Foundational IT Governance
A Foundational Framework for Governing Enterprise IT
Adapted from the “ISACA COBIT 5 Framework”

Steven Hunt
Enterprise IT Governance Strategist
NASA Ames Research Center

Michael Nelson
Director of Information Assurance
Logyx, LLC
ITG Presentation Suite

This presentation is integral to a series of concepts presented in a suite of documents as listed below. In order to thoroughly understand the aggregation of the concepts presented it is recommended that one review them in order as listed:

- Fundamental IT Governance Framework – Reference
- Fundamental IT Governance – Applied (NASA & ARC)
- Foundational IT Governance Framework – Reference
- Comprehensive IT Governance Framework
Agenda

• IT Governance Defined
• Foundational Enterprise IT Governance
  – What is COBIT / COBIT 5?
  – COBIT 5 Objectives
  – COBIT 5 Framework
  – COBIT 5 Benefits
• COBIT 5 Principles
  – Principle 1 – Meeting Stakeholder Needs
  – Principle 2 – Covering the Enterprise End-To-End
  – Principle 3 – Applying a Single Integrated Framework
  – Principle 4 – Enabling a Holistic Approach
  – Principle 5 – Separating Governance & Management
• COBIT Process Capability Model
• Implementation Guidance
• Summary & Recommendations
• Questions?
• References
IT Governance Defined

Governance

• Ensures that enterprise objectives are achieved by evaluating stakeholder needs, conditions, and options
• Sets direction through prioritization and decision making
• Monitors performance, compliance, and progress against the agreed upon direction and objectives

Management

• Plans, builds, runs, & monitors activities in alignment with the direction set by the governance body to achieve the enterprise objectives
IT Governance Defined

Integration of Governance & Management

• Distinction between Governance & Management often misunderstood

• **Effective integration of these two elements is critical** for successful IT Governance in any enterprise or organization

• IT Governance is **NOT** responsible for “rendering” IT infrastructure

• IT Governance is **IS** responsible for “oversight of the management processes” that render IT infrastructure
ITG Primary Objectives

Effective IT Governance achieves five primary objectives:

• **Strategic Alignment** –
  Ensure IT is aligned with the business – focus on aligning technology with the business and collaborative solutions

• **Value Delivery** –
  Ensure IT delivers value to the business – concentrating on optimizing expenses and proving the value of IT

• **Risk Management** –
  Ensure IT manages risk – addressing the safeguard of IT assets, disaster recovery, and continuity of operations

• **Resource Management** –
  Ensure IT manages resources – realizing the optimal investment in, and proper management of, critical IT resources

• **Performance Management** –
  Ensure IT manages performance – tracking & monitoring strategy implementation, project success, resource usage, process performance, and service delivery
Agenda

• IT Governance Defined
• **Foundational Enterprise IT Governance**
  – What is COBIT / COBIT 5?
  – COBIT 5 Objectives
  – COBIT 5 Framework
  – COBIT 5 Benefits
• COBIT 5 Principles
  – Principle 1 – Meeting Stakeholder Needs
  – Principle 2 – Covering the Enterprise End-To-End
  – Principle 3 – Applying a Single Integrated Framework
  – Principle 4 – Enabling a Holistic Approach
  – Principle 5 – Separating Governance & Management
• COBIT Process Capability Model
• Implementation Guidance
• Summary & Recommendations
• Questions?
• References
This presentation is based upon ISACA’s Foundational Enterprise IT Governance Framework known as COBIT 5
What is COBIT?

• Control Objectives for Information and Related Technology
  – Now simply referred to as “COBIT”

COBIT Evolution
What is COBIT 5?

• COBIT 5 is a Foundational enterprise IT Governance framework, providing a basis to effectively integrate other complimentary frameworks, standards, and practices.

• As a single overarching framework it serves as a consistent and integrated source of guidance in a non-technical, technology-agnostic, common language.

• COBIT 5 addresses the governance and management of information and related technology from an enterprise-wide, end-to-end perspective, including the activities and responsibilities of both the IT function and non-IT business functions.

• The end-to-end aspect is further supported by COBIT 5 coverage of all critical business elements, e.g. processes, organizational structures, principles & policies, culture, skills, service capabilities.
COBIT 5 Objectives

• Provide a renewed and authoritative full-spectrum framework for the governance and management of enterprise IT.

• Building on the current widely recognized and accepted COBIT framework, link together and reinforce all other major ISACA frameworks and guidance.

• Connect to and align with other major frameworks and standards (ISO 38500, ITIL, EA, NIST etc).

• Incorporate familiar components such as a Domain/Process model, Governance/Management Best Practices, RACI charts, and process input/output linkages.
The COBIT 5 Framework

• Major Update from version 4.1
• First Exposure Draft release - June 28, 2011
• Documents released on April 10, 2012
  – COBIT 5 Framework
  – COBIT 5 Enabling Processes
  – COBIT 5 Implementation
• Documents under development
  – COBIT 5 Enabling Information & other enabler guides
  – COBIT 5 for Information Security
  – COBIT 5 for Assurance
  – COBIT 5 for Risk
  – Other professional guides
The COBIT 5 Framework
The COBIT 5 Framework

• A governance & management framework
• Starts with stakeholder drivers and needs relative to IT
• Intended for all enterprises including non-profit and public sector
• Integrates, Links, and Reinforces other major frameworks and guidance:
  – IT Infrastructure Library (ITIL)
  – ISO Standards
  – The Open Group Architecture Framework (TOGAF)
  – Project Management Body Of Knowledge (PMBOK)
  – Val IT (value framework - ITGI)
  – Risk IT (risk framework - ITGI)
  – Business Model for Information Security (BMIS - ITGI)
  – IT Assurance Framework (ITAF - ITGI)
  – IT Governance Board Briefing (ITGI)
  – Taking Governance Forward (ITGI)
The COBIT 5 Framework

• Framework components
  – Principles
  – Architecture
  – Goals Cascade
  – Enablers
  – COBIT Process Assessment Model (PAM)
  – Implementation Guidance

• Includes familiar ITG Framework elements
  – Domain / Process Model
  – Governance / Management Best Practices
  – Granular Practice Activities
  – Process Inputs / Outputs
  – RACI charts
COBIT 5 Benefits

Incorporating an operational model, and a common language for all parts of the business involved in IT activities, is one of the most important and critical steps toward good governance. It provides a framework for:

- Integrating Best Practices
- Communicating with Stakeholders
- Measuring & Monitoring IT Performance
COBIT 5 Benefits

Enterprise-wide Benefits

• **Benefits realization** through Enterprise IT Governance
• **Business-user satisfaction** with IT engagement and services
• IT seen as a key enabler
• **Compliance** with relevant laws, regulations, and policies
COBIT 5 Benefits

Key Business Benefits
• **End-to-end** enterprise governance and management of IT
• **Transparency** in decision making

Key IT Benefits
• **Agility** of IT to respond to business needs
• **Alignment** of IT tasks/activities with business needs
• **Optimization** of:
  – IT assets & resources
  – IT-related business risk
  – Cost performance of IT
Agenda

• IT Governance Defined
• Foundational Enterprise IT Governance
  – What is COBIT / COBIT 5?
  – COBIT 5 Objectives
  – COBIT 5 Framework
  – COBIT 5 Benefits
• **COBIT 5 Principles**
  – Principle 1 – Meeting Stakeholder Needs
  – Principle 2 – Covering the Enterprise End-To-End
  – Principle 3 – Applying a Single Integrated Framework
  – Principle 4 – Enabling a Holistic Approach
  – Principle 5 – Separating Governance & Management
• COBIT Process Capability Model
• Implementation Guidance
• Summary & Recommendations
• Questions?
• References
IT Governance Principles

Principles and policies are the vehicle by which governance decisions are institutionalized within the enterprise and therefore are an interaction between governance decisions (direction setting) and management (execution of decisions)
COBIT 5 Principles

