Using COBIT 5 Framework for Cybersecurity Assessment

Hugh Burley, Trevor Hurst, and Ivor MacKay
Speakers

Trevor Hurst, Chief Information Officer
Ministry of Advanced Education, Skills & Training

Hugh Burley, Manager of Information Security/Information Security Officer
Thompson Rivers University/BCNET

Ivor MacKay, Manager, Information Technology
BCNET
Agenda

1. COBIT 5 Refresher
2. Why COBIT 5
3. Assessments
4. Q & A
COBIT 5 Refresher
COBIT 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
Meeting Stakeholder Needs

Figure 3—The Governance Objective: Value Creation

- Stakeholder Needs
- Governance Objective: Value Creation
  - Benefits Realisation
  - Risk Optimisation
  - Resource Optimisation
COBIT 5 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
Figure 15—COBIT 5 Governance and Management Key Areas

Business Needs

Governance
- Evaluate
  - Direct
  - Monitor

Management Feedback

Management
- Plan (APO)
- Build (BAI)
- Run (DSS)
- Monitor (MEA)
Figure 1—COBIT 5 Process Reference Model

Processes for Governance of Enterprise IT

Evaluate, Direct and Monitor

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

Align, Plan and Organise

- 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

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
Why COBIT 5?
Alignment

“How do I ensure all of our Digital investments contribute to Stakeholder Value and enable the strategy of my Institution?”

Tell a better story (funding)

“How do I better communicate the gaps in our environment and achieve better funding?”

Audit preparation (Risk Management)

“How do I ensure benefits are realized and IT risks are mitigated? How can I prepare for upcoming Audit and/or review activity?”
REPORT HIGHLIGHTS

USE OF IT COMES WITH RISKS:
FRAUD ERRORS SYSTEM DISRUPTION
Strong general computing controls can reduce the impact of risks.

BC government organizations SELF-ASSESSED A HIGHER AVERAGE MATURITY LEVEL THAN 2013

Majority of organizations self-assessed at MATURITY LEVEL 3 AND ABOVE

IT IS CRITICAL to government’s service delivery – from healthcare to education

Over 600 IT services are outsourced to external parties

78% of our previous IT audit recommendations were about general computing controls

69% of audited organizations lacked sufficient evidence to support their self-assessed levels

OAGBC General Computing Controls Report

COBIT Maturity

1. Assess and manage IT risks

2. Manage changes
COBIT Maturity

6. Ensure systems security

9. Monitor and evaluate IT performance
Assessments
Assessment vs Audit

Or is it really Gap Analysis vs. Internal Audit vs. Pre-Assessment
Differences Between the COBIT 4.1 and the COBIT 5

Figure 18—Summary of the COBIT 4.1 Maturity Model

Maturity Model (1 per Process)

- Non-existent
- Ad hoc
- Repeatable
- Defined Process
- Managed and Measurable
- Optimised

Maturity Levels:
- Maturity Level 0
- Maturity Level 1
- Maturity Level 2
- Maturity Level 3
- Maturity Level 4
- Maturity Level 5

Figure 19—Summary of the COBIT 5 Process Capability Model

Generic Process Capability Attributes

- Performance Attribute (PA) 1.1: Process Performance
- PA 2.1: Performance Management
- PA 2.2: Work Product Management
- PA 3.1: Process Definition
- PA 3.2: Process Deployment
- PA 4.1: Process Measurement
- PA 4.2: Process Control
- PA 5.1: Process Innovation
- PA 5.2: Process Optimisation

Process Levels:
- Incomplete Process
- Performed Process
- Managed Process
- Established Process
- Predictable Process
- Optimising Process
APO12 Manage Risk

APO13 Manage Security

BAI06 Manage Changes

DSS02 Manage Service Requests and Incidents
Assessment Methodology

**Phase 1: Data Gathering & Scoping**
- Gather policies and process documents
- Interview key personnel and define in-scope data & applications
- Confirm in-scope systems and business processes

**Phase 2: Risk Assessment**
- Assess:
  - General Security Standards
  - Physical Safeguards
  - Technical Safeguards
  - Organizational Requirements

**Phase 3: Gap Report & Remediation Plan**
- Develop:
  - Gap Report
  - Remediation options
  - Roadmap for achieving and maintaining compliance
- Executive buy-in of Remediation Reports

