REVIEW IT-GOVERNANCE

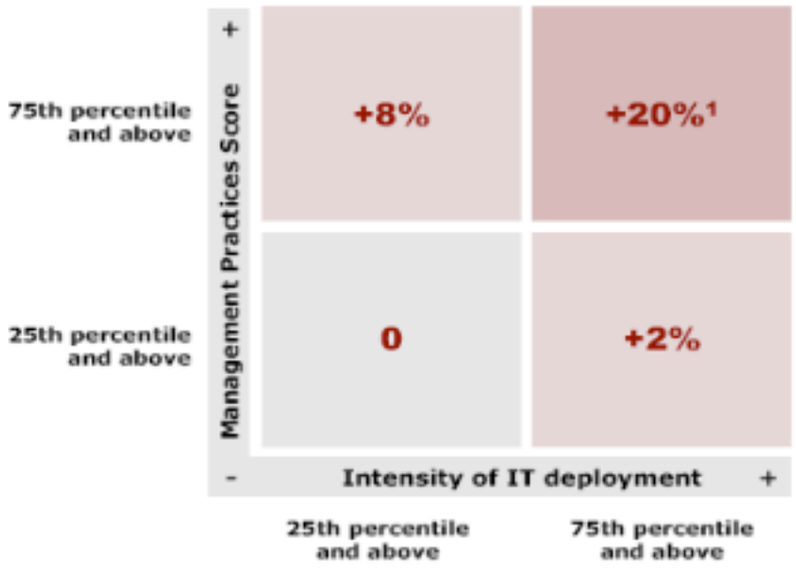
Dr. Ir. Yeffry Handoko Putra, M.T.

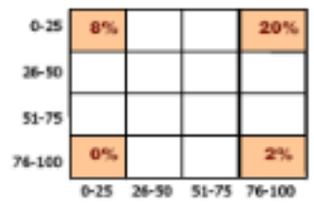
Presentation Outline

1. Introduction
2. IT Governance Framework
3. IT Governance Implementation
4. Control Framework for SOX
5. Using CobiT for C/SOX
6. Issues in Application Controls
7. Questions

What Makes IT Governance so important?

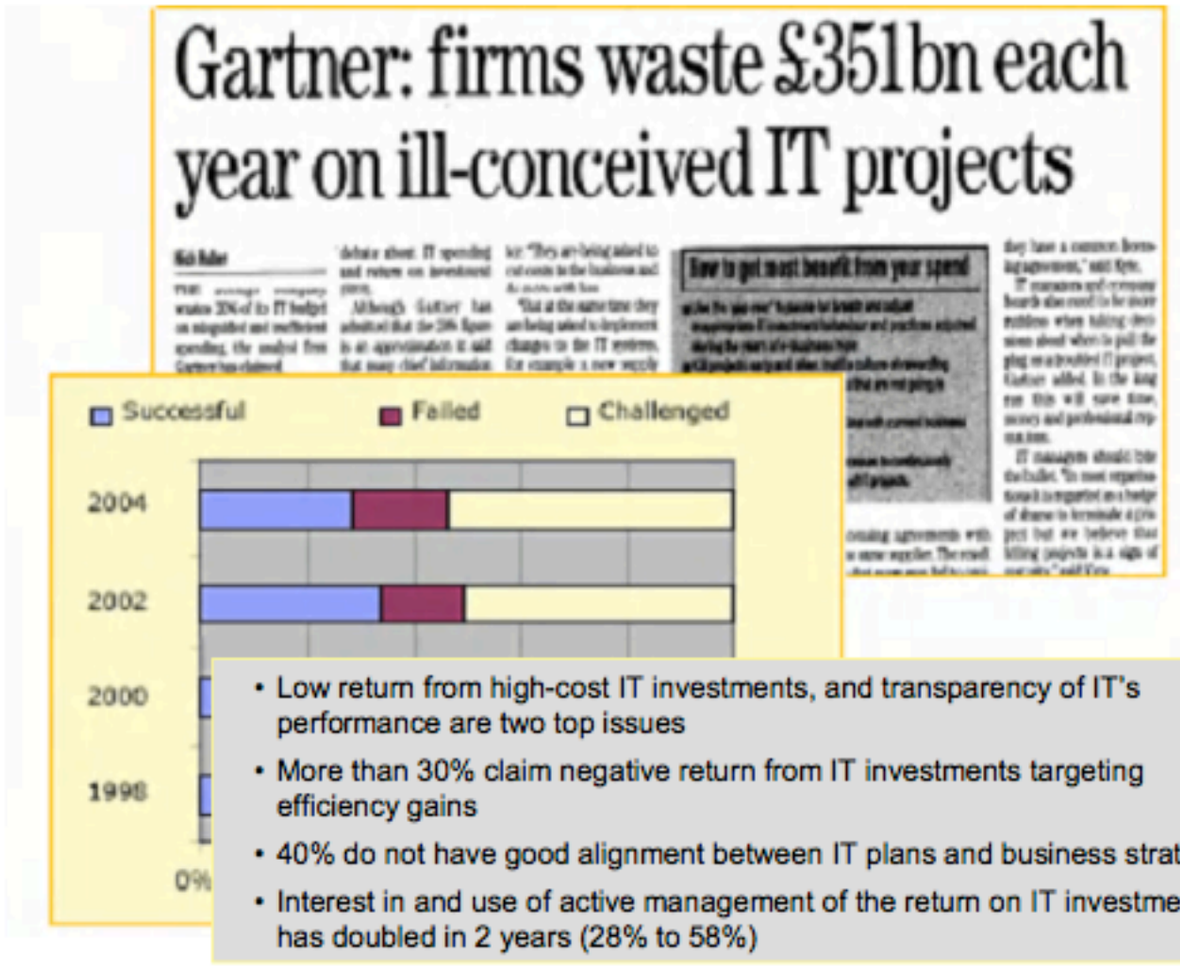
In October 2005 Mc Kinsey and the London School of Economics measured the increase in productivity from investments in IT versus investments in management practices in 100 enterprises.





Additional spending in Information Technology can raise productivity….but only in well managed companies!

What Makes IT Governance so important?



- Low return from high-cost IT investments, and transparency of IT's performance are two top issues
- More than 30% claim negative return from IT investments targeting efficiency gains
- 40% do not have good alignment between IT plans and business strategy
- Interest in and use of active management of the return on IT investments has doubled in 2 years (28% to 58%)

Drivers

- **Strategic importance of IT**
- **Extended Enterprise**
- **Regulatory requirements**
- **Cost optimisation**
- **Return on investment**

- Gartner – more than 600 billion $ thrown away annually on ill conceived or ill executed IT projects
- Standish Group – about 20% of projects fail outright, 50% are challenged and only 30% are successful
- ITGI 2005 Survey early findings confirm concerns

What makes IT Governance so important?

Shareholders want protection for the Enterprise's Share Price

"…if not filed, auditor must include a paragraph in its annual report that it cannot vouch for the enterprise's ability as a going concern…"

"…financial reporting system is not up to speed…"

"…the company has lost a third more of its market value yesterday as it revealed a virtual collapse of its financial reporting system…"

"…data entry problems…"

TIMES BUSINESS

Edited by Patience Wheatcroft ■ www.timesonline.co.uk/business

Tuesday
August 31 2004

US baker's accounts cupboard is laid bare

By James Doran
Wall Street Correspondent

THE low-carb diet craze that helped to slim American waistlines is having a similar effect on Interstate Bakeries, the country's biggest maker of forbidden pleasures such as the Twinkie and the Devil Dog.

As if its dwindling market share and a year-long stock price slide were not problems enough for Interstate, the company lost a third more of its market value yesterday as it revealed a virtual collapse of its financial reporting system.

The company disclosed to investors that it had not been able to collate financial information to complete its annual report for 2004 because of "data entry problems".

If Interstate, which has already delayed its earnings statement once, does not file the required paperwork with the US Securities and Exchange Commission, the market watchdog, by September 26, a series of potentially catastrophic default notices will ensue.

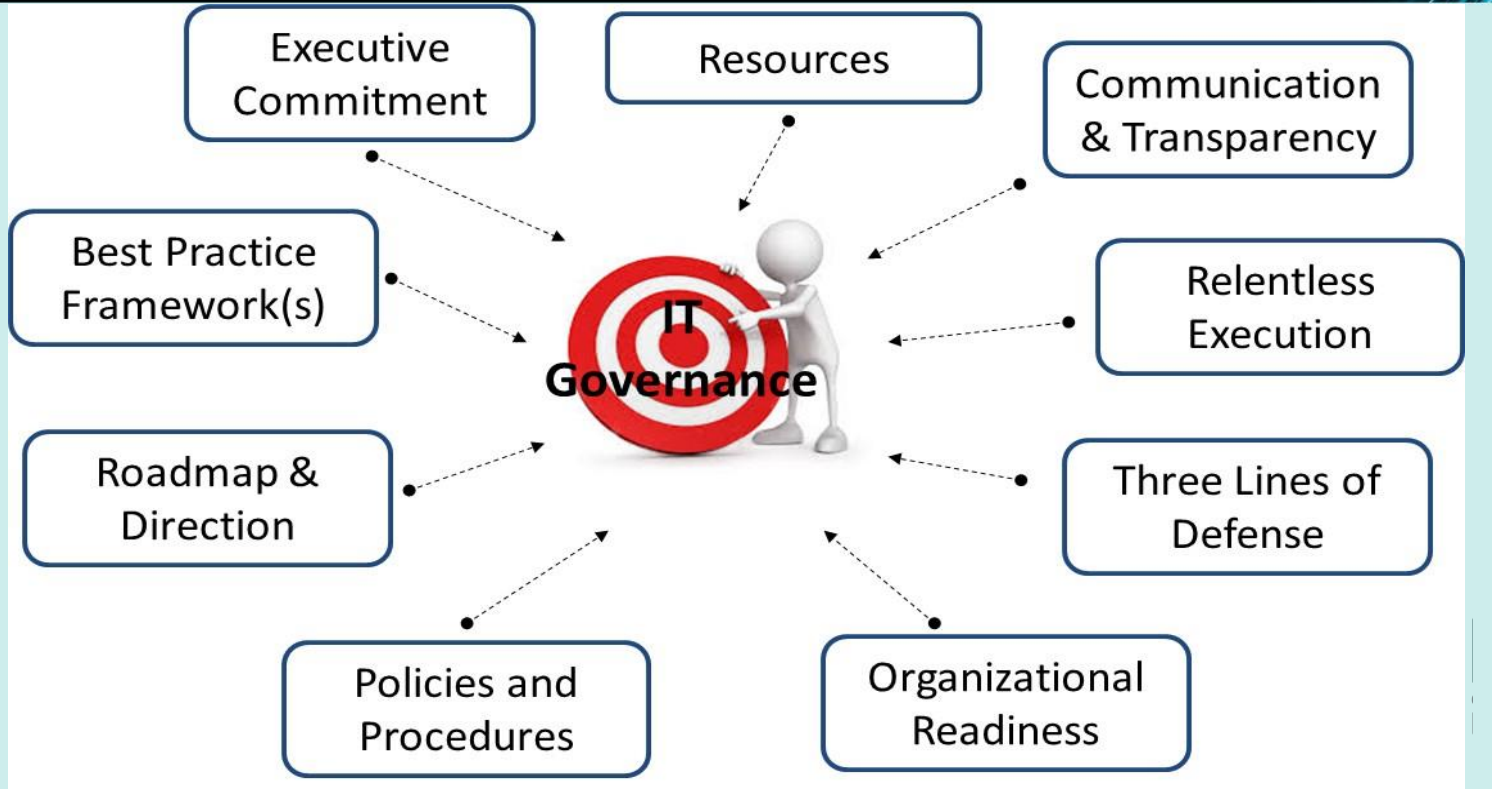
If the numbers are not filed, its auditors must include a paragraph in its annual report stating that it cannot vouch for Interstate's ability to continue as a going concern. Once that happens the company is automatically in default of its loan agreements.

