COBIT 5: an evolutionary framework and only framework to address the governance and management of enterprise IT

Slindile Khanyile
64 Jasper Hill, 309 1st Road
Midrand, 1686
+2772 026 2656
41998669@mylife.unisa.ac.za

Hanifa Abdullah
University of South Africa (UNISA)
P.O. Box 392
UNISA
0003
abdulh@unisa.ac.za

ABSTRACT
In many organizations, Information Technology (IT) has become vital in the support, sustainability and growth of the business. This pervasive use of technology has created a dependency on IT that calls for a specific focus on IT Governance. IT Governance is an integral part of enterprise governance exercised by the Board overseeing the definition and implementation of processes, structures and relational mechanism in the organization. This enables both the business and IT people to execute their responsibilities in support of business/IT alignment and the creation of business value from IT-enabled business investments. When approaching IT Governance, there are a number of frameworks, maintained by various governing bodies. The focus of this paper will be on the COBIT 5 framework as this framework concerns the governance and management of enterprise information. In order to operate a business both governance and management is needed.

The Control Objectives for Information and related Technology (COBIT) framework has become a globally accepted standard for IT governance. COBIT 5 is a major strategic improvement for ISACA, providing the next generation of ISACAs guidance on the enterprise governance of IT. Building on the more than 15 years of practical usage and application of COBIT by many enterprises and users from the business, IT, security and assurance communities, COBIT 5 is designed to meet the current needs of stakeholders and align with the most up-to-date thinking in enterprise governance and IT management techniques.

Categories and Subject Descriptors
K.6.0 [Management of Computing and Information Systems]

General Terms
Management, Measurement, Documentation, Security, Standardization, Theory

Keywords
IT Governance, IT Management, COBIT, Val IT, Risk IT, ITIL, ISO

1. INTRODUCTION
Originally, Information Technology was implemented to automate processes of enterprises and enable gains in productivity [1]. Over the years, IT has become the backbone of businesses to the point where it is impossible for many to function without it [2]. More and more organizations are becoming increasingly dependent on a broad range of technologies to manage and grow their business. IT is an integral part of most organizations today and will certainly become more critical in the future [3]. It is for this reason that organizations are now increasingly concerned about the accountability for making decisions around the use of IT in the best interest of the board, executives and all other stakeholders.

This has brought about an increased focus on IT governance. While there is no single, complete, off-the-shelf IT governance framework, there are a number of frameworks available that can serve as useful starting points for developing a governance model. Most of the existing frameworks are complementary, with strengths in different areas and so a mix-and match approach is often taken [4].

Weill and Ross state that in order to operate a business, it is necessary to have both good governance and management. [5] The difference between governance and management is that governance is about who makes the decisions whereas management has to do with making and implementing the decisions. Tracker supports this assertion by stating, “If management is about running the business, governance is about seeing that it is run properly. All companies thus require management as well as governance.” [6]. ITIL and ISO 17799 only address governance whereas COBIT 5 addresses both governance and management, thus making it a comprehensive framework for operating an organization.

This paper looks at how frameworks help organizations achieve IT governance with COBIT 5 being the focus because of its completeness. It makes a detailed examination of COBIT 5’s history, framework, benefits, principles, domains and processes, implementation and changes from COBIT 4.1.

2. IT GOVERNANCE
Gartner defines IT governance as the set of processes that ensure the effective and efficient use of IT enabling an
COBIT 5 addresses both IT and business functional areas and uses the Evaluate, Direct and Monitor model of ISO 38500 view that both IT governance and IT management are required. It also adopts the ISO 38500 enterprise information. It is more than IT governance and COBIT 5 concerns “the governance and management of enterprise governance and IT management techniques. These three definitions, although they are defining the same thing are similar yet distinct. This leads to the conclusion that there is more than one school of thought when it comes to IT governance. Musson states that there are three principal schools of thoughts on IT governance which are IT governance as a framework or an audit process, IT governance as IT decision-making and IT governance as a branch of corporate governance.

The focus of this paper is on COBIT 5 framework and how it covers both the governance and management of IT.

3. IT GOVERNANCE AND MANAGEMENT FRAMEWORK

The following section will provide an overview of the Cobit 5 framework.

