COBIT 5

Presented by
Brian Barnier
C5 Workgroup Member
brian@valuebridgeadvisors.com
Enterprises and their executives strive to:

- Maintain quality information to support business decisions.
- Generate business value from IT-enabled investments, i.e., achieve strategic goals and realise business benefits through effective and innovative use of IT.
- Achieve operational excellence through reliable and efficient application of technology.
- Maintain IT-related risk at an acceptable level.
- Optimise the cost of IT services and technology.

How can these benefits be realised to create enterprise stakeholder value?
Delivering enterprise stakeholder value requires good governance and management of information and technology (IT) assets.

Enterprise boards, executives and management have to embrace IT like any other significant part of the business.

External legal, regulatory and contractual compliance requirements related to enterprise use of information and technology are increasing, threatening value if breached.

COBIT 5 provides a comprehensive framework that assists enterprises to achieve their goals and deliver value through effective governance and management of enterprise IT.
Simply stated, COBIT 5 helps enterprises to create optimal value from IT by maintaining a balance between realising benefits and optimising risk levels and resource use.

COBIT 5 enables information and related technology to be governed and managed in a holistic manner for the whole enterprise, taking in the full end-to-end business and functional areas of responsibility, considering the IT-related interests of internal and external stakeholders.

The COBIT 5 principles and enablers are generic and useful for enterprises of all sizes, whether commercial, not-for-profit or in the public sector.
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
COBIT 5 enablers

COBIT 5 Enterprise Enablers

- Processes
- Organisational Structures
- Culture, Ethics and Behaviour

Principles, Policies and Frameworks

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

Resources
Governance and Management

- **Governance** ensures that enterprise objectives are achieved by **evaluating** stakeholder needs, conditions and options; setting **direction** through prioritisation and decision making; and **monitoring** performance, compliance and progress against agreed direction and objectives (EDM)

- **Management** plans, **builds, runs and monitors** activities in alignment with the direction set by the governance body to achieve the enterprise objectives (PBRM)
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.
About YOU

- Industry
- Role
- Years of use of ISACA products
YOUR situation

- How process oriented is your organization?
- How process oriented is your IT organization?
- To what extent does your organization currently use: COBIT, ValIT, Risk IT, Implementation Guide, BMIS, ITAF:
  - Full, Partial, Starting, Considering, No plans?
- Conduct a formal maturity assessment?
- If yes, maturity level?
Your management team

- **CIO background**
  - business, tech or equal balance?

- **What does your CIO think about ISACA products?**
  - Use!, if you want to, audit does, not so hot, not aware

- **CIO reports to**
  - CEO, CFO, COO, CAO, other?

- **What does that role think about ISACA products?**
  - Use!, if you want to, audit does, not so hot, not aware
Business needs

- Clarity of objectives
  - Business
  - IT

- What complications/hurdles are faced in by IT leaders in achieving these business objectives?
ISACA product use

- What is most helpful about ISACA products?
- What is most helpful about ISACA support?

- What challenges have you faced in adopting?
- What challenges have you faced in implementing?

- What do YOU most want to learn today?
Comparing COBIT 5 and 4.1
Transition Message

• COBIT 5 builds on previous versions of COBIT (and Val IT and Risk IT) and so enterprises can also build on what they have developed using earlier versions.
Enterprises exist to create value for their stakeholders. Consequently, any enterprise—commercial or not—will have value creation as a governance objective.

Value creation means: Realising benefits at an optimal resource cost while optimising risk.
Principle 1: Meeting Stakeholder Needs

- Stakeholder needs have to be transformed into an enterprise’s actionable strategy.
- The COBIT 5 goals cascade translates stakeholder needs into specific, actionable and customised goals within the context of the enterprise, IT-related goals and enabler goals.
Stakeholder needs can be related to a set of generic enterprise goals.

