Implementing Enterprise Governance of IT Using COBIT 5

‘A Business Driven Approach’
Presented
At Auditor General Pretoria
02 May 2013
by
Tichaona Zororo
CIA, CRMA, CISA, CISM, CRISC, CGEIT
B.Sc. Hons. Information Systems (MSU), P.G.D. Computer Auditing (WITS)
Emerging Technology – The Irrevocable Forces – The BIG 6

Increased Mobility

Cloud Computing

Technology has evolved the way business is contacted. More and more companies are using social media, mobile phones, and tablets to do their business.

Internet of Things

Consumerisation

Big Data

Social Media
Legal and Regulatory Drivers for Enterprise Governance of IT

A “tsunami” of regulations

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

Huge reputational risks
The Familiar IT Environment
The Business Case for Implementing Enterprise Governance of IT

Pain Points

- Board or senior management who are reluctant to engage with IT/IT matters
- Significant business incidents related to IT
- Hefty regulatory and contractual penalties
- Repeat findings and qualified audits
- Outsourcing problems leading to business failing to meet its goals
- Costly failed IT initiatives
- Significant business incidents related to IT
- IT Projects that do not address business needs
- IT enabled investments often delivered late and out of budget
Business Drivers for Enterprise Governance of IT

Trigger Events

- Mergers, Acquisitions or Divestitures
- An enterprise wide governance focus or project
- New appointment or changes at enterprise C-Level
- Desire to optimise value creation from IT enabled business changes
- Change in business operating or sourcing arrangements
- A shift in the market, economy or competitive position
- New business focus
- External audit or consultant assessments
- Significant technology change or paradigm shift
- New regulations or compliance requirements
IT Is Complicated.

Governance of Enterprise IT Does Not Have To Be.

An Anatomy of COBIT 5
## The Evolution of COBIT – 16 Years of Existence

<table>
<thead>
<tr>
<th>Year</th>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1996</td>
<td>COBiT 1</td>
<td>An Audit and Control Framework – Focus on Control Objectives</td>
</tr>
<tr>
<td>2000</td>
<td>COBiT 3</td>
<td>3rd Edition – An IT Management Framework – Management Guidelines added</td>
</tr>
<tr>
<td>2007</td>
<td>COBiT 4.1</td>
<td>An IT Governance Framework – Governance and Compliance processes added, Assurance processes removed</td>
</tr>
<tr>
<td>2012</td>
<td>COBIT 5</td>
<td>Governance of Enterprise IT Framework – Integrate all other ISACA frameworks – Val IT, BMIS, RISK IT</td>
</tr>
</tbody>
</table>

---

**COBIT**

Beyond Excellence®
COBIT 4.1 An IT Governance Framework – 2007 to 2012

- Governance and Compliance processes added, Assurance processes removed
- Focus on processes as the key enablers
- 4 Domains [PO, AI, DS, ME]
- 34 Processes
- 208 Control Objectives
- CMMI /PAM  ISO ISO/IEC 15504
Introduction to COBIT 5 – An integrated framework

A business framework for the Governance and Management of Enterprise IT

COBIT 5 builds on previous versions of COBIT, BMIS, Val IT and Risk IT. Aligned with current best practices, e.g., ITIL, ISO2007 1/2, TOGAF

ISO/IEC 38500

Principles
1. Responsibility
2. Strategy
3. Acquisition
4. Performance
5. Conformance
6. Human Resources
1. Stakeholder needs have to be transformed into an enterprise’s actionable strategy.

2. The COBIT 5 goals cascade translates stakeholder needs into specific, actionable and customised goals within the context of the enterprise, IT-related goals and enabler goals. These enterprise goals have been developed using the Balanced Scorecard (BSC) dimensions. (Kaplan, Robert S.; David P. Norton; The Balanced Scorecard: Translating Strategy into Action, Harvard University Press, USA, 1996)

3. The enterprise goals (Financial, Customer, Internal, Learning and Growth) are a list of commonly used goals that an enterprise has defined for itself.

