Recommendation for IT Governance Using the COBIT 4.1 Framework

William F. Slater, III, MBA, M.S., PMP, CISSP, CISA

Week 7 Assignment

CYBR 615 – Cybersecurity Governance and Compliance

January 27, 2013

Agenda

- Key Trends that Will Shape the Future of IT
- What is IT Governance?
- Recommendations for IT Governance
- Common Pitfalls of IT Governance
- Recommendations for COBIT-based IT Governance
- COBIT 4.1 vs. COBIT 5.0
- Conclusion
- References

Key Trends That Will Shape the Future of IT

- Measuring and Managing **EVERYTHING**
- Controlling Costs of **EVERYTHING**
- Optimization of **EVERYTHING**
- Automation of **EVERYTHING** using smart applications and smart hardware
- Trying to be as "GREEN" as possible in **EVERYTHING**
- Trying to get **EVERYTHING** done with as few people as possible, even ZERO people
- **EVERYTHING** will be under Risk Management and Information Security management (i.e. ISO 27001)
- **EVERYTHING** will be under Service Management (i.e. ITIL and ISO 20000)
- Continuous Process Improvement in **EVERYTHING**
- Watch word: Save Your Company Money by optimizing **EVERYTHING**, continually improving **EVERYTHING** and adding business value
- The move to the Cloud to save money and increase efficiencies will continue to INCREASE
- **EVERYTHING** will be subject to compliance and **AUDITING**
- **EVERYTHING is "On the Table"**

What Is IT Governance?

- IT Governance is a management-backed initiative that will implement a structured framework that will allow management to strategically align, measure, and manage Information Technology resources in a way that will increase their visibility and value to the business, which reducing risk and providing a means of continual improvement.
- IT Governance requires strong management and management support to be successful

IT Governance Focus Areas

- **Strategic alignment** focuses on ensuring the linkage of business and IT plans; defining, maintaining and validating the IT value proposition; and aligning IT operations with enterprise operations.
- **Value delivery** is about executing the value proposition throughout the delivery cycle,
- ensuring that IT delivers the promised benefits against the strategy, concentrating on optimizing costs and proving the intrinsic value of IT.
- **Resource management** is about the optimal investment in, and the proper management of, critical IT resources: applications, information, infrastructure and people. Key issues relate to the optimization of knowledge and infrastructure.
- **Risk management** requires risk awareness by senior corporate officers, a clear understanding of the enterprise's appetite for risk, understanding of compliance requirements, transparency about the significant risks to the enterprise and embedding of risk management responsibilities into the organization.
- **Performance measurement** tracks and monitors strategy implementation, project completion, resource usage, process performance and service delivery, using, for example, balanced scorecards that translate strategy into action to achieve goals measurable beyond conventional accounting.

From COBIT 4.1 Guide
By ISACA

Recommendations for IT Governance

- Adopt an IT Governance Framework
- IT Governance requires strong management and management support to be successful
- An IT Governance Framework will
  - Align IT capabilities with business goals and needs
  - Allow IT to be measured and managed in a structured way
  - Increase the value of IT to the organization
  - Reduce risk
  - Allow IT to be continual improved

