COBIT® 5
A globally accepted business framework for the governance and management of enterprise IT

Denver ISACA AGM Chapter Meeting
April 25, 2013

Debbie Lew (debbie.lew@ey.com  805-778-7049)
Agenda

► What is COBIT and background?
► Why COBIT – drivers?
► Review of the framework: key features
  ► COBIT 5 Principles
  ► COBIT Enablers
► COBIT 4.1 and COBIT 5 Differences
► Process Capability Model and Assessment
► Implementing COBIT – the basics
► COBIT Benefits
COBIT 5: The Business Framework for the governance and management of enterprise IT

- Internationally accepted good practices
- Management-oriented
- Supported by tools and training
- Freely available
- Sharing knowledge and leveraging expert volunteers
- Continually evolving
- Maintained by reputable not-for-profit organization
- Maps strongly to all major related standards
- Is a reference, set of best practices, not an “off-the-shelf” cure

The only framework that covers the end-to-end IT life cycle
The Evolution of COBIT 5

An business framework from ISACA, at www.isaca.org/cobit

© 2012 ISACA. All Rights Reserved.
Why Develop COBIT 5?

• ISACA Board of Directors directive: “Tie together and reinforce all ISACA knowledge assets with COBIT.”
• Provide a renewed and authoritative governance and management framework for enterprise information and related technology.
• Integrate all other major ISACA frameworks and guidance
• Align with other major frameworks and standards.
Drivers for COBIT5

► Provide guidance in:
  ► Enterprise architecture
  ► Asset and service management
  ► Emerging sourcing and organization models

► Innovation and emerging technologies (including streamlining product development, manufacturing and supply chain processes to deliver products to market with increasing levels of efficiency, speed and quality).

► End to end business and IT responsibilities

► Controls for user-initiated and user-controlled IT solutions
Business Needs

Enterprise are under constant pressure to:

► Increase benefits realization through effective and innovative use of enterprise IT:
  ► Generate business value from new enterprise investments with supporting IT investment
  ► Achieve operational excellence through application of technology
► Maintain IT related risk at an acceptable level
► Contain cost of IT services and technology
► Ensure business and IT collaboration, leading to business user satisfaction with IT engagement and services
► Comply with ever increasing relevant laws, regulations and policies.
Not simply IT: not only for big business!

- COBIT5 is about *governing and managing* information
  - Whatever medium is used
  - End to end throughout the enterprise

Information is equally important to:
- Global, multinational business
- National and local government
- Charities and not for profit enterprise
- Small to medium enterprises and
- Clubs and associations
COBIT5 Scope

Not simply IT: not only for big business!

► COBIT5 is about *governing and managing* information
  ► Whatever medium is used
  ► End to end throughout the enterprise

► Information is equally important to:
  ► Global, multinational business
  ► National and local government
  ► Charities and not for profit enterprise
  ► Small to medium enterprises and
  ► Clubs and associations
COBIT5 Scope

Not simply IT: not only for big business!

► COBIT5 is about governing and managing information
  ► Whatever medium is used
  ► End to end throughout the enterprise

► Information is equally important to:
  ► Global, multinational business
  ► National and local government
  ► Charities and not for profit enterprise
  ► Small to medium enterprises and
  ► Clubs and associations

© 2012 ISACA. All Rights Reserved.
COBIT5 Format

► Simplified
  ► COBIT5 directly addresses the needs of the viewer from different perspectives
  ► Development continues with specific practitioner guides (COBIT5 for Security was issued June 2012)

► COBIT5 is initially in 3 volumes:
  ► The Framework – Free Download
  ► The Process Reference Guide – Free to Members
  ► Implementation Guide – Free to Members

► COBIT5 is based on:
  ► 5 principles and
  ► 7 enablers
COBIT 5 Product Family

COBIT® 5

COBIT 5 Enabler Guides
- COBIT® 5: Enabling Processes
- COBIT® 5: Enabling Information
- Other Enabler Guides

COBIT 5 Professional Guides
- COBIT® 5 Implementation
- COBIT® 5 for Information Security
- COBIT® 5 for Assurance
- COBIT® 5 for Risk
- Other Professional Guides

COBIT 5 Online Collaborative Environment
Review of COBIT 5 Framework
COBIT 5 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

Source: COBIT® 5, figure 2. © 2012 ISACA® All rights reserved.
Principle 1: Meeting Stakeholder Needs

- Enterprises exist to **create value** for their stakeholders

- **Value creation**: realizing benefits at an optimal resource cost while optimizing risk.
Principle 1: Meeting Stakeholder Needs

► Enterprises exist to create value for their stakeholders
► Stakeholder needs have to be transformed into an enterprise’s actionable strategy.
► The COBIT 5 goals cascade allows the definition of priorities for:
  ► Implementation
  ► Improvement
  ► Assurance of enterprise governance of IT

Source: COBIT® 5, figure 4. © 2012 ISACA® All rights reserved.
Principle 1: Meeting Stakeholder Needs

► Enterprises have many stakeholders

► Governance is about
  ► Negotiating
  ► Deciding amongst different stakeholders’ value interests
  ► Considering all stakeholders when making benefit, resource and risk assessment decisions

