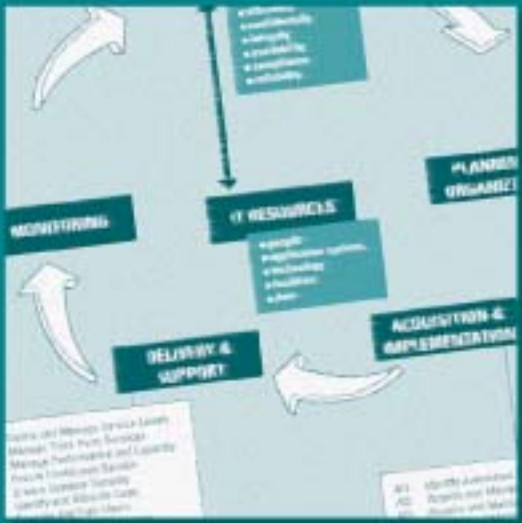
IT GOVERNANCE

IT Governance

a pocket guide

BASED ON CoBiT®



POCKET SERIES

COLOPHON

Title: IT Governance - A Pocket Guide, based on COBIT®

Authors: Koen Brand & Harry Boonen

Chief editor: Jan van Bon (Inform-IT, *editors & innovators*, the Netherlands)

International Review Team:
Rolf Akker, BHVB, the Netherlands (*previewer*)
Menno Arentsen, Ernst & Young EDP Audit, the Netherlands (*previewer*)
Raoul Assaf, ARTUTA, Argentina
David Aveiro, Organizational Engineering Center, Portugal
Gustav van den Berg, UWV, the Netherlands (*previewer*)
Pierre Bernard, Pink Elephant, Canada
David Bingham, Fujitsu Consulting, UK
Michael Böcker, Serima Consulting GmbH, Germany
József Borda, CISA, Hunaudit Ltd., Hungary
Maarten Bordewijk, PinkRoccade Educational Services, the Netherlands
Gerard Brantjes, Brantjes Advies Buro, the Netherlands
Luigi Buglione, École de Technologie Supérieure (ETS) - Université du Québec, Canada
Jeff Carter PMP, MSFmentor, USA
Marien de Clercq, University Centre for Information Technology - University of Nijmegen, the Netherlands
Rod Crowder, OpsCentre, Australia
Dr Brian Cusack, Auckland University of Technology, New Zealand
Kim Delgadillo, IBM Business Consulting Services, Belgium
Helga Dohle, exagon consulting & solutions gmbh, Germany
Ton Dohmen, PriceWaterhouseCoopers, the Netherlands (*previewer*)
Troy DuMoulin, Pink Elephant International, Canada
Isaac Eliahou, AtosOrigin, the Netherlands (*previewer*)
Martin Erb, USA
Péter Füzi, Salix Informatikai Bt, Hungary
Wolfgang Goltsche, Siemens Business Services, Germany
Vincent Haenecour, Consultis, Belgium
Oscar Halfhide, LogicaCMG, the Netherlands
Franz J. Hareter, Skybow AG, Switzerland
Hussein Hassanali Haji, Sidat Hyder Morshed Associates (Pvt.) Ltd., Pakistan
Peter Hill, Info Sec Africa, South Africa
Ton van den Hoogen, Tot Z BV, the Netherlands
Göran Jonsson, Sweden
Jörn Kettler, Serima Consulting GmbH, Germany
Sergei Konakov, 5-55, Russia
Ben Kooistra, Capgemini, the Netherlands

