“Understanding COBIT 5”

based on ISACA© Materials
www.isaca.org/cobit
Session Objectives

- Why COBIT is important
- What COBIT 5 is
  - Framework
  - Implementation Life Cycle
  - Process Reference Model
  - Process Assessment Method
- How to use COBIT
- What is different about COBIT 5 vs. COBIT 4.1
Why is COBIT important to Your Enterprise?

- IT audit and assurance de-facto standard
- Governance, Risk and Compliance
- Information Security
- Business value focused IT Process Framework
- ITIL, CMMI and PMBOK synergies
- Governance and Management processes
- “How to” monitor, evaluate, assess and improve business process performance
COBIT Framework to Achieve Business Goals

- Achieve Operational Excellence
- Generate Business Value
- Optimize Costs
- Maintain acceptable level of IT-related risk

Make Quality Business Decisions

Information Technology

Date: Thursday, March 7, 2013
ISACA Silicon Valley Chapter Spring 2013 Conference
A Business Framework for the Governance and Management of Enterprise IT

• Five Principles
• Seven Enablers
• Governance and Management
• Implementation Lifecycle
• Assessment Approach
Now a Complete Framework!

Governance of Enterprise IT

IT Governance
Management
Control
Audit

COBIT 1
COBIT 2
COBIT 3
COBIT 4.0/4.1
COBIT 5

Val IT 2.0 (2008)
Risk IT (2009)


www.isaca.org/cobit
COBIT 5 – Five Principles

1. Meeting Stakeholder Needs
2. Covering the Enterprise End-to-End
3. Applying a Single Integrated Framework
4. Enabling a Holistic Approach
5. Separating Governance From Management
Principle 1. Meeting Stakeholder Needs

Governance Objective: Create Value

Stakeholder Needs

Drive

Benefits Realization
Risk Optimization
Resource Optimization

Date: Thursday, March 7, 2013
ISACA Silicon Valley Chapter Spring 2013 Conference
Stakeholder Needs

Drive

Governance Objective: Create Value

Benefits Realization
Risk Optimization
Resource Optimization

Enterprise Goals
IT Related Goals
Enabler Goals

Influences

Cascades to

Cascades to

Date: Thursday, March 7, 2013
Principle 2. Covering the Enterprise End-to-End

Governance Objective: Create Value

Benefits Realization
Risk Optimization
Resource Optimization
Governance Enablers
Governance Scope
Roles, Activities and Relationships
Principle 2: Roles, Activities and Relationships

Owners and Stakeholders

Delegate

Governing Body

Set Direction

Accountable

Management

Instruct and Align

Monitor

Operations and Execution

Report

Date: Thursday, March 7, 2013

ISACA Silicon Valley Chapter Spring 2013 Conference
Diagram excerpt from COBIT 5 Essential Facts - Fact 4: “COBIT 5 brings order to complex standards, regulations and frameworks”
Principle 4. Enabling a Holistic Approach

- Processes
- Organizational Structures
- Culture, Ethics and Behavior

Principles, Policies and Frameworks

- Information
- Services Infrastructure Applications
- People, Skills and Competencies

RESOURCES

Date: Thursday, March 7, 2013
Enablers and Performance

Stakeholders
• Internal
• External

Goals
• Intrinsic
• Context
• Accessibility and Security

Life Cycle
• Plan
• Design
• Build
• Use
• Evaluate
• Dispose

Good Practices
• Practices
• Work Products

Goal Indicator Metrics
• Addressed?
• Achieved?

Practice Indicator Metrics
• Managed?
• Applied?

Date: Thursday, March 7, 2013
ISACA Silicon Valley Chapter Spring 2013 Conference
Principle 5: Governance

**Business Needs**

**Governance**

- Evaluate
- Direct
- Monitor

**Management**

- Plan (Align, Plan, Organize)
- Build (Build, Acquire, Implement)
- Run (Deliver, Service, Support)
- Monitor (Monitor, Evaluate, Assess)

--

Date: Thursday, March 7, 2013

ISACA Silicon Valley Chapter Spring 2013 Conference
The Seven Phases of the Implementation Life Cycle

1. What are the drivers?
   - Identify role players
   - Form implementation team
   - Establish desire to change
   - Recognise need to act
   - Monitor and evaluate

2. Where are we now?
   - Form implementation team
   - Define road map
   - Operate and use
   - Implement improvements
   - Build improvements

3. Where do we want to be?
   - Communicate outcome
   - Define target state
   - Assess current state
   - Operate new approaches
   - Embed new approaches

4. What needs to be done?
   - Plan programme
   - Execute plan
   - Did we get there?
   - Review effectiveness

5. How do we get there?
   - Define problems and opportunities
   - Programme management (outer ring)
   - Change enablement (middle ring)
   - Continual improvement life cycle (inner ring)