These enterprise goals have been developed using the Balanced Scorecard (BSC) dimensions. (Kaplan, Robert S.; David P. Norton; The Balanced Scorecard: Translating Strategy into Action, Harvard University Press, USA, 1996)

The enterprise goals are a list of commonly used goals that an enterprise has defined for itself.

Although this list is not exhaustive, most enterprise-specific goals can be easily mapped onto one or more of the generic enterprise goals.
## Stakeholder Value and Business Objectives (cont.)

<table>
<thead>
<tr>
<th>BSC Dimension</th>
<th>Enterprise Goals</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>
- The goals cascade is not ‘new’ to COBIT.
- It was introduced in COBIT 4.0 in 2005.
- Those COBIT users who have applied the thinking to their enterprises have found value.
- BUT not everyone has recognized this value.
- The goals cascade supports the COBIT 5 stakeholder needs principle that is fundamental to COBIT and has therefore been made prominent early in the COBIT 5 guidance.
- The goals cascade has been revisited and updated for the COBIT 5 release.
Governance and Management Defined

- **What sort of framework is COBIT?**
  - An IT audit and control framework?
    - COBIT (1996) and COBIT 2\textsuperscript{nd} Edition (1998)
    - Focus on Control Objectives
  - An IT management framework?
    - COBIT 3\textsuperscript{rd} Edition (2000)
    - Management Guidelines added
  - An IT governance framework?
    - COBIT 4.0 (2005) and COBIT 4.1 (2007)
    - Governance and compliance processes added
    - Assurance processes removed
- **BUT what is the difference between governance and management?**
Governance ensures that enterprise objectives are achieved by evaluating stakeholder needs, conditions and options; setting direction through prioritisation and decision making; and monitoring performance, compliance and progress against agreed-on direction and objectives (EDM).

Management plans, builds, runs and monitors activities in alignment with the direction set by the governance body to achieve the enterprise objectives (PBRM).
The COBIT 5 process reference model subdivides the IT-related practices and activities of the enterprise into two main areas—governance and management—with management further divided into domains of processes:

- The GOVERNANCE domain contains five governance processes; within each process, evaluate, direct and monitor (EDM) practices are defined.
- The four MANAGEMENT domains are in line with the responsibility areas of plan, build, run and monitor (PBRM)
Areas of Change

The following slides summarise the major changes in COBIT 5 content and how they may impact GEIT implementation/improvement:

1. New GEIT Principles
2. Increased Focus on Enablers
3. New Process Reference Model
4. New and Modified Processes
5. Practices and Activities
6. Goals and Metrics
7. Inputs and Outputs
8. RACI Charts
9. Process Capability Maturity Models and Assessments
1. New GEIT Principles

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
1. New GEIT Principles (cont.)

- Val IT and Risk IT frameworks are principles-based.
- Feedback indicated that principles are easy to understand and put into an enterprise context, allowing value to be derived from the supporting guidance more effectively.
- ISO/IEC 38500 also incorporates principles to underpin its messages to achieve the same market benefit delivery, although the principles in this standard and COBIT 5 are not the same.
2. Increased Focus on Enablers

• COBIT 4.1 did not have enablers! Yes it did—they were not called enablers, but they were there, explicitly or implicitly!
2. Increased Focus on Enablers (cont.)

- Information, infrastructure, applications (services) and people (people, skills and competencies) were COBIT 4.1 resources.
- Principles, policies and frameworks were mentioned in a few COBIT 4.1 processes.
- Processes were central to COBIT 4.1 use.
- Organisational structure was implied through the responsible, accountable, consulted or informed (RACI) roles and their definitions.
- Culture, ethics and behaviour were mentioned in a few COBIT 4.1 processes.
3. New Process Reference Model

- COBIT 5 is based on a revised process reference model with a new governance domain and several new and modified processes that now cover enterprise activities end-to-end—i.e., business and IT function areas.
- COBIT 5 consolidates COBIT 4.1, Val IT and Risk IT into one framework, and has been updated to align with current best practices—e.g., ITIL, TOGAF.
- The new model can be used as a guide for adjusting as necessary the enterprise’s own process model (just like COBIT 4.1).
3. New Process Reference Model (cont.)