Nicolay Krachun, Motorola GSG, Russia
Emmanuel Lagouvardos, CISA, Emporiki Bank,Greece
Alexandre Levinson, Tolkin, France
Peiwei Lu, SinoServiceOne Ltd, P.R.China
Steve Mann, SM2 Ltd, UK
Luis F. Martínez, Abast Systems, Spain
Jos Mertens, PlanIT, Belgium
Cees Michielsen, Océ-Technologies BV, the Netherlands
Peter Musgrave, Reccan Ltd, UK
Fred van Noord, GvIB Society for Information Security professionals, the Netherlands
Peter Palatinus, Hewlett-Packard GmbH, Germany
Michael Parkinson, KPMG, Australia
Antonio de Pastors, Synstar Computer Services, Spain
Vladimir Pavlov, eLine Software Inc., Ukraine
Gert van der Pijl, Erasmus University/Eurac, the Netherlands (*previewer*)
Karel van der Poel, Mirror42, the Netherlands (*previewer*)
Gerrit Post, the Netherlands (*previewer*)
Michael Pototsky, IT Expert, Russia
Sylvie Prime Van Parys, CRP Henri Tudor, Luxembourg
Ferran Puentes, Abast Systems, Spain
Max Shanahan, Max Shanahan & Associates, Australia
Andie Shih, ITIL International Examination Agency - North America
Ron Sintemaartensdijk, Sogeti Nederland, the Netherlands
Helen A. Sotiriou CISA, Emporiki Bank, Greece
Peter Spermon RE RI CISA, Inspectie Werk & Inkomen (IWI), the Netherlands
Rainer Sponholz, Ernst & Young AG, Germany
Heather Stebbings MSc. DMS, CSTC Consulting, UK
Fred Steenwinkel, VRO/IIA, the Netherlands (*previewer*)
Philip Stubbs, Sheridan Insititute of Technology and Advanced Learning, Canada
Ruedi Stucki, Zurich Financial Services, Switzerland
Maxim Taradin, JSC Vimpelcom (Beeline™), Russia
Karin Thelemann, Ernst & Young AG, Germany
Sascha Thies, exagon consulting & solutions gmbh, Germany
Antonio Valle, Abast Systems, Spain
Wiley Vasquez, BMC Software, USA
Han Verniers, LogicaCMG ICT Management, the Netherlands (*previewer*)
Jurgen van der Vlugt, ABN AMRO Bank, the Netherlands
Clemens Willemsen, KIBO, the Netherlands (*previewer*)
Conn Wood, Foster-Melliar, South Africa

People marked with '(*previewer*)' are members of the core project team and contributed to de design of this Pocket Guide

Publisher: Van Haren Publishing (info@vanharen.net)

ISBN: 90-77212-19-1

Editions: First impression, second edition, September 2004

Design & Layout: DTPresto Design & Layout, Zeewolde-NL

TABLE OF CONTENTS

FOREWORD

This IT Governance Pocket Guide is the result of a project that involved many experts from all over the world. It started out as a compact reference to one framework, but it grew into an original document on IT Governance, building on many pieces of knowledge from various sources, going back into the sources of these sources, and adding pieces to the puzzle.

The project started out in the Netherlands, where a dedicated preview team designed the initial structure of this guide. In the course of the project, a huge amount of material was made available by an international team of reviewers from all kinds of origin, ranging from highly experienced practitioners in the auditing business, to presidents of ISACA chapters and academics, and to skilled IT Service Management experts and trainers. The rare combination of knowledge that was collected, enabled the development of a new instrument that will fit both worlds: Auditing and IT Service Management. It will offer the auditors a bridge to the service management business - the new wave in IT - and it will offer the service management world its long desired next step: a management instrument that enables them to put the pieces of the puzzle together, get a clear picture, and get - and stay - *in control*.

And that is what we're after: to be in control. Not only because new rules force us to do so, but also because it will bring some meaning to all the effort that was spilled on the way getting here.

And although it definitely will not be 'the silver bullet', I do think this publication can bring us one big step ahead.
This guide is part of a project that will also produce a new infrastructure of training and certification facilities, as well as new initiatives in supporting software tools, and complementary guidance.
I sincerely hope you will enjoy the efforts of the team.

Any comments and suggestions regarding the content of this pocket guide are welcomed by the project team. Please mail to j.van.bon@inform-it.org

Jan van Bon,
chief editor

1 Introduction to IT Governance & CobiT

Introduction

This book provides an overview of IT Governance in a handy pocket guide format.

It is provided for two purposes. First, it is a quick-reference guide to IT Governance for people that are not acquainted with this field of work. Second, it is a high-level introduction to ITGI's[1] open standard 'CobiT' that will encourage further study. Please note that this guide follows the process structure of CobiT, since we found that to be best practice, but it differs from CobiT in several ways, adding new information to the structure, from the perspective of IT Service Management.

The pocket guide is aimed at Business and IT (Service) Managers, Consultants, Auditors and anyone interested in learning more about the possible application of IT Governance standards in the IT management domain. In addition, it provides students in IT and Business Administration with a compact reference to CobiT.

After an introduction to IT Governance and CobiT in general, you will find information about ITGI's CobiT publications, since we encourage the use of CobiT. In the next section, you will find a description of the 34 processes that were identified from many international standards. This Pocket Guide adds new information to the various sources that were used to describe IT Governance, including CobiT. Workflow diagrams and process models have been added as an extension to existing material. A full set of detailed descriptions will be made available in 'IT Governance - An Introduction', the training book that follows this pocket guide in 2004. The last part of the book provides some guidance on CobiT implementation and the relationship with other methods and frameworks.