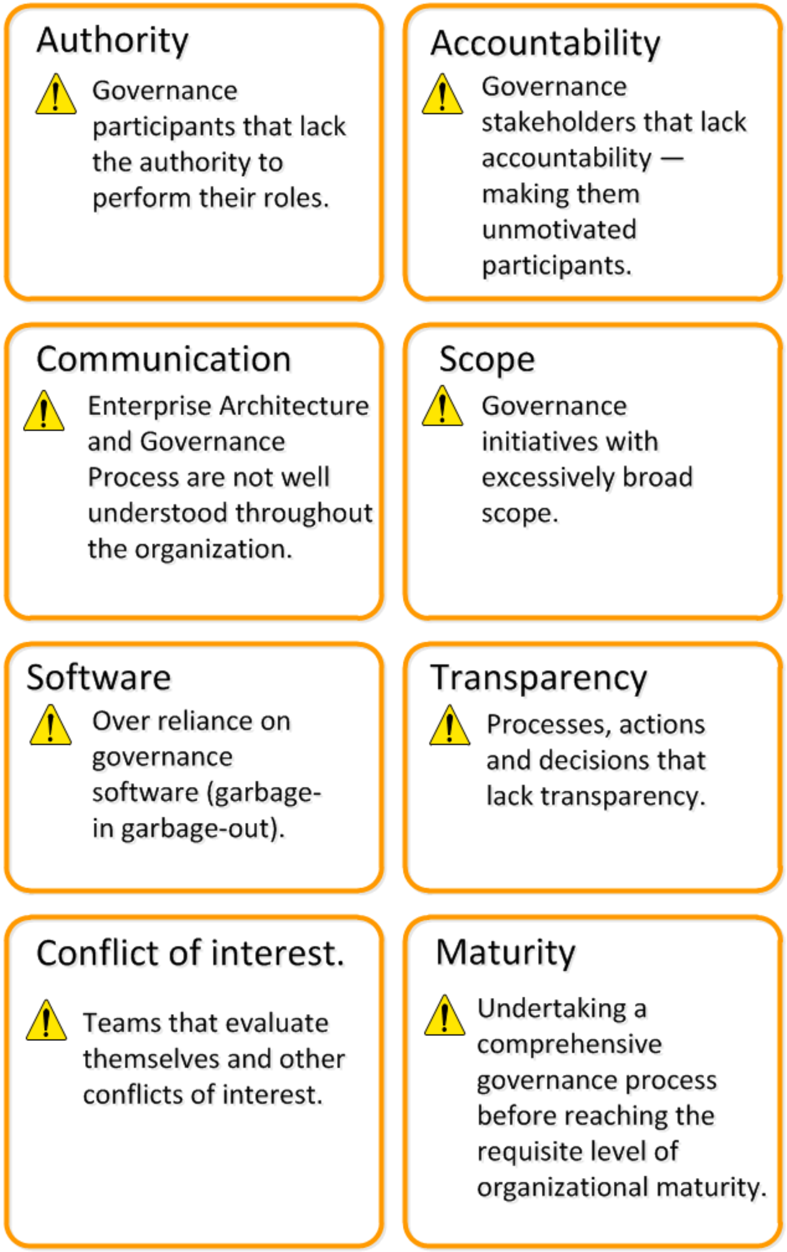
From COBIT 4.1 Guide
By ISACA

Common Pitfalls of IT Governance

- **Who does what now?**
  - Governance participants that lack the authority to perform their roles.
- **I'll get right on it!**
  - Governance stakeholders that lack accountability — making them unmotivated participants.
- **We do the what now?**
  - Key blueprints, standards and best practices that are not well communicated. The challenges in effectively communicating the enterprise architecture is often underestimated. The governance process itself can also be a challenge to communicate.
- **Keen to govern**
  - Governance initiatives with excessively broad scope. The assumption is often made that governance must cover the entire organization. Rolling out a new governance process is challenging and best done incrementally.
- **Magic software**
  - Over reliance on governance software (garbage-in garbage-out).
- **The black box process**
  - Processes, actions and decisions that lack transparency. Transparency facilitates understanding and trust in the governance process.
- **I watch you, you watch me**
  - Teams that evaluate themselves and other conflicts of interest.
- **Maturity please**
  - Organizations that undertake a comprehensive governance process before reaching the requisite level of organizational maturity.

From Simplicable.com

Common Pitfalls of IT Governance



Authority

⚠ Governance participants that lack the authority to perform their roles.

Accountability

⚠ Governance stakeholders that lack accountability — making them unmotivated participants.

Communication

⚠ Enterprise Architecture and Governance Process are not well understood throughout the organization.

Scope

⚠ Governance initiatives with excessively broad scope.

Software

⚠ Over reliance on governance software (garbage-in garbage-out).

Transparency

⚠ Processes, actions and decisions that lack transparency.

Conflict of interest.

⚠ Teams that evaluate themselves and other conflicts of interest.

Maturity

⚠ Undertaking a comprehensive governance process before reaching the requisite level of organizational maturity.