► For each decision, ask:
  ► For whom are the benefits?
  ► Who bears the risk?
  ► What resources are required?
## Principle 1: Meeting Stakeholder Needs

<table>
<thead>
<tr>
<th><strong>EXTERNAL STAKEHOLDERS</strong></th>
<th><strong>EXTERNAL STAKEHOLDER NEEDS</strong></th>
</tr>
</thead>
</table>
| Business partners, suppliers, shareholders, regulators/government, external users, customers, standardisation organisations, external auditors, consultants, etc. | • How do I know my business partner’s operations are secure and reliable?  
• How do I know the organisation is compliant with applicable rules and regulations?  
• How do I know the enterprise is maintaining an effective system of internal control? |

© 2012 ISACA. All Rights Reserved.
Principle 1: Meeting Stakeholder Needs

Internal stakeholder concerns include:

- How do I get value from the use of IT?
- How do I manage performance of IT?
- How can I best exploit new technology for new strategic opportunities?
- How do I know whether I’m compliant with all applicable laws and regulations?
- Am I running an efficient and resilient IT operation?
- How do I control cost of IT?
- Is the information I am processing adequately and appropriately secured?
- How critical is IT to sustaining the enterprise?
- What do I do if IT is not available?
## Enterprise Goals

### Figure 4—COBIT 5 Enterprise Goals

<table>
<thead>
<tr>
<th>BSC Dimension</th>
<th>Enterprise Goal</th>
<th>Relation to Governance Objectives</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Benefits Realisation</td>
</tr>
<tr>
<td>Financial</td>
<td>1. Stakeholder value of business investments</td>
<td>P</td>
</tr>
<tr>
<td></td>
<td>2. Portfolio of competitive products and services</td>
<td>P</td>
</tr>
<tr>
<td></td>
<td>3. Managed business risk (safeguarding of assets)</td>
<td>P</td>
</tr>
<tr>
<td></td>
<td>4. Compliance with external laws and regulations</td>
<td>P</td>
</tr>
<tr>
<td></td>
<td>5. Financial transparency</td>
<td>P</td>
</tr>
<tr>
<td>Customer</td>
<td>6. Customer-oriented service culture</td>
<td>P</td>
</tr>
<tr>
<td></td>
<td>7. Business service continuity and availability</td>
<td>P</td>
</tr>
<tr>
<td></td>
<td>8. Agile responses to a changing business environment</td>
<td>P</td>
</tr>
<tr>
<td></td>
<td>9. Information-based strategic decision making</td>
<td>P</td>
</tr>
<tr>
<td></td>
<td>10. Optimisation of service delivery costs</td>
<td>P</td>
</tr>
<tr>
<td>Internal</td>
<td>11. Optimisation of business process functionality</td>
<td>P</td>
</tr>
<tr>
<td></td>
<td>12. Optimisation of business process costs</td>
<td>P</td>
</tr>
<tr>
<td></td>
<td>13. Managed business change programmes</td>
<td>P</td>
</tr>
<tr>
<td></td>
<td>14. Operational and staff productivity</td>
<td>P</td>
</tr>
<tr>
<td></td>
<td>15. Compliance with internal policies</td>
<td>P</td>
</tr>
<tr>
<td>Learning and Growth</td>
<td>16. Skilled and motivated people</td>
<td>S</td>
</tr>
<tr>
<td></td>
<td>17. Product and business innovation culture</td>
<td>P</td>
</tr>
</tbody>
</table>

Source: COBIT® 5, © 2012 ISACA® All rights reserved.
## IT Related Goals

<table>
<thead>
<tr>
<th>IT BSC Dimension</th>
<th>Information and Related Technology Goal</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Financial</strong></td>
<td>01 Alignment of IT and business strategy</td>
</tr>
<tr>
<td></td>
<td>02 IT compliance and support for business compliance with external laws and regulations</td>
</tr>
<tr>
<td></td>
<td>03 Commitment of executive management for making IT-related decisions</td>
</tr>
<tr>
<td></td>
<td>04 Managed IT-related business risk</td>
</tr>
<tr>
<td></td>
<td>05 Realised benefits from IT-enabled investments and services portfolio</td>
</tr>
<tr>
<td></td>
<td>06 Transparency of IT costs, benefits and risk</td>
</tr>
<tr>
<td><strong>Customer</strong></td>
<td>07 Delivery of IT services in line with business requirements</td>
</tr>
<tr>
<td></td>
<td>08 Adequate use of applications, information and technology solutions</td>
</tr>
<tr>
<td><strong>Internal</strong></td>
<td>09 IT agility</td>
</tr>
<tr>
<td></td>
<td>10 Security of information, processing infrastructure and applications</td>
</tr>
<tr>
<td></td>
<td>11 Optimisation of IT assets, resources and capabilities</td>
</tr>
<tr>
<td></td>
<td>12 Enablement and support of business processes by integrating applications and technology into business processes</td>
</tr>
<tr>
<td></td>
<td>13 Delivery of programmes delivering benefits, on time, on budget, and meeting requirements and quality standards</td>
</tr>
<tr>
<td></td>
<td>14 Availability of reliable and useful information for decision making</td>
</tr>
<tr>
<td></td>
<td>15 IT compliance with internal policies</td>
</tr>
<tr>
<td><strong>Learning and Growth</strong></td>
<td>16 Competent and motivated business and IT personnel</td>
</tr>
<tr>
<td></td>
<td>17 Knowledge, expertise and initiatives for business innovation</td>
</tr>
</tbody>
</table>
Governance roles, activities and relationships:

