COBIT

Facteur de réussite du projet de mise en conformité

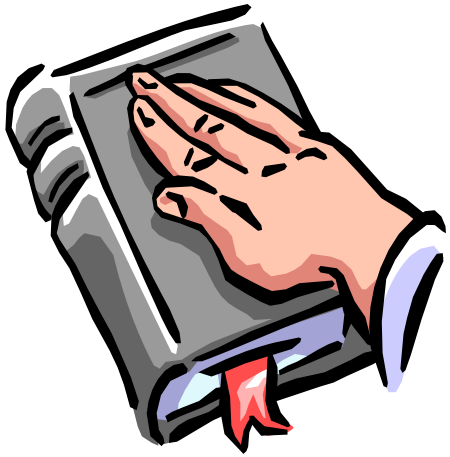
SOX

4 ème Symposium IT Governance
18 mai 2006

Patrick Dewulf
Directeur IS Governance

The ultimate objective for 2006 year end

SOX section 404
Management Assessment of Internal Control

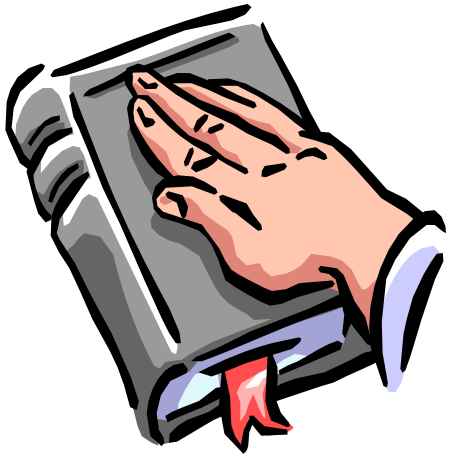


Management must prepare an annual report on internal controls over financial reporting

- Management must assert adequacy (design and efficiency) of internal controls
- Independant auditor must attest to management's assertion

Franck Riboud and Antoine Giscard d'Estaing will have to sign an attestation evaluating internal control and material weaknesses if any.

The ultimate objective for 2006 year end



SOX section 404
Annual Report Must Include

- **A recognition of management's responsibility for ….. Adequate internal controls**
- **Framework used to evaluate internal controls (COSO, COBIT,.)**
- **Management's assessment … as of the year-end-date**
- **The independant auditor's opinion on management's conclusion on … internal controls**
- **Any material weaknesses must be disclosed**
- **Changes that materially affected the control environment must be considered**

