

แนวทางการประยุกต์ใช้ ICT กับการบริหารราชการแนวใหม่และปัจจัยสู่ความสำเร็จ

กำพล ศรณะรัตน์

- ผู้อำนวยการฝ่าย ICT สำนักงานคณะกรรมการ ก.ล.ต.
- กรรมการผู้ทรงคุณวุฒิ ในคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์
- กรรมการธนาคารอาคารสงเคราะห์
- อาจารย์พิเศษ วิทยาลัยนวัตกรรม มหาวิทยาลัยธรรมศาสตร์
- นายกสมาคม CIO16 / TITAA
- กรรมการ/ที่ปรึกษา สมาคมต่างๆ อาทิ TISA, IAC, Thailand PKI Forum, CSA
- อนุกรรมการภายใต้ TMA, ETC
- ที่ปรึกษาด้าน IT หน่วยงานต่างๆ

Agenda

PPT

PPT

PPT

บทบาทของ CIO

เครื่องมือช่วย ให้คิดดี
ทำดี และหวังผลที่ดี

ปัจจัยสู่ความสำเร็จ

PPT

PPT

PPT

PPT

PPT



บทบาทของ CIO

CIO นั้นสำคัญไฉน

CIO: Does IT Matter?

วิสัยทัศน์กับการผลักดันงานเพื่อสนองธุรกิจ

การสร้างเครือข่ายและพันธมิตรธุรกิจ

การประสานความช่วยเหลือจากผู้มีความรู้ความสามารถ

การสร้างความตระหนักให้เห็นความสำคัญของงาน

กำหนดความสามารถของทีมงานให้เหมาะสม

การวิเคราะห์สภาพแวดล้อมหรือสภาพปัญหาให้ถ่องแท้

การสร้างเงื่อนไขที่จะก่อให้เกิดความโชคดี

การวางแผนงานและอ่านงานให้ออก เพื่อกำหนดทรัพยากรที่เหมาะสม

การเตรียมแผนสำรองฉุกเฉิน

การสร้างทีมเวิร์ค

CIO กับบทบาทการนำการเปลี่ยนแปลง



President's Management Agenda – George W. Bush 2002

วาระการบริหารงานของประธานาธิบดี (President's Management Agenda)
กล่าวถึงหัวข้อสำคัญ 5 เรื่องด้วยกัน ประกอบด้วย

กลยุทธ์ในการบริหารทรัพยากร
บุคคล (Strategic
Management of
Human Capital)

การสร้างความสามารถในการ
แข่งขัน (Competitive
Sourcing)

การเพิ่มความสามารถในการ
ประกอบการ (Improved
Financial
Performance)

การขยายการบริการรัฐบาล
อิเล็กทรอนิกส์ (Expanded
Electronic
Government)

การกำหนดงบประมาณตาม
สมรรถนะในการดำเนินงาน
(Budget and
Performance
Integration)



EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET

THE PRESIDENT'S
MANAGEMENT AGENDA

EXECUTION: The Discipline of Getting Things Done

พฤติกรรมที่สำคัญ 7 ประการของผู้นำ

เข้าใจพนักงานและธุรกิจขององค์กร (**Know your people and your business**)

ยึดมั่นกับความเป็นจริง (**Insist on realism**)

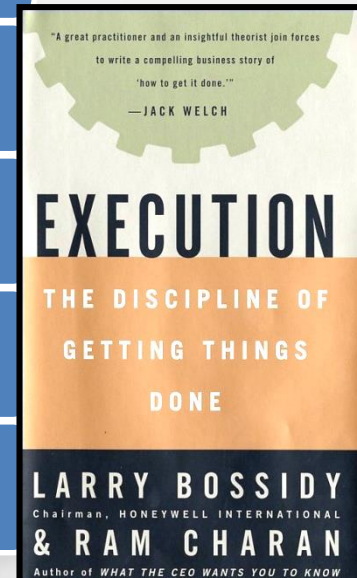
กำหนดเป้าหมายที่ชัดเจนและจัดลำดับความสำคัญ (**Set clear goals and priorities**)

มีการติดตามผล (**Follow through**)

ให้รางวัลผู้ปฏิบัติงาน (**Reward the doers**)

พัฒนาบุคลากร (**Expand people's capabilities**) ให้มีความสามารถเพิ่มขึ้น

เข้าใจตนเอง หนักแน่น ไม่ใช่อารมณ์ (**Know yourself... (it takes emotional fortitude)**)



New Trends of Core Competence for CIOs in the Private Sector in US and Japan - Based on the Surveys on CIO - Core Competences for ICT Value-added
by Toshio OBI, Professor, Waseda University, Japan

ความสามารถหลักของผู้ที่มาทำหน้าที่ **CIO** ของหน่วยงาน จะต้องสามารถดำรงบทบาททั้ง 3 ด้านพร้อมกัน ประกอบด้วย

1) ความสามารถในการจัดการ (**Management**) ต้องสามารถนำพาธุรกิจไปสู่การดำเนินธุรกิจในรูปแบบใหม่เพื่อการแข่งขันและอยู่รอดได้

2) ความสามารถในการบริหารจัดการความเสี่ยง และบริหาร ความมั่นคงปลอดภัย (**Risk/Security Management**) ต้องสามารถกำหนดกลยุทธ์เพื่อช่วยในการควบคุมความเสี่ยงภัยอันเนื่องมาจากภัยคุกคามต่างๆ ทั้งภัยธรรมชาติและการก่อการร้าย

3) ความสามารถในการบริหารจัดการความรู้ (**Knowledge Management**) ต้องสามารถบริหารความรู้ในองค์กรที่เป็นทรัพย์สินทางปัญญา และการปฏิบัติตามกฎหมาย **Sarbanes Oxley**

New Trends of Core Competence for CIOs in the Private Sector in US and Japan - Based on the Surveys on CIO - Core Competences for ICT Value-added
by Toshio OBI, Professor, Waseda University, Japan – Continued

บทบาทของ CIO ที่เปลี่ยนไปใช้ทักษะในเชิงการจัดการสูงขึ้นเรื่อยๆ CIO
จำเป็นต้องมีบทบาทต่อกลยุทธ์ขององค์กรมากขึ้น อันมีสาเหตุมาจาก

- 1) การเปลี่ยนแปลงทางเทคโนโลยีมีผลต่อวิถีชีวิตการทำงานปัจจุบันมากขึ้น (change of the era and society associated with the evolution of IT)
- 2) ข้อกำหนดของกฎหมาย Sarbanes Oxley ซึ่งเป็นกฎหมายที่เข้มงวดกับความรับผิดชอบของผู้บริหารและผู้สอบบัญชี (the new range by implementation of SOX Act)
- 3) อิทธิพลของภัยธรรมชาติและภัยก่อการร้ายที่รุนแรงมากขึ้นเรื่อยๆ (influence of the situation anxiety such as natural disaster and terrorism)

New Trends of Core Competence for CIOs in the Private Sector in US and Japan - Based on the Surveys on CIO - Core Competences for ICT Value-added
by Toshio OBI, Professor, Waseda University, Japan – Continued

ความสามารถหลัก 13 รายการประกอบด้วย



New role of CIO in US and Japan

เคลื่อนตัวสู่งานเชิงจัดการธุรกิจ (shifting to business management)

ตำแหน่งงานถัดไปของ CIO คือ CEO (the next position to CEO)

ความมีภาวะผู้นำและความสามารถในการสื่อสารเป็นสิ่งที่ CIO พึ่งมี (Leadership and communicative competence have come to be requested to CIO)

การบริหารจัดการกระบวนการทำงาน (Process management)

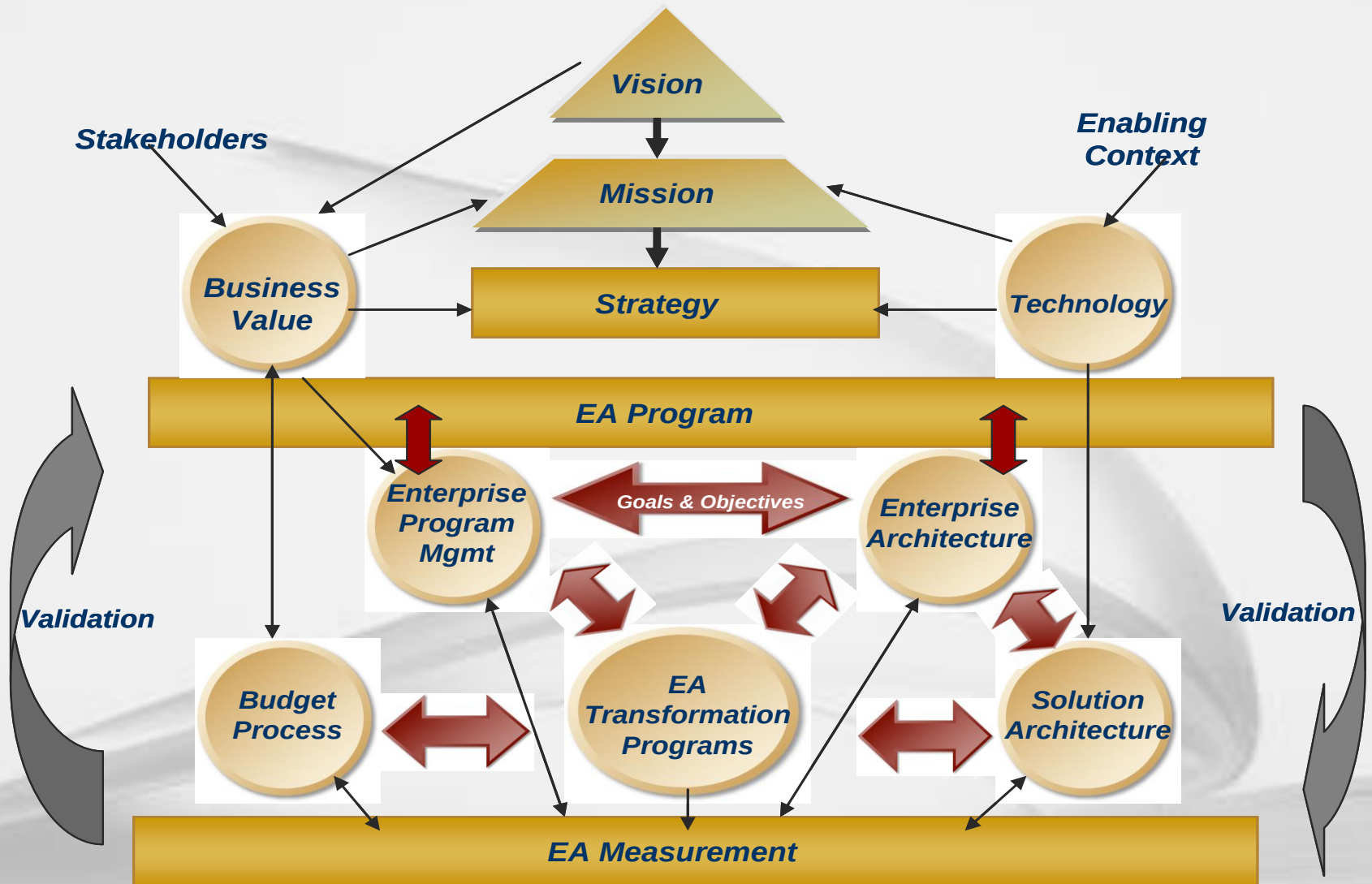
โครงสร้างทางสถาปัตยกรรมด้านไอทีขององค์กร (Enterprise Architecture)

การบริหารจัดการด้านความมั่นคงปลอดภัยและการบริหารความเสี่ยง (Security Risk Management)

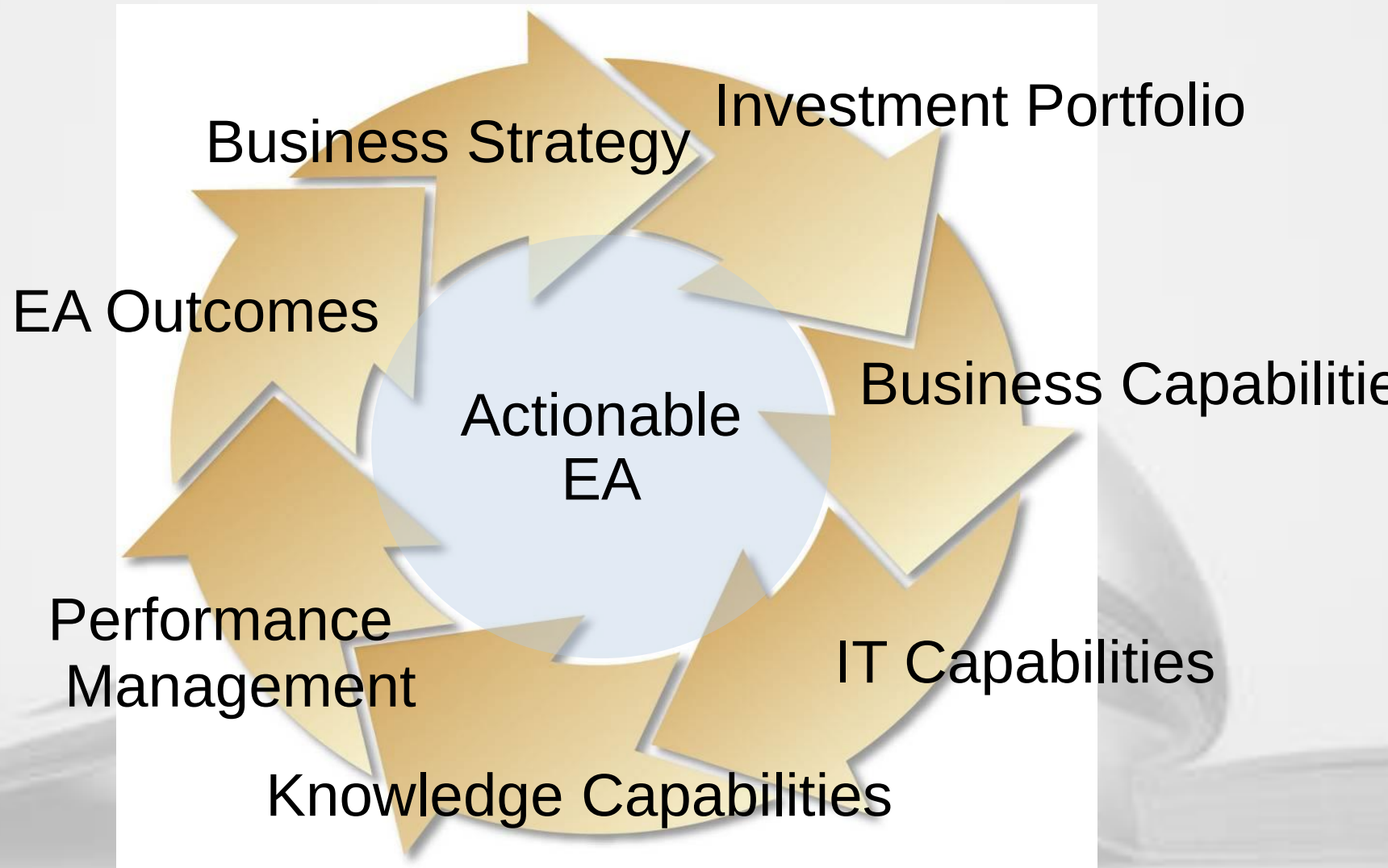
การบริหารความรู้ในองค์กร (Knowledge Management)

ให้ความสำคัญกับการป้องกันความเสียหายอันเกิดจากภัยธรรมชาติและภัยก่อการร้ายต่างๆ (Focus on the originality of “CIO for disaster prevention”)

What is EA (Enterprise Architecture)?



Actionable EA





ตัวช่วยให้คิดดี ทำดี หวังผลที่ดี

What is IT can do for
you?

คิดถึงประโยชน์ที่คาดว่าจะได้รับ

ประโยชน์ที่คาดว่าจะได้รับ

Displace labor

Enhance analyses

Reduce cycle times

Improve tracking

Improve communications

Integrate work

Transfer knowledge

Remove middle parties

Achieve GRC

ตัวอย่างการกำหนดตัวชี้วัด

(Measurement & Optimization of ICT Contribution & Benefit)

- Cost saving Initiative with following drivers:
 - streamline process
 - Retain customer
 - Reduce non value job
 - Use electronic instead of paper
 - Secure environment

ตัวอย่างการกำหนดตัวชี้วัด

Measurement & Optimization of ICT Contribution & Benefit

- Optimize business operation Initiative with
following drivers:

- Improve collaboration
- Enhance communication
- Improve productivity
- Improve decision making
- Secure access

ตัวอย่างการกำหนดตัวชี้วัด

Measurement & Optimization of ICT Contribution & Benefit

- Employee productivity Initiative with following drivers:

- Standardize process
- Improve efficiency and accuracy
- Talent management
- Create sharing culture

Measurement & Optimization of ICT Contribution & Benefit

- Grow revenue Initiative with following drivers:

- New differentiate products and services
- Pricing competitiveness
- Attract and retain new customer
- Generate revenue from assets

Measurement & Optimization of ICT Contribution & Benefit

- Improve customer service Initiative with following drivers:
 - Profit center rather than cost center
 - Improve productivity and effectiveness
 - Improve multi-channel customer experience

What is the Strategic Impact of IT?

คิดถึงงานไอทีที่ต้องคิดเชิงกลยุทธ์

เรื่องที่ต้องเผชิญ

- Time compression
- Customer expectations
- Organizational cycle time
- Global competitors
- Shorter product cycles
- Consolidation
- Governance, Risk Management and Compliance

เมื่อยุคสมัยเปลี่ยน

Industrial Model

- make and sell
- mass production
- channel focused
- processes are internally focused
- financial measures

Information Model

- sense and respond
- mass customization
- customer focused
- processes are externally focused
- customer measures

เมื่อยุคสมัยเปลี่ยน

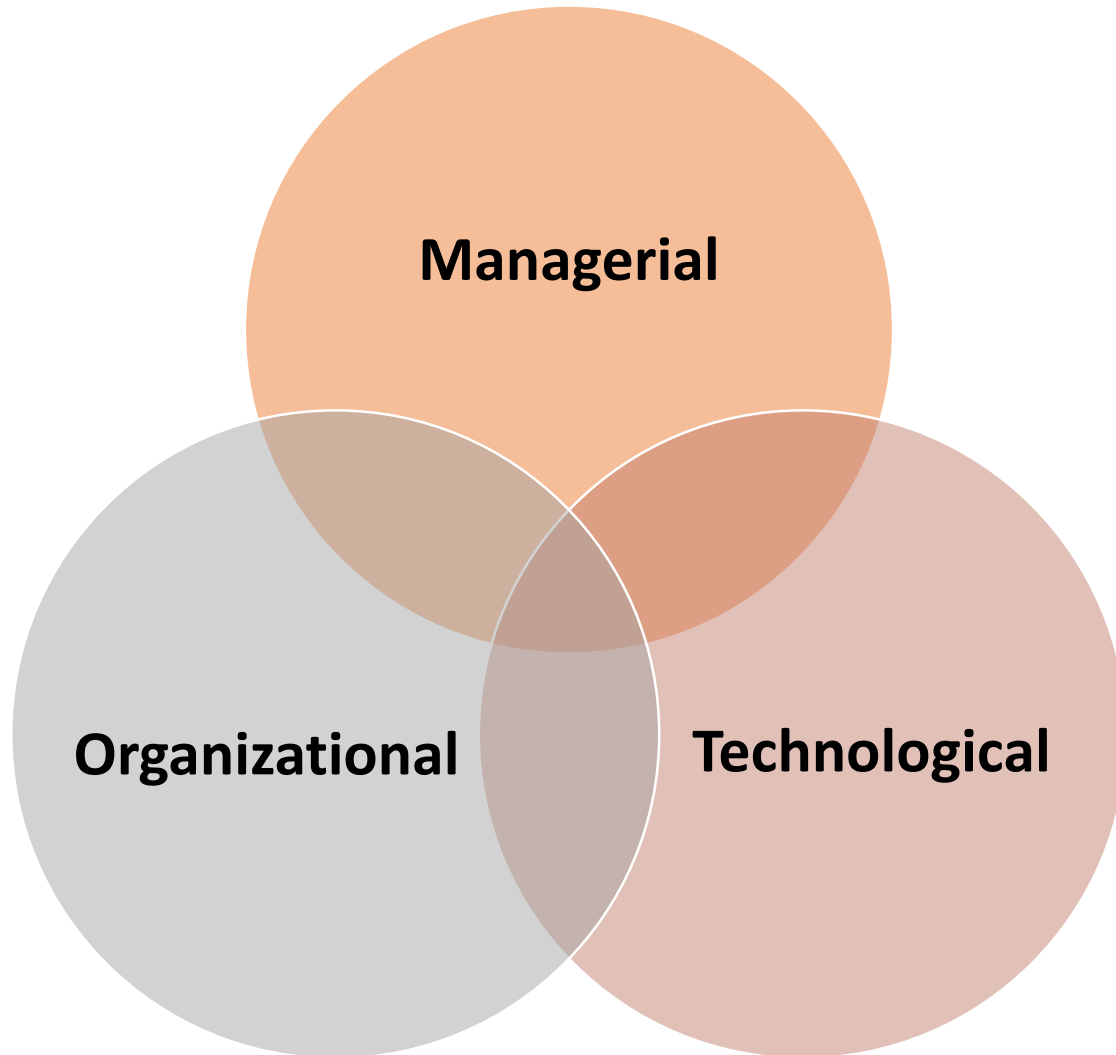
Industrial Model

- **make and sell**
- **mass production**
- **channel focused**
- **processes are internally focused**
- **financial measures**

Information Model

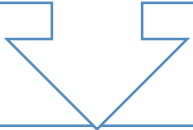
- **sense and respond**
- **mass customization**
- **Customer focused**
- **processes are externally focused**
- **customer measures**

องค์ประกอบที่ทำให้เกิดการเปลี่ยนแปลง

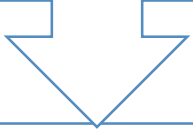


เมื่อจะต้องเปลี่ยน - > Creative Destruction

The innovation process is sometimes called the process of creative destruction.



If I get into a market first with a new product, you must do better than me to take away my profits.