- Define **Who** is involved in governance
- **How** they are involved
- **What** they do and
- **How** they interact

**COBIT 5** defines the difference between governance and management activities in principle 5
Principle 2: Covering the Enterprise End-to-End

Key components of a governance system

Source: COBIT® 5, figure 9. © 2012 ISACA®. All rights reserved.
Principle 3: Applying a Single Integrated Framework

COBIT5:

► Is complete in enterprise coverage
► Provides a basis to integrate effectively other frameworks, standards and practices used
► Aligns with the latest relevant standards and frameworks (COSO, ITIL, ISO, PMBOK, NIST etc)
► Integrates all knowledge previously dispersed over different ISACA frameworks (Risk IT, Val IT, BMIS)

Source: COBIT® 5, figure 12. © 2012 ISACA® All rights reserved.
Principle 3: Applying a Single Integrated Framework

Enablers provide structure to the COBIT 5 knowledge base.
Mapping of COBIT5

APPENDIX E. MAPPING OF COBIT 5
WITH THE MOST RELEVANT RELATED STANDARDS AND FRAMEWORKS

APPENDIX E
MAPPING OF COBIT 5 WITH THE MOST RELEVANT RELATED STANDARDS AND FRAMEWORKS

Introduction
This appendix compares COBIT 5 to the most relevant and used standards and frameworks in the governance space. For ISO/IEC 38500 this is done through a comparison based on the ISO/IEC 38500 principles; for the other comparisons a table format is used in which the COBIT 5 processes are mapped against the equivalent contents in the referred standard or framework.

COBIT 5 and ISO/IEC 38500
The following summarises how COBIT 5 supports adoption of the standard’s principles and implementation approach. The standard, ISO/IEC 38500:2008—Corporate governance of information technology, is based on six key principles. The practical implications of each principle are explained here, together with how COBIT 5 guidance enables good practice.

ISO/IEC 38500 Principles
PRINCIPLE 1—RESPONSIBILITY
What this means in practice:
The business (customer) and IT (provider) should collaborate in a partnership model utilising effective communications based on a positive and trusted relationship and demonstrating clarity regarding responsibility and accountability. For larger enterprises, an IT executive committee (also referred to as the IT strategy committee) acting on behalf of the board and chaired by a board member is a very effective mechanism for evaluating, directing and monitoring the use of IT in the enterprise and for advising the board on critical IT issues. Directors of small and medium-sized enterprises with a simpler command structure and shorter communication paths need to take a more direct approach when overseeing IT activities. In all cases, appropriate governance organisational structures, roles and responsibilities are required to be mandated from the governing body, providing clear ownership and accountability for important decisions and tasks. This should include relationships with key third-party IT service providers.

How ISACA’s guidance enables good practice:
1. The COBIT 5 framework defines a number of enablers for governance of enterprise IT. The ‘process’ enabler and the ‘organisational structures’ enabler, combined with the RACI7 charts, are particularly relevant in this context. They strongly advocate assignment of responsibilities, and provide examples of roles and responsibilities for board members and management for all key related processes and activities.
2. COBIT 5 Implementation explains the responsibilities of stakeholders and other involved parties when implementing or enhancing IT governance arrangements.
3. COBIT 5 has two levels of monitoring. The first level is relevant in a governance context. The process EDM05 Ensure stakeholder transparency explains the director’s role in monitoring and evaluating IT governance and IT performance with a generic method for establishing goals and objectives and related metrics.
Principle 4: Enabling a Holistic Approach

COBIT5 defines a set of enablers to support the implementation of a comprehensive governance and management system for enterprise IT.

COBIT5 enablers are:

► Factors that, individually and collectively, influence whether something will work
► Driven by the goals cascade
► Described by the COBIT5 framework in seven categories
Principle 4: Enabling a Holistic Approach
Principle 5: Separating Governance from Management

The COBIT 5 framework makes a clear distinction between governance and management.

► These two disciplines:
  ► Encompass different types of activities
  ► Require different organisational structures
  ► Serve different purposes

► Governance ensures that stakeholders needs, conditions and options are evaluated to determine balanced, agreed-on enterprise objectives to be achieved; setting direction through prioritisation and decision making; and monitoring performance and compliance against agreed-on direction and objectives.

► Management plans, builds, runs and monitors activities in alignment with the direction set by the governance body to achieve the enterprise objectives.
Principle 5: Separating Governance from Management

COBIT 5 is not prescriptive, but it advocates that organizations implement governance and management processes such that the key areas are covered, as shown.

