Bilgi Teknolojileri Yönetişim ve Denetim Konferansı

BTYD 2010

ISACA Serving IT Governance Professionals

Türkiye Bilişim Derneği 1971

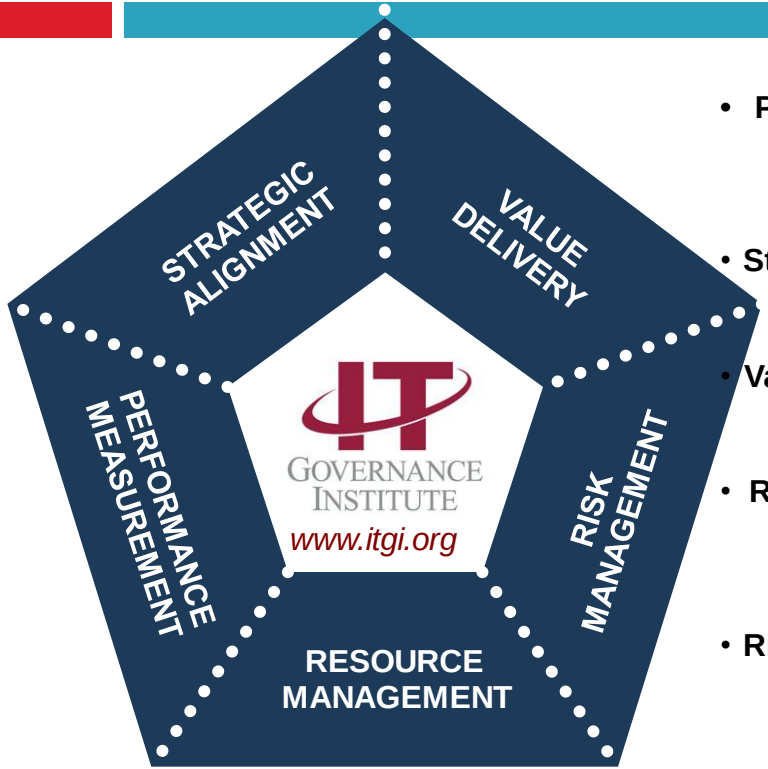
Türkiye İç Denetim Enstitüsü 1995

eDem TODAİE eDevlet Merkezi

COBIT

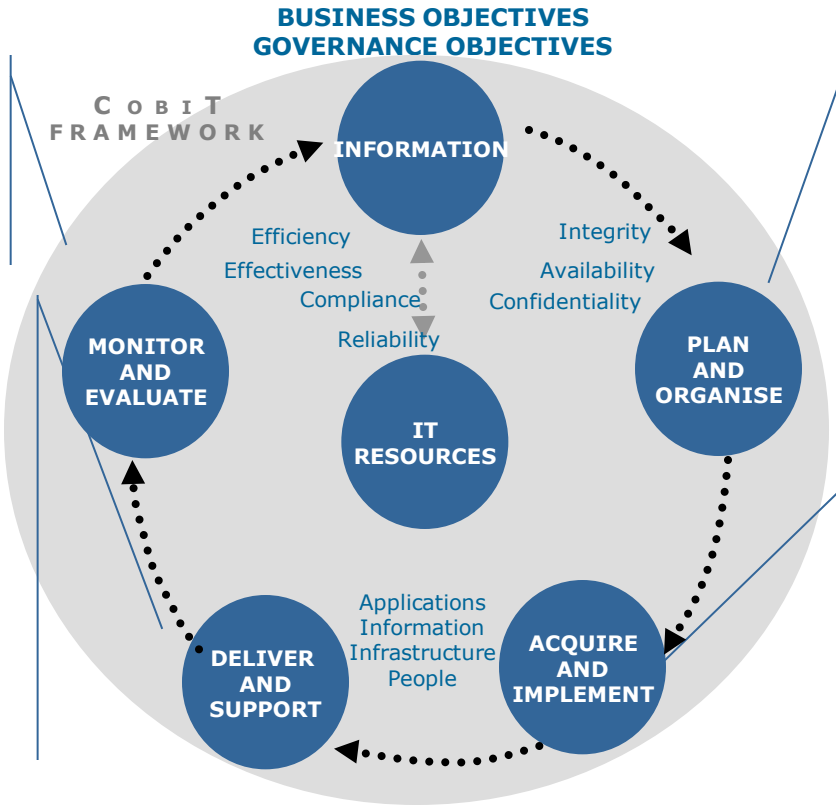
Kaya Kazmirci
Avea Internal Audit Director,
President ISACA Istanbul Chapter
kaya.kazmirci@isaca-istanbul.org
kaya.kazmirci@avea.com.tr
+90-555-255-8090
+90-532-487-7756

IT Governance Focus Areas



- **Performance measurement** tracks and monitors strategy implementation, project completion, resource usage, process performance and service delivery, using, for example, balanced scorecards that translate strategy into action to achieve goals measurable beyond conventional accounting
- **Strategic alignment** focuses on ensuring the linkage of business and IT plans; defining, maintaining and validating the IT value proposition; and aligning IT operations with enterprise operations.
- **Value delivery** is about executing the value proposition throughout the delivery cycle, ensuring that IT delivers the promised benefits against the strategy, concentrating on optimising costs and proving the intrinsic value of IT.
- **Resource management** is about the optimal investment in, and the proper management of, critical IT resources: applications, information, infrastructure and people. Key issues relate to the optimisation of knowledge and infrastructure.
- **Risk management** requires risk awareness by senior corporate officers, a clear understanding of the enterprise's appetite for risk, understanding of compliance requirements, transparency about the significant risks to the enterprise and embedding of risk management responsibilities into the organisation.