PRINCIPLE 1 – MEETING STAKEHOLDER NEEDS

PRINCIPLE 2 – COVERING THE ENTERPRISE END-TO-END

PRINCIPLE 3 – APPLYING A SINGLE INTEGRATED FRAMEWORK

PRINCIPLE 4 – ENABLING A HOLISTIC APPROACH

PRINCIPLE 5 – SEPARATING GOVERNANCE & MANAGEMENT
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
PRINCIPLE 1
MEETING STAKEHOLDER NEEDS

• **Stakeholder Needs are influenced by:**
  A number of drivers:
  – Strategy Changes
  – Changing Business (Mission) & Regulatory Environment
  – Technology Evolutions

• **Stakeholder Needs materialize in:**
  Expectations, concerns, or requirements that support one or more of three governance objectives which together comprise “Value”:
  – Benefits Realization
  – Risk Optimization
  – Resource Optimization
PRINCIPLE 1
MEETING STAKEHOLDER NEEDS

Goals Cascade:

• Provides the link between stakeholder needs and practical goals by translating these into increasing levels of detail and specificity:
  – Drivers
    – Stakeholder Needs
      – Enterprise Goals
        – IT related Goals
          – Enabler Goals (e.g. process goals)

• Allows setting specific goals at every level of the enterprise in support of the overall goals and stakeholder requirements
Goals Cascade

Stakeholder Drivers
(Environement, Technology Evolution, …)

Influence

Stakeholder Needs

Benefits Realisation
Risk Optimisation
Resource Optimisation

Cascade to

Enterprise Goals

Cascade to

IT-related Goals

Cascade to

Enabler Goals

Appendix D
Figure 5
Appendix B
Figure 6
Appendix C

Slide 32
Slide 30
Slide 47
Slide 34
Slides 48 – 49
PRINCIPLE 2
COVERING ENTERPRISE END-TO-END

• End-to-End coverage is achieved by identifying all stakeholder needs and determining how they link to governance & management decisions & activities

• Addresses governance and management of information technology from an enterprise-wide, end-to-end perspective

• This relates to the enterprise objectives of benefits realization, risk optimization, and resource optimization – i.e. “Value”
Stakeholder Needs

Maintain Our Focus

As service providers to our stakeholders we must remember that Enterprise goals are a proxy for Stakeholder Needs

How does IT Governance serve our customers?

From a stakeholders point of view it is valuable to understand how their needs relate to Enterprise & IT-related goals
# Stakeholder Needs

**Internal Stakeholders**
- Board
- CEO
- Chief financial officer (CFO)
- CIO
- Chief risk officer (CRO)
- Business executives
- Business process owners
- Business managers
- Risk managers
- Security managers
- Service managers
- Human resource (HR) managers
- Internal audit
- Privacy officers
- IT users
- IT managers
- Etc.

**Internal Stakeholder Questions**
- How do I get value from the use of IT? Are end users satisfied with the quality of the IT service?
- How do I manage performance of IT?
- How can I best exploit new technology for new strategic opportunities?
- How do I best build and structure my IT department?
- How dependent am I on external providers? How well are IT outsourcing agreements being managed?
- How do I obtain assurance over external providers?
- What are the (control) requirements for information?
- Did I address all IT-related risk?
- Am I running an efficient and resilient IT operation?
- How do I control the cost of IT? How do I use IT resources in the most effective and efficient manner?
- What are the most effective and efficient sourcing options?
- Do I have enough people for IT? How do I develop and maintain their skills, and how do I manage their performance?
- How do I get assurance over IT?
- Is the information I am processing well secured?
- How do I improve business agility through a more flexible IT environment?
- Do IT projects fail to deliver what they promised—and if so, why? Is IT standing in the way of executing the business strategy?
- How critical is IT to sustaining the enterprise? What do I do if IT is not available?
- What concrete vital primary business processes are dependent on IT, and what are the requirements of business processes?
- What has been the average overrun of the IT operational budgets? How often and how much do IT projects go over budget?
- How much of the IT effort goes to fighting fires rather than to enabling business improvements?
- Are sufficient IT resources and infrastructure available to meet required enterprise strategic objectives?
- How long does it take to make major IT decisions?
- Are the total IT efforts and investments transparent?
- Does IT support the enterprise in complying with regulations and service levels? How do I know whether I am compliant with all applicable regulations?

**External Stakeholders**
- Business partners
- Suppliers
- Shareholders
- Regulators/government
- External users
- Customers
- Standardisation organisations
- External auditors
- Consultants
- Etc.

**External Stakeholder Questions**
- How do I know my business partner’s operations are secure and reliable?
- How do I know the enterprise is compliant with applicable rules and regulations?
- How do I know the enterprise is maintaining an effective system of internal control?
- Do business partners have the information chain between them under control?
Enterprise Goals & Metrics

Enterprise Goals (17)
– Enterprise Goals Sample Metrics (54)
Enterprise Goals

1. Stakeholder value of business investments
2. Portfolio of competitive products and services
3. Managed business risks (safeguarding of assets)
4. Compliance with external laws and regulations
5. Financial transparency
6. Customer-oriented service culture
7. Business service continuity and availability
8. Agile responses to a changing business environment
9. Information-based strategic decision making
10. Optimization of service delivery costs
11. Optimization of business process functionality
12. Optimization of business process costs
13. Managed business change programs
14. Operational and staff productivity
15. Compliance with internal policies
16. Skilled and motivated people
17. Product and business innovation culture
## Enterprise Goals Sample Metrics

<table>
<thead>
<tr>
<th>BSC Dimension</th>
<th>Enterprise Goal</th>
<th>Metric</th>
</tr>
</thead>
<tbody>
<tr>
<td>Financial</td>
<td>1. Stakeholder value of business investments</td>
<td>• Percent of investments where value delivered meets stakeholder expectations</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Percent of products and services where expected benefits are realised</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Percent of investments where claimed benefits are met or exceeded</td>
</tr>
<tr>
<td></td>
<td>2. Portfolio of competitive products and services</td>
<td>• Percent of products and services that meet or exceed targets in revenues and/or market share</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Ratio of products and services per life cycle phase</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Percent of products and services that meet or exceed customer satisfaction targets</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Percent of products and services that provide competitive advantage</td>
</tr>
<tr>
<td></td>
<td>3. Managed business risk (safeguarding of assets)</td>
<td>• Percent of critical business objectives and services covered by risk assessment</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Ratio of significant incidents that were not identified in risk assessments vs. total incidents</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Frequency of update of risk profile</td>
</tr>
<tr>
<td></td>
<td>4. Compliance with external laws and regulations</td>
<td>• Cost of regulatory non-compliance, including settlements and fines</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Number of regulatory non-compliance issues causing public comment or negative publicity</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Number of regulatory non-compliance issues relating to contractual agreements with business partners</td>
</tr>
<tr>
<td></td>
<td>5. Financial transparency</td>
<td>• Percent of investment business cases with clearly defined and approved expected costs and benefits</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Percent of products and services with defined and approved operational costs and expected benefits</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Satisfaction survey regarding the transparency, understanding the transparency, under-standing the importance of transparency</td>
</tr>
</tbody>
</table>
### Stakeholder Needs to Enterprise Goals

<table>
<thead>
<tr>
<th>Stakeholder Needs</th>
<th>1.</th>
<th>2.</th>
<th>3.</th>
<th>4.</th>
<th>5.</th>
<th>6.</th>
<th>7.</th>
<th>8.</th>
<th>9.</th>
<th>10.</th>
<th>11.</th>
<th>12.</th>
<th>13.</th>
<th>14.</th>
<th>15.</th>
<th>16.</th>
<th>17.</th>
</tr>
</thead>
<tbody>
<tr>
<td>How do I get value from the use of IT? Are end users satisfied with the quality of the IT service?</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>How do I manage performance of IT?</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>How can I best exploit new technology for new strategic opportunities?</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>How do I best build and structure my IT department?</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>How dependent am I on external providers? How well are IT outsourcing agreements being managed? How do I obtain assurance over external providers?</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>What are the (control) requirements for information?</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Did I address all IT-related risk?</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Am I running an efficient and resilient IT operation?</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>How do I control the cost of IT? How do I use IT resources in the most effective and efficient manner? What are the most effective and efficient sourcing options?</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Do I have...</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
IT Related Goals & Metrics

