CobiT 5.0 Due for Release

by Pritam Bankar, CISA, CISM & M. E. Kabay, PhD, CISSP-ISSMP

Security professionals should constantly monitor developments in information technology (IT) governance for ideas that can support our work in developing, implementing, and monitoring information security. Today we have an overview of recent changes in the CobiT framework for IT governance from Pritam Bankar, CISA, CISM. What follows is entirely Mr Bankar's work with minor edits.

The Control Objectives for Information and Related Technology (CobiT) is a set of best practices (framework) for information technology (IT) Management & Governance. CobiT helps organizations meet today's business challenges in regulatory compliance, risk management and alignment of IT strategy with organizational goals. The first version was published by the Information Systems Audit and Control Association (ISACA) and the IT Governance Institute in 1996.

CobiT 4.1< http://www.isaca.org/Knowledge-Center/CobiT/Documents/CobiT4.pdf > was published in 2007 to provide IT practitioners and mangers with an IT governance model to deliver value from IT and to manage risks associated with IT. CobiT 4.1 is currently being updated to 5.0< http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/CobiT-5-Exposure-Draft.aspx > and will consolidate and integrate various frameworks like CobiT 4.1, Val IT 2.0< http://www.isaca.org/Knowledge-Center/Val-IT-IT-Value-Delivery-/Pages/Val-IT1.aspx >, RISK IT< http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/The-Risk-IT-Framework.aspx >, BMIS< http://www.isaca.org/Knowledge-Center/BMIS/Pages/Business-Model-for-Information-Security.aspx > and ITAF< http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/ITAF-A-Professional-Practices-Framework-for-IT-Assurance.aspx > to create a detailed framework for effective governance and management of IT. CobiT 5.0 is scheduled to be released in 2012.

CHANGES FROM 4.1

1. Stakeholder Expectations and Value Driven

The main driver behind CobiT 5.0 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 currently emphasized 4.1for benefits realization, risk balancing and cost optimization.

2. 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< http://www.38500.org/ > standard for "standard for corporate governance of information technology." The four domains in the management area are

- Align, Plan and Organize
- Build, Acquire and Implement
- Deliver, Service and Support
- Monitor, Evaluate and Assess

Even though the names have changed, the management domains are in line with the four equivalent domains of CobiT 4.1.

3. Process Model and Areas

CobiT 5.0 has 36 processes (CobiT 4.1 has 34). A few processes from CobiT 4.1 are merged in 5.0 and some single processes from 4.1 are split to form separate processes in 5.0 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.

4. 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< http://www.iso.org/iso/iso_catalogue.htm >, ITIL< http://www.itil-officialsite.com/ >, PMBOK< http://www.pmi.org/PMBOK-Guide-and-Standards.aspx >, TOGAF< http://www.opengroup.org/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.

5. 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< http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=38932 > 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

0 – Incomplete Process
1 – Performed Process
2 – Managed Process
3 – Established Process
4 – Predictable Process
5 –Optimizing Process

6. 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 5.0.

7. Enablers

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

- Processes
- Principles and Policies
- Organization structure
- Skills
- Culture
- Service Capability (from ITIL v3) and
- Information.

8. Control Objectives

Unlike the 210 control objectives in CobiT 4.1, there is no separate mention of control objectives in 5.0; such objectives are part of 208 management and governance practices. CobiT 5.0 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 5.0.

Section	Parameter	CobiT 4.1	CobiT 5.0
1	Driver	Best Practices	Stakeholder Expectations & Value
2	Domains Areas	4 Domain Areas	5 Domain Areas. Though domain names are different they align with the domains in 4.1
3	Process Areas	34 Processes	36 Processes
4	Framework	Only CobiT 4.1 Framework	Integrated framework – Val IT, Risk IT, ITAF, BMIS etc. with CobiT 4.1
5	Capability / Maturity Model	Maturity Model	Process Capability Model
	Goals Cascade	IT goals are derived from business goals of maintaining enterprise reputation and leadership	IT goals are derived from stakeholders needs and expectations
6	Enablers	No mention of Enablers	Identified 7 Enablers
7	Control Objectives	210 Control Objectives	No separate mention of control objectives but included as part of

IMPLEMENTING CobiT 5.0

It will be easier for an organization to start fresh with 5.0 than to transition from 4.1. Rebuilding the entire IT governance structure may be easier and more cost effective if an organization is at maturity level 2 or below, where processes are ad hoc, undefined and undocumented.

However, if an organization has heavily invested in 4.1 initiatives, they can align to 5.0 later after or arriving at a logical closure point. They can still leverage existing 4.1 documents with certain modifications to satisfy 5.0 requirements. The main difference will be to structure the processes from 4.1 into the governance and management domain.

CobiT 5.0 is comprehensive and voluminous; each organization should use relevant portions and customize to meet their specific objectives based on stakeholder needs and expectations.

CobiT 5.0 will make significant contributions to enterprise governance. With proper transition planning, the overall costs to the organization should be minimal and the benefits of great value.

* * *

Pritam Bankar< http://www.linkedin.com/in/pritambankar >, CISA, CISM is solution lead at Infosys< http://www.infosys.com >, a leading infrastructure security & compliance practice. He has more than eight years of experience and has led several IT strategy consulting engagements in the areas of information security, audits, compliance & regulations and IT Governance. Pritam has been a regular presenter at thought-leadership conferences and his articles are published in various information-security journals. He is also an active member of Cloud Control Matrix at Cloud Security Alliance< https://cloudsecurityalliance.org/research/ccm/ > forum and ISACA. Pritam holds a Master's degree in information systems in addition to a Bachelor's degree in engineering from Mumbai University< http://www.mu.ac.in/ >, India.

* * *

M. E. Kabay,< mailto:mekabay@gmail.com > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He Professor of Computer Information Systems in the School of Business and Management at Norwich University. Visit his Website for white papers and course materials.< http://www.mekabay.com/ >

* * *