CobiT Process Structure



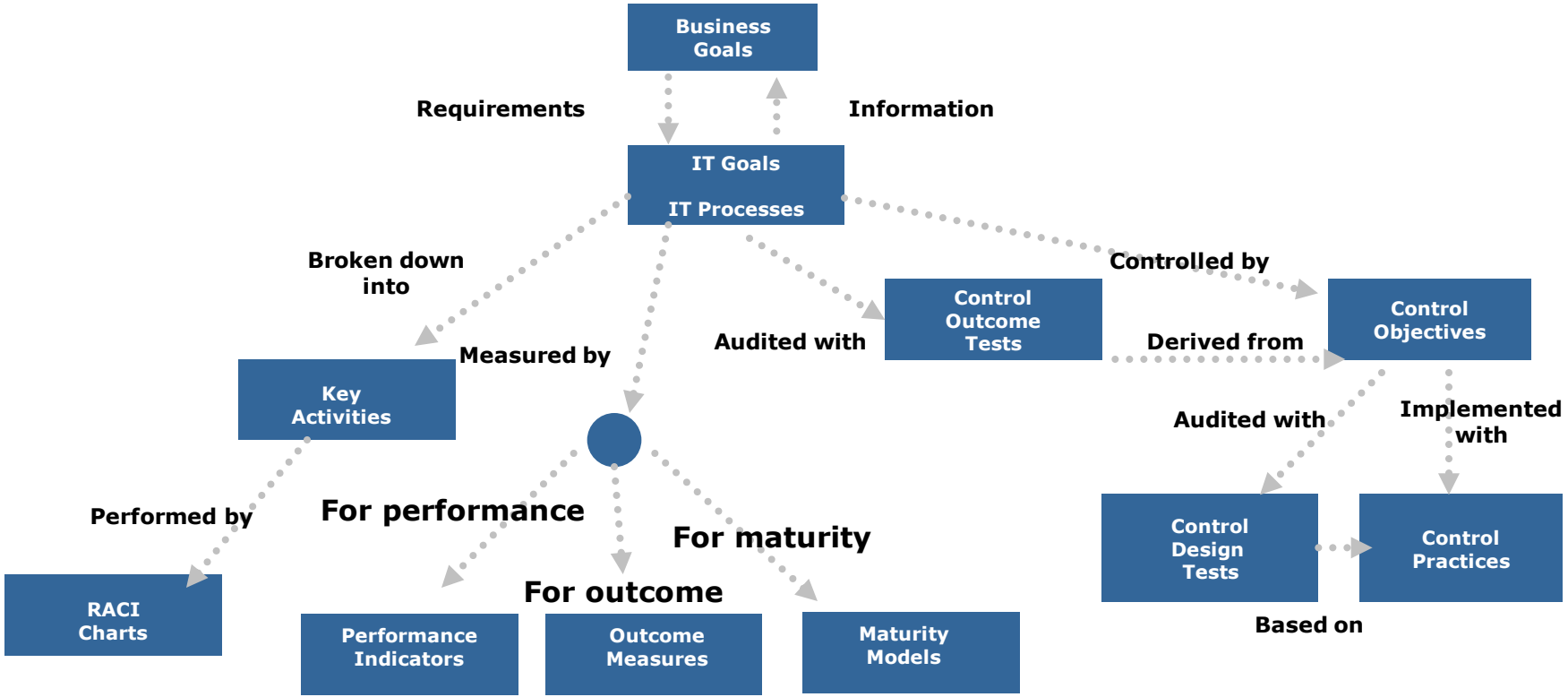
ME1	Monitor and evaluate IT performance.
ME2	Monitor and evaluate internal control.
ME3	Ensure regulatory compliance.
ME4	Provide IT governance.

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.

PO1	Define a strategic IT plan.
PO2	Define the information architecture.
PO3	Determine technological direction.
PO4	Define the IT processes, organisation and relationships.
PO5	Manage the IT investment.
PO6	Communicate management aims and direction.
PO7	Manage IT human resources.
PO8	Manage quality.
PO9	Assess and manage IT risks.
PO10	Manage projects.

AI1	Identify automated solutions.
AI2	Acquire and maintain application software.
AI3	Acquire and maintain technology infrastructure.
AI4	Enable operation and use.
AI5	Procure IT resources.
AI6	Manage changes.
AI7	Install and accredit solutions and change.