WE KNOW WE OPERATE SECURELY ALMOST EVERYWHERE

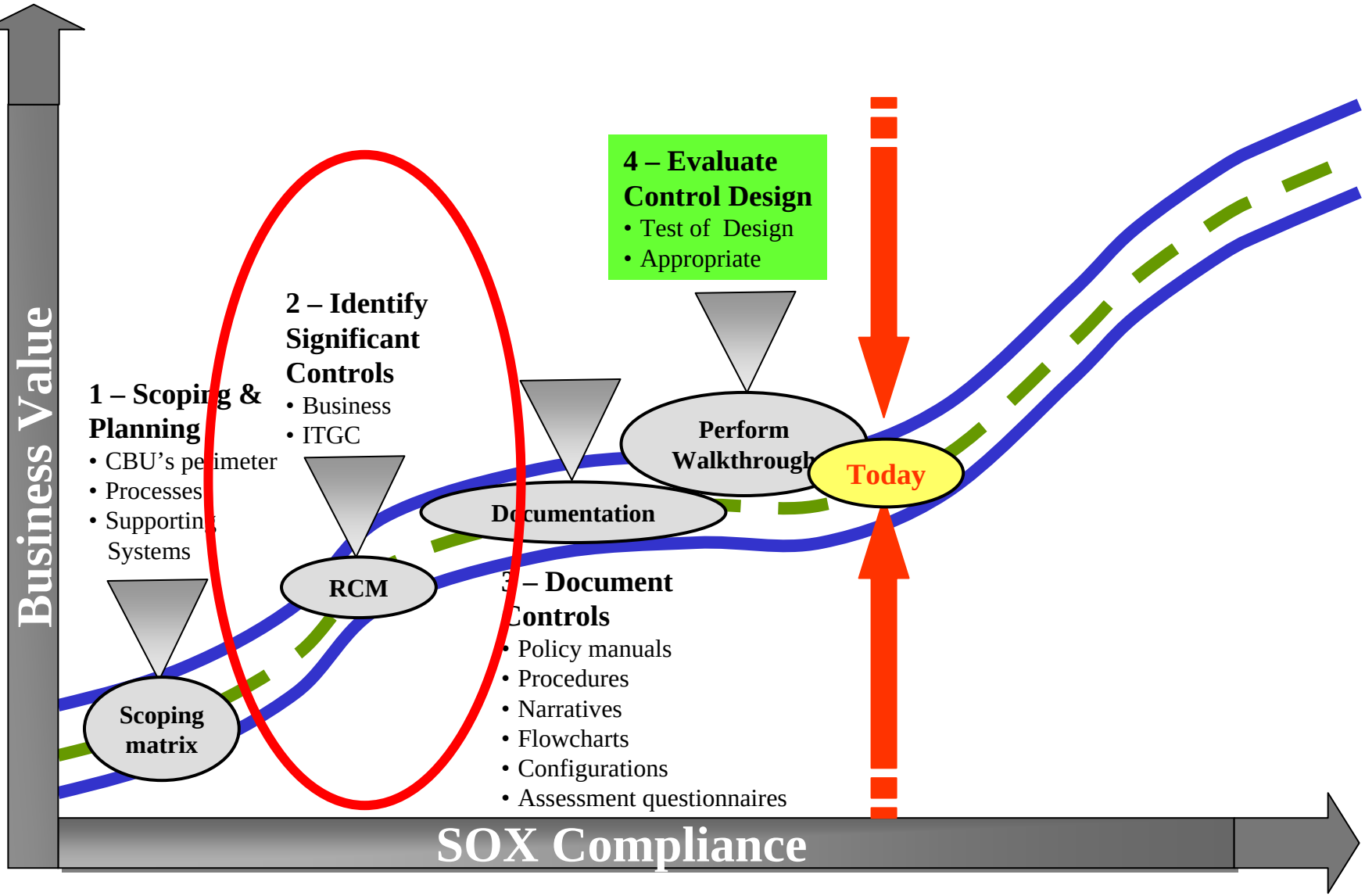
BUT SOX ASK US

- **TO DEMONSTRATE IT (tests of design)**
- **TO PROVE IT (test of operational efficiency)**

HOW ?

Project Road Map

COBIT & SOX



For IT, critical success factors are :

COBIT & SOX

The Company IT Framework used to evaluate internal controls

A common language with external auditors

Be sure all risks & control objectives are addressed

Simple to deploy, appropriation by local teams is key !

Execution

Appropriation by IT Top Management

Management

The starting point :

(As recommended by our Partner)

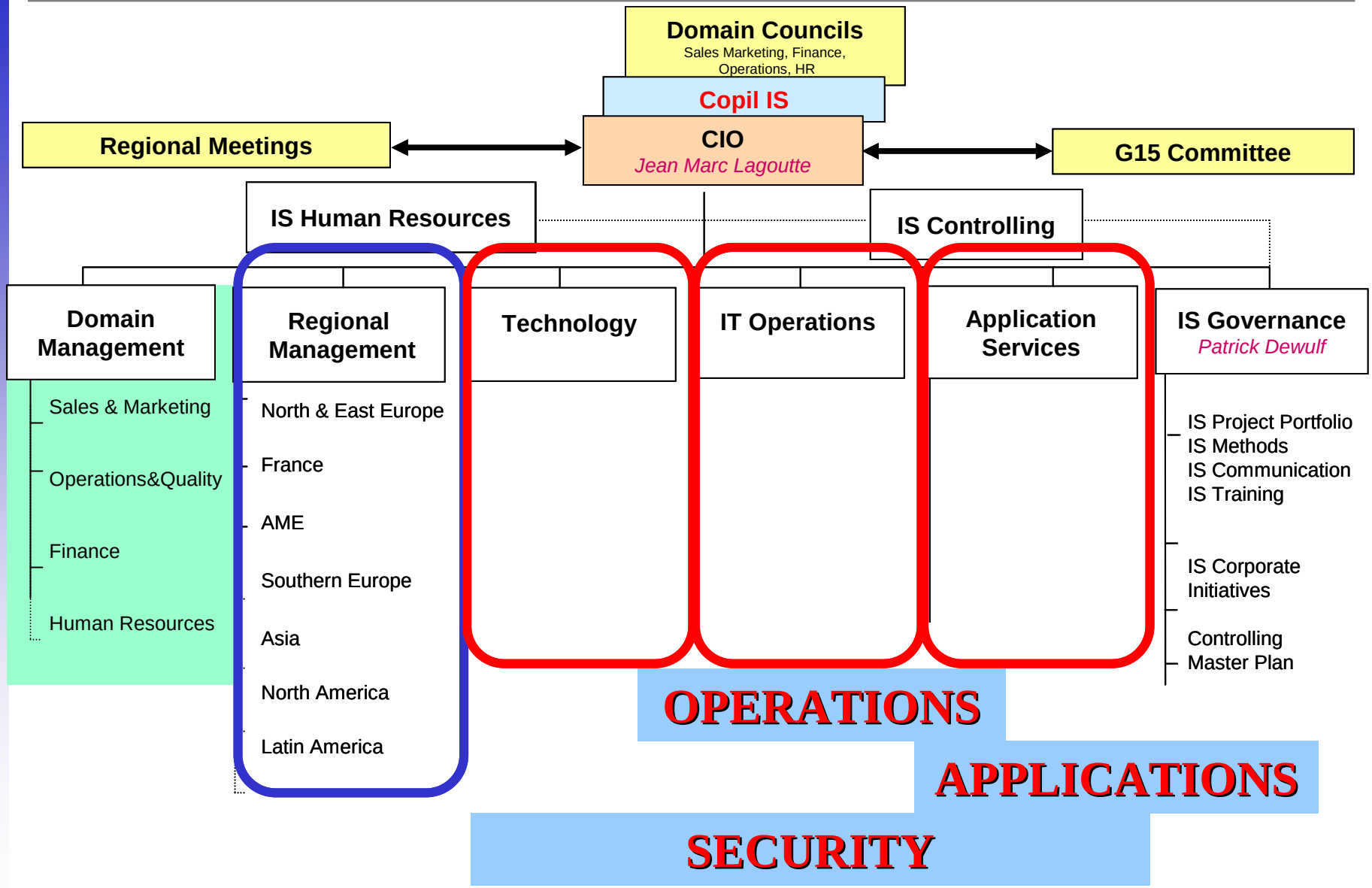
COBIT – IT Control Objectives for Sarbanes-Oxley

