

IT Governance and COBIT®

ISACA North of England Chapter

Leeds

November 26th 2008
Charles Mansour CISA





Me

Charles Mansour, CISA

23 Years in IT Audit

UK Customs 1980 - 1986

Banking and Financial Services 1986-2002

Audit & Risk Service 2002 – 2007

Past President of ISACA London Chapter

Involved with COBIT® since 1993

ISACA International Membership Board

Member

2004 -07

Copyright Charles Mansour, CISA & Risk Service 2006 COBIT® and COBIT 4.0® are IAIT® Copyright 1996, 2000, 2006 IAIT



Session Summary

1. IT Governance Overview
2. Introduction to COBIT®
3. Metrics for IT Governance
4. Implementing COBIT®
5. Where Are We Now?



IT Governance Overview

Everything Under Control?



Is IT Working??

“IT has been the longest running disappointment in business in the last 30 years!”
Jack Welch, Chairman, General Electric, World Economic Forum, Davos, 1997

“Technology can help fulfil a visionary dream, but often its use is closer to a sobering nightmare!”
Vesa Vaino, CEO Merita Bank, SIBOS, Helsinki, 1998

“I am writing a book on the history of information technology...in order to better understand why it is such a mess!”
Philippe Corniou, CIO, Renault, IT Governance Forum, Paris, 2001

“IT investments did not have an impact on productivity in 53 out of 59 economic sectors”

McKinsey report 2001

“50% of IT initiatives fail to meet business objectives.”

The IT aspects of corporate governance are one of the things that chief executives think they don't have to understand - until it bites them!

Peter Morriss KPMG

But sometimes they do get bitten..

- Denial of service
- Viruses
- Poor systems reliability
- Failed projects
- Website defacement
- Incorrect management reporting