1)The ITGI as a not-for-profit organization has made CobiT an Open Standard with the majority of documents available for free download from the Internet to encourage wide adoption, however reproduction of any of the CobiT content for commercial use is not permitted without the ITGI's prior consent.

Context

In a book about IT Governance it is sensible to analyse the position of IT Governance in relation to other governance frameworks. The most comprehensive framework encountered in literature is in a discussion paper by the Chartered Institute of Management Accountants (CIMA). In this paper Enterprise Governance is a term used to describe a framework that covers both the *Corporate Governance* and the *Business Governance* aspects of the organisation.

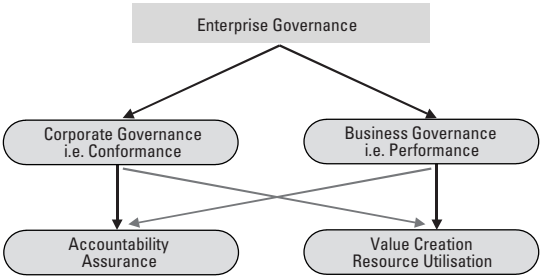


Figure 1.1 The Enterprise Governance framework (Source: CIMA)

CIMA uses the following definition of *Enterprise Governance*:

> *'Enterprise Governance is the set of responsibilities and practices exercised by the board and executive management with the goal of providing strategic direction, ensuring that objectives are achieved, ascertaining that risks are managed appropriately and verifying that the enterprise's resources are used responsibly (CIMA, referencing ISACF®).'*

According to CIMA there are two dimensions of Enterprise Governance: conformance and performance. In general, the conformance dimension is approached in the *ex post* (retrospective) view, while

the performance dimension is approached in the *ex ante* (prospective) view.

The lines in figure 1.1 show that, although conformance feeds directly to accountability & assurance and performance to value creation & resource utilisation, conformance can also feed to value creation & resource utilisation while performance can feed to accountability & assurance.

Corporate Governance, as the conformance dimension of Enterprise Governance, has had significant coverage following the recent corporate scandals. In the wake of these scandals, which also included the demise of one of the Big Five accountancy firms, new regulations designed to strengthen Corporate Governance were introduced in the US, in Europe and in many other jurisdictions. In the US the Sarbanes-Oxley Act was introduced for this reason. In Europe the Winter Report issued recommendations to provide for a modern regulatory framework for company law to the European Commission.

Among its recommendations is that companies that are traded on open markets provide a coherent and descriptive statement covering the key elements of Corporate Governance rules and practices in their annual report and on their web site.

The Organisation of Economic Co-operation and Development (OECD) defines *Corporate Governance* in the following way:

> *Corporate Governance is the system by which business corporations are directed and controlled. The Corporate Governance structure specifies the distribution of rights and responsibilities among different participants in the corporation, such as the board, managers, shareholders and other stakeholders, and spells out the rules and procedures for*

making decisions on corporate affairs. By doing this, it also provides the structure through which the company objectives are set, and the means of attaining those objectives and monitoring performance. (OECD)

The importance of good Corporate Governance is recognised worldwide. It must lead to improved responsiveness to shareholder interest by attempting to balance the CEO's power with the board's ability to act as genuine custodians of the organisation.

Business Governance, as the performance dimension of Enterprise Governance, focuses on the board's role in making strategic decisions, risk assessment and understanding the drivers for business performance.

The attention to Corporate Governance also raises the question whether the IT used for supporting business processes is adequately controlled. This leads to an increase in attention for IT Governance in many organisations. Because IT is an integral part of business operations, IT Governance is an integral ingredient of Corporate Governance.

IT Governance has been defined in many different ways. In this publication IT Governance is defined as follows:

IT Governance is the system by which IT within enterprises is directed and controlled. The IT Governance structure specifies the distribution of rights and responsibilities among different participants, such as the board, business and IT managers, and spells out the rules and procedures for making decisions on IT. By doing this, it also provides the structure through which the IT objectives are set, and the means of attaining those objectives and monitoring performance.

