

# CobiT Fundamentals

**Nejat Aksoy**

**Manager**

**Ernst & Young US**

# CobiT Fundamentals

**SF ISACA Fall Conference**

**[Nejat.aksoy@ey.com](mailto:Nejat.aksoy@ey.com)**

**+1 (408) 947 4953**

**This presentation focuses on COBIT, a best practice for IT Governance. The session will start with an overview of CobiT, will continue with more details (critical success factors, control objectives and key goal & performance indicators) on CobiT processes, with a focus on the specific demands of integrity, confidentiality, availability and reliability. The presentation will also include the future of CobiT and will end with implementation guidelines and some examples concerning utilization of CobiT.**



*September 26<sup>th</sup>, 2005*

Presented by: **NEJAT AKSOY**

# CobiT Fundamentals

## Agenda

- CobiT : An IT Control Framework
- CobiTIV Strategy
- Five Major Projects
  - IT Control Practices
  - Maturity Benchmarking
  - Implementation Guide
  - CobiT *Online*
  - CobiT *lite*
- CobiT Examples

# CobiT : An IT control framework

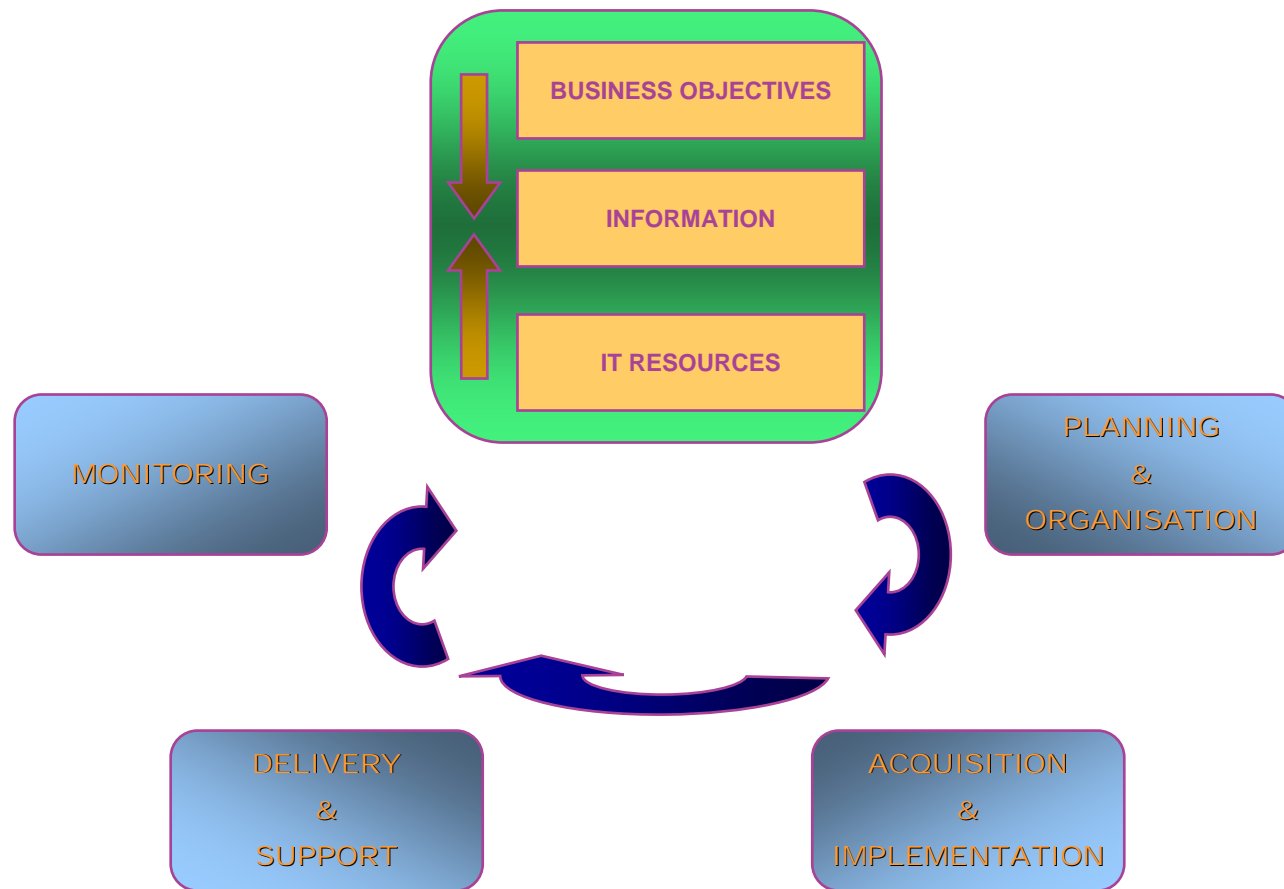
- ◆ Starts from the premise that IT needs to deliver the information that the enterprise needs to achieve its objectives.
- ◆ Promotes process focus and process ownership
- ◆ Divides IT into 34 processes belonging to four domains and provides a high level control objective for each
- ◆ Looks at fiduciary, 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 over 300 detailed control objectives

- ◆ Planning
- ◆ Acquiring & Implementing
- ◆ Delivery & Support
- ◆ Monitoring

- ◆ Effectiveness
- ◆ Efficiency
- ◆ Availability,
- ◆ Integrity
- ◆ Confidentiality
- ◆ Reliability
- ◆ Compliance.

# CobiT Framework IT Domains

IT PROCESSES ARE DEFINED WITHIN THE FOUR COBIT FRAMEWORK DOMAINS



# CobiT IT Domain Processes

PLANNING  
&  
ORGANISATION

## PLANNING & ORGANISATION

1. **Define a strategic IT plan**
2. **Define the information architecture**
3. **Determine the technological direction**
4. **Define the IT organisation and relationships**
5. **Manage the investment**
6. **Communicate management aims and directions**
7. **Manage human resources**
8. **Ensure compliance with external requirements**
9. **Assess risks**
10. **Manage project**
11. **Manage quality**

# CobiT IT Domain Processes

ACQUISITION  
&  
IMPLEMENTATION

## ACQUISITION & IMPLEMENTATION

- 1 Identify solutions
- 2 Acquire and maintain application software
- 3 Acquire and maintain technology architecture
- 4 Develop and maintain IT procedures
- 5 Install and accredit systems
- 6 Manage changes

# CobiT IT Domain Processes

DELIVERY  
&  
SUPPORT

## DELIVERY & SUPPORT

- 1 **Define Service Levels**
- 2 **Manage third-party services**
- 3 **Manage performance and capacity**
- 4 **Ensure continuous service**
- 5 **Ensure system security**
- 6 **Identify and attribute costs**
- 7 **Educate and train users**
- 8 **Assist and advise IT customers**
- 9 **Manage the configuration**
- 10 **Manage problems and incidents**
- 11 **Manage data**
- 12 **Manage facilities**
- 13 **Manage operations**

# CobiT IT Domain Processes

MONITORING

## MONITORING

- 1 **Monitor the processes**
- 2 **Assess the internal control adequacy**
- 3 **Obtain independent assurance**
- 4 **Provide for independent audit**

# **CobiT Control Objectives (even more detail!)**

## **DS5 ENSURE SYSTEMS SECURITY**

**5.1 Manage Security Measures**

**5.2 Identification, Authentication and Access**

**5.3 Security of Online Access to Data**

**5.4 User Account Management**

**5.5 Management Review of User Accounts**

**5.6 User Control of User Accounts**

**5.7 Security Surveillance**

**5.8 Data Classification**

**5.9 Central Identification and Access Rights**

**5.10 Violation and Security Activity Reports**

**5.11 Incident Handling**

**5.12 Re-Accreditation**

**5.13 Counterparty Trust**

**5.14 Transaction Authorisation**

**5.15 Non-Repudiation**

**5.16 Trusted Path**



*September 26<sup>th</sup>, 2005*

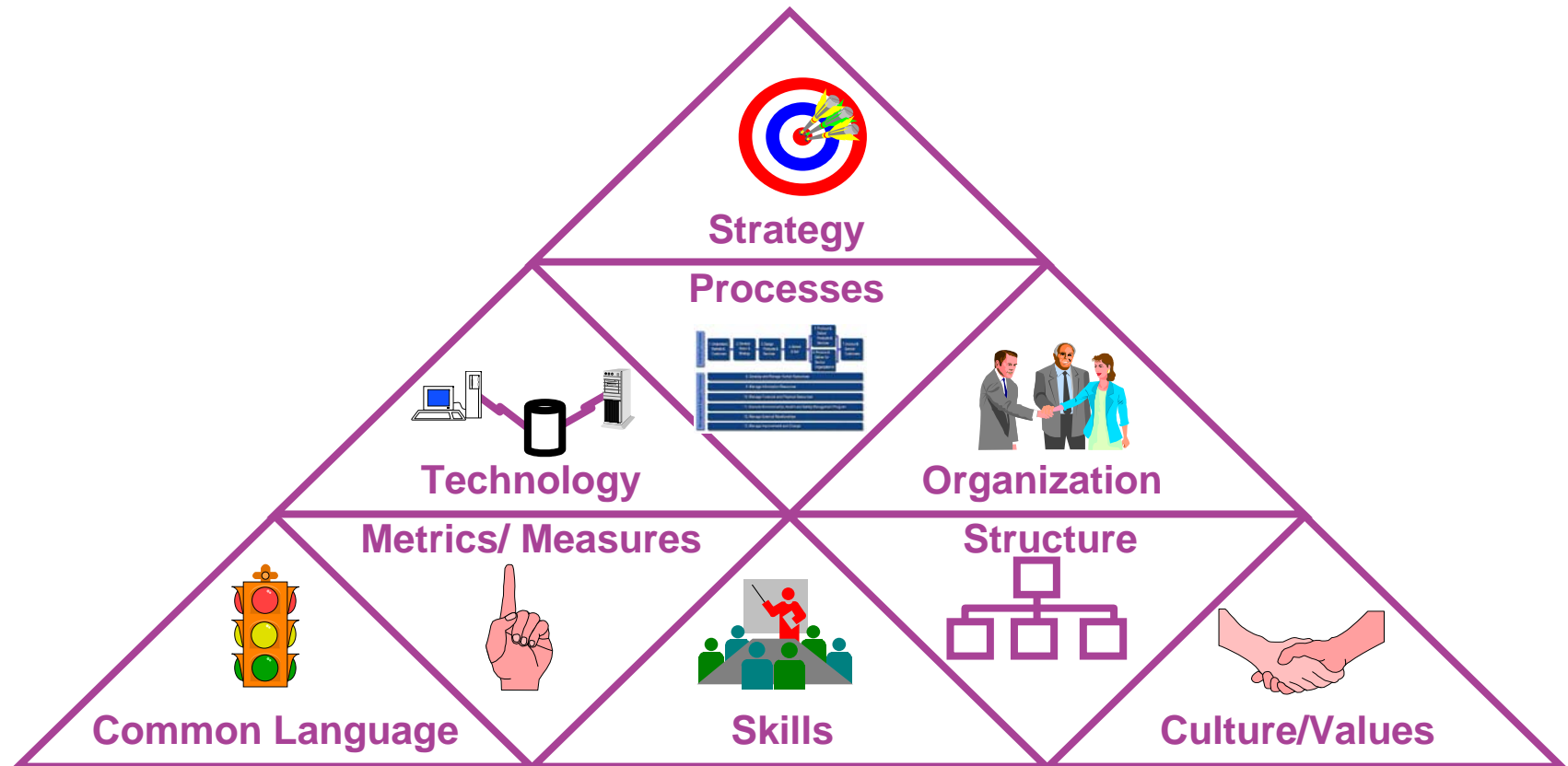
Presented by: **NEJAT AKSOY**

# Sources of IT Risk

**“IT related risk can be caused by any combination of the processes, systems (technology) or people (organization) who use various systems in the course of conducting business”**



# Sources of IT Risk



# Sources of IT Risk Definitions

## Strategy

- Goals & Objectives
- Key Stakeholders/Customers
- Value Proposition
- Implementation

## Technology

- Data Architecture and Ownership
- System and Network Architecture
- Configuration Choices
- Integration Methods
- Tools

## Processes

- Policies
- System, Business and Management Processes

## Organization

- Core Competencies
- Leadership Styles
- Communication Lines

## Common Language

- Risk language
- Process language
- Defining and discussing

## Metrics/Measures

- Success/Achievement
- Process Control
- Timing of Measurements

## Skills

- People/Training Needs
- Delivery Mechanisms
- Learning Organization

## Structure

- Organization Implications
- Roles, Responsibilities, and Skills Needed to Achieve the Goals and Objectives
- Individual Performance Measures

## Culture/Values

- Values and Beliefs
- Barriers

# CobiT Framework Risk Criteria

**“IT related events occurring during the course of conducting business, source risk which can be defined in terms of 7 key Risk Criteria”**

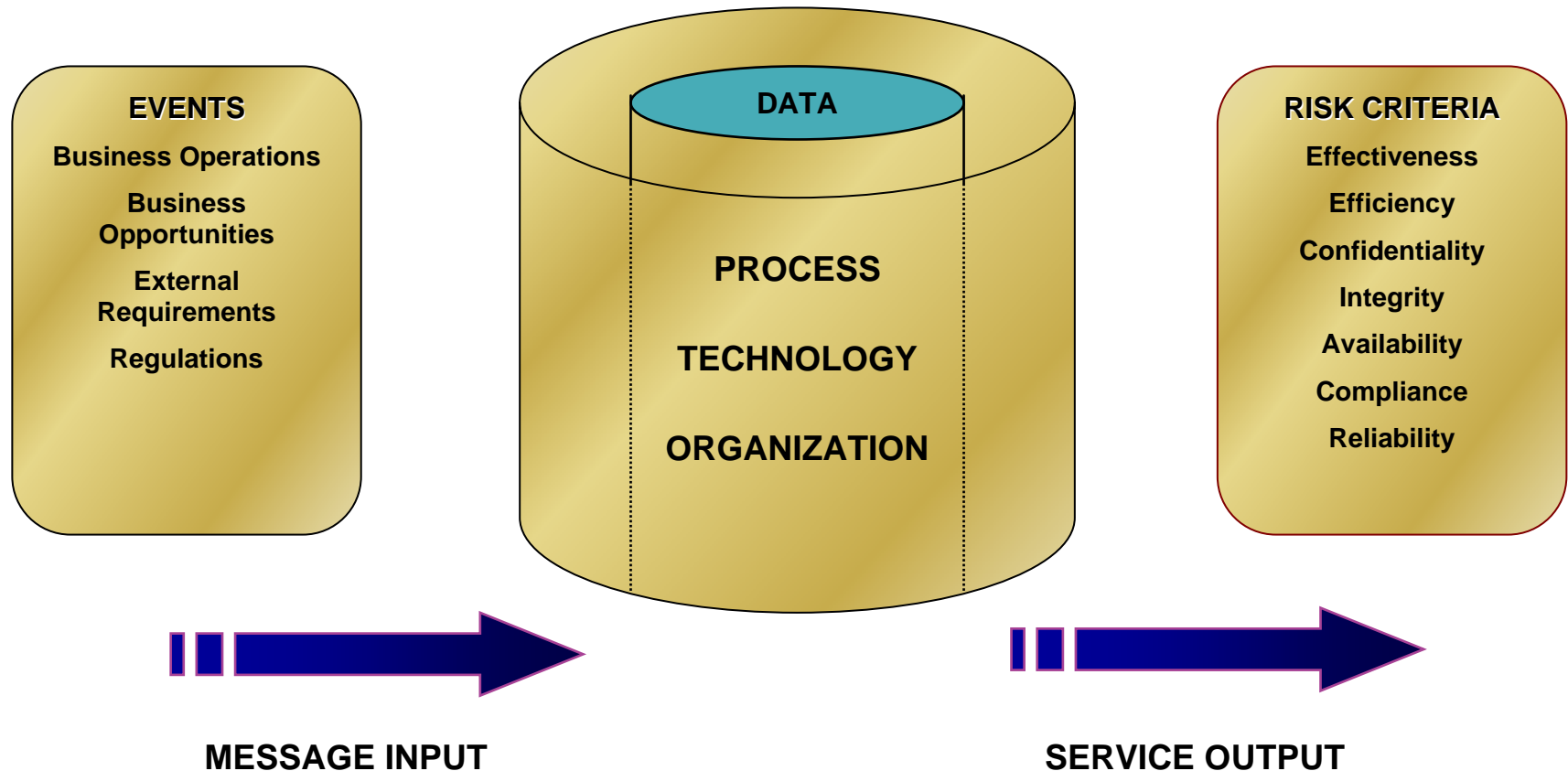


*September 26<sup>th</sup>, 2005*

Presented by: **NEJAT AKSOY**

# Risk Factors

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



# CobiT Framework Risk 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

AVAILABILITY

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

EFFICIENCY

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

COMPLIANCE

Deals with complying with laws, regulations and contractual arrangements.