IT Related Goals (17)

– IT Related Goals Sample Metrics (59)
IT Related Goals

1. Alignment of IT and business strategy
2. IT compliance and support for business compliance with external laws and regulations
3. Commitment of executive management for making IT-related decisions
4. Managed IT-related business risks
5. Realized benefits from IT-enabled investments and services portfolio
6. Transparency of IT costs, benefits, and risk
7. Delivery of IT services in line with business requirements
8. Adequate use of applications, information, and technology solutions
9. IT agility
10. Security of information, processing infrastructure, and applications
11. Optimization of IT assets, resources, and capabilities
12. Enablement and support of business processes by integrating applications and technology into business processes
13. Delivery of programs delivering benefits, on time, on budget, and meeting requirements and quality standards
14. Availability of reliable and useful information for decision making
15. IT compliance with internal policies
16. Competent and motivated business and IT personnel
17. Knowledge, expertise, and initiatives for business innovation
## IT Related Goals Sample Metrics

<table>
<thead>
<tr>
<th>BSC Dimension</th>
<th>IT-related Goal</th>
<th>Metric</th>
</tr>
</thead>
</table>
| Internal      | 09 IT agility  | • Level of satisfaction of business executives with IT’s responsiveness to new requirements  
• Number of critical business processes supported by up-to-date infrastructure and applications  
• Average time to turn strategic IT objectives into an agreed-on and approved initiative |
|               | 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   | • Number of incidents related to non-compliance to policy  
• Percent of stakeholders who understand IT policies and procedures |

COBIT 5 Process Taxonomy

Domains (5)

- **Processes** (37)
  - 129 Process **Goals**
  - 265 Related **Metrics**

- **Practices** (210)
  - RACI Chart (Detailed Role Based Assignments)

- **Activities** (1,115)
## COBIT 5 Process Taxonomy Examples

<table>
<thead>
<tr>
<th>Domains</th>
<th>Processes</th>
<th>Process Goals</th>
<th>Related Metrics</th>
<th>Practices</th>
<th>Activities</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>37</td>
<td>129</td>
<td>265</td>
<td>210</td>
<td>1,115</td>
</tr>
<tr>
<td>• Evaluate, Direct and Monitor</td>
<td>Example:</td>
<td>Example:</td>
<td>Example:</td>
<td>Example:</td>
<td>Example:</td>
</tr>
<tr>
<td>• Align, Plan and Organize</td>
<td>• Ensure Governance Framework Setting and Maintenance</td>
<td>• The IT strategy is cost-effective, appropriate, realistic, achievable, enterprise-focused and balanced</td>
<td>• Percent of projects in the IT project portfolio that can be directly traced back to the IT strategy</td>
<td>• Evaluate the governance system</td>
<td>• Track compliance with policies and procedures</td>
</tr>
<tr>
<td>• Build, Acquire and Implement</td>
<td>• Manage Enterprise Architecture</td>
<td>• IT is a value driver for the enterprise</td>
<td>• a) Percent total changes that are emergency fixes</td>
<td>• Evaluate, prioritize, and authorize change requests</td>
<td>• Review the portfolio on a regular basis to identify and exploit synergies, eliminate duplication between programs, and identify and mitigate risk</td>
</tr>
<tr>
<td>• Deliver, Service and Support</td>
<td>• Manage Budget and Costs</td>
<td>• Program business cases are evaluated and prioritized before funds are allocated</td>
<td>• b) Number of emergency changes not authorized after the change</td>
<td>• Review, maintain, and improve the continuity plan</td>
<td>• Define the required and currently available skills and competencies of internal and external resources to achieve enterprise, IT, and process goals</td>
</tr>
<tr>
<td>• Monitor, Evaluate and Assess</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
COBIT 5 Processes
Domain - Evaluate, Direct, & Monitor

1. EDM01: Ensure Governance Framework Setting and Maintenance
2. EDM02: Ensure Benefits Delivery
3. EDM03: Ensure Risk Optimization
4. EDM04: Ensure Resource Optimization
5. EDM05: Ensure Stakeholder Transparency
COBIT 5 Processes

Domain - Align, Plan, & Organize

6. APO01: Manage the IT Management Framework
7. APO02: Manage Strategy
8. APO03: Manage Enterprise Architecture
9. APO04: Manage Innovation
10. APO05: Manage Portfolio
11. APO06: Manage Budget and Costs
12. APO07: Manage Human Resources
13. APO08: Manage Relationships
14. APO09: Manage Service Agreements
15. APO10: Manage Suppliers
16. APO11: Manage Quality
17. APO12: Manage Risk
18. APO13: Manage Security
COBIT 5 Processes
Domain - Build, Acquire, & Implement

19. BAI01: Manage Programs and Projects
20. BAI02: Manage Requirements Definition
21. BAI03: Manage Solutions Identification and Build
22. BAI04: Manage Availability and Capacity
23. BAI05: Enable Organizational Change Enablement
24. BAI06: Manage Changes
25. BAI07: Manage Change Acceptance and Transitioning
26. BAI08: Manage Knowledge
27. BAI09: Manage Assets
28. BAI10: Manage Configuration
COBIT 5 Processes
Domain - Deliver, Service, & Support

29. DSS01: Manage Operations
30. DSS02: Manage Service Requests and Incidents
31. DSS03: Manage Problems
32. DSS04: Manage Continuity
33. DSS05: Manage Security Services
34. DSS06: Manage Business Process Controls
COBIT 5 Processes

Domain - Monitor, Evaluate, & Assess

35. MEA01: Monitor, Evaluate and Assess Performance and Conformance
36. MEA02: Monitor, Evaluate and Assess the System of Internal Control
37. MEA03: Monitor, Evaluate and Assess Compliance with External Requirements
# Process Model

<table>
<thead>
<tr>
<th>Identifier &amp; Name</th>
<th>Area &amp; Domain</th>
</tr>
</thead>
<tbody>
<tr>
<td>BAI06 Manage Changes</td>
<td>Area: Management Domain: Build, Acquire and Implement</td>
</tr>
</tbody>
</table>

## Process Description
Manage all changes in a controlled manner, including standard changes and emergency maintenance relating to business processes, applications and infrastructure. This includes change standards and procedures, impact assessment, prioritisation and authorisation, emergency changes, tracking, reporting, closure and documentation.

## Process Purpose Statement
Enable fast and reliable delivery of change to the business and mitigation of the risk of negatively impacting the stability or integrity of the changed environment.

## The process supports the achievement of a set of primary IT-related goals:

<table>
<thead>
<tr>
<th>IT-related Goal</th>
<th>Related Metrics</th>
</tr>
</thead>
<tbody>
<tr>
<td>04 Managed IT-related business risk</td>
<td>• Percent of critical business processes, IT services and IT-enabled business programmes covered by risk assessment</td>
</tr>
<tr>
<td></td>
<td>• Number of significant IT-related incidents that were not identified in risk assessment</td>
</tr>
<tr>
<td></td>
<td>• Percent of enterprise risk assessments including IT-related risk</td>
</tr>
<tr>
<td></td>
<td>• Frequency of update of risk profile</td>
</tr>
<tr>
<td>07 Delivery of IT services in line with business requirements</td>
<td>• Number of business disruptions due to IT service incidents</td>
</tr>
<tr>
<td></td>
<td>• Percent of business stakeholders satisfied that IT service delivery meets agreed-on service levels</td>
</tr>
<tr>
<td></td>
<td>• Percent of users satisfied with the quality of IT service delivery</td>
</tr>
<tr>
<td>10 Security of information, processing infrastructure and applications</td>
<td>• Number of security incidents causing financial loss, business disruption or public embarrassment</td>
</tr>
<tr>
<td></td>
<td>• Number of IT services with outstanding security requirements</td>
</tr>
<tr>
<td></td>
<td>• Time to grant, change and remove access privileges, compared to agreed-on service levels</td>
</tr>
<tr>
<td></td>
<td>• Frequency of security assessment against latest standards and guidelines</td>
</tr>
</tbody>
</table>