"The problem really isn't with liquidity or cashflow," an Interstate spokesman said. "It is our financial reporting systems that is not up to speed. We hope we will be able to rectify this by September 26."

Interstate has called in turnaround specialist to help with the problem. However, as soon the maker of Wonder Bread released its statement yesterday, its shares tumbled 34 per cent to $5.39.

A spokesman for Interstate said: "We have been hit by the low-carb phenomenon as has everyone else in our sector. But as we have a disproportionate share of the enriched white bread market we have probably been hit harder than anyone else."

Building Blocks



Let’s do a recap…

- Identify Stakeholders
- Define your “Good”
- Bring everyone along

- Choose Framework
- Formalize Documents
- Define controls
- Self-test controls
- Assess risk & maturity
- Measure & Act

- Rationalize processes
- Leverage automation
- Implement continuous monitoring
- Enhance your KPIs and analysis

Three Lines of Defense

1st Line of Defense	2nd Line of Defense	3rd Line of Defense
Business Unit	**Risk Management**	**Internal Audit**
Ownership: *take and manage risk*	**Control**: *set standards, monitor and challenge*	**Assurance**: *validate for quality and effectiveness*
Engaged in revenue generation, expense reduction, or operational support.	**Provide independent risk oversight across all risk types, business units and locations.**	**Independently and objectively review, test and evaluate organizational activities**

IT is considered mostly 1st line, but may perform some 2nd line activities

The 1st and 2nd line functions are expected to have strong governance and risk management programs and identify and remediate issues proactively.

Understand your Stakeholders

IT Groups

Regulatory Agencies

Everyone is a Risk Manager

Security Office

SOX Committee

You're there (or closer) if…

- You have full executive support
- You have the resources you need
- You no longer have to justify the value of proactive governance
- Your governance processes are streamlined
- Auditors are no longer finding major gaps

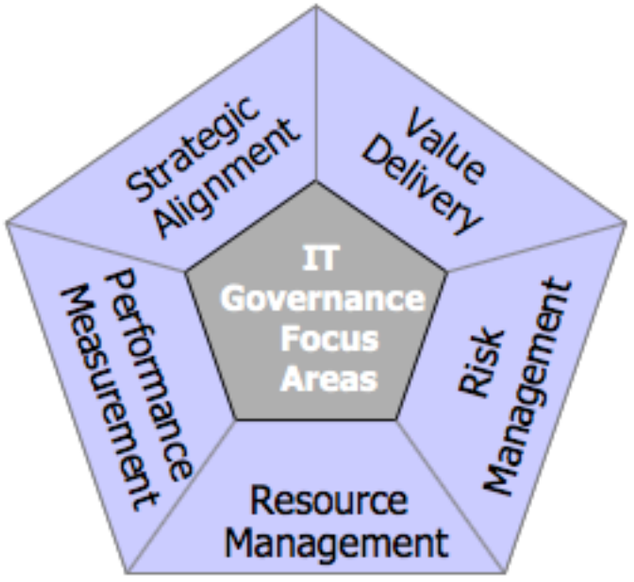
Presentation Outline

1. Introduction
2. IT Governance Framework
3. IT Governance Implementation
4. Control Framework for SOX
5. Using CobiT for C/SOX
6. Issues in Application Controls
7. Questions

What is IT Governance?

"**IT governance** is the responsibility of the board of directors and executive management. It is an integral part of enterprise governance and consists of the leadership and organisational structures and processes that ensure that the organisation's IT sustains and extends the organisation's strategies and objectives."

ITGI, Board Briefing on IT Governance



1. Strategic Alignment

Aligning with the business and providing collaborative solutions

2. Value Delivery

Executing the value proposition throughout the delivery cycle

3. Resource Management

Optimising the development and use of available resources

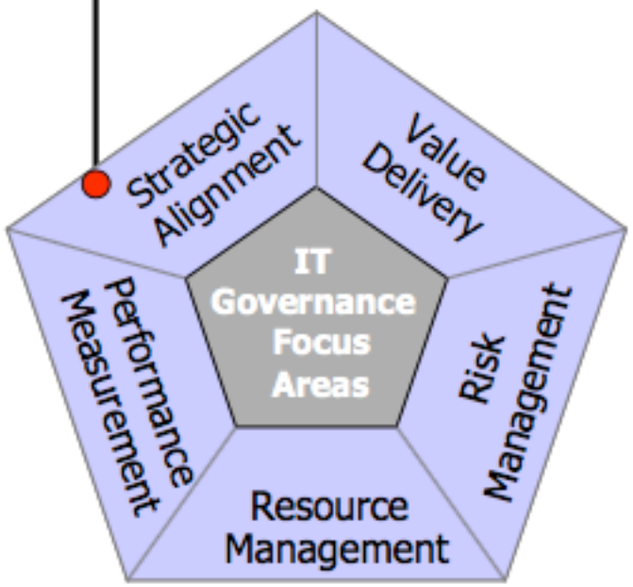
4. Risk Management

Safeguarding assets, disaster recovery and compliance

5. Performance Measurement

Monitoring results for corrective action

IT Governance – The Five Focus Areas



Strategic Alignment

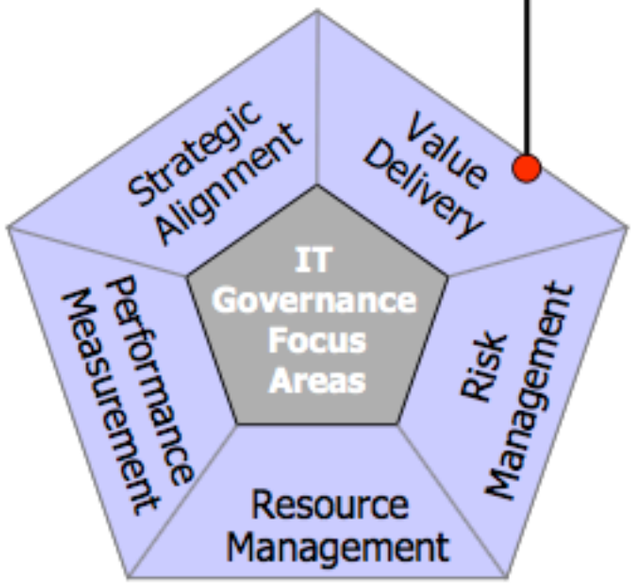
- Linking business and IT plan
- Defining, maintaining and validating the IT value proposition
- Aligning IT operations with the enterprise operations
- Provide collaborative solutions that
  - Add value and competitive positioning to the enterprise's products and services
  - Contain costs while improving administrative efficiency and managerial effectiveness

Best Practices

- Integrated approach to business/IT strategy
- Cascading strategy and objectives down into the organisation
- Co-responsibility of business and IT
- Clearer objectives for IT investments
- IT Strategy and IT Steering Committees

In 2003, 49% of respondents had implemented, were considering implementing or were in the process of implementing this phase of IT governance. In 2005, 70%.

IT Governance – The Five Focus Areas



Value Delivery

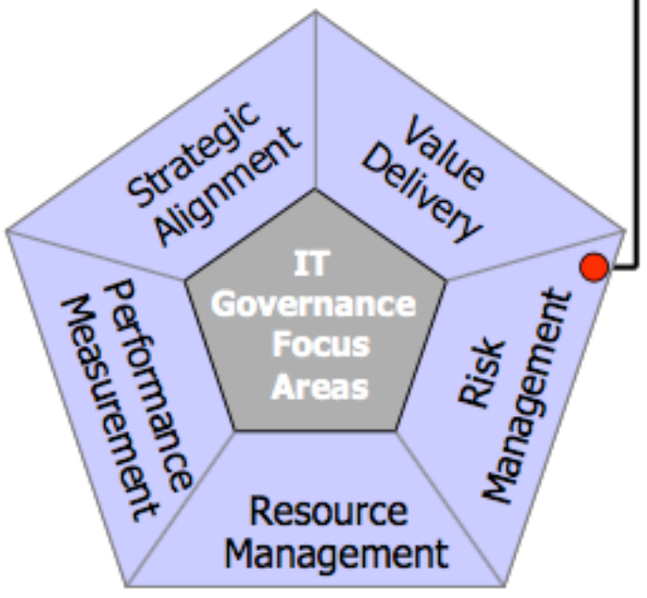
- Executing the value proposition throughout the delivery cycle
- Ensuring that IT delivers the promised benefits against the strategy
- Concentrating on optimising expenses & proving IT's value
- Controlling projects and operational processes with practices that increase the probability of success (quality, risk, time, budget, cost, etc.)

Best Practices

- Formal tracking of business value of IT
- Enabling effective value measurement (ROI, TCO, NOV…)
- Disciplined approach to project management with a larger role for the business
- Commitment to formal methodologies/processes for development and service delivery
- Enterprise architecture planning

In 2003, 39% of respondents had implemented, were considering implementing or were in the process of implementing this phase of IT governance. In 2005, 69%.