CONFIDENTIALITY

Concerns the protection of sensitive information from unauthorised disclosure

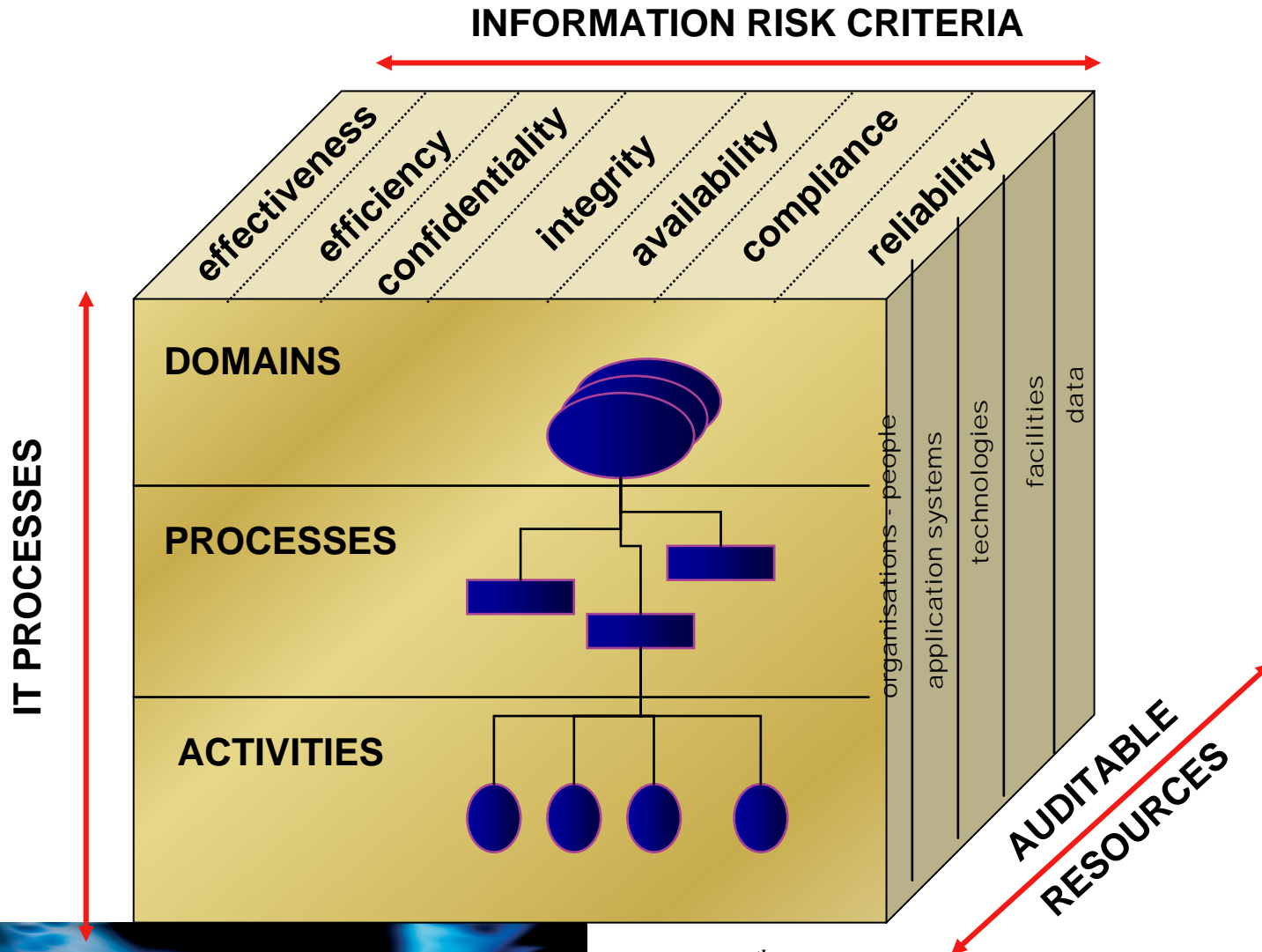
RELIABILITY OF INFORMATION

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

INTEGRITY

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

# CobiT Cube



# CobiT Framework Risk Categories

**“Once the IT sourced risk universe is defined, each of its components can be prioritized so they can be managed and audited optimally”**



*September 26<sup>th</sup>, 2005*

Presented by: **NEJAT AKSOY**

# CobiT : An IT control framework

## The Elements of COBIT -- What ?

Executive Summary -- “There is a Method...”

Framework -- “The Method Is...”

Control Objectives -- “Minimum Controls Are...”

Audit Guidelines -- “Here’s How You Audit...”

Implementation Guide -- “Here’s How You Implement”

Management Guide -- “Here’s How You Measure”

An open standard at [www.isaca.org](http://www.isaca.org)



September 26<sup>th</sup>, 2005

Presented by: **NEJAT AKSOY**

# CobiT : An IT control framework

## Why Should an Organisation Adopt COBIT?

IT an important element of Corporate Governance and Management  
Accountability

Ensure Business Oriented Solutions

Framework for Risk Assessment

As a means to communicate with

Management, Users and Auditors

Authoritative Basis

∞ internationally accepted

∞ exhaustive

∞ evolving

# CobiT : An IT control framework

Recent developments added a management and governance layer, providing management with a toolbox containing:

- Performance measurement elements (outcome measures and performance drivers for all IT processes)
- A list of critical success factors that provides succinct non-technical best practices for each IT process
- A maturity model to assist in benchmarking and decision-making for control over each IT process

# CobiT : An IT control framework

## Key Goal Indicators

- describes the outcome of the process, i.e. measurable after the fact; a measure of “what”; may describe the impact of not reaching the process goal
- is an indicator of the success of the process and its business contribution
- focusses on the customer and financial dimensions of the balanced scorecard

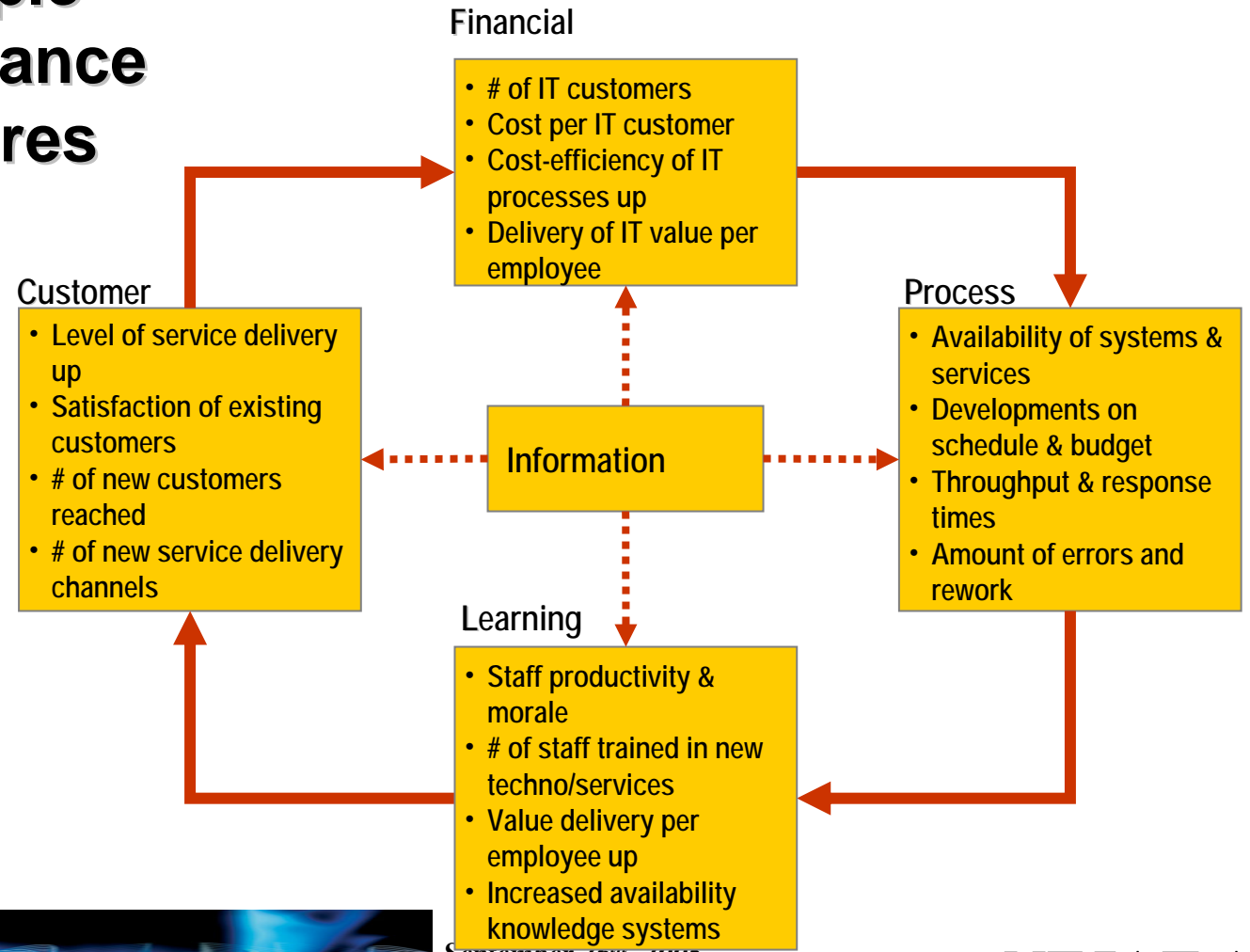
# CobiT : An IT control framework

## Key Performance Indicators

- are a measure of “how well” the process is performing
- predict the probability of success or failure
- focus on the process and learning dimensions of the balanced scorecard
- are expressed in precise measurable terms
- should help in improving the IT process

# CobiT : An IT control framework

## Example Performance Measures



# CobiT : An IT control framework

## Critical Success Factors

- the most important things to do to increase the probability of success of the process
- observable - usually measurable - characteristics of the organisation and process
- focus on obtaining, maintaining and leveraging capability, skills and behaviour

# CobiT : An IT control framework

## Critical Success Factors - Examples

### Strategy

- The IT Strategic plan clearly states a risk position such as leading-edge or road-tested, innovator or follower, and the required balance between time-to-market, cost of ownership and service quality

### Policy

- If you are not ready to enforce the policy, don't issue the policy

### Compliance

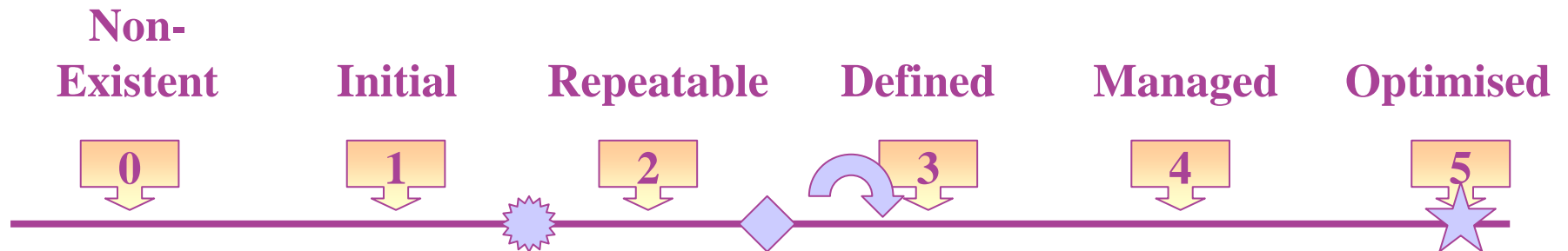
- A ' building permit ' programme for building IT systems and a ' drivers licence ' programme for those doing the building

### Security





- A good security plan takes time to evolve

# CobiT : An IT control framework

## Maturity Models



### Legend for symbols used

-  Enterprise current status
-  International standard guidelines
-  Industry best practice
-  Enterprise strategy

### Legend for rankings used

- 0 - Management processes are not applied at all
- 1 - Processes are ad hoc and disorganised
- 2 - Processes follow a regular pattern
- 3 - Processes are documented and communicated
- 4 - Processes are monitored and measured
- 5 - Best practices are followed and automated

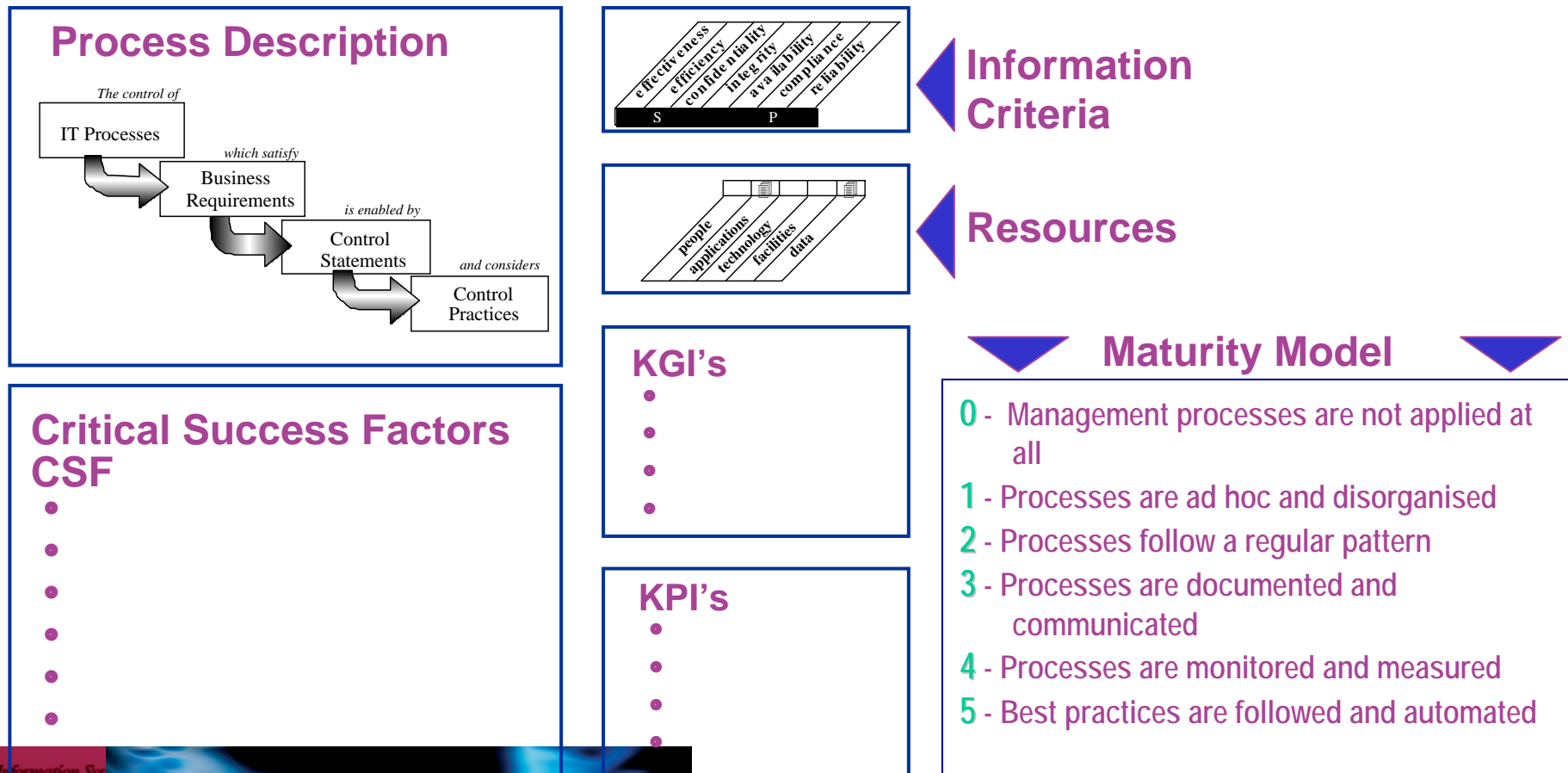


September 26<sup>th</sup>, 2005

Presented by: **NEJAT AKSOY**

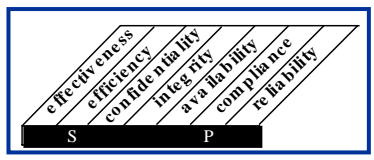
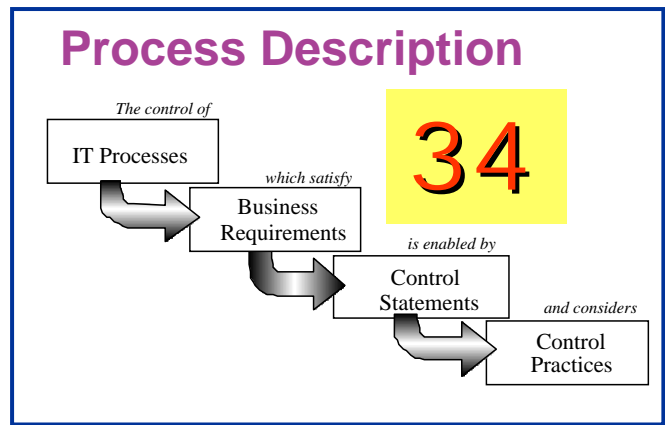
# CobiT : An IT control framework

