



Cost Management Controls in IT operations using COBIT Framework

Sanjiv Arora, CISA, CISM, CGEIT

Principal Consultant, CEO



**TECHNOLOGICS
& CONTROLS**

Protecting the ABCs of your business.

24-Oct-2009



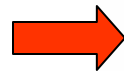
Agenda



- About Technologicals and Controls
- IT Governance
- COBIT framework
- Cost Management Controls in IT Operations using COBIT

Introduction : Technologic & Controls

- Founded in 2001
- Based in New Delhi, India
- Represented in USA and Australia
- Represented in Jaipur and Pune in India
- **Services:** IT Audits, Risk Management consulting, Information security assessment and management, IT Governance services, compliance and related services.
- **Products:** Sole reseller in India of DataSec S.R.L providing software solutions based on COBIT / ISO27001 / COSO and other standards



IT Governance – Need?

In all large corporations, there is a pervasive fear that someone, somewhere is having fun with a computer on company time. Networks help alleviate that fear.

- John C Dvorak



What is driving today's businesses?

Assertive Stakeholders
Aggressive Competition
Emerging Regulations
Recessionary trends direct / indirect
Extremely high IT Dependence



Impacts

Enterprise Governance

IT Governance - Alignment

Value Delivery Business Benefits

- Secure
 - On Time
 - Within Budgets
 - Good Quality
 - Reduce Expense
 - Proven best practices
- Customer satisfaction
 - Brand Loyalty
 - Competitive advantage
 - Profitability

Crux - Fill what's empty. Empty what's full. And scratch where it itches. – Murphy's law

Why COBIT?

- Better alignment based on business focus
- Demonstrates management viewpoint and expectations
- Clear ownerships and responsibilities based on processes
- Increasing acceptability with third parties and regulators
- Eases IT Governance communication between stakeholders and other parties
- Fulfillment of the COSO requirements for IT control environment

Absence of IT Governance framework: Impact

- Business and governance requirements are not delivered effectively without adopting a framework for IT to
 - Make a link to the business requirements
 - Measure performance against the requirements transparent
 - Organize its activities into a generally accepted process model
 - Identify the resources to be leveraged
 - Define management control objectives to be considered

COBIT Framework

- Plan and Organise
 - P01 - Define a Strategic IT Plan
 - P02 - Define the Information Architecture
 - P03 - Determine Technological Direction
 - P04 - Define the IT Processes, Organisation and Relationships
 - P05 - Manage the IT Investment
 - P06 - Communicate Management Aims and Direction
 - P07 - Manage IT Human Resources
 - P08 - Manage Quality
 - P09 - Assess and Manage IT Risks
 - P010 - Manage Projects
- Acquire and Implement
 - A11 - Identify Automated Solutions
 - A12 - Acquire and Maintain Application Software
 - A13 - Acquire and Maintain Technology Infrastructure
 - A14 - Enable Operation and Use
 - A15 - Procure IT Resources
 - A16 - Manage Changes
 - A17 - Install and Accredite Solutions and Changes
- Deliver and Support
 - DS1 - Define and Manage Service Levels
 - DS2 - Manage Third-party Services
 - DS3 - Manage Performance and Capacity
 - DS4 - Ensure Continuous Service
 - DS5 - Ensure Systems Security
 - DS6 - Identify and Allocate 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

Process **P04** Define the IT Processes, Organisation and Relationships

Description
An IT organisation is defined by considering requirements for staff, skills, functions, accountability, authority, roles and responsibilities, and supervision. This organisation is embedded into an IT process framework that ensures transparency and control as well as the involvement of senior executives and business management. A strategy committee ensures board oversight of IT, and one or more steering committees in which business and IT participate determine the prioritisation of IT

Business Requirement
Being agile in responding to the business strategy while complying with governance requirements and providing defined and competent points of contact

Is enabled by
- Defining an IT process framework
- Establishing appropriate organisational bodies and structure
- Defining roles and responsibilities

Considerations
Establishing transparent, flexible and responsive IT organisational structures and defining and implementing IT processes with owners, roles and responsibilities integrated into business and

Is Measured by
- Percent of roles with documented position and authority descriptions
- Number of business units/processes not supported by the IT organisation that should be supported, according to the strategy