## Goals & Sample Metrics of the Process Itself

<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>
# Process Model - RACI

## RACI Assignments

<table>
<thead>
<tr>
<th>BA06 RACI Chart</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Key Management Practice</strong></td>
</tr>
<tr>
<td>-----------------</td>
</tr>
<tr>
<td><strong>BA06.01</strong> Evaluate, prioritise and authorise change requests.</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td><strong>BA06.02</strong> Manage emergency changes.</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td><strong>BA06.03</strong> Track and report change status.</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td><strong>BA06.04</strong> Close and document the changes.</td>
</tr>
</tbody>
</table>

Practices Supporting the Process
## Practice Model – Practices & Activities

### BA06 Process Practices, Inputs/Outputs and Activities

<table>
<thead>
<tr>
<th>Management Practice</th>
<th>Inputs</th>
<th>Outputs</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>BA06.01</strong> Evaluate, prioritise and authorise change requests.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Evaluate all requests for change to determine the impact on business processes and IT services, and to assess whether change will adversely affect the operational environment and introduce unacceptable risk. Ensure that changes are logged, prioritised, categorised, assessed, authorised, planned and scheduled.</td>
<td>From</td>
<td>Description</td>
</tr>
<tr>
<td>BA03.05</td>
<td>Integrated and configured solution components</td>
<td>Impact assessments</td>
</tr>
<tr>
<td>DSS02.03</td>
<td>Approved service requests</td>
<td>Approved requests for change</td>
</tr>
<tr>
<td>DSS03.03</td>
<td>Proposed solutions to known errors</td>
<td></td>
</tr>
<tr>
<td>DSS03.05</td>
<td>Identified sustainable solutions</td>
<td>Change plan and schedule</td>
</tr>
<tr>
<td>DSS04.08</td>
<td>Approved changes to the plans</td>
<td></td>
</tr>
<tr>
<td>DSS06.01</td>
<td>Root cause analyses and recommendations</td>
<td></td>
</tr>
</tbody>
</table>

### Activities

1. Use formal change requests to enable business process owners and IT to request changes to business process, infrastructure, systems or applications. Make sure that all such changes arise only through the change request management process.

2. Categorise all requested changes (e.g., business process, infrastructure, operating systems, networks, application systems, purchased/packaged application software) and relate affected configuration items.

3. Prioritise all requested changes based on the business and technical requirements, resources required, and the legal, regulatory and contractual reasons for the requested change.

4. Plan and evaluate all requests in a structured fashion. Include an impact analysis on business process, infrastructure, systems and applications, business continuity plans (BCPs) and service providers to ensure that all affected components have been identified. Assess the likelihood of adversely affecting the operational environment and the risk of implementing the change. Consider security, legal, contractual and compliance implications of the requested change. Consider also inter-dependencies amongst changes. Involve business process owners in the assessment process, as appropriate.

5. Formally approve each change by business process owners, service managers and IT technical stakeholders, as appropriate. Changes that are low-risk and relatively frequent should be pre-approved as standard changes.

6. Plan and schedule all approved changes, ensuring all serviced impacted, such as third-party outsourced business services, are scheduled for planned downtime, maintenance or shared service windows.

7. Communicate all changes to business and IT stakeholders to enable them to plan for the change and to be prepared for its impact.
### Enterprise Goals Relation to Governance Objectives

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

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

*Foundational IT Governance Framework*
## IT Related Goals to COBIT 5 Processes

<table>
<thead>
<tr>
<th>COBIT 5 Process</th>
<th>Financial</th>
<th>Customer</th>
<th>Internal</th>
<th>Learning and Growth</th>
</tr>
</thead>
<tbody>
<tr>
<td>EDM01 Ensure Governance Framework Setting and Maintenance</td>
<td>P S P S S S P</td>
<td>S S S S S S S S S</td>
<td></td>
<td></td>
</tr>
<tr>
<td>EDM02 Ensure Benefits Delivery</td>
<td>P S P S P P S</td>
<td>S S S S S S S S S</td>
<td></td>
<td></td>
</tr>
<tr>
<td>EDM03 Ensure Risk Optimisation</td>
<td>S S S P P S S</td>
<td>P S S S S S P S</td>
<td></td>
<td></td>
</tr>
<tr>
<td>EDM04 Ensure Resource Optimisation</td>
<td>S S S S S S S</td>
<td>P P S S S S</td>
<td></td>
<td></td>
</tr>
<tr>
<td>EDM05 Ensure Stakeholder Transparency</td>
<td>S S P S S S</td>
<td></td>
<td>S S S S S</td>
<td></td>
</tr>
<tr>
<td>APO01 Manage the IT Management Framework</td>
<td>P P S S S P</td>
<td>S P S S S S S P</td>
<td></td>
<td></td>
</tr>
<tr>
<td>APO02 Manage Strategy</td>
<td>P S S S S P S</td>
<td>S S S S S S S S</td>
<td></td>
<td></td>
</tr>
<tr>
<td>APO03 Manage Enterprise Architecture</td>
<td>P S S S S S S</td>
<td></td>
<td>S S S S S</td>
<td></td>
</tr>
<tr>
<td>APO04 Manage Innovation</td>
<td>S S S P S S S</td>
<td>P S P S S S</td>
<td></td>
<td></td>
</tr>
<tr>
<td>APO05 Manage Portfolio</td>
<td>P S S P S S S</td>
<td>S S P S S S</td>
<td></td>
<td></td>
</tr>
<tr>
<td>APO06 Manage Budget and Costs</td>
<td>S S S P S S S</td>
<td>S S P S S S</td>
<td></td>
<td></td>
</tr>
<tr>
<td>APO07 Manage Human Resources</td>
<td>P S S S S S S</td>
<td></td>
<td>S S P S S S</td>
<td></td>
</tr>
<tr>
<td>APO08 Manage Relationships</td>
<td>P S S S S P S</td>
<td></td>
<td>S P S S S S</td>
<td></td>
</tr>
<tr>
<td>APO09 Manage Service Agreements</td>
<td>S S S S P S S</td>
<td></td>
<td>S S S S S S</td>
<td></td>
</tr>
<tr>
<td>APO10 Manage Suppliers</td>
<td>S P S S P S S</td>
<td></td>
<td>S S S S S S</td>
<td></td>
</tr>
<tr>
<td>APO11 Manage Quality</td>
<td>S S S S P S S</td>
<td></td>
<td>S S S S S S</td>
<td></td>
</tr>
<tr>
<td>APO12 Manage Risk</td>
<td>P P S S S P</td>
<td></td>
<td>S P S S S S</td>
<td></td>
</tr>
<tr>
<td>APO13 Manage Security</td>
<td>P S S S S P</td>
<td></td>
<td>S S S S S S</td>
<td></td>
</tr>
</tbody>
</table>

