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 maximize the value and minimize 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
- Governing Body
- Management

- Delegate
- Accountable
- Set Direction
- Monitor
- Instruct and Align
- Report
- Operations and Execution

---

COBIT 5 Governance and Management Key Areas

**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.
### Example Stakeholders for Information Security-related Information (Small/Medium Enterprise)

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Internal: Enterprise</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Board</td>
<td>U</td>
<td>I</td>
<td>U</td>
<td>I</td>
<td>A</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Chief executive officer (CEO)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Chief financial officer (CFO)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Chief information security officer (CISO)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Information security steering committee (ISSC)</td>
<td>A</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>U</td>
</tr>
<tr>
<td>Business process owner</td>
<td></td>
<td></td>
<td></td>
<td>U</td>
<td>U</td>
<td>U</td>
<td>U</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Head of human resources (HR)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Internal: IT</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Chief information officer (CIO)/IT manager</td>
<td></td>
<td></td>
<td></td>
<td>U</td>
<td>U</td>
<td>U</td>
<td>U</td>
<td>U</td>
<td>U</td>
<td>U</td>
</tr>
<tr>
<td>Information security manager (ISM)</td>
<td></td>
<td></td>
<td></td>
<td>U</td>
<td>U</td>
<td>U</td>
<td>O</td>
<td>O</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td><strong>External</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Investors</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Insurers</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Regulators</td>
<td>I</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Business Partners</td>
<td>I</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Vendors/Suppliers</td>
<td>I</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>External Auditors</td>
<td>I</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

An indication of the nature of the relationship of the stakeholder for each information type:
A—Approver
O—Originator
I—Informed of information type
U—User of information type

Source: COBIT 5 for Information Security, Figure 17
Advantages and Disadvantages of Potential Paths for Information Security Reporting

<table>
<thead>
<tr>
<th>Role</th>
<th>Advantages</th>
<th>Disadvantages</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chief executive officer (CEO)</td>
<td>Information risk is elevated to the highest level in the enterprise.</td>
<td>Information risk needs to be presented in a format that is understandable to the CEO. Given the multitude of responsibilities of the CEO, information risk might be monitored and managed at too high a level of abstraction or might not be fully understood in its relevant details.</td>
</tr>
<tr>
<td>Chief information officer (CIO)</td>
<td>Information security issues and solutions can be aligned with all IT initiatives.</td>
<td>Information risk may not be addressed due to other IT initiatives and deadlines taking precedence over information security. There is a potential conflict of interest. The work performed by information security professionals may be IT-focussed and not information security-focussed. In other words, there may be an insufficient business focus.</td>
</tr>
<tr>
<td>Chief financial officer (CFO)</td>
<td>Information security issues can be addressed from a financial business impact point of view.</td>
<td>Information risk may not be addressed due to financial initiatives and deadlines taking precedence over information security. There is a potential conflict of interest.</td>
</tr>
<tr>
<td>Chief risk officer (CRO)</td>
<td>Information risk is elevated to a position that can also look at risk from strategic, financial, operational, reputational and compliance perspectives.</td>
<td>This role does not exist in most enterprises. It is most often found in financial service organisations. In enterprises in which a CRO is not present, organisational risk decisions may be decided by the CEO or board of directors.</td>
</tr>
<tr>
<td>Chief technology officer (CTO)</td>
<td>Information security can be partnered and included in future technology road maps.</td>
<td>Information risk may not be addressed due to technology directions taking precedence over information security.</td>
</tr>
<tr>
<td>Chief operating officer (COO)</td>
<td>Information security issues and solutions can be addressed from the standpoint of impact to the business’ operations.</td>
<td>Information risk may not be addressed due to operational initiatives and deadlines taking precedence over information security.</td>
</tr>
<tr>
<td>Board of directors (indirect report)</td>
<td>Information risk is elevated to the highest level in the enterprise.</td>
<td>Information risk needs to be presented in a format that is understandable to board members, and hence may become too high-level to be relevant.</td>
</tr>
</tbody>
</table>

Source: COBIT 5 for Information Security, Figure 14

Policy Framework

```
Policy Framework

Information Security Principles
Information Security Policy
Specific Information Security Policies
Information Security Procedures
Information Security Requirements and Documentation

Input

Mandatory Information Security Standards, Frameworks and Models
Generic Information Security Standards, Frameworks and Models
```

Source: COBIT 5 for Information Security, Figure 10
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 Security Problems
- DSS04 Manage Continuity
- DSS05 Manage Security Services
- DSS06 Manage Business Process Controls

Monitor, Evaluate and Assess

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

Source: COBIT 5, figure 16
COBIT 5 Enterprise Enablers

1. Principles, Policies and Frameworks
2. Processes
3. Organisational Structures
4. Culture, Ethics and Behaviour
5. Information
6. Services, Infrastructure and Applications
7. People, Skills and Competencies

Resources

Source: COBIT 5, figure 12

COBIT 5 Enablers: Generic

Stakeholders
- Internal Stakeholders
- External Stakeholders

Goals
- Intrinsic Quality
- Contextual Quality (Relevance, Effectiveness)
- Accessibility and Security

Life Cycle
- Plan
- Design
- Build/Acquire/Create/Implement
- Use/Operate
- Evaluate/Monitor
- Update/Dispose

Good Practices
- Practices
- Work Products (Inputs/Outputs)

Enabler Performance Management

- Are Stakeholders Needs Addressed?
- Are Enabler Goals Achieved?
- Is Life Cycle Managed?
- Are Good Practices Applied?

Metrics for Achievement of Goals (Lag Indicators)
Metrics for Application of Practice (Lead Indicators)

Source: COBIT 5, figure 13

© 2013 ISACA. ALL RIGHTS RESERVED.
The Seven Phases of the Implementation Life Cycle

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

2. Define problems and define opportunities
   - Identify role players
   - Communicate team to change and use players' outcomes

3. Define road map
   - Form implementation team
   - Develop communications plan

4. Plan programme
   - Establish desire
   - Embed new approaches

5. Execute plan
   - Operate
   - Identify role
   - Communicate

6. Realise benefits
   - Monitor and evaluate
   - Recognise need to act

7. Review effectiveness
   - Compare expected to actual
   - Identify corrective actions

How do we keep the momentum going?

Did we get there?

Where do we want to be?

What needs to be done?

Summary of the COBIT 5 Process Capability Model

Generic Process Capability Attributes

|---------------------------------------------------|------------------------------|-------------------------------|--------------------------|---------------------------|---------------------------|--------------------------|---------------------------|---------------------------|

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

Source: COBIT 5, figure 19