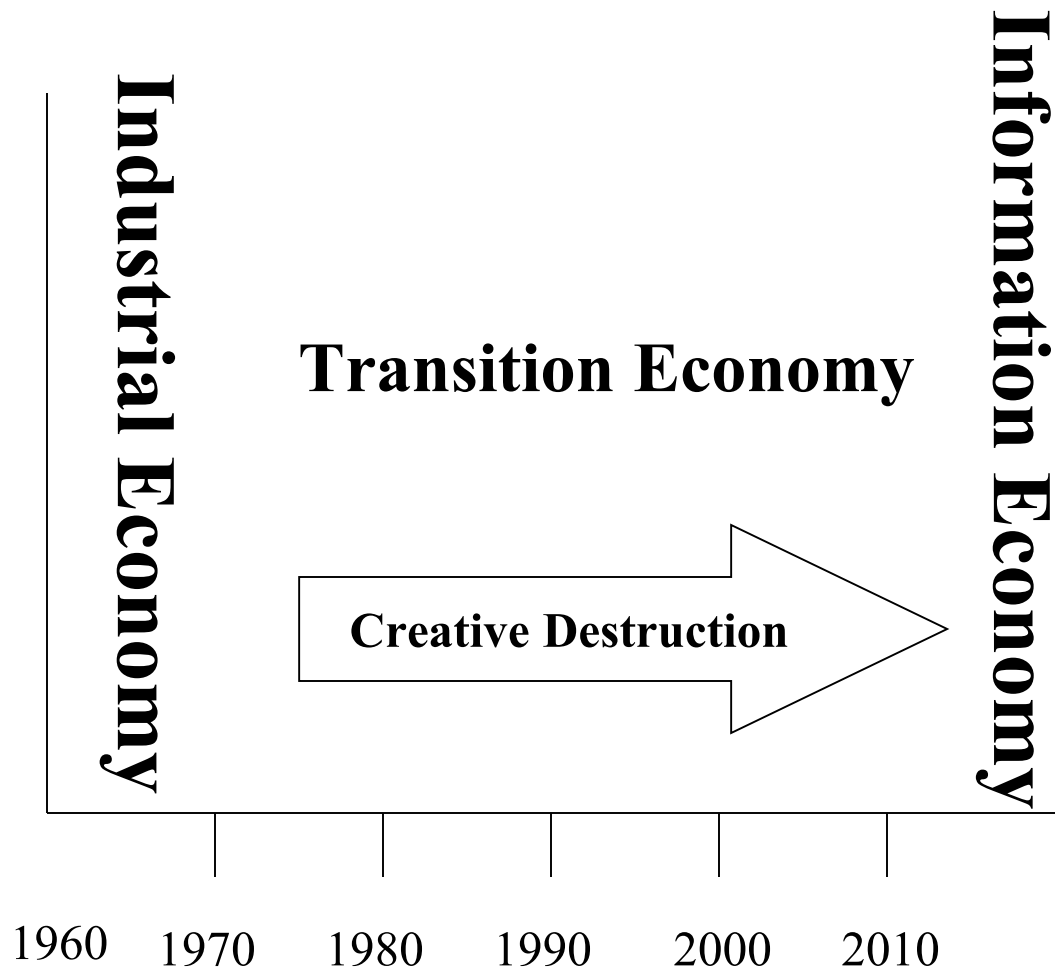
You create, and in so doing, you destroy my profits.

ต้องเปลี่ยนจึงจะก้าวข้ามยุคสมัยได้

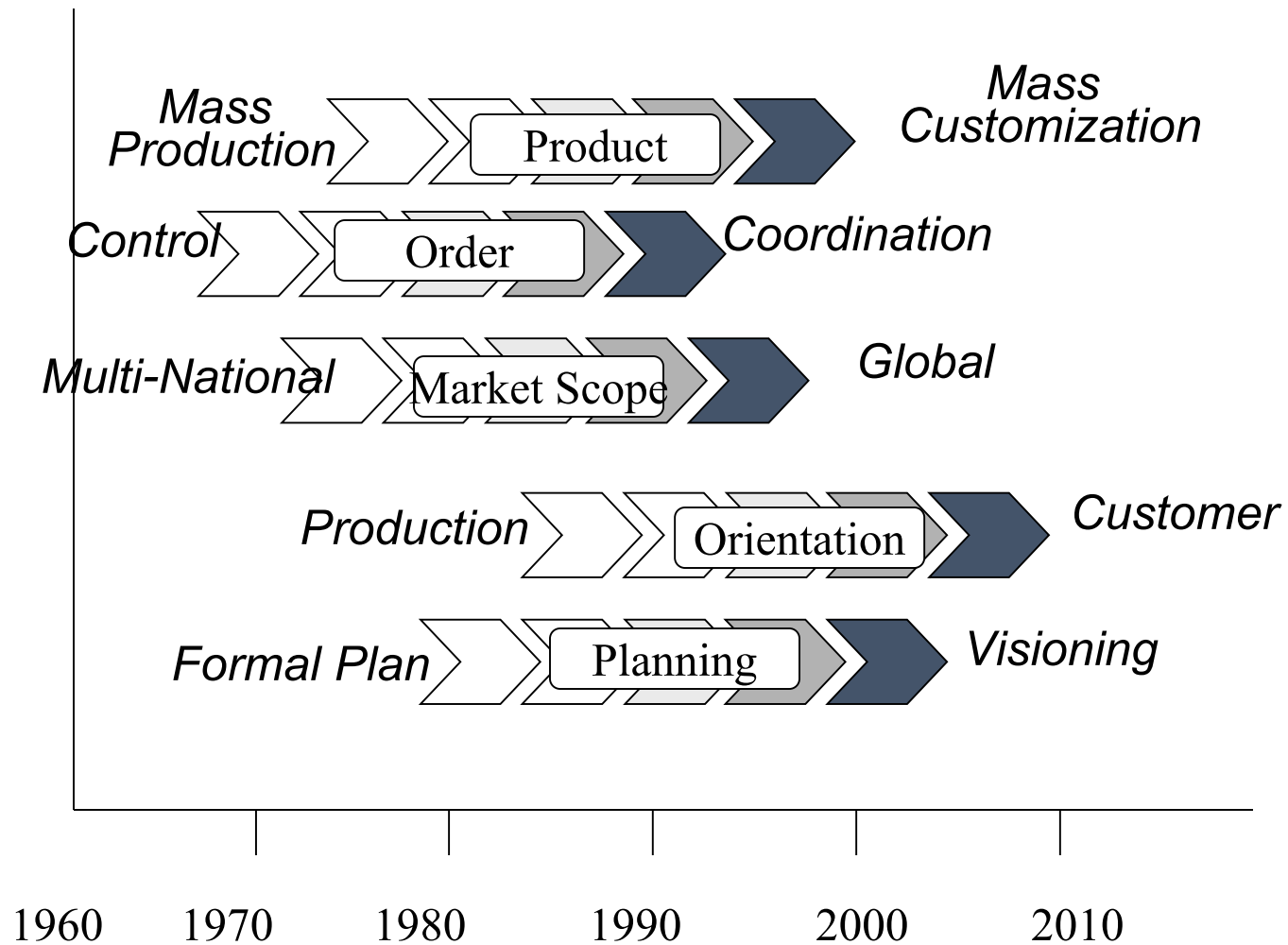
ระบบราชการ

ระบบราชการ

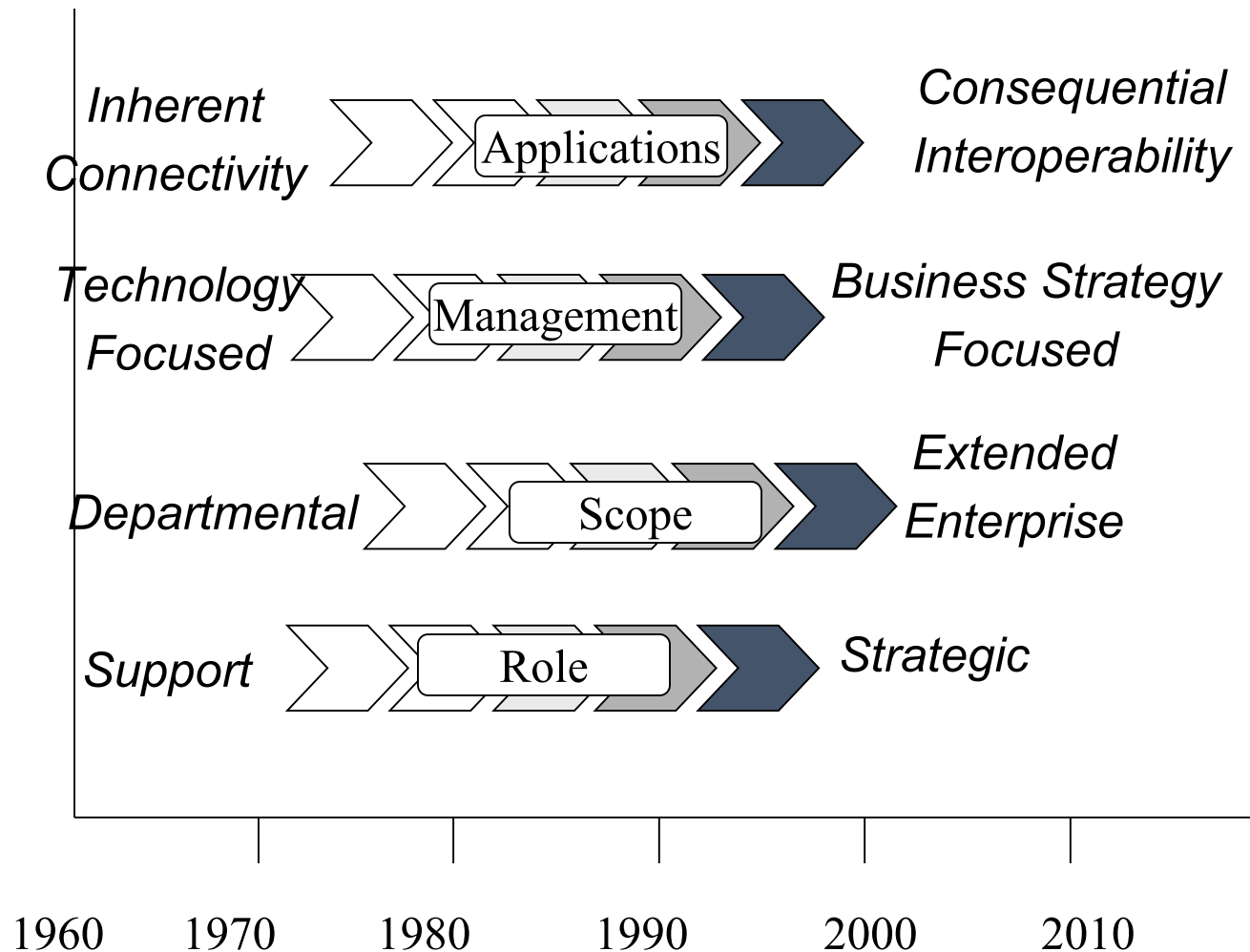
ระบบราชการ



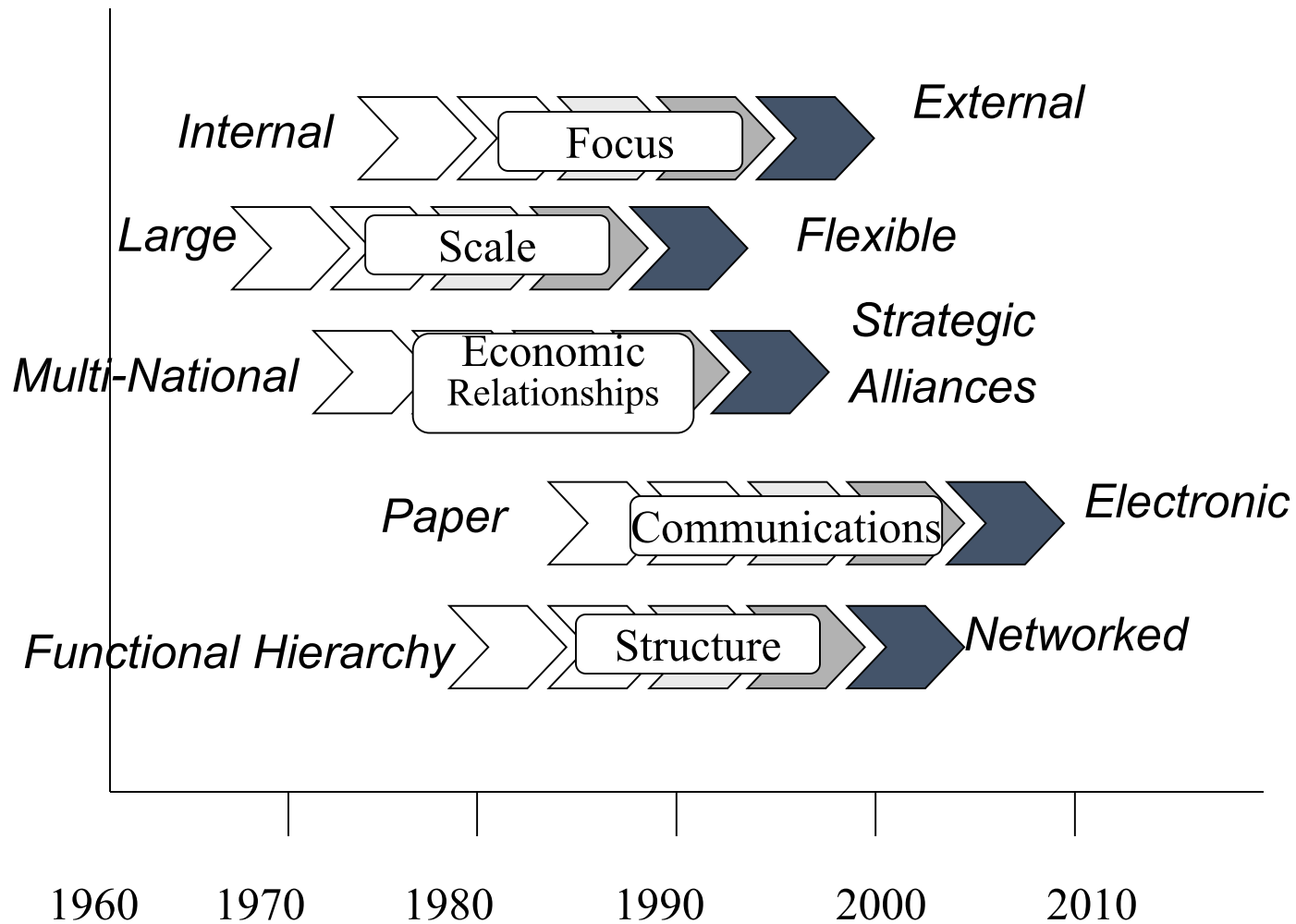
Managerial Change



Technological Change



Organizational Change



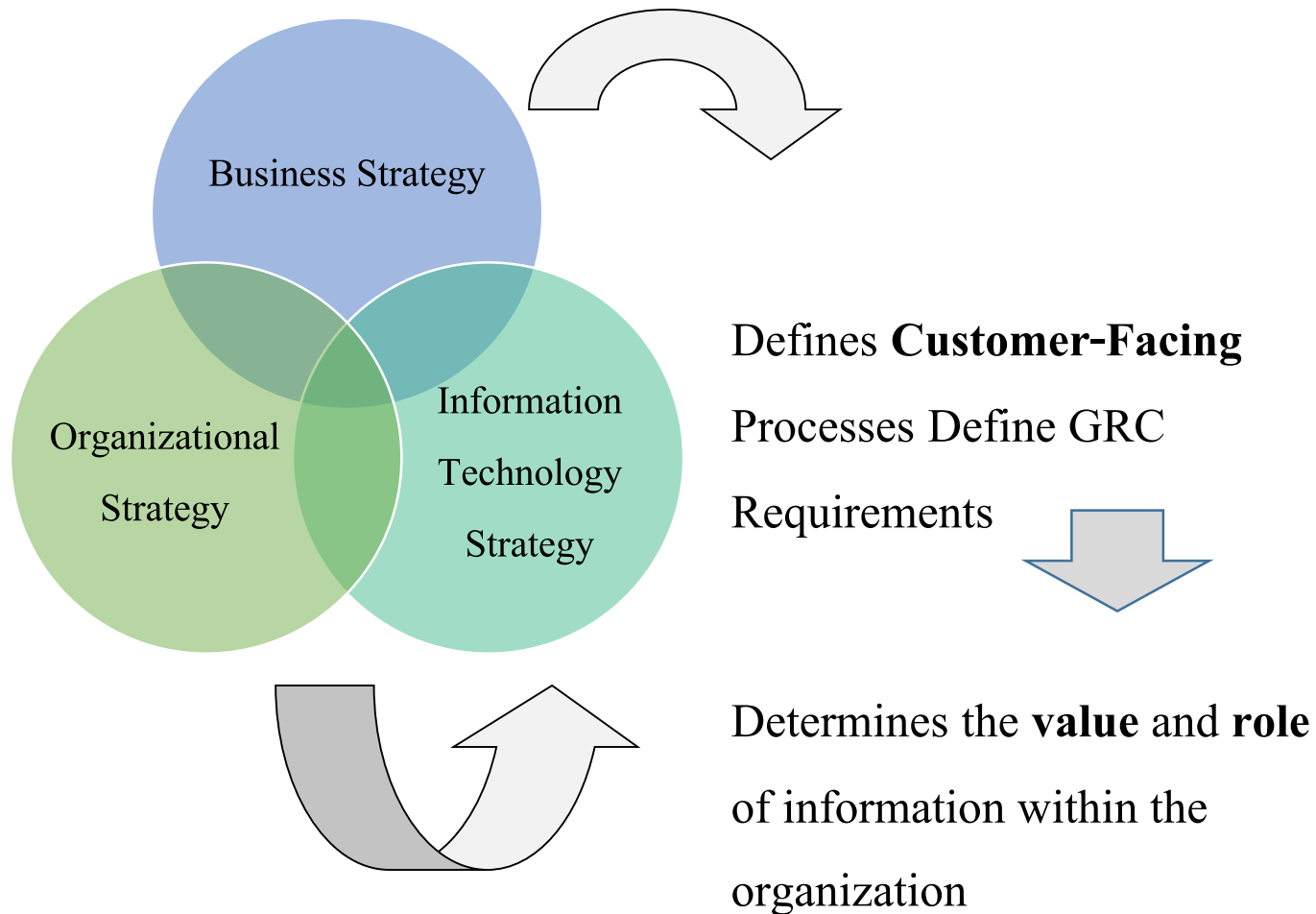
คิดและทำแบบผู้บริหารยุคใหม่

- How do we leverage our position in this changing environment?
- What moves do we anticipate our competition making?
- What adjustments should we make to our strategies?
- What is the impact on our value proposition?
- How will this affect my operating model?

กลยุทธ์ทั้ง 3 ด้าน



การเชื่อมโยงกลยุทธ์สู่การกำหนดตัวชี้วัด



Value of Information คือตัวขับเคลื่อน

Physical Supply Chain for the Marketplace

- Inbound logistics, production processes, outbound logistics, marketing, sale and distribution, service

Virtual Supply Chain for the Marketspace

- Gather, organize, select, synthesize, distribute

คิดดี ทำดี หวังผลที่ดี ดีกว่า ดีที่สุด

**Successfully designed and implemented
business**



**Systems enabled by information technology
can deliver these results:**

**Optimize value
chain
relationships**

**Differentiate or
create new
products/services**

**Improve cost
position**

High

Medium

Low

กรอบแนวคิดในภาพรวม - GRC

Governance

Risk Management

Compliance

ตัวช่วยแรก



What is GRC?

source: wikipedia

- **Governance** is the responsibility of **senior executive** management and focuses on creating organizational **transparency** by defining the mechanisms an organization uses to ensure that its constituents **follow established processes and policies**. A proper governance strategy implements systems to **monitor** and record current business activity, takes steps to ensure compliance with agreed policies, and provides for **corrective action** in cases where the rules have been ignored or misconstrued.
- **Risk Management** is the process by which an organization sets the risk tolerance, **identifies potential risks and prioritizes** the tolerance for risk based on the organization's business objectives. Risk Management **leverages internal controls** to manage and **mitigate risk** throughout the organization.
- **Compliance** is the process that records and monitors the controls, be they physical, logical or organizational, needed to **enable compliance with legislative or industry mandates as well as internal policies**

What is Governance and management ?

- **Governance**
Responsible for Board of Directors and can be delegated.
 - **Governance ensures that stakeholder needs, conditions and options are evaluated to determine balanced, agreed-on enterprise objectives to be achieved; setting direction through prioritisation and decision making; and monitoring performance and compliance against agreed-on direction and objectives.**
- **Management**
Responsible for CEO and can be delegated.
 - **Management plans, builds, runs and monitors activities in alignment with the direction set by the governance body to achieve the enterprise objectives.**

Source:

COBIT



GRC Mindset

- แนวคิด “GRC”
 - ทำให้องค์กรแสดงถึงความเป็น “Good Governance”
 - สร้างความน่าเชื่อถือให้กับองค์กร สินค้า และบริการ
 - ทำให้องค์กรสามารถสร้างคุณค่าเพิ่มในสินค้าและบริการ
 - สร้างความได้เปรียบในการแข่งขัน (Competitive Advantage)
 - ทำลายคู่แข่งแบบสร้างสรรค์ (Creative Destruction)
 - เสริมภาพลักษณ์ที่ดีให้กับองค์กร
 - สร้างจิตสำนึกในการปฏิบัติงานที่ดีให้กับพนักงานทุกคน (GRC DNA)

As information is a key resource for all enterprises, we 'executives' strive to.

- Maintain high-quality information to support business decisions.
- Generate business value from IT-enabled investment – achieve strategic goals and realize business benefits through effective and innovative use of IT.
- Achieve operational excellence through the reliable and efficient application of technology.
- Maintain IT-related risk at an acceptable level.
- Optimize the cost of IT services and technology.
- Comply with ever-increasing relevant laws, regulations, contractual agreements and policies.