## Management Guidelines Framework

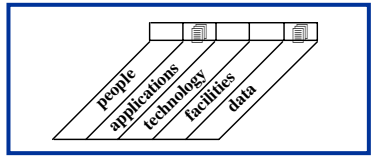


# CobiT : An IT control framework

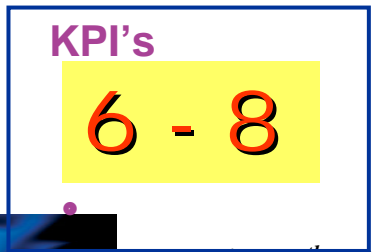
## Management Guidelines Framework



**Information Criteria**



**Resources**



**Maturity Model**

- 0 - Management processes are not applied at all
  - 1 - Processes are ad hoc and disorganised
  - 2 - Processes follow a regular pattern
  - 3 - Processes are documented and communicated
  - 4 - Processes are monitored and measured
  - 5 - Best practices are followed and automated
- 1**



# CobiT : An IT control framework

## Generic Process Guideline

**Control over an IT process and its activities with specific business goals**

**is determined by** the delivery of information to the business that addresses the required information criteria and **is measured by KGIs**

**is enabled by** creating and maintaining a system of process and control excellence appropriate for the business

**considers CSFs** that leverage specific IT resources and **is measured by KPIs**

# CobiT : An IT control framework

## Generic Process Guideline - Key Goal Indicators

- Increased level of service delivery
- Number of customers and cost per customer served
- Availability of systems and services
- Absence of integrity and confidentiality risks
- Cost efficiency of processes and operations
- Confirmation of reliability and effectiveness
- Adherence to development cost and schedule
- Cost efficiency of the process
- Staff productivity and morale
- Number of timely changes to processes and systems
- Improved productivity (e.g., delivery of value per employee)

# CobiT : An IT control framework

## Generic Process Guideline - Key Performance Indicators

- System downtime
- Throughput and response times
- Amount of errors and rework
- Number of staff trained in new technology and customer service skills
- Benchmark comparisons
- Number of non-compliance reportings
- Reduction in development and processing time

# CobiT : An IT control framework

## Generic Process Guideline - Critical Success Factors

- IT performance is **measured** in financial terms, as customer satisfaction, for process effectiveness and future capability; IT management is rewarded based on these measures
- The processes are **aligned** with the IT strategy and with the business goals; they are scalable and their resources are appropriately managed and leveraged
- Everyone involved in the process is **goal focused** and has the appropriate information on customers, on internal processes and on the consequences of their decisions
- Cross-divisional **co-operation** and teamwork, as well as continuous process improvement
- **Control practices** to increase transparency, reduce complexity, promote learning, provide flexibility and allow scalability
- Goals and objectives are **communicated** across all disciplines and are understood
- It is clear how to implement and monitor process objectives, who is **accountable** for process performance and who the **customers** of the process are
- A continuous process quality **improvement** effort is applied
- The required **quality of staff** and **availability of skills** exist

# CobiT : An IT control framework

## Generic Process Guideline - Maturity Model

- 0 Non Existent.** Complete lack of any recognisable processes. Organisation has not even recognised that there is an issue to be addressed.
- 1 Initial.** There is evidence that the organisation has recognised that the issues exist and need to be addressed. There are however no standardised processes but instead there are ad hoc approaches that tend to be applied on an individual or case by case basis. The overall approach to management is chaotic.
- 2 Repeatable.** Processes have developed to the stage where similar procedures are followed by different people undertaking the same task. There is no formal training or communication of standard procedures and responsibility is left to the individual. There is a high degree of reliance on the knowledge of individuals, hence errors are likely.
- 3 Defined.** Procedures have been standardised and documented, and communicated through training. It is however left to the individual to follow these processes, and any deviations would be unlikely to be detected. The procedures themselves are not sophisticated but are the formalisation of existing practices.
- 4 Managed.** It is possible to monitor and measure compliance with procedures and to take action where processes appear not to be working effectively. Processes are under constant improvement and provide good practice. Automation and tools are used in a limited or fragmented way.
- 5 Optimised.** Processes have been refined to a level of best practice, based on the results of continuous improvement and maturity modelling with other organisations. IT is used in an integrated way to automate the workflow and provide tools to improve quality and effectiveness.

# CobiT : An IT control framework

## Management Guidelines : What next ?

- How to compare with the industry
- Benchmarking
  - by industry, geography, size
  - for different IT environments
    - core business applications
    - intranet and office automation
    - emerging technologies
- CobiT Evolution
  - access to expert info
  - updates
  - small & medium sized organizations
  - implementation advise

# The future of CobiT

## Agenda

- CobiT : An IT Control Framework
- CobiT IV Strategy
- Five Major Projects
  - IT Control Practices
  - Maturity Benchmarking
  - Implementation Guide
  - CobiT *Online*
  - CobiT *lite*
- CobiT Examples

# CobiT IV Strategy

## Values

- Sharing knowledge
- Leveraging expertise
- Influencing good practices

## Vision

To be the internationally accepted standard for good practice in control over IT, and to assist users from assessment to implementation

## Mission

Through a coherent up-to-date product set, further influence and support an expanding target audience with on-line continuously up-to-date knowledge on IT control, assurance and governance

## Target Audience

executives & boards  
management  
professionals

who

monitor  
assess  
implement

what

# CobiT IV Strategy

## Values

↳ Vision

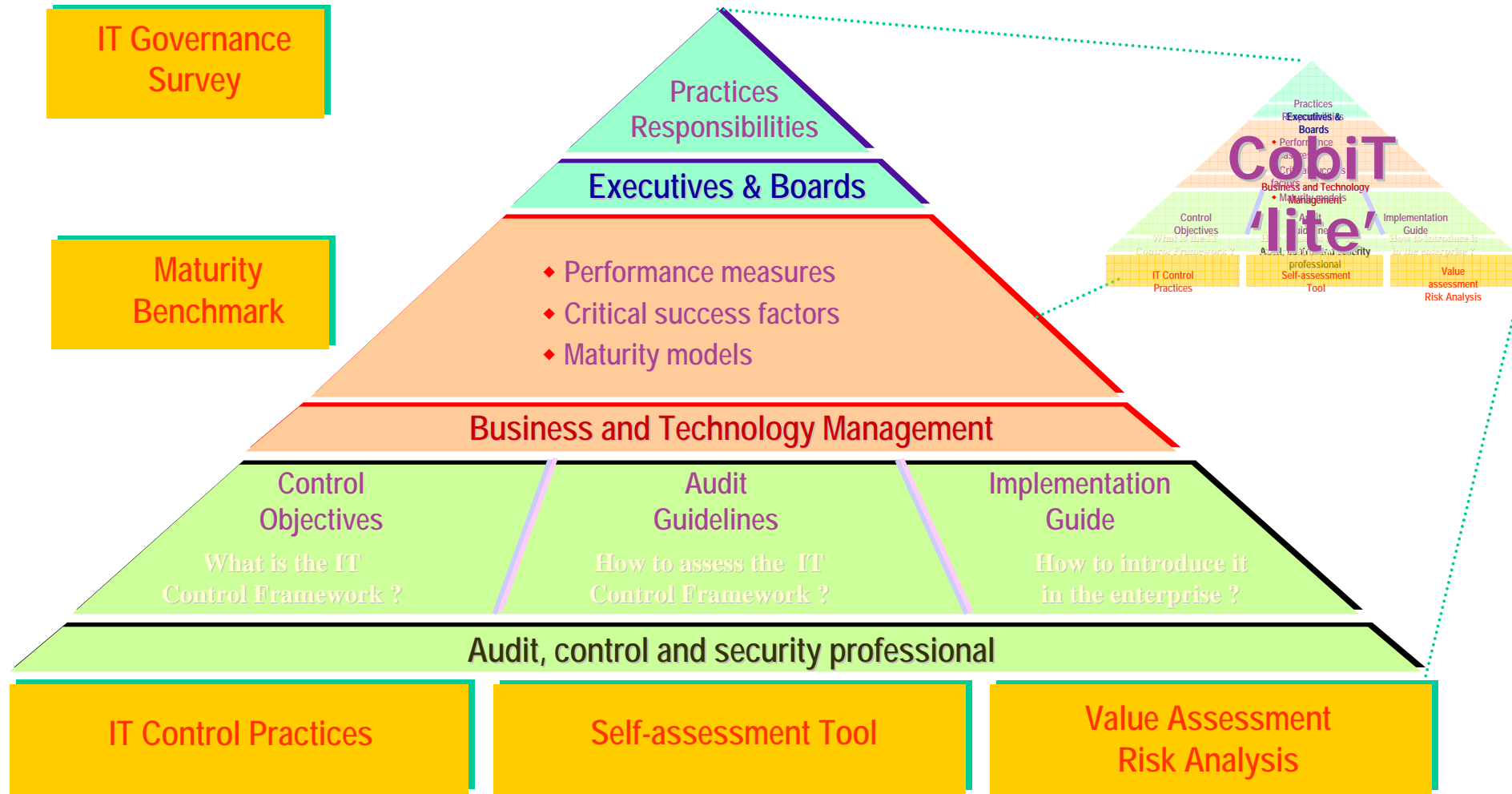
↳ Mission

↳ Strategy

- ◆ Leverage expertise CSC & others to deepen knowledge base
- ◆ To establish an effective and efficient update cycle
- ◆ To widen the audience through initiatives focused on academia, public sector, small and medium sized enterprises
- ◆ To align with IT Governance requirements
- ◆ To expand implementation advise
- ◆ To build online tools that support
  - 📁 knowledge capturing & sharing
  - 📁 measurement
  - 📁 benchmarking
  - 📁 self-assessment
  - 📁 gap-analysis & implementation

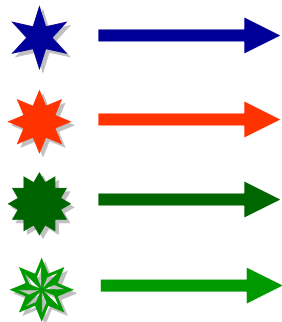
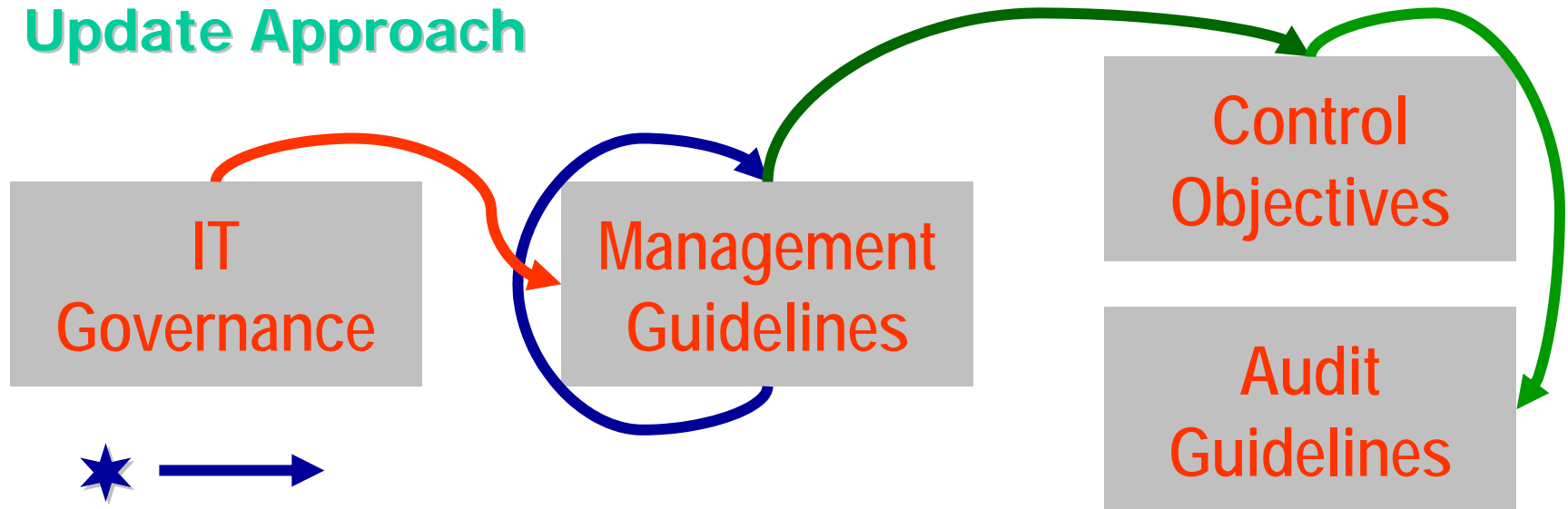


# CobiT IV - Product Structure



# CobiT IV Updates

## Update Approach



September 26<sup>th</sup>, 2005

Presented by: **NEJAT AKSOY**




# The future of CobiT

## Agenda

- CobiT : An IT Control Framework
- CobiTIV Strategy
- Five Major Projects
  - IT Control Practices
    - Maturity Benchmarking
    - Implementation Guide
    - CobiT *Online*
    - CobiT *lite*
  - CobiT Examples

# IT Control Practices

## Deliverable

	Practice	Risk/Value	
PO9.5.4	When employees are given their account, they should be provided with initial or refresh- er training and awareness on computer security issues. They should be asked to review the rules and regulations for system access and confirm they have understood.	<ul style="list-style-type: none"> <li>• Ignorance of compliance requirements and sanctions leading to rules not being respected.</li> <li>• Ignoring rules that are too generic or descriptive</li> <li>• Absence of awareness leading to weak discipline</li> </ul>	effectiveness 
			cost-efficiency 
			expedience 

**Future development for integration with CobiT /ite and Implementation Guide**



# IT Control Practices

## Requirements

- The benefits listed under 'why do it' are tangible and motivate to implement controls
- The set of control practices is *complete* (e.g. key controls) and implementation satisfies the control objective
- Control practices listed are generally accepted as *good business practice*
- Control practices suggest *sustainable* solutions
- The control practices are *effective* in addressing the risk linked to not achieving the detailed control objective
- The control practices suggest *efficient* solutions
- The wording of the control practices is *concise* while providing clear and unambiguous guidance on what is expected for implementation
- The control practices are *realistic*

Risk/value statements developed at the detailed control objective level rather than at the practice level.

Where possible, begin with an introductory "stem", followed by bullet points

No more than 5 risk/value statements for any given control objective

Get guidance for content from CSFs & Considerations in Framework

At least 2 practices per detailed control objective

Number of practices no more than twice

the number of risk/value statements

### 3. Control Practices for PO-9

#### PO-9.1. Business Risk Assessment

##### Why do it?

The provision of a systematic risk assessment framework in line with the control practices will:

- ◆ Avoid the decline in the effectiveness of the risk assessment process over time as a result of staff turnover and the time taken to transfer knowledge between skilled risk assessors and new recruits
- ◆ Ensure frequent updates to accommodate new forms of business and IT risk (e.g., the loss of intellectual capital, which weakens the capability for business innovation)
- ◆ Promote the effective management of risk as the cross-discipline
- ◆ Result in opportunities for organizational synergy and avoidance of duplication of risk management effort by aligning the IT risk assessment framework with the broader corporate and IT governance processes
- ◆ Involve senior management representing the major business and IT functions and therefore increase the initial acceptance of the framework and facilitate their continued and active support of the risk assessment process

##### Control Practices

- PO-9.1.1. Senior management, representing the major business and IT functions, develops a systematic risk assessment framework and establishes a policy to define risk limits and risk tolerance.
- PO-9.1.2. An integrated business and IT risk assessment framework and approach, which forms part of the broader Corporate Governance initiatives, is used. This integrated framework supports a holistic risk assessment approach that reviews the global as well as systems specific risk.
- PO-9.1.3. The business risk assessment process is regularly updated with the results of audits, inspections and identified incidents. The potential business impacts of new technologies are continually evaluated and are also used to update the risk assessment process.
- PO-9.1.4. The risk assessment framework provides an important input to both the business and the IT strategy. The value of this input is increased by the participation of senior management from across the organization in the risk assessment process and the continual scanning of new technologies that impact on the business.