4. Enterprise-specific goals can be easily mapped onto one or more of the generic enterprise goals.
<table>
<thead>
<tr>
<th>IT BSC Dimension</th>
<th>Enterprise Goal</th>
<th>Information &amp; Related Technology Goal</th>
</tr>
</thead>
<tbody>
<tr>
<td>Financial</td>
<td>Stakeholder value of business investments</td>
<td>Alignment of IT &amp; business strategy</td>
</tr>
<tr>
<td></td>
<td>Portfolio of competitive products &amp; services</td>
<td>IT compliance and support for business compliance with external laws</td>
</tr>
<tr>
<td></td>
<td>Managed business risk (safeguarding of assets)</td>
<td>Commitment of executive management for making IT related decisions</td>
</tr>
<tr>
<td></td>
<td>Compliance with external laws and regulations</td>
<td>Managed IT related business risk</td>
</tr>
<tr>
<td></td>
<td>Financial Transparency</td>
<td>Realised benefits from IT-enabled investments and services portfolio</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Transparency of IT costs, benefits and risk</td>
</tr>
<tr>
<td>Customer</td>
<td>Customer-oriented service culture</td>
<td>Delivery of IT services in line with business requirements</td>
</tr>
<tr>
<td></td>
<td>Business service continuity and availability</td>
<td>Adequate use of applications, information and technology solutions</td>
</tr>
<tr>
<td></td>
<td>Agile responses to a changing business environment</td>
<td>IT agility</td>
</tr>
<tr>
<td></td>
<td>Information based strategic decision making</td>
<td>Security of information, processing infrastructure and applications</td>
</tr>
<tr>
<td></td>
<td>Optimisation of service delivery costs</td>
<td>Optimisation of IT assets, resources and capabilities</td>
</tr>
<tr>
<td>Internal Business Processes</td>
<td>Optimisation of business process functionality</td>
<td>Enablement and support of business processes by integrating applications and technology into business processes</td>
</tr>
<tr>
<td>What business processes must we excel at to satisfy our stakeholders and customers?</td>
<td>Optimisation of business process costs</td>
<td>Delivery of programmes delivering benefits, on time, on budget and meeting requirements and quality standards</td>
</tr>
<tr>
<td></td>
<td>Managed business change programmes</td>
<td>Availability of reliable and useful information for decision making</td>
</tr>
<tr>
<td></td>
<td>Operational and staff productivity</td>
<td>IT compliance with internal policies</td>
</tr>
<tr>
<td></td>
<td>Compliance with internal policies</td>
<td></td>
</tr>
<tr>
<td>Learning &amp; Growth</td>
<td>Skilled and motivated people</td>
<td>Competent and motivated business and IT personnel</td>
</tr>
<tr>
<td>How will we sustain our ability to change and improve to achieve our vision?</td>
<td>Product and business innovation culture</td>
<td>Knowledge, expertise and initiatives for business innovation</td>
</tr>
</tbody>
</table>
Principles and Enablers

COBIT 5 brings together the five principles that allow the enterprise to build an effective governance and management framework based on a holistic set of seven government and management enablers that optimises information and technology investment and use for the benefit of stakeholders.

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

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
**Governance processes**—Governance processes deal with the stakeholder governance objectives — value delivery, risk optimisation and resource optimisation—and include practices and activities aimed at evaluating strategic options, providing direction to IT and monitoring the outcome (Evaluate, direct and monitor [EDM]—in line with the ISO/IEC 38500 standard concepts).

**Management plans, builds, runs and monitors** activities in alignment with the direction set by the governance body to achieve the enterprise objectives (PBRM).
1. 2 main process domains (Governance (EDM), Management (Plan, Build, Run and Monitor))
2. 5 Domains (EDM, Plan (APO), Build/implementation (BAI), Run/execution (DSS), Monitor (MEA))
3. 37 processes (5 Governance and 32 Management)
4. The disappearance of control objectives
5. 210 practices (15 EDM, 195 PBRM (72 APO, 68 BAI, 38 DSS, 17 MEA))
5 processes, 15 practices:

1. EDM01 Establishing and Maintaining a Governance Framework
2. EDM02 Benefits Realisation (Ensure Benefits Delivery)
3. EDM03 Ensure Risk Optimisation (Value Preservation)
4. EDM04 Ensure Resource Optimisation
5. EDM05 Ensure Stakeholder Transparency
**Management Domain – PBRM (Responsibility – Execution)**