IT Governance – The Five Focus Areas



Risk Management

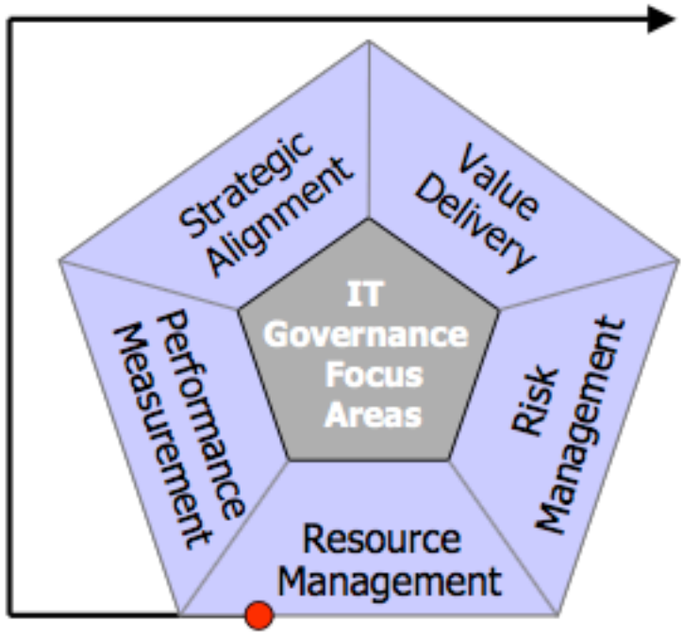
- Requires risk awareness of senior corporate officers, a clear understanding of the enterprise's appetite for risk and transparency about the significant risks to the enterprise
- Embeds risk management responsibilities in the operation of the enterprise
- Addresses the safeguard of IT assets, disaster recovery and continuity of operations

Best Practices

- Awareness of IT risks based on continuous assessment
- Transparency to all stakeholders
- Establishing responsibility and embedding risk management into the organisation
- An integral part of compliance and assurance
- Use of formal IT risk and control frameworks
- Process management disciplines

In 2003, 34% of respondents had implemented, were considering implementing or were in the process of implementing this phase of IT governance. In 2005, 78%.

IT Governance – The Five Focus Areas



Resource Management

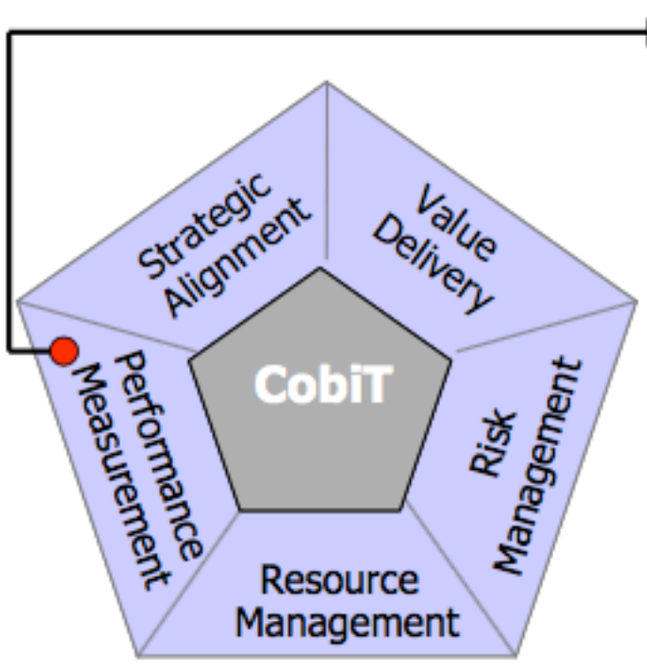
- Optimal investment, use and allocation of IT resources and capabilities (people, applications, infrastructure, data)
- Maximising the efficiency of these assets and optimising their costs
- Optimising knowledge and the IT infrastructure
- Knowing where and how to outsource

Best Practices

- Supply/demand balancing
- Practices to train and sustain skilled staff including Career Centres for project assigned staff
- Consumption-based chargeback
- Transparency in expense management and cost allocation
- Formalised vendor management disciplines

In 2003, 50% of respondents had implemented, were considering implementing or were in the process of implementing this phase of IT governance. In 2005, 75%.

IT Governance – The Five Focus Areas



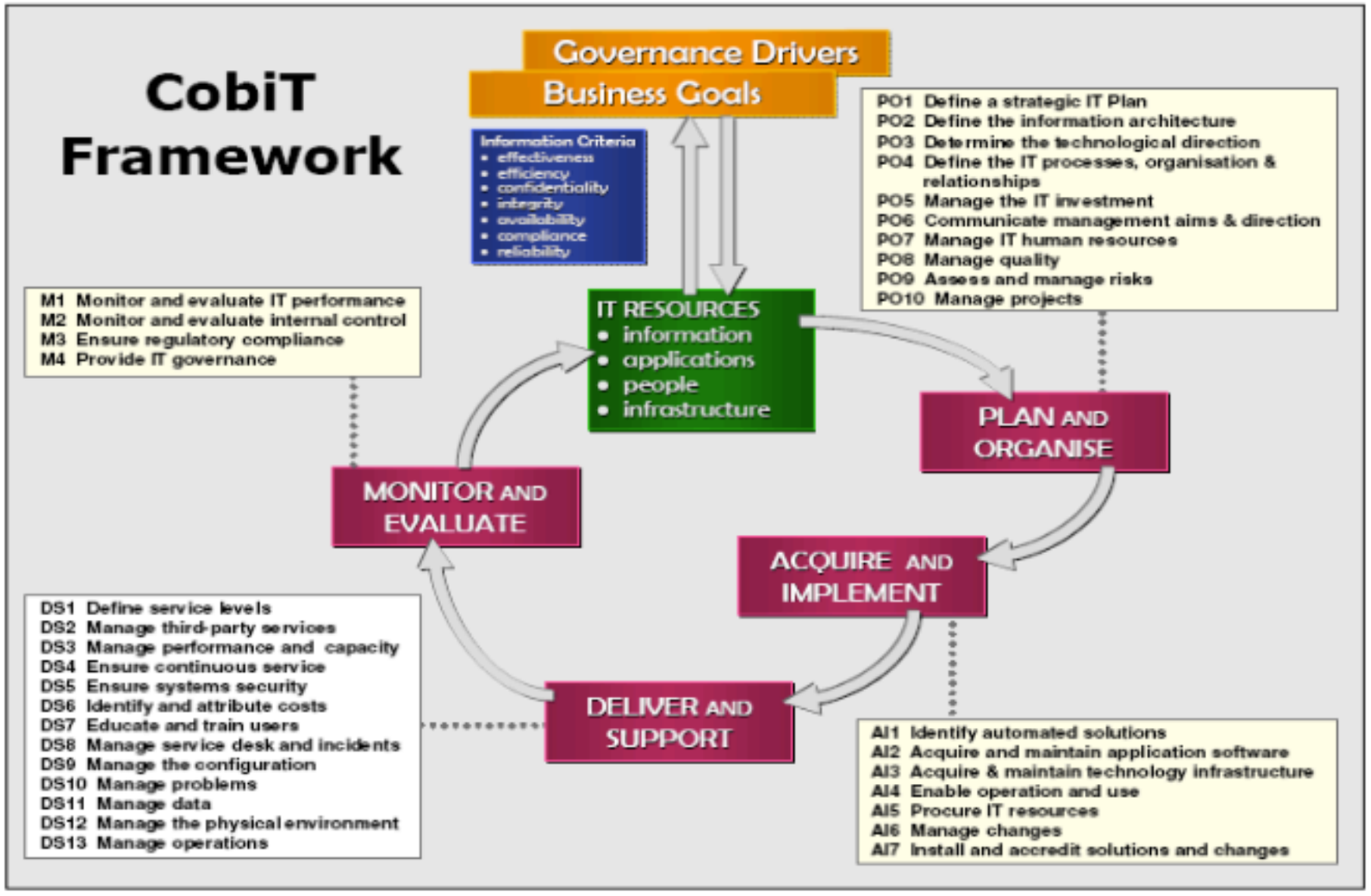
Performance Measurement

- Using balanced scorecards that translate strategy into action to achieve goals measurable beyond conventional accounting
- Measuring relationships and assets necessary to compete: customer focus, process efficiency and the ability to learn and grow
- Tracking project delivery and monitoring IT services

Best Practices

- IT Balanced Scorecard as emerging reporting system
- A management reporting system that feeds back into the strategy
- Use of benchmarking for performance comparison
- IT Scorecard approval by the key stakeholders for alignment

In 2003, 34% of respondents had implemented, were considering implementing or were in the process of implementing this phase of IT governance. In 2005, 67%.


CobiT Framework
Governance Drivers
Business Goals
Information Criteria
• effectiveness
• efficiency
• confidentiality
• integrity
• availability
• compliance
• reliability
PO1 Define a strategic IT Plan
PO2 Define the information architecture
PO3 Determine the technological direction
PO4 Define the IT processes, organisation & relationships
PO5 Manage the IT investment
PO6 Communicate management aims & direction
PO7 Manage IT human resources
PO8 Manage quality
PO9 Assess and manage risks
PO10 Manage projects
M1 Monitor and evaluate IT performance
M2 Monitor and evaluate internal control
M3 Ensure regulatory compliance
M4 Provide IT governance
IT RESOURCES
• information
• applications
• people
• infrastructure
PLAN AND ORGANISE
ACQUIRE AND IMPLEMENT
DELIVER AND SUPPORT
MONITOR AND EVALUATE
DS1 Define service levels
DS2 Manage third-party services
DS3 Manage performance and capacity
DS4 Ensure continuous service
DS5 Ensure systems security
DS6 Identify and attribute costs
DS7 Educate and train users
DS8 Manage service desk and incidents
DS9 Manage the configuration
DS10 Manage problems
DS11 Manage data
DS12 Manage the physical environment
DS13 Manage operations
AI1 Identify automated solutions
AI2 Acquire and maintain application software
AI3 Acquire & maintain technology infrastructure
AI4 Enable operation and use
AI5 Procure IT resources
AI6 Manage changes
AI7 Install and accredit solutions and changes