Desirable Score

IT Resources

Info. Criteria

Domain

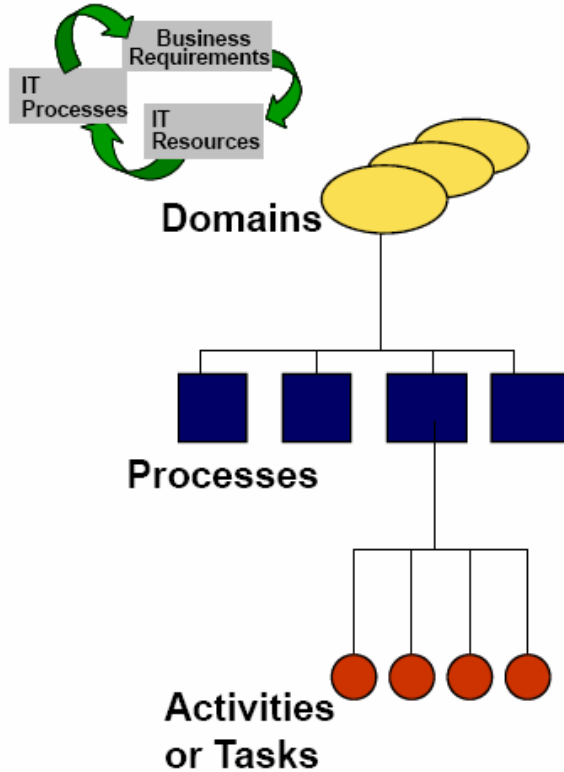
IT Governance Areas

- Value Delivery
- S** Strategic Alignment
- P** Risk Management
- P** Resource Management
- Performance Measurement

COBIT Framework

Figure 4—Interrelationships of COBIT Components

Process Orientation

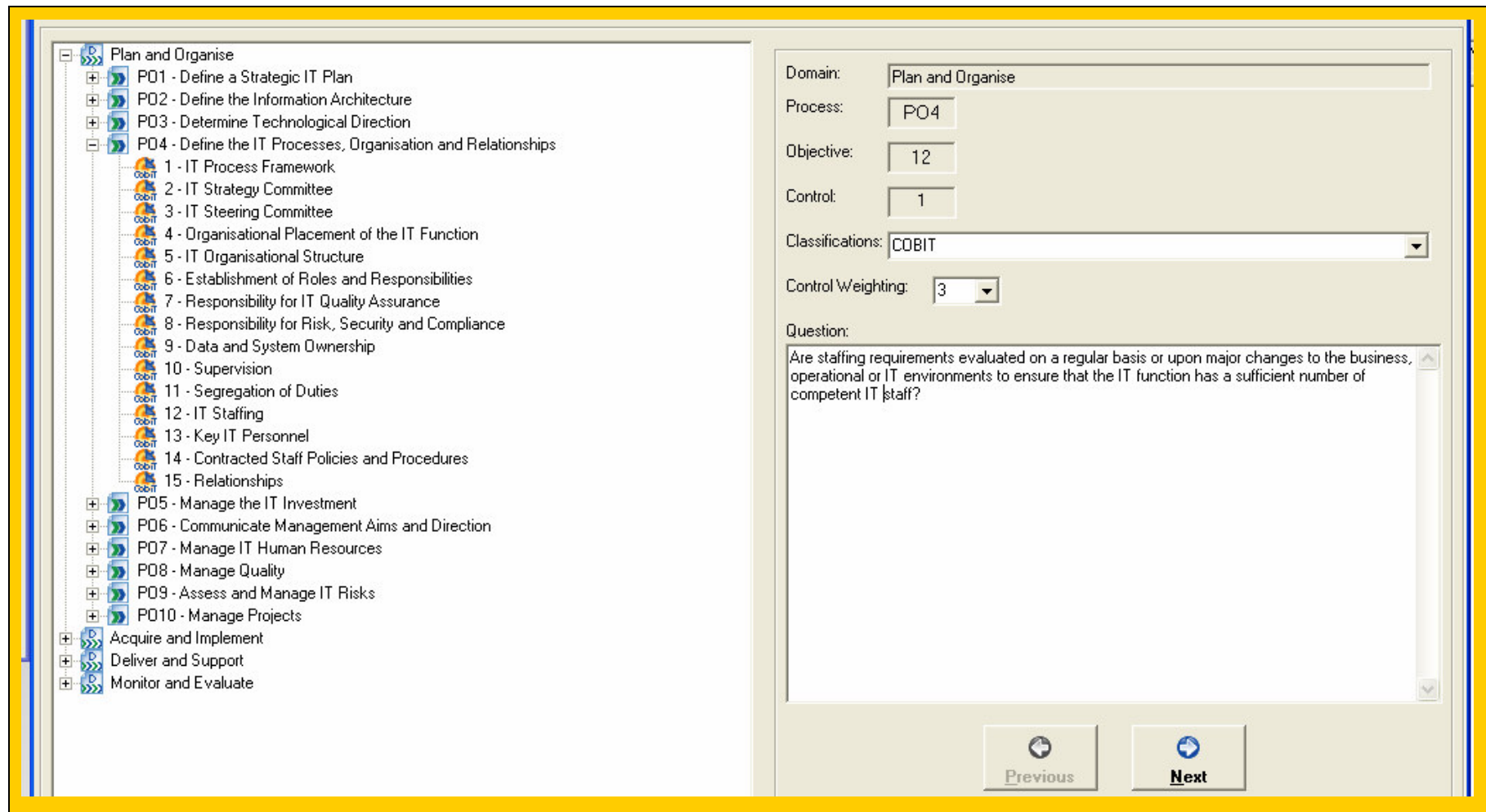
Natural grouping of processes, often matching an organisational domain of responsibility