GRC Framework - implication

Governance, Risk,
Compliance

Business
Value

Internal Control

Regulatory
Compliance

Risk
Management

Social
Responsibilities

Business
Strategic
Objectives

Stakeholder
Satisfaction

SEC GRC Framework

SOX

Sarbanes Oxley Act ,
International Laws

Thai E- Transaction Laws

Organization Requirement

COSO

(The Committee of Sponsoring Organizations of the
Treadway Commission) - Financial Reporting &
Business Process Oriented

Thai OAG

(Office of The Auditor General)

CobiT 3rd Edition, CobiT4.0, CobiT 4.1, COBIT5

Control Objectives for Information and related Technology IT oriented bridging
the gap between business processes and IT controls

ITIL

(IT Infrastructure Library)

ISO/IEC

17799/2700X
The Code of Practice for
ISM

Lessons Learned /other Standard

**Balancing Strategies on
Process, People and
Technology**

ตัวช่วยถัดไป

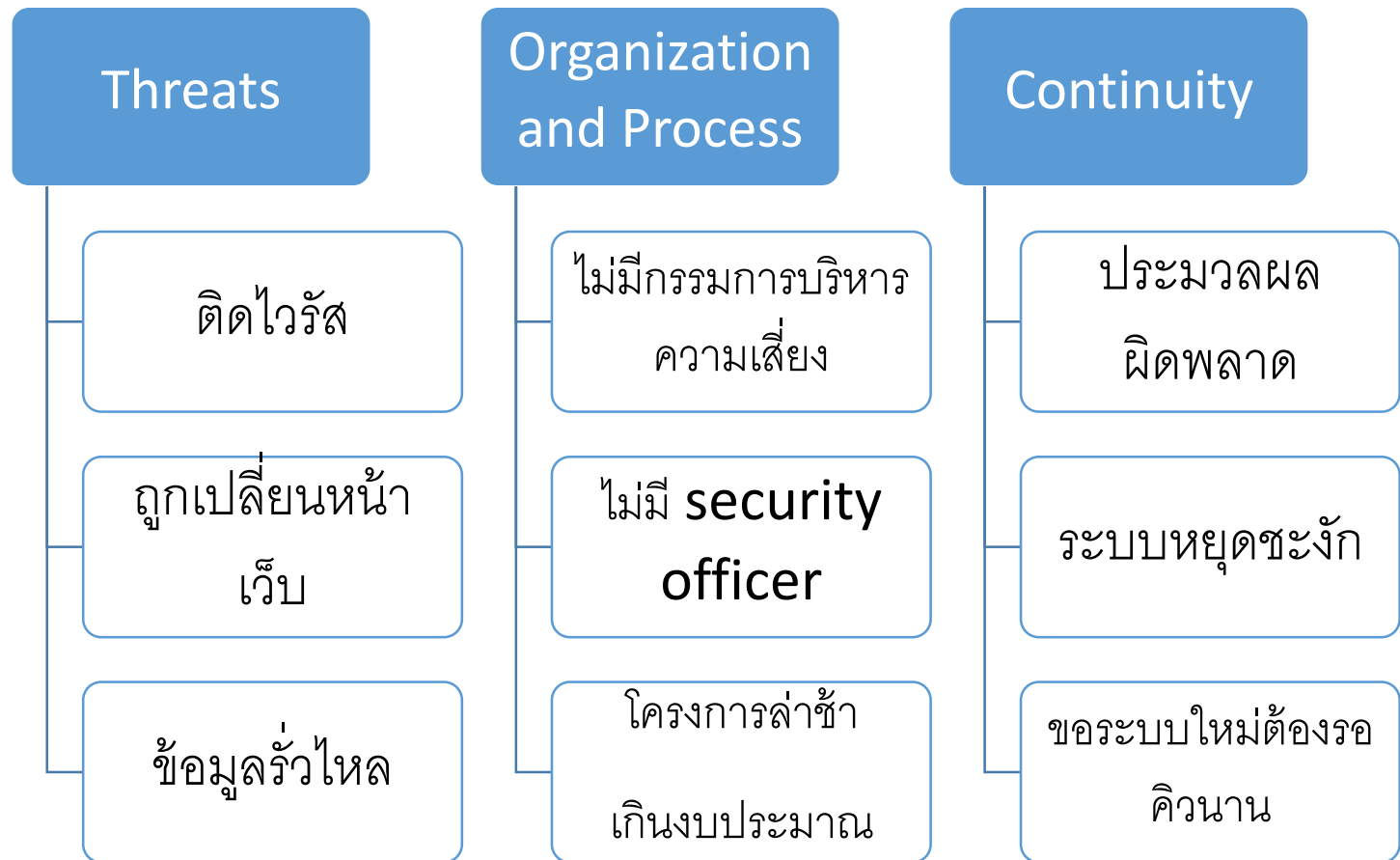
What is IT Risk Management?

การบริหารความเสี่ยง

สิ่งที่ต้องดำเนินการในการบริหารความเสี่ยง

- Health Check
 - Threat
 - Organization and process
 - Continuity
- Enterprise Risk management
- ICT Risk Management

เช็คสุขภาพ — ปัญหาเหล่านี้ พบบ้างไหม



Enterprise Risk Management (ERM) Defined:

“... a process, effected by an entity's board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risks to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives.”

*Source: COSO Enterprise Risk Management – Integrated Framework. 2004. COSO.
(Committee of Sponsoring Organizations of the Treadway Commission)*

WHAT IS COSO ?

COSO = COmmittee of Sponsoring Organizations

- **American Accounting Association (AAA)**
- **American Institute of CPAs (AICPA)**
- **Financial Executives Institute (FEI)**
- **The Institute of Internal Auditors (IIA)**
- **The Institute of Management Accountant (IMA)**

WHAT IS COSO ?

- *ความเป็นมา*
- สืบเนื่องจากวิกฤตทางการเมืองและเศรษฐกิจของสหรัฐอเมริกา ในช่วงปีค.ศ.1970 จนถึงปีค.ศ.1977 สหรัฐฯได้ประกาศกฎหมายแนวปฏิบัติเกี่ยวกับความไม่สุจริตในการให้สินบนต่างชาติ (the 1977 Foreign Corrupt Practices Act – FCPA) ซึ่งส่วนสำคัญส่วนหนึ่ง กำหนดให้มีการควบคุมภายใน ต่อมาเดือนตุลาคม ค.ศ.1985 มีการจัดตั้งองค์กรอิสระ คือ คณะกรรมการเพื่อการรายงานการทุจริตแห่งชาติ (National Commission on Fraudulent Financial Reporting หรือเรียกย่อ Treadway Commission เพื่อให้เกียรติ Mr.Stephen R Treadway ผู้ก่อตั้งซึ่งตีพิมพ์รายงานครั้งแรกในปี ค.ศ. 1987 ภายใต้การสนับสนุนของคณะกรรมการวิชาชีพอิสระอื่นๆที่ต่อมาเรียกว่า The Committee of Sponsoring Organization of the Treadway Commission (COSO)

http://en.wikipedia.org/wiki/COSO#Key_concepts_of_the_COSO_framework

Why ERM Is Important

Underlying principles:

- Every entity, whether for-profit or not, exists to realize value for its stakeholders.
- Value is created, preserved, or eroded by management decisions in all activities, from setting strategy to operating the enterprise day-to-day.

Why ERM Is Important

ERM supports value creation by enabling management to:

- Deal effectively with potential future events that create uncertainty.
- Respond in a manner that reduces the likelihood of downside outcomes and increases the upside.

Enterprise Risk Management — Integrated Framework

This COSO ERM framework defines essential components, suggests a common language, and provides clear direction and guidance for enterprise risk management.

The ERM Framework

- Entity objectives can be viewed in the context of four categories:
 - Strategic
 - Operations
 - Reporting
 - Compliance



The ERM Framework

ERM considers activities at all levels of the organization:

- Enterprise-level
- Division or subsidiary
- Business unit process



The ERM Framework

Enterprise risk management requires an entity to take a *portfolio view* of risk.

- Management considers how individual risks interrelate.
- Management develops a portfolio view from two perspectives:
 - Business unit level
 - Entity level

The ERM Framework

The eight components of the framework are interrelated ...

- สภาพแวดล้อมภายใน
- การกำหนดวัตถุประสงค์
- การระบุเหตุการณ์เสี่ยง
- การประเมินความเสี่ยง
- การจัดการความเสี่ยง
- ออกแบบกิจกรรมควบคุม
- สารสนเทศและการสื่อสาร
- การติดตามผล

วัตถุประสงค์
• ระดับกระบวนการ



วัตถุประสงค์
ระดับ
องค์กร

Internal Control

A strong system of internal control is essential to effective ERM.

Key Implementation Factors

Organizational design of business

Establishing an ERM organization

Performing risk assessments

Determining overall risk appetite

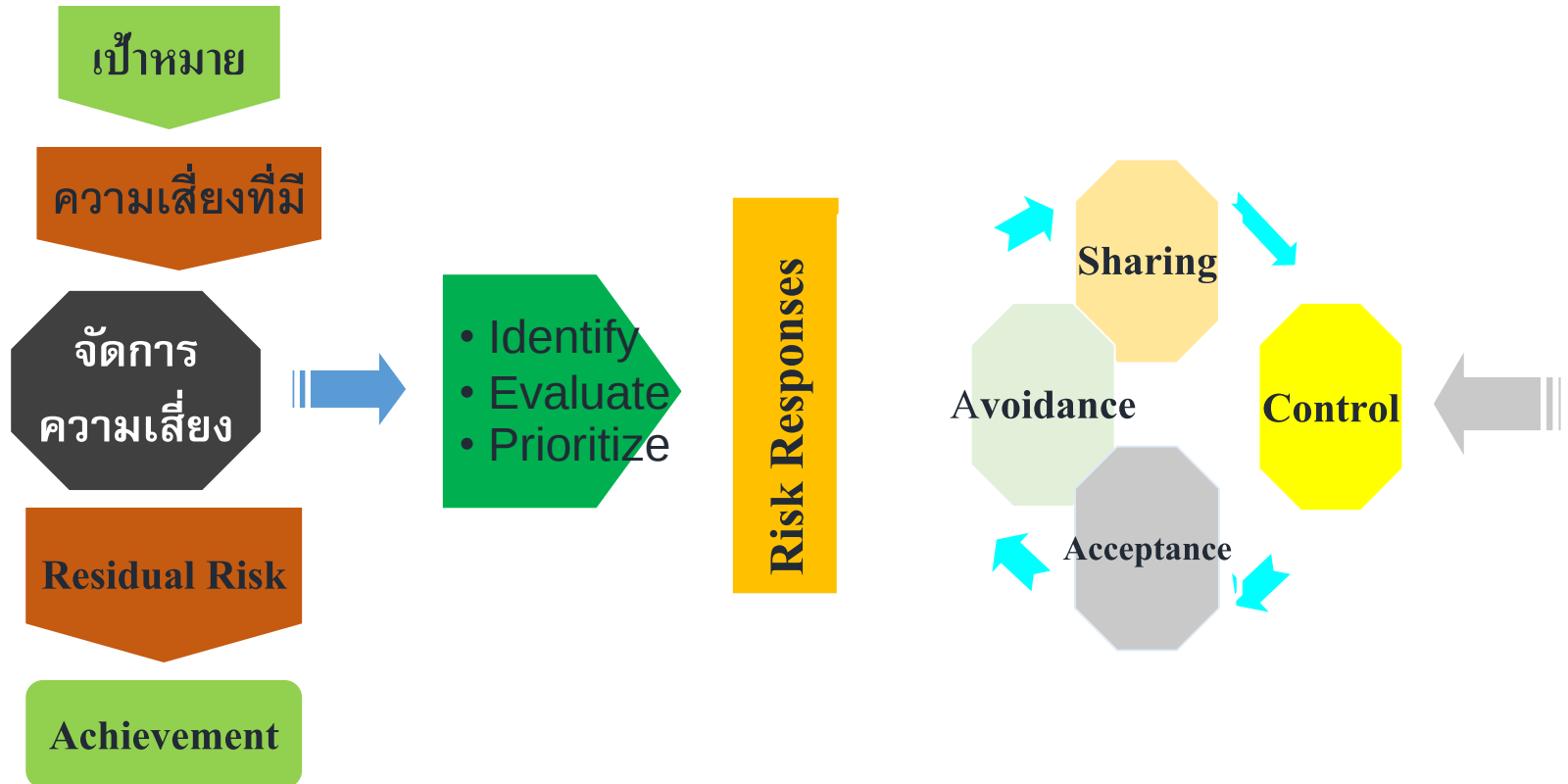
Identifying risk responses

Communication of risk results

Monitoring

Oversight & periodic review by management

หลักการบริหารความเสี่ยง



Risk management Guide for IT Systems

1. Integration of risk management into SDLC

- Initiation
- Development or acquisition
- Implementation
- Operation or maintenance
- Disposal

2. Risk management

- Risk assessment
- Risk mitigation
- Evaluation and assessment

เลือกมาตรฐานไหนดี

NIST

**National Institute of
Standards and Technology**

Technology Administration

U.S. Department of Commerce

Matrix of Risk Level (Risk Map)

Threat Likelihood	Impact		
	Low (10)	Medium (50)	High (100)
High (1.0)	Low $10 \times 1.0 = 10$	Medium $50 \times 1.0 = 50$	High $100 \times 1.0 = 100$
Medium (0.5)	Low $10 \times 0.5 = 5$	Medium $50 \times 0.5 = 25$	Medium $100 \times 0.5 = 50$
Low (0.1)	Low $10 \times 0.1 = 1$	Low $50 \times 0.1 = 5$	Low $100 \times 0.1 = 10$

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

Matrix of Risk Level (Another Firm)

Threat Likelihood	Impact		
	Low (10)	Medium (50)	High (100)
High (1.0)	Low $10 \times 1.0 = 10$	Medium $50 \times 1.0 = 50$	High $100 \times 1.0 = 100$
Medium (0.5)	Low $10 \times 0.5 = 5$	Medium $50 \times 0.5 = 25$	Medium $100 \times 0.5 = 50$
Low (0.1)	Low $10 \times 0.1 = 1$	Low $50 \times 0.1 = 5$	Low $100 \times 0.1 = 10$

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

อีกมาตรฐานที่แนะนำ

IT Risk

Turning Business Threats into
Competitive Advantage

Harvard Business School Press

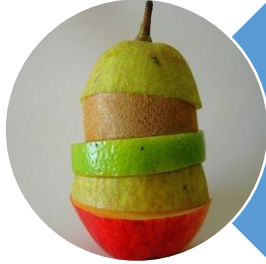
IT Risk — Turning Business Threats into Competitive Advantage — HBSP

- The 4A Risk Management Framework
 - Availability
 - Keep the systems and business processes running, and recover from interruptions
 - Access
 - Ensure appropriate access
 - Potential for misuse of sensitive information
 - Accuracy
 - Provide correct, timely and complete information that meets stakeholders' requirement
 - Agility
 - Posses the capability to change with managed cost and speed

3 Core Disciplines of IT Risk Management



A well-structured
foundation of IT assets



A well-designed and
executed risk governance
process



A risk-aware culture

Key IT Risk Factors

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

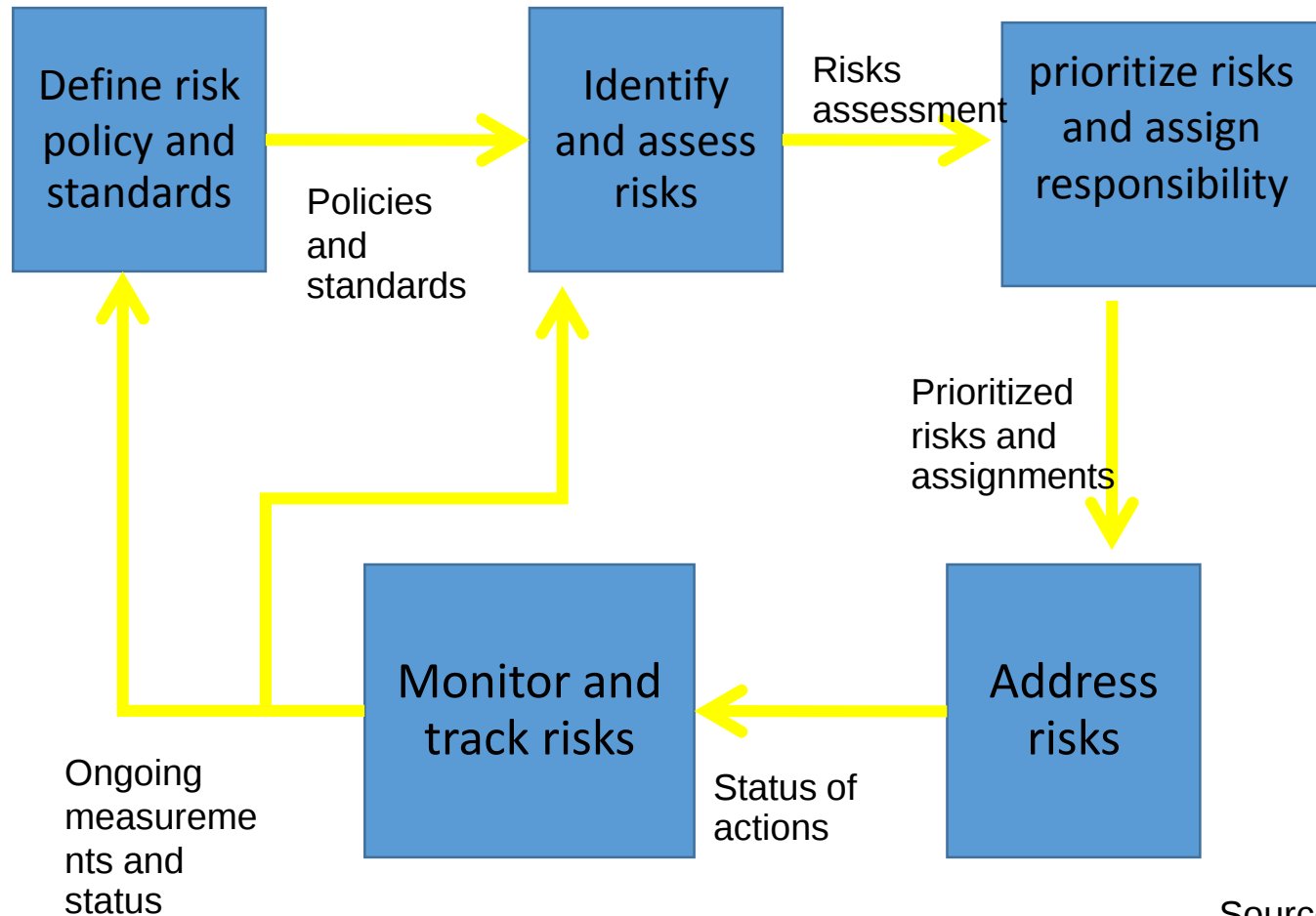
Key IT Risk Factors

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

Key IT Risk Factors

- Accuracy
 - Applications do not meet business requirement
 - Manual data integration required
 - Significant implementation under way or recently completed
- Agility
 - Poor IT-business relations
 - Poor project delivery

IT Risk Governance process



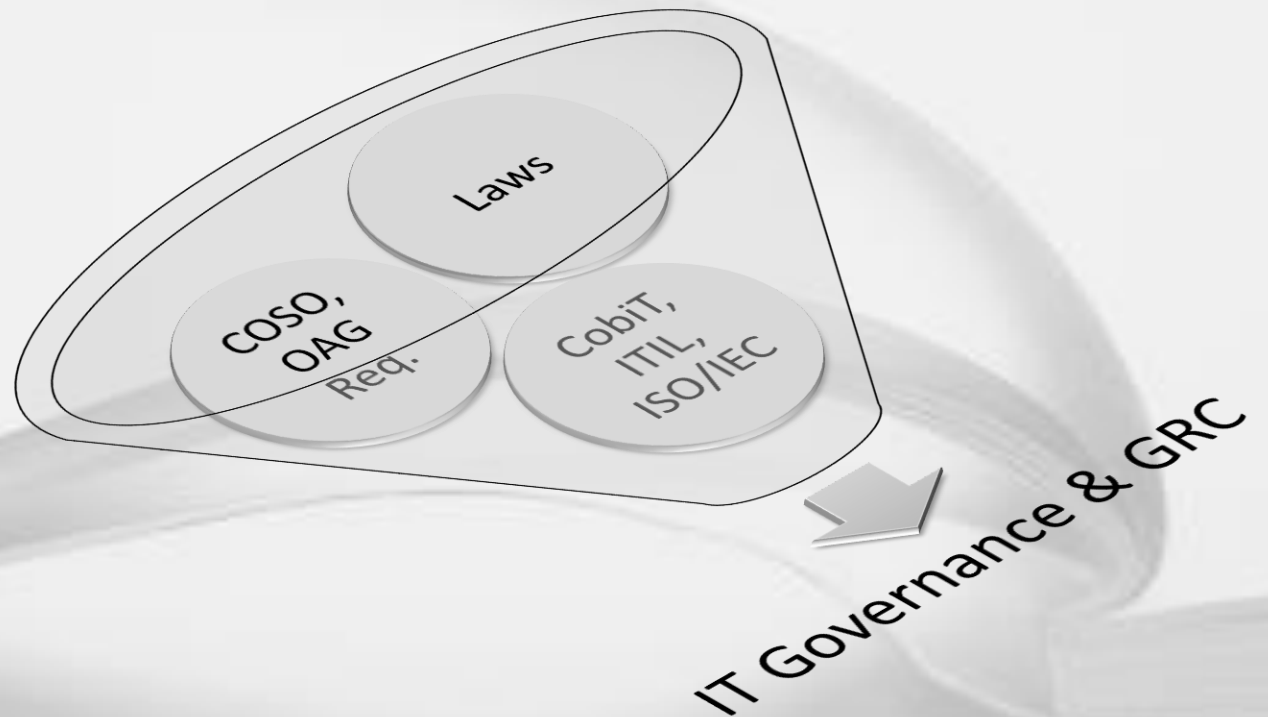
Source:
Gartner

ตัวช่วยถัดไป

IT Governance & IT Best Practices

ไอทีภิบาลและแนวปฏิบัติที่ดีเลิศ

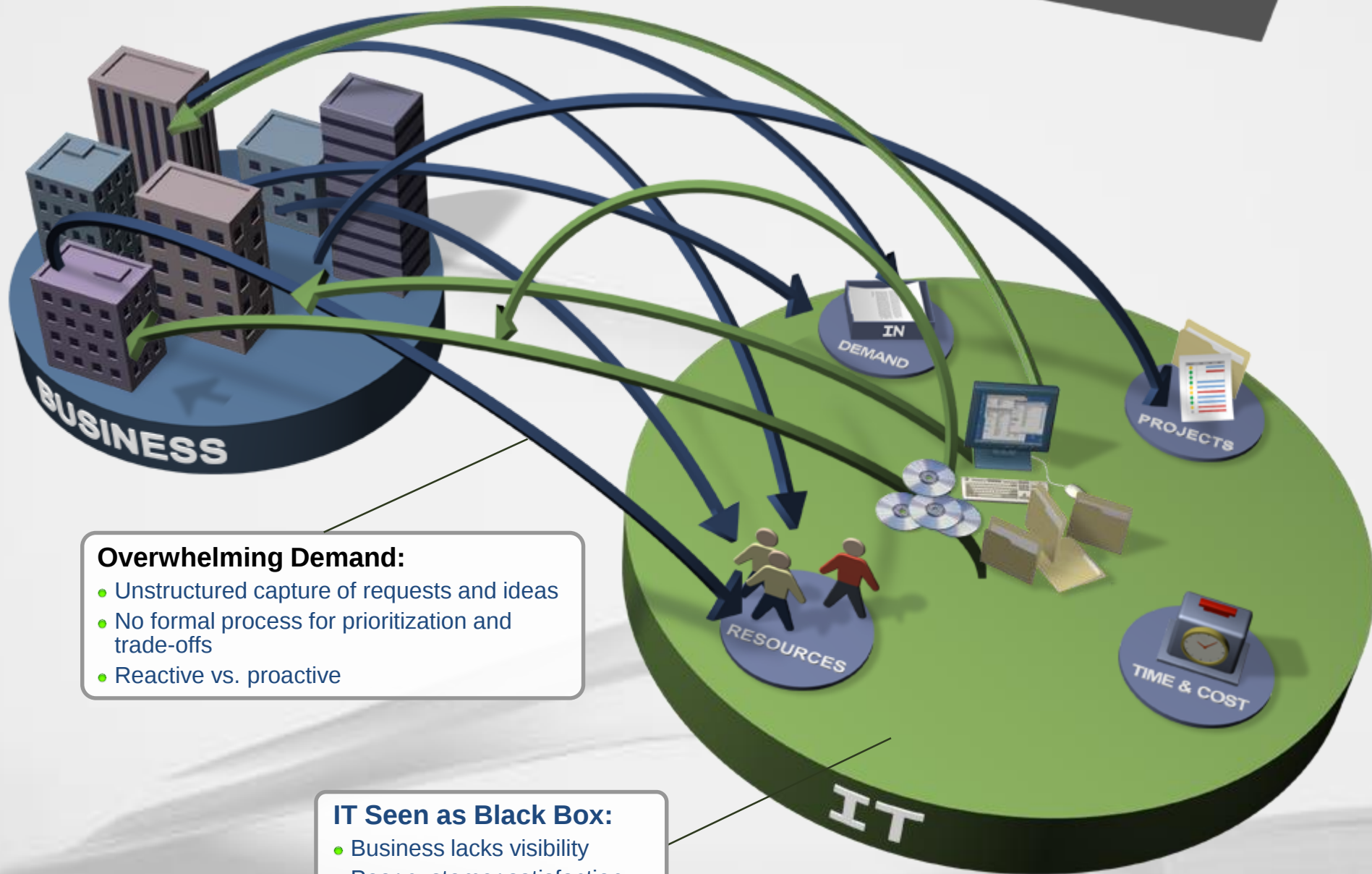
What We Need To Achieve?



