

IT Governance by Examples (based on Cobit 4.1)

By

Kent Ka lok Tong

Copyright © 2011

TipTec Development

Publisher: TipTec Development

Author's email: freemant2000@yahoo.com

Book website: <http://www.agileskills2.org>

Notice: All rights reserved. No part of this publication may be reproduced, stored in a retrieval system or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, without the prior written permission of the publisher.

ISBN: 978-1-4357-8868-8

Edition: First edition January 2011

Foreword

How to maximize the value of IT to your company?

If you're a CIO or an IT manager who would like to maximize the value of IT to your company, then this book is for you. It explains a framework of the best practices (Cobit) for IT to strategically align with the business, to deliver business values at low costs with low risks, using concrete and easy-to-understand examples.

Why should you choose this book?

- It uses concrete examples to demonstrate the true meaning of the abstract concepts.
- It is concise. There is no lengthy, abstract description.
- Free sample chapters are available on <http://www.agilekills2.org>. You can judge it yourself.

Target audience and prerequisites

This book is suitable for:

- CIOs who would like to learn Cobit and/or to enhance their current governance framework with Cobit.
- IT managers who would like to learn the best practices in IT governance to further advance their career.
- IT team leaders who would like to learn the core concepts in IT management.

In order to understand what's in the book, you need to know the basic purposes of the common IT applications and technologies such as CRM, collaboration platform, e-learning, POS, Windows, Linux, OS, web server, database server, firewall, etc. You do NOT need to know any technical details. You do NOT need any formal management knowledge either.

Organization of the book

The book is organized into four parts:

1. Chapters 1-10: They are about strategic or long term planning and defining the fundamental elements of the framework.

2. Chapters 11-18: They are about the introduction of IT solutions (evaluating, buying, developing, implementing).
3. Chapters 19-31: They are about operating and supporting the IT services.
4. Chapters 32-35: They are about the overall evaluation of how well you're doing.

Acknowledgments

I'd like to thank:

- Helena Lei for suggesting that I write this book.
- Eugenia Chan Peng U for doing book cover and layout design.

Table of Contents

Foreword.....	3
How to maximize the value of IT to your company?.....	3
Why should you choose this book?.....	3
Target audience and prerequisites.....	3
Organization of the book.....	3
Acknowledgments.....	4
Chapter 1 Strategic IT Planning.....	11
What is strategic IT planning?.....	12
Costs and resources.....	12
Risks.....	13
Control objective.....	13
Maturity level.....	13
Chapter 2 Defining Information Architecture.....	15
Creating, maintaining and using information for the business.....	16
Keeping information correct.....	16
Keeping information consistent.....	16
Keeping information secure.....	17
Making sure the information & the processing system are available.....	17
Archiving or removing the information.....	17
Delegating the management responsibility of information.....	17
Information architecture.....	18
Chapter 3 Determining Technological Direction.....	19
The need for enterprise wide standardized technologies.....	20
What about legacy technologies?.....	21
Looking forward and updating your standardized technologies.....	21
Chapter 4 Defining IT Processes.....	23
What is a process?.....	24
Seeking support.....	24
Continuous care and delegation.....	25
Defining IT processes.....	25
Chapter 5 Defining IT Organization and Relationships.....	27
The CIO job position and relationships.....	28
Other strategic positions in IT and relationships.....	28
Protecting from the loss or malfunctioning of key individuals.....	28

Chapter 6 Managing IT Investments.....	31
Forecasting (planning) the business values and costs.....	32
Tracking the costs.....	33
Tracking the business values.....	33
Quantifying business values.....	34
Chapter 7 Communicating Management Aims and Direction.....	35
Defining or maintaining IT policies, standards and procedures	36
Rolling out the IT policies, standards and procedures.....	37
Compliance.....	37
Chapter 8 Managing IT Human Resources.....	39
It is the people who will make or break the IT capability.....	40
People tending to comply by laws and ethics.....	40
People with the right skills.....	41
People with the right attitudes.....	41
Motivating people.....	41
Chapter 9 Managing Quality.....	43
What is quality?.....	44
How to ensure quality?.....	44
Ensuring quality throughout the whole enterprise.....	45
Summary.....	45
Chapter 10 Managing IT Risks.....	47
Life could be at stake.....	48
Identifying and assessing the risks.....	48
Mitigating the risks.....	49
Transferring the risks.....	49
Monitoring and reviewing the risks.....	50
Chapter 11 Managing Projects.....	51
Scope, cost and schedule.....	52
Good planning.....	52
Uncertainties, changes, monitoring and control.....	53
Quality as the 4th major constraint.....	54
Keeping the sponsor happy to fuel the project.....	54
Getting long lasting benefits out of the project.....	54
Coordination between projects.....	55
Adopting and tailoring a project management framework.....	55
Chapter 12 Identifying Automated Solutions.....	57
Buy or build.....	58
Breaking the system into small pieces.....	58