Danone IT Organisation

COBIT & SOX

IT Organisation

COBIT & SOX



Danone ITGC Framework

Internal Control within DANONE

COBIT & SOX

- Internal Control is not a new concept, it is already part of every aspects of your day to day business.
- It includes all systems you have built to organize, supervise and report on your activities : job descriptions and training programs of your managers, IT systems you use, reporting and procedures you have defined are for example, key elements of the quality of internal control of your department.
- According to COSO* standards, the official internal control framework chosen by Danone, Internal Control is a process supported by the DICE system, validated by Management designed to provide reasonable assurance regarding the achievement of objectives in the following categories:
  - ➔ Reliability of Financial Reporting
  - ➔ Effectiveness and Efficiency of Operations
  - ➔ Compliance with Applicable Laws and Regulations
- * COSO (Committee of Sponsoring Organizations of The Treadway Commission) - September 1992

Since 2002, DICE
Danone Internal Control Environnement

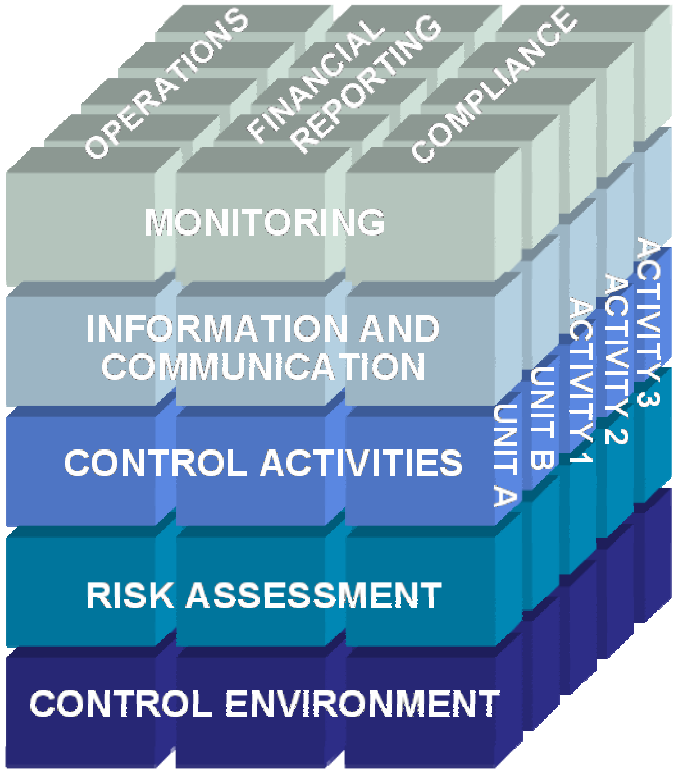
The COSO Framework

Objectives:

What is Danone achieving to control through its internal controls?

Components:

What are the different elements of internal control?