Corporate Governance	Business Governance	IT Governance
Separation of ownership and control	Direction and control of the business	Direction and control of IT
Ex post	*Ex ante*	*Ex ante*
• Duties of Directors/ Leaders • Legislative/Fiduciary Compliance & Control • Shareholder Rights • Ethics & Integrity • Business Operations, Risks & Control • Financial Accounting & Reporting • Asset Management • Risk Management	• Business Goals & Objectives • Business Strategy & Planning • Business Activities & Processes • Innovation & Research Capabilities • Knowledge & Intellectual Capital • Information & its Management • Human Resources Management • Customer Service & Relationships • In- and External Communication • Performance Control	• IT Objectives • Alignment with Enterprise Objectives • IT Resources • Information Knowledge Management • IT Strategy & Planning • IT Acquisition & Implementation • IT Operations, Risks & Control • IT Asset Management • IT Risk Management

Table 1.1 Governance characteristics

Table 1.1, on the previous page, compares the most important characteristics of Corporate Governance, Business Governance and IT Governance within Enterprise Governance.

IT Governance ensures that IT is properly aligned with business processes and is properly organised and controlled. IT Governance provides the structure that links IT processes, IT resources and information to enterprise strategies and objectives.

IT Governance integrates and institutionalises best practices of planning, organising, acquiring, implementing, delivering, supporting, and monitoring IT performance, to ensure that the enterprise's information and related technology support its business objectives. IT Governance enables the enterprise to take full advantage of its information, thereby maximising benefits and capitalising on opportunities thus leveraging competitive advantage.

Sources for IT Governance

Regarding governance there are several sources that provide basic knowledge. In the following paragraphs some background on the major sources is presented.

COSO

In 1992, the Committee of Sponsoring Organizations of the Treadway Commission issued '*Internal Control - Integrated Framework'*. This publication established a framework for internal control and provided evaluation tools which business and other entities can use to evaluate their control systems (figure 1.2).

The framework identifies and describes five interrelated components necessary for effective internal control.

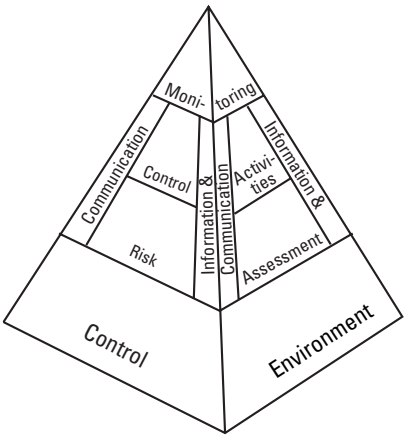


Figure 1.2 COSO Internal Control - Integrated Framework (Source COSO)

In *'Internal Control - Integrated Framework'*, COSO defined internal control as a process, effected by an entity's board of directors, management and other personnel, designed to provide reasonable assurance regarding the achievement of objectives in the following categories:

- Effectiveness and efficiency of operations
- Reliability of financial reporting
- Compliance with applicable laws and regulations.

In 2004 the COSO Enterprise Risk Management (ERM) is to be published. *Enterprise risk management* is broader than internal control, expanding and elaborating on internal control to form a more robust conceptualisation focusing more fully on risk. The enterprise risk management framework expands on the internal control framework as follows:

- Four categories of objectives are specified: *operations*, *reporting*, *compliance* and *strategic objectives*. Reporting now includes reports used internally by management and those issued to external parties. Strategic objectives have been added as a new category.
- ERM considers risk from a 'portfolio' perspective.
- The framework takes into consideration the amount of risk a company is willing to accept to achieve its goals.
- Events that can influence the company are identified. Those that can hold negative impact represent risks.
- Risk assessment is extended.
- ERM identifies four categories of risk response - *avoid*, *reduce*, *share* and *accept*. Responses are being considered both for individual risk effect and for aggregate effect.
- ERM expands on the information and communication component, considering data derived from past, present and potential future events.
- ERM describes the role and responsibilities of risk officers and expands on the role of a company's board of directors.

Code of Practice for Information Security Management (ISO/IEC 17799/BS7799)

ISO 17799 is a code of practice for information security management. This code of practice takes a baseline approach to information security. It provides 127 information security guidelines structured under 10 major headings to enable readers to identify the security controls that are appropriate to their particular business or specific area of responsibility. The standard provides guidance on the following subjects:

- Security policy
- Security organisation
- Asset classification and control
- Personnel security

- Physical and environmental security
- Communications and operations management
- Access control
- System development and maintenance
- Business Continuity management
- Compliance.

BS7799-2 is a companion standard to ISO/IEC 17799. It is a management standard, based on risk assessment and the Plan-Do-Check-Act model, which are two vital ingredients of Corporate Governance. It provides a basis on which to build the management controls necessary to achieve an organisation's mission, to manage risk, to assure effective control and to seek improvements where appropriate.