Source: COBIT® 5, figure 15. © 2012 ISACA® All rights reserved.
COBIT 5 includes a process reference model (PRM), which defines and describes in detail a number of governance and management processes.
Process Reference Model

► Represents all the processes normally found in an enterprise relating to IT
► Provides a common reference model understandable to IT and business managers.
► Provides a common language
► Provides a framework for measuring, monitoring IT performance, communicating with service providers, and integrating best mgmt. practices
► Subdivides governance (1) and management (4) domains.
► 36 Processes
► Harmonized with other frameworks and standards

© 2012 ISACA. All Rights Reserved.
COBIT5
Process Reference Model:

Processes for Governance of Enterprise IT
Evaluate, Direct and Monitor

Align, Plan and Organise
AP001 Manage the IT Management Framework
AP002 Manage Strategy
AP003 Manage Enterprise Architecture
AP004 Manage Innovation
AP005 Manage Portfolio
AP006 Manage Budget and Costs
AP007 Manage Human Resources
AP008 Manage Relationships
AP009 Manage Service Agreements
AP010 Manage Suppliers
AP011 Manage Quality
AP012 Manage Risk
AP013 Manage Security

Build, Acquire and Implement
BA001 Manage Programmes and Projects
BA002 Manage Requirements Definition
BA003 Manage Solutions Identification and Build
BA004 Manage Availability and Capacity
BA005 Manage Organisational Change Enablement
BA006 Manage Changes
BA007 Manage Change Acceptance and Transitioning
BA008 Manage Knowledge
BA009 Manage Assets
BA010 Manage Configuration

Deliver, Service and Support
DS001 Manage Operations
DS002 Manage Service Requests and Incidents
DS003 Manage Problems
DS004 Manage Continuity
DS005 Manage Security Services
DS006 Manage Business Process Controls

Processes for Management of Enterprise IT

Source: COBIT® 5, figure 16. © 2012 ISACA® All rights reserved.
Exercise – Enabling a holistic approach

Developing enablers for AP012 process – Manage Risk

<table>
<thead>
<tr>
<th>AP012 Manage Risk</th>
</tr>
</thead>
<tbody>
<tr>
<td>Area: Management</td>
</tr>
<tr>
<td>Domain: Align, Plan, and Organise</td>
</tr>
</tbody>
</table>

Process Description
Continually identify, assess and reduce IT-related risk within levels of tolerance set by enterprise executive management.

Process Purpose Statement
Integrate the management of IT-related risk with overall ERM, and balance the costs and benefits of managing IT-related enterprise risk.
Challenges to Success?

- **Programme management** (outer ring)
- **Change enablement** (middle ring)
- **Continual improvement life cycle** (inner ring)
Challenges to Success?

1. What are the drivers?

2. Where are we now?

3. Where do we want to be?

4. What needs to be done?

5. How do we get there?

6. Did we get there?

7. How do we keep the momentum going?

- Programme management (outer ring)
- Change enablement (middle ring)
- Continual improvement life cycle (inner ring)

Plan programme
Define problems and opportunities
Define road map
Identify role players
Communicate outcome
Define current state
Define target state
Form implementation team
Recognise need to act
Monitor and evaluate
Implement improvements
Operate and use
Identify new approaches
Sustain
Establish desire to change
Review effectiveness

Ernst & Young
Quality In Everything We Do
COBIT 4.1 and COBIT 5 Differences
The major changes in COBIT 5 content and how they may impact GEIT* implementation/improvement are:

1. New GEIT principles
2. Increased **focus on enablers**
3. New and modified processes
4. Separated governance and management practices and activities
5. Revised and expanded goals and metrics
6. Defined inputs and outputs
7. More detailed RACI charts
8. Process Capability Assessment Model

(* Governance of Enterprise Information Technology)
COBIT 5 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

Source: COBIT® 5, figure 2. © 2012 ISACA® All rights reserved.
The COBIT 5 Enterprise Enablers

1. Principles, Policies and Frameworks

2. Processes
3. Organisational Structures
4. Culture, Ethics and Behaviour

5. Information
6. Services, Infrastructure and Applications
7. People, Skills and Competencies

© 2012 ISACA. All Rights Reserved.
New and Modified Processes

► There are several new and modified processes that reflect current thinking, in particular:
► APO03 Manage enterprise architecture
► APO04 Manage innovation
► APO05 Manage portfolio
► APO06 Manage budget and costs
► APO08 Manage relationships
► APO13 Manage security
► BAI05 Management organizational change enablement
► BAI08 Manage knowledge
► BAI09 Manage assets
► DSS05 Manage security service
► DSS06 Manage business process controls
Separating governance from management

► COBIT 5 introduces five new governance processes

► This guidance:
  ► Helps enterprises to further refine and strengthen executive management-level GEIT practices and activities
  ► Supports GEIT integration with existing enterprise governance practices and is aligned with ISO/IEC 38500

© 2012 ISACA. All Rights Reserved.
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

- AP001 Manage the IT Management Framework
- AP002 Manage Strategy
- AP003 Manage Enterprise Architecture
- AP004 Manage Innovation
- AP005 Manage Portfolio
- AP006 Manage Budget and Costs
- AP007 Manage Human Resources
- AP008 Manage Relationships
- AP009 Manage Service Agreements
- AP010 Manage Suppliers
- AP011 Manage Quality
- AP012 Manage Risk
- AP013 Manage Security

Build, Acquire and Implement

- BA001 Manage Programmes and Projects
- BA002 Manage Requirements Definition
- BA003 Manage Solutions Identification and Build
- BA004 Manage Availability and Capacity
- BA005 Manage Organisational Change Enablement
- BA006 Manage Changes
- BA007 Manage Change Acceptance and Transitioning
- BA008 Manage Knowledge
- BA009 Manage Assets
- BA010 Manage Configuration

Deliver, Service and Support

- DS001 Manage Operations
- DS002 Manage Service Requests and Incidents
- DS003 Manage Problems
- DS004 Manage Continuity
- DS005 Manage Security Services
- DS006 Manage Business Process Controls

Processes for Management of Enterprise IT

© 2012 ISACA. All Rights Reserved.
COBIT5 and Legacy ISACA Frameworks
### Figure 14—COBIT 4.1 Control Objectives Mapped to COBIT 5 (cont.)

