Software Process & Quality Management

Mel Rosso-Llopart © 2018

CoBit - Control Objectives for Information and Related Technology

Mel Rosso-Llopart
Senior Lecturer, Executive Education Program
Institute for Software Research
Carnegie Mellon University

Software Process & Quality Management

CoBit - Control Objectives for Information and Related Technology

DUY TÂN UNIVERSITY

Truong Dinh Huy
Tel: 0982.132.352
truongdinhhuy@dtu.edu.vn

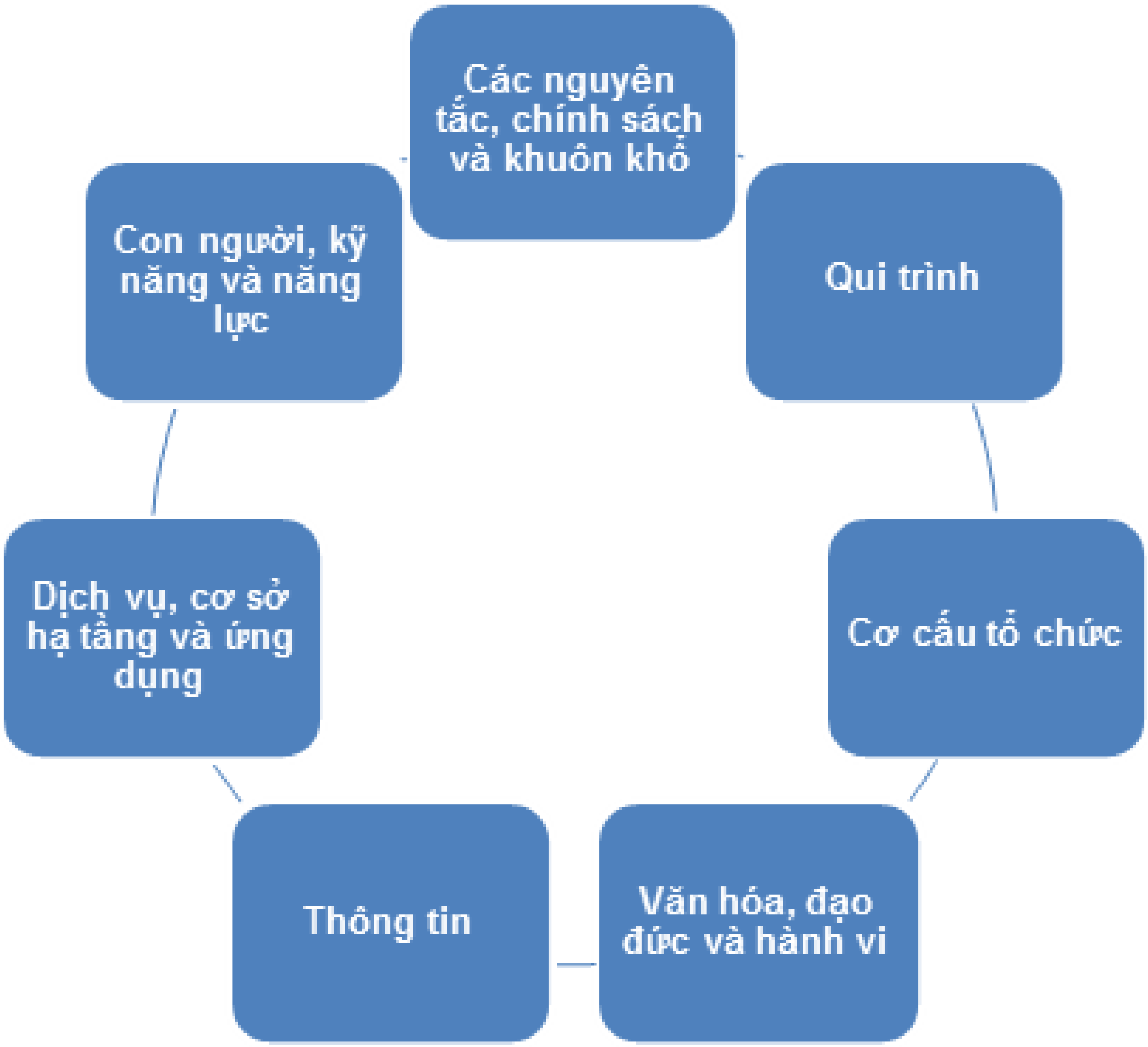
History of CoBit

- 1996 - CoBit was developed by ISACF (Information Systems Audit and Control Foundation)
- 1998 - Founding of the ITGI (IT Governance Institute)
- 1998 - ITGI begins an initiative for better IT Governance, focused around CoBit.
- http://www.isaca.org
  http://www.itgi.org