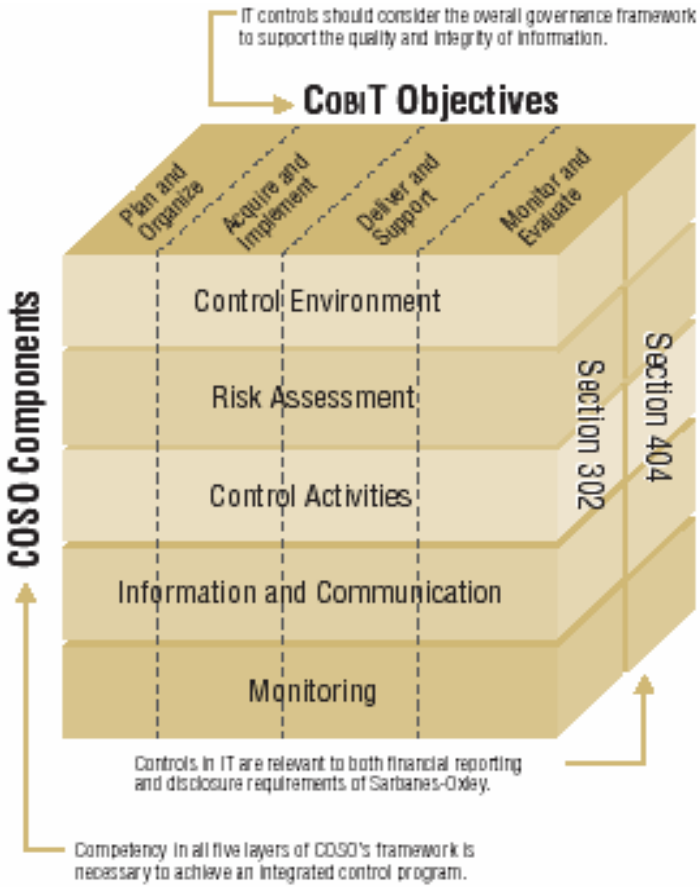


Scope:

Where should Danone evaluate its controls?

IT teams are not familiar with these concepts !!

COBIT, a model for IT people



- CobiT (Control Objectives for Information Related Technology)
- Framework developed and published by IT Governance Institute (ITGI)
- Partnered with Information Systems Audit and Control Association (ISACA)
- 34 IT Processes
- 318 detailed Control Objectives

COBIT has to be mapped against COSO

COBIT to COSO

COBIT Processes to COSO Components mapping

COBIT Processes			COSO Component: Control Environment	Risk Assessment	Control Activities	Information and Communication	Monitoring
PO1	Define a Strategic IT Plan	IT strategic planning is required to manage and direct all IT resources in line with the business strategy and priorities. The ITfunction and business stakeholders are responsible for ensuring that optimal value is realised from project and service portfo		P		S	S
PO2	Define the Information Architecture	The information systems function should create and regularly update a business information model and define the appropriatesystems to optimise the use of this information. This encompasses the development of a corporate data dictionary with theorganisatio			P	P	
PO3	Determine Technological Direction	The information services function should determine the technology direction to support the business. This requires the creation of atechnological infrastructure plan and an architecture board that sets and manages clear and realistic expectations of what		S	P	S	
PO4	Define the IT Processes, Organisation and Relationships	An IT organisation must be defined considering requirements for staff, skills, functions, accountability, authority, roles andresponsibilities, and supervision. This organisation is to be embedded into an IT process framework that ensures transparency and	P			S	S
PO5	Manage the IT Investment	Establish and maintain a framework to manage IT-enabled investment programmes that encompasses cost, benefits, prioritisationwithin budget, a formal budgeting process and management against the budget. Work with stakeholders to identify and control thetot		S	P		
PO6	Communicate Management Aims and Direction	Management should develop an enterprise IT control framework and define and communicate policies. An ongoing communicationprogramme should be implemented to articulate the mission, service objectives, policies and procedures, etc., approved andsupported b	P			P	

COSO Components

Control Activities will be documented almost through RCMs

Other COSO Components will be documented through DICE IT for SOX Questionnaire and the Company Level report prepared at the Group level

Source COBIT™

How to map COBIT processes for SOX

- As recommended by the PCAOB (corporation created by the Sarbanes Oxley act to oversee the auditors of public companies), Danone designed its response to the Sarbanes Oxley act arround the three following processes :

  - ➔ **Security Management**
  - ➔ **Operations Management**
  - ➔ **Program Change Management**

- We mapped corresponding COBIT processes accordingly

Documentation Standards
Risk Based Approach

We have identified, based on the COBIT and the corresponding **control objectives**, a set of **key IT risks** that Danone had to face for Sarbanes Oxley purposes.

For each risk, we have defined a set of standard controls that mitigate those risks. Those controls could be of different levels:

- **Entity and Company level controls**: high level controls related mainly to IT governance, guidance, policies, control environment and IT organization.
- **CBU level controls**: key controls that are operated at the CBU level, or operated once for the whole CBU.
- **Application, OS and database level controls**: controls aiming at controlling the IT processes from the initial stages of the need of modification of an application, to managing operations, security and access rights.