<table>
<thead>
<tr>
<th>COBIT 4.1 Control Objective</th>
<th>Covered in COBIT 5 by:</th>
</tr>
</thead>
<tbody>
<tr>
<td>P04.5 IT Organisational Structure</td>
<td>APO01.01</td>
</tr>
<tr>
<td>P04.6 Establishment of Roles and Responsibilities</td>
<td>APO01.02</td>
</tr>
<tr>
<td>P04.7 Responsibility for IT Quality Assurance</td>
<td>APO11.01</td>
</tr>
<tr>
<td>P04.8 Responsibility for Risk, Security and Compliance</td>
<td>Deleted—these specific roles are no longer explicitly specified as a practice.</td>
</tr>
<tr>
<td>P04.9 Data and System Ownership</td>
<td>APO01.06</td>
</tr>
<tr>
<td>P04.10 Supervision</td>
<td>APO01.02</td>
</tr>
<tr>
<td>P04.11 Segregation of Duties</td>
<td>APO01.02; DSS08.02</td>
</tr>
<tr>
<td>P04.12 IT Staffing</td>
<td>APO07.01</td>
</tr>
<tr>
<td>P04.13 Key IT Personnel</td>
<td>APO07.02</td>
</tr>
<tr>
<td>P04.14 Contracted Staff Policies and Procedures</td>
<td>APO07.06</td>
</tr>
<tr>
<td>P04.15 Relationships</td>
<td>APO01.01</td>
</tr>
<tr>
<td>P05.1 Financial Management Framework</td>
<td>APO06.01</td>
</tr>
<tr>
<td>P05.2 Prioritisation Within IT Budget</td>
<td>APO06.02</td>
</tr>
<tr>
<td>P05.3 IT Budgeting</td>
<td>APO06.03</td>
</tr>
<tr>
<td>P05.4 Cost Management</td>
<td>APO06.04-05</td>
</tr>
</tbody>
</table>
COBIT 5 Processes

► Cover end-to-end business and IT activities

► Provides a more holistic and complete coverage of practices

► Makes the involvement, responsibilities and accountabilities of business stakeholders in the use of IT more explicit and transparent.

Source © 2012 ISACA® All rights reserved.
The COBIT5 governance and management practices can be related to:

- COBIT 4.1 control objectives
- Val IT and Risk IT processes

The COBIT 5 activities are related to:

- COBIT 4.1 control practices
- Val IT and Risk IT management practices

Source © 2012 ISACA® All rights reserved.
Goals and Metrics
Inputs and Outputs

COBIT 5

► Follows the same goal and metric concepts as COBIT 4.1, Val IT and Risk IT renamed as :
  ► Enterprise goals,
  ► IT-related goals
  ► Process goals
► Provides a revised goals cascade
► Provides inputs and outputs for every management practice
  ► COBIT 4.1 only provided these at the process level

Source © 2012 ISACA® All rights reserved.
Inputs and Outputs

### BAIO1 Process Practices, Inputs/Outputs and Activities

<table>
<thead>
<tr>
<th>Management Practice</th>
<th>Inputs</th>
<th>Outputs</th>
<th>To</th>
</tr>
</thead>
<tbody>
<tr>
<td>BAIO1.01 Maintain a standard approach for programme and project management.</td>
<td>From EDM02.02 Requirements for stage-gate reviews</td>
<td>Updated programme and project management approaches</td>
<td>Internal</td>
</tr>
<tr>
<td>Maintain a standard approach for programme and project management that enables</td>
<td>From EDM02.03 Actions to improve value delivery</td>
<td></td>
<td></td>
</tr>
<tr>
<td>governance and management review and decision making and delivery management</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>activities focussed on achieving value and goals (requirements, risk, costs,</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>schedule, quality) for the business in a consistent manner.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>From AP003.04 Architecture governance requirements</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Implementation phase descriptions</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>From AP005.05 Updated portfolios of programmes, services and assets</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>From AP010.04 Identified supplier delivery risk</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

#### Activities

1. Maintain and enforce a standard approach to programme and project management aligned to the enterprise’s specific environment and with good practice based on defined process and use of appropriate technology. Ensure that the approach covers the full life cycle and disciplines to be followed, including the management of scope, resources, risk, cost, quality, time, communication, stakeholder involvement, procurement, change control, integration and benefit realisation.