A series of joined activities with natural control breaks

Actions needed to achieve a measurable result—activities have a life cycle, whereas tasks are discrete

Source – ITGI presentation materials

COBIT – Key Objectives and Controls

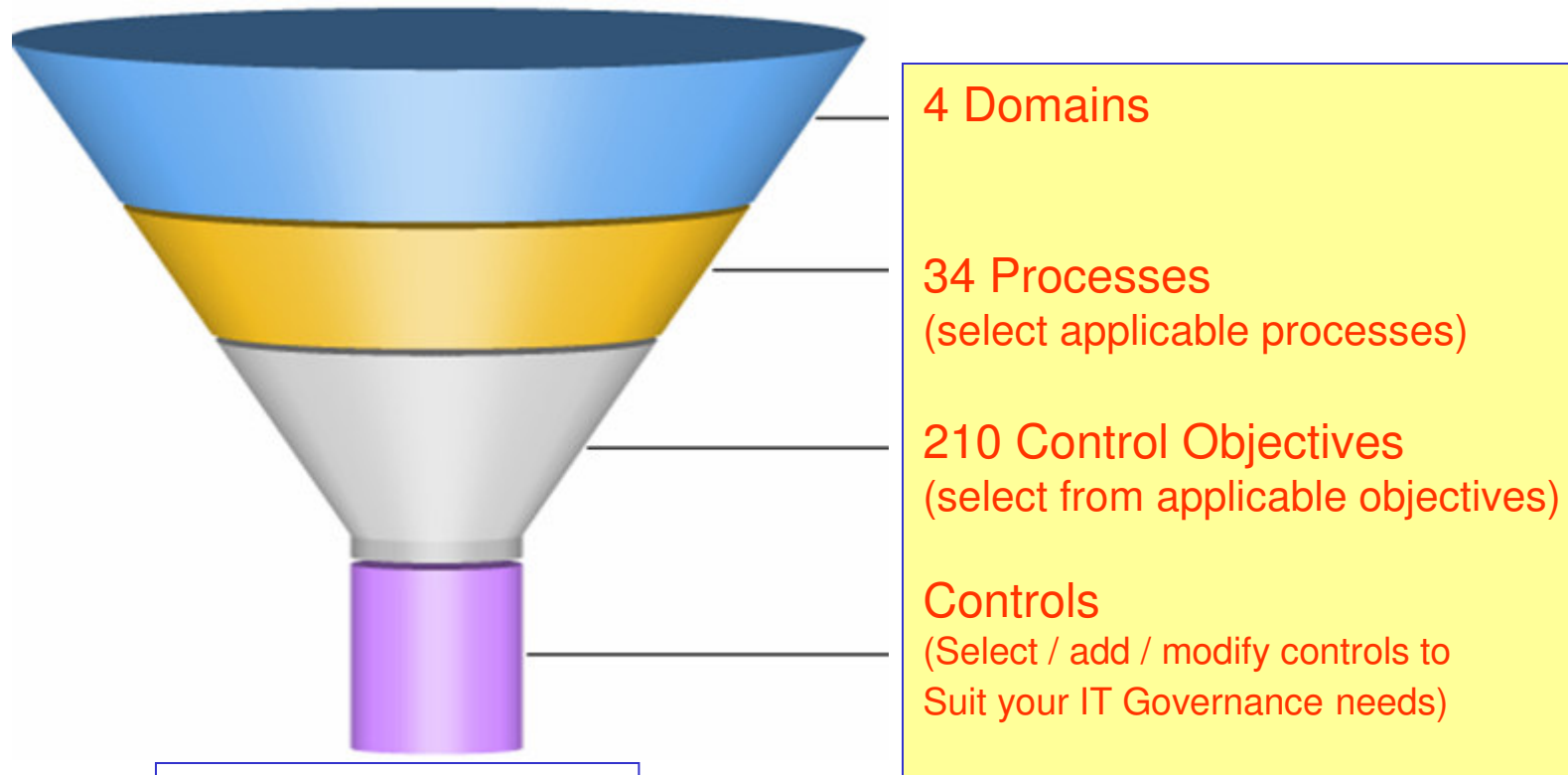


The screenshot displays the COBIT software interface. On the left, a tree view shows the hierarchy of domains and processes. The 'Plan and Organise' domain is expanded, showing processes PO1 through PO10. Under PO4, 'Define the IT Processes, Organisation and Relationships', 15 objectives are listed, including '12 - IT Staffing'. On the right, the control configuration panel shows the following details:

- Domain: Plan and Organise
- Process: PO4
- Objective: 12
- Control: 1
- Classifications: COBIT
- Control Weighting: 3
- Question: Are staffing requirements evaluated on a regular basis or upon major changes to the business, operational or IT environments to ensure that the IT function has a sufficient number of competent IT staff?

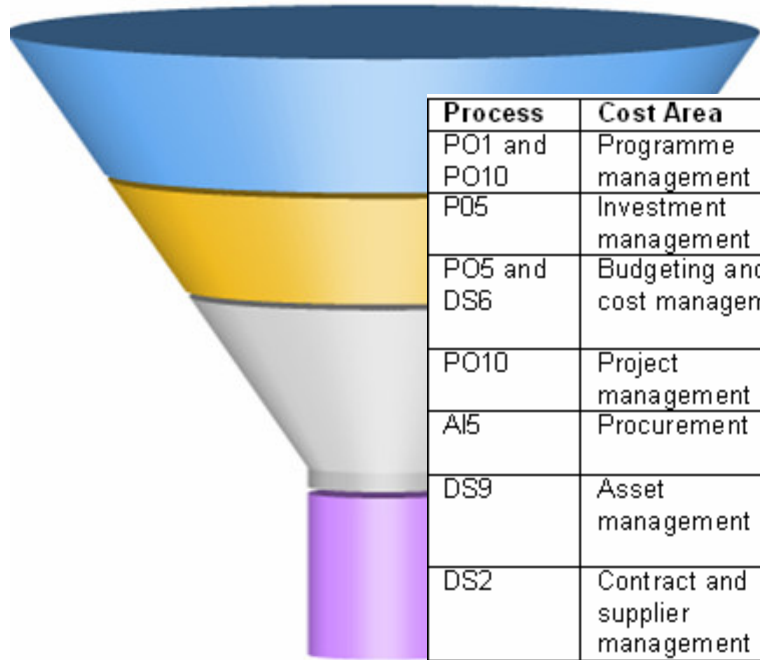
At the bottom of the control configuration panel, there are 'Previous' and 'Next' navigation buttons.

COBIT – Map Business objectives using Funnel Approach



* Equals =
4 Domains
22 processes
145 controls objectives
N Controls
* An example