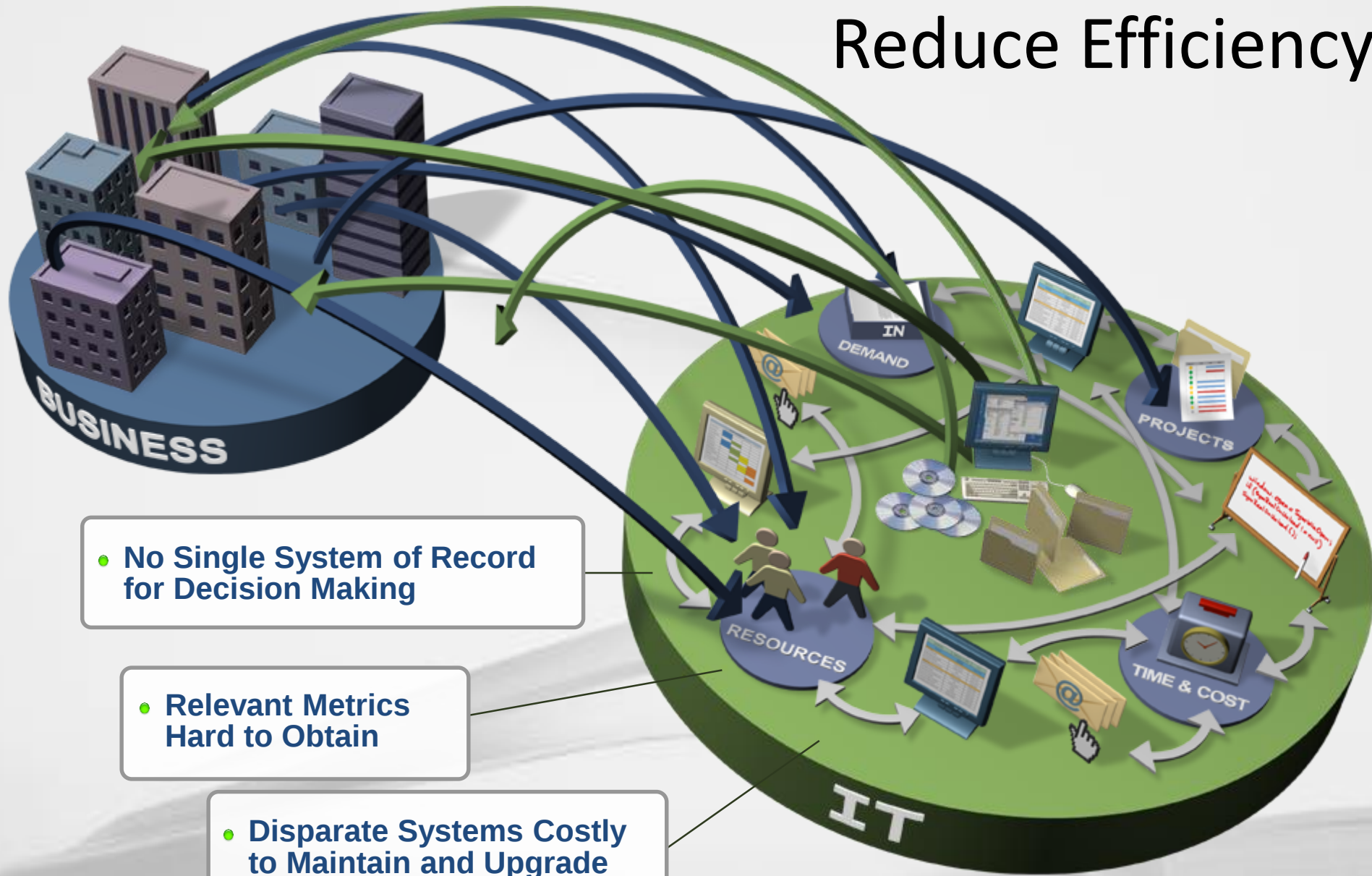


What is IT Governance

WHAT IS IT GOVERNANCE?

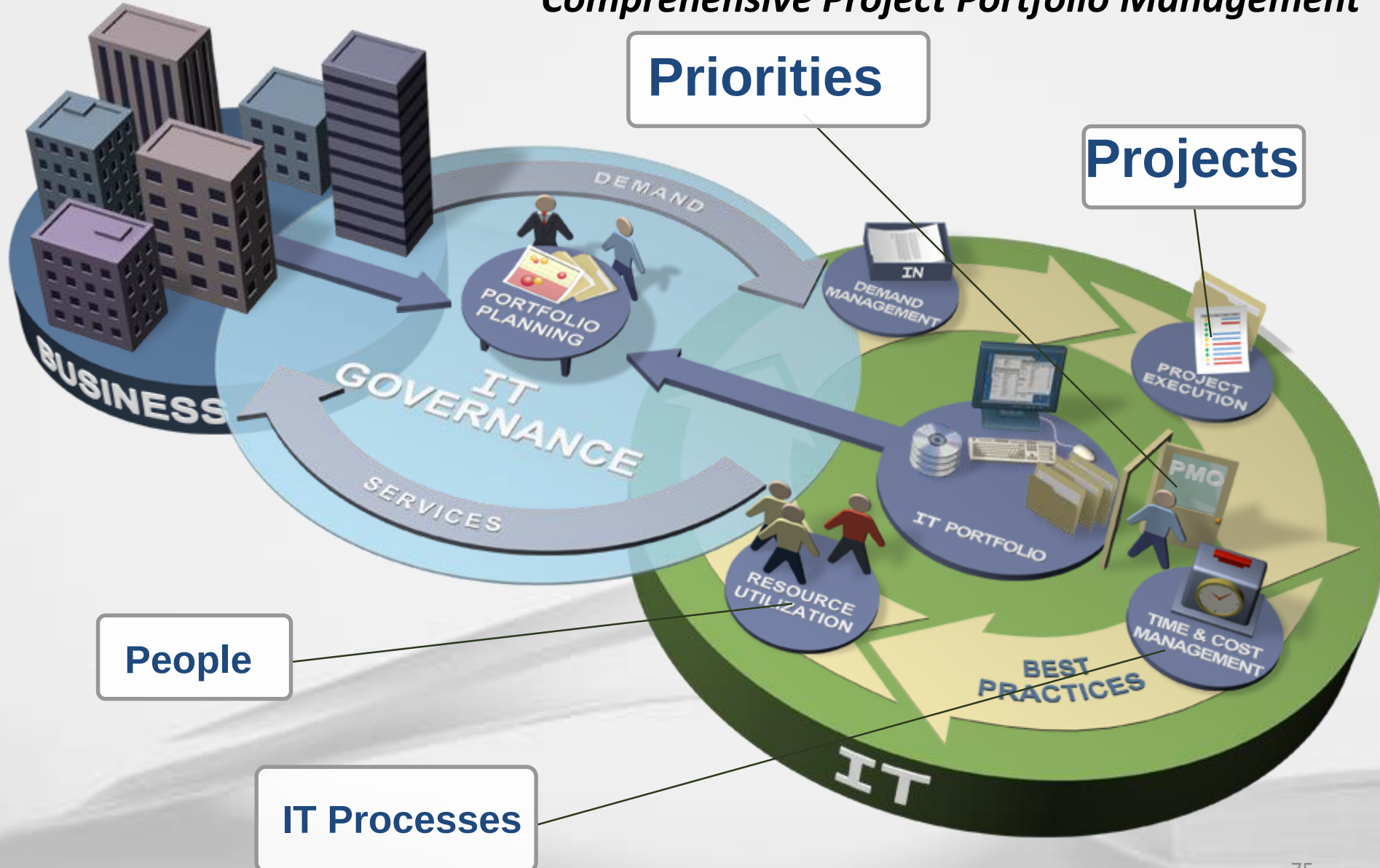


Disparate Systems Reduce Efficiency



Efficiency

Comprehensive Project Portfolio Management



IT Governance Landscape



Blueprint
for
Success

IT Governance is about :

Improving Engagement and Efficiency

**What is
Engagement?**

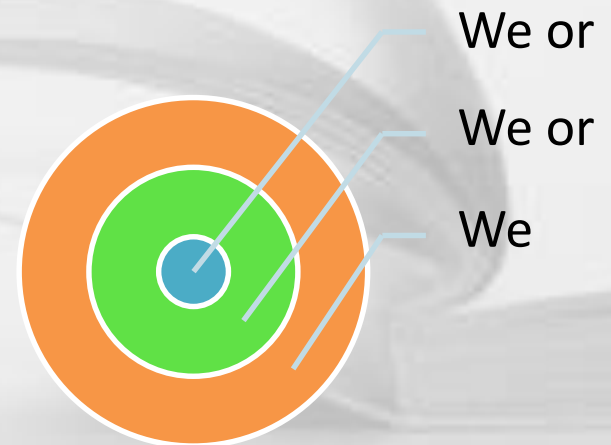
**Doing the
Right Things**

**What is
Efficiency?**

**Doing
Things Right**

Consequently management functions also need to focus on:

- **WHERE** the market is going
- **WHERE** your firm is relative to this changing market and competitors, and
- **HOW** you may need to re-position yourself to ensure continued competitive relevance.





IT Governance Resources and Implementation Step

IT GOVERNANCE RESOURCES AND IMPLEMENTATION STEP

COSO – Internal Control for Corporate Governance



IT Governance

What is COSO?

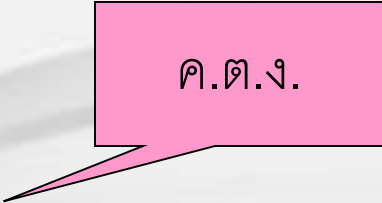
- Committee of Sponsoring Organization (COSO) of the Treadway Commission
“Internal Control – Integrated Framework”
(<http://www.coso.org/>)
- Organization-wide applicability
- Reporting target is Executive Board
- Created by professional auditor associations

COSO and IT Governance

- **COSO is the most widely recognized framework for Corporate Governance**
- **COSO However, did not provide sufficient details on IT**
- **CobiT has become the control framework for IT Governance**

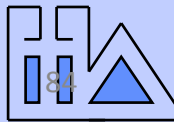
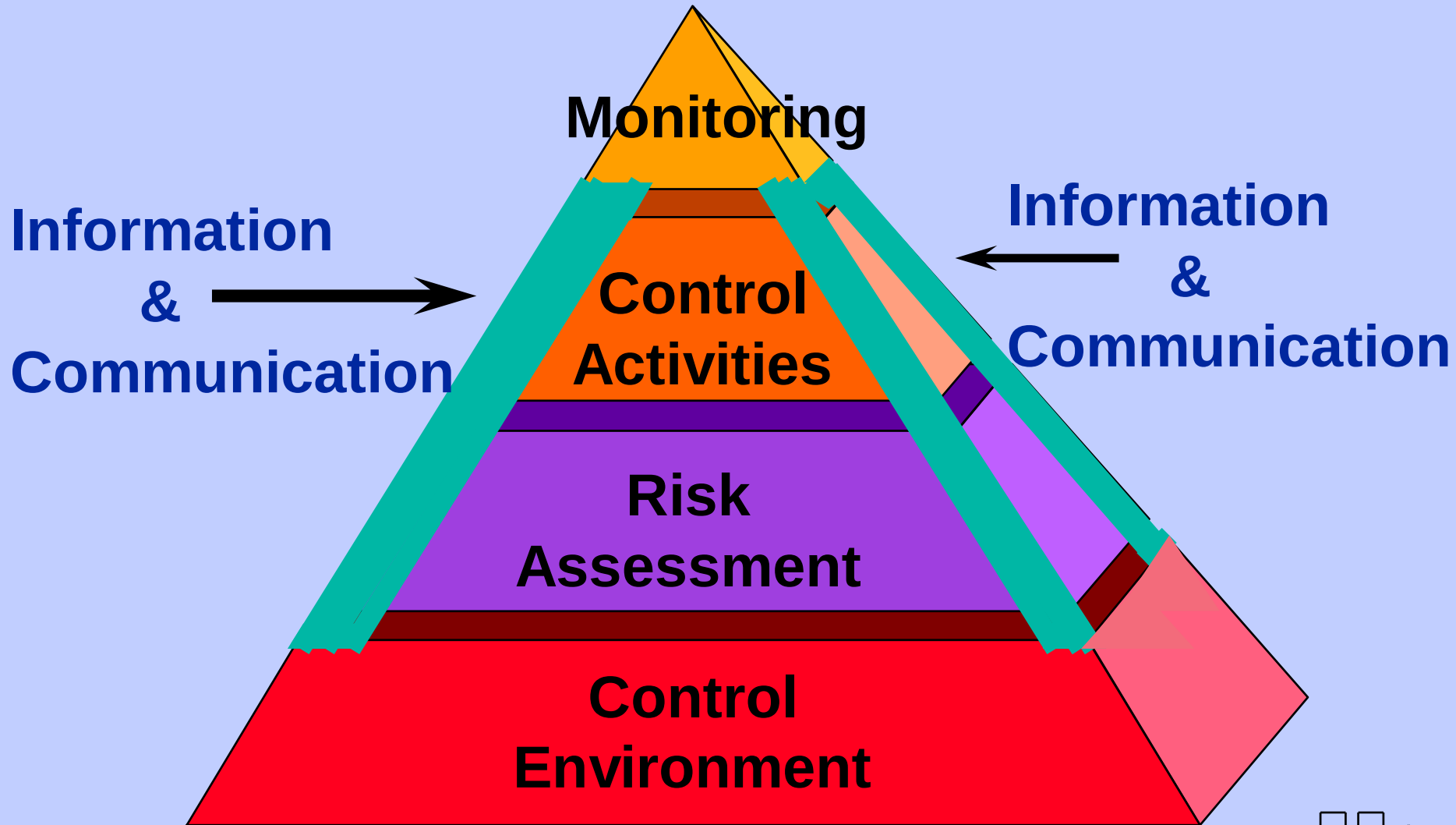
Internal Control Framework

- In 1992, COSO developed a model for evaluating internal controls
- Defines internal control as "a process, designed to provide reasonable assurance of the achievement of objectives in the following categories":
 - Effectiveness and efficiency of operations
 - Reliability of financial reporting
 - Compliance with applicable laws and regulations
- COSO has become the definitive standard for internal control
- In "effective" control systems, the objectives are supported by
 - Control Environment
 - Risk Assessment
 - Control Activities
 - Quality of Information
 - Monitoring
- Compliance rules do not specify which framework companies must use (others include CoBIT, CoCo, ACC, Turnbull Report)

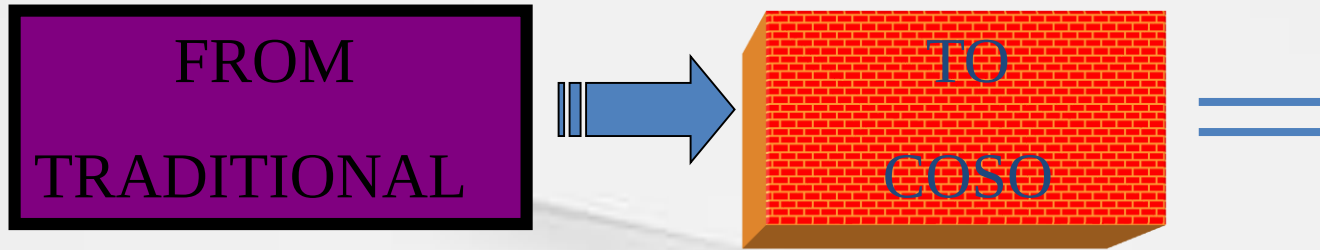


ค.ต.ง.