**COBIT 5 Process Key**
- **P**: Primary
- **S**: Supporting
<table>
<thead>
<tr>
<th>IT-related Goal</th>
<th>01</th>
<th>02</th>
<th>03</th>
<th>04</th>
<th>05</th>
<th>06</th>
<th>07</th>
<th>08</th>
<th>09</th>
<th>10</th>
<th>11</th>
<th>12</th>
<th>13</th>
<th>14</th>
<th>15</th>
<th>16</th>
<th>17</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>IT-Related Goals to COBIT 5 Processes</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**COBIT 5 Process**

| BA01 | Manage Programmes and Projects | P | S | P | P | S | S | S | S | S | S | S | S | S | S | S | S |
| BA02 | Manage Requirements Definition | P | S | S | S | S | S | S | S | S | S | S | S | S | S | S | S |
| BA03 | Manage Solutions Identification and Build | S | S | S | S | P | S | S | S | S | S | S | S | S | S | S | S |
| BA04 | Manage Availability and Capacity | S | S | S | P | S | S | S | P | S | S | S | S | S | S | S | S |
| BA05 | Manage Organisational Change Enablement | S | S | S | S | S | P | S | S | S | S | S | S | S | S | S | S |
| BA06 | Manage Changes | S | P | S | S | S | S | P | S | S | S | S | S | S | S | S | S |
| BA07 | Manage Changes Acceptance and Transitioning | S | S | S | S | S | S | S | S | S | S | S | S | S | S | S | S |
| BA08 | Manage Knowledge | S | S | S | S | S | S | S | S | S | S | S | S | S | S | S | S |
| BA09 | Manage Assets | S | S | S | S | S | S | S | S | S | S | S | S | S | S | S | S |
| BA10 | Manage Configuration | P | S | S | S | S | S | S | S | S | S | S | S | S | S | S | S |
| DSS01 | Manage Operations | S | P | S | S | S | S | S | S | S | S | S | S | S | S | S | S |
| DSS02 | Manage Service Requests and Incidents | P | S | S | S | S | S | S | S | S | S | S | S | S | S | S | S |
| DSS03 | Manage Problems | S | P | S | S | S | S | S | S | S | S | S | S | S | S | S | S |
| DSS04 | Manage Continuity | S | S | S | S | S | S | S | S | S | S | S | S | S | S | S | S |
| DSS05 | Manage Security Services | S | P | S | S | S | S | S | S | S | S | S | S | S | S | S | S |
| DSS06 | Manage Business Process Controls | S | P | S | S | S | S | S | S | S | S | S | S | S | S | S | S |
| MEA01 | Monitor, Evaluate and Assess Performance and Conformance | S | S | S | S | S | S | S | S | S | S | S | S | S | S | S | S |
| MEA02 | Monitor, Evaluate and Assess the System of Internal Control | P | P | S | S | S | S | S | S | S | S | S | S | S | S | S | S |
| MEA03 | Monitor, Evaluate and Assess Compliance With External Requirements | P | P | S | S | S | S | S | S | S | S | S | S | S | S | S | S |
PRINCIPLE 3
APPLYING A SINGLE INTEGRATED FRAMEWORK

COBIT 5 is an Integrated Framework:

• Integrates existing ISACA guidance on governance and management of enterprise IT
• Aligns with current relevant standards & frameworks
• Simple architecture for structuring a consistent body of guidance materials
COBIT 5 Architecture

Enablers:
- Principles, Policies, & Frameworks
- Processes
- Organizational Structures
- Cultures, Ethics, Behaviors
- Information
- Services Infrastructure Applications
- People, Skills, & Competencies
PRINCIPLE 4
ENABLING A HOLISTIC APPROACH

• **Purpose** of enablers is to implement an effective & efficient governance and management system for enterprise IT

• **Defined as** anything that facilitates achievement of enterprise governance objectives, including resources such as information and people

• **IT-related goals define what enablers should achieve**

• **Seven categories:**
  – Principles, Policies, & Frameworks
  – Processes
  – Organizational Structures
  – Culture, Ethics, & Behavior
  – Information
  – Services Infrastructure Applications
  – People, Skills, & Competences
COBIT 5 Enablers

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

1. Principles, Policies and Frameworks

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

Resources
Generic Enabler Model

- A governance system is a complex interaction amongst all enablers
- Having a simple, structured, and uniform way to analyze each enabler can facilitate adoption and successful integration
- Enablers all have certain elements in common therefore a generic model standardizes conceptualization
Enabler Dimensions

• Stakeholders —
  – Can be internal or external to the organization, and have their own interests and needs, which can be conflicting
  – Stakeholders needs translate to enterprise goals, then IT-related goals, and ultimately to enabler goals

• Goals —
  – Enablers provide value by achieving multiple goals
  – Properties of goals associated with performance metrics are:
    • Outcomes expected of the enabler (associated with Lag indicators)
    • Operation of the enabler itself (associated with Lead indicators)
  – Qualities associated with goals are categorized as follows:
    • Intrinsic quality — The extent to which enablers work accurately, objectively, and provide accurate, objective and reputable results
    • Contextual quality — The extent to which enablers and their outcomes are fit for purpose given the context in which they operate
    • Access and Security — The extent to which enablers and their outcomes are accessible and secured
Enabler Dimensions

• **Life Cycle** —
  Phases consist of:
  – Plan
  – Design
  – Build/acquire & implement
  – Use/operate
  – Evaluate/monitor
  – Update/dispose

• **Good Practice** —
  – Guidance as to how best implement the enabler
  – Good Practice can be:
    • Internal – provided within COBIT 5
    • External – provided outside COBIT 5
  – Work Products (inputs/outputs)
Enabler Performance Management

• To manage performance of enablers, metrics associated with the following enabler dimensions must be developed, implemented, and monitored:
  – **Stakeholders**: Are stakeholder needs addressed?
  – **Goals**: Are enabler goals achieved?
  – **Life Cycle**: Is the enabler life cycle managed?
  – **Good Practices**: Are good practices applied?

• **Metrics** associated with enablers measure either:
  – **Achievement of goals** (lag indicators)
    • Stakeholder requirements met
    • Enabler goals achieved
  – **Application of Good Practice** (lead indicators)
    • Life cycle managed
    • Good practices applied
Principles, Policies, & Frameworks

Additional information available in “Appendix G” of the COBIT 5 Framework
Additional information available in “Appendix G” of the COBIT 5 Framework
Organizational Structures

Additional information available in “Appendix G” of the COBIT 5 Framework
Culture & Behavior

Additional information available in “Appendix G” of the COBIT 5 Framework
Information

Additional information available in “Appendix G” of the COBIT 5 Framework
Services, Infrastructure, & Capabilities

Additional information available in “Appendix G” of the COBIT 5 Framework
People, Skills, & Competencies

Additional information available in “Appendix G” of the COBIT 5 Framework
## Skill Categories

<table>
<thead>
<tr>
<th>Process Domain</th>
<th>Examples of Skill Categories</th>
</tr>
</thead>
<tbody>
<tr>
<td>Evaluate, Direct and Monitor (EDM)</td>
<td>• Governance of enterprise IT</td>
</tr>
<tr>
<td>Align, Plan and Organise (APO)</td>
<td>• IT policy formulation</td>
</tr>
<tr>
<td></td>
<td>• IT strategy</td>
</tr>
<tr>
<td></td>
<td>• Enterprise architecture</td>
</tr>
<tr>
<td></td>
<td>• Innovation</td>
</tr>
<tr>
<td></td>
<td>• Financial management</td>
</tr>
<tr>
<td></td>
<td>• Portfolio management</td>
</tr>
<tr>
<td>Build, Acquire and Implement (BAI)</td>
<td>• Business analysis</td>
</tr>
<tr>
<td></td>
<td>• Project management</td>
</tr>
<tr>
<td></td>
<td>• Usability evaluation</td>
</tr>
<tr>
<td></td>
<td>• Requirements definition and management</td>
</tr>
<tr>
<td></td>
<td>• Programming</td>
</tr>
<tr>
<td></td>
<td>• System ergonomics</td>
</tr>
<tr>
<td></td>
<td>• Software decommissioning</td>
</tr>
<tr>
<td></td>
<td>• Capacity management</td>
</tr>
<tr>
<td>Deliver, Service and Support (DSS)</td>
<td>• Availability management</td>
</tr>
<tr>
<td></td>
<td>• Problem management</td>
</tr>
<tr>
<td></td>
<td>• Service desk and incident management</td>
</tr>
<tr>
<td></td>
<td>• Security administration</td>
</tr>
<tr>
<td></td>
<td>• IT operations</td>
</tr>
<tr>
<td></td>
<td>• Database administration</td>
</tr>
<tr>
<td>Monitor, Evaluate and Assess (MEA)</td>
<td>• Compliance review</td>
</tr>
<tr>
<td></td>
<td>• Performance monitoring</td>
</tr>
<tr>
<td></td>
<td>• Controls audit</td>
</tr>
</tbody>
</table>
COBIT 5 framework makes a clear distinction between Governance and Management