CobiT Components



COBIT Metrics Enable Performance Measurement

Performance measurement includes:

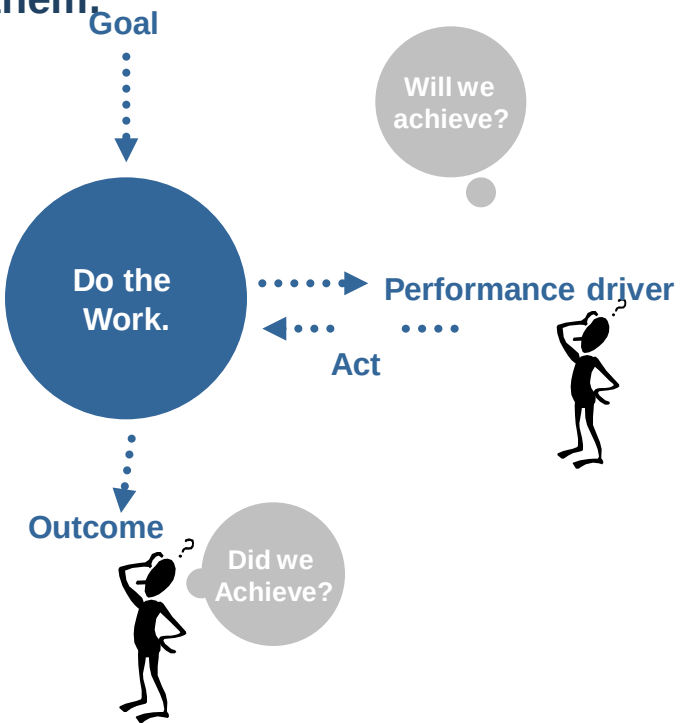
- **Goals and metrics:**
  - Demonstrate the value added by the IT organisation.
  - Determine the effectiveness of the IT organisation.
  - Set guidelines for the IT strategic plan.
  - Communicate and motivate about IT performance.
  - Establish IT management reporting.

Key stakeholders approval of an IT scorecard including specific metrics is an IT governance best practice.

Outcome Measures and Performance Drivers

COBIT provides two different types of metrics to measure against goals, and there is a cause-and-effect relationship between them.

- Outcome measures tell—after the fact—whether a goal has been achieved. They:
  - Focus on the customer and financial results
- Performance drivers:
  - Are a measure of how well the process is performing
  - Predict the probability of success or failure in the future, i.e., are 'lead' indicators
  - Focus on the process and learning dimensions of the balanced scorecard
  - Will help in improving the IT process when measured and acted upon