Starting from COBIT Control objectives

Domain : Acquire & Implement
Process : Acquire and Maintain Application Software
Activity : Development of Application Software

AI2	Acquire and Maintain Application Software	Applications have to be made available in line with business requirements. This process covers the design of the applications, theproper inclusion of application controls and security requirements, and the actual development and configuration according to	AI2.5	Configuration and Implementation of Acquired Application Software	Customise and implement acquired automated functionality using configuration, acceptance and testing procedures. Issues toconsider include validation against contractual terms, the organisation's information architecture, existing applications,interoperab
AI2	Acquire and Maintain Application Software	Applications have to be made available in line with business requirements. This process covers the design of the applications, theproper inclusion of application controls and security requirements, and the actual development and configuration according to	AI2.6	Major Upgrades to Existing Systems	Follow a similar development process as for the development of new systems in the event of major changes to existing systems thatresult in significant change in current designs and/or functionality. Issues to consider include impact analysis, cost/benefit
AI2	Acquire and Maintain Application Software	Applications have to be made available in line with business requirements. This process covers the design of the applications, theproper inclusion of application controls and security requirements, and the actual development and configuration according to	AI2.7	Development of Application Software	Ensure that automated functionality is developed in accordance with design specifications, development and documentationstandards and quality requirements. Approve and sign off on each key stage of the application software development processfollowing suc
AI2	Acquire and Maintain Application Software	Applications have to be made available in line with business requirements. This process covers the design of the applications, theproper inclusion of application controls and security	AI2.8	Software Quality Assurance	Develop, resource and execute a software quality assurance plan to obtain the quality specified in the requirements definition andthe organisation's quality policies and procedures. Issues to consider in the quality assurance plan include specification of

WHAT IS THE RISKS AGAINST THE CONTROL OBJECTIVE ?

And define the risk and the Company Control (s) to mitigate the risk

COBIT & SOX

Risk Names	Risk	Sub-process	Control reference	Control Names	Control standard description
Unauthorized program changes	Changes made to applications are not authorized, valid and approved prior to being placed into the Production environment.	Program development & change	ITC18	Change management procedure based on a change request form	All changes to Sox critical applications/systems are managed according to strict management rules. The change request form includes : - formal specification approval by the users - technical validation - documentation update - adequate testing - formal acceptance by the users before going live - transfer request to production

As a result we defined 40 key controls

COBIT & SOX

Summary	
Nb of ressources	3
Nb of hints CBU Level	12
Total Nb of hints	89

CBU

CBU Level

LOCAL Applications

Treasury Mana | Payroll HR Acc | Time

CBU Level Controls

Local Application Level Controls

S

Op

Pr
C

CENTRAL Applications

SAP Themis

Central Application Level Controls	Security	ITC03	User account management procedure	x
		ITC04	Periodical reviews of access rights	x
		ITC05	Administrator rights limited to restricted number of personnel	x
	Operations	ITC14	Job scheduling approval	x

Operating Systems

Windows

OS Level Controls	Security	ITC01	System default passwords changes	x
		ITC02	Operating systems patches installation and follow-up	
		ITC03	User account management procedure	x
		ITC04	Periodical reviews of access rights	x
		ITC05	Administrator rights limited to restricted number of personnel	x
		ITC07	ID/Password authentication	x
		ITC08	Password constraints	x