3.1 COBIT

The Control Objectives for Information and Related Technology (COBIT) has become a globally accepted standard for IT governance, created by the Information Systems Audit and Control Association (now known as simply “ISACA”) and the IT Governance Institute (ITGI) in 1996 [8]. COBIT 5 is an end-to-end umbrella framework that pulls together many existing frameworks that is designed to meet the current needs of stakeholders and align with the most up-to-date thinking in enterprise governance and IT management techniques.

COBIT 5 concerns “the governance and management of enterprise information.” It is more than IT governance and includes information governance. It also adopts the ISO 38500 view that both IT governance and IT management are required and uses the Evaluate, Direct and Monitor model of ISO 38500.

COBIT 5 addresses both IT and business functional areas across the enterprise and considers the IT related interests of all stakeholders. It helps organizations to create value to IT investments by maintaining a balance between optimizing risk levels and realizing benefits.

3.1.1 Background of COBIT 5

COBIT has had the following major releases:

- In 1996, the first edition of COBIT was released.
- In 1998, the second edition added “Management Guidelines”.
- In 2000, the third edition was released.
- In 2003, an on-line version became available.
- In December 2005, the fourth edition was initially released and in May 2007, the 4.1 revision was released [16]. COBIT 5 was released in April 2012; it addresses governance and management of enterprise IT.

COBIT 5 combines COBIT 4.1, Val IT 2.0 and Risk IT as well as concepts from the Business Model for Information for a detailed framework for the effective governance and management of IT enabled business [18]. While COBIT 4.1 ensures that IT is working as effectively as possible to maximize the benefits of technology investment, Val IT helps enterprises make better decisions about where to invest, ensuring that the investment is consistent with the business strategy. Similarly, COBIT 4.1 provides a set of controls to mitigate IT risk in IT processes whilst Risk IT provides a framework for enterprises to identify, govern and manage IT-related risks.

COBIT 5 also aligns itself at a high level with existing frameworks such as ITIL and TOGAF, PMBOK, PRINCE 2 and ISO which makes it an umbrella for governance and management or IT [18].

3.1.2 Drivers of COBIT 5

COBIT 4.1 was widely accepted across the IT community as the framework for IT governance. However following an extensive review of the stakeholders, a number of drivers were identified leading to the development of COBIT 5. These drivers included [19].

- The requirement to help stakeholders to understand how various frameworks, good practices and standards can be used together.
- The need to ensure that the scope covers the full end-to-end business and functional IT responsibilities, as well as the need to cover all aspects that lead to effective IT governance and management of enterprise IT.
- The need to provide further guidance in high areas of interest, such as enterprise architecture, asset and service management, management of IT innovation and emerging technologies.
- The need to link together and reinforce all major ISACA research, frameworks and guidance i.e. COBIT, Val IT and Risk IT.
- The need to connect to and align with (where relevant) with other major frameworks and standards such as ITIL, TOGAF, PMBOK, PRINCE 2 and ISO.

3.1.3 Benefits of implementing COBIT 5

According to the IT Governance Institute, when looking at business outcomes of the Governance of Enterprise IT (GEIT), companies who have implemented COBIT 5 are experiencing improved management of IT-related risk, improved
communication and relationships between business and IT, lower IT costs, improved IT delivery of business objectives and improved competitiveness [20].

COBIT 5 provides a clear distinction between governance and management of IT, providing a holistic view of the enterprise which covers the business and IT from end-to-end and enables the effective governance and management of enterprise IT assets [21]. It enables business user satisfaction with IT engagement to the business to achieve business objectives [22]. COBIT 5 also provides an easy to access Process Reference Guide at the same level of detail because it consolidates all previous research of ISACA [21].

3.1.4 COBIT 5 Principles
COBIT 5 is built on 5 key principles for the governance and management of enterprise Information Technology [18]. The following section provides an overview of the principles.

Principle 1: Meeting Stakeholder Needs
Enterprises exist to create value for their stakeholders; therefore value creation is a governance objective for any enterprise. Value creation means realizing benefits at an optimal resource cost whilst optimizing risk.

Principle 2: Covering the Enterprise End-to-End
COBIT 5 integrates the governance of enterprise IT into enterprise governance; it therefore covers the organization holistically, the focus is not just on the IT function. It also covers the enterprise end to end for all matters relating to IT thereby providing a basis to effectively integrate other frameworks, standards and practices used.