© 2018 CMU-ISR

CoBiT là một chuẩn quốc tế về quản lý CNTT gồm những khuôn mẫu(framework) về các thực hành tốt nhất về quản lý CNTT do ISACA và ITGI xây dựng năm 1996. CoBiT cung cấp cho các nhà quản lý, những người kiểm tra và những người sử dụng IT một loạt các cách đo lường, dụng cụ đo, các quy trình và các hướng dẫn thực hành tốt nhất để giúp tăng tối đa lợi nhuận thông qua việc sử dụng công nghệ thông tin; giúp quản lý và kiểm soát IT trong tổ chức, doanh nghiệp.

Mục đích của COBIT là "nghiên cứu, phát triển, quảng bá và xúc tiến các mục tiêu của kiểm soát CNTT dành cho các nhà quản lý doanh nghiệp và những người kiểm tra áp dụng vào trong các hoạt động công việc"



Các nguyên tắc, chính sách và khuôn khổ

Qui trình

Cơ cấu tổ chức

Văn hóa, đạo đức và hành vi

Thông tin

Dịch vụ, cơ sở hạ tầng và ứng dụng

Con người, kỹ năng và năng lực

COBIT® được thiết kế với hơn 200 mục tiêu kiểm soát, phục vụ cho 34 quy trình CNTT chính yếu tổ chức theo bốn lĩnh vực quan trọng là:

- **Lập kế hoạch & Tổ chức (*Plan & Organize*),**
- **Xây dựng & Triển Khai (*Acquire & Implement*),**
- **Bàn giao & Hỗ trợ (*Deliver & Support*),**
- **Giám sát & Đánh giá (*Monitor & Evalute*).**

Tất cả những tiêu thức trên được thiết kế để đảm bảo 5 yêu cầu chính của tổ chức, doanh nghiệp đối với CNTT bao gồm:

- **Liên kết chiến lược (Strategic Alignment),**
- **Hiện thực hoá giá trị cam kết (*Value Delivery*),**
- **Quản lý nguồn lực (*Resource Management*),**
- **Quản lý rủi ro (*Risk Management*) và**
- **Quản lý thực hiện (*Performance Measurement*).**

What is COBIT?

- COBIT (Control Objectives for Information and Related Technology) is globally accepted as being the most comprehensive work for IT governance, organization, as well as IT process and risk management.
- COBIT provides good practices for the management of IT processes in a manageable and logical structure, meeting the multiple needs of enterprise management by **bridging the gaps between business risks, technical issues, control needs and performance measurement requirements.**