2. Update the programme and project management approach based on lessons learned from its use.
Metrics
IT Related Sample Goal Metrics

<table>
<thead>
<tr>
<th>Internal</th>
<th>09 IT agility</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• Level of satisfaction of business executives with IT’s responsiveness to new requirements</td>
</tr>
<tr>
<td></td>
<td>• Number of critical business processes supported by up-to-date infrastructure and applications</td>
</tr>
<tr>
<td></td>
<td>• Average time to turn strategic IT objectives into an agreed-on and approved initiative</td>
</tr>
</tbody>
</table>

| 10 Security of information, processing infrastructure and applications | • Number of security incidents causing financial loss, business disruption or public embarrassment |
|                                                                      | • Number of IT services with outstanding security requirements |
|                                                                      | • Time to grant, change and remove access privileges, compared to agreed-on service levels |
|                                                                      | • Frequency of security assessment against latest standards and guidelines |

| 11 Optimisation of IT assets, resources and capabilities | • Frequency of capability maturity and cost optimisation assessments |
|                                                          | • Trend of assessment results |
|                                                          | • Satisfaction levels of business and IT executives with IT-related costs and capabilities |

| 12 Enablement and support of business processes by integrating applications and technology into business processes | • Number of business processing incidents caused by technology integration errors |
|                                                                                                              | • Number of business process changes that need to be delayed or reworked because of technology integration issues |
|                                                                                                              | • Number of IT-enabled business programmes delayed or incurring additional cost due to technology integration issues |
|                                                                                                              | • Number of applications or critical infrastructures operating in silos and not integrated |

| 13 Delivery of programmes delivering benefits, on time, on budget, and meeting requirements and quality standards | • Number of programmes/projects on time and within budget |
|                                                                                                              | • Percent of stakeholders satisfied with programme/project quality |
|                                                                                                              | • Number of programmes needing significant rework due to quality defects |
|                                                                                                              | • Cost of application maintenance vs. overall IT cost |

| 14 Availability of reliable and useful information for decision making | • Level of business user satisfaction with quality and timeliness (or availability) of management information |
|                                                                       | • Number of business process incidents caused by non-availability of information |
|                                                                       | • Ratio and extent of erroneous business decisions where erroneous or unavailable information was a key factor |

| 15 IT compliance with internal policies | • Number of incidents related to non-compliance to policy |
|                                        | • Percent of stakeholders who understand policies |
|                                        | • Percent of policies supported by effective standards and working practices |
|                                        | • Frequency of policies review and update |

Source: COBIT® 5, © 2012 ISACA® All rights reserved.
## Metrics

### Process goals and related metrics

**BAI06 – Manage Changes**

<table>
<thead>
<tr>
<th>Process Goal</th>
<th>Related Metrics</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Authorised changes are made in a timely manner and with minimal errors.</td>
<td>• Amount of rework caused by failed changes</td>
</tr>
<tr>
<td></td>
<td>• Reduced time and effort required to make changes</td>
</tr>
<tr>
<td></td>
<td>• Number and age of backlogged change requests</td>
</tr>
<tr>
<td>2. Impact assessments reveal the effect of the change on all affected components.</td>
<td>• Percent of unsuccessful changes due to inadequate impact assessments</td>
</tr>
<tr>
<td>3. All emergency changes are reviewed and authorised after the change.</td>
<td>• Percent of total changes that are emergency fixes</td>
</tr>
<tr>
<td></td>
<td>• Number of emergency changes not authorised after the change</td>
</tr>
<tr>
<td>4. Key stakeholders are kept informed of all aspects of the change.</td>
<td>• Stakeholder feedback ratings on satisfaction with communications</td>
</tr>
</tbody>
</table>

Source: COBIT® 5, © 2012 ISACA® All rights reserved.
COBIT5
RACI Charts:

► Provides RACI* charts describing roles and responsibilities
  ► *Responsible, Accountable, Consulted, Informed
► Provides a more complete, detailed and clearer range of generic business and IT role players and charts enabling better definition of role player responsibilities or level of involvement when designing and implementing processes.
► For example…..

© 2012 ISACA. All Rights Reserved.
RACI Charts

RACI Chart

Activities
- Create and maintain a technology infrastructure plan.
- Create and maintain technology standards.
- Publish technology standards.
- Monitor technology evolution.
- Define (future) strategic use of new technology.

A RACI chart identifies who is Responsible, Accountable, Consulted and/or Informed.

EDM01 RACI Chart

Key Governance Practice
- EDM01.01 Evaluate the governance system.
- EDM01.02 Direct the governance system.
- EDM01.03 Monitor the governance system.
Process Capability Maturity Models and Assessments
What is the new COBIT Assessment Programme?

- COBIT 5 will be supported by a new *process capability assessment approach* based on ISO/IEC 15504

- The COBIT Assessment Programme includes:
  - **COBIT Process Assessment Model (PAM):** Using COBIT 5
  - **COBIT Assessor Guide:** Using COBIT 5
  - **COBIT Self Assessment Guide:** Using COBIT 5

- *Identical COBIT 4.1 versions also available*

- The COBIT 5 PAM is based on the ISO 15504 compliant process assessment model
What is a process assessment?

► ISO/IEC 15504-4 identifies process assessment as an activity that can be performed either as part of a process improvement initiative or as part of a capability determination approach.