Common IT Governance Pitfalls
© simplicable.com

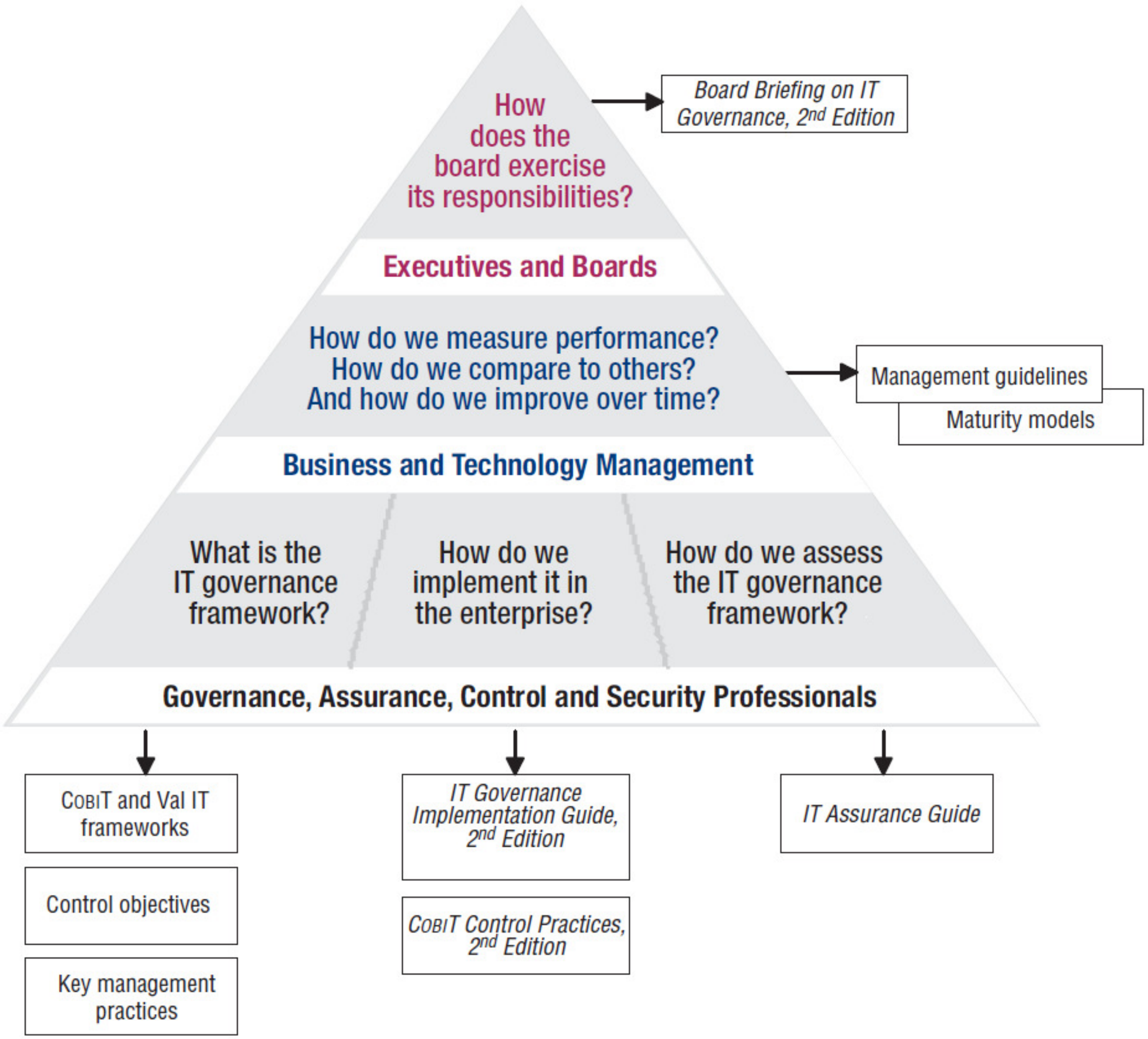
From Simplicable.com

What Is COBIT?

- ISACA's IT Governance Framework
- It is well-structured, easy to follow, and when implemented, it will allow this organization to accomplish each of these objectives:
  - Alignment of IT capabilities with business goals and needs
  - Establishment of performance objectives and Measurement of progress
  - Increase the value of IT to the organization
  - Reduce risk
  - Continual improvement
- Currently on Version 5, but version 4.1 is still in common use

From COBIT 4.1 Guide
By ISACA

The COBIT Top-Down Governance Pyramid



How does the board exercise its responsibilities?

Board Briefing on IT Governance, 2nd Edition

Executives and Boards

How do we measure performance?
How do we compare to others?
And how do we improve over time?

Management guidelines

Maturity models

Business and Technology Management

What is the IT governance framework?

How do we implement it in the enterprise?

How do we assess the IT governance framework?

