent of major suppliers subject to monitoring





Control Objectives

DS2 Manage Third-party Services

DS2.1 Identification of All Supplier Relationships
Identify all supplier services, and categorise them according to supplier type, significance and criticality. Maintain formal documentation of technical and organisational relationships covering the roles and responsibilities, goals, expected deliverables, and credentials of representatives of these suppliers.

DS2.2 Supplier Relationship Management
Formalise the supplier relationship management process for each supplier. The relationship owners should liaise on customer and supplier issues and ensure the quality of the relationship based on trust and transparency (e.g., through SLAs).

DS2.3 Supplier Risk Management
Identify and mitigate risks relating to suppliers' ability to continue effective service delivery in a secure and efficient manner on a continual basis. Ensure that contracts conform to universal business standards in accordance with legal and regulatory requirements. Risk management should further consider non-disclosure agreements (NDAs), escrow contracts, continued supplier viability, conformance with security requirements, alternative suppliers, penalties and rewards, etc.

DS2.4 Supplier Performance Monitoring
Establish a process to monitor service delivery to ensure that the supplier is meeting current business requirements and continuing to adhere to the contract agreements and SLAs, and that performance is competitive with alternative suppliers and market conditions.

Management Guidelines

DS2 Manage Third-party Services

From	Inputs
PO1	IT sourcing strategy
PO8	Acquisition standards
AI5	Contractual arrangements, third-party relationship management requirements
DS1	SLAs, contract review report
DS4	Disaster service requirements, including roles and responsibilities

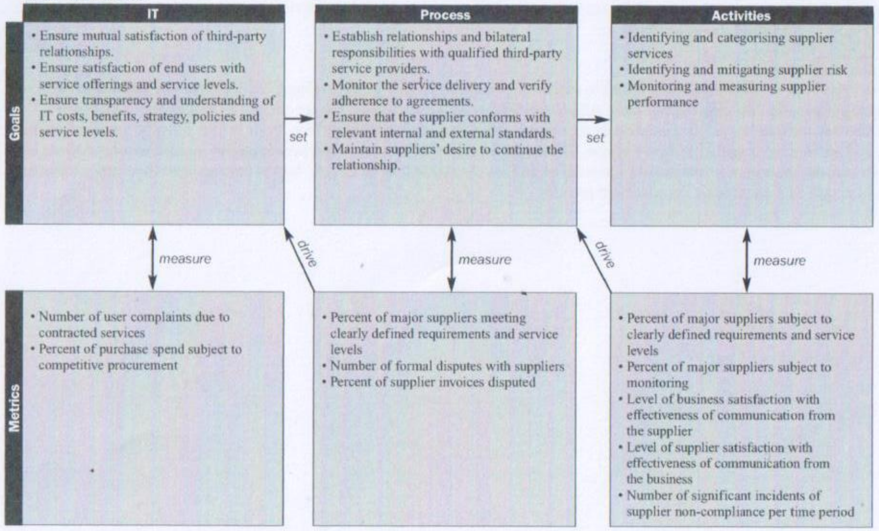
Outputs	To						
Process performance reports	ME1						
Supplier catalogue	AI5						
Supplier risks	PO9						

RACI Chart

Activities \ Functions	CEO	CFO	Business Executive	CIO	Business Process Owner	Head Operations	Chief Architect	Head Development	Head IT Administration	PMO	Compliance, Audit, Risk and Security
Identify and categorise third-party service relationships.				I	C	R	C	R	A/R	C	C
Define and document supplier management processes.		C		A	I	R	I	R	R	C	C
Establish supplier evaluation and selection policies and procedures.		C		A	C	C		C	R	C	C
Identify, assess and mitigate supplier risks.		I		A		R		R	R	C	C
Monitor supplier service delivery.				R	A	R		R	R	C	C
Evaluate long-term goals of the service relationship for all stakeholders.	C	C	C	A/R	C	C	C	C	R	C	C

A **RACI** chart identifies who is **R**esponsible, **A**ccountable, **C**onsulted and/or **I**nformed.