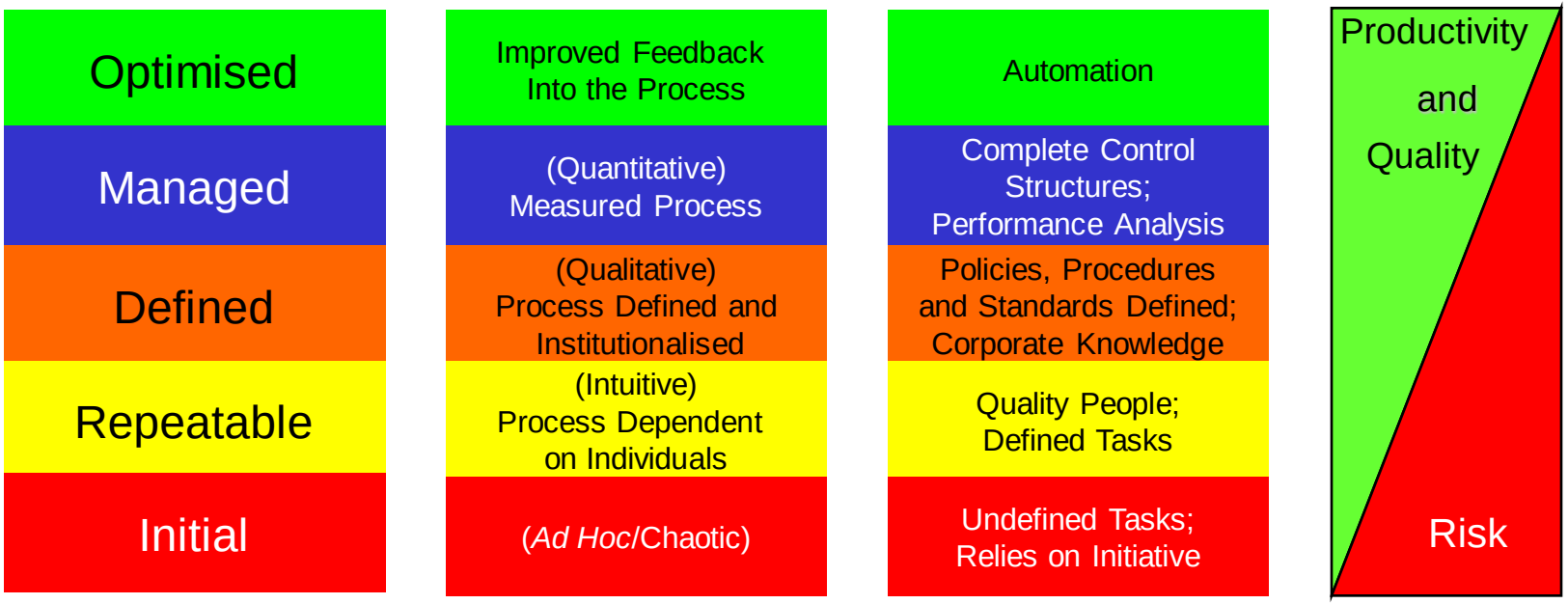


Performance Drivers From Improvement Actions Measure Success

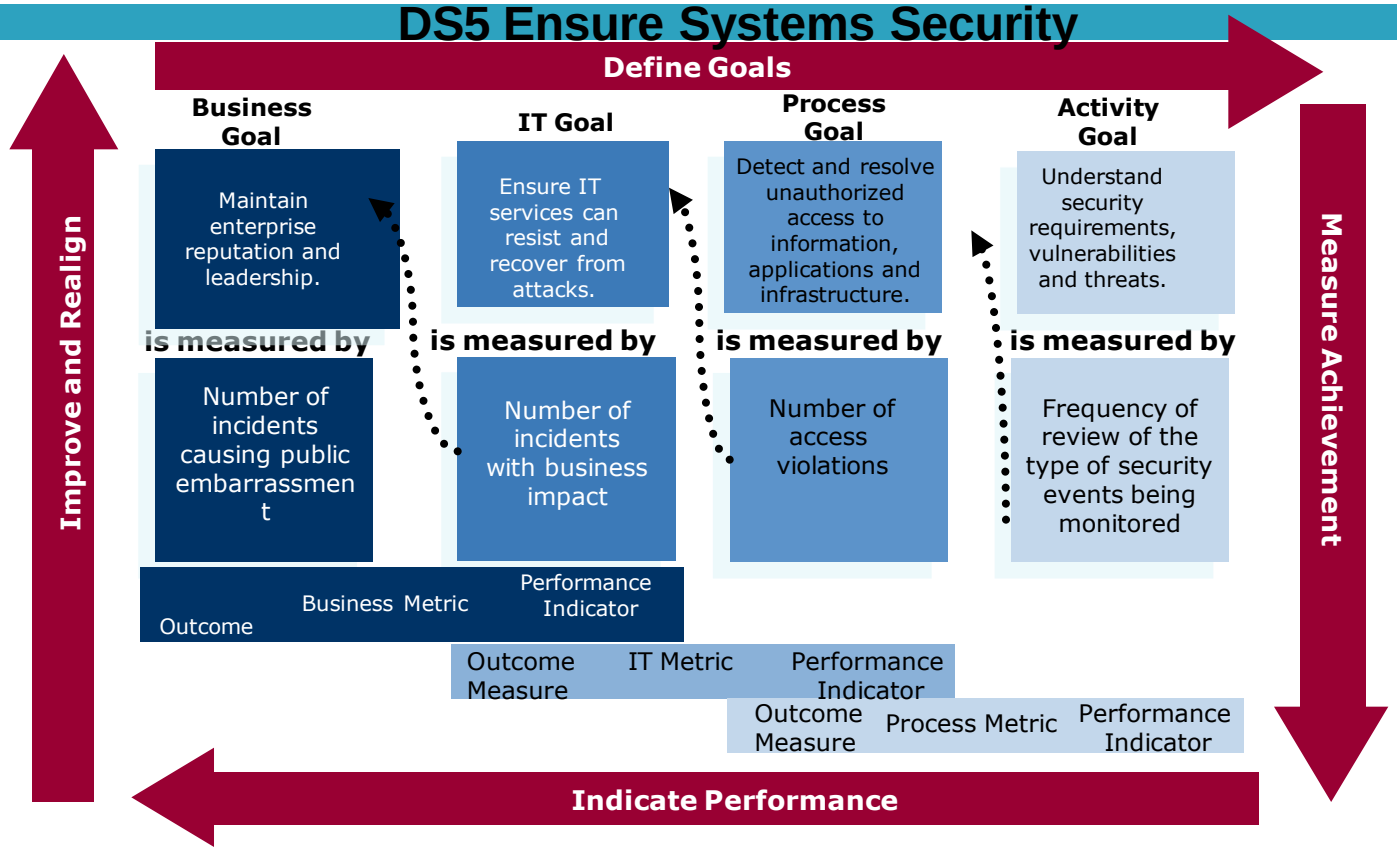
Use performance drivers to measure success:

- The performance drivers derived from improvement initiatives are the measures designed to ensure success of the improvement project and that the goals (outcome measures) are met over time.
- The actual metrics and targets will be set based on an assessment of current practices and performance and a decision about what level of improvement is desired in a specified time frame.
- Over time, these metrics and targets may be modified in the light of experience (practicality to gather the statistics, and the reasonableness of the targets).