COSO Framework



Changed in Auditor Point of View



REACTIVE

FOCUS ON PEOPLE

DETECT/CORRECT

INSPECT IN QUALITY

SURVIVAL OF FITTEST

AUDIT DRIVEN SOLUTIONS

PROACTIVE

FOCUS ON OPPORTUNITIES

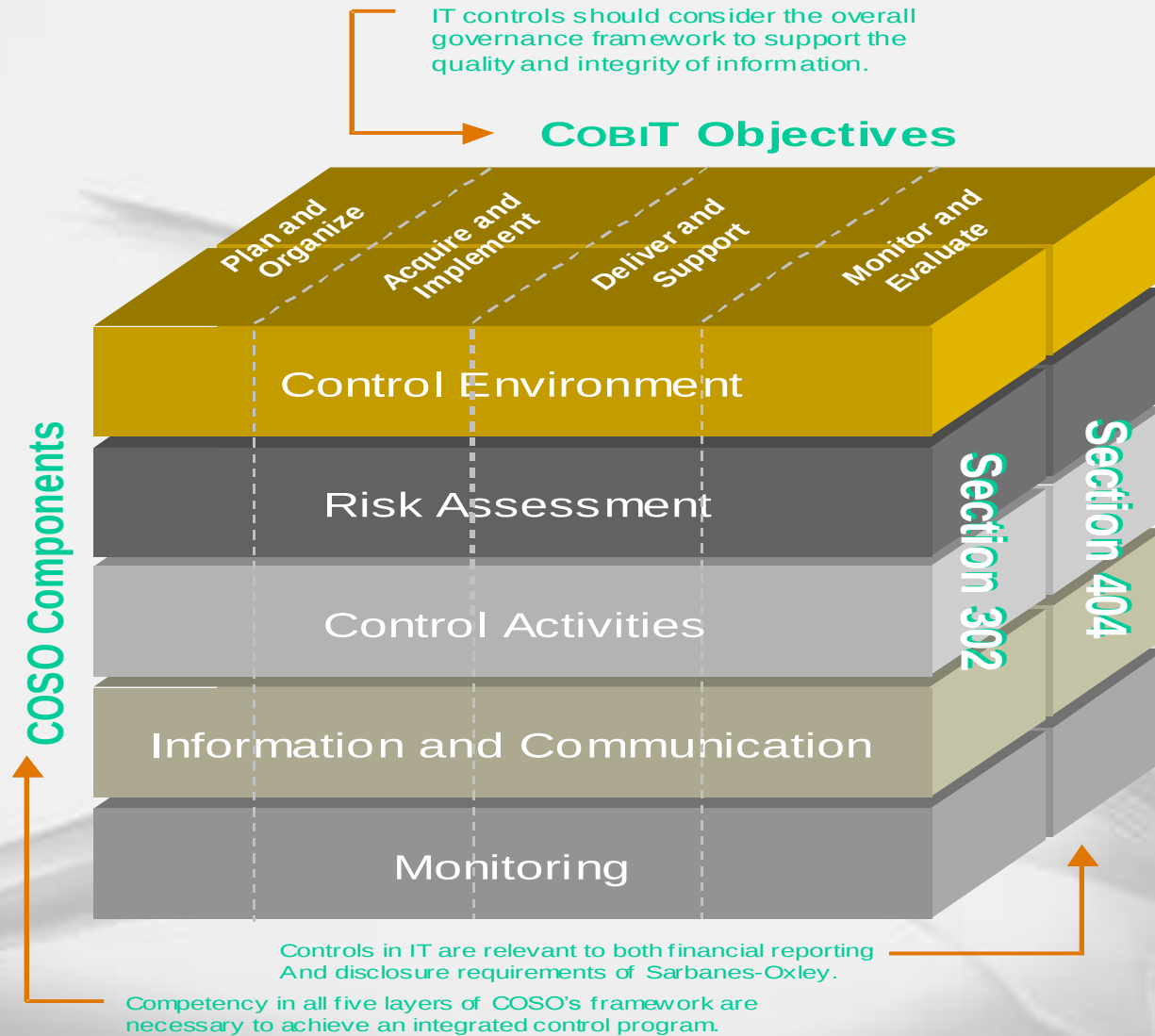
PREVENT/MONITOR

BUILD IN QUALITY

EVERYONE CAN CONTRIBUTE

OPERATIONS DRIVEN SOLUTIONS

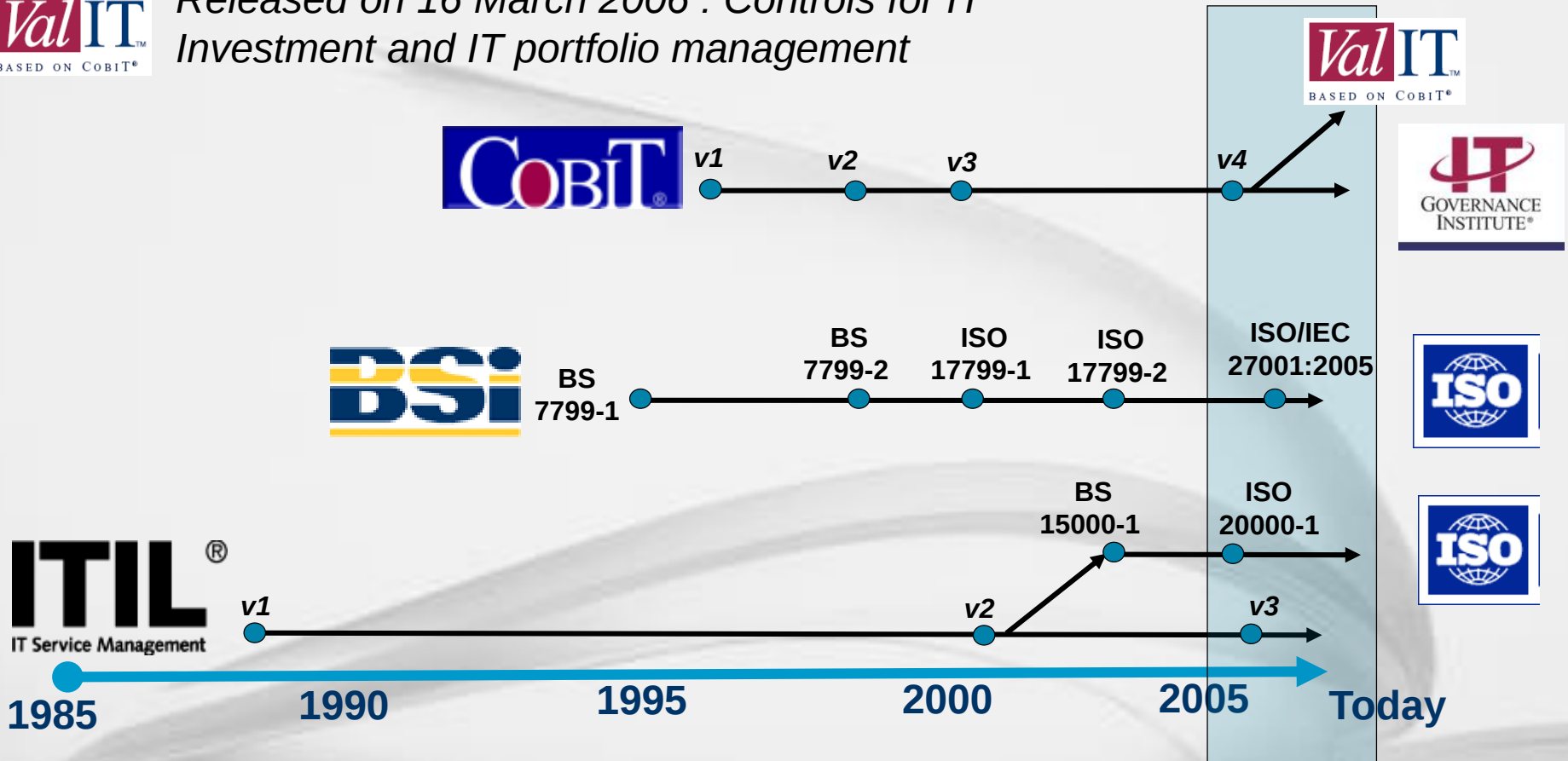
SOX, COSO and COBIT®



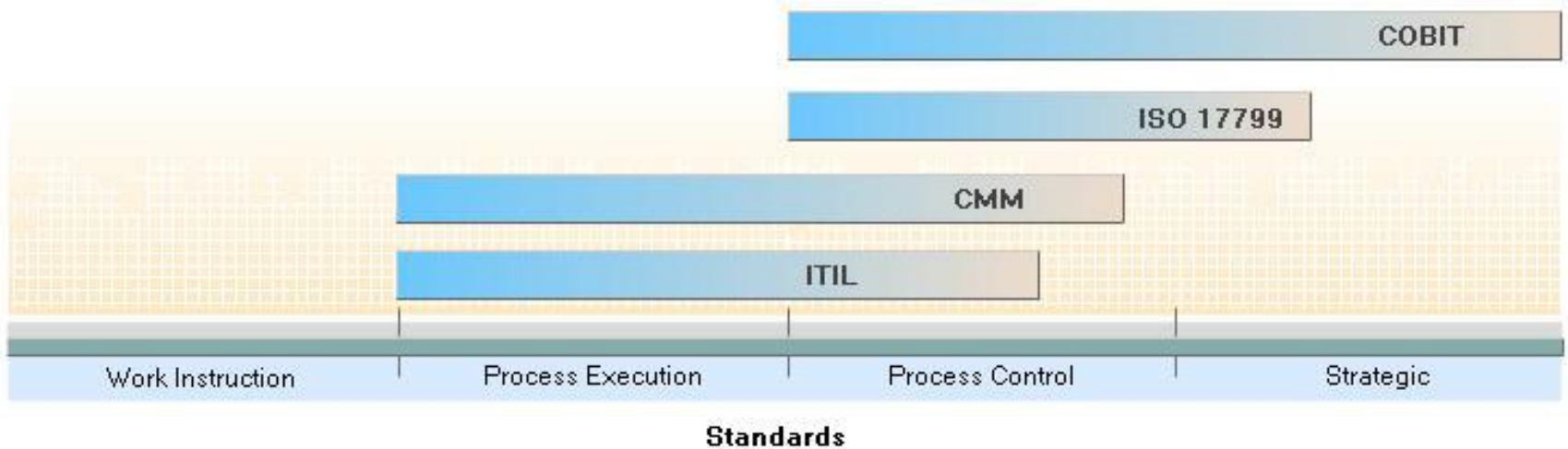
IT Processes & Best Practices



Released on 16 March 2006 : Controls for IT Investment and IT portfolio management



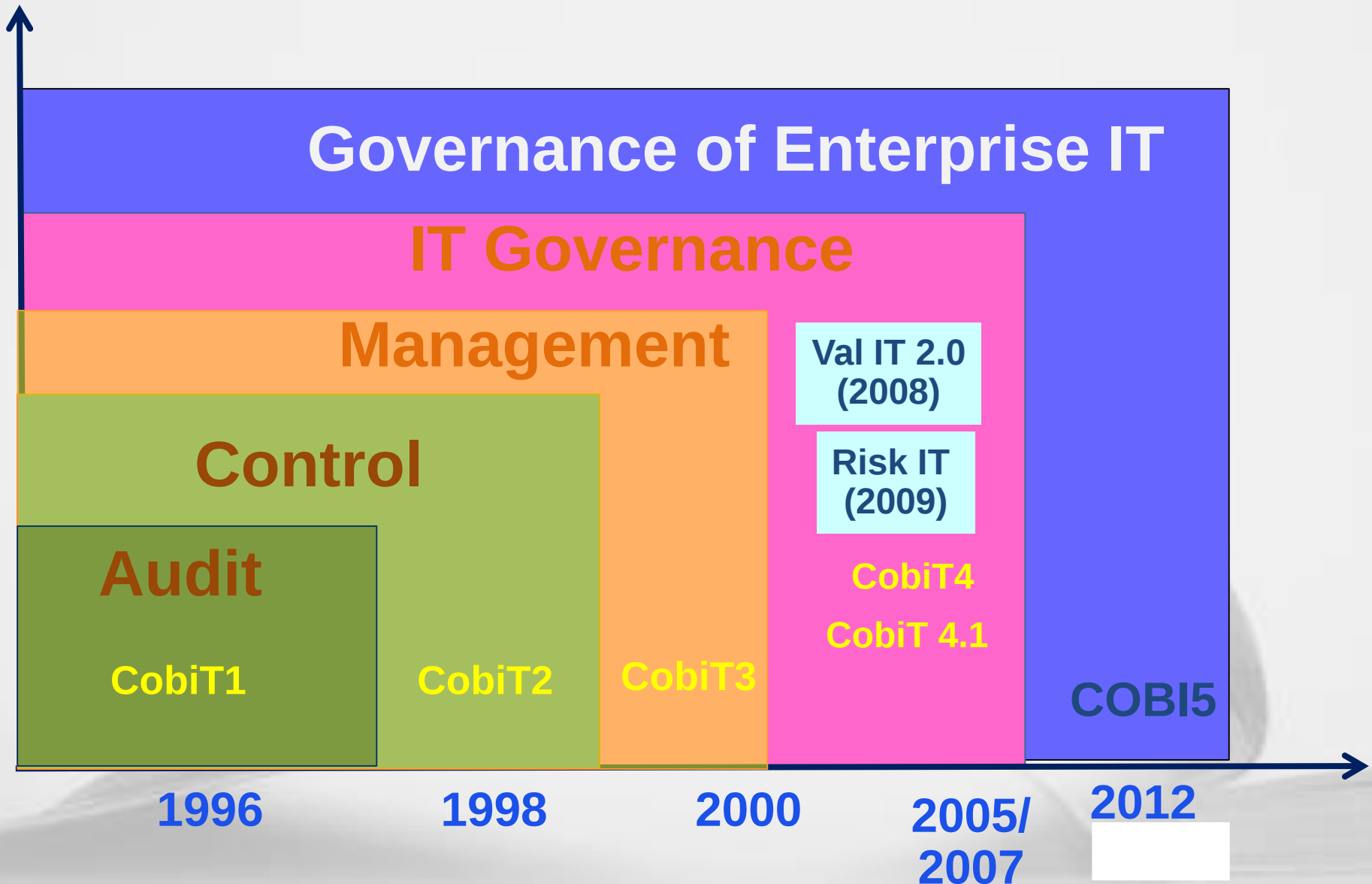
Roles of “Best Practices”



What is COBIT?

- **Control Objectives for Information and related Technology (COBIT)**
- COBIT is an IT governance framework and supporting tool set that allows managers to bridge the gap between control requirements, technical issues and business risk.
- COBIT emphasizes regulatory compliance, helps organizations to increase value attained from IT, enables alignment and simplifies implementation of the COBIT framework.

History of COBIT



What is CobiT?

- Controls for IT Governance
 - Add value while balancing risk versus return for IT and its processes.”
- Format
 - “The control of *IT Processes* which satisfy *Business Requirements* is enabled by *Control Statements* considering *Control Practices*”

What is CobiT?

- Evaluation of CobiT controls
 - Assessment of maturity rating described for each control, ranging from 0 (non-existent) to 5 (optimized),
 - Performance measurement
 - Business goals
 - IT goals
 - Process goals
 - Activity goals

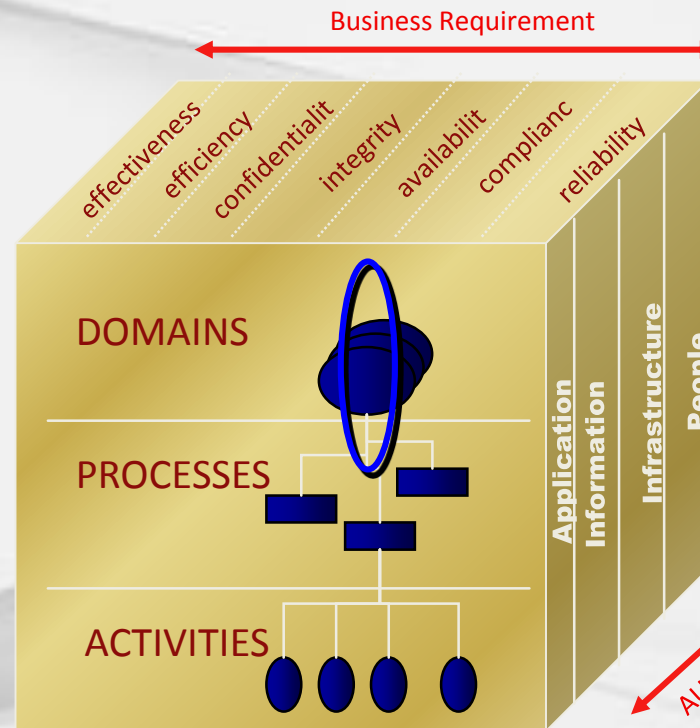
CobiT Cube

Control Criteria

EXPEDIENCE

CONTRIBUTION

IT PROCESSES



SUSTAINABILITY

AUDITABLE
RESOURCES

EFFORT

CobiT Control Domains

- **Planning and Organization Controls**
 - 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

CobiT Control Domains

- Acquisition and Implementation Controls
 - AI1 Identify automated solutions
 - AI2 Acquire and maintain application software
 - AI3 Acquire and maintain technology infrastructure
 - AI4 Enhance operation and use
 - AI5 Procure IT resources
 - AI6 Manage changes
 - AI7 Install and accredit solutions and changes

CobiT Control Domains

- **Delivery and Support Controls**
 - 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

CobiT Control Domains

- Monitoring and Evaluating Controls
 - ME1 Monitor and evaluate IT performance
 - ME2 Monitor and evaluate internal control
 - ME3 Ensure compliance with external requirements
 - ME4 Provide IT governance

COBIT 5 - 2012

COBIT 5 - 2012



What is IT Governance?

Governance ensures that stakeholder needs, conditions and options are evaluated to determine balanced, agreed-on enterprise objectives to be achieved; setting direction through prioritisation and decision making; and monitoring performance and compliance against agreed-on direction and objectives

In most enterprises, overall governance is the **responsibility of the board of directors** under the leadership of the chairperson. Specific governance responsibilities **may be delegated** to special organisational structures **at an appropriate level**, particularly in larger, complex enterprises.

What is IT Management?

Management plans, builds, runs and monitors activities in alignment with the direction set by the governance body to achieve the enterprise objectives.

In most enterprises, management is the **responsibility of the executive management** under the leadership of the chief executive officer (CEO).

5 Principles for Governance and management of Enterprise IT

Principle 1: Meeting Stakeholder Needs

Principle 2: Covering the Enterprise End-to-End

Principle 3: Applying a Single, Integrated Framework

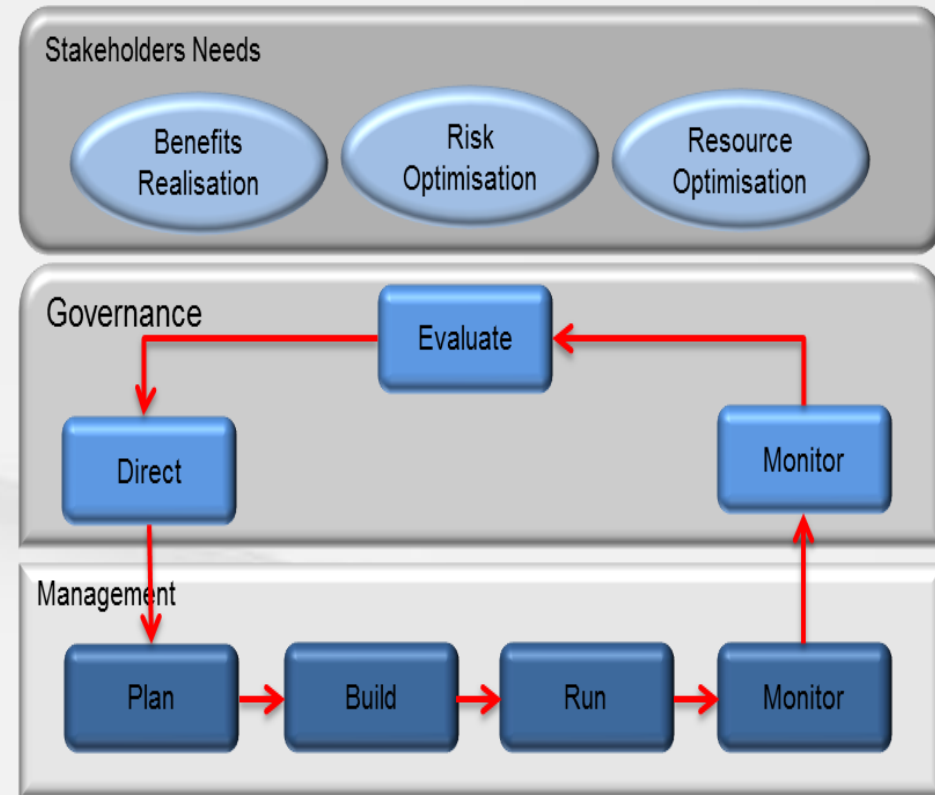
Principle 4: Enabling a Holistic Approach

Principle 5: Separating Governance From Management

กรอบการดำเนินงานสำหรับการกำกับดูแล และการบริหารจัดการไอทีระดับองค์กร

วัตถุประสงค์ เพื่อช่วยให้บรรลุเป้าหมาย (goal) ทางธุรกิจ โดยการรักษาสสมดุลระหว่าง

- การได้รับผลประโยชน์
- การจัดการความเสี่ยงอย่างเหมาะสม
- การใช้ทรัพยากรให้เกิดประโยชน์สูงสุด



การกำกับดูแล (Governance)

เพื่อให้มั่นใจได้ว่าทุกความต้องการ เงื่อนไข และทางเลือกของ Stakeholder ได้รับการประเมิน

- กำหนด goal และเห็นชอบร่วมกัน
- กำหนดทิศทางผ่านการจัดลำดับความสำคัญ
- เฝ้าติดตามประสิทธิภาพในการทำงาน และการปฏิบัติตามกฎระเบียบต่างๆ

การบริหารจัดการ (Management)

ผู้บริหาร วางแผน สร้าง ดำเนินงาน และเฝ้าติดตามกิจกรรมต่างๆ ให้สอดคล้องกับทิศทางที่กำหนด เพื่อให้บรรลุวัตถุประสงค์ขององค์กร

กรอบการดำเนินงานสำหรับการกำกับดูแล และการบริหารจัดการไอทีระดับองค์กร

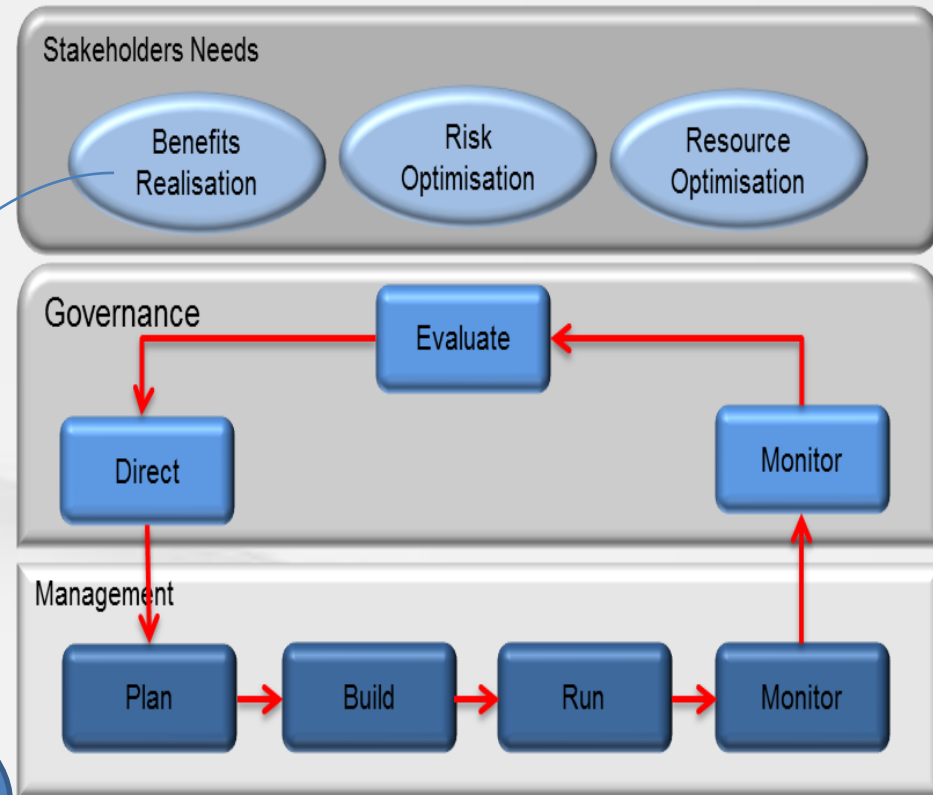
วัตถุประสงค์ เพื่อช่วยให้บรรลุเป้าหมาย (goal) ทางธุรกิจ โดยการรักษาสมดุลระหว่าง

- การได้รับผลประโยชน์
- การจัดการความเสี่ยงอย่างเหมาะสม
- การใช้ทรัพยากรให้เกิดประโยชน์สูงสุด

วัดผลแบบ BSC

(financial/customer/process/
learning & growth) เช่น เกิด

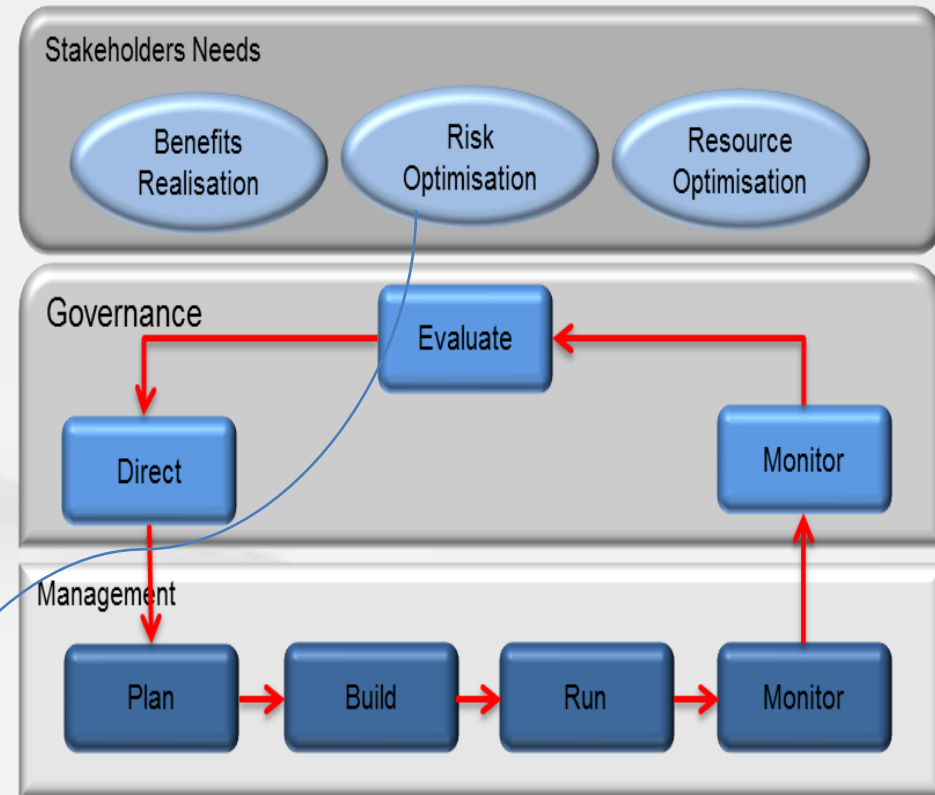
ผลิตภัณฑ์หรือบริการใหม่ๆ / ความโปร่งใสทาง
การเงิน / บริการต่อเนื่อง / มีประสิทธิภาพ /
ส่งเสริมนวัตกรรม / ลดต้นทุน เป็นต้น



กรอบการดำเนินงานสำหรับการกำกับดูแล และการบริหารจัดการไอทีระดับองค์กร

วัตถุประสงค์ เพื่อช่วยให้บรรลุเป้าหมาย (goal) ทางธุรกิจ โดยการรักษาสมดุลระหว่าง

- การได้รับผลประโยชน์
- การจัดการความเสี่ยงอย่างเหมาะสม
- การใช้ทรัพยากรให้เกิดประโยชน์สูงสุด