► The purpose of process improvement is to continually improve the enterprise’s effectiveness and efficiency.

► The purpose of process capability determination is to identify the strengths, weaknesses and risk of selected processes with respect to a particular specified requirement through the processes used and their alignment with the business need.

► It provides an understandable, logical, repeatable, reliable and robust methodology for assessing the capability of IT processes.

© 2012 ISACA. All Rights Reserved.
What’s different?

But don’t we already have maturity models for COBIT 4.1 processes?

The new COBIT assessment programme is:

- A robust assessment process based on ISO 15504
- An alignment of COBIT’s maturity model scale with the international standard
- A new capability-based assessment model which includes:
  - Specific process requirements derived from COBIT 4.1
  - Ability to achieve process attributes based on ISO 15504
  - Evidence requirements
  - Assessor qualifications and experiential requirements

Results in a more robust, objective and repeatable assessment

Assessment results will likely vary from existing COBIT maturity models!
Maturity Model

P09 Assess and Manage IT Risks

Management of the process of Assess and manage IT risks that satisfies the business requirement for IT of analysing and communicating IT risks and their potential impact on business processes and goals is:

0 Non-existent when
Risk assessment for processes and business decisions does not occur. The organisation does not consider the business impacts associated with security vulnerabilities and development project uncertainties. Risk management is not identified as relevant to acquiring IT solutions and delivering IT services.

1 Initial/Ad Hoc when
IT risks are considered in an ad hoc manner. Informal assessments of project risk take place as determined by each project. Risk assessments are sometimes identified in a project plan but are rarely assigned to specific management. Specific IT-related risks, such as security, availability and integrity, are occasionally considered on a project-by-project basis. IT-related risks affecting day-to-day operations are seldom discussed at management meetings. Where risks have been considered, mitigation is inconsistent. There is an emerging understanding that IT risks are important and need to be considered.

2 Repeatable but Intuitive when
A developing risk assessment approach exists and is implemented at the discretion of the project managers. The risk management is usually at a high level and is typically applied only to major projects or in response to problems. Risk mitigation processes are starting to be implemented where risks are identified.

3 Defined when
An organisation-wide risk management policy defines when and how to conduct risk assessments. Risk management follows a defined process that is documented. Risk management training is available to all staff members. Decisions to follow the risk management process and receive training are left to the individual's discretion. The methodology for the assessment of risk is convincing and sound and ensures that key risks to the business are identified. A process to mitigate key risks is usually instituted once the risks are identified. Job descriptions consider risk management responsibilities.

4 Managed and Measurable when
The assessment and management of risk are standard procedures. Exceptions to the risk management process are reported to IT management. IT risk management is a senior management-level responsibility. Risk is assessed and mitigated at the individual project level and also regularly with regard to the overall IT operation. Management is advised on changes in the business and IT environment that could significantly affect the IT-related risk scenarios. Management is able to monitor the risk position and make informed decisions regarding the exposure it is willing to accept. All identified risks have a nominated owner, and senior management and IT management determine the levels of risk that the organisation will tolerate. IT management develops standard measures for assessing risk and defining risk/return ratios. Management budgets for an operational risk management project to reassess risks on a regular basis. A risk management database is established, and part of the risk management processes is beginning to be automated. IT management considers risk mitigation strategies.

5 Optimised when
Risk management develops to the stage where a structured, organisation-wide process is enforced and well managed. Good practices are applied across the entire organisation. The capture, analysis and reporting of risk management data are highly automated.
Guidance is drawn from leaders in the field, and the IT organisation takes part in peer groups to exchange experiences. Risk management is truly integrated into all business and IT operations, is well accepted and extensively involves the users of IT services. Management detects and acts when major IT operational and investment decisions are made without consideration of the risk management plan. Management continually assesses risk mitigation strategies.
Differences to COBIT Maturity Model

- The COBIT 4.1 PAM uses a measurement framework that is **similar** in terminology to the existing maturity models in COBIT 4.1
- While the words are similar the scales are **NOT** the same:
  - The COBIT PAM uses the capability scale from ISO/IEC 15504, whereas the existing COBIT maturity models uses a scale derived from SEI\CMM
  - A PAM level 3 is **NOT** the same as a CMM level 3
  - Assessments done under the PAM are likely to result in ‘lower’ scores
  - PAM assessments are based on more fully defined and defensible attributes

<table>
<thead>
<tr>
<th>COBIT 4.1 Process Maturity Level</th>
<th>ISO/IEC 15504 Process Capability Level</th>
<th>Attribute</th>
</tr>
</thead>
<tbody>
<tr>
<td>5 Optimised</td>
<td>5 Optimizing</td>
<td>PA 5.1 Process innovation</td>
</tr>
<tr>
<td></td>
<td></td>
<td>PA 5.2 Process optimization</td>
</tr>
<tr>
<td>4 Managed and measurable</td>
<td>4 Predictable</td>
<td>PA 4.1 Process measurement</td>
</tr>
<tr>
<td></td>
<td></td>
<td>PA 4.2 Process control</td>
</tr>
<tr>
<td>3 Defined</td>
<td>3 Established</td>
<td>PA 3.1 Process definition</td>
</tr>
<tr>
<td></td>
<td></td>
<td>PA 3.2 Process deployment</td>
</tr>
<tr>
<td>2 Repeatable but intuitive</td>
<td>2 Managed</td>
<td>PA 2.1 Performance management</td>
</tr>
<tr>
<td></td>
<td></td>
<td>PA 2.2 Work product management</td>
</tr>
<tr>
<td>1 Initial/ad hoc</td>
<td>1 Performed</td>
<td>PA 1.1 Process performance</td>
</tr>
<tr>
<td>0 Non-existent</td>
<td>0 Incomplete</td>
<td></td>
</tr>
</tbody>
</table>
Process Capability Model and Assessments