CobiT Maturity: A Benchmarkable Metric



COBIT and Performance Measurement

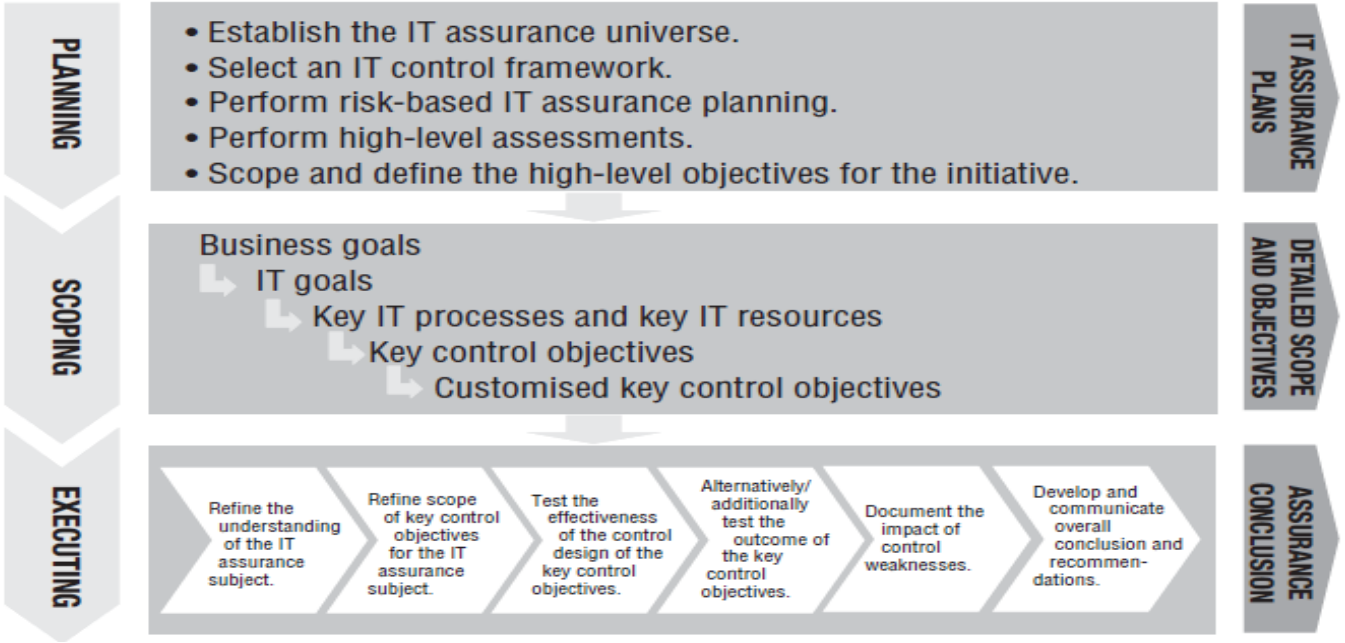


DS3 Manage Performance & Capacity

Business	IT	Process	Activity
Optimising the performance of IT infrastructure, resources and capabilities in response to business needs	• Respond to business requirements in alignment with the business strategy. • Make sure that IT services are available as required. • Optimise the IT infrastructure, resources and capabilities.	• Monitor and measure peak load & transaction response times. • Meet response-time SLAs. • Minimise transaction failures. • Minimise downtime • Optimise utilisation of IT resources.	• Planning & providing system capacity & availability • Monitoring & reporting system performance • Modelling & forecasting system performance
is measured by	**is measured by**	**is measured by**	**is measured by**
• # of hours lost per user per month due to insufficient capcty planning • % of peaks where target utilisation is exceeded • % of response-time SLAs not met	• # of hours lost per user per month due to insufficient capacity planning • # of critical business processes not covered by a defined service availability plan	• Peak load and overall utilisation rates • % of peaks where target utilisation is exceeded • % of response-time SLAs not met • Transaction failure rate	• Freq of perf & cap forecasting • % of assets included in capacity reviews • % of assets monitred through centralised tool(s)

Avea Maturity Assessment

- DS3 Manage Performance and Capacity
- PO3 Determine Technological Direction



Audit Project : DS3 Manage Performance and Capacity

Control Objectives

DS3.1 Performance and Capacity Planning

Establish a planning process for the review of performance and capacity of IT resources to ensure that cost-justifiable capacity and performance are available to process the agreed-upon workloads as determined by the SLAs. Capacity and performance plans should leverage appropriate modelling techniques to produce a model of the current and forecasted performance, capacity and throughput of the IT resources.

DS3.2 Current Performance and Capacity

Assess current performance and capacity of IT resources to determine if sufficient capacity and performance exist to deliver against agreed-upon service levels.

DS3.3 Future Performance and Capacity

Conduct performance and capacity forecasting of IT resources at regular intervals to minimise the risk of service disruptions due to insufficient capacity or performance degradation, and identify excess capacity for possible redeployment. Identify workload trends and determine forecasts to be input to performance and capacity plans.

DS3.4 IT Resources Availability

Provide the required capacity and performance, taking into account aspects such as normal workloads, contingencies, storage requirements and IT resource life cycles. Provisions such as prioritising tasks, fault-tolerance mechanisms and resource allocation practices should be made. Management should ensure that contingency plans properly address availability, capacity and performance of individual IT resources.

DS3.5 Monitoring and Reporting

Continuously monitor the performance and capacity of IT resources. Data gathered should serve two purposes:

• To maintain and tune current performance within IT and address such issues as resilience, contingency, current and projected workloads, storage plans, and resource acquisition

• To report delivered service availability to the business, as required by the SLAs

Audit Project : PO3 Determine Technological Direction

Control Objectives

PO3.1 Technological Direction Planning

Analyze existing and emerging technologies, and plan which technological direction is appropriate to realize the IT strategy and the business systems architecture. Also identify in the plan which technologies have the potential to create business opportunities. The plan should address systems architecture, technological direction, migration strategies and contingency aspects of infrastructure components.