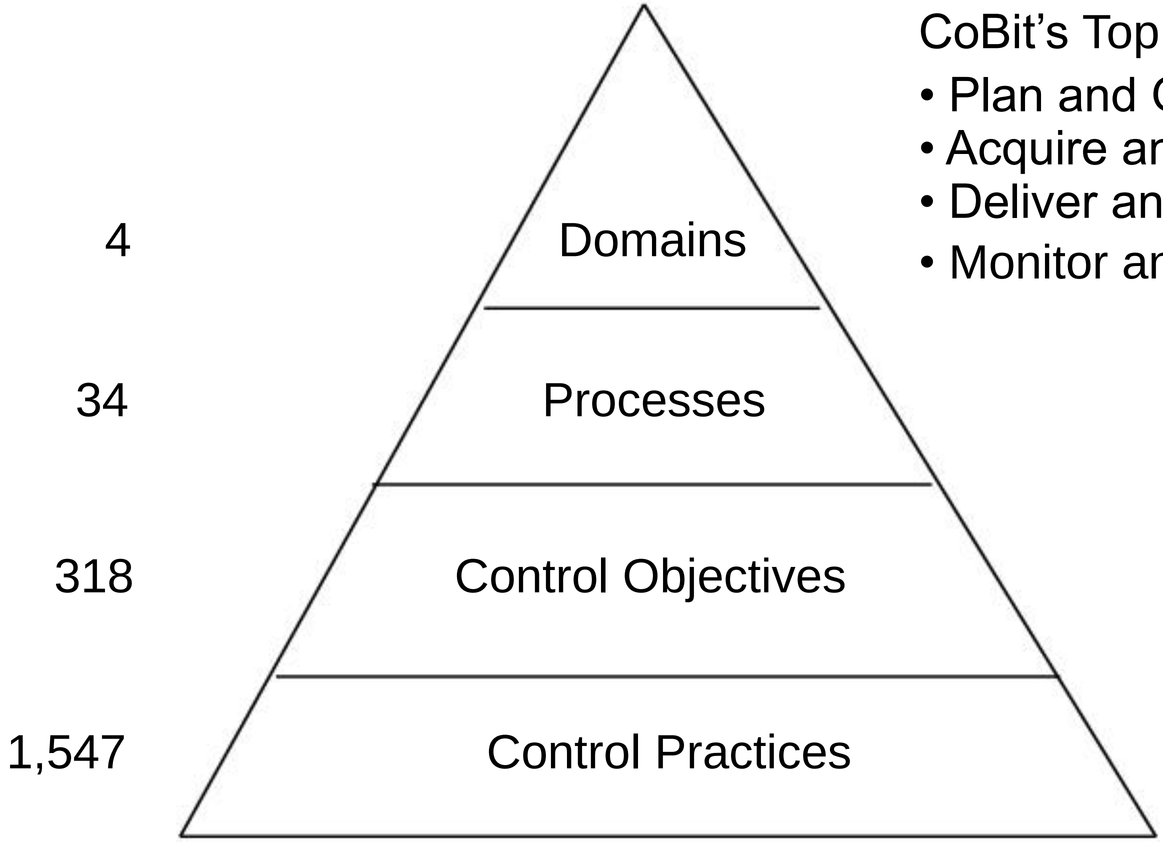
- The COBIT mission is to research, develop, publicize and promote an authoritative, up-to-date, international set of generally accepted information technology control objectives for day-to-day use by business managers and auditors.

More History - Deming Cycle

- Deming Cycle - continuous improvement process

- CoBit uses - Plan-Do-Check-Act Cycle
- CoBit reflects
  - Information need - Corporate view
  - Information technology - IT Governance

CoBit's Hierarchy



CoBit's Top Down Approach

- Plan and Organize (PO)
- Acquire and Implement (AI)
- Deliver and Support (DS)
- Monitor and Evaluation (M)

Point of View for CoBit

- Starts from the premise that IT needs to deliver the information that the enterprise needs to achieve its objectives.
- Promotes process focus and process ownership
- Divides IT into 34 processes belonging to four domains and provides a high level control objective for each
- Looks at fiduciary, quality and security needs of enterprises, providing seven information criteria that can be used to generically define what the business requires from IT
- Is supported by a set of 318 detailed control objectives

1. Planning
2. Acquiring & Implementing
3. Delivery & Support
4. Monitoring

1. Effectiveness
2. Efficiency
3. Availability
4. Integrity
5. Confidentiality
6. Reliability
7. Compliance

CoBit Definitions - 7 Information Criteria

EFFECTIVENESS

Deals with information being relevant and pertinent to the business process as well as being delivered in a timely, correct, consistent and usable manner

EFFICIENCY

Concerns the provision of the information through the optimal use of resources

CONFIDENTIALITY

Concerns the protection of sensitive information from unauthorized disclosure

INTEGRITY

Relates to the accuracy and completeness of information as well as to its validity in accordance with business values and expectations

AVAILABILITY

Relates to the information being available when required by the business process now and in the future