#### PO-9.2. Risk Assessment Approach

##### Why do it?

A "Why Do It?" justifies the implementation of the Control Practice by stating how it can assist in controlling and managing risk and/or increasing benefits, either immediately or by establishing a basis for continuous improvement. Managing risk means decreasing the probability of adverse consequences from threats and vulnerabilities, safeguarding the assets, and limiting the impact on the business. Increasing benefits means achieving efficiency and/or effectiveness gains.

Use the information criteria, KGIs, KPIs

Only key controls!

IT Control Practices are key control mechanisms that support the achievement of control objectives as well as the prevention, detection and correction of undesired events through responsible use of resources, appropriate management of risk, and alignment of IT with business.

September 26<sup>th</sup>, 2005

Presented by: **NEJAT AKSOY**

# The future of CobiT

# Agenda

- CobiT : An IT Control Framework
- CobiTIV Strategy
- Four Major Projects
  - IT Control Practices
  - Maturity Benchmarking
  - Implementation Guide
  - CobiT *Online*
  - CobiT *lite*
- CobiT Examples

Tick one	
SIZE	
Large	>5000M\$* or > 15000 staff
Medium	>500M\$* or > 1500 staff
Small	>50M\$* or > 150 staff
	* in turnover, budget or revenue

Date (yymmdd)	
Assessor #	
Organisation #	



**CobIT**  
**Control and Governance Maturity Survey**

GEOGRAHY	
NA	North America (US, CA, MX)
EMEA	Europe, Middle East & Africa
AA	Asia and Oceania
SA	South & Central America
Global	Operating in different regions

Please provide a high level profile of the organisation being benchmarked by ticking the

INDUSTRY	
Prod	
Ret	
Fin	
Publ	
Ph/H	

# Maturity Benchmark

IT Serv	IT Service Providers
Other	Other

Please also identify where relevant, drivers that push organisations to move up a level, and inhibitors from getting from one level to the next.

Process	Domain I	Domain II	Domain III	DRIVERS	INHIBITORS
PO1 define a strategic IT plan					
PO3 determine the technological direction					
PO5 manage the IT investment					
PO9 assess risks					
PO10 manage projects					
AI1 identify solutions					
AI2 acquire and maintain applications s/w					
AI5 Install and accredit systems					
AI6 manage changes					
DS1 define service levels					
DS4 ensure continuous service					
DS5 ensure system security					
DS10 manage problems and incidents					
DS11 manage data					
M1 monitor the processes					



September 26<sup>th</sup>, 2005

Presented by: **NEJAT AKSOY**

# Maturity Benchmark

## Drivers

- Compliance with law, standards and regulations
- Cost reduction
- Mission and goals
- Performance improvement
- Risk reduction
- Reputation and trust
- Competitive environment
- Corporate values
- Political/economic environment

## Inhibitors

- Budget limitations
- Availability of skilled staff
- Management awareness
- Management commitment
- Lack of ownership
- Existing architecture
- No easy solution
- Resource conflicts/priorities
- Lack of tools
- Political/economic environment

# Maturity Benchmark

## Reference

	Core systems				Process
	Finance	Health / Pharma	Public Sector	Retail / Manufac	Weight
<b>Po1</b>	3	3	3	2	
<b>Po3</b>	4	3	2	2	
<b>Po5</b>	3	2	4	3	
<b>Po9</b>	2	3	3	1	
<b>Po10</b>	3	3	1	3	
<b>A11</b>	3	2	1	1	
<b>A12</b>	2	3	1	2	
<b>A15</b>	2	3	1	2	
<b>A16</b>	3	3	2	3	
<b>DS1</b>	2	2	2	2	
<b>DS4</b>	4	3	3	3	
<b>DS5</b>	4	3	3	2	
<b>DS10</b>	3	3	2	2	
<b>DS11</b>	4	2	1	2	
<b>M1</b>	3	2	2	1	

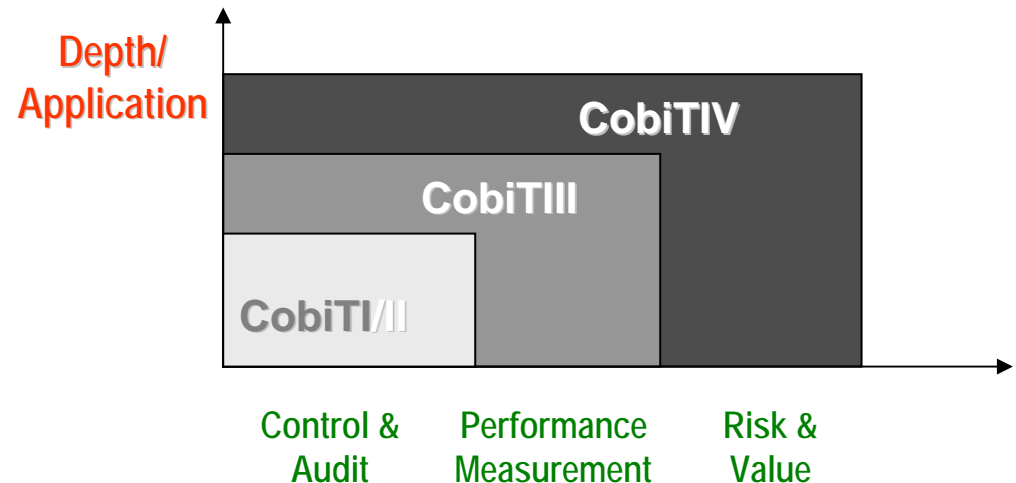
# The future of CobiT

## Agenda

- CobiT : An IT Control Framework
- CobiTIV Strategy
- Four Major Projects
  - IT Control Practices
  - Maturity Benchmarking
  - **Implementation Guide**
  - CobiT *Online*
  - CobiT *lite*
- CobiT Examples

# Implementation Guide

- Fit with IT Governance
- Drivers
- As-Is & To-Be
- Gap Analysis and Roadmap
  - Improvement Plan
  - 'Smart' things that need to be done
- Tools
  - Risk analysis
  - Decision-support
  - Control Diagnostic
- Updates
  - Reuse
  - Technology update



# Implementation Guide

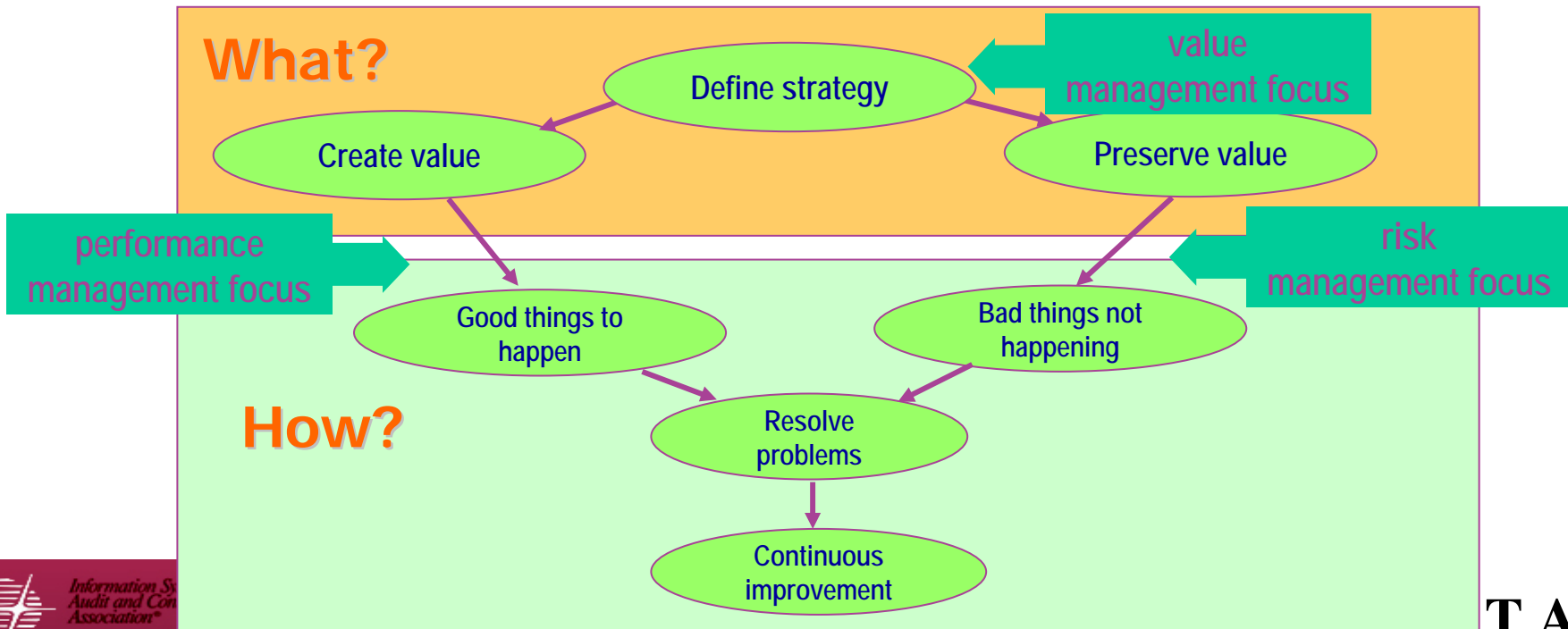
## Drivers and Definitions

Control Framework Implementation needs first an enterprise driver which is

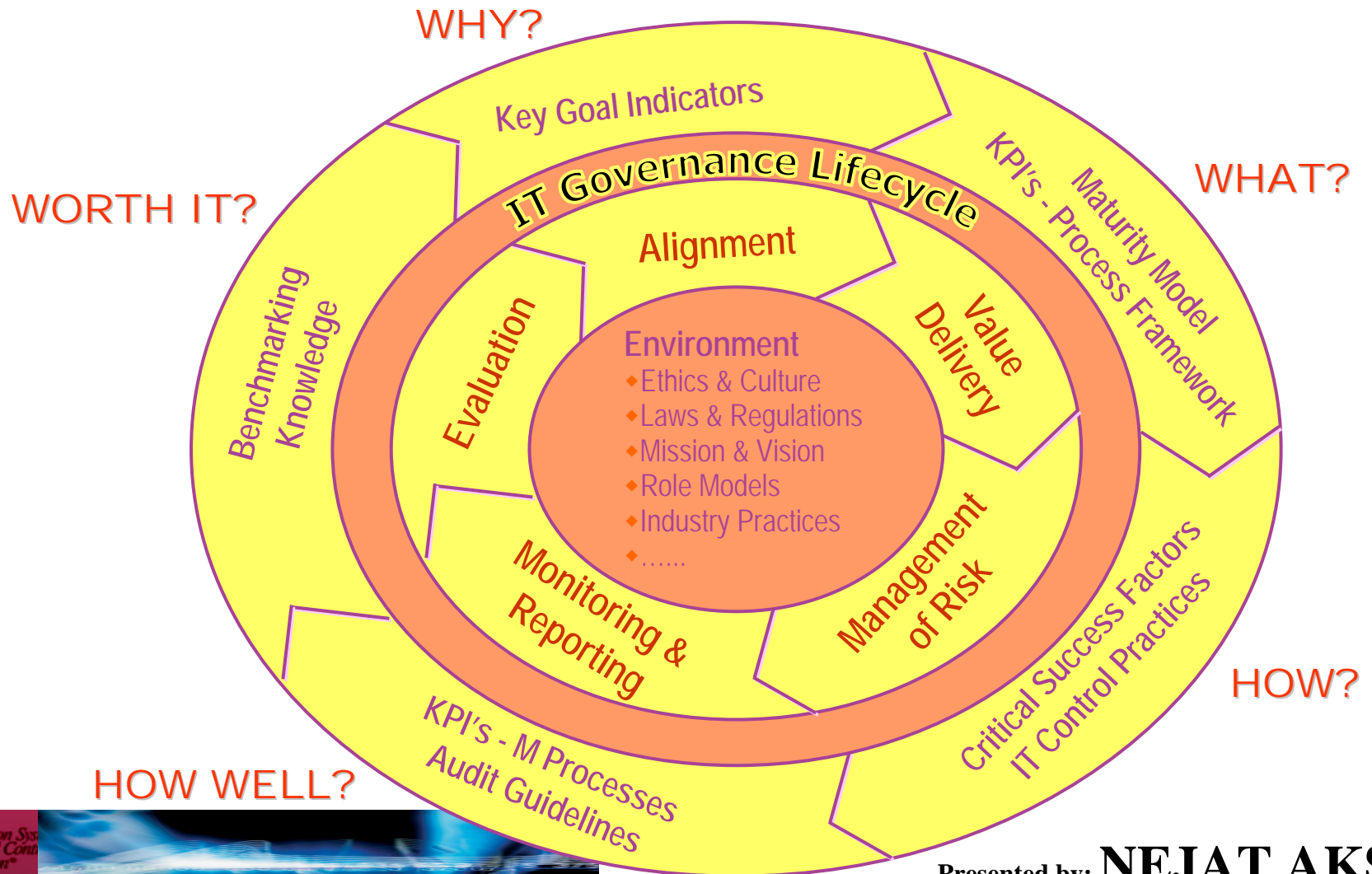
- value expectation
- risk assurance
- performance requirement

Second,

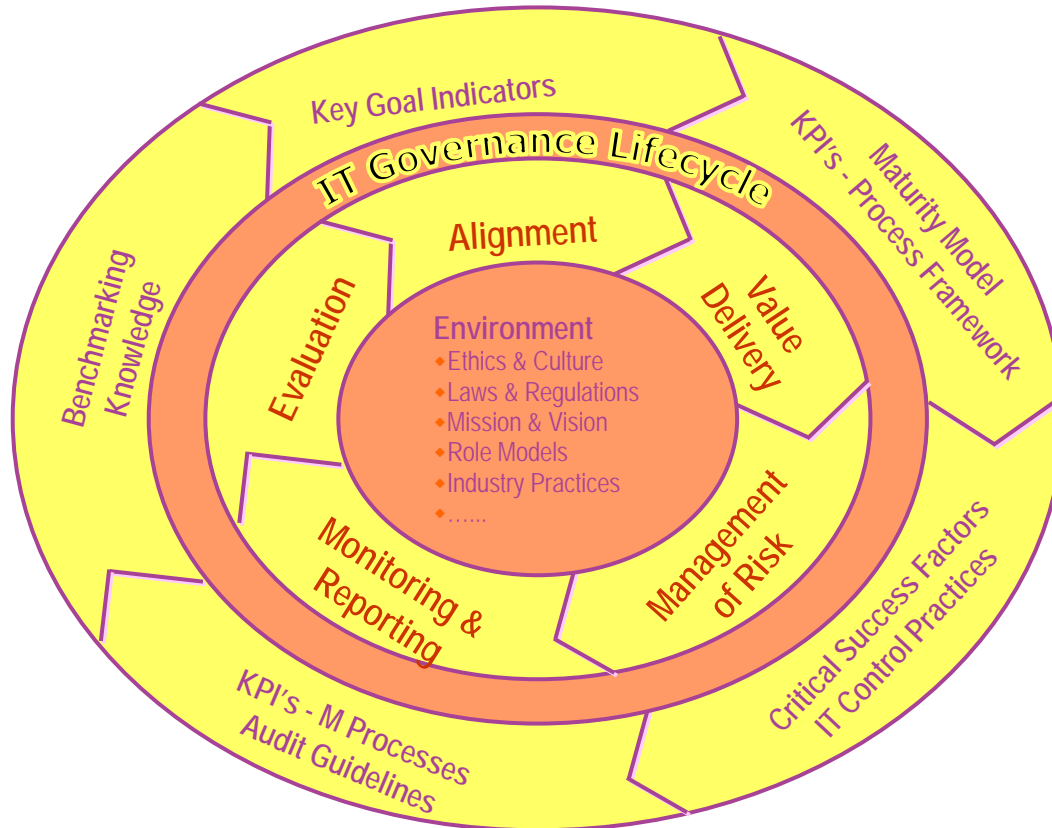
- the actual situation is measured (as-is),
- the preferred future situation is defined (to be)
- the gap is analysed
- an action plan is proposed



# Implementation Guide



# Implementation Guide



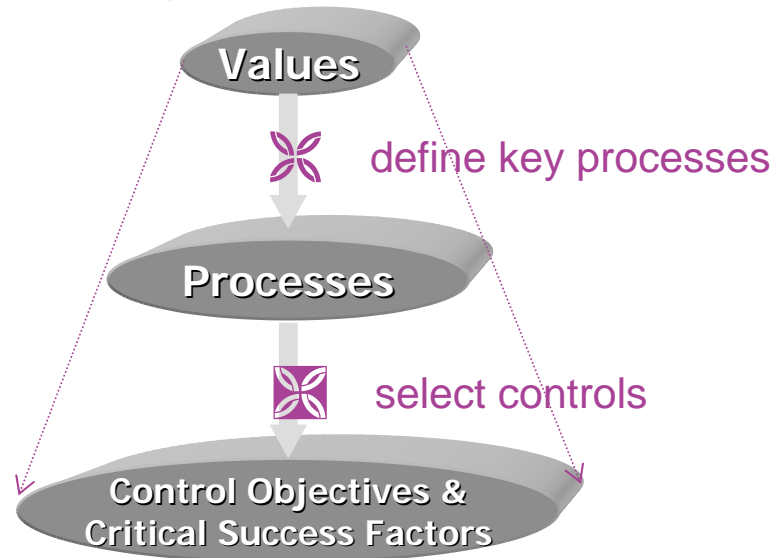
## Change Roadmap



# Implementation Guide

## From drivers with tools to solutions

↗ define your values and risks



### TOOLS

- ↗ & ✿ value/risk analysis
- ✿ maturity models and decision analysis
- ↗ Boston Squares for control cost vs risk and control cost vs value

✿ sanity check : does this deliver business value?