*Align, Plan & Organise*

1. Manage the IT management framework
2. Manage Strategy
3. Manage enterprise architecture
4. Manage Innovation
5. Manage Portfolio
6. Manage budget and costs
7. Manage human resources
8. Manage relationships
9. Manage service agreements
10. Manage suppliers
11. Manage quality
12. Manage Risk
13. Manage Security

*Build, Acquire & Implement*

1. Manage programmes and projects
2. Manage requirements definition
3. Manage solutions identification & build
4. Manage availability and capacity
5. Manage change enablement
6. Manage changes
7. Manage change acceptance and transitioning
8. Manage knowledge
9. Manage assets
10. Manage Configuration

*Deliver, Service & Support*

1. Manage operations
2. Manage service requests and incidents
3. Manage problems
4. Manage continuity
5. Manage security services
6. Manage business controls

*Monitor, Evaluate & Assess*

1. MEA performance and conformance
2. MEA system of internal controls
3. MEA compliance with external requirements
The Benefits of Implementing GEIT Using COBIT 5

- A common language for executives, business and IT staff
- A view, understandable to management, of what IT does
- A better understanding of how the business and IT can work together for successful delivery of IT enabled initiatives
- Better alignment, based on a business focus and quality IT services
- Improved efficiency and optimization of cost
- More effective management of IT and reduced operational risk
- Clear policy development and more efficient and successful audits
- Clear ownership and responsibilities, based on process orientation
Rolling out COBIT 5 the Enterprise Context

Fit For Purpose:

- Organisations operate in different context as determined by external and internal factors. The concepts should be clearly understood and considered when adopting COBIT 5.

- Every organization needs to formulate its own implementation plan or road map, depending on factors in the enterprise’s specific environment.

Key Enterprise Factors to Consider:

- Ethics and culture
- Legal and regulatory requirements
- Governance, policies and practices
- Mission, vision and values
- Business plan and strategic intentions
- Operating model and level of maturity
- Risk appetite
- Capabilities
- Roles and responsibilities – structures – Governance Officer, Risk Officer, Compliance Officer

From fire fighting/reactive/audit findings focused approach to a proactive approach

One size does not fit all

Cut your own size
Key Success Factors

- **Tone at the top:**
  1. The board should mandate adoption and adaption of a GEIT framework as an integral part of enterprise governance development
  2. Top management should provide the direction and mandate for initiative as well as visible **on-going commitment and support**

- Understanding of the business and IT objectives by all parties supporting the initiative

- Effective communication

- Creating an enabling environment

- Fit for purpose to optimize on the unique context of the enterprise

- Focusing on quick wins and prioritising the most beneficial improvements that are the easiest to implement

- Overcoming human behavioral and cultural barriers

- **Stakeholders Involvement:**
  1. Board and executive management
  2. Executive business management, IT management and process owners
  3. Business management, IT management and process owners
  4. Risk, compliance and legal experts
  5. Audit
A Life Cycle Approach

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?
8. Review effectiveness
9. Identify role players

- Plan programme
- Execute plan
- Realise benefits

- Define problems and opportunities
- Define road map
- Establish desire to change
- Sustain

- Initiate programme
- Recognise need to act
- Monitor and evaluate
- Implement improvements
- Operate and use

- Embed new approaches
- Operate and use
- Form implementation team

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

EGiT Beyond Excellence®
Implementation Life Cycle Phases

The 7 phases of the implementation life cycle

- What are the drivers?
- Where are we now?
- Where do we want to be?
- What needs to be done?
- How do we get there?
- Did we get there?
- How do we keep the momentum going?

Programme management phases

- Initiate programme
- Define problems and opportunities
- Define road map
- Plan programme
- Execute
- Realise benefits
- Review effectiveness

John Thorp’s Four Ares

Are we doing the right things? (The Strategic Question)

Are we getting the benefits? (The Value Question)

Are we doing them the right way? (The Architecture Question)

Are we getting them done well? (The Delivery Question)
Implementation Life Cycle Phases

Change enablement

- Establish desire to change
- Form implementation team
- Communicate outcome
- Identify role players
- Operate and use
- Enabled new approaches
- Sustain

Continual improvement life cycle

- Recognise need to act
- Assess current state
- Define target state
- Build improvements
- Implement improvements
- Operate and measure
- Operate and evaluate
Unlocking IT Value – Transforming IT Enabled Investments into Business Value