6. Is the momentum still there?
   - Monitor and evaluate
   - Sustain

7. How do we keep the momentum going?
   - Review effectiveness

8. Did we get there?
   - Identify role players
   - Form implementation team
   - Establish desire to change
   - Recognise need to act
   - Monitor and evaluate
Process Capability Assessment Approach

- Detailed guidance for COBIT 5
- ISO/IEC 15504 Compliant method
- COBIT 5 Enabling Processes are defined as ISO/IEC 15504 compliant process reference model
- Raises bar – incomplete process if there is not evidence (metrics and work products) that purpose/goals are largely achieved
- Aligns with ITIL TIPA Assessment method
COBIT 5 PAM

Capable Measurement System

Optimizing
Predictable
Established
Managed
Performed
Incomplete

Level 5
Level 4
Level 3
Level 2
Level 1
Level 0

PRM
- Purpose
- Outcomes
- Base Practices
- Work Products
COBIT 5 Enabling Processes

- Goals Cascade
- Process model explanation
- Diagram of Model
- Details for 37 Processes:
  - Purpose
  - Practices
  - Goals & Metrics
  - Activities & RACI
  - Work Products
COBIT 5 Process Reference Model

Processes for Governance of Enterprise IT

Evaluate, Direct and Monitor

- EDM01 Ensure Governance Framework Setting and Maintenance
- EDM02 Ensure Benefits Delivery
- EDM03 Ensure Risk Optimisation
- EDM04 Ensure Resource Optimisation
- EDM05 Ensure Stakeholder Transparency

Align, Plan and Organise

- APO01 Manage the IT Management Framework
- APO02 Manage Strategy
- APO03 Manage Enterprise Architecture
- APO04 Manage Innovation
- APO05 Manage Portfolio
- APO06 Manage Budget and Costs
- APO07 Manage Human Resources
- APO08 Manage Relationships
- APO09 Manage Service Agreements
- APO10 Manage Suppliers
- APO11 Manage Quality
- APO12 Manage Risk
- APO13 Manage Security

Build, Acquire and Implement

- BAI01 Manage Programmes and Projects
- BAI02 Manage Requirements Definition
- BAI03 Manage Solutions Identification and Build
- BAI04 Manage Availability and Capacity
- BAI05 Manage Organisational Change Enablement
- BAI06 Manage Changes
- BAI07 Manage Change Acceptance and Transitioning
- BAI08 Manage Knowledge
- BAI09 Manage Assets
- BAI10 Manage Configuration

Deliver, Service and Support

- DSS01 Manage Operations
- DSS02 Manage Service Requests and Incidents
- DSS03 Manage Problems
- DSS04 Manage Continuity
- DSS05 Manage Security Services
- DSS06 Manage Business Process Controls

Processes for Management of Enterprise IT

Monitor, Evaluate and Assess

- MEA01 Monitor, Evaluate and Assess Performance and Conformance
- MEA02 Monitor, Evaluate and Assess the System of Internal Control
- MEA03 Monitor, Evaluate and Assess Compliance With External Requirements
COBIT 4.1 Framework

**Business Objectives**

**Governance Objectives**

**Monitor and Evaluate**
- ME1 Monitor and evaluate IT performance.
- ME2 Monitor and evaluate internal controls.
- ME3 Ensure compliance with external requirements.
- ME4 Provide IT governance.

**Information Criteria**
- Effectiveness
- Efficiency
- Confidentiality
- Integrity
- Availability
- Compliance
- Reliability

**IT Resources**
- Applications
- Information
- Infrastructure
- People

**Plan and Organise**
- 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.

**Acquire and Implement**
- 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 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.
COBIT 4.1 v.s COBIT 5

**COBIT 4.1**
- Governance embedded
- No Val IT and Risk IT
- IT Management and Audit focus

**COBIT 5.0**
- 5 Principles
- “Principle-driven” approach
- Bridge from COBIT 4.1
- Enablers developed as “Pulled”
Thanks!

Great ideas need landing gear as well as wings.
~C.D. Jackson

Debra Mallette, CGEIT, CISA, CSSBB
Sr. Process Consultant/Specialist
Enterprise Process Delivery Management (EPDM)

Kaiser Permanente
IT IMG Business & Supplier Management Services, EPDM
(BSMS - Formerly IT IMG Supplier Services Management)
5810 Owens Drive, MS F-1039
Pleasanton, CA 94588

925 924 5123 (office)
8 504 5123 (tie line)
510 295 3217 (mobile phone)
debra.mallette (sametime)

----------

kp.org/thrive