↗ rank on risk and/or value and on cost and expedience of the solution, then identify quick wins and long term strategies

# Implementation Guide

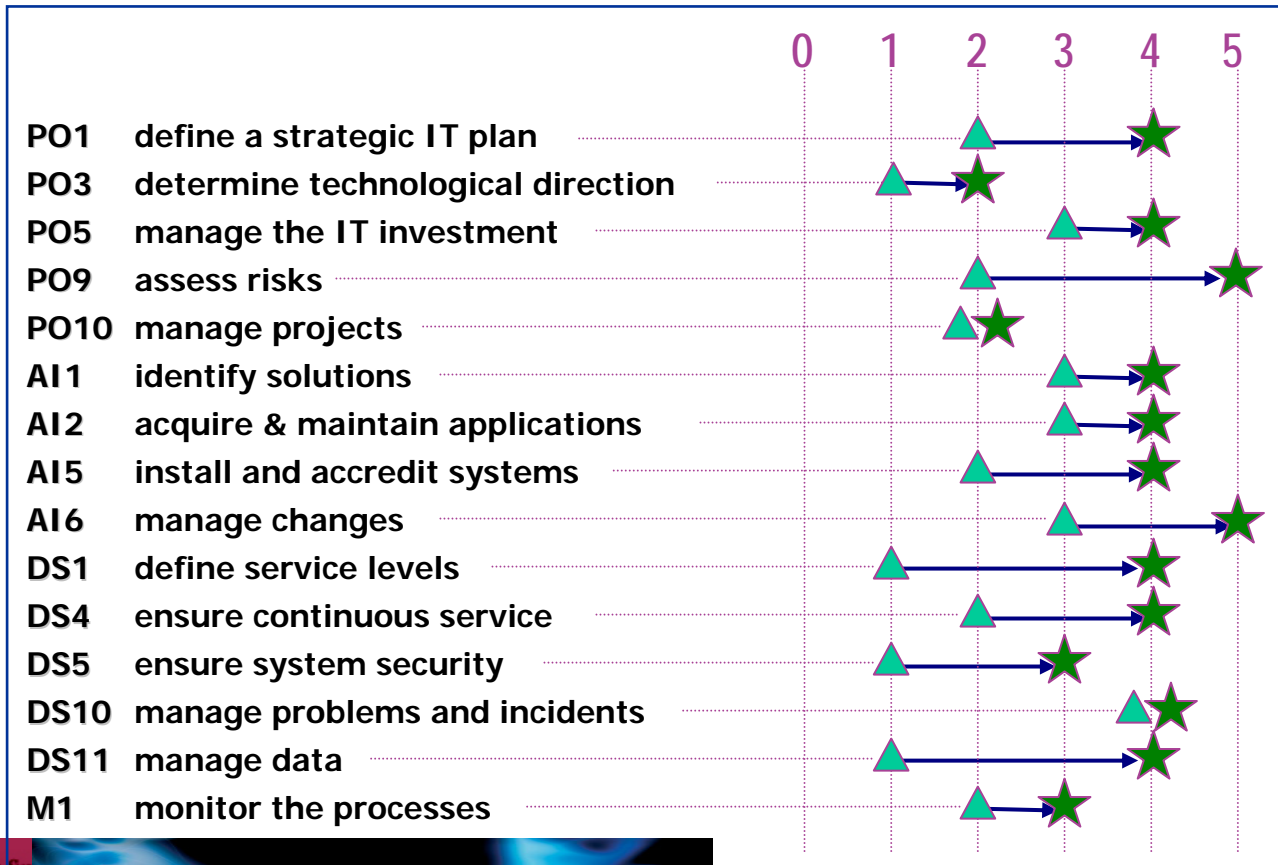
## IT Control Diagnostic → Drivers

Management's Technology Concerns		IT Domains and Processes						
		COST OPTIMISATION	ALIGNING IT AND BUSINESS	IT SERVICE DELIVERY	SELECTIVE OUTSOURCING	RESOURCE MANAGEMENT	SECURITY	ENTERPRISE ARCHITECTURE
<b>Planning &amp; Organisation</b>								
PO1	Define a Strategic Information Technology Plan		x		x			
PO2	Define the Information Architecture		x				x	x
PO3	Determine the Technology Direction		x		x			x
PO4	Define the IT Organisation and Relationships	x	x	x	x			x
PO5	Manage the Investment in Information Technology	x			x	x		
PO6	Communicate Management Aims and Direction						x	
PO7	Manage Human Resources	x			x	x	x	
PO8	Ensure Compliance with External Requirements						x	
PO9	Assess Risks						x	
PO10	Manage Projects	x	x	x				
PO11	Manage Quality	x						
<b>Acquisition &amp; Implementation</b>								
A11	Identify Solutions		x		x		x	x
A12	Acquire and Maintain Application Software	x					x	
A13	Acquire and Maintain Technology Architecture	x					x	x
A14	Develop and Maintain Information Technology Procedures							
A15	Install and Accredite Systems						x	
A16	Manage Changes	x		x		x	x	
<b>Delivery &amp; Support</b>								
DS1	Define Service Levels		x	x			x	
DS2	Manage Third-Party Services	x		x	x	x	x	
DS3	Manage Performance and Capacity			x			x	
DS4	Ensure Continuous Service			x				
DS5	Ensure Systems Security							x

- ☞ COST OPTIMISATION
- ☞ ALIGNING IT AND BUSINESS
- ☞ IT SERVICE DELIVERY
- ☞ SELECTIVE OUTSOURCING
- ☞ RESOURCE MANAGEMENT
- ☞ SECURITY
- ☞ ENTERPRISE ARCHITECTURE
- ☞ SYSTEMS INTEGRATION
- ☞ IT VALUE DELIVERY
- ☞ PRIORITISING & PLANNING IT

# Implementation Guide

## Maturity Gap Analysis



▲ As-Is

★ To-Be

September 26<sup>th</sup>, 2005

Presented by: **NEJAT AKSOY**

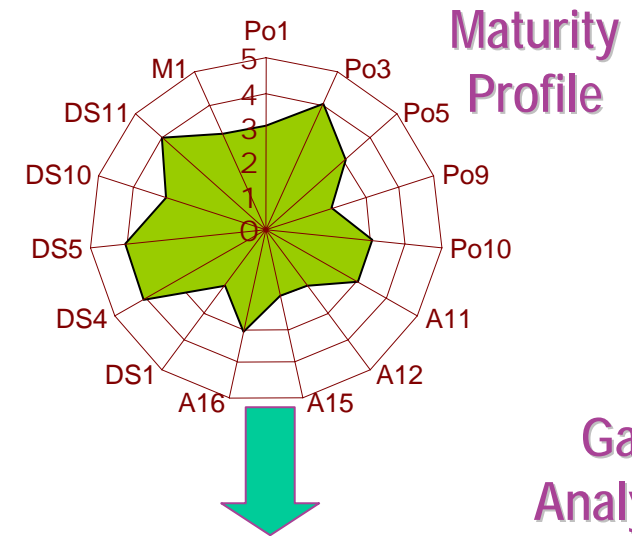
# Implementation Guide

## IT Control Diagnostic

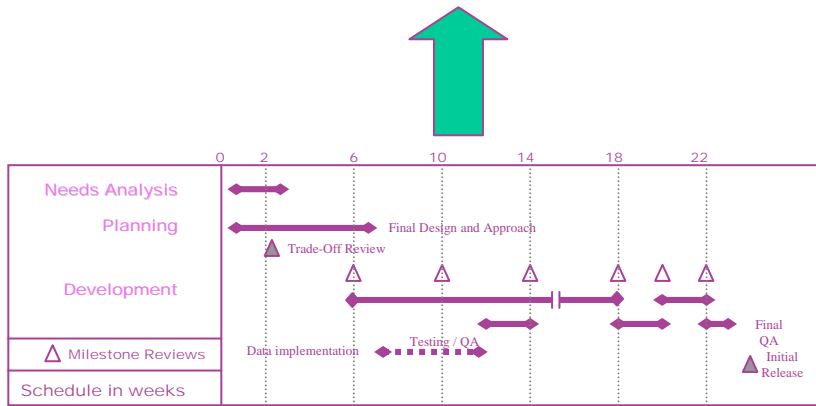
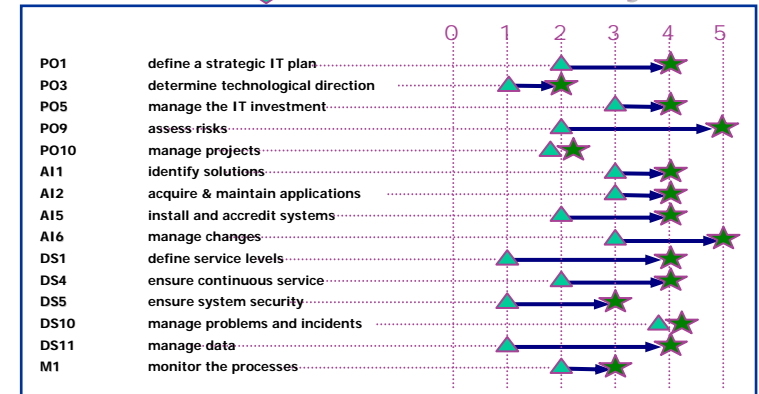
**Management's Technology Concerns**

**IT Domains and Processes**

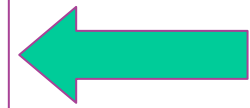
	Strategic Planning	Business Process Management	Information Security	IT Infrastructure	IT Service Management	IT Governance
<b>Planning Organization</b>						
PO1 Define a Strategic Information Technology Plan	*	*	*	*	*	*
PO2 Develop the Technology Strategy	*	*	*	*	*	*
PO3 Develop the IT Investment Strategy	*	*	*	*	*	*
PO4 Define the IT Organization and Relationships	*	*	*	*	*	*
PO5 Manage the Investment in Information Technology	*	*	*	*	*	*
PO6 Communicate Management Aims and Direction	*	*	*	*	*	*
PO7 Manage Human Resources	*	*	*	*	*	*
PO8 Ensure Compliance with Ethical Requirements	*	*	*	*	*	*
PO9 Assess Risks	*	*	*	*	*	*
PO10 Manage Projects	*	*	*	*	*	*
PO11 Manage Quality	*	*	*	*	*	*
<b>Acquisition &amp; Implementation</b>						
A1 Identify Solutions	*	*	*	*	*	*
A2 Acquire and Maintain Applications Software	*	*	*	*	*	*
A3 Acquire and Maintain Technology Architecture	*	*	*	*	*	*
A4 Develop and Maintain Information Technology Procedures	*	*	*	*	*	*
A5 Install and Upgrade Systems	*	*	*	*	*	*
A6 Manage Changes	*	*	*	*	*	*
<b>Delivery &amp; Support</b>						
DS1 Define Service Levels	*	*	*	*	*	*
DS2 Manage Third-Party Services	*	*	*	*	*	*
DS3 Manage Performance and Capacity	*	*	*	*	*	*
DS4 Ensure Continuity Service	*	*	*	*	*	*
DS5 Ensure Systems Security	*	*	*	*	*	*
DS6 Security and Abuse Cases	*	*	*	*	*	*
DS7 Educate and Train Users	*	*	*	*	*	*
DS8 Assist and Advise Information Technology Customers	*	*	*	*	*	*
DS9 Manage the Configuration	*	*	*	*	*	*
DS10 Manage Problems and Incidents	*	*	*	*	*	*
DS11 Manage Data	*	*	*	*	*	*
DS12 Manage Facilities	*	*	*	*	*	*
DS13 Manage Operations	*	*	*	*	*	*
<b>Monitoring</b>						
M1 Monitor the Process	*	*	*	*	*	*
M2 Assess Internal Control Adequacy	*	*	*	*	*	*
M3 Obtain Independent Assurance	*	*	*	*	*	*
M4 Provide for Independent Audit	*	*	*	*	*	*



## Gap Analysis

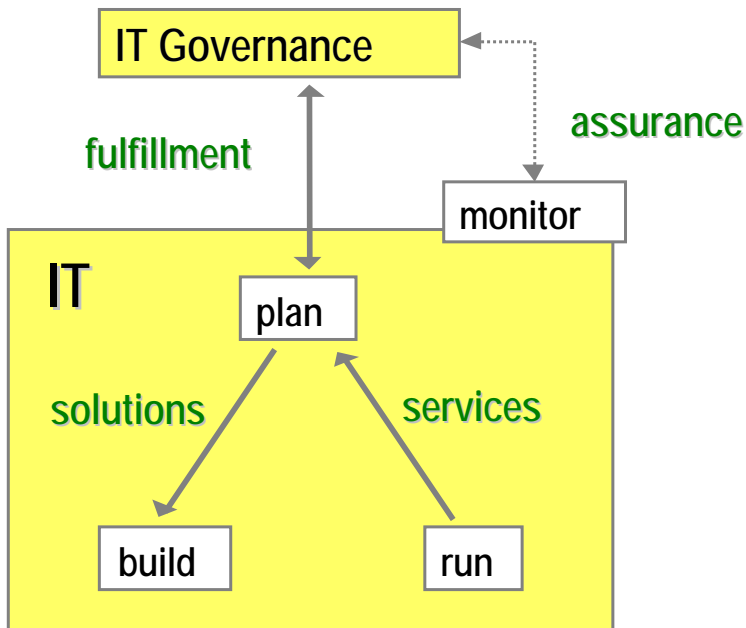


## Roadmap

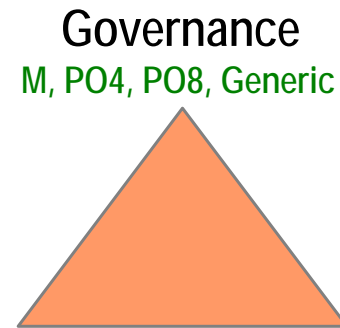


# Implementation Guide

## Clarify Process Structure



cost	PO5
quality	PO11
risk	PO9
change	AI6
project	PO10
security	DS4, DS5
investment	PO5



Create value

PO1, PO3, PO10, AI1, AI6

Maintain value

PO9, DS4, DS10, DS11, DS13

September 26<sup>th</sup>, 2005

Presented by: **NEJAT AKSOY**



# The future of CobiT

## Agenda

- CobiT : An IT Control Framework
- CobiTIV Strategy
- Five Major Projects
  - IT Control Practices
  - Maturity Benchmarking
  - Implementation Guide
  - **CobiT *Online***
  - CobiT *lite*
- CobiT Examples