PO3.2 Technology Infrastructure Plan

Create and maintain a technology infrastructure plan that is in accordance with the IT strategic and tactical plans. The plan should be based on the technological direction and include contingency arrangements and direction for acquisition of technology resources. It should consider changes in the competitive environment, economies of scale for information systems staffing and investments and improved interoperability of platforms and applications.

PO3.3 Monitor Future Trends and Regulations

Establish a process to monitor the business sector, industry, technology, infrastructure, legal and regulatory environment trends. Incorporate the consequences of these trends into the development of the IT technology infrastructure plan.

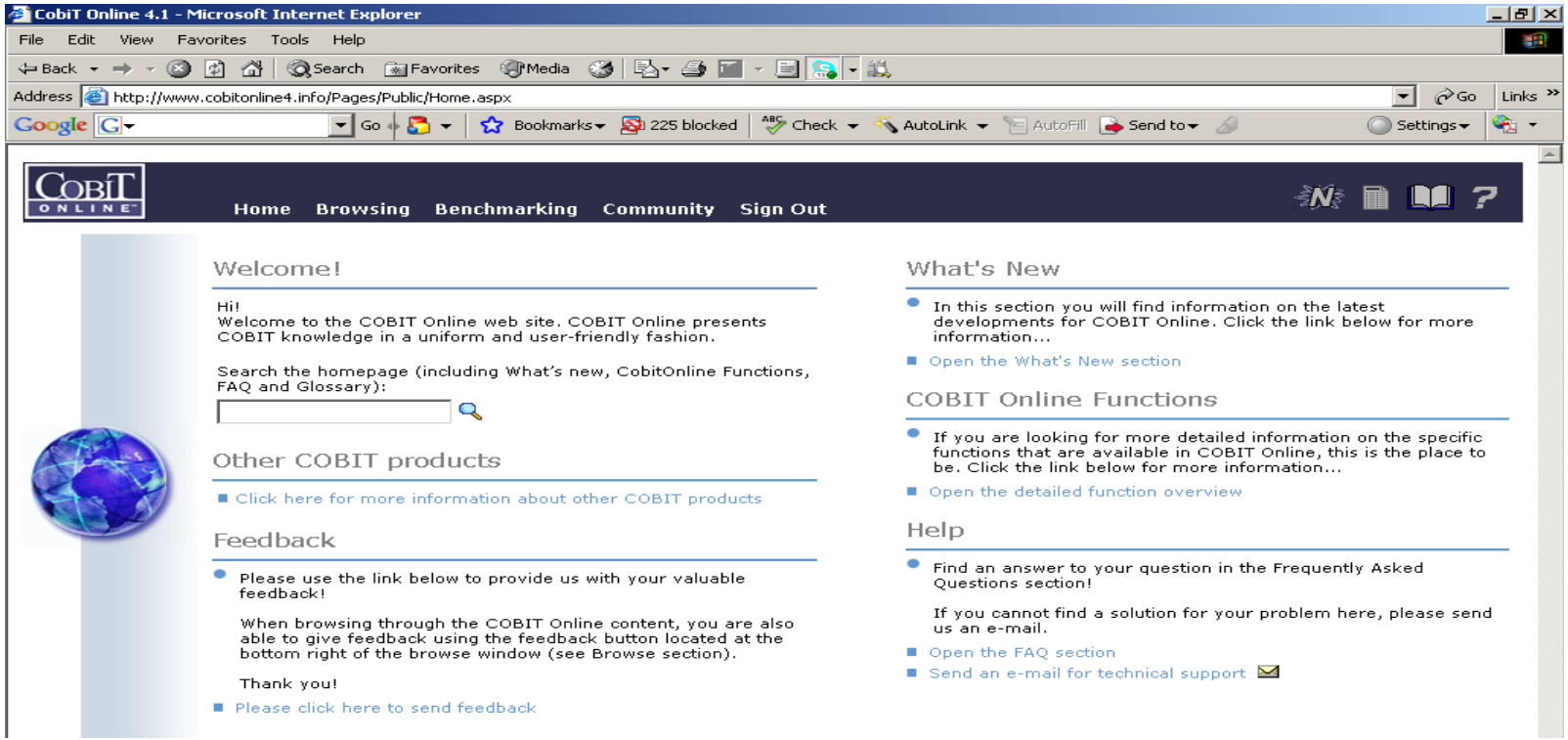
PO3.4 Technology Standards

To provide consistent, effective and secure technological solutions enterprise wide, establish a technology forum to provide technology guidelines, advice on infrastructure products and guidance on the selection of technology, and measure compliance with these standards and guidelines. This forum should direct technology standards and practices based on their business relevance, risks and compliance with external requirements.