► The COBIT Assessment Programme approach is more robust, reliable and repeatable as a process capability assessment method

► The COBIT Assessment Programme supports:
  ► Formal assessments by accredited assessors
  ► Less rigorous self-assessments for internal gap analysis and process improvement planning

► The COBIT Assessment Programme, in the future, will also potentially enable an enterprise to obtain an independent and certified assessments aligned to the ISO/IEC standard
Process Capability Model and Assessments

Level 5: Optimizing process
- PA 5.1: Process innovation attribute
- PA 5.2: Process optimization attribute

Level 4: Predictable process
- PA 4.1: Process measurement attribute
- PA 4.2: Process control attribute

Level 3: Established process
- PA 3.1: Process definition attribute
- PA 3.2: Process deployment attribute

Level 2: Managed process
- PA 2.1: Performance management attribute
- PA 2.2: Work product management attribute

Level 1: Performed process
- PA 1.1: Process performance attribute

Level 0: Incomplete process
- Incomplete: The process is not implemented or fails to achieve its purpose

Optimizing: The process is continuously improved to meet relevant current and projected business goals.

Predictable: The process is enacted consistently within defined limits.

Established: A defined process is used based on a standard process.

Managed: The process is managed and work products are established, controlled, and maintained.

Performed: The process is implemented and achieves its process purpose.

Incomplete: The process is not implemented or fails to achieve its purpose.

Source: COBIT® 5, © 2012 ISACA® All rights reserved.
Implementing COBIT 5

The COBIT 5 Implementation Guide was released at the same time as the COBIT 5 Framework and COBIT 5 Enabling Processes
Continual life cycle approach

- Programme management (outer ring)
- Change enablement (middle ring)
- Continual improvement life cycle (inner ring)
Challenges to Success?

1. What are the drivers?
2. Where are we now?
3. What do we want to be?
4. What needs to be done?
5. How do we get there?
6. Did we get there?
7. How do we keep the momentum going?
8. Review effectiveness
9. Realise benefits

- Programme management (outer ring)
- Change enablement (middle ring)
- Continual improvement life cycle (inner ring)
Benefits of Using COBIT® 5

► Enterprise wide benefits:
  ► Increased value creation through effective governance and management of enterprise information and technology assets
  ► Increased business user satisfaction with IT engagement and services–IT seen as a key enabler.
  ► Increased compliance with relevant laws, regulations and policies
  ► IT function becomes more business focused
  ► Increases IT’s contribution to the enterprise and the management of information
  ► “Companies with effective IT governance have profits that are 20% higher than other companies pursuing similar strategies”

COBIT 5: Verticals

COBIT 5 for Information Security

Products in Planning or Development

COBIT 5: Enabling Information
A detailed reference guide for the Information enabler for the governance and management of enterprise IT (GEIT). This guide further explains the Information Model (based on the COBIT 5 generic enabler model) and provides examples of fully elaborated information entities. This guide should be considered the "information" equivalent of COBIT 5: Enabling Processes. It is scheduled to be available in the second quarter of 2013.

COBIT 5 for Risk
This development project will create an information risk view of COBIT 5, which will serve as the information risk specific guidance as it relates to COBIT for ISACA’s information risk constituents. The guide should be considered the risk focused equivalent of the COBIT 5 for Information Security publication within the COBIT 5 family of products. The product is scheduled to be issued during the third quarter of 2013.

COBIT 5 for Assurance
This publication creates an information assurance view of COBIT 5, to provide guidance for ISACA’s information assurance constituents. It should be considered as the assurance equivalent of COBIT 5 for Information Security. It is scheduled to be available in the second quarter of 2013.

COBIT Translations
We are currently reviewing COBIT 5 translation business cases submitted by chapters. If your chapter would like to submit a business case, please visit the chapter-protected area of the ISACA web site. Individuals willing to review translations of COBIT 5 are invited to contact translation@isaca.org.

COBIT 5 Online
ISACA is exploring the implications of the release of COBIT 5 on the COBIT Online service. Currently:

Page 68
In Summary…

COBIT 5 brings together the five principles that allow the enterprise to build an effective governance and management framework based on a holistic set of seven enablers that optimises information and technology investment and use for the benefit of stakeholders.
Ernst & Young

Assurance | Tax | Transactions | Advisory

About Ernst & Young
Ernst & Young is a global leader in assurance, tax, transaction and advisory services. Worldwide, our 130,000 people are united by our shared values and an unwavering commitment to quality. We make a difference by helping our people, our clients and our wider communities achieve potential.

For more information, please visit www.ey.com.