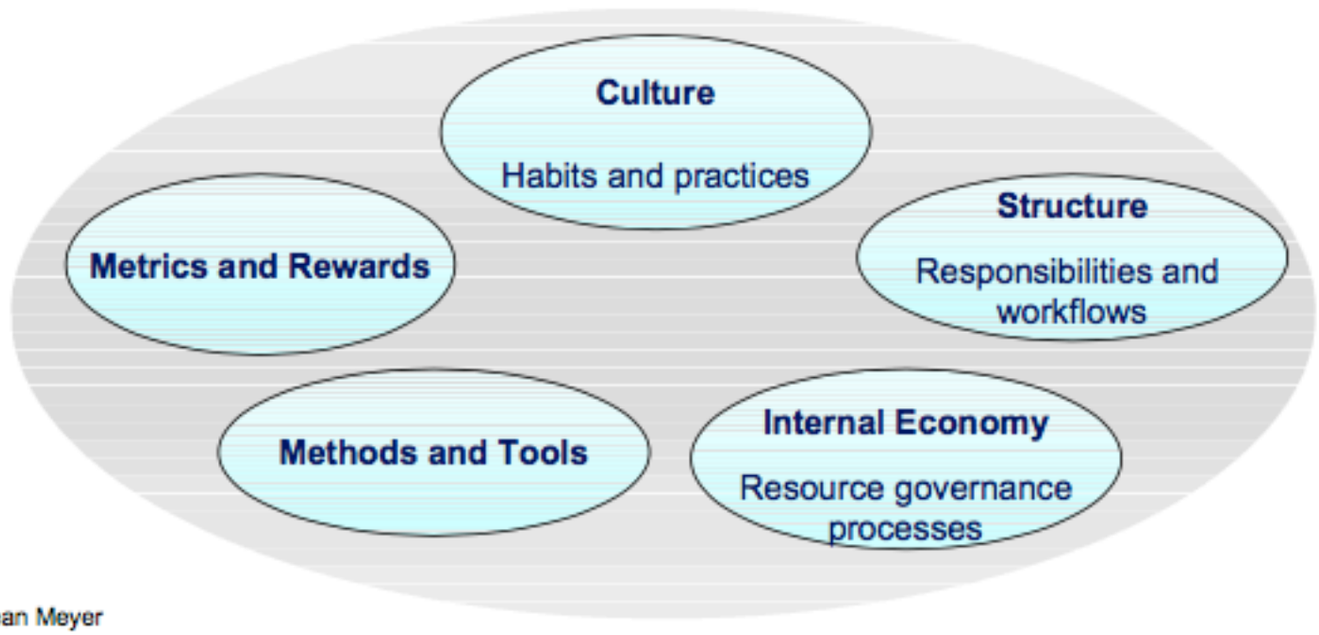
Presentation Outline

1. Introduction
2. IT Governance Framework
3. IT Governance Implementation
4. Control Framework for SOX
5. Using CobiT for C/SOX
6. Issues in Application Controls
7. Questions

Organisational Systems

The focus areas of IT Governance must be embedded within the organisation's systems.

Organisational systems are relatively stable, influence everyone's performance and can be consciously designed.



Source: N. Dean Meyer

Strategic Alignment

Alignment is achieved within the structure of the companies' annual planning and budgeting process through the transparency of the value/risk versus cost propositions..

Structure	
Strategy	Inter-company I.S. Executive Committee, ISEC
Development	Line of Business Steering Committees, Account Managers
Operations	Business Process Owners, Account Managers, Service Delivery Managers
Governance	Executive/Risk Management Committees, Functional Leadership

Internal Economy

⇩ I.S. expenses are targeted and capped (zero tolerance)
⇩ I.S. expenses are fully burdened and recovered by consumption-based chargeback (zero profit)
⇩ Lines of business have clear ROE targets which include I.S. chargebacks

Methods & Tools	
Strategy	I.S. Strategy Map, Balanced Scorecard, CobiT
Development	Business Case Disciplines > $500K
Operations	Service Level Agreements, I.S. Product and Service Standards
Governance	Risk / Compliance / Maturity Assessments (CobiT)

Metrics & Rewards	
Financial Targets	Minimum 15% annual growth in shareholder earnings, 18% ROE: Company, Line of Business
Contributing Metrics	Sales, Expense Management, Customer Service, Project Delivery, Service Achievement
Rewards	Ties to management incentives, stock option / purchase plans

Culture

⇩ Empowered hierarchy, command and control management style
⇩ Rigorous approaches to analysis, planning and risk management (fact-based)
⇩ Strong preference for measurable, verifiable benefits

Value Delivery

Value delivery is ensured on business projects and operations through co-responsibility with business leaders and on governance through direct accountability to the executive committees.

Structure	
Development	Business sponsors, I.S. Project Managers, I.S. leadership teams, A.C.T., PMI-based methodology, formal SDLC methodologies
Operations	Business process owners, Service Delivery Managers, Service Management Process
Governance	Risk Management Committee (risk, compliance, audit, I.S.)

Internal Economy

⇩ I.S. expense budgets are allocated to lines of business and specific activities, these allocations act as expense caps
⇩ Allocations are exceeded only by formal change control first considering scope reduction
⇩ Expense over-runs at the activity level are offset within the lines of business (LOB's), or failing that, across the LOB's

Methods & Tools	
Development	Bates Project Management, SEI-CMMI, Enterprise Architecture, TeamPlay, SAP
Operations	ITIL, CobiT, SAP
Governance	CobiT, SAP, Terms of Engagement

Metrics & Rewards	
Development	Co-responsibility for results with business (quality, risk, time, cost)
Operations	Co-responsibility for results with business (service, cost, problem management)
Governance	Accountability to executive committees (incidents, maturity, audits, initiative completions)
Rewards	Ties to incentives at next levels of management and practitioners

Culture

⇩ Active, hands-on management of emerging results and adjusting actions
⇩ Business partnership: business says "what", I.S. says "how"
⇩ I.S. is a professional services organisation: we charge for our services, strive for repeatable performance

Risk Management

Risk management is approached by selecting an acceptable risk level based upon the detailed assessments of exposure, probability of occurrence, compliance to legal or regulatory requirements and emerging industry good practice.

Structure	
Executive	Executive committee sponsorship, risk committee oversight
Risk Management	I.S. Risk Management Office with focus on risk assessment, security, privacy, DR, compliance and process / quality management
Supplier Management	Vendor Relations Team focuses on leveraged purchasing and contractual risks

Internal Economy

- ⇩ Governance improvements are structured as internal I.S. initiatives and compete for approval along with business projects
- ⇩ Scrutiny is also focused on the total expenditures on risk management activities

Methods & Tools	
Risk Management	COSO/Methodware: Enterprise Risk Assessor
Security	CobiT, ISO 17799
Disaster Recovery	CobiT, IBM maturity framework
Control	CobiT, COSO

Metrics & Rewards	
Progress	Measured through initiative completions, maturity assessments and audits
Results	Avoidance of major incidents (non-occurrence, response)
Rewards	Tied to incentive based on results, progress and quality of assessments

Culture

- ⇩ Willingness to accept reasonable level of risk
- ⇩ Risks must be explained in detail and target maturity levels justified
- ⇩ Risk management viewed as overhead, value proposition is challenging

Resource Management

Resource management is the most direct and controllable leverage point to ensure the delivery of our financial targets and is the focus of our detailed and active management approach.

Structure

Development	Business steering committees, business sponsors, I.S. project managers
Operations	Business process owners, Account Managers, Service Delivery Managers
Governance	Risk Management Committee, functional leadership, ISFM, Career Centres, ISHR Organisation

Internal Economy

⇩ I.S. expense budgets are allocated to lines of business and specific activities, these allocations act as expense caps
⇩ I.S. is accountable to manage within its budget (gatekeeper role)
⇩ Business leaders cannot spend above their I.S. budget without approval of the president.

Methods & Tools

Financial	SAP, TeamPlay, MICS, Remedy
Human Resources	TimeControl, SEI-PCMMI, Career Centres for project assigned staff
Assets	Applications / Data Inventory, Remedy

Metrics & Rewards

Financial	Expense management, unit cost targets
Human Resources	Utilisation / "billable" ratios, blended labour rates, benchmark staffing ratios
Assets	Managed seat costs, recovery for assets
Rewards	Tied to management incentives at all levels

Culture

⇩ Strong belief in internal expense management capability
⇩ Decided preference for internal sourcing and control
⇩ Expectation of managers to know / be engaged at a detailed level and be fiscally responsible

Performance Measurement

Performance measurement is an essential element of the management discipline to drive delivery, validate the effectiveness of business and I.S. strategy and to trigger management rewards based on company performance and individual contributions to its achievement.

Structure	
Strategy	I.S. Executive Committee, ISFM, Process Management function
Development	I.S. Project Managers, I.S. Project Management Office
Operations	Account Managers, Service Delivery Managers, Service Management Process
Governance	Risk Management Organisation, Internal Audit, Compliance Officers

Internal Economy

- ⇩ Measurement investments are reviewed along with other control costs
- ⇩ Measurement systems must demonstrate that control information is actionable and costs do not exceed the value obtained.

Methods & Tools	
Strategy	I.S. Balanced Scorecard, CobiT
Development	Major Projects Review methodology
Operations	Operations Management Report by LOB, ITIL
Governance	CobiT

Metrics & Rewards	
Metrics	Measurable outcomes are required for all management objectives
Rewards	Rewards and bonuses are only triggered when results are measured

Culture

- ⇩ Belief: "If you cannot measure it, you cannot manage it"
- ⇩ "Show me" culture, insistence on demonstrable results
- ⇩ "We deliver on our commitments"

Key IT Governance Practices

- Executive and business level steering committees
- Clear roles and responsibilities – business sponsors say “what”, IT says “how” (Terms of Engagement)
- Internal economy model – supply/demand balancing, consumption based chargeback
- Use of best practice frameworks for process and control
- Linkage of measured results to rewards
- Strong culture of rigorous analysis, fact-based decision making and active, hands-on management