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 Changes 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 Systems of Internal Control
- MEA03 Monitor, Evaluate and Assess Compliance With External Requirements
4. New and Modified Processes

• COBIT 5 introduces five new governance processes that have leveraged and improved COBIT 4.1, Val IT and Risk IT governance approaches.

• 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
COBIT 5 has clarified management level processes and integrated COBIT 4.1, Val IT and Risk IT content into one process reference model.
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 Manage organisational change enablement.
- BAI08 Manage knowledge.
- BAI09 Manage assets.
- DSS05 Manage security service.
- DSS06 Manage business process controls.
COBIT 5 processes now cover end-to-end business and IT activities—i.e., a full enterprise-level view.

This provides for a more holistic and complete coverage of practices reflecting the pervasive enterprisewide nature of IT use.

It makes the involvement, responsibilities and accountabilities of business stakeholders in the use of IT more explicit and transparent.
5. Practices and Activities

- The COBIT 5 governance or management practices are equivalent to the COBIT 4.1 control objectives and Val IT and Risk IT processes.
  

- The COBIT 5 activities are equivalent to the COBIT 4.1 control practices and Val IT and Risk IT management practices.

- COBIT 5 integrates and updates all of the previous content into the one new model, making it easier for users to understand and use this material when implementing improvements.
6. Goals and Metrics

- COBIT 5 follows the same goal and metric concepts as COBIT 4.1, Val IT and Risk IT, but these are renamed enterprise goals, IT-related goals and process goals reflecting an enterprise level view.
- COBIT 5 provides a revised goals cascade based on enterprise goals driving IT-related goals and then supported by critical processes.
- COBIT 5 provides examples of goals and metrics at the enterprise, process and management practice levels. This is a change to COBIT 4.1, Val IT and Risk IT, which went down one level lower.
COBIT 5 provides inputs and outputs for every management practice, whereas COBIT 4.1 only provided these at the process level.

This provides additional detailed guidance for designing processes to include essential work products and to assist with interprocess integration.
8. RACI Charts

- COBIT 5 provides RACI charts describing roles and responsibilities in a similar way to COBIT4.1, Val IT and Risk IT.
- COBIT 5 provides a more complete, detailed and clearer range of generic business and IT role players and charts than COBIT 4.1 for each management practice, enabling better definition of role player responsibilities or level of involvement when designing and implementing processes.
### 8. RACI Charts (cont.)

#### RACI Chart

<table>
<thead>
<tr>
<th>Activities</th>
<th>CIO</th>
<th>CTO</th>
<th>Business Executive</th>
<th>CIO</th>
<th>Business Process Owner</th>
<th>Head Architect</th>
<th>IT Consultant</th>
<th>PMO</th>
<th>Compliance, Risk &amp; Security</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create and maintain a technology infrastructure plan.</td>
<td>I</td>
<td>I</td>
<td>A</td>
<td>C</td>
<td>R</td>
<td>C</td>
<td>C</td>
<td>C</td>
<td></td>
</tr>
<tr>
<td>Create and maintain technology standards.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Publish technology standards.</td>
<td>I</td>
<td>I</td>
<td>A</td>
<td></td>
<td>I</td>
<td>C</td>
<td>I</td>
<td>I</td>
<td></td>
</tr>
<tr>
<td>Monitor technology evolution.</td>
<td>I</td>
<td>I</td>
<td>A</td>
<td></td>
<td>C</td>
<td>R</td>
<td>C</td>
<td>C</td>
<td></td>
</tr>
<tr>
<td>Define (future) (strategic) use of new technology.</td>
<td></td>
<td></td>
<td></td>
<td>C</td>
<td>C</td>
<td>A</td>
<td>C</td>
<td>R</td>
<td></td>
</tr>
<tr>
<td>C</td>
<td>C</td>
<td>C</td>
<td>C</td>
<td>C</td>
<td>C</td>
<td>C</td>
<td>C</td>
<td>C</td>
<td></td>
</tr>
</tbody>
</table>