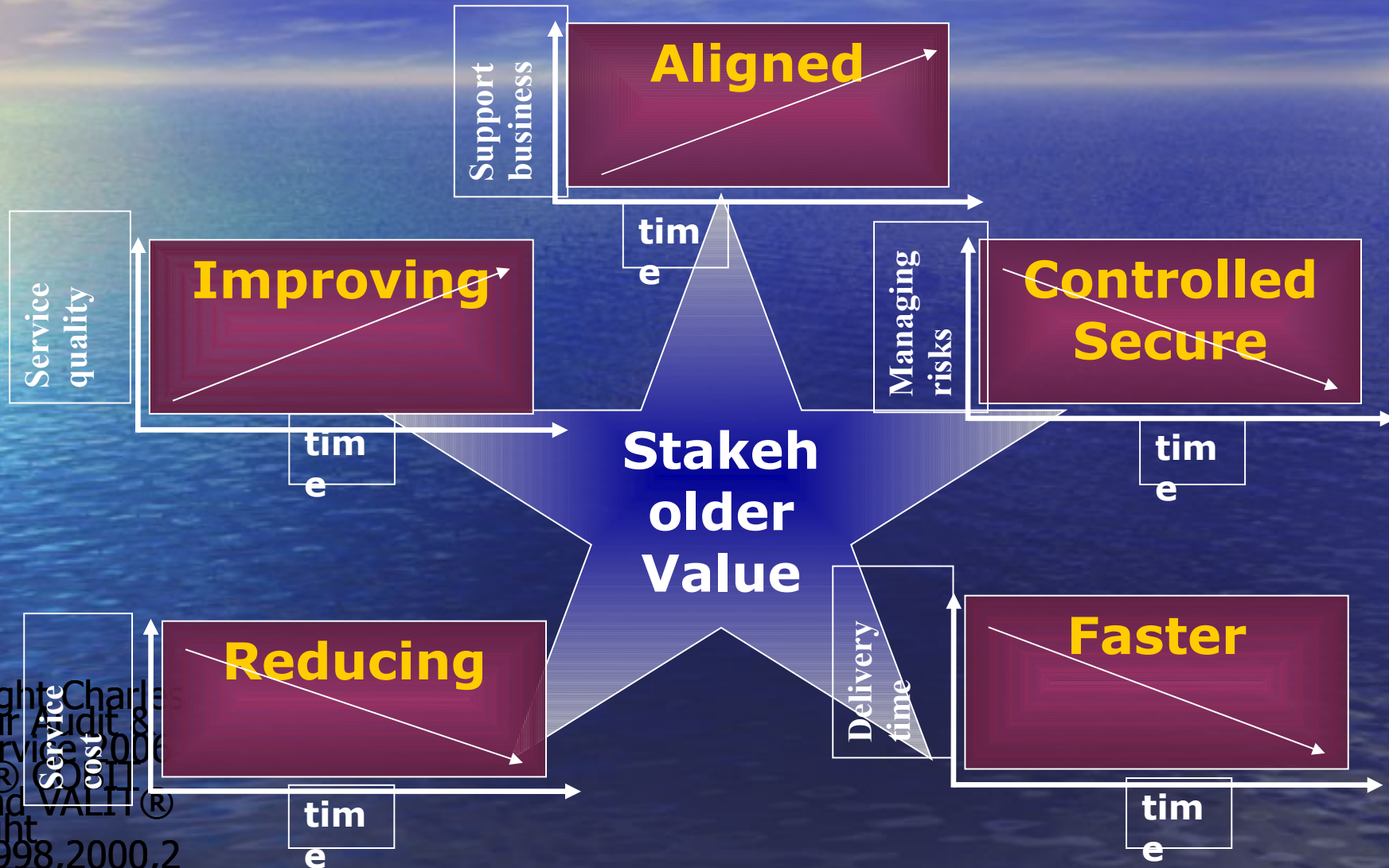
• Excess costs

IT Is Critical to Most Businesses

This criticality arises from:

- The increasing dependence on reliable, accurate and timely information and the systems and communications that deliver it
- The need for 24/7/365 availability to do business and to ensure customer trust
- The dependence on entities beyond the direct control of the enterprise
- IT failures and security breaches increasingly impacting reputation and enterprise value
- The potential for technologies to dramatically change organisations and business practices, create new opportunities and reduce costs

What do we want to achieve ?



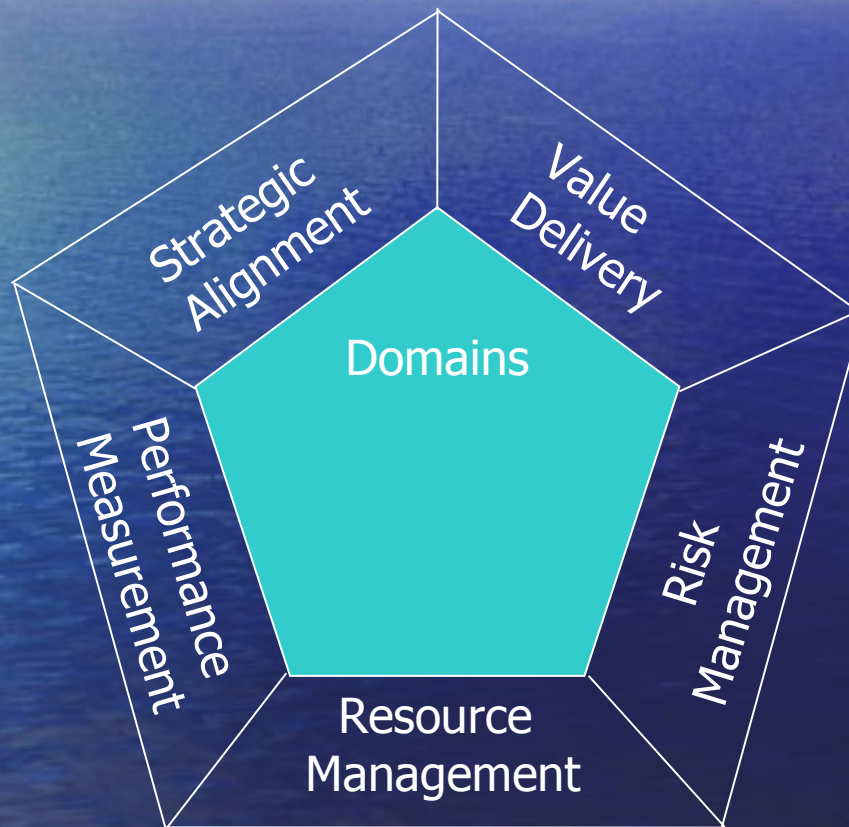
IT Governance Problem Indicators include.....