ITIL

ITIL is the acronym for the 'IT Infrastructure Library' guidelines developed by the CCTA (now OGC) in Norwich, England, for the British government. ITIL is a best practice framework for IT Service Management and is seen as the *de facto* global standard in this area. For example, ITIL provides the foundation for the Microsoft Operations Framework (MOF) and for the HP IT Service Management Reference Model.

ITIL consists of a series of books giving best practice guidance for service management, with the guidelines describing what rather than how. Service management is tailored to the size, the internal culture and the requirements of the company. An important focus is the provision of quality IT services.

Best known ITIL books (figure 1.3) are the **Service Support** book, which describes the Service Desk and the Incident Management, Problem Management, Configuration Management, Change

Management and Release Management processes, and the **Service Delivery** book, which describes processes for Capacity Management, Financial Management for IT Services, Availability Management, Service Level Management and IT Service Continuity Management.

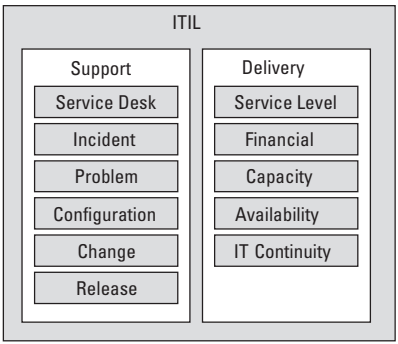


Figure 1.3 Best known ITIL Processes (Note: the Service Desk is not a process but an organisational unit)

The other core ITIL books are shown in figure 1.4.

The book **Planning to Implement Service Management** explains the steps necessary to identify how an organisation might expect to benefit from ITIL and how to achieve these benefits.

The **ICT Infrastructure Management** book is concerned with the processes, organisation and tools needed to provide a stable IT and communications infrastructure.

The **Application Management book** is a guide for business users, developers and service managers, and describes how applications

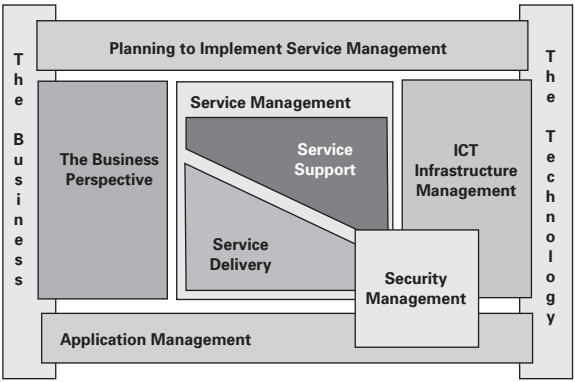


Figure 1.4 The ITIL publication structure (source OGC)

can be managed from a service management perspective.

Security Management is described in a separate book, and has connections with several of the other domains.

The **Business Perspective** book is to be published in 2004, and is concerned with helping business managers to understand IT service provision.

CMM / SPICE (ISO/IEC 15504)

The first Capability Maturity Model was developed by the Software Engineering Institute (SEI) of the Carnegie Mellon University and describes the principles and practices underlying software development process maturity. It was intended to help software organisations improve their software processes by following an evolutionary path from ad hoc, chaotic processes to mature, disciplined software processes. This CMM was organised into five maturity levels:
1. Initial - The software process is characterised as ad hoc, and

occasionally even chaotic. Few processes are defined, and success depends on individual effort and heroics.

2. *Repeatable* - Basic project management processes are established to track cost, schedule, and functionality. The necessary process discipline is in place to repeat earlier successes on projects with similar applications.
3. *Defined* - The software process for both management and engineering activities is documented, standardised, and integrated into a standard software process for the organisation. All projects use an approved, tailored version of the organisation's standard software process for developing and maintaining software.
4. *Managed* - Detailed measurements of the software process and product quality are collected. Both the software process and products are quantitatively understood and controlled.
5. *Optimising* - Continuous process improvement is enabled by quantitative feedback from the process and from piloting innovative ideas and technologies.

Predictability, effectiveness, and control of an organisation's software processes are believed to improve as the organisation moves up these five levels. While not rigorous, the empirical evidence to date supports this belief.