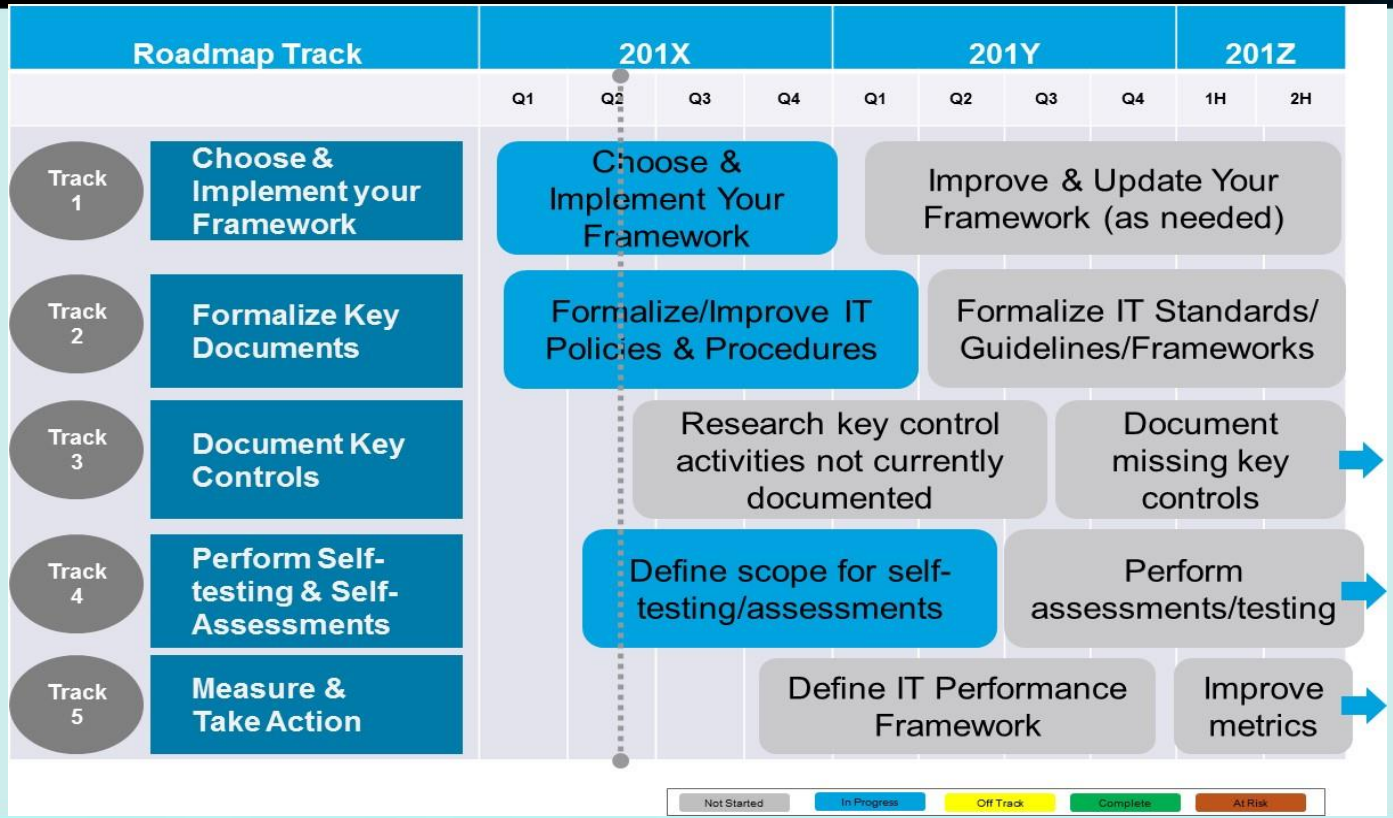
Define what your “Good” looks like

- Define the skill set and resources you need
- Describe roles and responsibilities

- Leverage best practices and frameworks
- Create a roadmap of activities and timelines
- Clearly articulate your scope of coverage
- Add key details applicable to your organization