- IT not on Board Room agenda
- IT not directly represented at Board level
- IT and Business strategy not concurrently prepared and aligned
- IT managed by technology rather than by business focus
- History of late or failed business system implementations
- IT seen as a cost rather than as a provider of value
- External or internal perception that organisation is not making the most of technology
- Inadequate or non-existent IT related metrics
- Technology investments justified on cost savings rather than on revenue enhancement

Reasons to Implement an IT Governance Framework

-we obtain maximum value from our investment in IT ;
-we continue to focus our IT investments in highest value areas;
-the efficiency and effectiveness of our IT operations compares well against our competitors;
-we obtain maximum leverage globally from our IT investments.
-we continue to attract and retain the best people;
-IT properly supports, enables, and enhances our business;
-we improve our ability to manage our IT related project portfolio;
-IT related risks are being properly managed and mitigated.

IT Governance Domains



Example Statement on Corporate Governance

- xxxx is committed to good corporate governance practices. xxx's Board of Directors has adopted a Corporate Governance Policy, which govern the functions, structure, membership and conduct of the Board. The Board has also adopted written charters for each of its three standing committees, including the Audit Committee, Compensation Committee and Corporate Governance Committee. xxx's Global Business Code of Conduct applies to all xxx employees worldwide, and to all xxx consultants, independent contractors, business partners and other representatives in the xxx community, worldwide. xxx is committed to promoting integrity and maintaining high standards of ethical conduct in all of its activities.

- **Nothing about IT!**

IT's Role in the Business

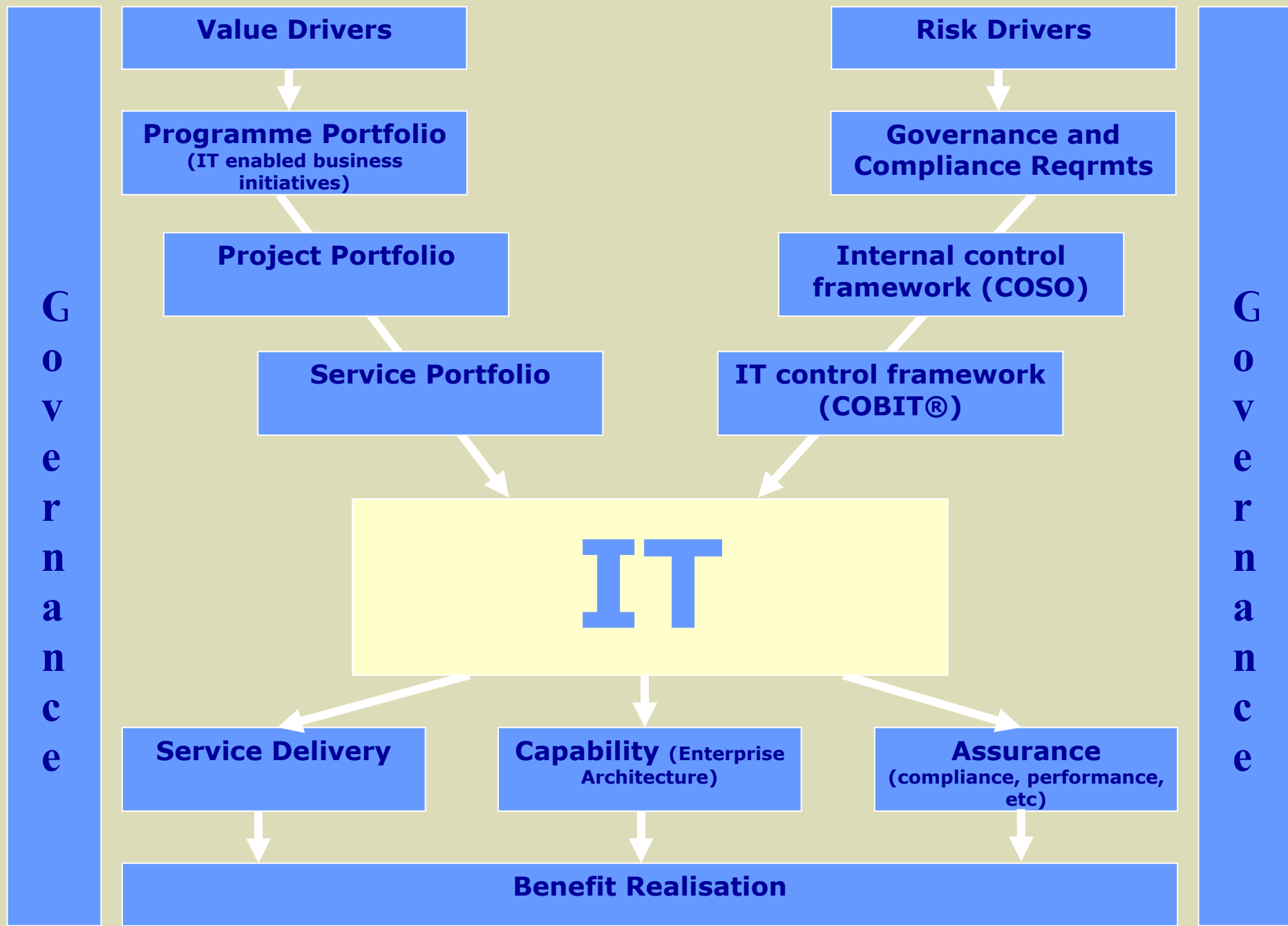
- Treated in many enterprises as a critical support unit ignored by Board
 - Along with HR and Finance
- IT is MISSION CRITICAL in most of today's enterprises
- But still not on Board Agenda
- **NO IT = No Business!**