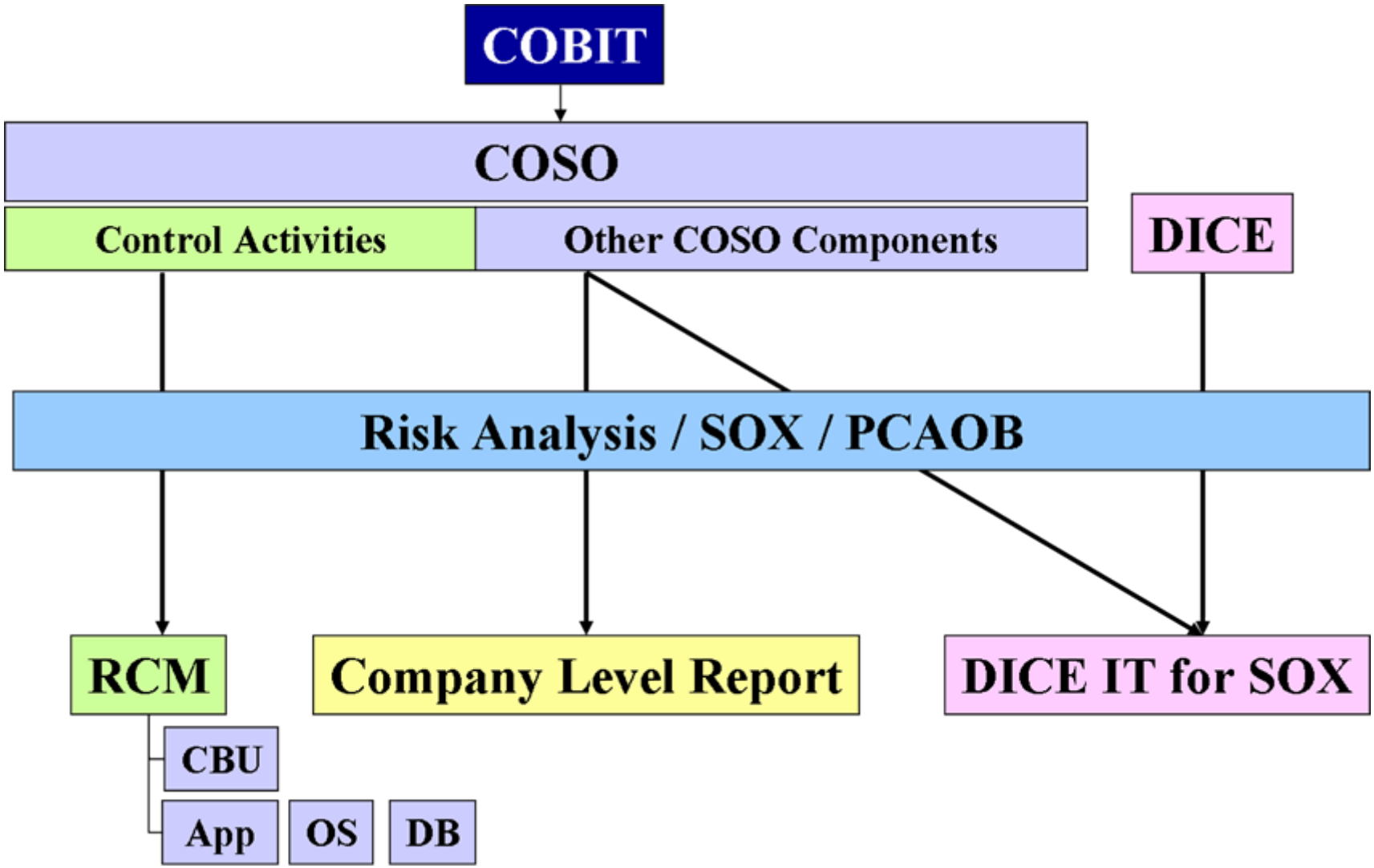
Databases

Oracle

DB Level Controls	Security	ITC01	System default passwords changes	x
		ITC02	Operating systems patches installation and follow-up	
		ITC03	User account management procedure	x
		ITC04	Periodical reviews of access rights	x
		ITC05	Administrator rights limited to restricted number of personnel	x
		ITC07	ID/Password authentication	x
		ITC08	Password constraints	x