- Identify when and how you will leverage technology

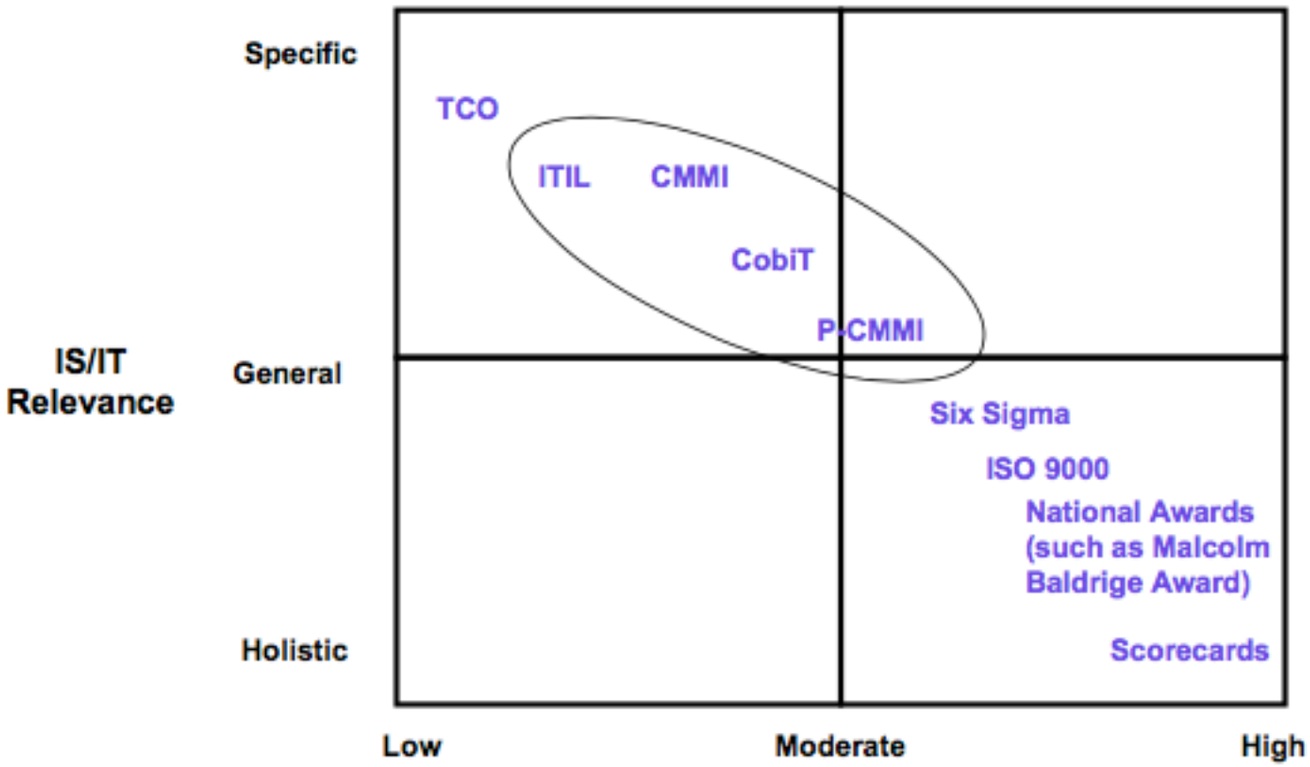
Sample High-Level IT Governance Roadmap



Bring everyone along

- Executives
- Employees
- Contactors
- Third parties

Process Model Selection



CMMI = Capability Maturity Model Integration

CobiT = Control Objectives for Information and Related Technology

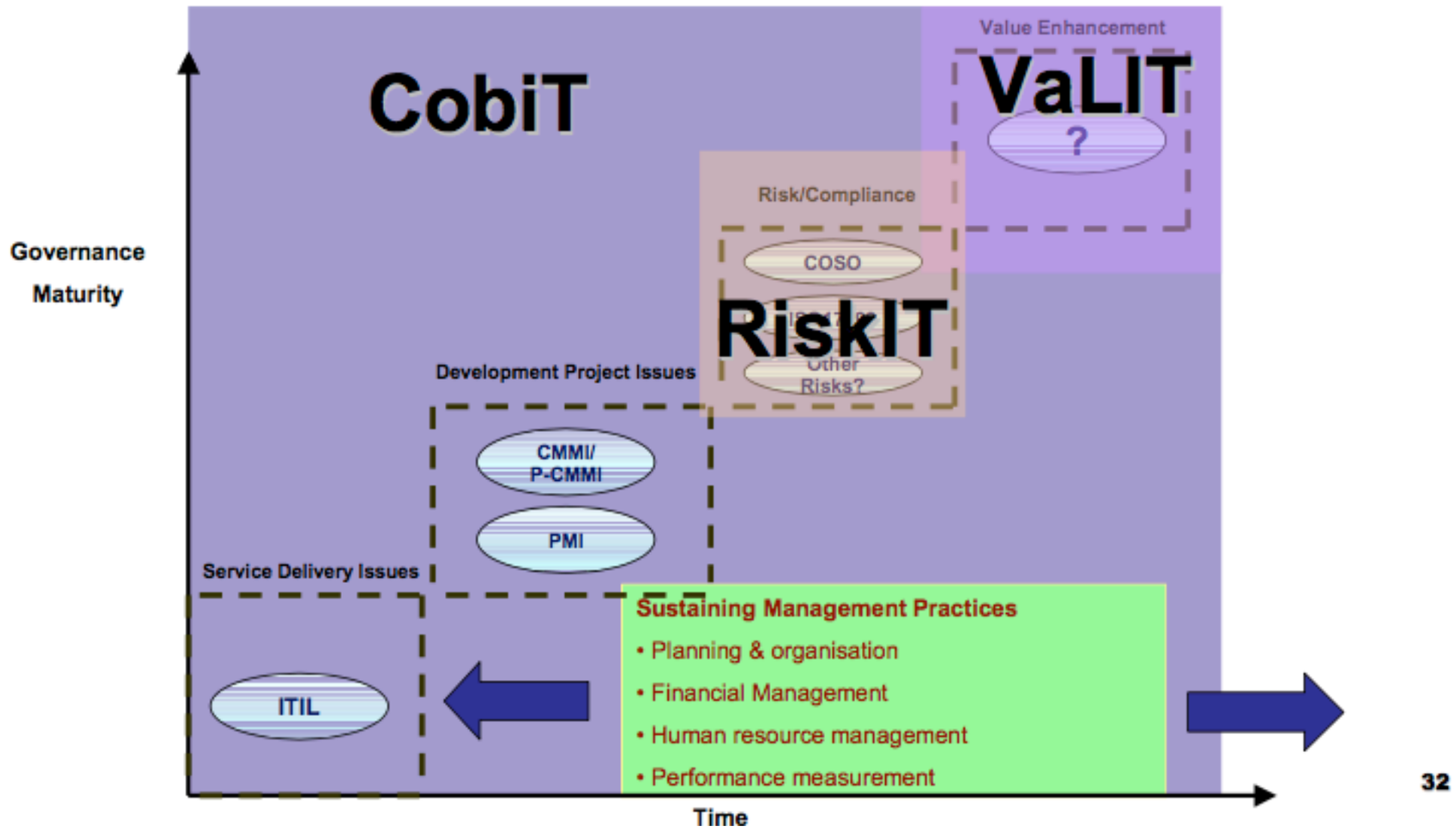
ITIL = IT Information Library

TCO = Total Cost of Ownership

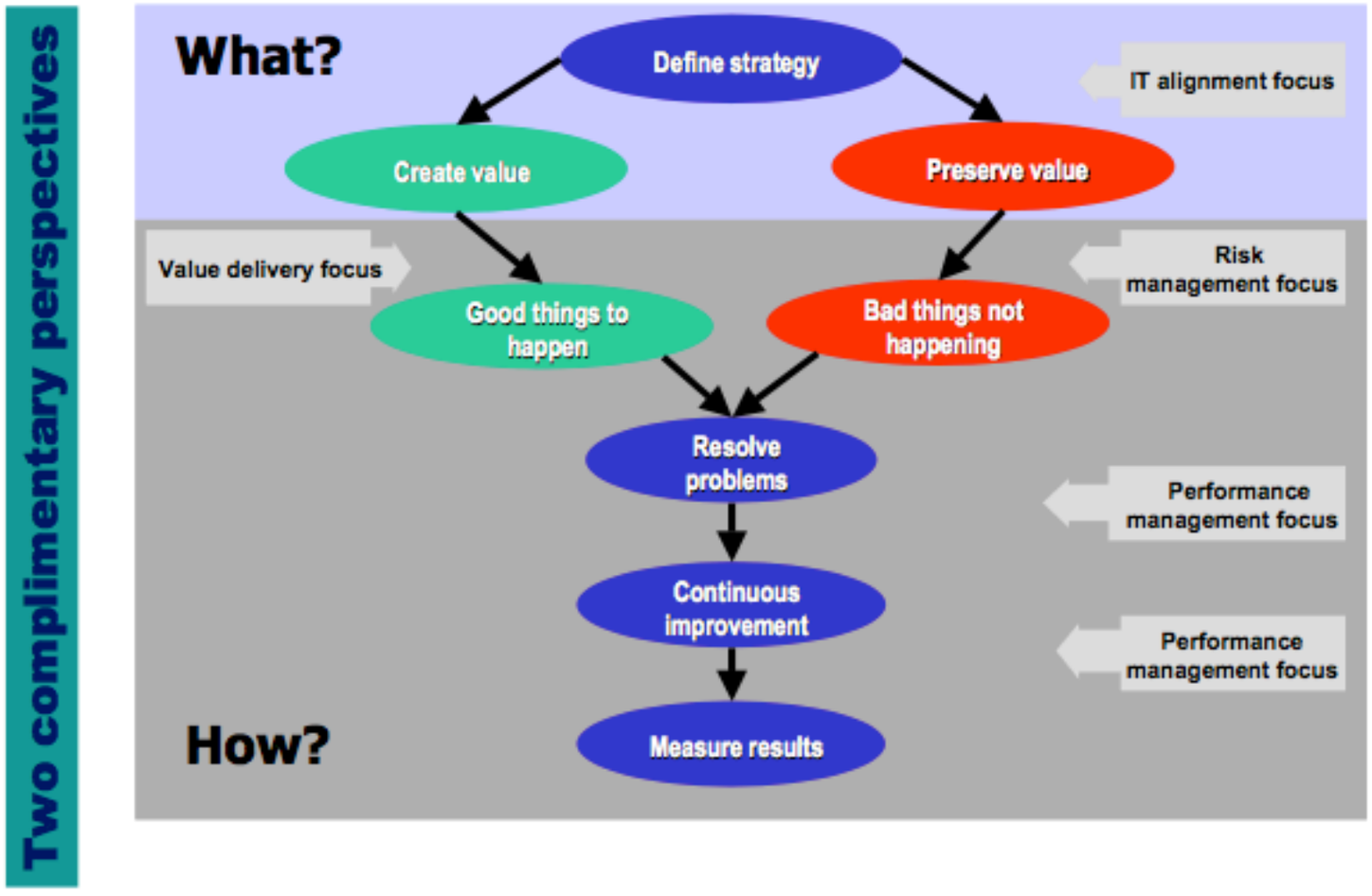
Source: Gartner Research (June 2003)

Governance Maturity over time

IT Governance matures over time – Where is your roadmap?



CobiT Implementation Guide



General Approach to Governance Implementation

1. Identify priority issue(s) (governance or business drivers)
2. Map to IT goals, process and affected resources
3. Assign to Process Owner
4. Resolve issue and adjust process/resources
5. Use responsibility matrix to determine job impacts
6. Change job descriptions/expectations
7. Change measurement/monitoring systems
8. Incorporate into performance appraisals/reward processes

Presentation Outline

1. Introduction
2. IT Governance Framework
3. IT Governance Implementation
4. Control Framework for SOX
5. Using CobiT for C/SOX
6. Issues in Application Controls
7. Questions

The Cost of SOX

FINANCIAL SERVICES

SOX cited as audit costs jump 10%

BY DUNCAN MAVIN

Canada's largest firms paid their auditors more than $600-million last year, a jump of almost 10% from $554-million the previous year.

Audit costs have risen significantly in recent years, especially due to the impact of complex new regulations such as the Sarbanes-Oxley Act, known as SOX.

Some observers had anticipated fee increases would settle down once the industry adjusted to the new rules. However, the latest survey of fees paid by the top 100 companies in the Toronto Stock Exchange from Toronto-based Workflow International Inc. indicates the cost of obtaining an audit report is still on the rise.

"Ten per cent is more than you'd think the cost would go up in a low inflation environment," said Workflow's David Slater. "But there's no question we are seeing greater complexity and risks having an impact."

Rising audit costs resulting from SOX and other rule changes have increased the amount of time and effort auditors say is needed for them to do their work. That has created a shortage of qualified staff, which has also pushed up auditors' salaries, and therefore audit costs. On top of that, some auditors complain they can no longer obtain indemnity insurance to cover the risk of being sued for their work, and that risk is also factored into fees.

Meanwhile, the so-called Big Four audit firms — **Deloitte & Touche LLP**, **Pricewaterhouse Coopers LLP**, **Ernst & Young LLP** and **KPMG LLP** — continue to dominate Canada's audit market, sharing 99% of total fees paid by companies in the survey. **Grant Thornton LLP** and survey newcomer **Soberman LLP** share the remaining 1%.

Deloitte has the largest share, commanding 39% of fees paid to auditors by Canada's big firms, up from 36% in the previous survey. Deloitte was paid $236-million according to the latest results, up $38-million from $198-million.

Nortel Networks Corp., a Deloitte client, paid out more than any other company.

Nortel, whose accounts have been under more scrutiny than perhaps any other Canadian company, paid Deloitte $81-million for audit and related work, a hike of $7-million from $74-million the year before.

One significant shift in the data, noted Mr. Slater, is that the amount paid to auditors for services other than the annual audit has fallen from about 30% of total fees two years ago to about 15% in the latest set of figures.