The Board's View of IT?



Copyright Charles
Mansour Audit &
Risk Service 2006
COBIT® COBIT
4.0® and VALIT®
Copyright
1996, 1998, 2000,
2006 by IT

www.willthomas.net



Value Drivers

Risk Drivers

Programme Portfolio

(IT enabled business initiatives)

Governance and Compliance Reqrmts

Project Portfolio

Internal control framework (COSO)

Service Portfolio

IT control framework (COBIT®)

IT

Service Delivery

Capability (Enterprise Architecture)

Assurance (compliance, performance, etc)

Benefit Realisation

G
o
v
e
r
n
a
n
c
e

G
o
v
e
r
n
a
n
c
e

● Introduction to COBIT®



LEADING THE IT GOVERNANCE COMMUNITY

COBIT®

4.1

Framework
Control Objectives
Management Guidelines
Maturity Models

Copyright Charles
Mansour Audit &
Risk Service 2006
COBIT® COBIT
4.0® and VALIT®
Copyright
1996, 1998, 2000, 2
006 by IT

What is COBIT®?

- Best Practice
- Framework of Domains and Processes
- Benchmark
- Source of metrics

How Does it Work?

- Links IT to Business Requirements
- Organises IT activities into domains (4) and processes (34)
- 214 Control Objectives
- Identifies major IT resources
- Provides management control objectives
- Provides suggested measures

How Can COBIT® Help?

- IT and Business Strategic Planning
- Aligning IT and Business Goals
- Recruiting and Retaining IT Staff
- Measuring IT and IS Organisation Efficiency
- Using IT for Competitive Breakthroughs
- Reducing IT Costs
- Demonstrating Business Value of IT
- Developing an IT Architecture
- Improving Project Delivery

COBIT®'s Audience

- Board
 - Overall responsibility for IT Governance
 - Balance risk and control investment in an often unpredictable Business and IT environment
 - Issues
 - Management
- Senior Management
 - Provide ongoing assurance on the security and controls of the IT services upon which they depend to deliver their products and services to internal and external customers
 - Measure performance
 - Benchmark
 - Address Gaps
- Governance, Control & Audit
 - Control Objectives

