Selected Guidance From the COBIT 5 Family

These charts and figures are elements of COBIT 5 and its supporting guides. This excerpt is available as a complimentary PDF (www.isaca.org/cobit) and for purchase in hard copy (www.isaca.org/bookstore). It provides an overview of the COBIT 5 guidance, its five principles and seven enablers. We encourage you to share this document with your enterprise leaders, team members, clients and/or consultants.

COBIT enables enterprises to maximise the value and minimise the risk related to information, which has become the currency of the 21st century. COBIT 5 is a comprehensive framework of globally accepted principles, practices, analytical tools and models that can help any enterprise effectively address critical business issues related to the governance and management of information and technology. Additional information is available at www.isaca.org/cobit.
Governance and Management in COBIT 5

**Governance Objective: Value Creation**

- Benefits Realisation
- Risk Optimisation
- Resource Optimisation

Governance Enablers → Governance Scope

Roles, Activities and Relationships

**Key Roles, Activities and Relationships**

Roles, Activities and Relationships

- Owners and Stakeholders
- Governance Body
- Management
- Operations and Execution

- Delegate
- Accountable
- Instruct and Align
- Monitor
- Report

**COBIT 5 Governance and Management Key Areas**

Business Needs

**Governance**

- Evaluate
- Direct
- Monitor

**Management**

- Plan (APO)
- Build (BAI)
- Run (DSS)
- Monitor (MEA)

Source: COBIT 5, figure 8

Source: COBIT 5, figure 9

Source: COBIT 5, figure 15

© 2013 ISACA. All rights reserved.
Two Perspectives on Risk

Risk Function Perspective

The risk function perspective describes how to build and sustain a risk function in the enterprise by using the COBIT 5 enablers.

Risk Management Perspective

The risk management perspective looks at core risk governance and risk management processes and risk scenarios. This perspective describes how risk can be mitigated by using COBIT 5 enablers.

Source: COBIT 5 for Risk, figure 8

Scope of COBIT 5 for Risk

COBIT 5 Framework

COBIT 5: Enabling Processes

Source: COBIT 5 for Risk, figure 10
### Risk Scenario Overview

**The Risk Management Process (AP012)**
- **AP012.01 Collect Data**
- **AP012.02 Analyse Risk**
- **AP012.03 Maintain a Risk Profile**
- **AP012.04 Articulate Risk**
- **AP012.05 Define a Risk Management Action Portfolio**
- **AP012.06 Respond to Risk**

**Top Down**
- **Business Goals**
  - Identify business objectives.
  - Identify scenarios with highest impact on achievement of business objectives.

**Risk Scenarios**
- **Generic Risk Scenarios**
  - Identify hypothetical scenarios.
  - Reduce through high-level analysis.

**Bottom Up**
- **Risk Factors**
  - Internal Environmental Factors
  - External Environmental Factors
  - Risk Management Capabilities
  - IT-related Capabilities

### Risk Scenario Structure

**Event**
- Disclosure
- Interruption
- Modification
- Theft
- Destruction
- Ineffective design
- Ineffective execution
- Rules and regulations
- Inappropriate use

**Asset/Resource**
- People and skills
- Organisational structures
- Process
- Infrastructure (facilities)
- IT infrastructure
- Information
- Applications

**Actor**
- Internal (staff, contractor)
- External (competitor, outsider, business partner, regulator, market)

**Threat Type**
- Malicious
- Accidental
- Error
- Failure
- Nature
- External requirement

**Time**
- Duration
- Timing occurrence (critical or non-critical)
- Detection
- Time lag

Source: COBIT 5 for Risk, figure 34

© 2013 ISACA. All rights reserved.
Supporting Processes for the Risk Function

Processes for Governance of Enterprise IT

Evaluate, Direct and Monitor

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

Align, Plan and Organise

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

Build, Acquire and Implement

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

Deliver, Service and Support

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

Processes for Management of Enterprise IT

This figure highlights the key supporting COBIT 5 processes (shown in dark pink), as well as the other supporting processes (shown in light pink). The core risk processes are shown in light blue.

Source: COBIT 5 for Risk, figure 18
The Seven Phases of the Implementation Life Cycle

1. What are the drivers?
   - Programme management (outer ring)
   - Change enablement (middle ring)
   - Continual improvement life cycle (inner ring)

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?

Summary of the COBIT 5 Process Capability Model

Generic Process Capability Attributes

- Incomplete Process
- Performed Process
- Managed Process
- Established Process
- Predictable Process
- Optimising Process

Source: COBIT 5, figure 17 and COBIT 5 Implementation, figure 6

Source: COBIT 5, figure 19