COMPLIANCE

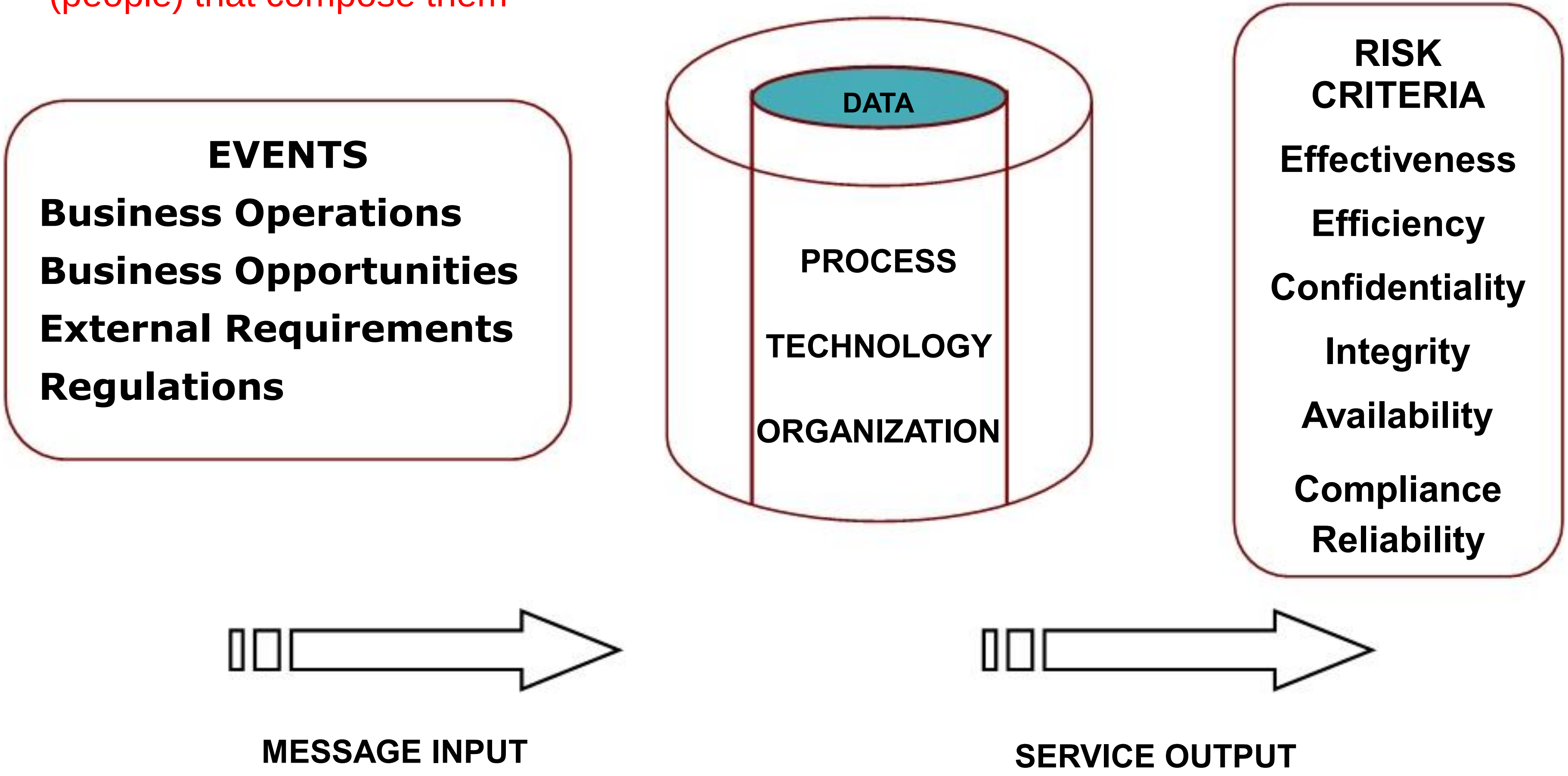
Deals with complying with laws, regulations and contractual arrangements.

RELIABILITY OF INFORMATION

Relates to the provision of appropriate information for the workforce of the organization

General Information Risk Criteria

Events can be defined in terms of the processes, technology (systems) and organization (people) that compose them



EVENTS

Business Operations

Business Opportunities

External Requirements

Regulations

DATA

PROCESS

TECHNOLOGY

ORGANIZATION

RISK CRITERIA

Effectiveness

Efficiency

Confidentiality

Integrity

Availability

Compliance

Reliability

MESSAGE INPUT

SERVICE OUTPUT

The 4 COBIT Domains

1. Planning & Organization
2. Acquisition & Implementation
3. Delivery & Support
4. Monitoring & Evaluation

Planning and Organization

- This domain covers strategy and tactics, and concerns the identification of the way IT can best contribute to the achievement of the business objectives.
- Furthermore, the realization of the strategic vision needs to be planned, communicated and managed for different perspectives.
- Finally, a proper organization as well as technological infrastructure must be put in place.