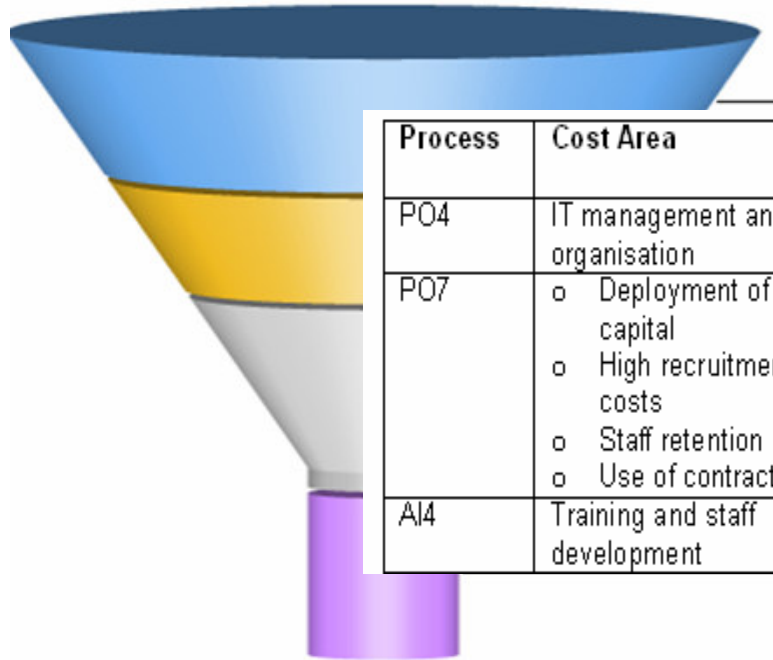
COBIT – Processes and Controls – Tangible Cost Management



Process	Cost Area	Immature Processes and tangible cost savings
PO1 and PO10	Programme management	Inability to prioritise and cancel IT initiatives
PO5	Investment management	Poor business cases and returns on IT-related Investments
PO5 and DS6	Budgeting and cost management	Poor understanding of current costs; inability to optimise the budget and identify how to spend less but obtain more value
PO10	Project management	Projects running late and over budget
AI5	Procurement	Inability to negotiate good deals and obtain value for Money
DS9	Asset management	Cost of assets not understood; bad asset replacement strategy; software licenses not being used, hardware maintenance too high
DS2	Contract and supplier management	Bad supplier relationships and poor service/product delivery
DS1 and DS8	Service levels and service desk	Poor service delivery; service calls and incidents too High
DS13	Operations and systems management	Too many tools and not enough efficiency; no standardization procedures

Cost Management Controls = Selected 10 processes

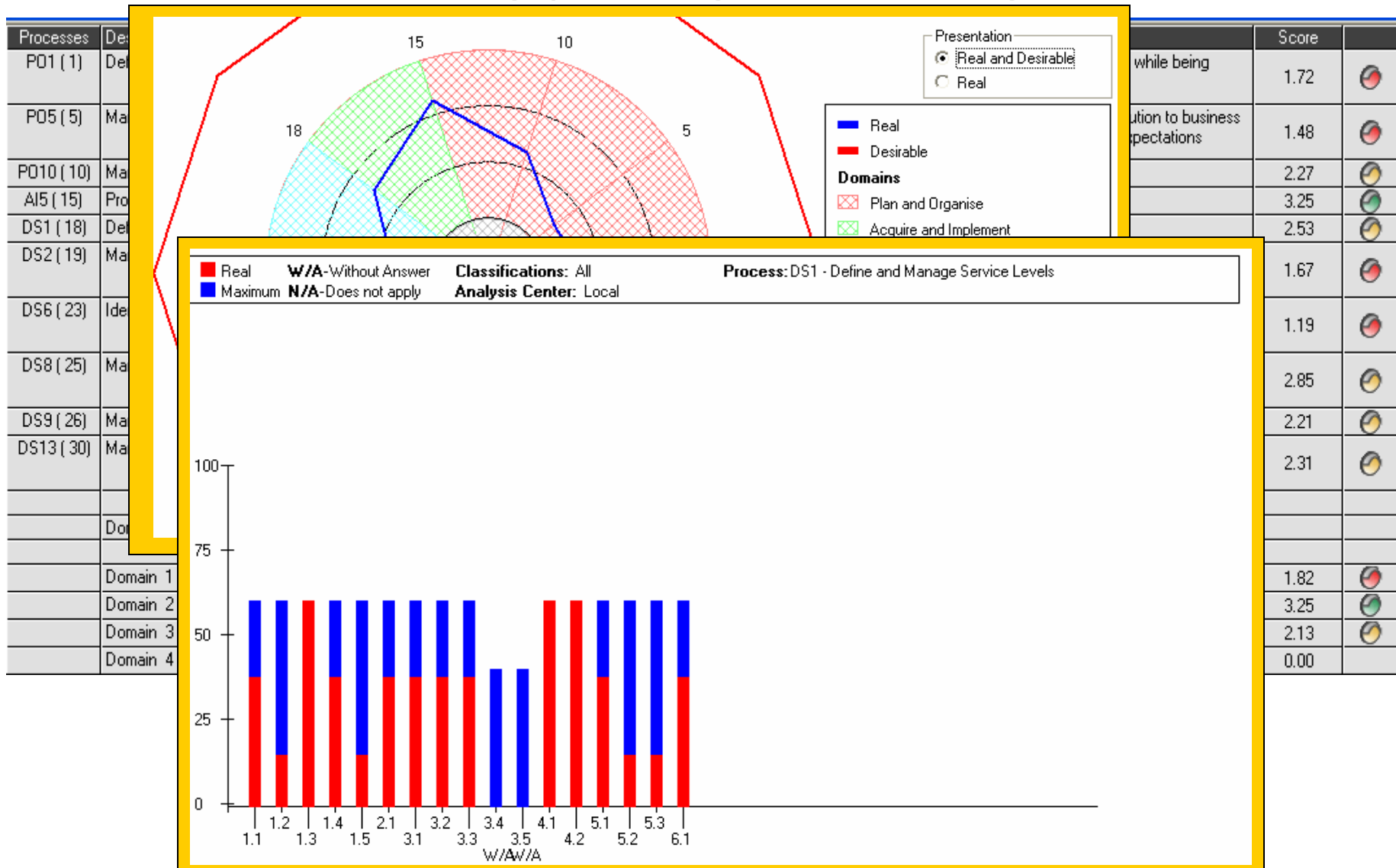
COBIT – Processes and Controls – Excess Labour Management