COBIT® and Other Standards

- COSO
- ISO38500

COSO and IT Governance

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

ISO38500: Corporate Governance of Information Technology

- Published June 2008
- A 'high level principles based advisory standard' for Directors when evaluating, directing and monitoring the use of IT in their organisations
- Provides 'broad guidance on the role of the governing body'

encourages organisations to use appropriate

ISO38500: Objectives

- Assuring stakeholders that if the standard is followed they can have confidence in the organisation's corporate governance of IT
- Informing and guiding directors in governing the use of IT in their organisations
- Providing a basis for the corporate governance

ISO38500

- Framework for Good Corporate Governance of IT
 - Six Principles
 1. Responsibility
 2. Strategy
 3. Acquisition
 4. Performance
 5. Conformance

Three Main Tasks

- Evaluate
 - Examine
 - Continuously Evaluate
 - Current and Future Business Needs
- Direct
 - Assign and Direct Responsibilities for Plans (IT Investment) and Policies (Sound Behaviour)

Three Main Tasks (cont'd)

- Monitor
 - Using appropriate measurement systems, the performance of IT
 - Ensure in line with business objectives
 - Regulatory, etc compliance

COBIT® and Other Standards



Copyright © Mansour Audit & Risk Service 2006
COBIT® COBIT
4.0® and VALIT®
Copyright
1996, 1998, 2000, 2
006 by IT

COBIT® Management Guidelines

- Contains the requirements to establish an IT Governance Framework
- For each Process (34)
 - Business Requirement for IT
 - Key IT Goals
 - Key Controls
 - Key Metrics
 - Impact on
 - IT Resources
 - Information Criteria
 - Control Objectives
 - Capability Maturity Model
 - Key Management Activities
 - RACI Chart
 - Goals and Detailed Metrics

How to Identify Critical IT Domains, Processes and Control Objectives

- Depends on the enterprise
- What matters?
- Risk Assessment
- Who knows?
 - IT Director
 - Finance Director
 - Executive
 - Business Unit Managers
- Senior Management workshop a good approach
- **Business knows the business it's in!**

Metrics

“In IT, if you are playing the game and not keeping score, you are only practising.”

IT Balanced Scorecard – Refinements from Traditional Version

- IT Governance requires a different perspective
 - Enterprise contribution—How do business executives view the IT department?
 - User orientation—How do users view the IT department?
 - Operational excellence—How effective and efficient are the IT processes?
 - Future orientation—How well is IT positioned to meet future needs?

Sample IT Balanced Scorecard

Corporate Contribution

- Ensuring effective IT governance*
- Align IT with business objectives
 - Deliver value
 - Manage costs
 - Manage risks
 - Achieve intercompany synergies

Customer Orientation

- Measuring up to business expectations*
- Service Provider
- Demonstrate competitive costs
 - Deliver good service
- Strategic Contributor
- Achieve positive impact on business processes
 - Enable achievement of business strategies

Future Orientation

- Building the foundation for future delivery and continuous learning and growth*
- Attract and retain people with key competencies
 - Focus on professional learning and development
 - Build a climate of empowerment and responsibility
 - Measure/reward individual and team performance
 - Capture knowledge to improve performance

Information

Operational Excellence

- Performing the IT functions with increasing credibility and impact*
- Operational Excellence
- Mature internal IT processes
 - Manage operational service performance
 - Achieve economies of scale
 - Build standard, reliable technology platforms
 - Deliver successful IT projects
- Business Partnership
- Deliver successful IT projects
 - Support technology users
 - Plan and manage IT service delivery
 - Understand business unit strategies
- Technology Leadership
- Understand business unit strategies
 - Propose and validate enabling solutions
 - Understand emerging technologies
 - Develop enterprise architecture

Implementation

Copyright Charles
Mansour Audit &
Risk Service 2006
COBIT® COBIT
4.0® and VALIT®
Copyright
1996, 1998, 2000, 2
006 by IT

Who Should 'Own' COBIT® IT Governance Processes

- Boardroom should 'own' the IT Governance process
- Process Owner for IT is CIO or the IT Director
 - Responsible for day to day working
 - Collation of data
- Usually responsible for preparing flows of information up to Senior Management