# CobiTOnline

## Goal Statement

- Repository of all knowledge relative to IT governance, performance measurement, control assurance, control objectives and practices
- Web-based multi-user browsing, sharing and assessment tool that can at the same time be the front-end for
  - practice surveys
  - metrics for benchmarking

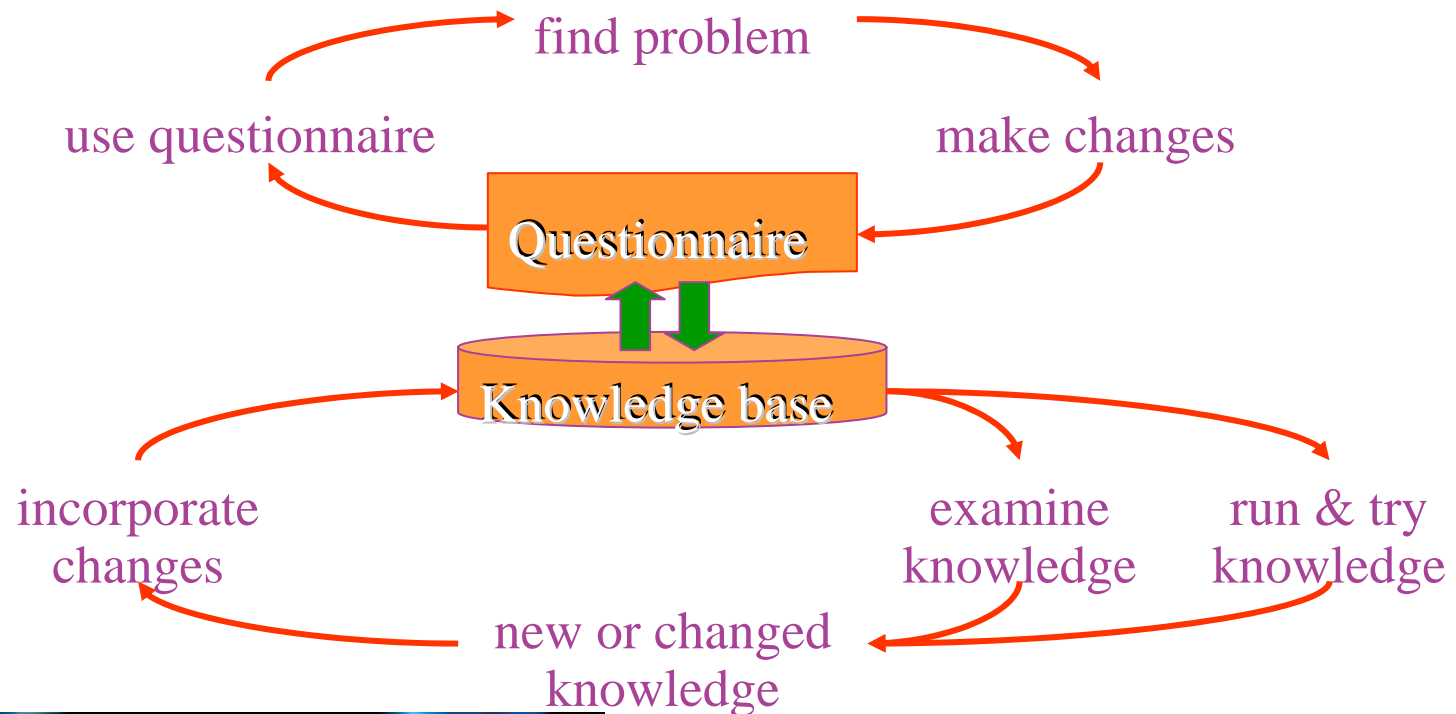


September 26<sup>th</sup>, 2005

Presented by: **NEJAT AKSOY**

# CobiTOnline

- Seeking and depositing knowledge is basically the same process ..... in reverse



# CobiTOnline

## Statement of Need

- **Generally an Increased Emphasis on IT Control and Security**
- **Market**
  - General economic environment creating pressure on costs; do the smart things...
  - Increased Risk Awareness emphasized by 9-11
  - Increased compliance requirements
  - Increased Scrutiny of Use of IT Resources
- **Profession**
  - Increasing Use of Internal Self-Assessment
  - No Widely Adopted or Used Software Tool and Content for IT Compliance Reviews
- **CobiT**
  - Need to Sustain its Acceptance in the Marketplace
  - Need to Explore Additional Methods of Distributing and Interacting with CobiT
  - Need to Increase Accessibility of CobiT to 30,000 + ISACA members
  - Need to Leverage Tools and Knowledge Base for Continuing Education

# CobiTOnline

## Project Objectives

- To promote COBIT as the industry standard for control and governance of IT
- To provide a forum for sharing IT control and governance information
- To generally improve the quality and completeness of this information
- To facilitate wider use and adoption of COBIT by providing an online product
- To raise the consistency of controls for the use of IT in enterprises
- To build databases related to industry practices and costs of deploying and maintaining IT in enterprises
- To gather feedback from industry on how to improve COBIT material



September 26<sup>th</sup>, 2005

Presented by: **NEJAT AKSOY**

# CobiTOnline

## Value Proposition

### Access to Information and Tools

- Knowledge - What is the latest up-to-date CobiT information?
- Self-assessment - What is the status of my IT governance and control?
- Comparison -
  - Benchmarking to Standards - How does it measure against COBIT?
  - Benchmarking to Peers - How does it compare to my peers?
  - Benchmarking to Self - How has it changed over time?

### Improved Control Assurance, Risk Management and Security

- Enhances Quality of Reviews - Standard and consistent baseline
- Saves Time - Easy to use tool
- Easy Access to Reference Material during Reviews
- Supports performance management of IT risk, control and security, establishing As-Is and To-Be positions, identifying gaps and defining implementation road maps.



September 26<sup>th</sup>, 2005

Presented by: **NEJAT AKSOY**

# CobiTOnline

## Product Objectives

- To provide an easily accessible online Library of CobiT materials and data
- To provide an interface for maintaining CobiT content and for implementing future version of COBIT content
- To include appropriate security features and obtain certification (e.g., WebTrust)
- To enable the capture of user data by authorized individuals
- To enable users to compare certain elements of client data against peer data
- To provide a method for Users to recommend changes to CobiT material
- To provide a capability to survey users on a variety of CobiT and governance related topics
- To enable users working together to share files
- To provide certain community features for users to share comments and experiences related to the control and use of CobiT and the governance of IT



September 26<sup>th</sup>, 2005

Presented by: **NEJAT AKSOY**

# CobiTOnline

## Product Overview

**A web-based, multi-user tool that is the front end for . . .**

Presentation of COBIT Material

Assessment against COBIT

Comparison of the result of self-assessments to Benchmarks of Peers

Surveys of Maturity and Practices

User Feedback - Process for Recommending Changes to COBIT Material

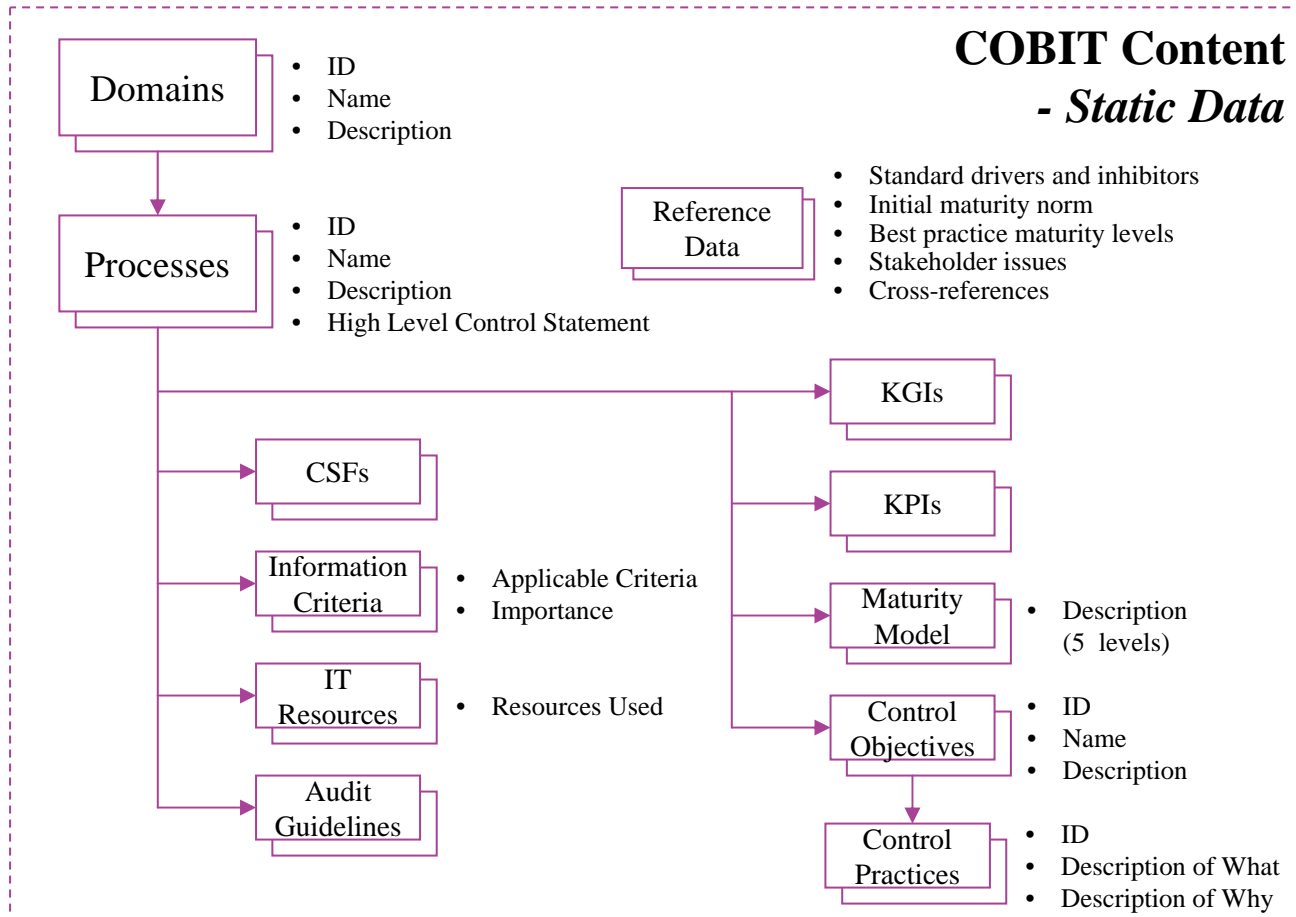
Performance improvement planning based on road maps and gap analysis



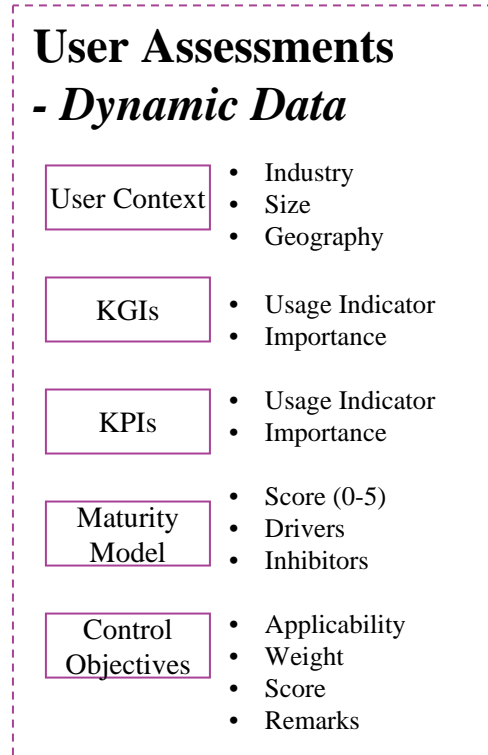
September 26<sup>th</sup>, 2005

Presented by: **NEJAT AKSOY**

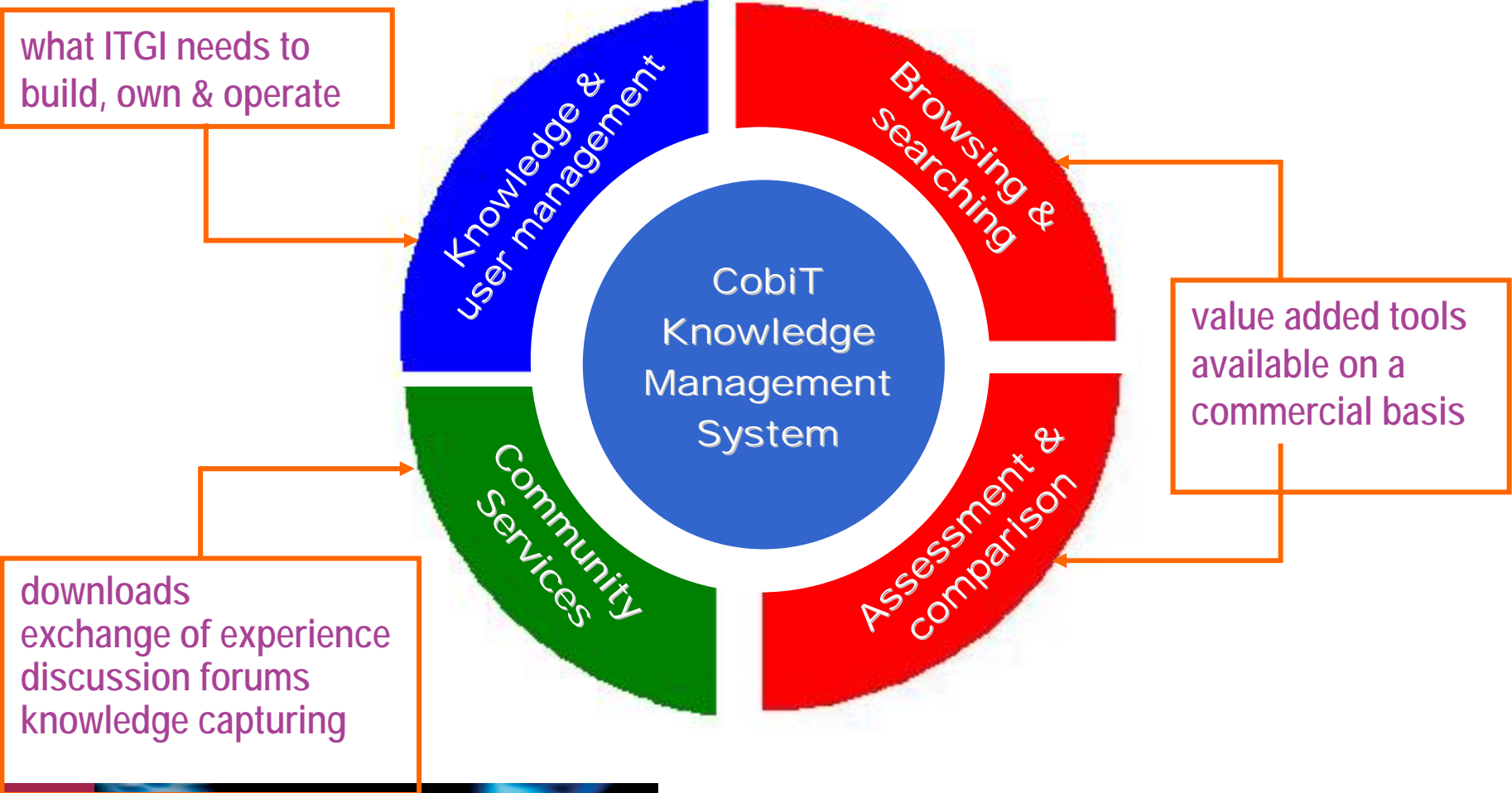
# CobiTOnline



## High Level Data Structure



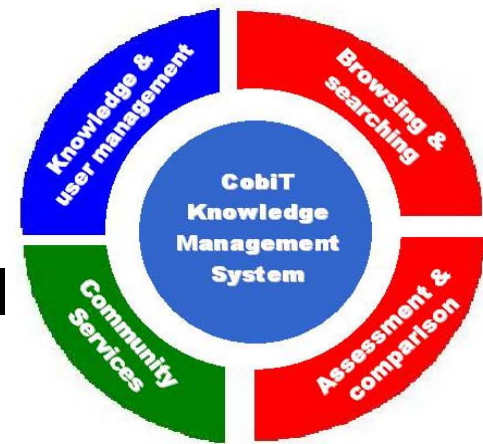
# CobiTOnline



# CobiTOnline

## Measures of Success

- Volume of usage
- Size of benchmark database
- Number of user-suggested and expert-approved updates to knowledge base
- Favorable reviews in trade and professional press
- Frequency, timeliness and cost-efficiency of CobiT releases