Narrowing the uncertainties.....	59
Presenting the result.....	59
Chapter 13 Acquiring and Maintaining Application Software.....	61
Determining the architecture of the application.....	62
Determining the component structures for features.....	62
Managing quality.....	62
Maintaining a business focus.....	63
Controlling the scope.....	63
Configuring and implementing the application.....	64
Preventing tampering to the database.....	64
Maintenances and major upgrades.....	64
3rd party software.....	65
Chapter 14 Acquiring and Maintaining Technology Infrastructure.....	67
Acquiring and implementing required infrastructure.....	68
Ensuring availability.....	68
Change management.....	68
Ensuring security.....	69
Chapter 15 Enabling Operation and Use.....	71
Transferring the knowledge.....	72
Chapter 16 Procuring IT Resources.....	73
Procurement procedures and strategies.....	74
Selecting a supplier.....	75
Establishing a contract.....	75
Managing the contract.....	75
Chapter 17 Managing Changes.....	77
Changes.....	78
Change management.....	78
Chapter 18 Installing and Accrediting Solutions and Changes....	81
Risks with solution deployments.....	82
Testing in a test environment.....	82
User acceptance testing.....	82
Implementation plan.....	83
Parallel versions.....	83
Post implementation review.....	84
Deploying changes.....	84
Chapter 19 Defining and Managing Service Levels.....	85
Defining indicators for the quality of IT services.....	86
Designing for availability.....	87

Providing service continuity after disasters.....	87
Monitoring if the SLA is met.....	88
Reviewing the SLA, OLA and UC.....	88
Chapter 20 Managing Third Party Services.....	89
Managing 3rd party IT services.....	90
Supplier relationship management.....	91
Risks due to lack of transparency.....	92
Chapter 21 Managing Performance and Capacity.....	93
Designing for performance.....	94
Designing for capacity.....	94
Planning for the future.....	94
Planning for abnormal times.....	95
Planning for life cycles of the IT resources.....	95
Monitoring and reporting.....	95
Chapter 22 Ensuring Continuous Services.....	97
Disaster recovery plan.....	98
Testing the plan.....	100
Making the plan available.....	100
Maintaining the plan.....	100
Reviewing.....	100
Creating an IT continuity framework.....	100
Chapter 23 Ensuring Systems Security.....	103
Identity management.....	104
Attacks from those without an identity.....	105
Responding to security incidents.....	106
Exchanging sensitive data.....	106
Cryptographic keys as identities.....	106
Security testing.....	107
IT security plan and management support.....	107
Chapter 24 Identifying and Allocating Costs.....	109
Presenting the IT budget.....	110
Calculating the cost for an IT service.....	110
Enabling customer choices on the demand side.....	113
Monitoring and review.....	114
Chapter 25 Educating and Training Users.....	117
Training for new users.....	118
Ensuring the training objective is met.....	119
Training for existing users.....	119
Training for new IT services.....	119