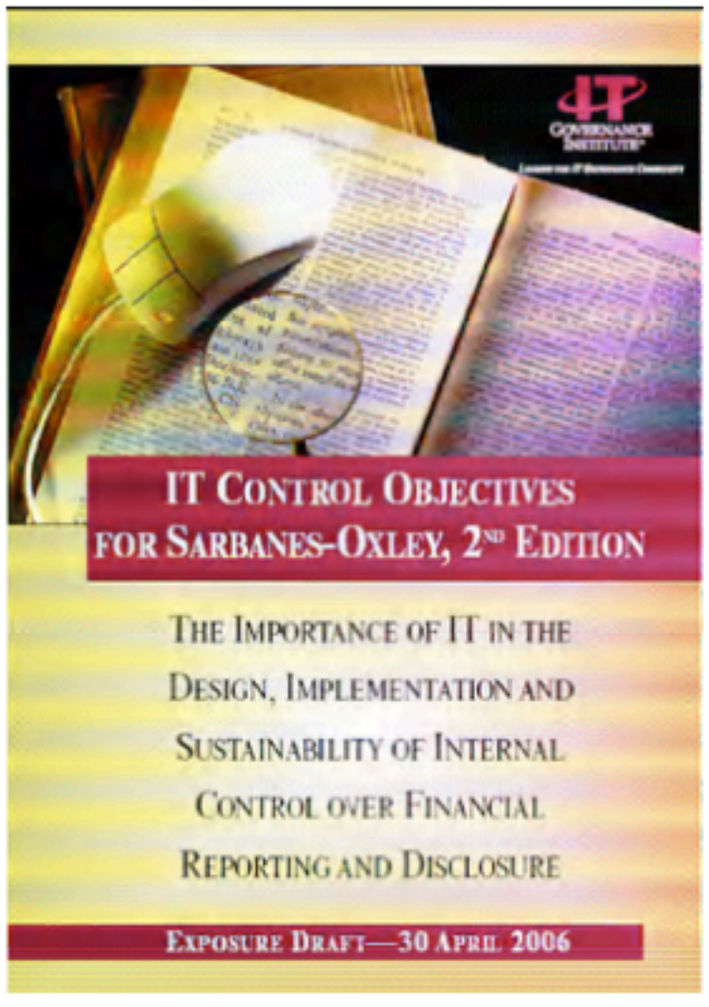
Financial Post
dmavin@nationalpost.com

IT, SOX and CobiT

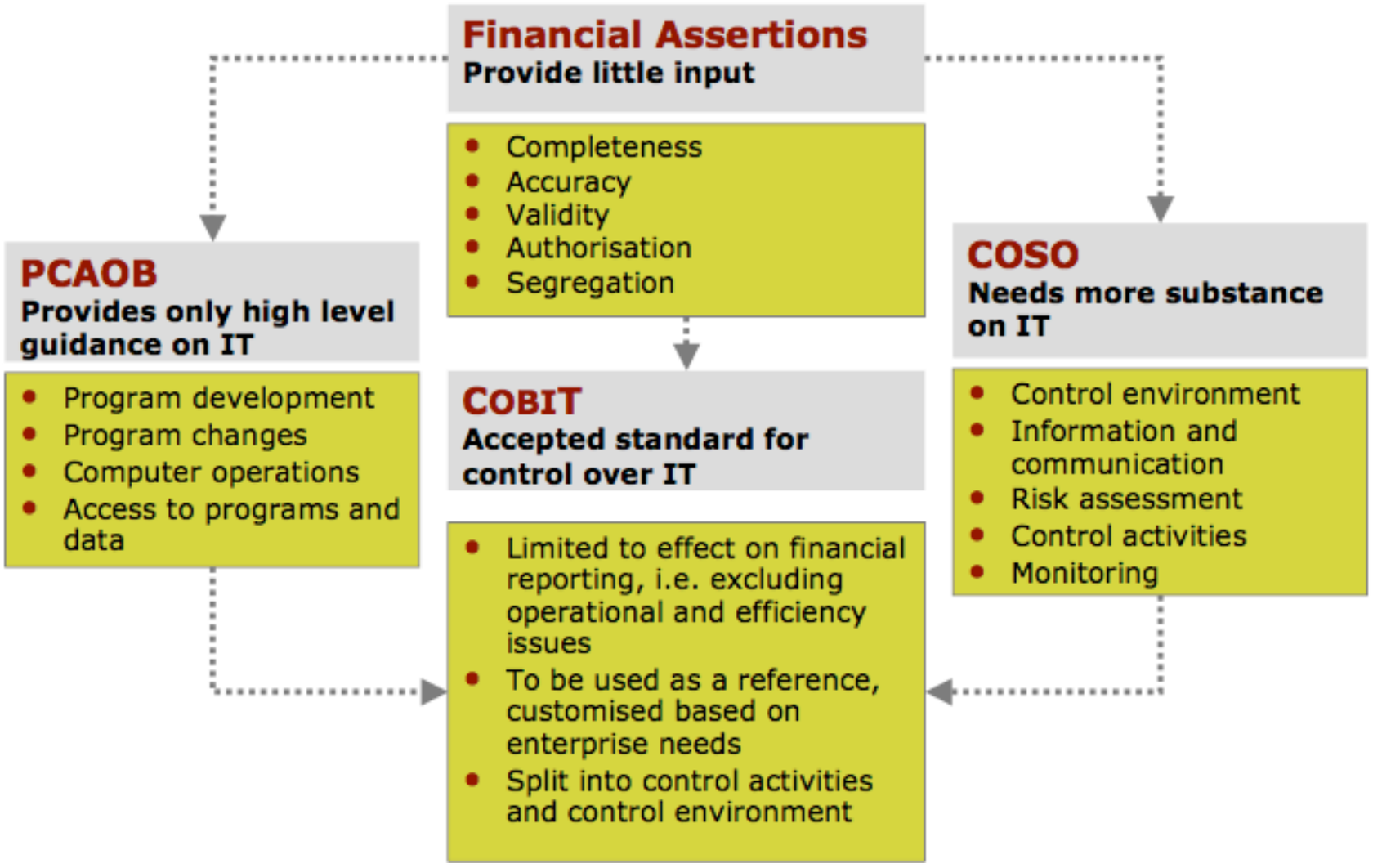
Internal Control

COSO

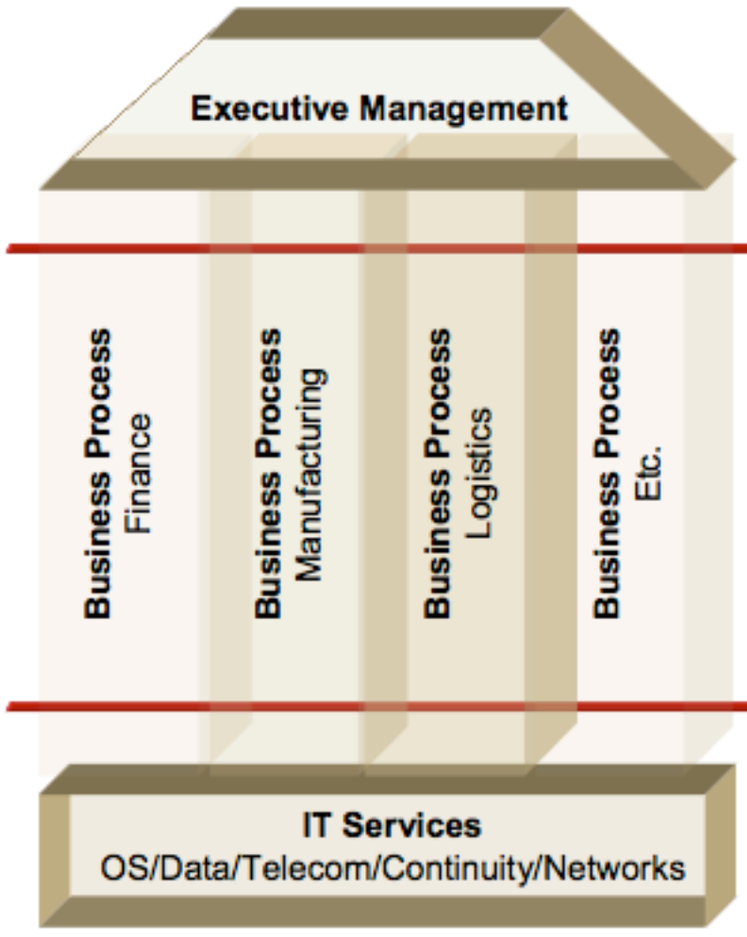
CobiT



IT, SOX and CobiT



Organisation Controls



Entity-level Controls
Entity-level Controls set the tone and culture of the organisation. IT entity-level controls are part of a company's overall environment.

Controls include:
- Strategies and plans
- Policies and procedures
- Risk assessment activities
- Training and education
- Quality assurance
- Internal audit

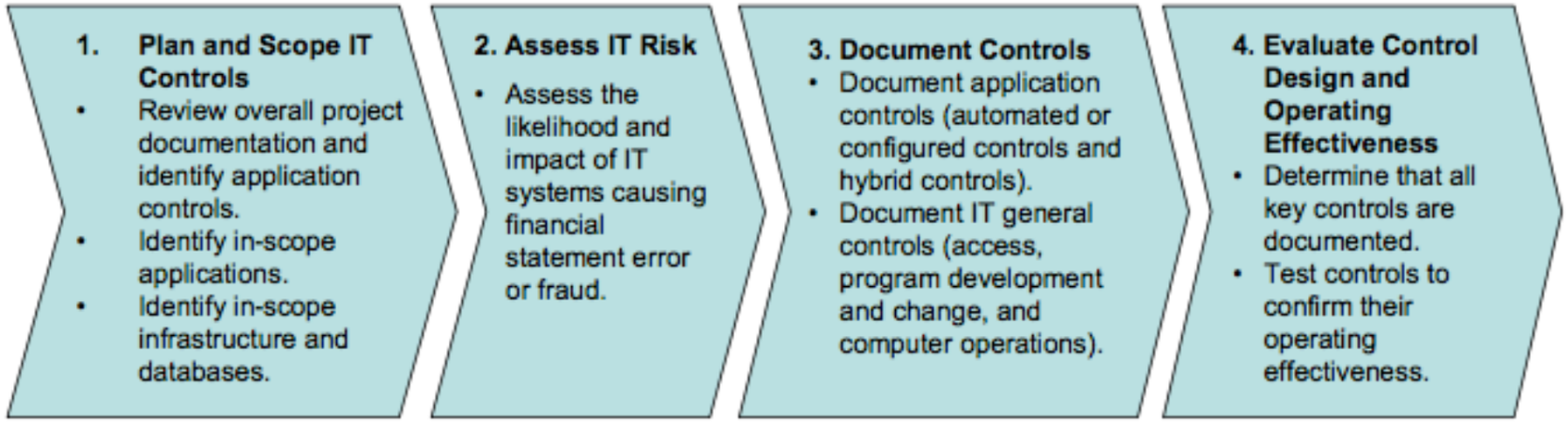
Application Controls
Controls embedded within business process applications directly support financial control objectives. Such controls can be found in most financial applications including large systems such as SAP and Oracle as well as smaller OTS systems such as ACCPAC.

Control objectives/assertions include:
- Completeness
- Accuracy
- Existence/authorisation
- Presentation/disclosure

IT General Controls
Controls embedded within IT Processes that provide a reliable operating environment and support the effective operation of application controls.

Controls include:
- Program development
- Program changes
- Access to programs and data
- Computer operations

C/SOX Roadmap



Presentation Outline

1. Introduction
2. IT Governance Framework
3. IT Governance Implementation
4. Control Framework for SOX
5. Using CobiT for C/SOX
6. Issues in Application Controls
7. Questions

C/SOX – An Enterprise Approach

Corporate Projects (GWL & IGM):

Level 0

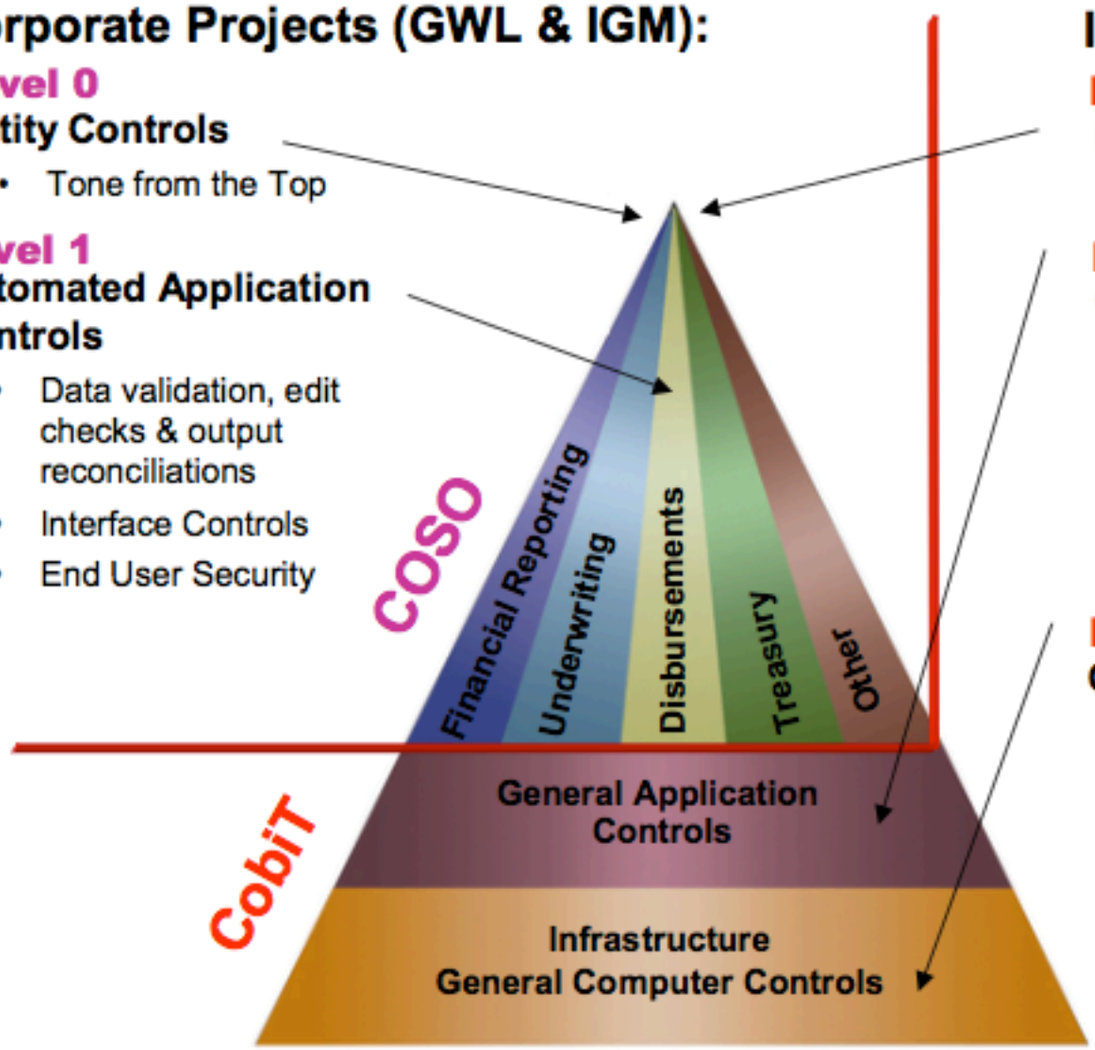
Entity Controls

- Tone from the Top

Level 1

Automated Application Controls

- Data validation, edit checks & output reconciliations
- Interface Controls
- End User Security