**Phase 4: Remediation Plan Implementation**
- Plan remediation program
- Implement necessary controls & technology safeguards
- Define maintenance workflow for controls
KEY AREA: RISK

a) Level of risk acceptance
b) Risk review
c) Risk approval

KEY AREA: MANAGING SECURITY

a) What is your Security Standards/Model/Framework: ISO27001, NIST
b) Are you tracking your Security events
c) BCP/DRP
### Risk Assessment Consequence Table

<table>
<thead>
<tr>
<th>Threat</th>
<th>Insignificant</th>
<th>Minor</th>
<th>Significant</th>
<th>Major</th>
<th>Catastrophic</th>
</tr>
</thead>
<tbody>
<tr>
<td>Insignificant</td>
<td>-1</td>
<td>-2</td>
<td>-3</td>
<td>-4</td>
<td>-5</td>
</tr>
<tr>
<td>Minor</td>
<td>-2</td>
<td>-4</td>
<td>-6</td>
<td>-8</td>
<td>-10</td>
</tr>
<tr>
<td>Significant</td>
<td>-3</td>
<td>-6</td>
<td>-9</td>
<td>-12</td>
<td>-15</td>
</tr>
<tr>
<td>Major</td>
<td>-4</td>
<td>-8</td>
<td>-12</td>
<td>-16</td>
<td>-20</td>
</tr>
<tr>
<td>Catastrophic</td>
<td>-5</td>
<td>-10</td>
<td>-15</td>
<td>-20</td>
<td>-25</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Consequence</th>
<th>Rare</th>
<th>Unlikely</th>
<th>Possible</th>
<th>Probable</th>
<th>Likely</th>
<th>Almost Certain</th>
</tr>
</thead>
<tbody>
<tr>
<td>Compelling</td>
<td>5</td>
<td>10</td>
<td>15</td>
<td>20</td>
<td>25</td>
<td>30</td>
</tr>
<tr>
<td>Substantial</td>
<td>4</td>
<td>8</td>
<td>12</td>
<td>16</td>
<td>20</td>
<td>24</td>
</tr>
<tr>
<td>Reasonable</td>
<td>3</td>
<td>6</td>
<td>9</td>
<td>12</td>
<td>15</td>
<td>18</td>
</tr>
<tr>
<td>Modest</td>
<td>2</td>
<td>4</td>
<td>6</td>
<td>8</td>
<td>10</td>
<td>12</td>
</tr>
<tr>
<td>Insignificant+</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>6</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Final Rating</th>
</tr>
</thead>
<tbody>
<tr>
<td>Compelling</td>
</tr>
<tr>
<td>Considerable</td>
</tr>
<tr>
<td>Fair</td>
</tr>
<tr>
<td>Small</td>
</tr>
<tr>
<td>insignificant</td>
</tr>
<tr>
<td>Low</td>
</tr>
<tr>
<td>Medium</td>
</tr>
<tr>
<td>High</td>
</tr>
<tr>
<td>Critical</td>
</tr>
</tbody>
</table>

### Threat / Opportunity Matrix

- **High**
- **Considerable**
- **Fair**
- **Small**
- **Insignificant**
- **Low**
- **Medium**
- **High**
- **Critical**
KEY AREA: MANAGING CHANGE

a) Methods of assessing change and its risks
b) Approval process

KEY AREA: MANAGE SERVICE REQUESTS AND INCIDENTS

a) Problem tracking
b) Evidence of reviewing Incidents and Requests
Self-Assessment

**Figure 6—Self-assessment Process**

1. **Step 1**
   - Decide on process to assess—scoping.

2. **Step 2**
   - Determine level 1 capability.

3. **Step 3**
   - Determine capability for levels 2 to 5.

4. **Step 4**
   - Record and summarise capability levels.

5. **Step 5**
   - Plan process improvement.
Self-Assessment

http://www.isaca.org/COBIT/Pages/Self-Assessment-Guide.aspx
Self-Assessment

http://www.isaca.org/COBIT/Pages/COBIT-5-PAM.aspx
Info~Tech

IT Management & Governance Framework

A comprehensive and connected set of research to help you optimize and improve your core IT processes.

BCNET Conference 2018