# The future of CobiT

## Agenda

- CobiT : An IT Control Framework
- CobiTIV Strategy
- Five Major Projects
  - IT Control Practices
  - Maturity Benchmarking
  - Implementation Guide
  - CobiT *Online*
  - CobiT *Lite*
- CobiT Examples

# CobiT : An IT control framework

## The most important IT Processes

34

15

7

Survey

PO1	define a strategic IT plan
PO3	determine the technological direction
PO5	manage the IT investment
PO9	assess risks
PO10	manage projects
AI1	identify solutions
AI2	acquire and maintain applications s/w
AI5	install and accredit systems
AI6	manage changes
DS1	define service levels
DS4	ensure continuous service
DS5	ensure system security
DS10	manage problems and incidents
DS11	manage data
M1	monitor the processes

# CobiTlite

## Early stages

- difference in control environment
- preselection of processes and objectives
  - 15 most important processes
  - 318 CO's down to 90 plus 15 simplified
- simple presentation form
- brainstorm approach

control

- short communications path
- effective span of control
- simple command structure
- less build, more buy
- less complex IT infrastructure
- less 'savvy' about IT
- take more risk
- strong profit orientation
- less segregation
- less IT capabilities

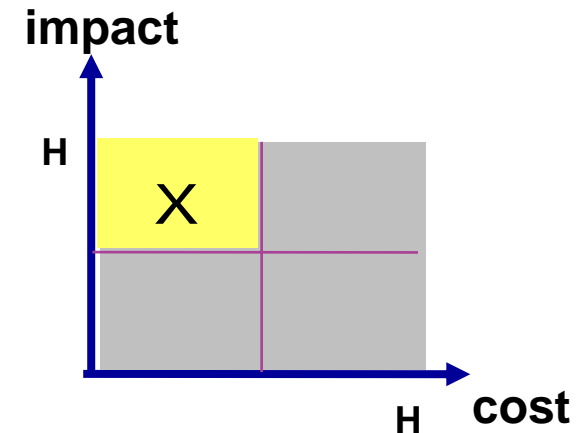
process

- PO1 define strategic IT plan
- PO3 determine technological direction
- PO5 manage the IT investment
- PO9 assess risks
- PO10 manage projects
- AI1 identify solutions
- AI2 acquire & maintain applications s/w
- AI5 install and accredit systems
- AI6 manage changes
- DS1 define service levels
- DS4 ensure continuous service
- DS5 ensure system security
- DS10 manage problems and incidents
- DS11 manage data
- M1 monitor the processes

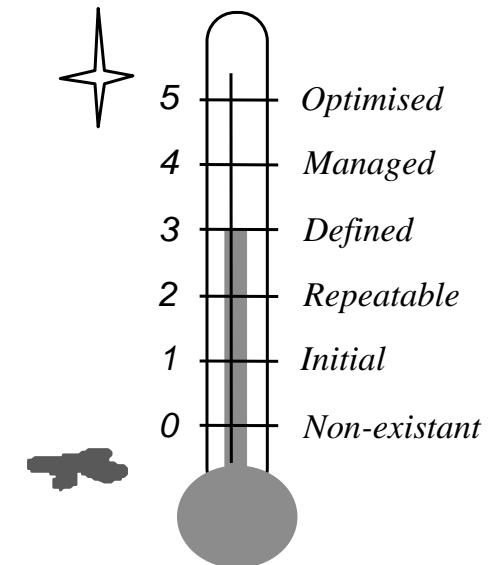
# CobiTlite

## Early stages

- ◆ 80/20 - 'smart things to do'
- ◆ high effectiveness, low cost and expedient
- ◆ 'mini' minimim baseline approach
- ◆ maximise at level 3

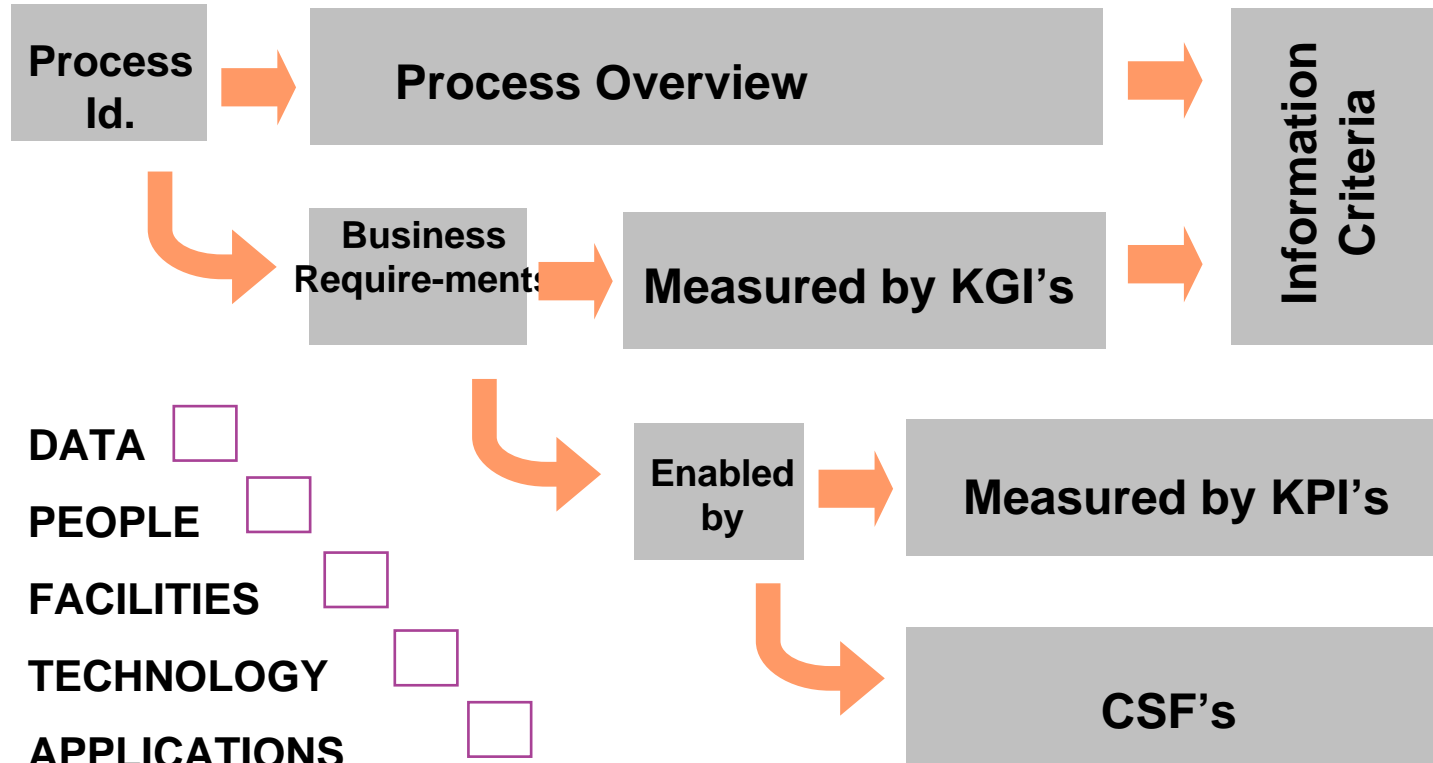


	Practice	Risk/Value	
PO9.5.4	When employees are given their account, they should be provided with initial or refresh-er training and awareness on computer security issues. They should be asked to review the rules and regulations for system access and confirm they have understood.	<ul style="list-style-type: none"> <li>• Ignorance of compliance requirements and sanctions leading to rules not being respected.</li> <li>• Ignoring rules that are too generic or descriptive</li> <li>• Absence of awareness leading to weak discipline</li> </ul>	effectiveness
			cost-efficiency
			expedience



# CobiTlite

## Presentation Form



# The future of CobiT

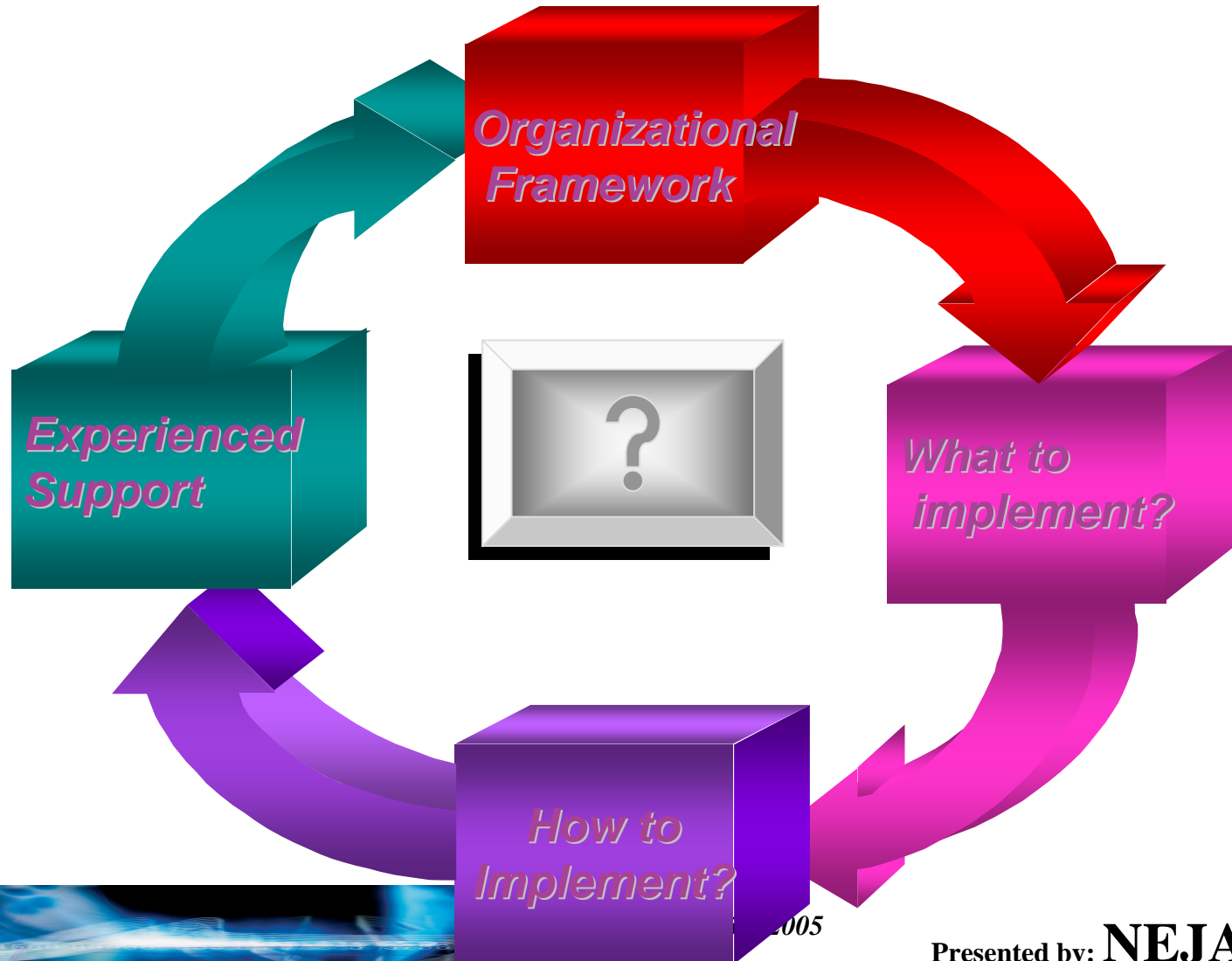
## Agenda

- CobiT : An IT Control Framework
- CobiTIV Strategy
- Five Major Projects
  - IT Control Practices
  - Maturity Benchmarking
  - Implementation Guide
  - CobiT *Online*
  - CobiT *lite*
- CobiT Examples

# CobiT is a very rich standard

- CobiT was developed by experts with extensive experience in many different industries
  - It includes all of the processes that can take place within an IT organization
  - It describes CSF's, KPI's, KGI's and processes that may not necessarily be relevant to a given organization's needs
  - Depending on the organization, attempting to implement the complete standard can cost more than the value created by a successful implementation
  - Cobit can be used to develop:
    - IT Governance
- As well as
- IT Audit

# CobiT should be adapted to the target organization's needs



# CobiT Framework Component To Implement

	CobiT Component	What for	Who cares?	
Strategic IT Audit	KPI, KGI	IT from to cost to profit	Board of Directors IT Directors	Audit Department
	Critical Success Factor	To evolve	Board of Directors IT Director	
	Maturity Model	Where to evolve	Board of Directors IT Director User Department	
Governance Model	Control objectives	Managing App'n System	User Department IT Director	
	Control objectives	Managing IT Processes	IT Director User Department	

September 26<sup>th</sup>, 2005

Presented by: **NEJAT AKSOY**

# What to implement

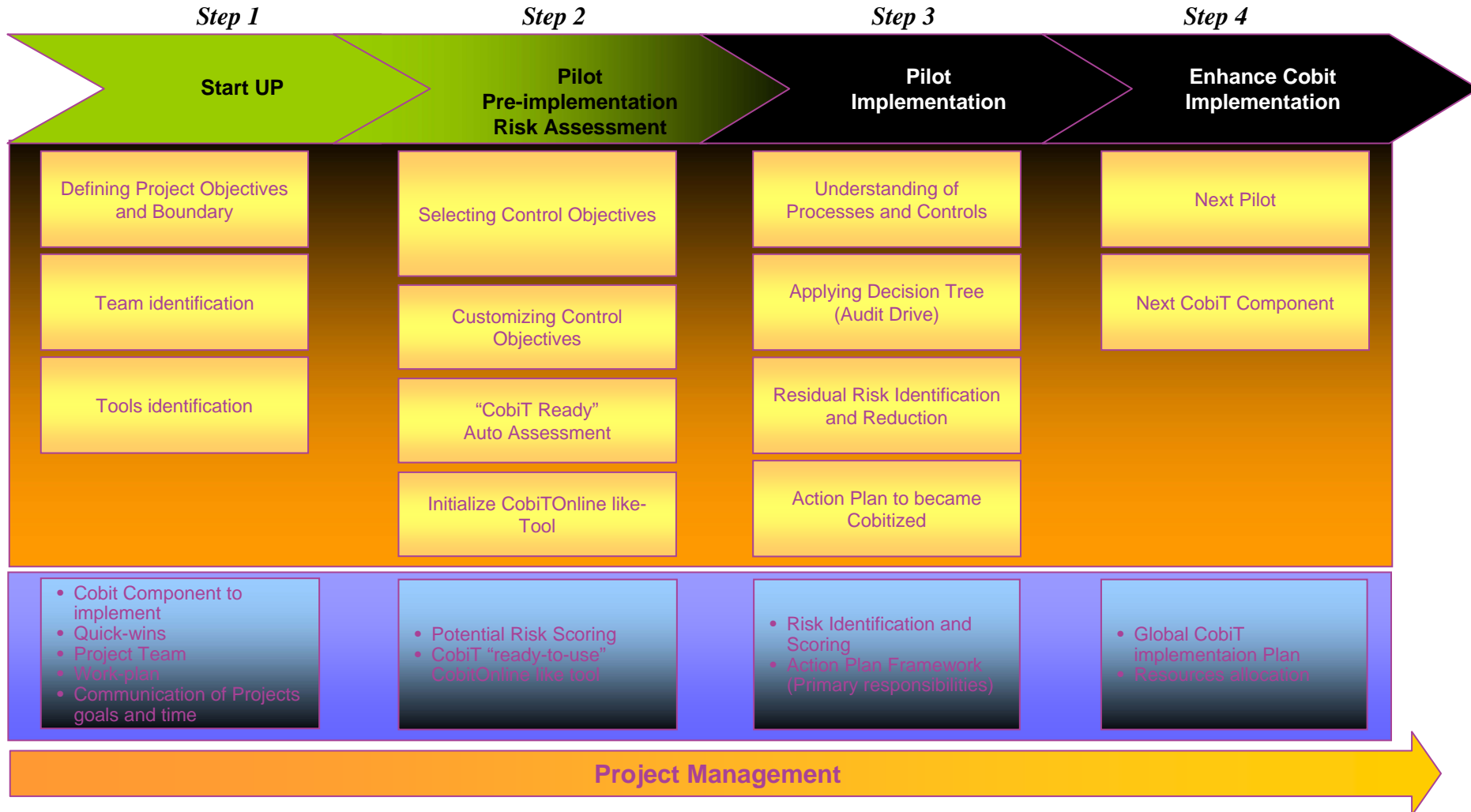
## Flat CobiT Implementation ?