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

#### EDM01 RACI Chart

| Key Governance Practice | Board | Chief Executive Officer | Chief Financial Officer | Chief Operating Officer | Chief Architect | Business Executives | Business Process Owners | Strategy Executive Committee | Steering (Programmes/Projects) Committee | Value Management Office | Chief Information Security Officer | Chief Information Officer | Architecture Board | Enterprise Risk Committee | Head Human Resources | Compliance | Audit | Chief Architect | Head IT Operations | Head IT Administration | Service Manager | Information Security Manager | Business Continuity Manager | Privacy Office |
|-------------------------|-------|-------------------------|-------------------------|-------------------------|----------------|---------------------|-------------------------|--------------------------------|--------------------------------|---------------------|--------------------------|----------------------|-------------------|---------------------------|---------------------|-------------|------|----------------|--------------------------|----------------------|-------------------|---------------------------|------------------|
| EDM01.01 Evaluate the governance system.                                  |       | A                        | R                       | C                       | C             | R                   | R                       | C                             | C                  | C                       | C                    | R                | C                         | C                   | C           | C    | R              | R                       | R                    | R                 | R                         | R                |
| EDM01.02 Direct the governance system.                                    |       | A                        | R                       | C                       | R             | C                   | I                       | C                             | C                  | C                       | R                    | C                | C                         | I                   | I           | I    | C              | I                       | I                    | I                 | I                         | I                |
| EDM01.03 Monitor the governance system.                                   |       | A                        | R                       | C                       | R             | I                   | I                       | C                             | C                  | C                       | R                    | C                | C                         | I                   | I           | I    | C              | I                       | I                    | I                 | I                         | I                |
9. Process Capability Maturity Models and Assessments

- COBIT 5 discontinues the COBIT 4.1, Val IT and Risk IT CMM-based capability maturity modelling approach.
- COBIT 5 will be supported by a new process capability assessment approach based on ISO/IEC 15504, and the COBIT Assessment Programme has already been established for COBIT 4.1 as an alternative to the CMM approach. 
  www.isaca.org/Knowledge-Center/cobit/Pages/COBIT-Assessment-Programme.aspx
- The COBIT 4.1, Val IT and Risk IT CMM-based approaches are not considered compatible with the ISO/IEC 15504 approach because the methods use different attributes and measurement scales.
<table>
<thead>
<tr>
<th>COBIT 4.1 Maturity Model Levels</th>
<th>COBIT 5 ISO/IEC 15504 Based Capability Levels</th>
<th>Meaning of the COBIT 5 ISO/IEC 15504 Based Capability Levels</th>
<th>Context</th>
</tr>
</thead>
<tbody>
<tr>
<td>5. Optimised</td>
<td>5. Optimised</td>
<td>Continuously improved to meet relevant current and projected enterprise goals.</td>
<td>Enterprise view/ corporate knowledge</td>
</tr>
<tr>
<td>4. Managed and Measurable</td>
<td>4. Predictable</td>
<td>Operates within defined limits to achieve its process outcomes.</td>
<td></td>
</tr>
<tr>
<td>3. Defined</td>
<td>3. Established</td>
<td>Implemented using a defined process that is capable of achieving its process outcomes.</td>
<td></td>
</tr>
<tr>
<td>N/A</td>
<td>2. Managed</td>
<td>Implemented in a managed fashion (planned, monitored and adjusted) and its work products are appropriately established, controlled and maintained.</td>
<td>Instance view/ individual knowledge</td>
</tr>
<tr>
<td>N/A</td>
<td>1. Performed</td>
<td>Process achieves its process purpose.</td>
<td></td>
</tr>
<tr>
<td>2. Repeatable</td>
<td>0. Incomplete</td>
<td>Not implemented or little or no evidence of any systematic achievement of the process purpose.</td>
<td></td>
</tr>
<tr>
<td>1. Ad Hoc</td>
<td>0. Non-existent</td>
<td></td>
<td></td>
</tr>
<tr>
<td>0. Non-existent</td>
<td>0. Incomplete</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
9. Process Capability Maturity Models and Assessments (cont.)
The COBIT Assessment Programme approach is considered by ISACA to be more robust, reliable and repeatable as a process capability assessment method.