Governance, Assurance, Control and Security Professionals

CobiT and Val IT frameworks

Control objectives

Key management practices

IT Governance Implementation Guide, 2nd Edition

CobiT Control Practices, 2nd Edition

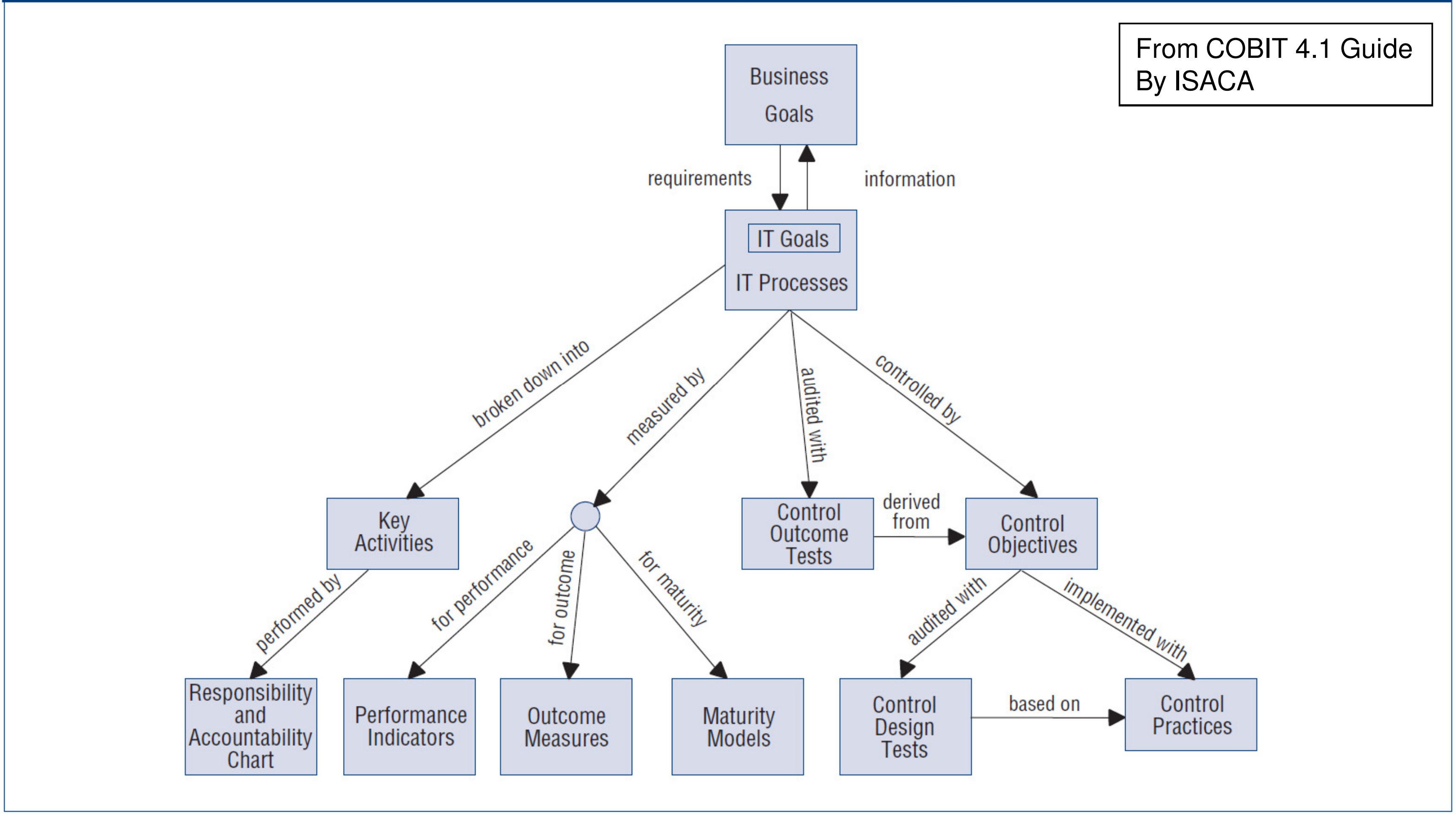
IT Assurance Guide

This CobiT-based product diagram presents the generally applicable products and their primary audience. There are also derived products for specific purposes (*IT Control Objectives for Sarbanes-Oxley, 2nd Edition*), for domains such as security (CobiT *Security Baseline* and *Information Security Governance: Guidance for Boards of Directors and Executive Management*), or for specific enterprises (CobiT *Quickstart* for small and medium-sized enterprises or for large enterprises wishing to ramp up to a more extensive IT governance implementation).