- Different types of activities
- Require different organizational structures
- Serve different purposes
Governance & Management Processes
Governance

• Ensures that enterprise objectives are achieved by evaluating stakeholder needs, conditions, and options
• Sets direction through prioritization and decision making
• Monitors performance, compliance, and progress against the agreed upon direction and objectives

Management

• Plans, builds, runs, & monitors activities in alignment with the direction set by the governance body to achieve the enterprise objectives
IT Governance

Integration of Governance & Management

- Distinction between Governance & Management often misunderstood
- Effective integration of these two elements is critical for successful governance of any IT enterprise or organization
- IT Governance is NOT responsible for “rendering” IT infrastructure
- IT Governance IS responsible for “oversight of management processes” that render IT infrastructure
Roles, Activities, & Relationships
PRINCIPLE 5
SEPERRATING GOVERNANCE & MANAGEMENT
Process Reference Model
Divides governance and management processes into two primary domains:

- **Governance** (1 Domain, 5 Processes)
  Within each process, evaluate, direct, and monitor practices are defined.

- **Management** (4 Domains, 32 Processes)
  In line with responsibility areas of plan, build, run, and monitor, provide an end-to-end coverage of IT Management.

The processes cover the full spectrum of business and IT activities related to governance and management of enterprise IT thus making the process model truly enterprise-wide
Agenda

• IT Governance Defined
• Foundational Enterprise IT Governance
  – What is COBIT / COBIT 5?
  – COBIT 5 Objectives
  – COBIT 5 Framework
  – COBIT 5 Benefits
• COBIT 5 Principles
  – Principle 1 – Meeting Stakeholder Needs
  – Principle 2 – Covering the Enterprise End-To-End
  – Principle 3 – Applying a Single Integrated Framework
  – Principle 4 – Enabling a Holistic Approach
  – Principle 5 – Separating Governance & Management
• COBIT Process Capability Model
• Implementation Guidance
• Summary & Recommendations
• Questions?
• References
Based upon ISO/IEC 15504 Software Engineering — Process Assessment standard while incorporating more granular elements. It provides:

- A means to measure the performance of any Governance or Management process
- Identification of areas for improvement

The model is documented in ISACA publication COBIT® Process Assessment Model (PAM): Using COBIT® 4.1
Process Capability Model

Six Process Capability Levels:

• **0. Incomplete**— Process not implemented or fails to achieve its purpose. Little or no evidence of any systematic achievement of the process purpose exist.

• **1. Performed (one attribute)** — The implemented process achieves its process purpose. This requires the process performance attribute to be largely achieved which means the process is being successfully performed.

• **2. Managed (two attributes)** — Process is now implemented in a managed fashion (planned, monitored, and adjusted) and its work products are appropriately established, controlled, and maintained.

• **3. Established (two attributes)** — Process is now implemented using a defined process that is capable of achieving its intended outcomes.

• **4. Predictable (two attributes)** — Process now operates within defined limits to achieve its intended outcomes.

• **5. Optimizing (two attributes)** — Process is continuously improved to meet relevant current and projected business goals.
Process Capability Model
# Process Capability Model Comparison

<table>
<thead>
<tr>
<th>Commonly Recognized Maturity 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>
</tr>
</thead>
<tbody>
<tr>
<td>5. Optimized</td>
<td>5. Optimized</td>
<td>Continuously improved to meet relevant current and projected enterprise goals</td>
</tr>
<tr>
<td>4. Managed</td>
<td>4. Predictable</td>
<td>Operates within defined limits to achieve its process outcomes</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>
</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>
</tr>
<tr>
<td>2. Under Development</td>
<td>1. Performed</td>
<td>Process achieves its process purpose</td>
</tr>
<tr>
<td>1. Initial Capability</td>
<td>1. Performed</td>
<td></td>
</tr>
<tr>
<td>0. Non-existent</td>
<td>0. Incomplete</td>
<td>Not implemented or little or no evidence of any systematic achievement of the process purpose</td>
</tr>
</tbody>
</table>
Observations:

• The ISO model collapses traditional capability Levels 1 & 2 (Initial Capability & Under Development) under 15504 Level 1 (Performed)

• This produces some loss of granularity through the initial integration and development phases

• The result is a loss of detail relative to tracking, reporting, and management of the IT Governance development and implementation process
Process Capability Assessment

The ISO 15504-based assessment approach facilitates the following objectives:

- Provide a measurement scale and associated guidance to assess the nine capability attributes for each process
- Enables management to benchmark process capability so they can measure and monitor current capabilities
- Enable ‘as-is’ and ‘to-be’ process capability status and gap analysis to support management investment decisions with regard to process improvement
- Provide information required for process capability trend analysis
Process Capability Assessment

The ISO/IEC 15504 process capability assessment approach defines information required for assessment in the ‘Process Reference Model’ as follows:

- **Process description** with purpose statements
- **Base practices**, which are the equivalent of process governance or management practices in COBIT 5 terms
- **Work products**, which are the equivalent of inputs and outputs in COBIT 5 terms
Process Capability Assessment Scale

- **N (Not achieved)** — There is little or no evidence of achievement of the defined attribute in the assessed process. (0 to 15 percent achievement)

- **P (Partially achieved)** — There is some evidence of an approach to, and some achievement of, the defined attribute in the assessed process. Some aspects of achievement of the attribute may be unpredictable. (15 to 50 percent achievement)

- **L (Largely achieved)** — There is evidence of a systematic approach to, and significant achievement of, the defined attribute in the assessed process. Some weakness related to this attribute may exist in the assessed process. (50 to 85 percent achievement)

- **F (Fully achieved)** — There is evidence of a complete and systematic approach to, and full achievement of, the defined attribute in the assessed process. No significant weaknesses related to this attribute exist in the assessed process. (85 to 100 percent achievement)
Process Capability Attribute

• Based on ISO/IEC 15504 Process Assessment Model

• The model makes a distinction between:
  – Basic Capability Level (1)
    Indicates that a process is generally achieving its stated goals and that good practices are, to a large extent, applied. These attributes are unique for each process.
  – Advanced Capability Levels (2 through 5)
    Indicates increasing levels of sophistication, providing greater efficiency, formalization, control, optimization, etc. For each level multiple attributes must be achieved. These attributes are generic for all processes.
Process Capability Assessment Procedure

Capability Level 1 Assessment:

1. **Assess the process outcomes** as they are documented in the detailed process descriptions and assign an ISO/IEC 15504 rating to each objective.

2. **Assess the base practices** (governance or management) using the same rating scale.

3. **Assess the work products** to determine the extent to which a specific attribute has been achieved.

Capability Levels 2-5 Assessment:

ISO/IEC 15504 provides generic practices & descriptions for each of the remaining capability levels.
COBIT 4.1 PAM Example

Purpose

Process Outcomes

Base Practices

Work Products
  - Inputs
  - Outputs
## COBIT 5 PAM Example

### Description

**Process Description**
Manage all changes in a controlled manner, including standard changes and emergency maintenance relating to business processes, applications and infrastructure. This includes change standards and procedures, impact assessment, prioritisation and authorisation, emergency changes, tracking, reporting, closure and documentation.

### Purpose

**Process Purpose Statement**
Enable fast and reliable delivery of change to the business and mitigation of the risk of negatively impacting the stability or integrity of the changed environment.