Different curricula for different user groups.....	119
Updating the curriculum for new business needs.....	119
Improving the training.....	120
Chapter 26 Managing Service Desk and Incidents.....	121
Establishing a service desk to ensure value delivery.....	122
Taking ownership.....	122
Prioritizing incidents.....	122
Keeping the user informed until incident closure.....	123
Using the incidents as feedback for improvements.....	123
Chapter 27 Managing the Configuration.....	125
Configuration repository.....	126
What information to store in the CMDB?.....	127
Keeping the information updated.....	127
Keeping license information.....	128
Chapter 28 Managing Problems.....	129
Preventing the same incidents in the future.....	130
Prioritizing the problems.....	130
Ownership of the problem.....	130
Identifying the root cause.....	130
Resolving the problem.....	130
Preventing high impact incidents in the future.....	131
Chapter 29 Managing Data.....	133
Managing data in IT operations.....	134
Archiving and purging data.....	134
Backup and restore.....	135
Media library.....	135
Batch processing.....	135
Disposal.....	135
Chapter 30 Managing the Physical Environment.....	137
Providing a good physical environment.....	138
Risks with the physical environment.....	138
Chapter 31 Managing Operations.....	141
Managing IT operations.....	142
Chapter 32 Monitoring and Evaluating IT Performance.....	143
At the end of the day, how well IT is doing?.....	144
Remediation.....	145
Chapter 33 Monitoring and Evaluating Internal Controls.....	147
Are the internal IT controls working?.....	148
Chapter 34 Ensuring Compliance with External Requirements.....	149

Is IT complying with the external requirements?.....	150
Chapter 35 Providing IT Governance.....	151
Are you providing IT Governance well?.....	152
References.....	153
Alphabetical Index.....	154

Chapter 1

Strategic IT Planning



What is strategic IT planning?

Simply put, strategic IT planning is to suggest various IT solutions to support business objectives or strategies. For example, suppose that you are the CIO of a school and that the school has an objective of improving education quality. It may have defined business strategies to achieve that objective like:

- Making learning fun
- Engaging parents
- ...

As the CIO of the school, you could suggest various IT solutions to support one of those strategies. For example, for the first strategy ("Making learning fun"), you may suggest some possible IT strategies:

- Provide educational games to the teachers.
- Provide training to enable teachers to develop interactive courseware.
- Locate and provide the best student-engaging lecture videos to the teachers.
- ...

Note that each IT strategy must have a clear linkage to the business strategy so that it will create business value. For example, it is assumed that educational games will make learning fun because students like playing games.

Value is one of the three major concerns of Cobit and in IT governance in general. Cobit is a popular framework for IT governance. It stands for **Control Objectives for IT**. You'll see what control objective means in the future.

Costs and resources

After coming up with these IT strategies, you will explain them to the CEO (the principal) and business executives (the vice principals) to let them choose which ones to proceed. However, without the information regarding the costs incurred by the needed resources for each IT strategy, it is just impossible to choose (cost is the second major concern of Cobit). So, you have to provide such information. For example, for the IT strategy of providing educational games, you may need:

- \$1,000 (cost) for a site license for each game (software).
- Teachers (people) to attend a training session.
- Technical support team (people) to provide support to the teachers (service).
- A server (hardware) to host the games.
- A certain internal network bandwidth (network).

- ...

Using this information you can estimate the total cost.

For these resources (people, software, hardware, network) to work together, you need processes. For example, for the support service, you need to define a process to handle the support requests; for the server to host the games, you need a process to maintain its security. This supply or implementation side of IT (resources, processes) is called Enterprise architecture for IT in Cobit.

Risks

What if some students become addicted to the games? What if some parents don't want their kids to play games? These risks must be communicated to the CEO and business executives to help them choose which IT strategies to pursue (risk is the third major concern of Cobit).

Control objective

So, you can perform strategic IT planning as described above. But how to ensure the desired output (IT strategies as selected by the CEO will have good value, low cost and low risk) will be produced? For example, there are some success factors:

- You (the CIO) knows the business objectives and strategies well.
- The CEO is willing to make clear decisions.
- You, the CEO and business executives can discuss and negotiate well.
- You can plan (estimate) the costs, risks and other needed resources well.

Each process has its own such success factors and they're key to ensure that the process is effective (producing the desired output) and efficient (producing the output at low cost, at fast speed, etc.). Such success factors are called control objectives in Cobit and is a key concept in Cobit (recall that the term Cobit simply stands for **C**ontrol **O**bjectives for **I**T).

Maturity level

However, even if you're doing the strategic IT planning process very well, it doesn't mean that the process is embedded in the DNA of the organization. For example, if you leave the organization and your successor doesn't do it or does it poorly, then it is not in the DNA of the organization. This is reflected in the "maturity level" of the process:

- Level 0 (No process): The organization has no process at all.
- Level 1 (Ad-hoc): Different people in the organization have different

processes to do the same thing.