Principle 3: Applying a Single Integrated Framework
Most IT related standards and best practices only address a certain portion of IT activities, COBIT aligns with other relevant standards and frameworks at a high level thereby making it an overarching framework for governance and management of enterprise IT

Principle 4: Enabling a Holistic Approach
Effective governance and management of enterprise IT requires a holistic approach to IT, COBIT 5 implements comprehensive governance and management of enterprise IT through enablers. Enablers are things that enable the enterprise to achieve its objectives. COBIT 5 defines 7 categories of enablers:
- Principles, Policies and Frameworks
- Processes
- Organizational Structures
- Culture, Ethics and Behavior
- Information
- Services, Infrastructure and Applications
- People, Skills and Competencies

Principle 5: Separating Governance from Management
The COBIT 5 framework makes a clear distinction between governance and management. These two disciplines fundamentally serve a different purpose, each include different types of activities and require different organizational structures.

Governance ensures that stakeholder needs, conditions and options are evaluated to determine balanced, agreed-on enterprise objectives to be achieved; setting direction through prioritization and decision making; and monitoring performance and compliance against agreed-on direction and objectives (EDM)

Management plans builds runs and monitors activities in alignment with the direction set by the governance body to achieve the enterprise objectives (PBRM).

3.1.5 COBIT5 Domains and Processes
COBIT 5 has 5 domains which are divided into governance and management domains; each domain has processes which enable it to achieve its objective(s) [18]. One domain addresses the governance and the other four domains cover management.

The governance of enterprise IT (EDM) domain contains five processes within each process, evaluate, direct and monitor practices are defined.

The management of enterprise IT domains are in line with the responsibility areas of plan, build, run and monitor. The 32 processes in these for domains are broken up as follows:
- Align, Plan and Organize (APO): 13 processes
- Build, Acquire and Implement (BAI): 10 processes
- Deliver, Service and Support (DSS): 6 processes
- Monitor, Evaluate and Assess (MEA): 3 processes

3.1.5.1 Governance of Enterprise IT
The following table lists the high-level IT processes for the EDM domain.

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

3.1.5.2 Management of Enterprise IT
The following sections examine the four domains and the processes that fall under the management of enterprise IT [23]

3.1.5.2.1 Align, Plan and Organize (APO)
The Planning and Organization domain covers the use of information and technology and how best it can be used in an organization to help achieve the organization’s goals and objectives. It also highlights the organizational and infrastructural form IT is to take in order to achieve the optimal results and to generate the most benefits from the use of IT.

The following table lists the high-level IT processes for the APO domain.
Table 2 High Level IT Processes for the APO Domain

<table>
<thead>
<tr>
<th>APO01</th>
<th>Manage the IT Management Framework</th>
</tr>
</thead>
<tbody>
<tr>
<td>APO02</td>
<td>Manage Strategy</td>
</tr>
<tr>
<td>APO03</td>
<td>Manage Enterprise Architecture</td>
</tr>
<tr>
<td>APO04</td>
<td>Manage Innovation</td>
</tr>
<tr>
<td>APO05</td>
<td>Manage Portfolio</td>
</tr>
<tr>
<td>APO06</td>
<td>Manage Budget and Costs</td>
</tr>
<tr>
<td>APO07</td>
<td>Manage Human Relations</td>
</tr>
<tr>
<td>APO08</td>
<td>Manage Relationships</td>
</tr>
<tr>
<td>APO09</td>
<td>Manage Service Agreements</td>
</tr>
<tr>
<td>APO10</td>
<td>Manage Suppliers</td>
</tr>
<tr>
<td>APO11</td>
<td>Manage Quality</td>
</tr>
<tr>
<td>APO12</td>
<td>Manage Risk</td>
</tr>
<tr>
<td>APO13</td>
<td>Manage Security</td>
</tr>
</tbody>
</table>

3.1.5.2.2 Build, Acquire and Implement (BAI)
The Build, Acquire and Implement domain covers identifying IT requirements, acquiring the technology, and implementing it within the company’s current business processes.
The following table lists the high level control objectives for the BAI domain.