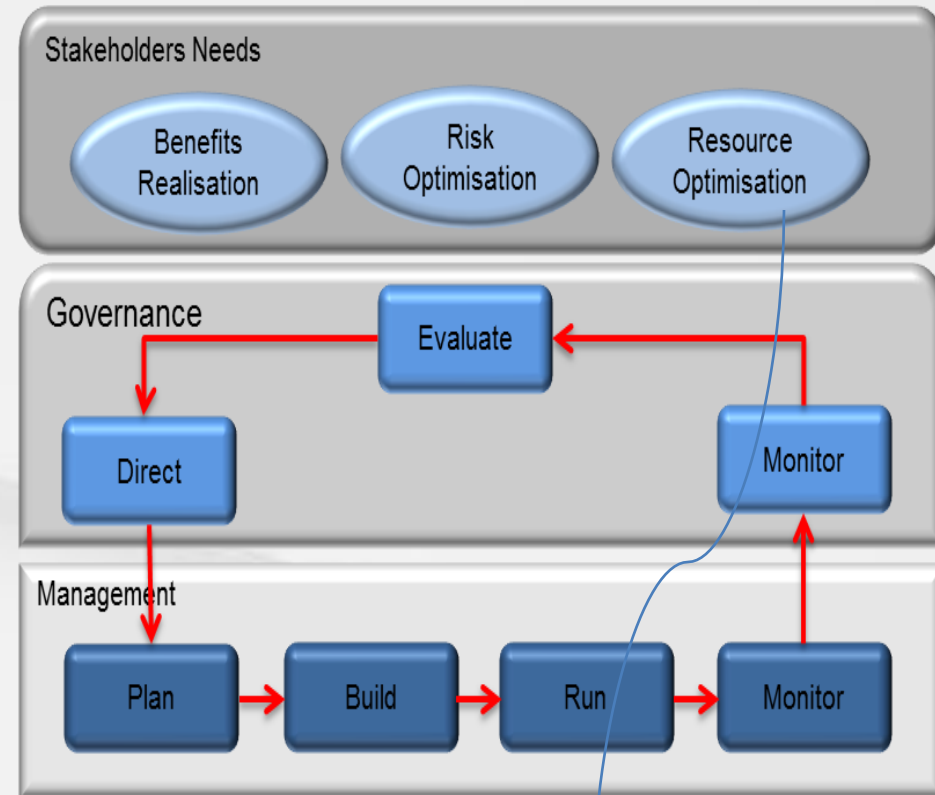


การให้บริการต่อเนื่อง / การปฏิบัติ
ตามนโยบายที่กำหนด / ตัดสินใจ
บนพื้นฐานของสารสนเทศ

กรอบการดำเนินงานสำหรับการกำกับดูแล และการบริหารจัดการไอทีระดับองค์กร

วัตถุประสงค์ เพื่อช่วยให้บรรลุเป้าหมาย (goal) ทางธุรกิจ โดยการรักษาสมดุลระหว่าง

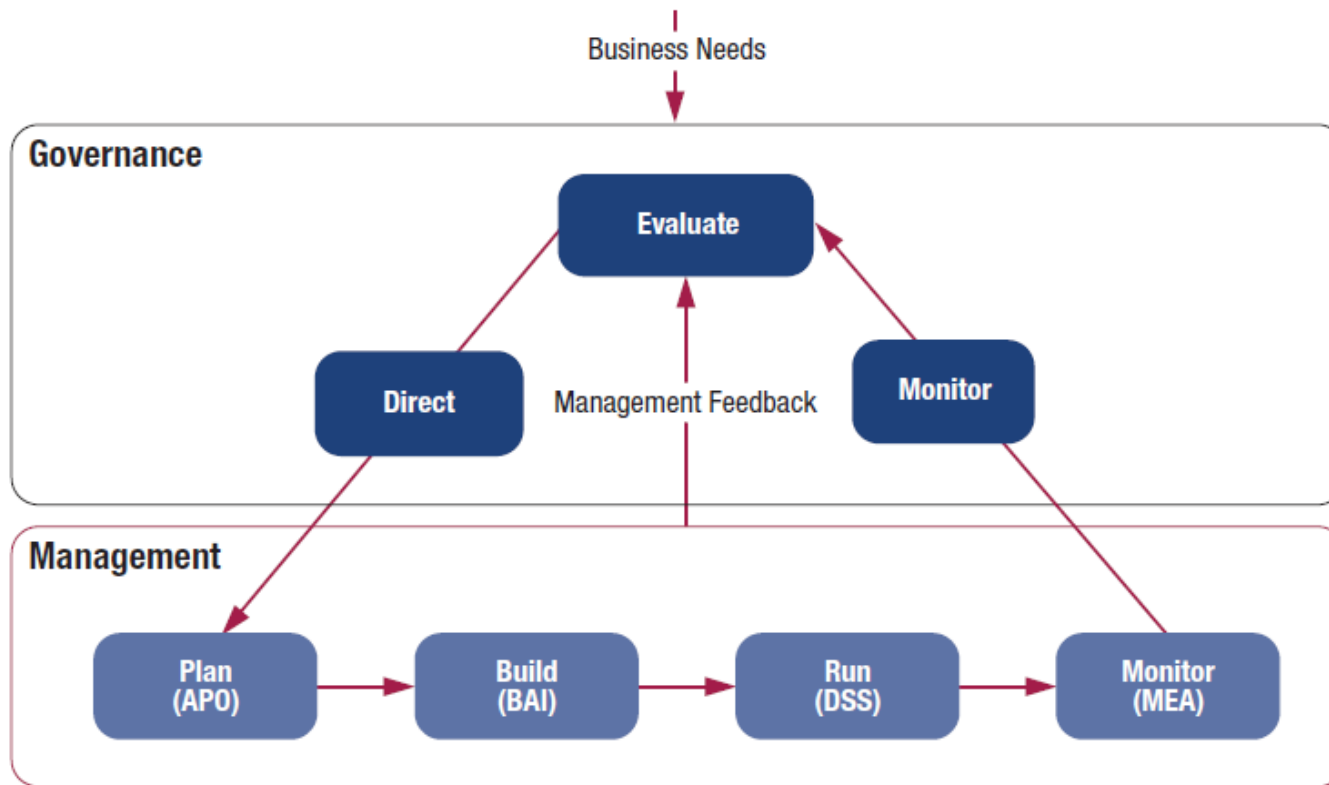
- การได้รับผลประโยชน์
- การจัดการความเสี่ยงอย่างเหมาะสม
- การใช้ทรัพยากรให้เกิดประโยชน์สูงสุด



ต้นทุนการให้บริการลดลง /
กระบวนการทำงานมีประสิทธิภาพ
/ บุคลากรมีทักษะเพิ่มขึ้น

Governance and Management Key Areas

Figure 15—COBIT 5 Governance and Management Key Areas



Process Reference Model

Figure 16—COBIT 5 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

AP001 Manage the IT Management Framework

AP002 Manage Strategy

AP003 Manage Enterprise Architecture

AP004 Manage Innovation

AP005 Manage Portfolio

AP006 Manage Budget and Costs

AP007 Manage Human Resources

AP008 Manage Relationships

AP009 Manage Service Agreements

AP010 Manage Suppliers

AP011 Manage Quality

AP012 Manage Risk

AP013 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

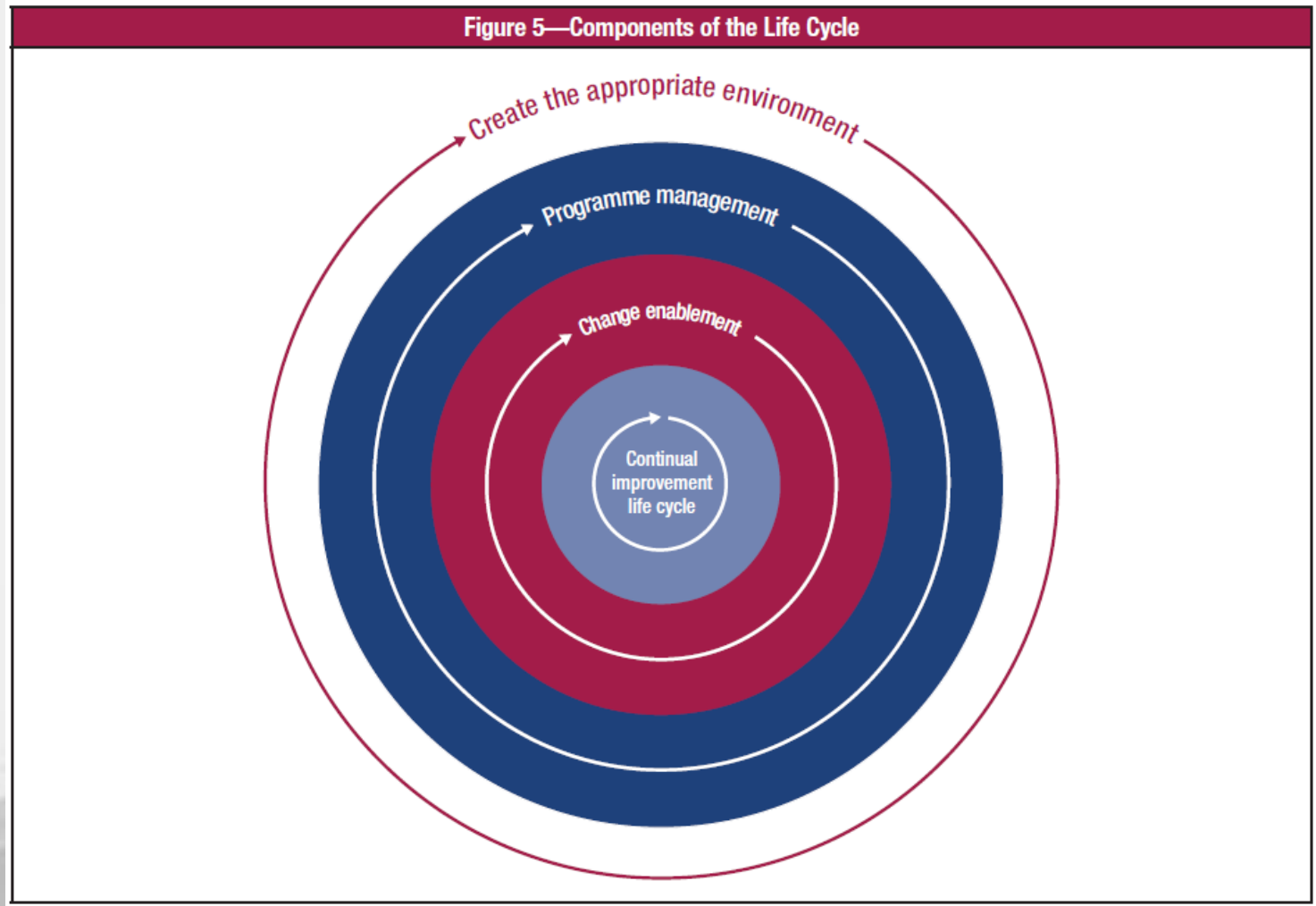
DSS04 Manage Continuity

DSS05 Manage Security Services

DSS06 Manage Business Process Controls

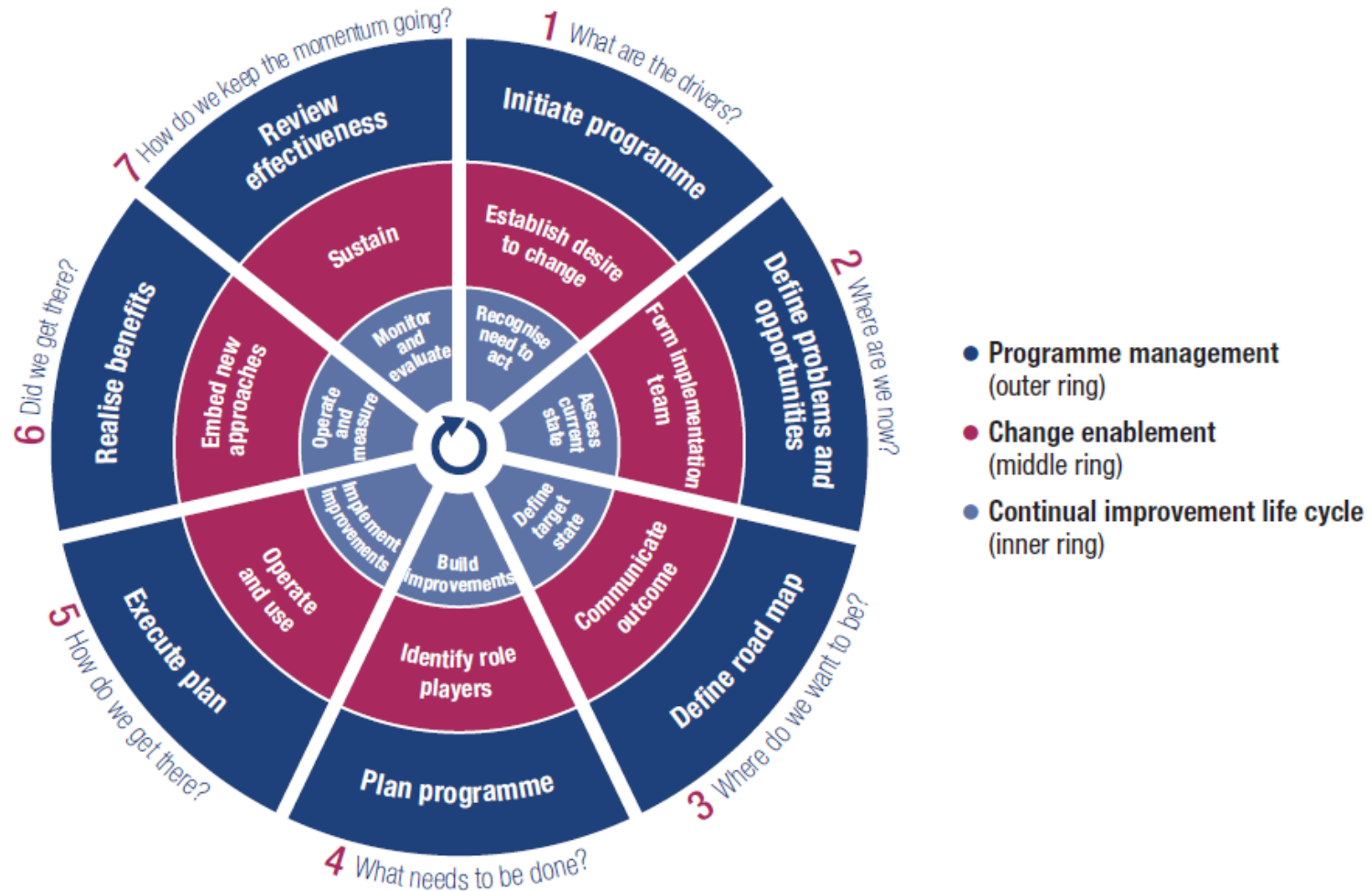
Processes for Management of Enterprise IT