Board Toolkit: Tasks and Responsibilities

| IT Governance Activities | Board and/or Management | Activity Type | IT Governance Activities | Board and/or Management | Activity Type |
|--|-------------------------|---------------|--|-------------------------|---------------|
| Become informed of role and impact of IT on the enterprise | B/M | Plan | Make transformation happen | B/M | Direct |
| Set direction and expected return | B | Direct | Define constraints within which to operate | B | Direct |
| Determine required capabilities and investments | M | Plan | Acquire and mobilise resources | M | Organise |
| Assign responsibilities | B/M | Direct | Measure performance | B | Control |
| Sustain current operations | M | Organise | Manage risk | B/M | Control |
| | | | Obtain assurance | B | Control |

IT Governance Self Assessment

- The concise IT Governance Self-Assessment checklist provided in the section Implementation Guide, asks management to determine, for each of the COBIT® processes:
 - how important the process is for their business objectives;
 - whether the process is well performed (the combination of importance and performance provide a strong indicator of risk)
 - who performs the process and who is accountable for the process (and is accountability unequivocal and accepted);
 - whether the process and its control is formalised, i.e., is there a thorough contract for an outsourced activity or a clear set of documented procedures for internal processes; and
 - whether the process is audited.

IT Governance Self Assessment

| Risk | | | | Who Does It? | | | | | | |
|------------|-------------|---|--|--------------|-------|---------|------------|---------|----------|---------------------|
| Importance | Performance | Importance – how important for the organisation on a scale from 1 (not at all) to 5 (vary) Performance – how well it is done from 1 (don't know or badly) to 5 (vary well) Audited – Yes, No or ? Formality – is there a contract, an SLA or a clearly documented procedure (Yes, No or ?) Accountable – Name or "don't know" | | IT | Other | Outside | Don't Know | Audited | Formally | Who is accountable? |
| | | COBIT's Domains and Processes | | | | | | | | |
| | | PLANNING & ORGANISATION | | | | | | | | |
| | | PO1 | Define a Strategic IT Plan | | | | | | | |
| | | PO2 | Define the Information Architecture | | | | | | | |
| | | PO3 | Determine the Technological Direction | | | | | | | |
| | | PO4 | Define the IT Organisation and Relationships | | | | | | | |
| | | PO5 | Manage the Information Technology Investment | | | | | | | |
| | | PO6 | Communicate Management Aims and Direction | | | | | | | |
| | | PO7 | Manage Human Resources | | | | | | | |
| | | PO8 | Ensure Compliance with External Requirements | | | | | | | |
| | | PO9 | Assess Risks | | | | | | | |
| | | PO10 | Manage Projects | | | | | | | |

IT Governance Self Assessment Cut Down Version

- For each of the COBIT® processes (34)
 - RAG report
 - Assessment of Current Status
 - Business Impact
 - Risk
 - All Red
 - Consider for attention

● Needs to be open and honest

Where are we?

| INITIAL COBIT EVALUATION | | | | |
|-------------------------------|--|----------------|-----------------|--------|
| IT GOVERNANCE SELF-ASSESSMENT | | Current Status | Business Impact | Risk |
| COBIT DOMAINS AND PROCESSES | | Good | High | High |
| | | Satisfactory | Medium | Medium |
| | | Weak | Low | Low |
| Planning and Organisation | | | | |
| PO1 | Define a Strategic IT Plan | Weak | Medium | Medium |
| PO2 | Define the Information Architecture | Weak | High | High |
| PO3 | Determine the Technological Direction | Good | High | High |
| PO4 | Define the IT Organisation and Relationships | Weak | High | High |
| PO5 | Manage the IT Investment | Weak | Medium | Medium |
| PO6 | Communicate Management Aims and Direction | Weak | Low | Low |
| PO7 | Manage Human Resources | Satisfactory | Low | Low |
| PO8 | Ensure Compliance with External Requirements | Satisfactory | High | Low |
| PO9 | Assess Risks | Good | High | Low |
| PO10 | Manage Projects | Weak | Medium | Low |
| PO11 | Manage Quality | Weak | Low | Low |

Where are we?