- Large
- Time consuming
- Generic

## Value Added Implementation ?

- Quick-win oriented
- Organizational Specific** CobiT implementation (Value Added to the Organization)
- Tools** supported implementation (Value Added to Work to be performed)
  - Decisions Tree
  - Database Cobit Tool
  - Best Practices

# A limited CobiT implementation



# Why Outside Support?

To choose the component to start with

To guide the selection and the customizing of Control Objectives

To derive benefits from the integration of CobiT and other tools

- Drivers to guide Audit/Governance Activities (Decision Tree)
- Direct access to reference material (Best Practices)
- CobiTOnline like Cobit Tool to serve as repository for collecting and documenting Activities
- Balanced and tested Work Programs to perform Audit/Governance activities

To compare YOUR implementation to others

To have both Local Experts and International Experts

To help you to implement CobiT as more than an Audit tool

# Some CobiT Examples



*September 26<sup>th</sup>, 2005*

Presented by: **NEJAT AKSOY**

# Telco CobiT IT Audit Approach (Very Limited)

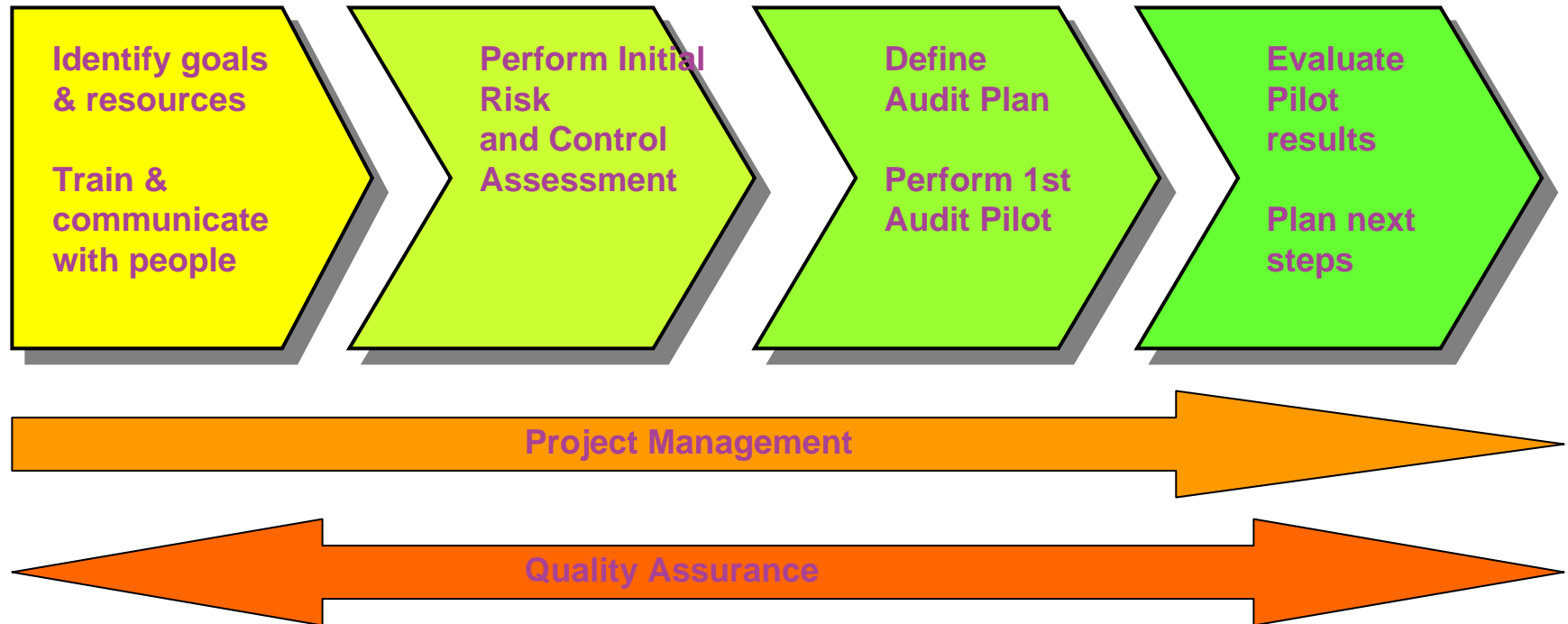


# Telco CobiT IT Audit Approach (Very Limited)

CobiT Procss	Telco Processes to be Audited	CobiT Process Description	Audit Difficulty	Process Improvement Possibility	Activities	Audit Duration and Manpower
DS3	Rating - Billing	Manage Performance and Capacity	Max	Max	CSF, KPI, KGI Assessments Sun E10000 System Performance Testing	2 Weeks - 1 Auditor
DS4	Rating - Billing	Ensure Continuous Service	Max	Max	CSF, KPI, KGI Assessments, Network Testing	1 Week- 1 Auditori
DS5	Rating - Billing	Ensure Systems Security	Max	Max	CSF, KPI, KGI Assessments Network ve Unix System Security Testing	2 Weeks - 2 Auditors



# Bank CobiT IT Audit Approach (Very Detailed)



# Some Deliverables

## Strategic IT & Audit Stream

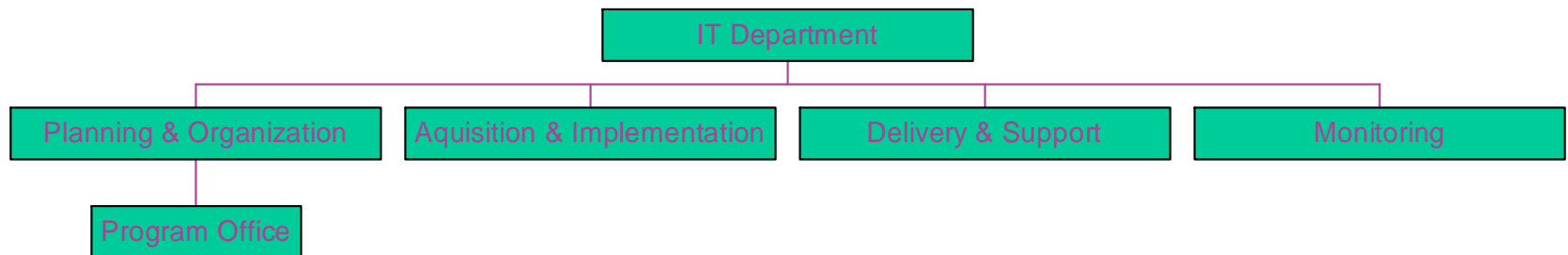
- Migration Plan and Guidelines on “How to further COBITize” the organization, with actions and milestones, defining the key players and their roles
- IT Audit and Control Handbook (within the CobiTOnline like Tool) and related documentation (to be further developed within and after the commencement of the project).
- Audit and Findings Report Templates
- Checklists and Tools which are of Global Best Practice nature and COBIT compatible to be adopted according to prior project phases and steps
- Documentation describing the future IT Audit function (the approach, organization and monitoring) with the required IT Audit and Control capabilities and capacity requirements
- Clear definition of career path for the Audit professionals
- Documented ISACA and CISA exam knowledge base with major points to be addressed within the “Prospective IT Auditors” training sessions
- IT Auditor Training Plan and Recommendations

# Bank CobiT IT Audit Approach (Very Detailed)

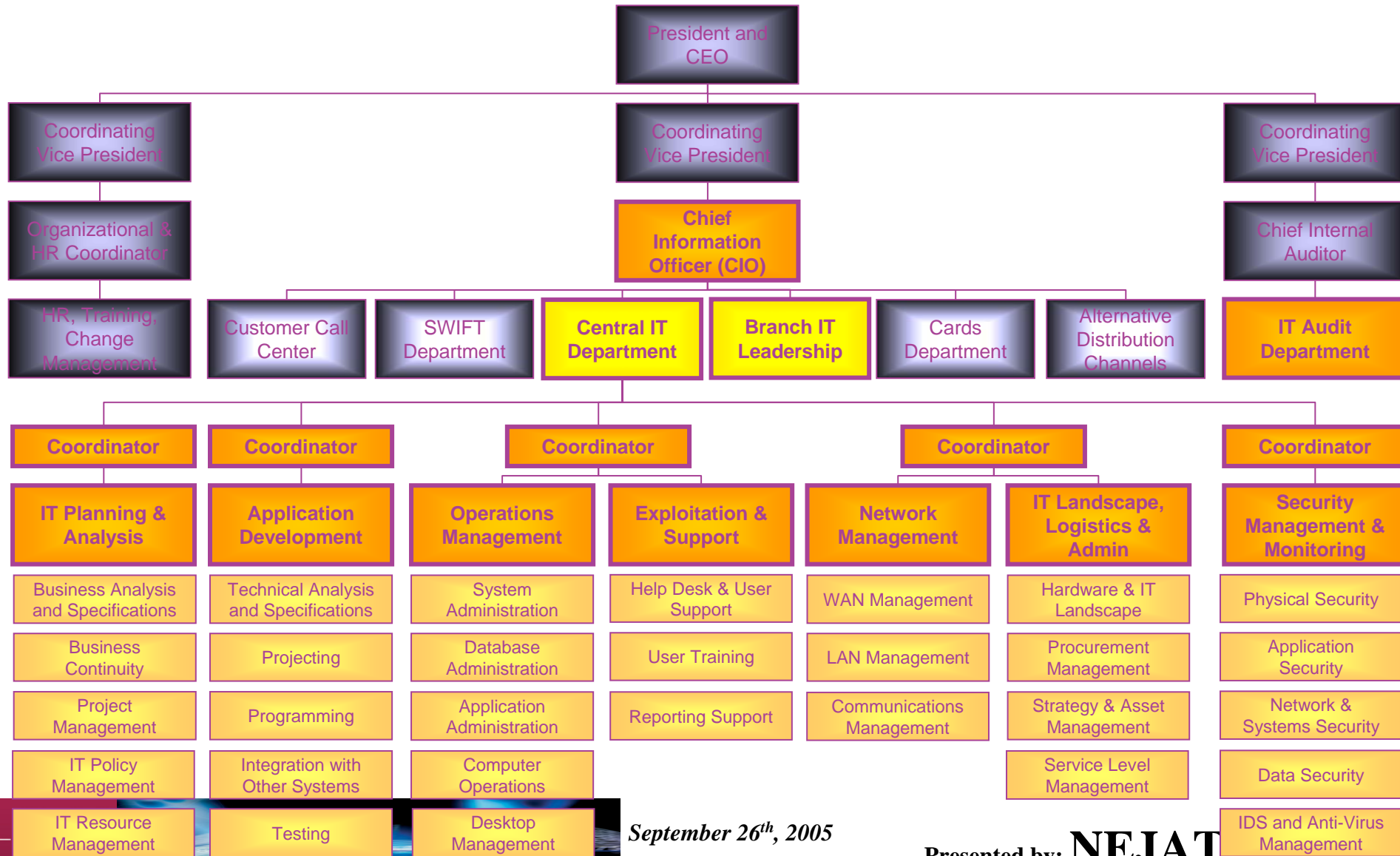
Process Definitions		Quick Wins	Short Term (lower impact)	Short Term (lower likelihood of success)	Long Term
PO01	Define a Strategic IT Plan	PO01R3	PO01R1	PO01R4	PO01R2
PO02	Define the Information Architecture			PO2R1,PO2R2	PO2R3,PO2R4
PO03	Determine Technological Direction	PO3R1	PO3R4	PO3R2	PO3R3, PO3R5
PO04	Define the IT Organisation and Relationships		PO4R2	PO4R1, PO4R3, PO4R4	
PO05	Manage the IT Investment	PO5R1			PO5R2, PO5R3, PO5R4
PO06	Communicate Management Aims and Direction		PO6R3	PO6R2	PO6R1

# Bank CobiT Based IT Organization Governance Model - Project Approach

Objectives and targets presented above require us to identify, build, and implement the most optimal and most feasible organizational model for the Bank IT organization (referred to as “best fit”). In order to accomplish this target, we have developed a 5-phase approach:



# Bank CobiT Based IT Organization Governance Model – Preliminary To-Be Organization

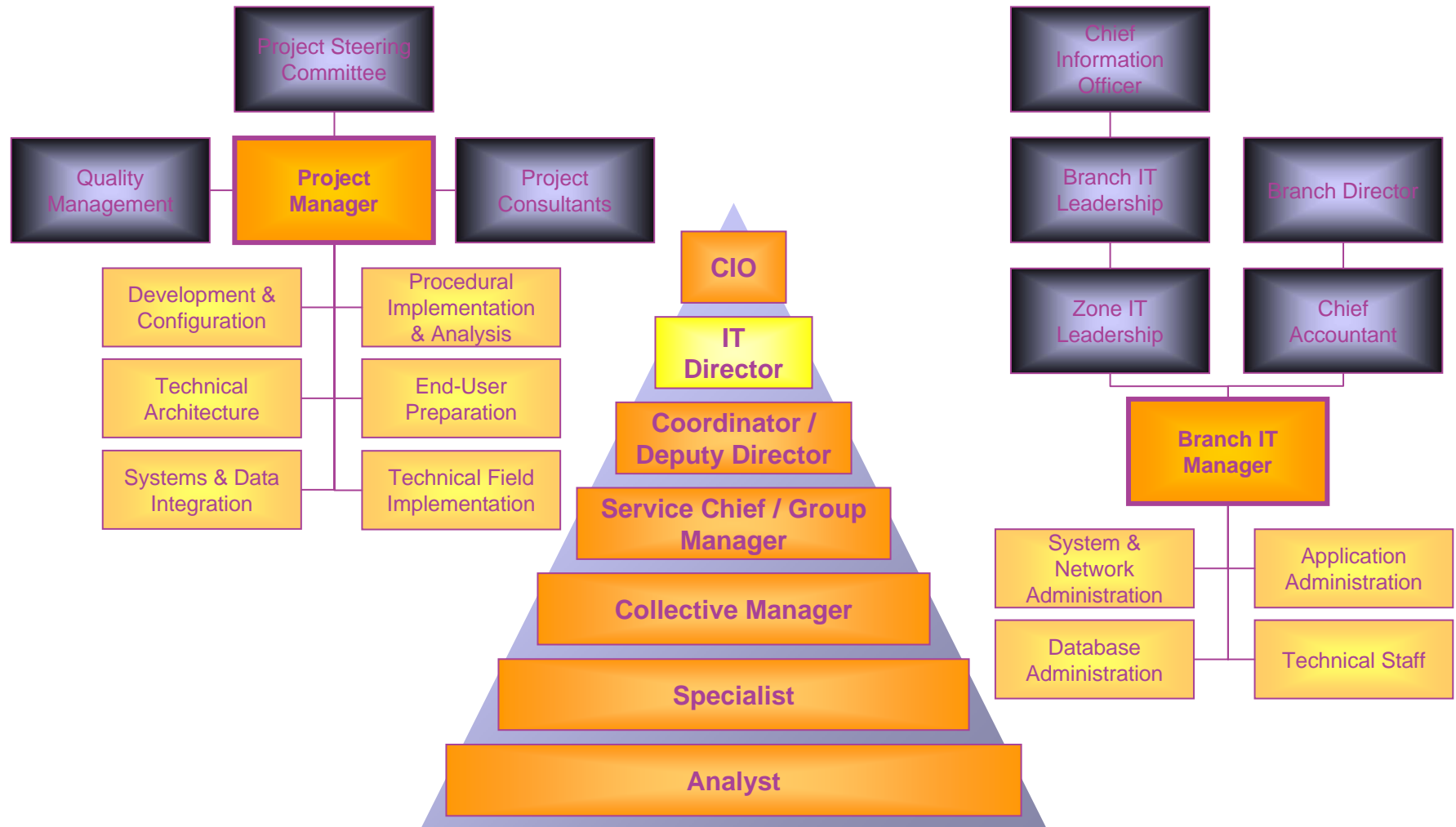


September 26<sup>th</sup>, 2005

Presented by: **NEJAT**



# Bank CobiT Based IT Organization Governance Model – Preliminary To-Be Organization



# To Reach Me For More Information

## Nejat Aksoy

Manager

Ernst & Young US

Nejat.aksoy@ey.com

+1 (408) 947 4953

 **ERNST & YOUNG**

*Quality In Everything We Do*



September 26<sup>th</sup>, 2005

Presented by: **NEJAT AKSOY**