Acquisition and Implementation

- To realize the IT strategy, IT solutions need to be identified, developed or acquired, as well as implemented and integrated into the business process.
- In addition, changes in and maintenance of existing systems are covered by this domain to make sure that the life cycle is continued for these systems.

Delivery and Support

- This domain is concerned with the actual delivery of required services, which range from traditional operations over security and continuity aspects to training.
- In order to deliver services, the necessary support processes must be set up.
- This domain includes the actual processing of data by application systems, often classified under application controls.

Monitoring & Evaluation

- All IT processes need to be regularly assessed over time for their quality and compliance with control requirements.
- This domain thus addresses management's oversight of the organization's control process and independent assurance provided by internal and external audit or obtained from alternative sources.
- The assessment if the values are as expected and meet with organizational expectations.

IT Governance is the Key Issue

- Enterprises are sacrificing money, productivity and competitive advantage by not implementing effective IT governance

- Executives need a better way to:
  - Direct IT for optimal advantage
  - Measure the value provided by IT
  - Manage IT-related risks

COBIT® is a Road Map to Good IT Governance

- Accepted globally as a set of tools that ens effectively

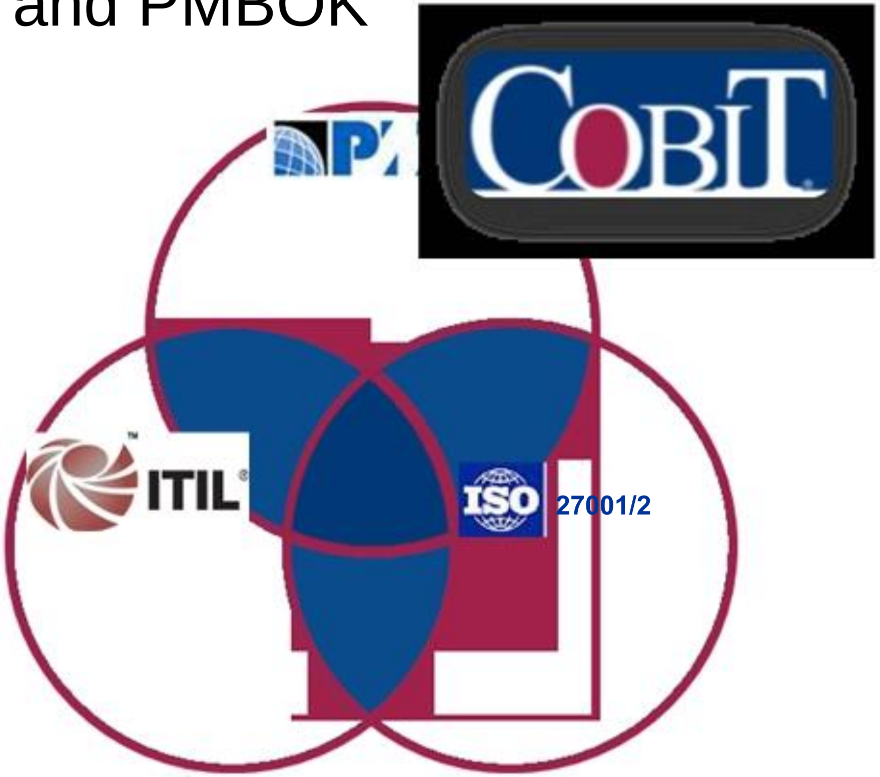
- Functions as an overarching framework
- Provides common language to communicate goals, objectives and expected results to all stakeholders
- Based on, and integrates, industry standards and good practices in:

  - Strategic alignment of IT with business goals
  - Value delivery of services and new projects -
  Risk management

  - Resource management -
  Performance measurement

COBIT® Harmonises with other Standards

- COBIT is often used at the highest level of IT governance
- It harmonizes practices and standards such as ITIL, ISO 27001 and 27002, and PMBOK
  - Improves their alignment to business needs
  - Covers full spectrum of IT-related activities