Process	Cost Area	Immature people related process and excessive labour cost
PO4	IT management and organisation	Ineffective outsourcing arrangements; IT organisation not optimal for business needs
PO7	<ul style="list-style-type: none"> o Deployment of human capital o High recruitment costs o Staff retention o Use of contractors 	<ul style="list-style-type: none"> o Skills not aligned to competencies; highly qualified handling staff firefighting issues o Inability to hire staff required o High staff turnover; low staff morale o High contractor costs as percentage of overall staff costs
AI4	Training and staff development	High degree of errors and rework; poor feedback regarding staff learning and development

Too many cooks.....!

COBIT – Assessment and gaps – Tangible Cost Management



COBIT – Tangible Cost Management – Concerns / Saving

Process	Cost Area	Immature Processes	Possible un-attended concerns in IT Operations	Tangible Saving options
PO1 and PO10	Programme management	Inability to prioritise and cancel IT initiatives	<ul style="list-style-type: none"> o Projects are never ending – Custom software o Underutilization of tools, SW 	<ul style="list-style-type: none"> o Stop recurring expense o Do not renew AMC, licenses
PO5	Investment management	Poor business cases and returns on IT-related Investments	<ul style="list-style-type: none"> o HW Investments based on current poor performance of Servers – lack of CBA o Applications developed or modified regularly 	<ul style="list-style-type: none"> o Avoid / defer purchase o Workaround / deploy alternate cheaper solution
PO5 and DS6	Budgeting and cost management	Poor understanding of current costs; inability to optimise the budget and identify how to spend less but obtain more value	<ul style="list-style-type: none"> o Expense and costs booked under one common accounting – IT Expenditure o Consumable consumption, ISD/STD expenses, o AC and lighting expense o Manual Server management 	<ul style="list-style-type: none"> o Measure and control exp under Servers, VPN, Internet, AMC SW, Licenses o Reduce number of printers o Use Skype, gotomeeting, mikogo, yuuguu o Automate operations, warnings
PO10	Project management	Projects running late and over budget	<ul style="list-style-type: none"> o Project scoping, resource management o Vendor re-selection / re-negotiation o Unclear quality objective 	<ul style="list-style-type: none"> o Use timebox / fixed cost delivery o Replace vendor / reduce scope and cost o Link final payments to delivery of objectives