I.S. Project:

Level 0

I.S. Entity Controls

- Support Tone from the Top

Level 2

General Application Controls

- System development
- Change control
- Data Recovery
- Database management
- Programmer security

Level 3

General Computer Controls

- Change & Configuration management
- Network Administration
- Security Administration
- Data center operations
- Database Administration
- O/S Administration

IT Entity Controls (Level 0)

		COSO Component				
Process ID	CobiT IT Process	Program Development	Risk Assessment	Control Activities	Information and Communication	Monitoring
PO1	Define IT Strategic Planning		•		•	•
PO4	Define the IT processes, organisation and relationships	•			•	•
PO6	Communicate management aims and directions	•			•	
PO7	Manage IT human resources	•			•	
PO8	Manage quality	•		•	•	•
PO9	Assess and manage IT risks		•			
DS7	Educate and train users	•			•	
ME1	Monitor and evaluate IT performance			•	•	•
ME2	Monitor and evaluate internal control	•				•
ME3	Ensure regulatory compliance			•	•	•
ME4	Provide IT governance	•				•

IT General Controls (Level 2 & 3)

		PCAOB Control Headings			
Process ID	CobiT IT Process	Control Environment	Program Changes	Computer Operations	Access to Programs and Data
AI2	Acquire and maintain application software	•	•	•	•
AI3	Acquire and maintain technology infrastructure	•	•	•	
AI4	Enable operation and use	•	•	•	•
AI6	Manage changes		•		•
AI7	Install and accredit solutions and changes	•	•	•	•
DS1	Define and manage service levels	•	•	•	•
DS2	Manage 3rd party services	•	•	•	•
DS5	Ensure systems security			•	•
DS9	Manage the configuration			•	•
DS8	Manage incidents			•	
DS10	Manage problems			•	
DS11	Manage data			•	•
DS13	Manage operations			•	•

Presentation Outline

1. Introduction
2. IT Governance Framework
3. IT Governance Implementation
4. Control Framework for SOX
5. Using CobiT for C/SOX
6. Issues in Application Controls
7. Questions

Issues in Application Controls

- **The need for risk management is not appreciated**
  - Demonstrate the value received for the investment in controls
  - Conduct regular communication and change management

- **Business slow to recognise responsibility for Application Controls**
  - Ensure Application Control and IT General Control teams coordinate
  - Acknowledge shared responsibility for sign-off

- **Many older application do not have the required controls**
  - If risk is high, identify compensating controls
  - If risk is low, waive the requirement on a case-by-case basis

Issues in Application Controls

- **Difficult to determine an 'appropriate and measured response'**
  - Identify critical business processes based on risk and materiality
  - Limit work to high priority processes

- **There is a general lack of internal control expertise**
  - Define and implement standardised monitoring processes
  - Minimise the risk of re-work – Do it right the first time!

- **No definitive guidance from consultants or government**
  - Use common sense based on experience
  - Be able to justify the decisions made

Some Useful References (2/3)

Formalize Key Documents & Define Controls

- ISACA **COBIT 5.0** Framework
- Information Technology Infrastructure Library (**ITIL**) for IT Service Management
- National Institute of Standards and Technology (**NIST**) and the **ISO/IEC 27000** family for Information Security
- **PMBOK Guide** from the Project Management Institute for Project Management
- **Regulatory guidance/standards** in your industry
- The Open Group Architecture Framework (**TOGAF**) for Enterprise Architecture

Some Useful References (3/3)

Perform Self-Testing & Self-Assessments

- ISACA **COBIT 5.0** Framework
- ISACA **Risk IT** Framework
- Operationally Critical Threat, Asset, and Vulnerability Evaluation (**OCTAVE**) Framework from Carnegie Mellon

Measure & Act

- Balanced Scorecard Framework (**BSC**) from the Balanced Scorecard Institute (BSI)

EXAMPLE IT GOVERNANCE FOR UNIVERSITY

Figure 5. IT Governance Framework from JISC (2007a)

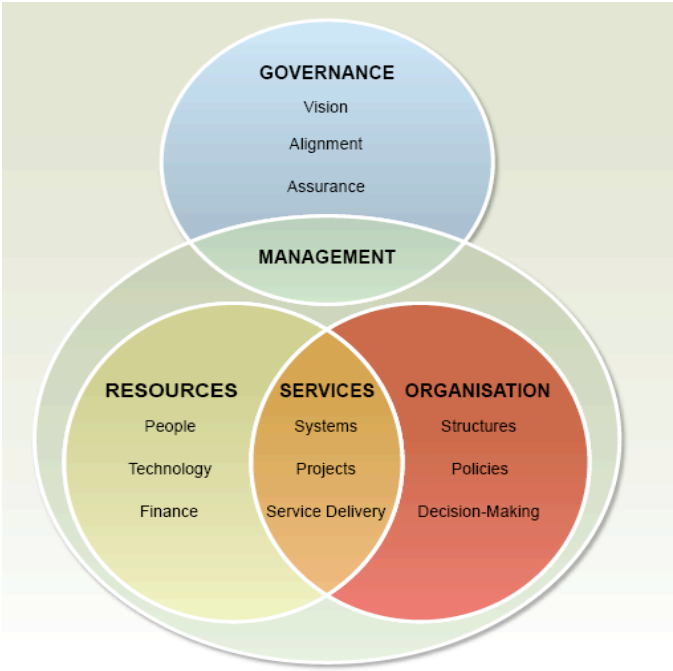


Figure 6. IT Governance Framework for Universities (ITG4U)

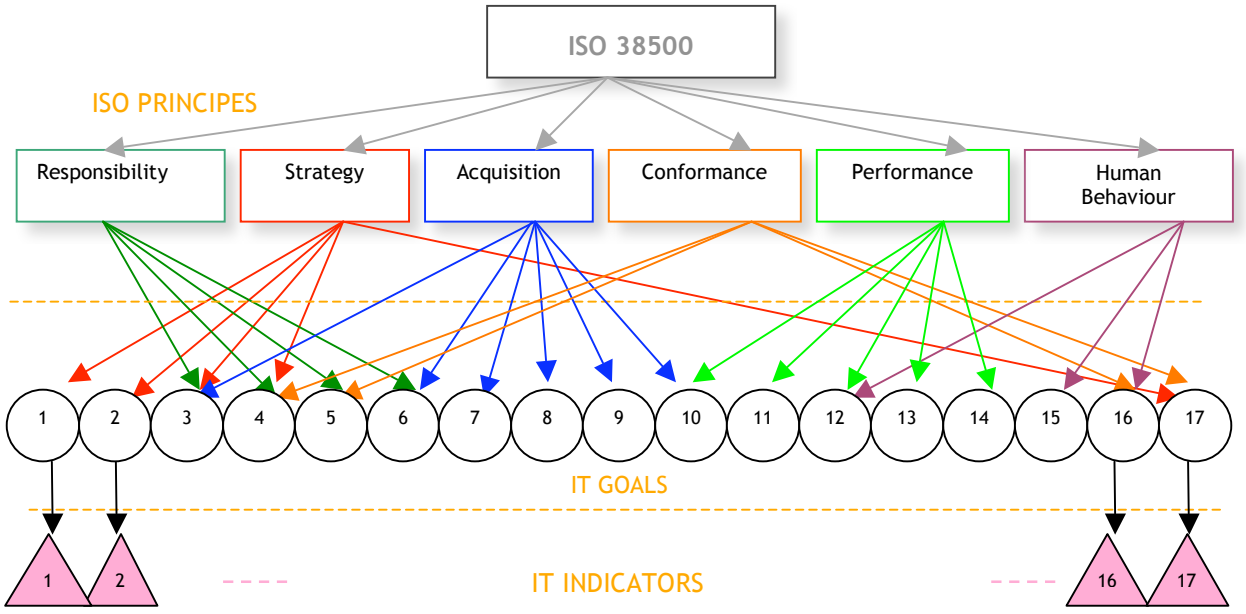


Table 1. IT Goals for ITG4U framework

1	Have a very clear idea of the vision and IT strategy for the whole university.
2	Align the IT strategy and the institutional strategy (business strategy).
3	Reach IT objectives using an integral IT governance system.
4	Have a decision making structure aligned with the IT strategy.
5	Provide high level IT policies and procedures which comply with external laws and regulations and support international standards.
6	Make IT decisions that are correctly reasoned and effective.
7	Know and achieve the return value on IT investment.
8	IT projects must achieve the planned goals.
9	Define an IT architecture that will include process definition and system integration.
10	Acquire the necessary technology to fulfil the requirements of the institution.
11	Guarantee that the established ITs are working according to plan.
12	IT-based services must meet the level required by the users.
13	Know and manage IT associated risks.
14	Ensure that IT systems are flexible and agile in responding to future changes.
15	Have adequate and sufficiently trained staff who can govern IT efficiently.
16	Incorporate respect for people and social and environmental values within the IT strategy.
17	Exchange IT experiences with other organisations and with society as a whole.

Table 2. IT Goals mapping several frameworks

						C		COBIT
					UK			JISC (United Kingdom)
				WR				Weill y Ross
			CM					Calder-Moir
		E						ECAR (EDUCAUSE)
	V							Van Grembergen
R								CRUE Researchers
								IT Goals from ITG4U
		E	CM		UK	C	1	Have a very clear idea of the vision and IT strategy for the whole university.
	V	E	CM		UK	C	2	Align the IT strategy and the institutional strategy (business strategy).
		E	CM	WR	UK	C	3	Reach IT objectives using an integral IT governance system.
	V		CM	WR	UK	C	4	Have a decision making structure aligned with the IT strategy.
	V	E	CM	WR	UK	C	5	Provide high level IT policies and procedures which comply with external laws and regulations and support international standards.
		E		WR	UK	C	6	Make IT decisions that are correctly reasoned and effective.
	V	E	CM	WR	UK	C	7	Know and achieve the return value on IT investment.
	V	E	CM	WR	UK	C	8	IT projects must achieve the planned goals.
	V	E	CM	WR		C	9	Define an IT architecture that will include process definition and system integration.
	V	E	CM	WR	UK	C	10	Acquire the necessary technology to fulfil the requirements of the institution.
	V				UK	C	11	Guarantee that the established ITs are working according to plan.
	V	E	CM		UK	C	12	IT based services must meet the level required by the users.
	V		CM			C	13	Know and manage IT associated risks.
	V		CM			C	14	Ensure that IT systems are flexible and agile in responding to future changes.
	V	E	CM		UK	C	15	Have adequate and sufficiently trained staff who can govern IT efficiently.
R							16	Incorporate respect for people and social and environmental values within the IT strategy.
R							17	Exchange IT experiences with other organisations and with society as a whole