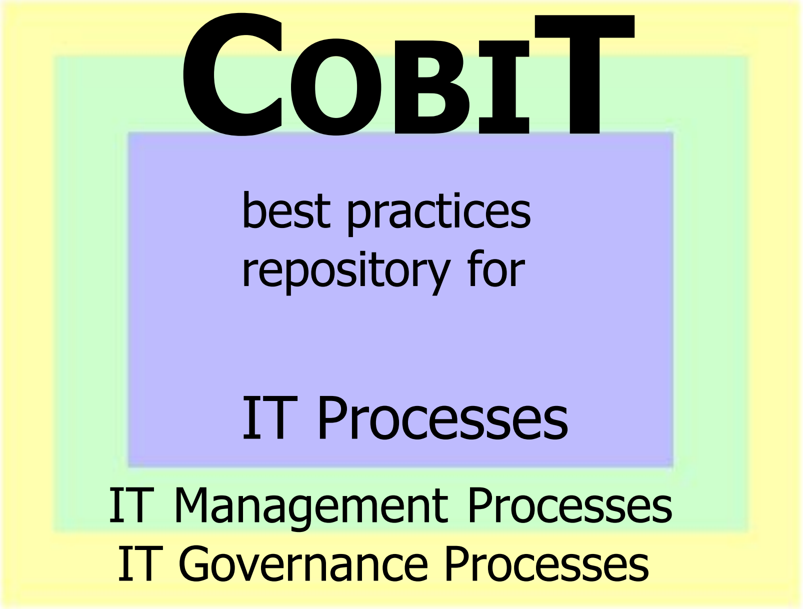


 2009 ISACA All Rights reserved. 17

Why and How is COBIT Used?

COBIT as a response to the needs

- Incorporates major international standards
- Has become the *de facto* standard for overall control over IT
- Starts from business requirements
- Is process-oriented



COBIT

best practices repository for

IT Processes

IT Management Processes

IT Governance Processes

COBIT Framework

Criteria

- Effectiveness
- Efficiency
- Confidenciality
- Integrity
- Availability
- Compliance
- Reliability

PO1 Define a strategic IT plan
PO2 Define the information architecture
PO3 Determine the technological direction
PO4 Define the IT organisation and relationships
PO5 Manage the IT investment
PO6 Communicate management aims and direction
PO7 Manage human resources
PO8 Ensure compliance with external requirements
PO9 Assess risks
PO10 Manage projects
PO11 Manage quality

IT RESOURCES

- Data
- Applicatio
- Technology
- Facilities
- People

M1 Monitor the process
M2 Assess internal control adequacy
M3 Obtain independent assurance
M4 Provide for independent audit

PLAN AND ORGANISE

MONITOR AND EVALUATE

ACQUIRE AND IMPLEMENT

DS1 Define service levels DS2
Manage third-party services DS3
Manage peformance and capac DS4
Ensure continuous service
DS5 Ensure systems security
DS6 Identify and attribute costs
DS7 Educate and train users
DS8 Assist and advise IT customers
DS9 Manage the configuration
DS10 Manage problems and incidents
DS11 Manage data
DS12 Manage facilities
DS13 Manage operations

DELIVER AND SUPPORT

AI1 Identify automated solutions
AI2 Acquire and mantain application software
AI3 Acquire and maintain technology infrastructure
AI4 Develop and maintain IT procedures
AI5 Install and accredit systems
AI6 Manage changes

Basic CoBit Documentation Support

Executive Summary	There is a method…
Framework	The method is…
Control Objectives	Minimum controls are…
Audit Guidelines	Here is how you audit…
Implementation Toolset	Here is how you implement…
Management Guidelines	Here is how you measure…

References

http://ecci.com.vn/tu-van/dich-vu/trien-khai-cobit

http://quantri-cntt.blogspot.com/2013/06/gioi-thieu-ve-cobit.html

http://www.isaca.org/COBIT/Documents/Recognition-table.pdf

http://www.isaca.org/Knowledge-Center/cobit/Pages/COBIT-Case-Studies.aspx

http://www.isaca.org/Knowledge-Center/COBIT/Pages/Overview.aspx

Homework
Prepare - Case study 2 (FibreNet Project)