- Level 2 (Repeatable): Different people in the organization follow the same process, but the process is informal (not written down), so it is not formally reviewed, approved nor used for training.
- Level 3 (Defined): The process is formally defined.
- Level 4 (Managed): The process is continuously improved.
- Level 5 (Optimized): The process is considered among the best in that industry.

Chapter 2

Defining Information Architecture



Creating, maintaining and using information for the business

Suppose that you're the owner of a retail store. You'd like to use IT to enhance your business (so, you're also acting as the CIO in addition to the CEO). You figure that if some products are missing on shelves, you'll lose business. So, you have to replenish the items on shelves from the storage area promptly and reorder the items if they're running out in the storage area in a just-in-time manner. To do that, you can use a POS system to keep track of the items sold, the items on shelves and in the storage area. That is, you need to create, maintain and use information that is modeling the real world. That's probably the most common purpose of business IT systems.

However, there comes a cost of storing information: you have to take good care of (manage) the information properly otherwise bad things can happen. This is like owning a car or a dog: once you own it, you have to keep it clean, keep it healthy and etc.

Keeping information correct

One problem with storing information is that, if unmanaged, the information can become erroneous. For example, the data in the POS may not match the real world as time goes by, so you need to perform inventory from time to time to reconcile them (a process to keep information correct).

Keeping information consistent

Another problem is that information, if it is duplicate, will become inconsistent. For example, while the POS system contains the information about your suppliers, you may also need to input such information into your accounting system for the accounts payable. Why is this a problem? Let's say if a supplier changes his address and informs you, you will have to update it in both the POS system and the accounting system. If you forget to do either, the information will become inconsistent.

How to solve this problem? The ideal solution is to not duplicate the data. For example, if both the POS system and the accounting system support it, they could be put into the same database but in different schemas (one schema for each application), while storing the supplier information into a third schema to be shared. If this is not supported (some applications may not allow you to specify the schema), you may have to synchronize the supplier information somehow between two databases. Both approaches can be considered enterprise-wide data coordination between different applications, departments or processes.

Keeping information secure

In addition, once keeping the information, you must keep it secure. For the information regarding the product items, it is not that confidential (confidentiality is one aspect of information security), but you must prevent ordinary users or other people from changing their retail prices (integrity is the second aspect of information security). For the financial information (accessed through the accounting system), reports like profit and loss should be confidential and accessible to the management of the company only.

Making sure the information & the processing system are available

As the operation of your business now relies on the POS system to read and update the product item information, if the database (information) or the POS system (processing system) breaks, your business will be severely hindered. Therefore, you must ensure the availability of the database and the POS system (availability is the third aspect of information security).

How to do that? You should conduct backups of the database and the POS system and practice restorations regularly. You could also consider redundant hardware (e.g., RAID, fault-tolerant server, dual power supply), redundant power (UPS or power generator), redundant systems (e.g., database replication, server cluster) and disaster recovery planning.

Archiving or removing the information

Finally, for better performance of the system or to save space, you may want to archive the information to a long term storage (e.g., DVD) as historical records.

In some companies, if the law requires that the information be kept for a certain years, they will remove that information after meeting that requirement in case that the information could be used against them in court (just think the Hong Kong celebrity Edison Chen who failed to really delete his photos in his laptop!).

Delegating the management responsibility of information

As there is a lot of different information in the company, it is difficult to depend on you, an individual, to decide how much care should be put on that information (How strong should the access control be? How long to keep the information? How much availability?). Therefore, for each type of information (e.g., financial information, product information), you (acting as the compliance officer or chief security officer) should ensure that there is a process to assign someone as the owner of that information, then let him decide how much

management care is required. Usually, this can be done by classifying the data (e.g., in security: top secret, confidential, internal use, public. In availability: highly available, important, normal, rarely needed).

Information architecture

In summary, to support the business, you plan what information to create, maintain and use, how to keep it correct, consistent (sharing or synchronizing), secure (confidential, untempered, available), when and how to archive or remove it. The processes, methods and documents you create to achieve the above purposes (properly managing the information) are called the information architecture for the enterprise.