Component of the Life Cycle



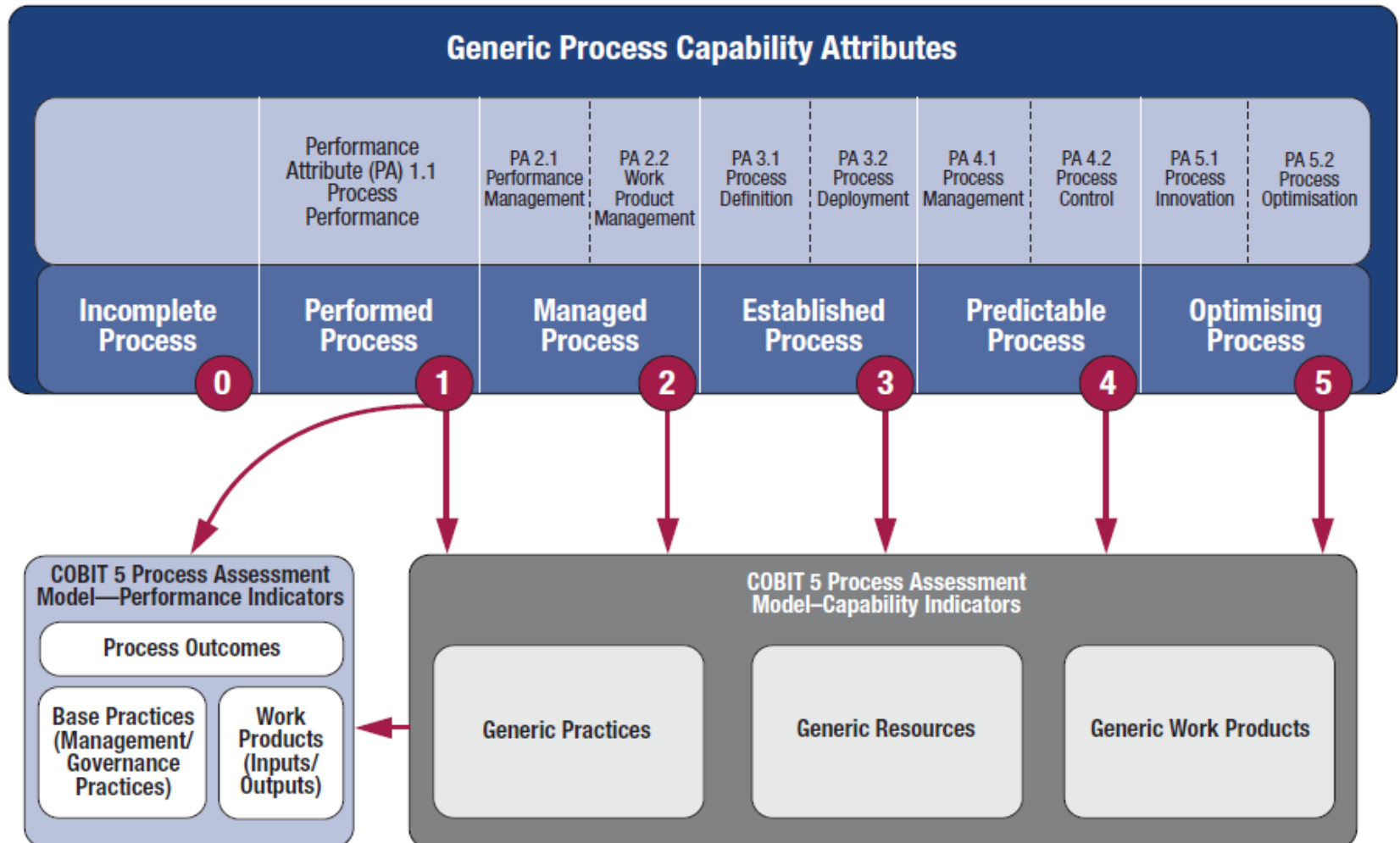
Implementation Guide

Figure 6—Seven Phases of the Implementation Life Cycle



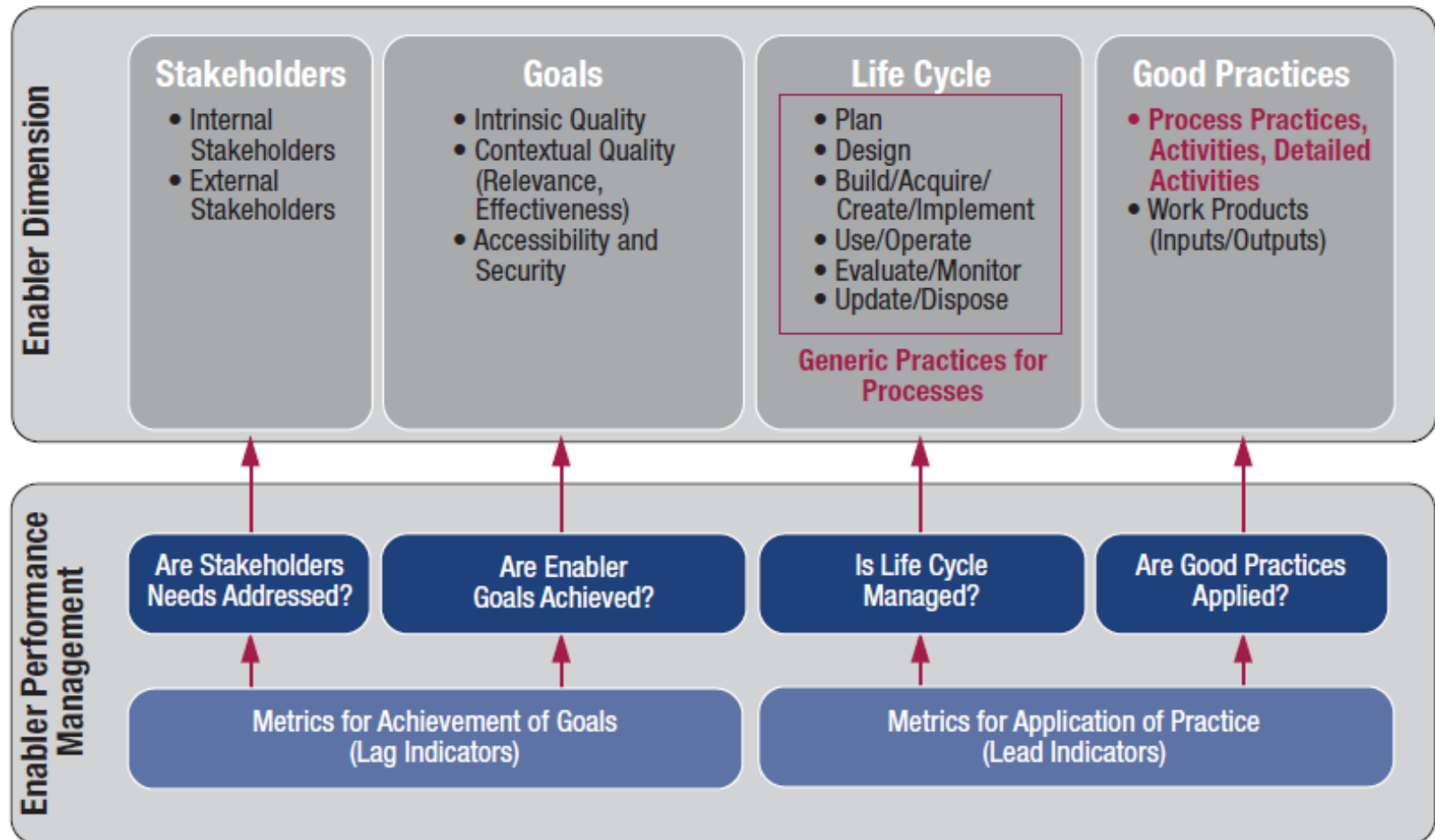
Maturity Model

Figure 19—Summary of the COBIT 5 Process Capability Model



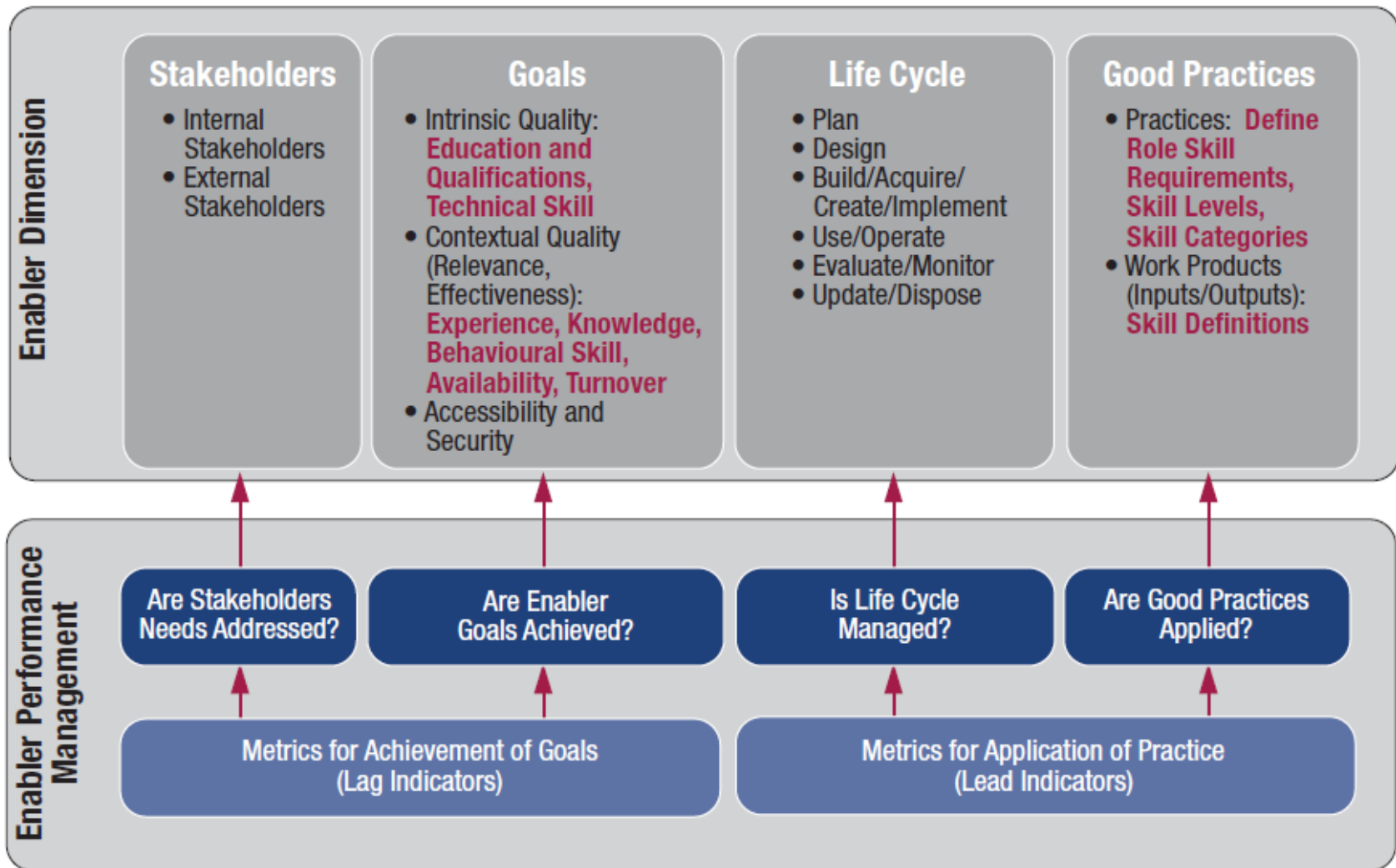
Processes and Measurements

Figure 29—COBIT 5 Enabler: Processes



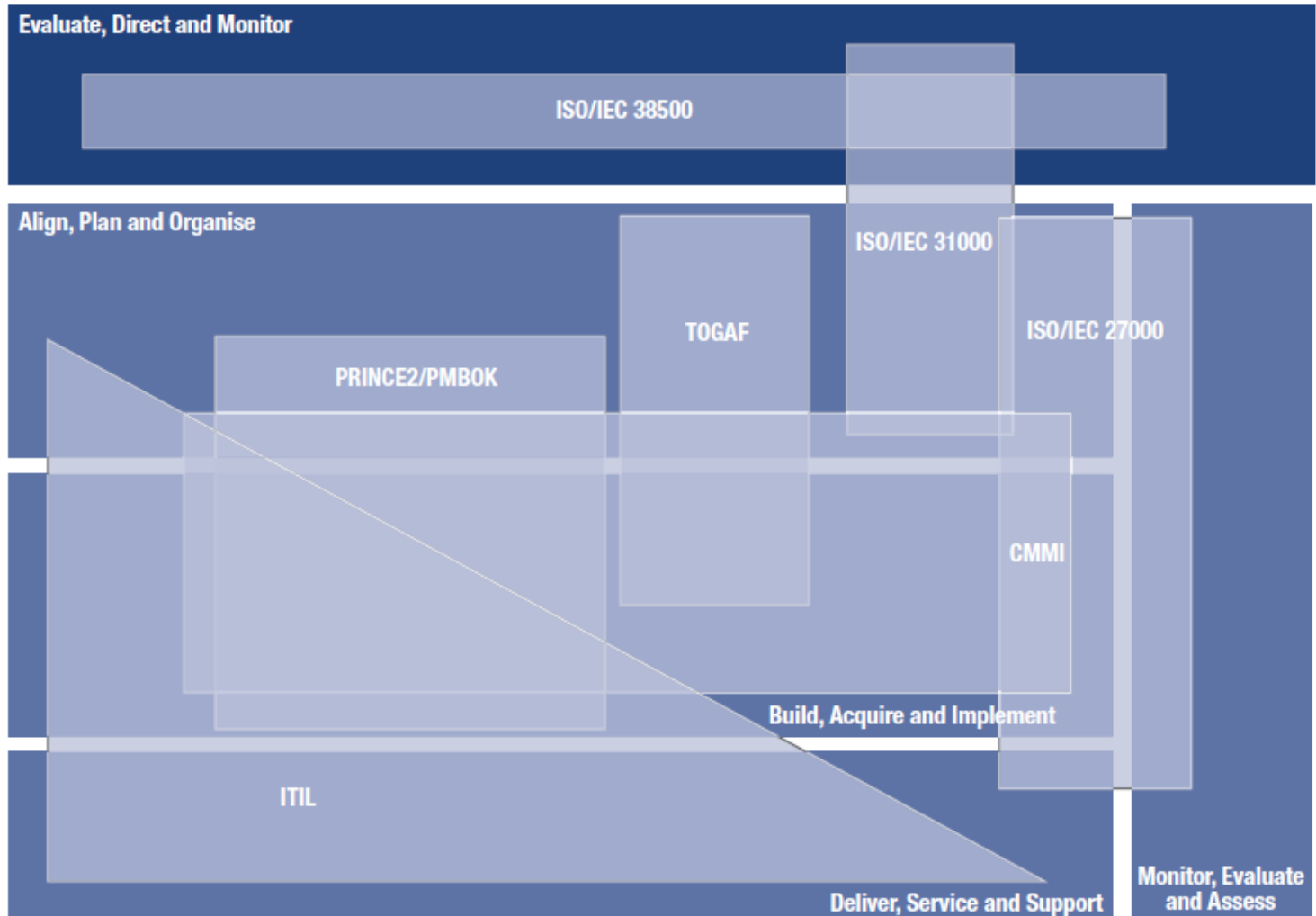
Sample

Figure 38—COBIT 5 Enabler: People, Skills and Competencies



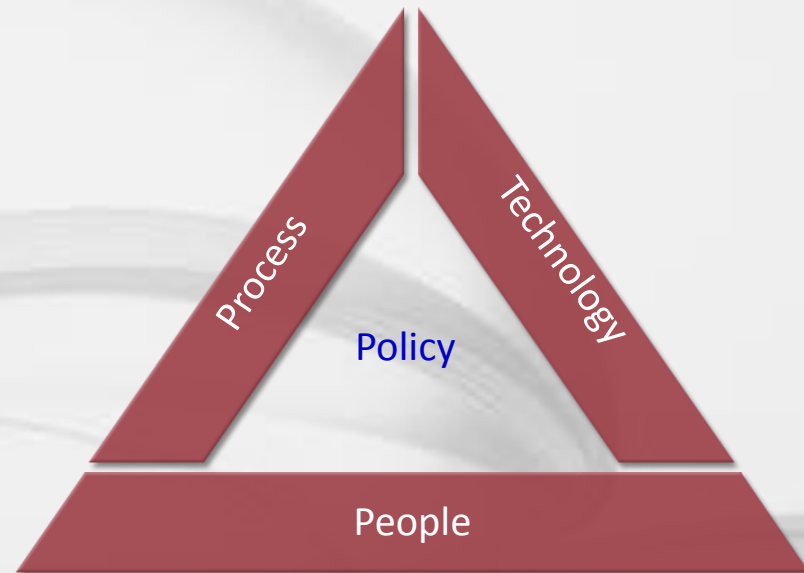
IT Best Practices Alignment

Figure 25—COBIT 5 Coverage of Other Standards and Frameworks



What's ISO / IEC 27001 ?

- A set of control base on the best practices in information Security;
- An international standard covering every aspect of information security:
 - Equipment;
 - Management policies;
 - Human resources;
 - Legal aspects.



What is ?

ISO/IEC 27000 Series

ISO/IEC 27000

vocabulary and definitions
terminology for all of these standards

ISO/IEC 27001

the main Information Security Management
System
requirements standard (specification)

ISO/IEC 27002

currently known as [ISO 17799](#)
this is the Code of Practice

ISO/IEC 27003

implementation guidance

ISO/IEC 27004

will be a new Information Security
Management Metrics and
Measurement standard

ISO/IEC 27005

a new Information Security Risk
Management standard

ISO/IEC 27006

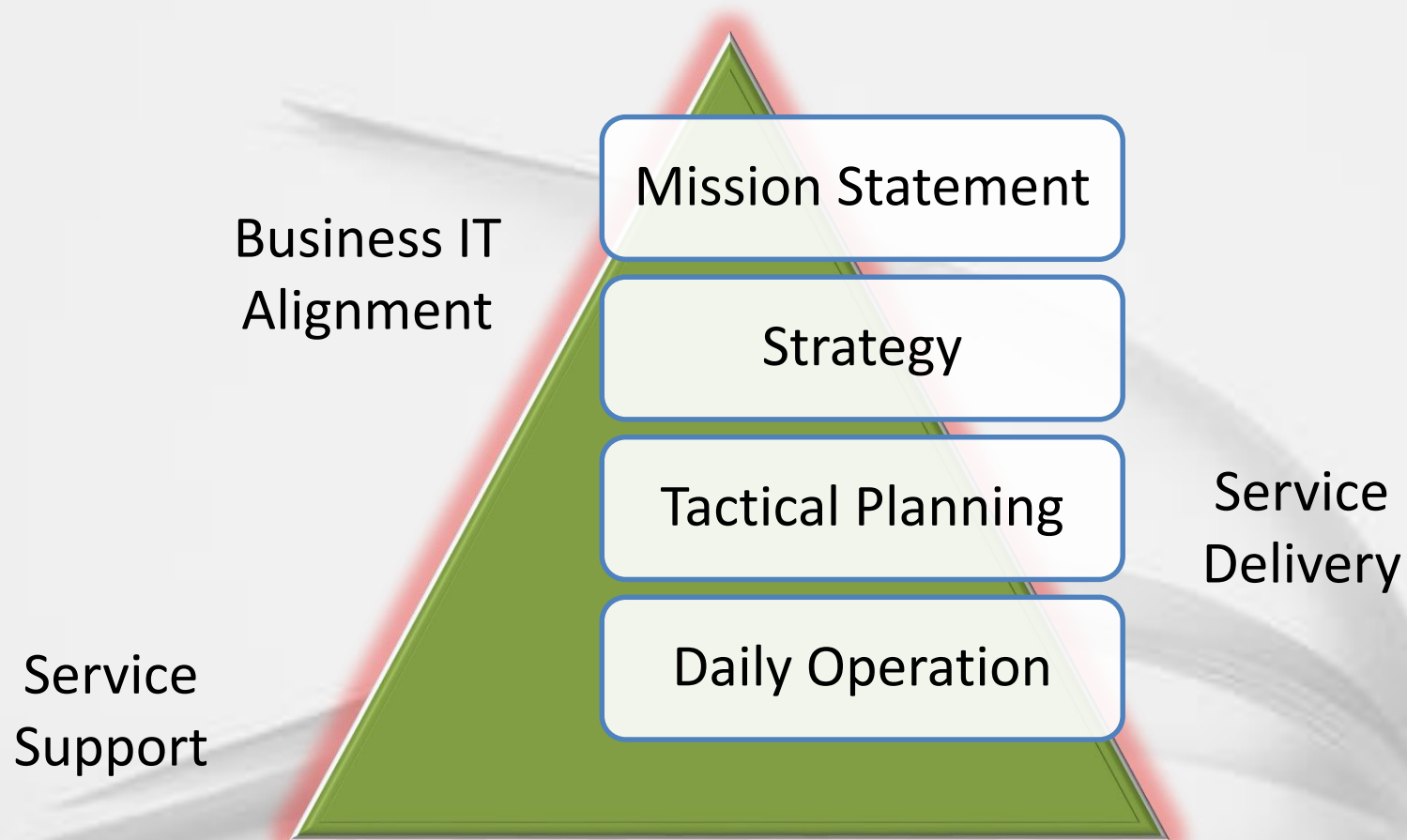
a new standard: "Guidelines for information and
communications technology disaster recovery
services"

What is ITIL? (“eye-till”)*

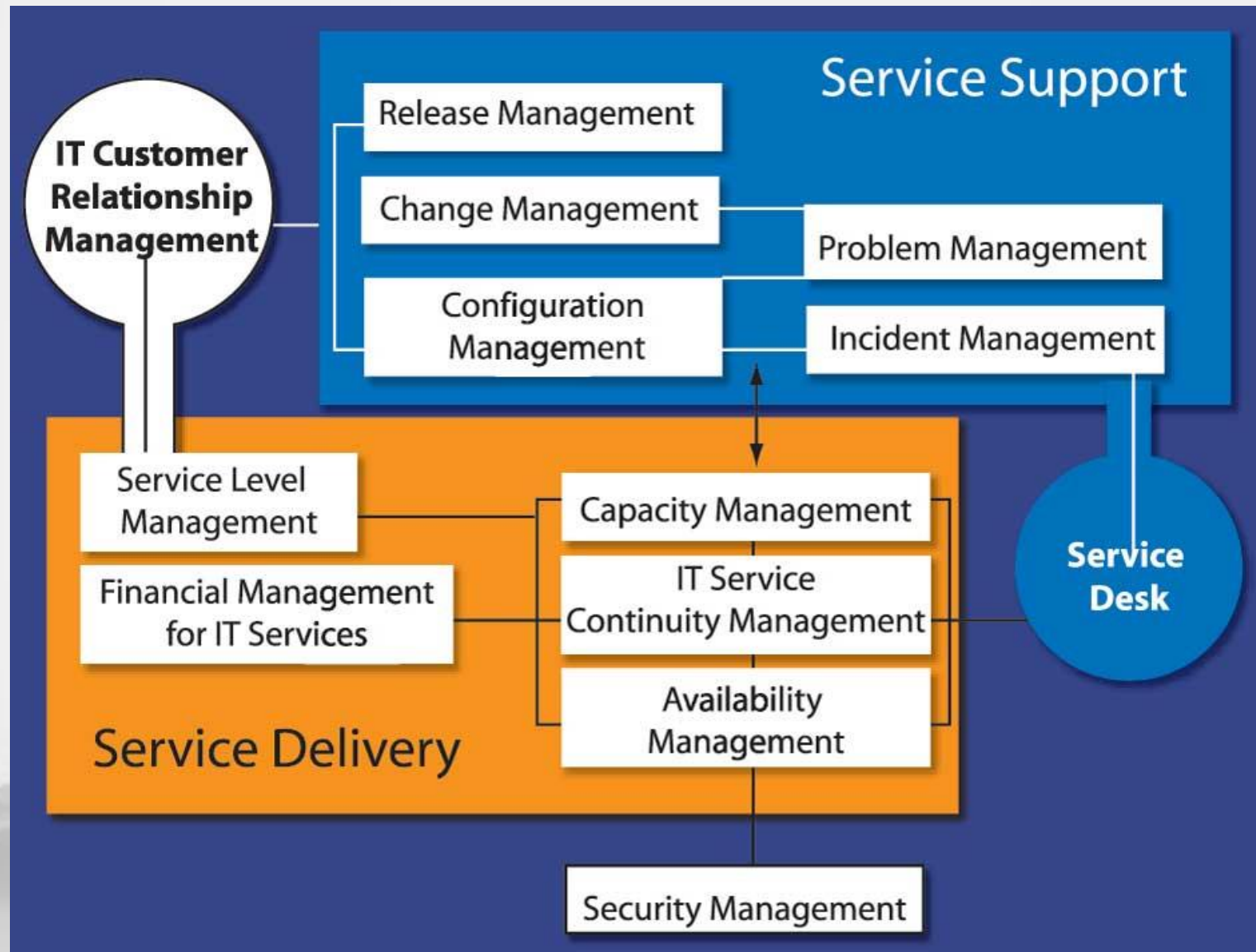
- IT Infrastructure Library
(<http://www.ogc.gov.uk/>)
- Descriptions of IT processes and controls, especially Service Management
- Reporting target is CIO and IT senior management
- Created by British Gov., using set of IT best practices from public and private sectors worldwide