PO3.5 IT Architecture Board

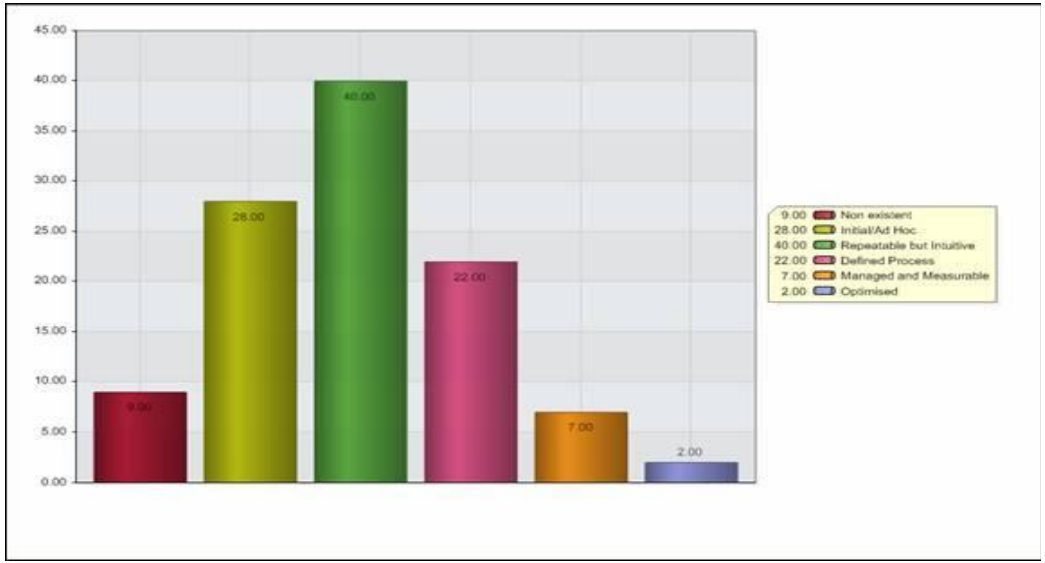
Establish an IT architecture board to provide architecture guidelines and advice on their application, and to verify compliance. This entity should direct IT architecture design, ensuring that it enables the business strategy and considers regulatory compliance and continuity requirements. This is related/linked to PO2 Define the information architecture

Benchmarking w/CobiT Online



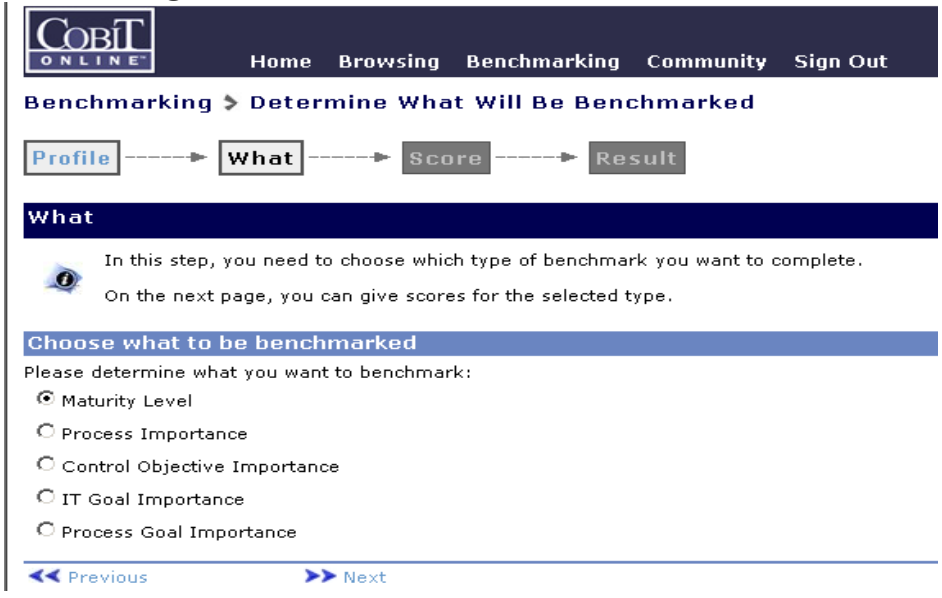
CobiT Benchmarking

The Benchmarking facility enables users to input scores (such as process maturity levels, process importance, control objective importance, IT goal importance, IT process goal importance) and then extract anonymous comparisons with data input other users.



What to Benchmark?

- Maturity Level, Process Importance, IT Goal Importance
- Process Goal Importance, Control Objection Importance
- Control Practice Usage



Score (Based on min 8 entries)

- Maturity level: On a scale of 0-5
- Process importance: On a scale of low/medium/high
- IT goal importance: On a scale of Low/Medium/High
- Process goal importance: On a scale of Low/Medium/High
- Control objective importance: On a scale of low/medium/high
- Control practice usage: Scored as used/not used/NA

COBIT 5 Initiative

- The initiative charge from the Board of Directors is to “tie together and reinforce all ISACA knowledge assets with COBIT 5“
- The COBIT 5 Task Force:
  - Includes experts from across the ISACA constituency groups
  - Is co-chaired by John Lainhart (Past International President) and Derek Oliver (Past Chair of the BMIS Development Committee)
  - Reports to the Framework Committee and then the Knowledge Board.\

COBIT 5 Objectives

COBIT 5 will:

- Provide a renewed and authoritative governance and management framework for enterprise information and related technology, building on the current widely recognized and accepted COBIT framework, linking together and reinforcing all other major ISACA frameworks such as:

Val IT	**Risk IT**
BMIS	**ITAF**
Board Briefing	**Taking Governance Forward**

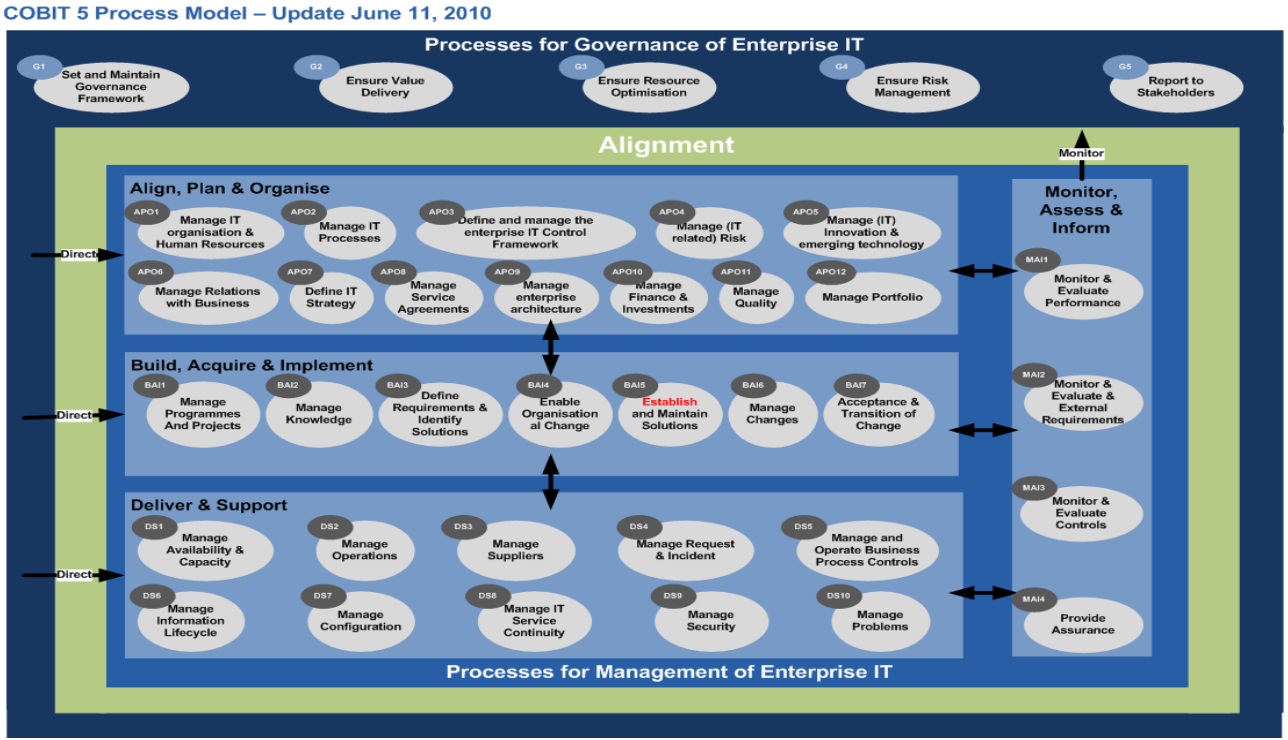
- Connect to other major frameworks and standards in the marketplace (ITIL, ISO standards, etc.)

What Will Be Delivered?

- An enterprisewide, business and IT "end-to-end' framework addressing governance and management of information and related technology
- The framework structure will include familiar components such as a domain/process model and other components such as governance/management practices, RACI charts, and inputs/ outputs.
- An initial COBIT 5 product architecture, specifying which types of "products" and other "guidance" that could developed for specific IT professional audiences (e.g. assurance, security, risk) in support of enterprise business needs

Draft Framework

- A work in progress today



Potential Products

The proposed COBIT 5 product architecture will over time deliver products based on the overarching COBIT framework. Examples include:

- COBIT [for] Security *(in planning now!)*
- COBIT for Governance
- COBIT for Management
- COBIT for Assurance
- COBIT for Control
- COBIT for Risk
- COBIT for Compliance
- COBIT for Value
- COBIT for Applications

Key Messages

- Major evolution of the COBIT framework—incorporating the latest governance and management thinking; actively be a part of the development of this global initiative and drive its direction. COBIT 5 pulls ISACA frameworks together into one cohesive, comprehensive (‘end to end’) picture—and fill in gaps
- Simplify navigation and use—easier to navigate ISACA framework material and more practical to use
- Provide a common language to cross professional disciplines
- COBIT 5 builds on existing market capital of the brand (reputation, credibility, investment, experience)

Key Messages

- Significance of information and related technology is growing—IT is a business issue; get involved, get engaged; see ‘value’ from IT by implementing good governance
- You can’t meet your organizational goals without effective governance of enterprise IT
- Enterprise leadership need to champion effective governance and management of enterprise IT—COBIT can help
- COBIT provides a basis for evaluating, directing and monitoring enterprise use of IT

BTYD 2010

www.btyd.org