The process supports the achievement of a set of primary IT-related goals:

<table>
<thead>
<tr>
<th>IT-related Goal</th>
<th>Related Metrics</th>
</tr>
</thead>
<tbody>
<tr>
<td>04 Managed IT-related business risk</td>
<td>• Percent of critical business processes, IT services and IT-enabled business programmes covered by risk assessment</td>
</tr>
<tr>
<td></td>
<td>• Number of significant IT-related incidents that were not identified in risk assessment</td>
</tr>
<tr>
<td></td>
<td>• Percent of enterprise risk assessments including IT-related risk</td>
</tr>
<tr>
<td></td>
<td>• Frequency of update of risk profile</td>
</tr>
<tr>
<td>07 Delivery of IT services in line with business requirements</td>
<td>• Number of business disruptions due to IT service incidents</td>
</tr>
<tr>
<td></td>
<td>• Percent of business stakeholders satisfied that IT service delivery meets agreed-on service levels</td>
</tr>
<tr>
<td></td>
<td>• Percent of users satisfied with the quality of IT service delivery</td>
</tr>
<tr>
<td>10 Security of information, processing infrastructure and applications</td>
<td>• Number of security incidents causing financial loss, business disruption or public embarrassment</td>
</tr>
<tr>
<td></td>
<td>• Number of IT services with outstanding security requirements</td>
</tr>
<tr>
<td></td>
<td>• Time to grant, change and remove access privileges, compared to agreed-on service levels</td>
</tr>
<tr>
<td></td>
<td>• Frequency of security assessment against latest standards and guidelines</td>
</tr>
</tbody>
</table>

### Goals & Sample Metrics of the Process Itself

#### Process Goals and Metrics

<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>2. Impact assessments reveal the effect of the change on all affected components.</td>
<td>• Reduced time and effort required to make changes</td>
</tr>
<tr>
<td>3. All emergency changes are reviewed and authorised after the change.</td>
<td>• Number and age of backlogged change requests</td>
</tr>
<tr>
<td>4. Key stakeholders are kept informed of all aspects of the change.</td>
<td>• Percent of unsuccessful changes due to inadequate impact assessments</td>
</tr>
<tr>
<td></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></td>
<td>• Stakeholder feedback ratings on satisfaction with communications</td>
</tr>
</tbody>
</table>
## COBIT 5 PAM Example

### Inputs

<table>
<thead>
<tr>
<th>Practice Description</th>
<th>From</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>BA106.01 Evaluate, prioritise and authorise change requests.</td>
<td>BA103.05</td>
<td>Integrated and configured solution components</td>
</tr>
<tr>
<td>DSS02.03 Approved service requests</td>
<td>DSS03.03</td>
<td>Proposed solutions to known errors</td>
</tr>
<tr>
<td>DSS03.05 Identified sustainable solutions</td>
<td>DSS04.08</td>
<td>Approved changes to the plans</td>
</tr>
<tr>
<td>DSS06.01 Root cause analyses and recommendations</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Outputs

<table>
<thead>
<tr>
<th>From</th>
<th>Description</th>
<th>To</th>
</tr>
</thead>
<tbody>
<tr>
<td>BA103.05</td>
<td>Impact assessments</td>
<td>Internal</td>
</tr>
<tr>
<td>DSS02.03</td>
<td>Approved requests for change</td>
<td>BA107.01</td>
</tr>
<tr>
<td>DSS03.03</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DSS04.08</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DSS06.01</td>
<td>Change plan and schedule</td>
<td>BA107.01</td>
</tr>
</tbody>
</table>

### Activities

1. Use formal change requests to enable business process owners and IT to request changes to business process, infrastructure, systems or applications. Make sure that all such changes arise only through the change request management process.

2. Categorise all requested changes (e.g., business process, infrastructure, operating systems, networks, application systems, purchased/packaged application software) and relate affected configuration items.

3. Prioritise all requested changes based on the business and technical requirements, resources required, and the legal, regulatory and contractual reasons for the requested change.

4. Plan and evaluate all requests in a structured fashion. Include an impact analysis on business process, infrastructure, systems and applications, business continuity plans (BCPs) and service providers to ensure that all affected components have been identified. Assess the likelihood of adversely affecting the operational environment and the risk of implementing the change. Consider security, legal, contractual and compliance implications of the requested change. Consider also inter-dependencies amongst changes. Involve business process owners in the assessment process, as appropriate.

5. Formally approve each change by business process owners, service managers and IT technical stakeholders, as appropriate. Changes that are low-risk and relatively frequent should be pre-approved as standard changes.

6. Plan and schedule all approved changes.

7. Consider any transitional plans for any other impacted business processes, systems, applications, applications, etc.

---

4/29/12

Foundational IT Governance Framework
### 4.2 LEVEL 2—MANAGED PROCESS

Process Performance is now implemented in a managed fashion (planned, monitored and adjusted) and its work products are appropriately established, controlled and maintained.

**PA 2.1 Performance Management**—A measure of the extent to which the performance of the process is managed. As a result of full achievement of this attribute:

- a. Objectives for the performance of the process are identified.
- b. Performance of the process is planned and monitored.
- c. Performance of the process is adjusted to meet plans.
- d. Responsibilities and authorities for performing the process are defined, assigned and communicated.
- e. Resources and information necessary for performing the process are identified, made available, allocated and used.
- f. Interfaces between the involved parties are managed to ensure effective communication and clear assignment of responsibility.

The GPs and GWPs that provide evidence of achievement of the attribute are shown in figure 7.

<table>
<thead>
<tr>
<th>Result of Full Achievement of the Attribute</th>
<th>Generic Practices (GPs)</th>
<th>Generic Work Products (GWPs)</th>
</tr>
</thead>
<tbody>
<tr>
<td>a. Objectives for the performance of the process are identified.</td>
<td>GP 2.1.1 Identify the objectives for the performance of the process. The performance objectives, scoped together with assumptions and constraints, are defined and communicated.</td>
<td>GWP 1.0 Process documentation should outline the process scope. GWP 2.0 Process plan should provide details of the process performance objectives.</td>
</tr>
<tr>
<td>b. Performance of the process is planned and monitored.</td>
<td>GP 2.1.2 Plan and monitor the performance of the process to fulfil the identified objectives. Basic measures of process performance linked to business objectives are established and monitored. They include key milestones, required activities, estimates and schedules.</td>
<td>GWP 2.0 Process plan should provide details of the process performance objectives. GWP 9.0 Process performance records should provide details of the outcomes. Note: At this level, the record of process performance may be in the form of performance issues.</td>
</tr>
</tbody>
</table>
Generic Work Product Taxonomy

Level 5: Optimising
The process is continuously improved to meet current and projected business goals.

Level 4: Predictable
The process is executed consistently within defined limits.

Level 3: Established
A standard process is defined and used throughout the organisation.

Level 2: Managed
The process is managed and results are specified, controlled and maintained.

Level 1: Performed
The process is performed and achieves its purpose.

GWP 1.0 Process Document
GWP 2.0 Process Plan
GWP 3.0 Quality Plan
GWP 4.0 Quality Records
GWP 5.0 Policies and Standards
GWP 6.0 Performance Improvement Plan
GWP 7.0 Process Measurement Plan
GWP 8.0 Process Control Plan
GWP 9.0 Process Performance Records
# Generic Work Product