Table 3 High-level Processes for the BAI Domain

<table>
<thead>
<tr>
<th>BAI01</th>
<th>Manage Programs and Projects</th>
</tr>
</thead>
<tbody>
<tr>
<td>BAI02</td>
<td>Manage Requirements Definition</td>
</tr>
<tr>
<td>BAI03</td>
<td>Manage Solutions Identification and Build</td>
</tr>
<tr>
<td>BAI04</td>
<td>Manage Availability and Capacity</td>
</tr>
<tr>
<td>BAI05</td>
<td>Manage Organizational Change Enablement</td>
</tr>
<tr>
<td>BAI06</td>
<td>Manage Changes</td>
</tr>
<tr>
<td>BAI07</td>
<td>Manage Changes Acceptance and Transitioning</td>
</tr>
<tr>
<td>BAI08</td>
<td>Manage Knowledge</td>
</tr>
<tr>
<td>BAI09</td>
<td>Manage Assets</td>
</tr>
<tr>
<td>BAI10</td>
<td>Manage Configuration</td>
</tr>
</tbody>
</table>

3.1.5.2.3 Deliver, Service and Support (DSS)
The Deliver, Service and Support domain focuses on the delivery aspects of the information technology. It covers areas such as the execution of the applications within the IT system and its results, as well as, the support processes that enable the effective and efficient execution of these IT systems.
The following table lists the high level control objectives for the DSS domain.

Table 4 High-level Processes for the DSS Domain

<table>
<thead>
<tr>
<th>DSS01</th>
<th>Manage Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>DSS02</td>
<td>Manage Service Requests and Incidents</td>
</tr>
<tr>
<td>DSS03</td>
<td>Manage Problems</td>
</tr>
<tr>
<td>DSS04</td>
<td>Manage Continuity</td>
</tr>
<tr>
<td>DSS05</td>
<td>Manage Security Services</td>
</tr>
<tr>
<td>DSS06</td>
<td>Manage Business Process Controls</td>
</tr>
</tbody>
</table>

3.1.5.2.4 Monitor, Evaluate and Assess (MEA)
The Monitor, Evaluate and Assess domain deals with a company’s strategy in assessing the needs of the company and whether or not the current IT system still meets the objectives for which it was designed and the controls necessary to comply with regulatory requirements. Monitoring also covers the issue of an independent assessment of the effectiveness of IT system in its ability to meet business objectives and the company’s control processes by internal and external auditors.

The following table lists the high level control objectives for the MEA domain.

Table 5 High-level Processes for the MEA Domains

<table>
<thead>
<tr>
<th>MEA01</th>
<th>Monitor, Evaluate and Assess Performance and Conformance</th>
</tr>
</thead>
<tbody>
<tr>
<td>MEA02</td>
<td>Monitor, Evaluate and Assess the System of Internal Control</td>
</tr>
<tr>
<td>MEA03</td>
<td>Evaluate and Assess Compliance with External Requirements</td>
</tr>
</tbody>
</table>

3.1.6 Implementing COBIT 5
COBIT 5 builds on previous versions of COBIT, Val IT and Risk IT. Enterprises can build on the work they have put into their previous version of COBIT [24].

When implementing COBIT 5, the organization must determine which stakeholder interests have priority, what their expectations are, what the IT functions capability to satisfy these expectations are and who is accountable for doing so. This requires knowledge about the underlying processes and management system that supports the IT function to deliver the services and performance expected [24].

Upgrading existing implementations of the COBIT 4.1 process model will require minor adjustments such as combining existing processes and moving practices between processes [18].

3.1.6.1 Changes from COBIT 4.1
The following section provides an overview of the changes from COBIT 4.1 [25].

Stakeholder Expectations and Value Driven:
The main driver behind COBIT 5 is stakeholder expectations and values. These changes ensure that the needs of both internal and external customers are considered in addition to the enterprise strategy and goals which are emphasized in COBIT 4.1 for benefits realization, risk balancing and cost optimization.

Domain Areas:
COBIT 5 has five domains under governance and management. The governance section provides guidance on evaluation, direction and monitoring of IT processes and is aligned with the ISO38500 “standard for corporate governance of information technology.” The management domains are in line with the four equivalent domains of COBIT 4.1.