ITGC Documentation

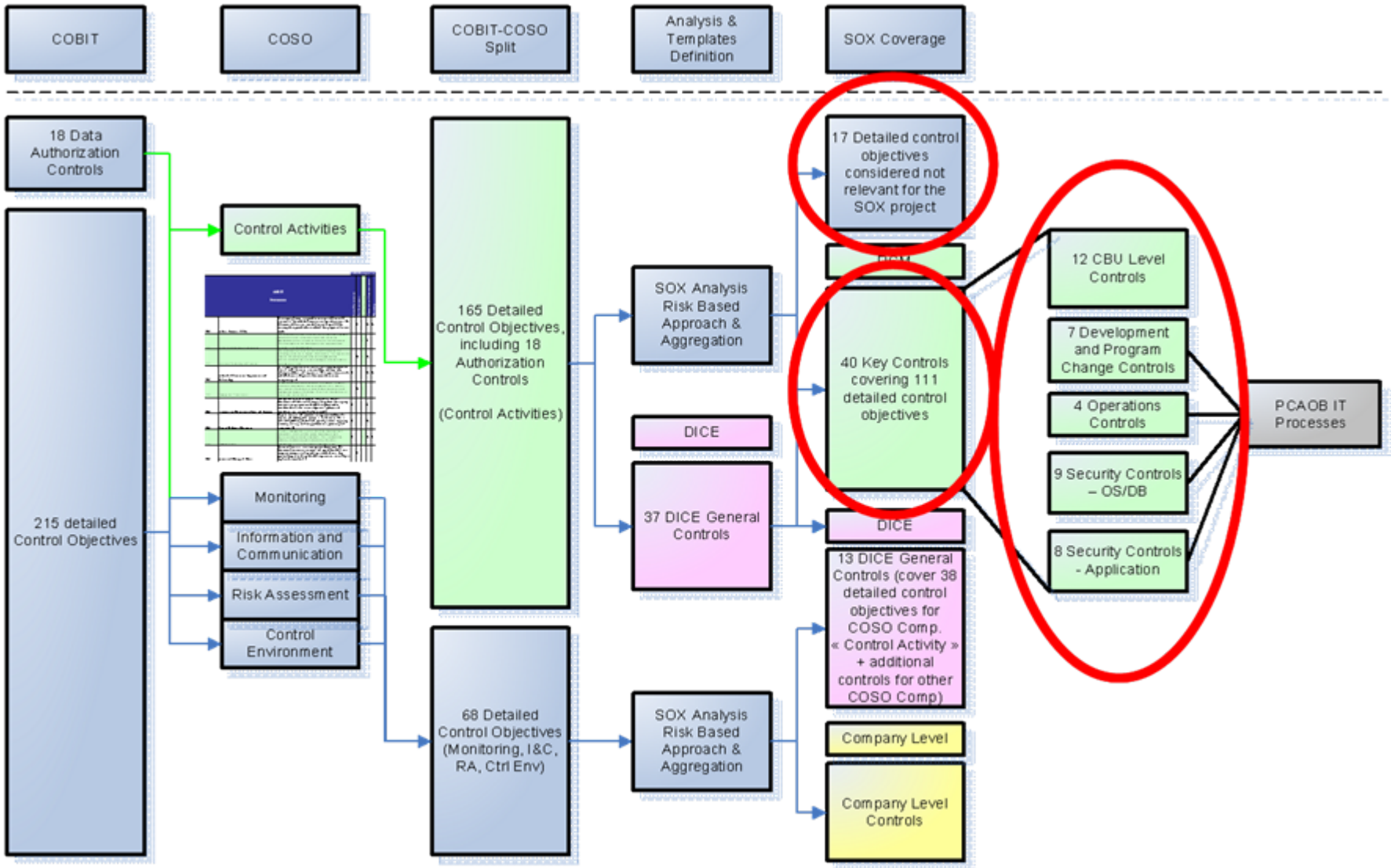
Documentation standards definition process



IT GC Documentation

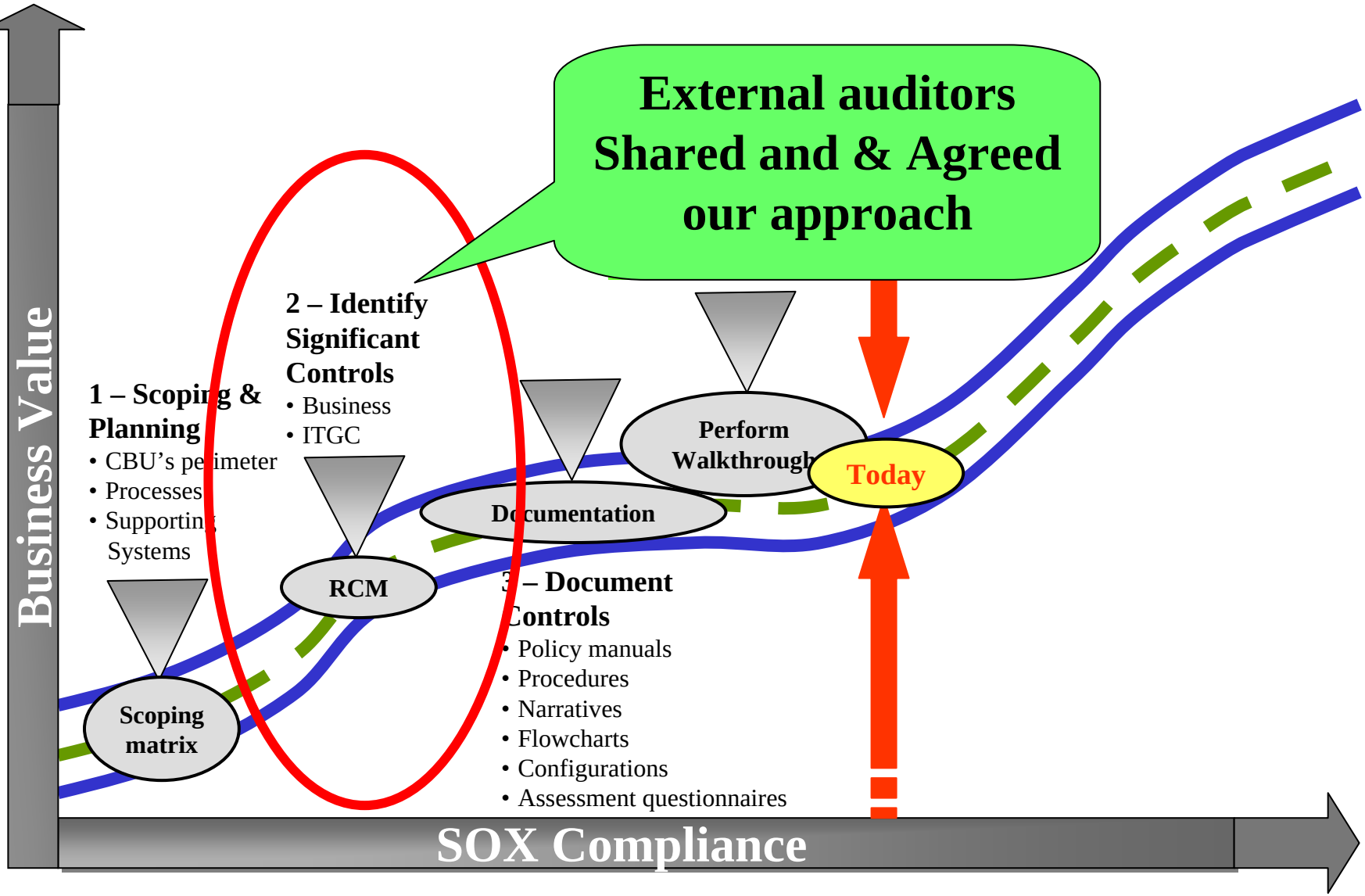
Documentation Standards Definition Process