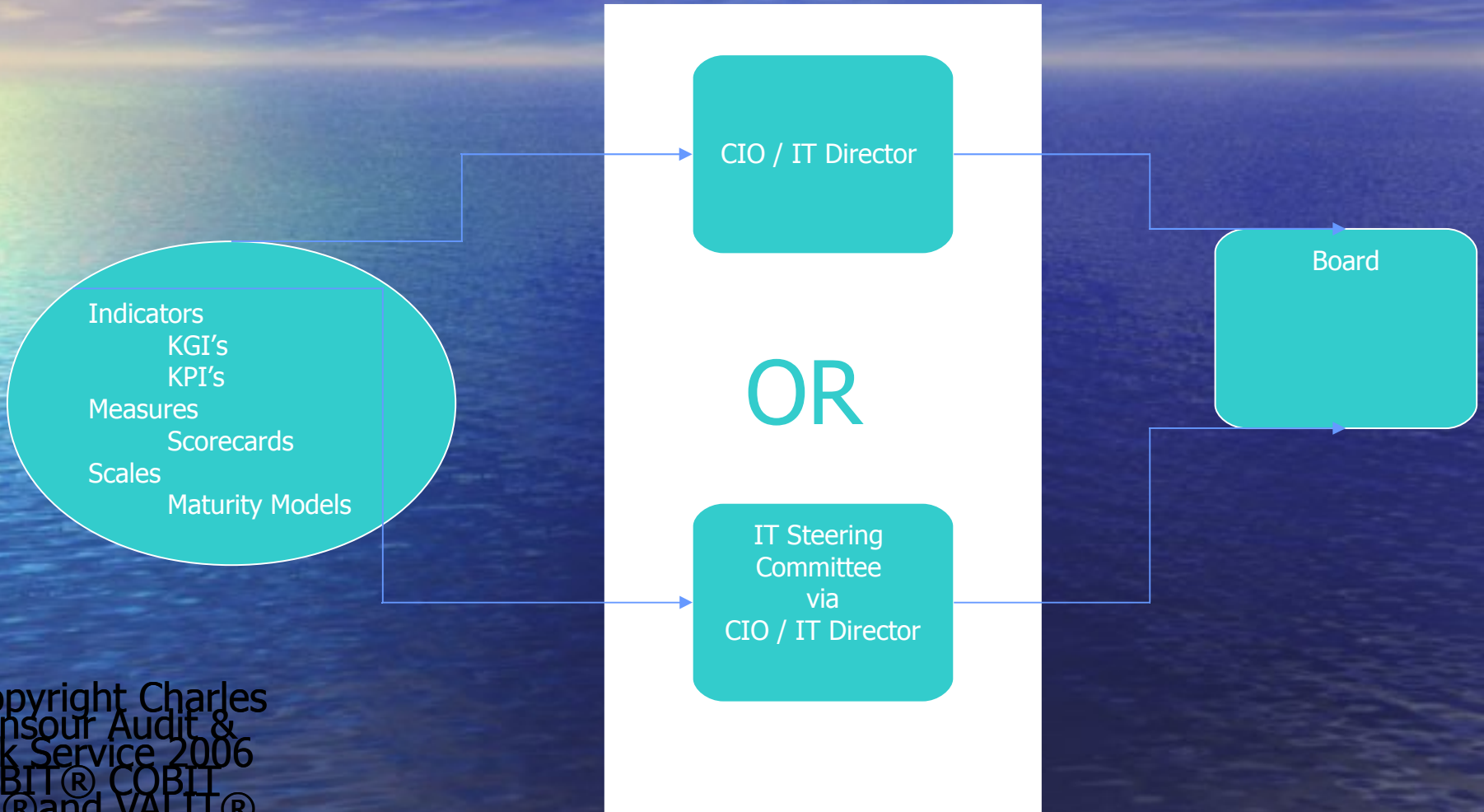
INITIAL COBIT EVALUATION

| IT GOVERNANCE SELF-ASSESSMENT | | Current Status | Business Impact | Risk |
|-------------------------------|---------------------------------------|----------------|-----------------|--------|
| COBIT DOMAINS AND PROCESSES | | Good | High | High |
| | | Satisfactory | Medium | Medium |
| | | Weak | Low | Low |
| Manage Change | | Good | Low | Medium |
| 6.1 | Change Request Initiation and Control | Good | Low | Medium |
| 6.2 | Impact Assessment | Weak | Low | Medium |
| 6.3 | Control of Changes | Good | Low | Medium |
| 6.4 | Documentation and Procedures | Weak | Low | Low |
| 6.5 | Authorised Maintenance | Good | Low | Low |
| 6.6 | Software Release Policy | Good | Low | Low |
| 6.7 | Distribution of Software | Good | Low | Low |

How to Implement

- Consider a COBIT® process area for 'piloting'
 - Ideally a process that can show benefit
- Needs 'friendly' process area management
- Treat it as a project
- Needs to demonstrate tangible business benefit before decision makers will be convinced to 'roll out' to other areas

Reporting



Implementation Considerations

- How far should we go, and is the cost justified by the benefit?
- What are the indicators of good performance?
- What are the critical success factors?
- What are the risks of not achieving our objectives?
- What do others do?

● How do we measure and compare?

COBIT® Limitations

- COBIT® alone won't put a Governance Culture in place
 - Still need commitment and tone from the top
 - COBIT® gives you the tools to persuade
- COBIT® itself won't change minds
 - Key people need orientation and education
- COBIT® is not industry specific
 - Need to tailor approach to fit your business

Beware of.....

- Assuming that you haven't got effective IT Governance in place
 - Use the checklists and Maturity Models to make sure there's a job to do
- Producing a 25 page Governance report for the Board
 - It won't get read even if it's good news
 - One or two sides of A4 is best
 - If there's a lot of detail, maybe an IT Steering Committee filtering Board reporting is better
- Overestimating benefits
 - Be realistic
- Underestimating effort involved

Wrong things to do