The COBIT Assessment Programme supports:

- Formal assessments by accredited assessors (assessor training is being developed)
- 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.
What materials support the COBIT Assessment Programme approach?

- **COBIT Process Assessment Model (PAM): Using COBIT 4.1**—Serves as a base reference document for the performance of a capability assessment of an organisation’s current IT processes against COBIT

- **COBIT Assessor Guide: Using COBIT 4.1**—Provides details on how to undertake a full ISO-compliant assessment

- **COBIT Self-assessment Guide: Using COBIT 4.1**—Provides guidance on how to perform a basic self-assessment of an organisation’s current IT process capability levels against COBIT processes

The above materials exist to support COBIT 4.1-based assessments now; versions will be produced to support COBIT 5-based assessments.
COBIT 4.1, Val IT and Risk IT users wishing to move to the new COBIT Assessment Programme approach will need to realign their previous ratings, adopt and learn the new method, and initiate a new set of assessments in order to gain the benefits of the new approach.

Although some of the information gathered from previous assessments may be reusable, care will be needed in migrating this information forward because there are significant differences in requirements.
COBIT 4.1, Val IT and Risk IT users wishing to continue with the CMM-based approach, either as an interim or ongoing approach, can use the COBIT 5 guidance, but must use the COBIT 4.1 generic attribute table without the high-level maturity models.
COBIT 5 Implementation
The improvement of the governance of enterprise IT (GEIT) is widely recognised by top management as an essential part of enterprise governance.

Information and the pervasiveness of information technology are increasingly part of every aspect of business and public life.

The need to drive more value from IT investments and manage an increasing array of IT-related risk has never been greater.

Increasing regulation and legislation over business use of information is also driving heightened awareness of the importance of a well-governed and managed IT environment.
COBIT 5 Implementation (cont.)

- ISACA has developed the COBIT 5 framework to help enterprises implement sound governance enablers. Indeed, implementing good GEIT is almost impossible without engaging an effective governance framework. Best practices and standards are also available to underpin COBIT 5.

- Frameworks, best practices and standards are useful only if they are adopted and adapted effectively. There are challenges that need to be overcome and issues that need to be addressed if GEIT is to be implemented successfully.

- **COBIT 5: Implementation** provides guidance on how to do this.
COBIT 5 Implementation (cont.)

• COBIT 5: Implementation covers the following subjects:
  • Positioning GEIT within an enterprise
  • Taking the first steps towards improving GEIT
  • Implementation challenges and success factors
  • Enabling GEIT-related organisational and behavioural change
  • Implementing continual improvement that includes change enablement and programme management
  • Using COBIT 5 and its components
COBIT 5 Implementation (cont.)

Source: COBIT® 5, figure 17. © 2012 ISACA® All rights reserved.
COBIT 5
Future Supporting Products
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

Source: COBIT® 5, figure 11. © 2012 ISACA® All rights reserved.
COBIT 5 Future Supporting Products

Future supporting products:

• Professional Guides:
  • COBIT 5 for Information Security
  • COBIT 5 for Assurance
  • COBIT 5 for Risk

• Enabler Guides:
  • COBIT 5: Enabling Information

• COBIT Online Replacement

• COBIT Assessment Programme:
  • Process Assessment Model (PAM): Using COBIT 5
  • Assessor Guide: Using COBIT 5
  • Self-assessment Guide: Using COBIT 5