From COBIT 4.1 Guide
By ISACA

COBIT Components: The Interrelationships

Figure 4—Interrelationships of CobiT Components



From COBIT 4.1 Guide
By ISACA

COBIT’s Information Criteria

- **Effectiveness** deals with information being relevant and pertinent to the business process as well as being delivered in a timely, correct, consistent and usable manner.
- **Efficiency** concerns the provision of information through the optimal (most productive and economical) use of resources.
- **Confidentiality** concerns the protection of sensitive information from unauthorized disclosure.
- **Integrity** relates to the accuracy and completeness of information as well as to its validity in accordance with business values and expectations.
- **Availability** relates to information being available when required by the business process now and in the future. It also concerns the safeguarding of necessary resources and associated capabilities.
- **Compliance** deals with complying with the laws, regulations and contractual arrangements to which the business process is subject, i.e., externally imposed business criteria as well as internal policies.
- **Reliability** relates to the provision of appropriate information for management to operate the entity and exercise its fiduciary and governance responsibilities.

From COBIT 4.1 Guide
By ISACA

Recommendations for COBIT-based IT Governance

- COBIT is a mature IT Governance Framework that offers many measurable benefits
- Adoption of COBIT will allow this organization to achieve the following goals
  - Alignment of IT capabilities with business goals and needs
  - Establishment of goals, and measurement oand management of IT in a structured way
  - Increase the value of IT to the organization
  - Risk reduction
  - Continual improvement of IT

From COBIT 4.1 Guide
By ISACA

COBIT 4.1 vs. COBIT 5.0

- COBIT 5.0 is very similar to COBIT 4.1, except that is more prescriptive on the use of Balanced Scorecards, measurement, management, and continual improvement.

Conclusion

- IT Governance offers the best hope for well-managed IT Resources.
- IT Governance requires strong management and management support to be successful
- COBIT is well-structured, easy to follow, and when implemented, it will allow this organization to accomplish each of these objectives:
  - Alignment of IT capabilities with business goals and needs
  - Establishment of performance objectives and Measurement of progress
  - Increase the value of IT to the organization
  - Risk reduction
  - Continual improvement

From COBIT 4.1 Guide
By ISACA

References

- ISACA. (2012) The ISACA website. Retrieved from on http://ww.isaca.org on December 15, 2012.
- Simplicable.com (2011). 8 Common IT Governance Pitfalls. Retrieved from www.simplicable.com on May 15, 2011.

References

- ISO. (2006). ISO 17021 - Conformity assessment ⍰ Requirements for bodies providing audit and certification of management systems. Retrieved from http://isiri.org/portal/File/ShowFile.aspx?ID=746a125a-d702-477e-8e23-165d321dd57a on July 18, 2011.
- ISO. (2011). ISO 19011 - Guidelines for auditing management systems. Retrieved from http://www.cnis.gov.cn/wzgg/201202/P020120229378899282521.pdf on July 18, 2011.
- LaChapelle, E. (2011). ISO 27001 Lead Auditor Course Material from PECB (www.pecb.org). From a course delivered in Dallas, TX in July 2011.
- Lincke, S. (2011). The Small Business Information Security Workbook. Retrieved from http://itm.iit.edu/netsecure11/SusanLincke_SmallBizSecWorkbook.pdf on May 15, 2012.
- SANS. (2012. SANS IT Audit Courses. Retrieved from http:// it-audit.sans.org on December 14, 2012.
- Senft, S., et al. (2013). Information Technology Control and Audit, fourth edition.Boca Raton, FL: CRC Press.
- THEIIA. 2012. The Institute of Internal Auditors. Retrieved from https://na.theiia.org/certification/cia-certification/pages/cia-certification.aspx on December 16, 2012.
- Wikipedia. (2012). Information Technology Audit. Retrieved from http://en.wikipedia.org/wiki/Information_technology_audit on December 15, 2012.
- Wright, C. S. (2007). A Taxonomy of Information Systems Audits Assessments and Reviews. Retrieved from http://www.sans.org/reading_room/whitepapers/auditing/taxonomy-information-systems-audits-assessments-reviews_1801 July 23, 2007.