<table>
<thead>
<tr>
<th>GWP ID</th>
<th>GWP</th>
<th>Typical Contents</th>
<th>Related GP</th>
<th>Additional Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>Process Documentation</td>
<td>Process name</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Process owner</td>
<td>GP 2.1.4</td>
<td>The person responsible for the design of the process. This includes being responsible for the creation, update and approval of documents (procedures, work instructions/protocols) to support the process.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Process scope</td>
<td>GP 2.1.1</td>
<td>A clear statement of where the process begins and ends</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Process roles</td>
<td>GP 2.1.6</td>
<td>Details of key roles in the process:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• Supplier(s) and inputs</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• Output and customers</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Process map</td>
<td>GP 3.1.2</td>
<td>Generally, in the form of a schematic picture of a process to show the sequential flow of work. In most cases, there will be a map showing flows across a number of processes.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>RACI chart</td>
<td>GP 2.1.4</td>
<td>Identifies who is responsible, accountable, consulted and informed with respect to each of the key activities in the process</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>GP 2.1.6</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Internal control matrix</td>
<td>GP 2.2.2</td>
<td>Matrix showing identified risks within the business process together with identified controls</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Process procedures</td>
<td>GP 3.1.1</td>
<td>A document outlining the activities required to achieve the required process outcomes</td>
</tr>
<tr>
<td>2.0</td>
<td>Process Plan</td>
<td>Process performance objectives</td>
<td>GP 2.1.1</td>
<td>Will vary, depending on the process. However, there should be evidence of targets such as milestones, required activities, estimated output volumes or schedules.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>GP 2.1.2</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Process resourcing</td>
<td>GP 2.1.5</td>
<td>A plan indicating resources and information required to meet the performance required for the process, and information on what resources are to be supplied</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>GP 3.2.4</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Process communication</td>
<td>GP 2.1.4</td>
<td>A plan for the communication required for the process. It should include such things as the:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>GP 2.1.6</td>
<td>• Responsibility for communication</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>GP 3.2.3</td>
<td>• Target audience</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• Timing of communication</td>
</tr>
</tbody>
</table>
Agenda

• IT Governance Defined
• Foundational Enterprise IT Governance
  – What is COBIT / COBIT 5?
  – COBIT 5 Objectives
  – COBIT 5 Framework
  – COBIT 5 Benefits
• COBIT 5 Principles
  – Principle 1 – Meeting Stakeholder Needs
  – Principle 2 – Covering the Enterprise End-To-End
  – Principle 3 – Applying a Single Integrated Framework
  – Principle 4 – Enabling a Holistic Approach
  – Principle 5 – Separating Governance & Management
• COBIT Process Capability Model
• Implementation Guidance
• Summary & Recommendations
• Questions?
• References
Implementation Life Cycle

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?

- Review effectiveness
- Initiate programme
- Define problems and opportunities
- Establish desire to change
- Sustain
- Monitor and evaluate
- Recognise need to act
- Form implementation team

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

- Plan programme
- Identify role players
- Build improvements
- Operate and measure improvements
- Embed new approaches
- Realise benefits
- Execute plan
- Define road map

4/29/12

Foundational IT Governance Framework
Implementation Guidance

COBIT 5 Implementation Guide

• Based on a continual improvement life cycle
• Not intended as a prescriptive approach or complete solution
• Designed as a guide to:
  – Assist in the creation of successful outcomes
  – Leverage best practices
  – Avoid commonly encountered pitfalls
• Supported by an implementation tool kit containing a variety of resources:
  – Self-assessment, measurement, and diagnostic tools
  – Presentations aimed at various audiences
  – Related articles & further explanations
Implementation Guidance

Key factors for successful implementation:

• **Top management providing:**
  – Direction and mandate for the initiative
  – Visible ongoing commitment & support

• Stakeholder commitment & support

• All parties supporting governance and management processes need to understand the business & IT objectives

• Key roles and responsibilities should be defined and assigned

• Ensuring effective communication and enablement of the necessary changes

• **Tailoring ITG framework** as well as other supporting best practices and standards to fit the unique context of the organization

• **Focusing on quick wins and prioritizing** the most beneficial improvements
Implementation Life Cycle Approach

• Provides a way for enterprises to address the complexity and challenges typically encountered during implementation of a Comprehensive IT Governance framework

• Three inter-related life cycle components:
  – Program Management
    Governance of the Process Management program
  – Change Enablement
    Addressing the behavioral and cultural aspects
  – Continual Improvement Life Cycle
    Not a one-off project
Seven Phases of the Implementation Life Cycle

Phase 1 – Initiate Program
• Recognize and agree on need for an implementation or improvement initiative
• Identify current pain points & triggers
• Create a desire to change at executive management levels

Phase 2 – Define Problems & Opportunities
• Leverage framework mappings of enterprise goals, to IT-related goals, to associated IT processes & activities, reconciling organizational ITG equivalents with framework defaults
• Perform high-level analysis to understand and scope the framework towards selecting high-priority areas for assessment
• Define scope of the assessment
• Assess current process capabilities and identify issues or deficiencies
• Define target process capabilities
Seven Phases of the Implementation Life Cycle

Phase 3 – Define Roadmap
- Perform a detailed analysis to identify gaps and potential solutions
- Select & prioritize improvement targets

Phase 4 – Plan Program
- Plan practical solutions by defining projects supported by justifiable business cases
- Develop a change plan for implementation
- Structure large-scale initiatives as multiple iterations of the life cycle

Phase 5 – Execute Plan
- Implement detailed improvement projects, leveraging enterprise program, project, & process management capabilities, standards & practices
- Monitor, measure and report on project progress
- Implement performance management by using the framework’s goals and metrics to define measures and monitoring mechanisms
- Ensure business alignment is achieved and maintained
- Ensure engagement & commitment of top management & stakeholders throughout implementation
Seven Phases of the Implementation Life Cycle

Phase 6 – Realize Benefits
• Ensure sustainable operation of new or improved enablers
• Monitor achievement of expected benefits

Phase 7 – Review Effectiveness
• Review overall initiative success
• Identify further requirements for ITG implementation
• Reinforce need for continual improvement
Agenda

• IT Governance Defined

• Foundational Enterprise IT Governance
  – What is COBIT / COBIT 5?
  – COBIT 5 Objectives
  – COBIT 5 Framework
  – COBIT 5 Benefits

• COBIT 5 Principles
  – Principle 1 – Meeting Stakeholder Needs
  – Principle 2 – Covering the Enterprise End-To-End
  – Principle 3 – Applying a Single Integrated Framework
  – Principle 4 – Enabling a Holistic Approach
  – Principle 5 – Separating Governance & Management

• COBIT Process Capability Model

• Implementation Guidance

• Summary & Recommendations

• Questions?

• References
Summary

• **IT Governance Defined**
  – Distinction between Governance & Management often misunderstood
  – Effective integration of these two elements is critical for successful IT Governance in any enterprise or organization

• **Foundational Enterprise IT Governance**
Understanding of ITG Core Concepts is required to fully grasp the constructs presented herein
Summary

• **COBIT 5 Principles**
  Principles and policies are the vehicle by which governance decisions are institutionalized within the enterprise and therefore are an interaction between governance decisions (direction setting) and management (execution of decisions).

• **COBIT Process Capability Model**
  The COBIT 5 framework presents IT Governance in a process-centric context and therefore provides granular definition of the capability assessment model as applied to the Process enabler.
• Implementation Guidance
  – Optimal value can only be realized from COBIT if it is effectively adopted and adapted to suit each enterprise’s unique environment.
  – Each implementation approach needs to address specific challenges including managing changes to culture and behavior.
Summary

• This has presented an overview of a “Foundational” IT Governance framework

• Based upon ISACA’s Foundational Enterprise IT Governance Framework known as COBIT 5

• This establishes the foundation of comprehensive IT Governance
Recommendations

• Develop a Comprehensive IT Governance framework based upon international best practice frameworks & concepts.

• To include the Fundamental & Foundational frameworks outlined in this and previous presentations.
Questions?
References

• COBIT 5
  – http://www.isaca.org/
• COBIT 5: Enabling Processes
  – http://www.isaca.org/
• COBIT 5 Implementation
  – http://www.isaca.org/
• COBIT 5 Update PowerPoint Presentation
  – http://www.isaca.org/Knowledge-Center/cobit/Pages/COBIT-5-Initiative-Status-Update.aspx
• COBIT Process Assessment Model (PAM) (COBIT 4.1 version)
  – http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/COBIT-Assessment-Program.aspx
• Implementing and Continually Improving IT Governance (ISACA member only)
• ISO/IEC TS 15504:2011 Information technology - Process assessment
• COBIT 5: Enabling Information (in planning)
• COBIT 5 For Information Security (under development, available July 2012)
• COBIT 5 For Risk (in planning)
• COBIT 5 For Assurance (in planning)
• COBIT 5 Online (in planning)
• COBIT Translations (in development)