COBIT & SOX



Project Road Map

COBIT & SOX



For IT, critical success factors are :

COBIT & SOX

The Company IT Framework used to evaluate internal controls

A common langage with external auditors

Be sure all risks & control objectives are adressed

Simple to deploy, appropriation by local teams is key !

Execution

Appropriation by IT Top Management

Management

Domain readiness

COBIT & SOX

Control type	Control reference	Control Names	Ready	Scope
CBU Level controls	ITC24	Firewall	84%	25
	ITC25	Public servers in DMZ	84%	25
	ITC26	Inbound connections secured by VPN	72%	25
	ITC27	E-mail filtering gateway	68%	25
	ITC28	**Project Management methodology**	**52%**	**25**
	ITC29	Anti-virus software	80%	25
	ITC30	**Termination procedure**	**48%**	**25**
	ITC32	Physical security policy	56%	25
	ITC36	Smoke and heat detectors. Fire extinguishing devic	80%	25
	ITC37	Air conditionning	80%	25
	ITC38	Power supply safeguarded by UPS	88%	25
			72%	**275**
Dev & change controls	ITC17	Standard application documentation	70%	115
	ITC18	Change management procedure based on a change	66%	115
	ITC19	Program Testing	63%	115
	ITC20	User documentation	73%	115
	ITC21	Transfer to production	67%	115
	ITC22	Application patches follow-up	75%	115
	ITC23	Service contract	79%	115
			70%	**805**
Operations controls	ITC13	Operations documentation	64%	115
	ITC14	Job scheduling approval	76%	115
	ITC15	Job & backup execution monitoring	70%	115
	ITC16	Incident tracking, follow-up and escalation procedu	72%	115
			70%	**460**
Security controls	ITC01	System default passwords changes	71%	171
	ITC02	**Operating systems patches installation and fol**	**39%**	**56**
	ITC03	User account management procedure	60%	242
	ITC04	**Periodical reviews of access rights**	**51%**	**242**
	ITC05	Administrator rights limited to restricted number of	74%	167
	ITC07	ID/Password authentication	75%	166
	ITC08	Password constraints	64%	166
	ITC10	Backup procedures	70%	115
	ITC12	Restore procedure and testing	71%	115
			65%	**1 440**
Total			**68%**	**2 980**

Appropriate by Region

COBIT & SOX

Control type	Region	Ready	Scope
CBU Level controls	Region 1	68%	44
	Region 2	97%	33
	Region 3	66%	77
	Region 4	59%	22
	Region 5	64%	44
	Region 6	86%	22
	Region 7	76%	33
		72%	**275**
Dev & change controls	Region 1	49%	49
	Region 2	89%	126
	Region 3	69%	231
	Region 4	64%	70
	Region 5	73%	126
	Region 6	83%	112
	Region 7	**45%**	**91**
		70%	**805**
Operations controls	Region 1	79%	28
	Region 2	89%	72
	Region 3	71%	132
	Region 4	70%	40
	Region 5	76%	72
	Region 6	78%	64
	Region 7	**21%**	**52**
		70%	**460**
Security controls	Region 1	53%	74
	Region 2	83%	184
	Region 3	72%	469
	Region 4	**29%**	**124**
	Region 5	74%	243
	Region 6	71%	172
	Region 7	**36%**	**174**
		65%	**1 440**
Total		**68%**	**2 980**

COBIT

Facteur de réussite du projet de mise en conformité

SOX

4 ème Symposium IT Governance
18 mai 2006