Goals and Metrics



- Ensure mutual satisfaction of third-party relationships.
- Ensure satisfaction of end users with service offerings and service levels.
- Ensure transparency and understanding of IT costs, benefits, strategy, policies and service levels.

- Establish relationships and bilateral responsibilities with qualified third-party service providers.
- Monitor the service delivery and verify adherence to agreements.
- Ensure that the supplier conforms with relevant internal and external standards.
- Maintain suppliers' desire to continue the relationship.

- Identifying and categorising supplier services
- Identifying and mitigating supplier risk
- Monitoring and measuring supplier performance

- Number of user complaints due to contracted services
- Percent of purchase spend subject to competitive procurement

- Percent of major suppliers meeting clearly defined requirements and service levels
- Number of formal disputes with suppliers
- Percent of supplier invoices disputed

- Percent of major suppliers subject to clearly defined requirements and service levels
- Percent of major suppliers subject to monitoring
- Level of business satisfaction with effectiveness of communication from the supplier
- Level of supplier satisfaction with effectiveness of communication from the business
- Number of significant incidents of supplier non-compliance per time period

Maturity Model

DS2 Manage Third-party Services

Management of the process of *Manage third-party services* that satisfies the business requirement for IT of *providing satisfactory third-party services whilst being transparent about benefits, costs and risks* is:

0 Non-existent when
Responsibilities and accountabilities are not defined. There are no formal policies and procedures regarding contracting with third parties. Third-party services are neither approved nor reviewed by management. There are no measurement activities and no reporting by third parties. In the absence of a contractual obligation for reporting, senior management is not aware of the quality of the service delivered.

1 Initial/*Ad Hoc* when
Management is aware of the need to have documented policies and procedures for third-party management, including signed contracts. There are no standard terms of agreement with service providers. Measurement of the services provided is informal and reactive. Practices are dependent on the experience (e.g., on demand) of the individual and the supplier.

2 Repeatable but Intuitive when
The process for overseeing third-party service providers, associated risks and the delivery of services is informal. A signed, *pro forma* contract is used with standard vendor terms and conditions (e.g., the description of services to be provided). Reports on the services provided are available, but do not support business objectives.

3 Defined when
Well-documented procedures are in place to govern third-party services, with clear processes for vetting and negotiating with vendors. When an agreement for the provision of services is made, the relationship with the third party is purely a contractual one. The nature of the services to be provided is detailed in the contract and includes legal, operational and control requirements. The responsibility for oversight of third-party services is assigned. Contractual terms are based on standardised templates. The business risk associated with the third-party services is assessed and reported.

4 Managed and Measurable when
Formal and standardised criteria are established for defining the terms of engagement, including scope of work, services/deliverables to be provided, assumptions, schedule, costs, billing arrangements and responsibilities. Responsibilities for contract and vendor management are assigned. Vendor qualifications, risks and capabilities are verified on a continual basis. Service requirements are defined and linked to business objectives. A process exists to review service performance against contractual terms, providing input to assess current and future third-party services. Transfer pricing models are used in the procurement process. All parties involved are aware of service, cost and milestone expectations. Agreed-upon goals and metrics for the oversight of service providers exist.

5 Optimised when
Contracts signed with third parties are reviewed periodically at predefined intervals. The responsibility for managing suppliers and the quality of the services provided is assigned. Evidence of contract compliance to operational, legal and control provisions is monitored, and corrective action is enforced. The third party is subject to independent periodic review, and feedback on performance is provided and used to improve service delivery. Measurements vary in response to changing business conditions. Measures support early detection of potential problems with third-party services. Comprehensive, defined reporting of service level achievement is linked to the third-party compensation. Management adjusts the process of third-party service acquisition and monitoring based on the measurers.