Cont'd

COBIT – Tangible Cost Management – Concerns / Saving

Process	Cost Area	Immature Processes	Possible un-attended concerns in IT Operations	Tangible Saving options
AI5	Procurement	Inability to negotiate good deals and obtain value for Money	<ul style="list-style-type: none"> o IT market and changing vendor service portfolios not understood o Deals are not negotiated on renewal o SLA concept followed 	<ul style="list-style-type: none"> o Identify innovative solutions- reduce vendor dependency o Negotiate each renewal after fresh research o SLA – measurement on reducing exceptions instead of on-time
DS9	Asset management	Cost of assets not understood; bad asset replacement strategy; software licenses not being used, hardware maintenance too high	<ul style="list-style-type: none"> o Successful application replaced due to obsolete technology o TCO is not measured for implemented infrastructure, service and solutions 	<ul style="list-style-type: none"> o Replace / amend only where business objectives are failing o Install SOA, Dashboards on legacy systems o Install thin client with minimal TCO
DS2	Contract and supplier management	Bad supplier relationships and poor service/product delivery	<ul style="list-style-type: none"> o Accepting low value delivery by known vendors / branded products o Non existence or lack of implementation of penalty clauses o 'Chalta hai attitude' 	<ul style="list-style-type: none"> o Ensure vendor is pushed, pulled and active at all times o Measure service failures / setup high penalty rates o Only few % of customer make noise – Change to Most % customers
DS1 and DS8	Service levels and service desk	Poor service delivery; service calls and incidents too High	<ul style="list-style-type: none"> o Repeat calls are not analyzed o Root cause not established 	<ul style="list-style-type: none"> o Reduce disruption of user services – 'Because of Computer...' o Implementation of RCA and solutions so that only unique / non-time consuming problems remain
DS13	Operations and systems management	Too many tools and not enough efficiency; no standardization procedures	<ul style="list-style-type: none"> o Unused automated tools o Lack of time / initiative with IT to improve controls o Procedures, 	<ul style="list-style-type: none"> o Deploy tools, if monitoring resources feasible o Ensure regular compliance after implementation o Manage documentation within practical limits

COBIT – Tangible Cost Management – Recommendation – DS2

Recommendations					
Sel.	Process	Proc.	Assigned tasks	Progress	Description
	19 (DS2)	0			Define and regularly review criteria to identify and categorise all supplier relationships according to the supplier type, significance and criticality of service. The list should include a category describing vendors as preferred, non-preferred or not re
	19 (DS2)	0			Establish and maintain a detailed register of suppliers, including name, scope, purpose of the service, expected deliverables, service objectives and key contact details.
	19 (DS2)	0			Define and formalise roles and responsibilities for each service supplier.
	19 (DS2)	0			Assign relationship owners for all suppliers and make them accountable for the quality of service(s) provided.
	19 (DS2)	0			Document the supplier relationship managers and communicate the information within the organisation.
	19 (DS2)	0			Establish and document a formal communication process between the organisation and the service provider.
	19 (DS2)	0			Ensure that contracts with key service suppliers provide for a review of supplier internal controls by management or independent third parties.
	19 (DS2)	0			Regularly review the reports between the organisation and the service supplier.
	19 (DS2)	0			Register incidents caused by suppliers and report them using the company's incident management process.

Customize recommendations according to business objectives.



COBIT – Tangible Cost Management–Tasks/linked Recommendation

Identifier: Name:

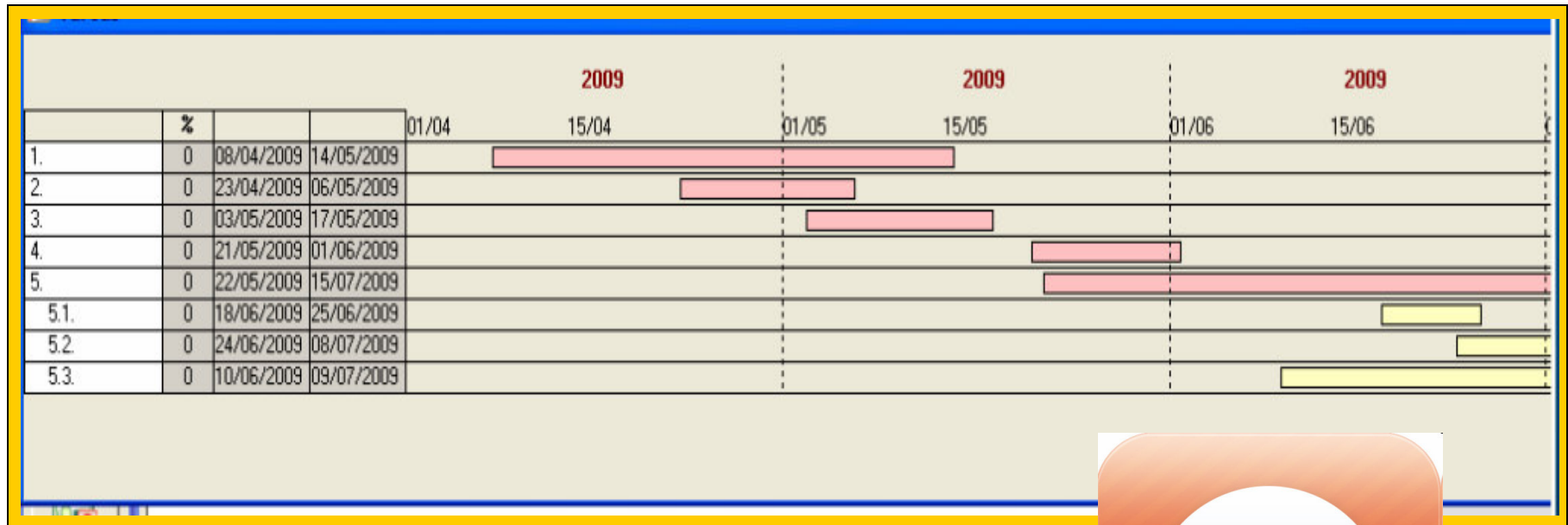
1. Review vendor performance
2. Meet with vendors
3. Quarterly review