The idea of describing process maturity has expanded enormously since the first Software CMM was developed. Nowadays CMMs can be found for People, Software Acquisition, Systems Engineering, Integrated Product Development and IT Services. Several CMMs have been integrated by SEI into the Capability Maturity Model® Integration (CMMI℠). CMMI is consistent and compatible with ISO/IEC 15504, which is a framework for assessment methods. This standard results from the work of the Software Process Improvement and Capability determination (SPICE) initiative, which delivered a first draft in 1995.

CobiT uses a maturity model as a means of assessing the maturity of the processes described in the different CobiT domains and to help organisations set their maturity goals for these processes. The CobiT Maturity model knows the following levels:

0. *Non-existent* - There is a complete lack of any recognisable processes. The organisation has not even recognised that there is an issue to be addressed.
1. *Initial / Ad Hoc* - There is evidence that the organisation has recognised that the issues exist and need to be addressed. There are, however, no standardised processes, but instead there are ad hoc approaches applied on an individual or case-by-case basis. The overall approach to management is disorganised.
2. *Repeatable but Intuitive* - Processes have developed to the stage where similar procedures are followed by different individuals undertaking the same task. There is no formal training and the communication of standard procedures and responsibilities is left to the individual. There is a high degree of reliance on the knowledge of individuals and therefore errors are likely.
3. *Defined Process* - Procedures have been standardised and documented and communicated through training. It is however left to the individual to follow these processes and it is unlikely that deviations will be detected. The procedures themselves are not sophisticated but are a formalisation of existing practices.
4. *Managed and Measurable* - It is possible to monitor and measure compliance with procedures and to take action where processes appear not to be working effectively or efficiently. Processes are under improvement and provide good internal practice. Continuous improvement is beginning to be addressed. Automation and tools are used in a limited and fragmented way.
5. *Optimised* - Processes have been refined to a level of external best practice, based on results of continuous improvement and maturity modelling with other organisations. IT is used in an integrated way to automate the workflow, providing tools to improve

quality and effectiveness and making the organisation adaptive to its ever-changing environment.

Common Criteria (ISO/IEC 15408)

The Common Criteria represents the outcome of a series of efforts to develop criteria for evaluation of IT security that are broadly useful within the international community. In the 1980's and 1990's different countries worked upon developing their own criteria for security.

In June 1993, seven European and North American governmental organisations, constituting the Common Criteria project sponsoring organisations, pooled their efforts and began a joint activity to align their separate criteria into a single set of IT security criteria that could be widely used. This activity was named the Common Criteria Project. Its purpose was to resolve the conceptual and technical differences found in the source criteria and to deliver the results to ISO as a contribution to the international standard under development.

In 1999 ISO published its 'Evaluation Criteria for Information Technology Security' (ISO/IEC 15408). ISO continues the use of the term 'Common Criteria' within this document.

The Common Criteria is a means to define, assess, and measure the security aspects of ICT products. The Common Criteria supports understanding of 'what the product does' (security functionality) and 'how sure you are of that' (security assurance).

The Common Criteria are useful for product developers by providing them with the knowledge they need to design ICT products in such a way that they can pass an evaluation. For ICT products certified against Common Criteria, customers can be sure of which security aspects of the product were tested and how these aspects were tested.

The pocket guide "IT Governance, a pocket guide - based on COBIT" is the first publication of the joint Governance project team of ISACA-NL chapter, ITSMF-NL chapter and EXIN.

Title: "IT Governance, a pocket guide - based on COBIT"

ISBN: 9077212191

Authors: Harry Boonen & Koen Brand

Price: 14,95 Euro excl. VAT

Sales channels:
- Van Haren Publishing
- ISACA chapters
- ITSMF-NL
- regular web shops like ITILbooks

Publisher: Van Haren Publishing (http://www.vanharen.net)

Summary:

http://en.itsmportal.net/goto/literatuur/boek/205.xml

IT Governance

a pocket guide

BASED ON COBIT®

This pocket guide is the first result of a project that was started by ISACA-NL Chapter, ITSMF-NL Chapter and EXIN. The aim of this project was to develop a management instrument for IT Governance issues, in such a way that it would fit current standards for CIO's and IT managers, like ITIL, common ISO quality and security standards, and the Balanced Scorecard.

The structure of the project was based upon several other initiatives in the IT market, that were successfully run for ITSMF, EXIN and others, concerning various management instruments.

We think this pocket guide will be a valuable asset for CIO's and IT managers, in developing more grip on their IT organisation's performance, helping them to get in control.

Jan den Boer
President
ITSMF NL

Erik Pols
President
ISACA NL Chapter

Joep van Nieuwstadt
Managing director
EXIN

ISBN
90-77212-19-1