- Implement IT Governance by 'pushing up' rather than 'cascading down'
- Pretend you've convinced the key players when you haven't
- Lose focus
- Fail to deliver benefits
- Fail to include third party / outsource companies in governance scope

Right Things to do

- Emphasise the downstream benefits
- Get a COBIT® Champion at an early stage
 - Must be at Executive level
 - Involve at key stages
- Get the right people on board
- If IT needs Board level representation
 - Appoint an IT Director
- Pick a pilot that will deliver tangible benefit
- Educate
- Plan IT Governance Implementation as a Project
- Be realistic and honest
 - Don't overstate the benefits

But Don't Forget

- If you can get IT Governance in place
 - The benefits are huge
 - You don't just transform IT, you transform the enterprise!
 - Better ROI from IT
 - Better strategic alignment
 - IT Doing the right things at the right time
 - Better management of key risks
 - More competitive IT effort
 - Getting the right people in IT

IT Governance Global Status Report - 2008

- Key Messages

- Good IT governance practices are known and applied but not universally
- Organisations know who can help them implement IT Governance, but appreciation for the available expertise and delivery capability is only average

IT Governance Global Status Report - 2008

- Key Messages

- Action is being taken or plans are underway to implement IT governance activities. A large increase is evident when compared with the 2006 report
- Organisations use the well known frameworks and solutions

IT Governance Global Status Report - 2008

● Key Messages

- COBIT® awareness has exceeded 50 percent and adoption and use remains at about 30 percent
 - 25 to 35 percent of respondents apply COBIT® very strictly or are very strict
 - 50 percent of respondents indicate that COBIT® is 'one of the reference sources'
 - In general there is high appreciation of COBIT®, as has been seen in prior reports

Operations Control

Copyright Charles
Mansour Audit &
Risk Service 2006
COBIT® COBIT
4.0® and VALIT®
Copyright
1996, 1998, 2000, 2
006 by IT

Thank you!

Copyright Charles
Mansour Audit &
Risk Service 2006
COBIT® COBIT
4.0® and VALIT®
Copyright
1996, 1998, 2000, 2
006 by IT