Task

Task

Tasks				Recommendations	Responsible Party
Sel.	Process	Proc.	Description	Name	
	19 (DS2)	0	Ensure that contracts with key service suppliers provide for a review of supplier internal controls by management or independent third parties.		
✓	19 (DS2)	0	Regularly review the reports between the organisation and the service supplier.		
✓	19 (DS2)	0	Register incidents caused by suppliers and report them using the company's internal incident management process.		
	19 (DS2)	0	Periodically review and assess supplier performance against established and agreed-upon service levels. Clearly communicate suggested changes to the service supplier.		
	19 (DS2)	0	Identify and monitor supplier risks in accordance with the organisation's established risk management		
	19 (DS2)	0	Identify and document in the contract supplier risks (and remedies) associated with the supplier's inability to fulfil the contractual agreement(s).		
✓	19 (DS2)	0	When defining the contract, consider remedies including software escrow agreements, alternative suppliers or standby agreements in the event of supplier		
	19 (DS2)	0	Review all contracts for legal and regulatory requirements.		

COBIT – Tangible Cost Management–Tasks Manage / Comply



Verify and validate to ensure compliance and success.



COBIT – Tangible Cost Management– Communicate Results

- Proactive IT initiatives and operational improvements
- Enhance credibility of the IT organization
- Benefits
 - Tangibles
 - Current period vs previous period
 - % saving from alternate options
 - Forecast reduction in expense / ROI
 - Intangibles
 - Efficiency of operations
 - Reduced incidents
 - High uptime
 - Link to business objectives
 - Faster product launch
 - Timely service delivery
 - Increase in customers / revenue



COBIT – Comprehensiveness and other standards

■ Comprehensiveness

- Business operations completely dependent on IT
- Business applications (ERP), workflows, resource sharing, communication (chat, email, video conferencing) controls are all logical controls
- Approval and authorization – financial or non-financial is mostly handled by logical controls
- Confidentiality is primarily managed within technology
- COBIT encompasses all aspects of IT Governance

■ Other standards where COBIT is useful

- ITIL
- SOX compliance
- PCI-DSS
- NIST
- HIPAA
- ISO27001
- Others

COBIT – Other Standards

Common misunderstanding: We already have xyz standard, so we do not need COBIT.

What?	COSO, ISO 9001, King II, Sarbanes-Oxley, Industry BEE Charter												
What?	COBIT Domains												
	Plan and Organize			Acquire and Implement			Deliver and Support			Monitor and Evaluate			
How?	Business and IT Alignment	Well and Ross	TOGAF	PMBOK	CMMI	Various SDLC Methods	ITIL	ISO 17799	TICKIT	NIST 800	Balanced Scorecard	Board Briefing on IT Governance, 2 nd Edition	ISACA IS Auditing Standards

- Corporate Governance
- IT Governance

This figure is illustrative only.

Always draw your curves, then plot your reading. – Murphy's law

COBIT – Cost Management Controls in the IT operations

We thank you and appreciate your valuable time
for today's session.

Good Night.
Have a great weekend.

Sanjiv Arora,
Technologies and Controls
www.tech-controls.com