Process Model and Areas:
COBIT 5 has 36 processes (COBIT 4.1 has 34). A few processes from COBIT 4.1 are merged in COBIT 5 and some single processes from COBIT 4.1 are split to form separate processes in COBIT 5 to allow for more specific guidance. For
example, ME4 – Provide it Governance from COBIT 4.1 is split into five separate processes (EDM1 to EDM5) under the new Governance Domain. Two new processes are introduced:

- AP01- Define Management Framework for IT
- BA18 – Knowledge Management.

Integrated Framework:
Different frameworks such as Val IT, Risk IT, BMIS, ITAF and relevant data points from various standards and best practices from organization such as ISO, ITIL, PMBOK, TOGAF and COBIT 4.1 are consolidated into a single framework providing a single source of guidance. This integration will support a holistic view of management and governance in the enterprise.

Capability/Maturity Model:
COBIT 4.1 has a process maturity model to assess the maturity of current state of enterprise and identify the steps to improve the process to achieve desired maturity level. This older maturity model is replaced by a process capability model based on ISO 15504 which is a software process assessment standard. Capability-level names are adopted from that standard. The new levels for the capability and maturity model are mentioned in section 3.3.4.

Goals Cascade:
COBIT 5 provides a link between stakeholders’ expectations and practical goals providing more specific details. IT goals are derived from enterprise business goals, which in turn are derived from stakeholder expectations and values. This goal linkage is represented as a goal cascade in 5.

Enablers:
COBIT 5 has seven categories of interrelated enablers and is driven by the goal cascade. The seven enablers for achieving enterprise goals are

- Principles, Policies and Frameworks
- Processes
- Organizational Structures
- Culture, Ethics and Behavior
- Information
- Services, Infrastructure and Applications
- People, Skills and Competencies

Control Objectives:
Unlike the 210 control objectives in COBIT 4.1, there is no separate mention of control objectives in 5; such objectives are part of 208 management and governance practices. COBIT 5 is driven by stakeholder needs and not primarily by best practices.

Summary of Changes:
The following table summarizes the significant differences between COBIT 4.1 and COBIT 5 [27].

<table>
<thead>
<tr>
<th>Table 6 Summary of Changes</th>
<th>COBIT 4.1</th>
<th>COBIT 5</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Driver</td>
<td>Best Practice</td>
</tr>
<tr>
<td>2</td>
<td>Domain Areas</td>
<td>4 Domain Areas</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Section</th>
<th>Parameter</th>
<th>COBIT 4.1</th>
<th>COBIT 5</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>Process Areas</td>
<td>34 Processes</td>
<td>36 Processes</td>
</tr>
<tr>
<td>4</td>
<td>Framework</td>
<td>Only COBIT 4.1 Framework</td>
<td>Integrated framework – Val IT, Risk IT, ITAF, BMIS etc. with COBIT 4.1</td>
</tr>
<tr>
<td>5</td>
<td>Capability/ Maturity Model</td>
<td>Maturity Models</td>
<td>Process Capability Model</td>
</tr>
<tr>
<td>6</td>
<td>Goals Cascade</td>
<td>IT goals are derived from business goals of maintaining enterprise reputation and leadership</td>
<td>IT goals are derived from stakeholder needs and expectations</td>
</tr>
<tr>
<td>7</td>
<td>Enablers</td>
<td>No mention of enablers</td>
<td>Identified 7 enablers</td>
</tr>
<tr>
<td>8</td>
<td>Control Objectives</td>
<td>210 Control Objectives</td>
<td>No separate mention of control objectives but included as part of Management and Governance Practices</td>
</tr>
</tbody>
</table>

4. HOW COBIT ACHIEVES IT GOVERNANCE

The COBIT 5 Evaluate, Direct and Monitor (EDM) process set is designed to govern and encapsulate the processes of all other management processes. This major upgrade in COBIT 5 is intended to increase awareness of the need for a structured governance framework for all organizations at an enterprise-wide level, from operations to the strategic board [26].

Governance practices are considered at their best when they are linked and embedded as continuous management life cycles, such as enterprise risk management, in all processes within an. In the past the distinction between governance and management has been blurry, adopting COBIT 5 is an opportunity to clarify and address the difference.

5. CONCLUSION

COBIT 5 is the only framework that addresses governance and management of enterprise IT. There are lots of opportunities for future research as COBIT 5 is still very new.
6. REFERENCES