•* *US pronunciation. In the UK, this is pronounced “it-ill”*

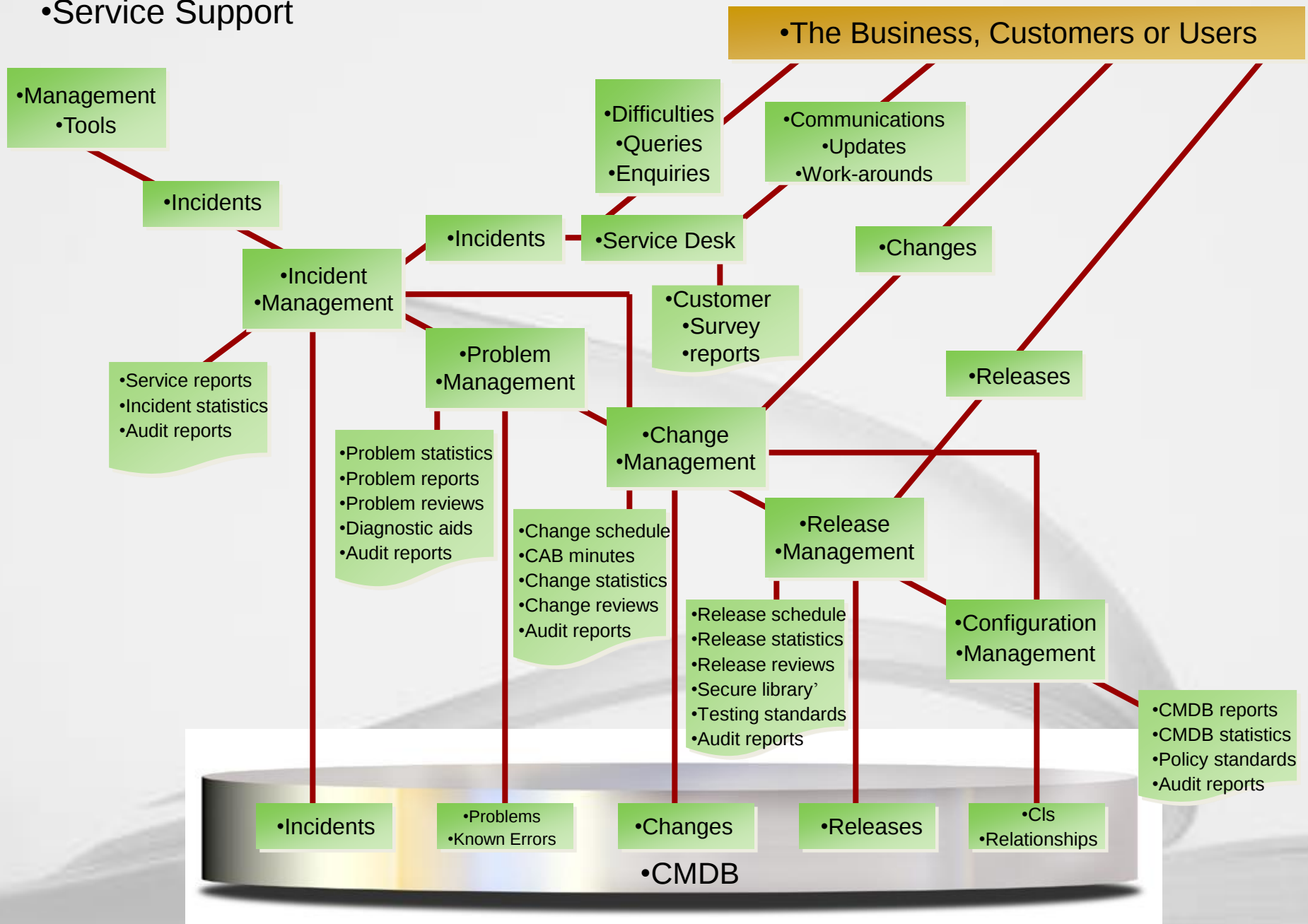
ITIL - IT Infrastructure Library



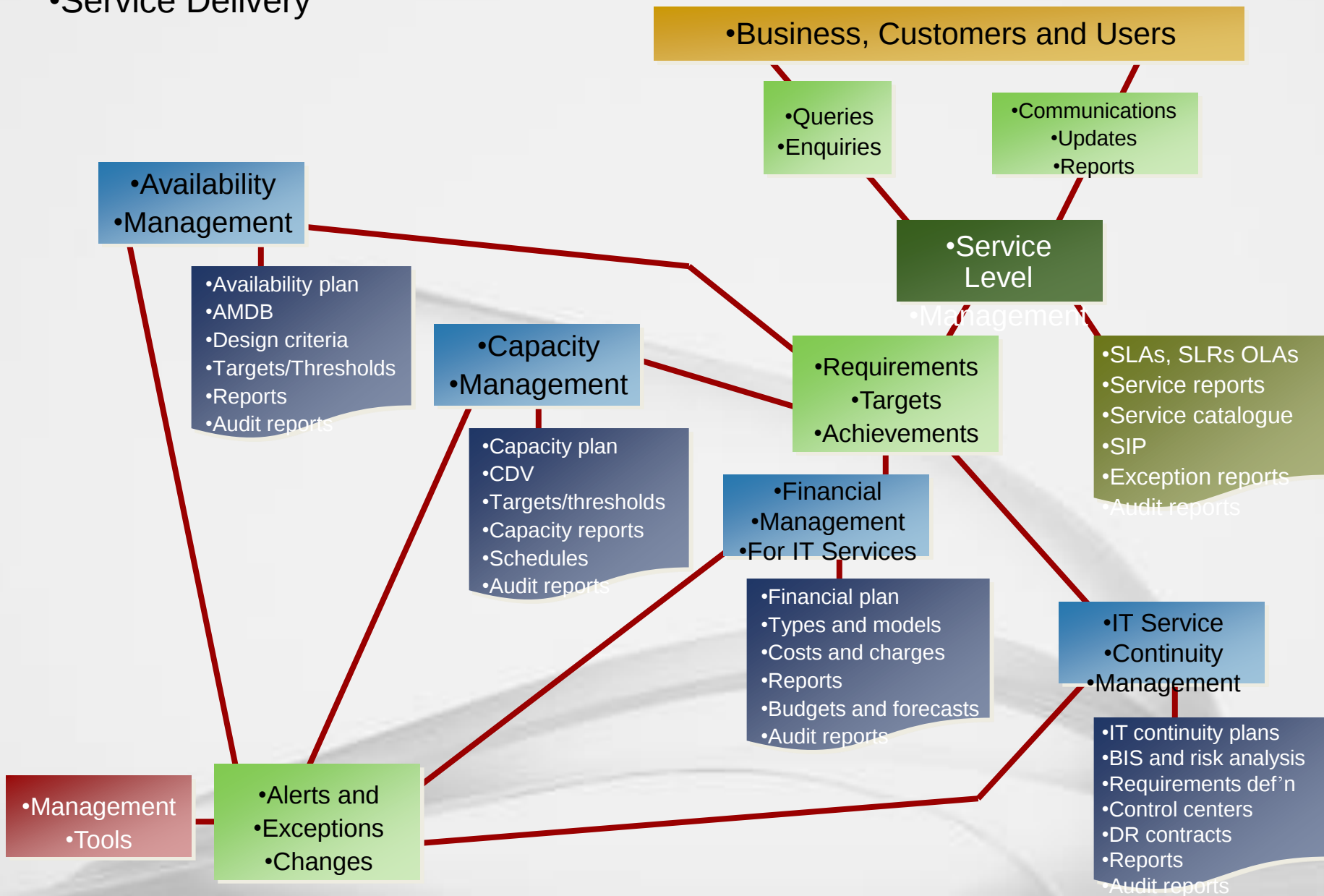
ITIL Service Management Best Practices



•Service Support



•Service Delivery

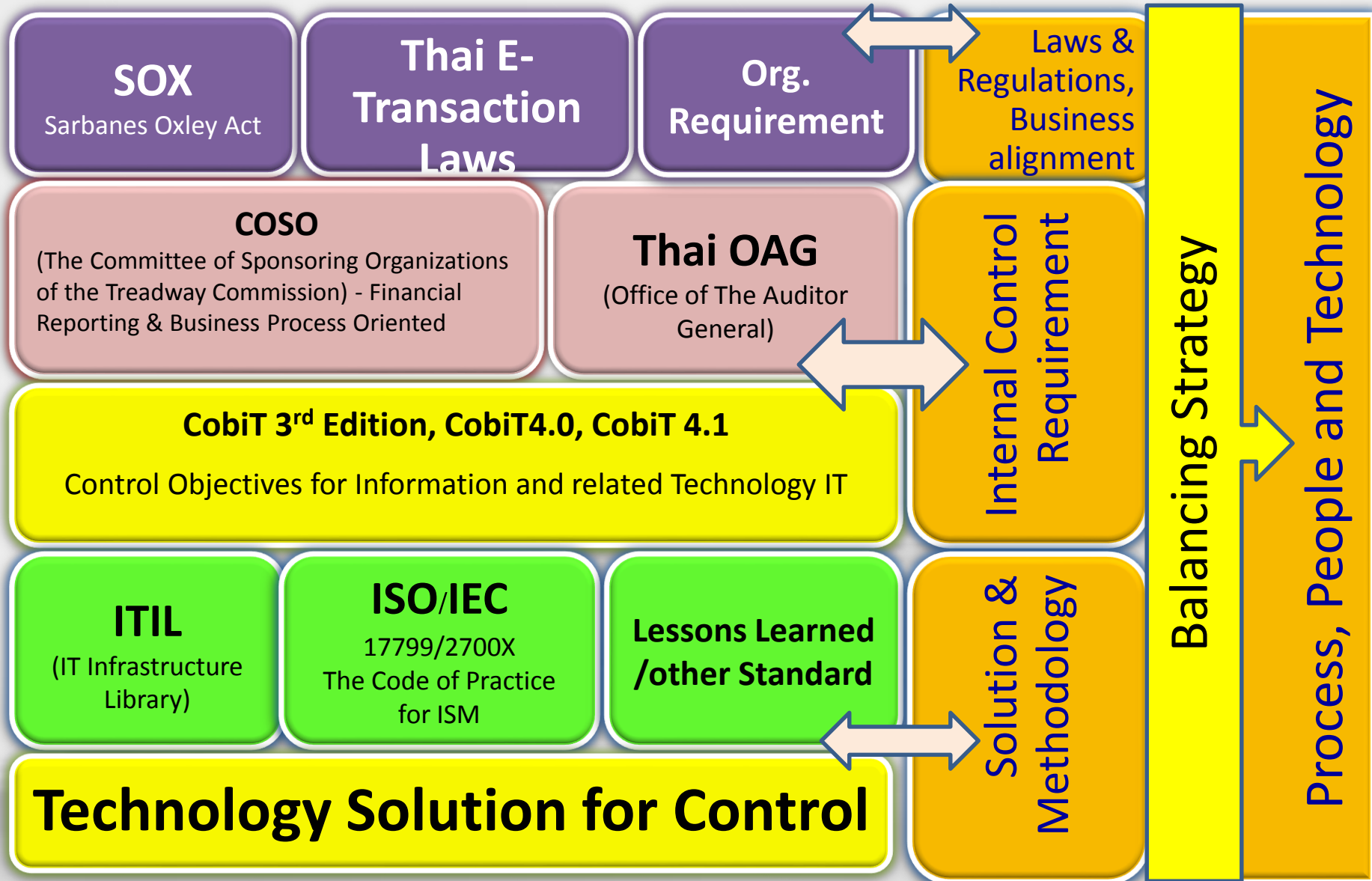


IT Management – Lessons Learned

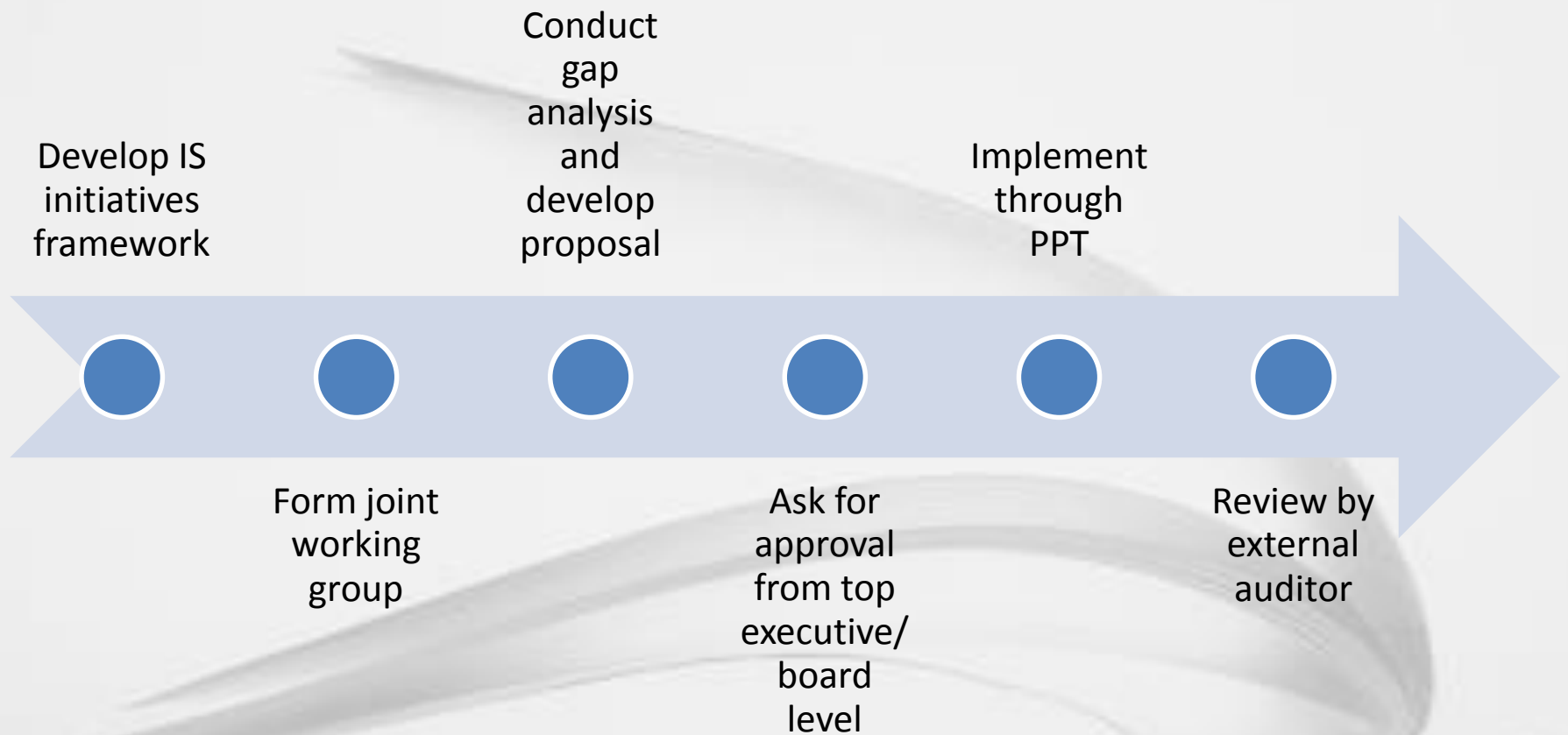
- Initiate SEC GRC Framework
 - Implement IT Governance within SEC
 - Issue Regulations for Securities Companies
- 

GRC Framework

- Displayed in Integrated Approach



Implementation Steps Within SEC



Implementation Steps

Regulating
Securities
Companies

Identify Risk Categories
& Develop RBA

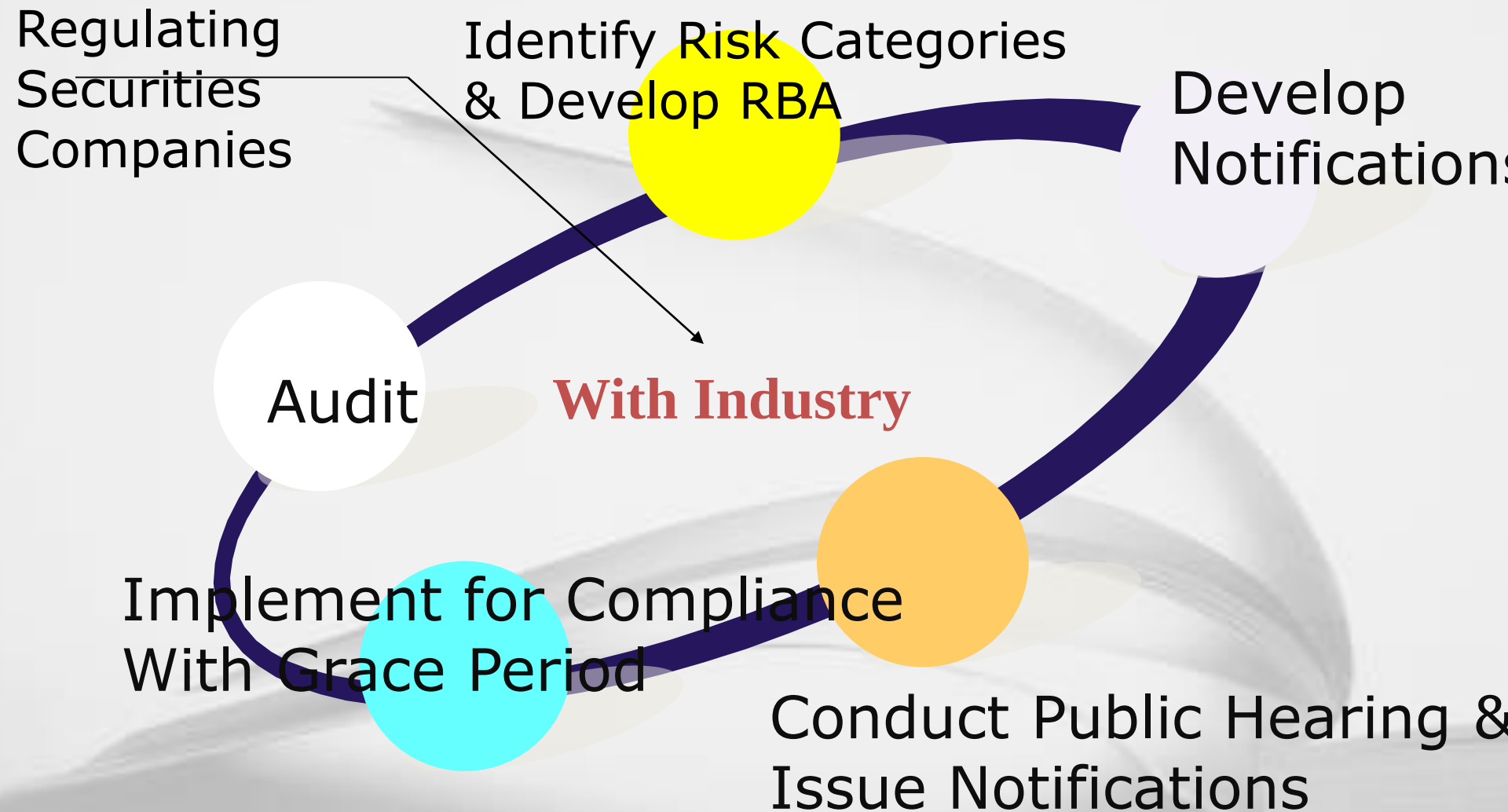
Develop
Notifications

Audit

With Industry

Implement for Compliance
With Grace Period

Conduct Public Hearing &
Issue Notifications



SEC Roles – Securities Companies

Adopt Risk-Based Approach
Identify Securities Companies Risk Categories

Prudential Risk

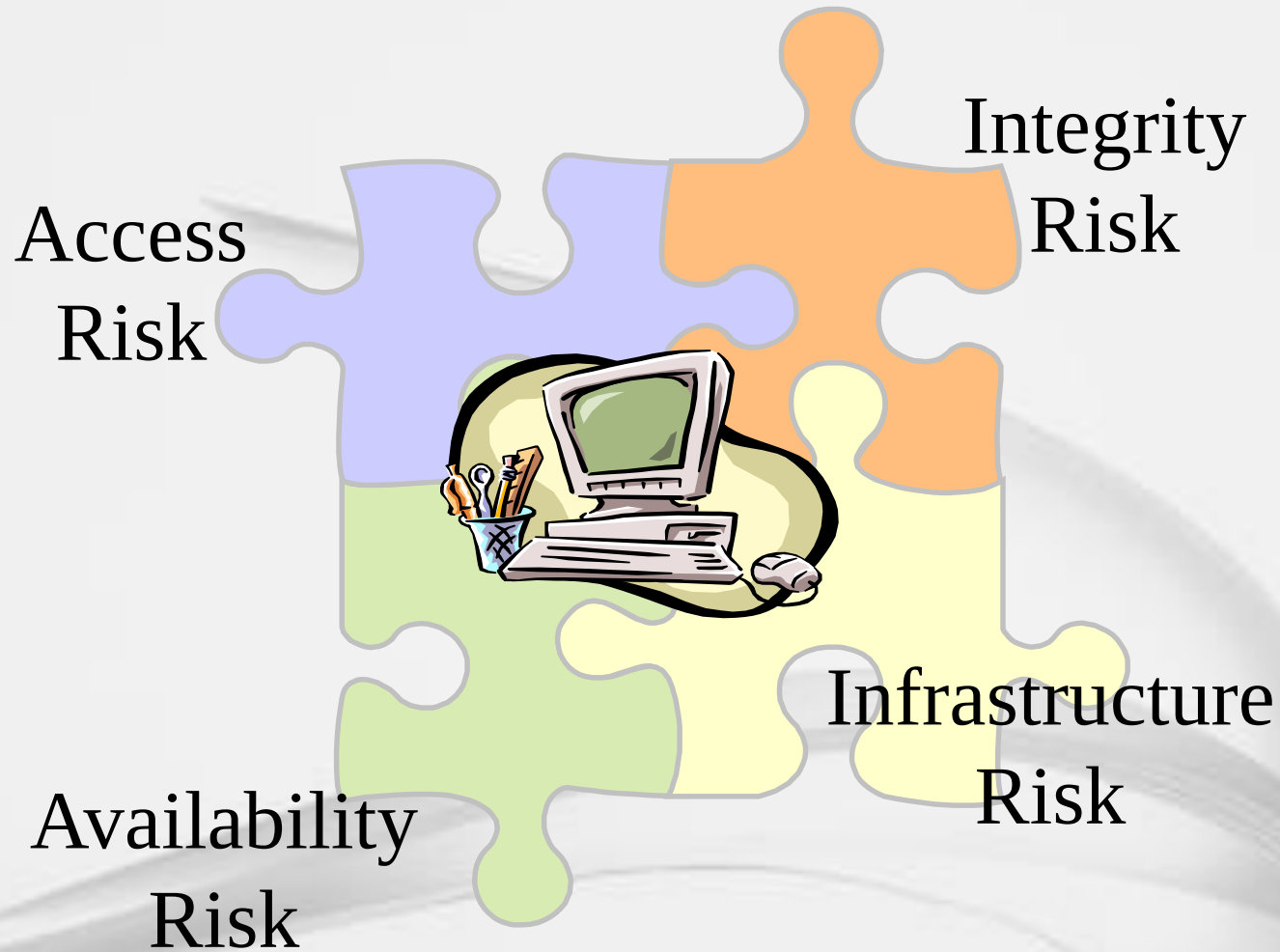
Control Risk

Consumer Relationship Risk

IT Risk

Business Risk

IT Risk Categories



Formats of IT Regulations

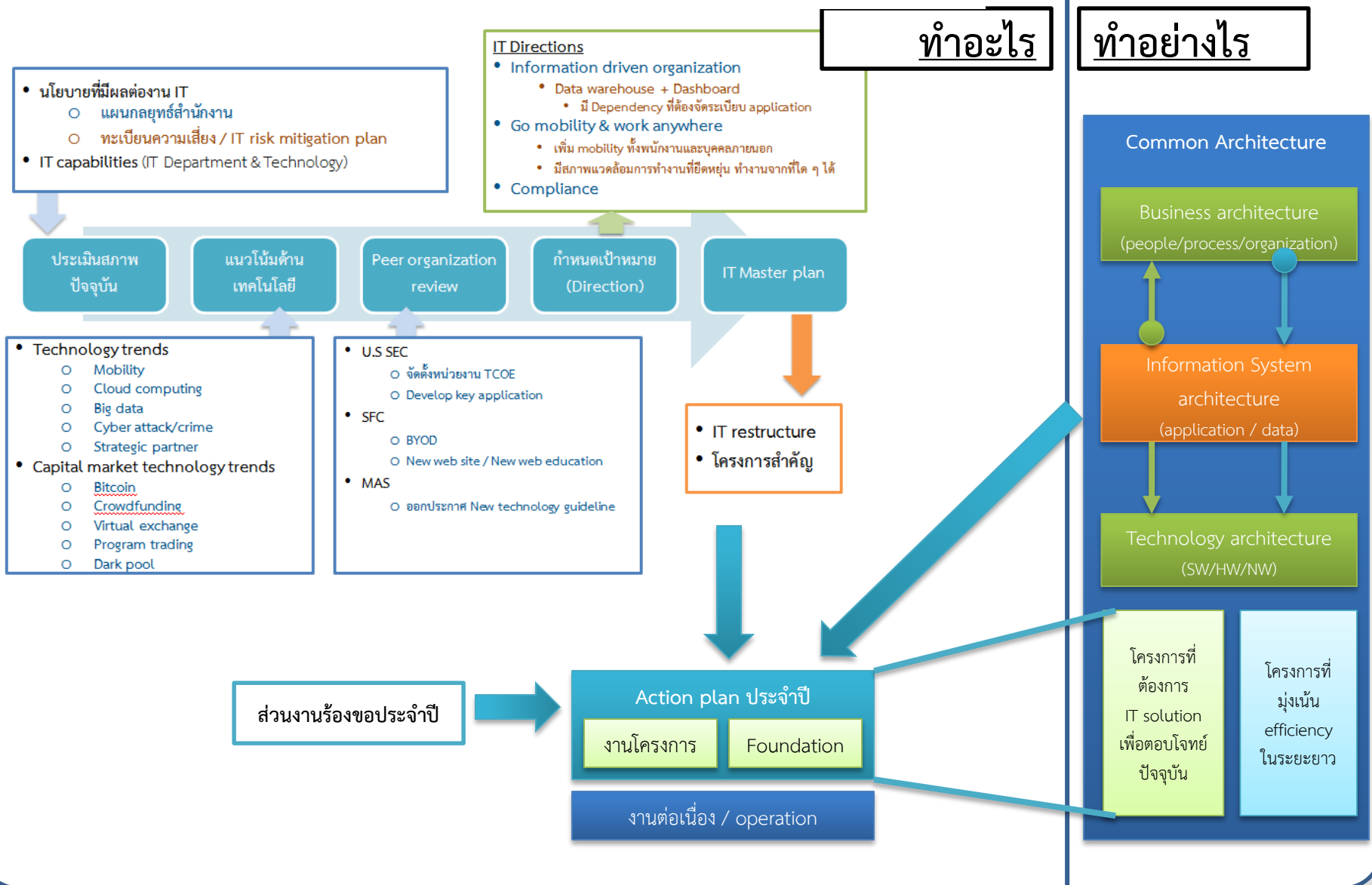
Regulation

ประกาศสำนักงานคณะกรรมการกำกับ
หลักทรัพย์และตลาดหลักทรัพย์
ที่ **สธ./น. 34 /2547** เรื่อง การควบคุม
การปฏิบัติงานและการรักษาความ
ปลอดภัยด้านเทคโนโลยีสารสนเทศของ
บริษัทหลักทรัพย์

Guideline

ประกาศสำนักงานคณะกรรมการกำกับ
หลักทรัพย์และตลาดหลักทรัพย์
ที่ **อธ./น. 5/2547** เรื่อง แนวทางปฏิบัติ
ในการควบคุมการปฏิบัติงานและการ
รักษาความปลอดภัยด้านเทคโนโลยี
สารสนเทศของบริษัทหลักทรัพย์

กรอบการกำหนดแผนงานและการดำเนินการของฝ่ายเทคโนโลยี





ปัจจัยสู่ความสำเร็จ

ปัจจัยสู่ความสำเร็จ จาก Lessons Learned

Top Executives Involvement

Business Partnership, not IT Alone

Facilitating rather than Regulating

Business Incentives, not Legislation

Aiming to Best Practices, not Minimum Requirements

Not Reinventing The Wheel

Processes and People rather than Technology

Alert Mode / Always Paranoid

Employee Disciplines / Mindset / Privacy

Continuous Enforcement / Improvement



Q&A

KUMPOL@SEC DOT OR DOT TH