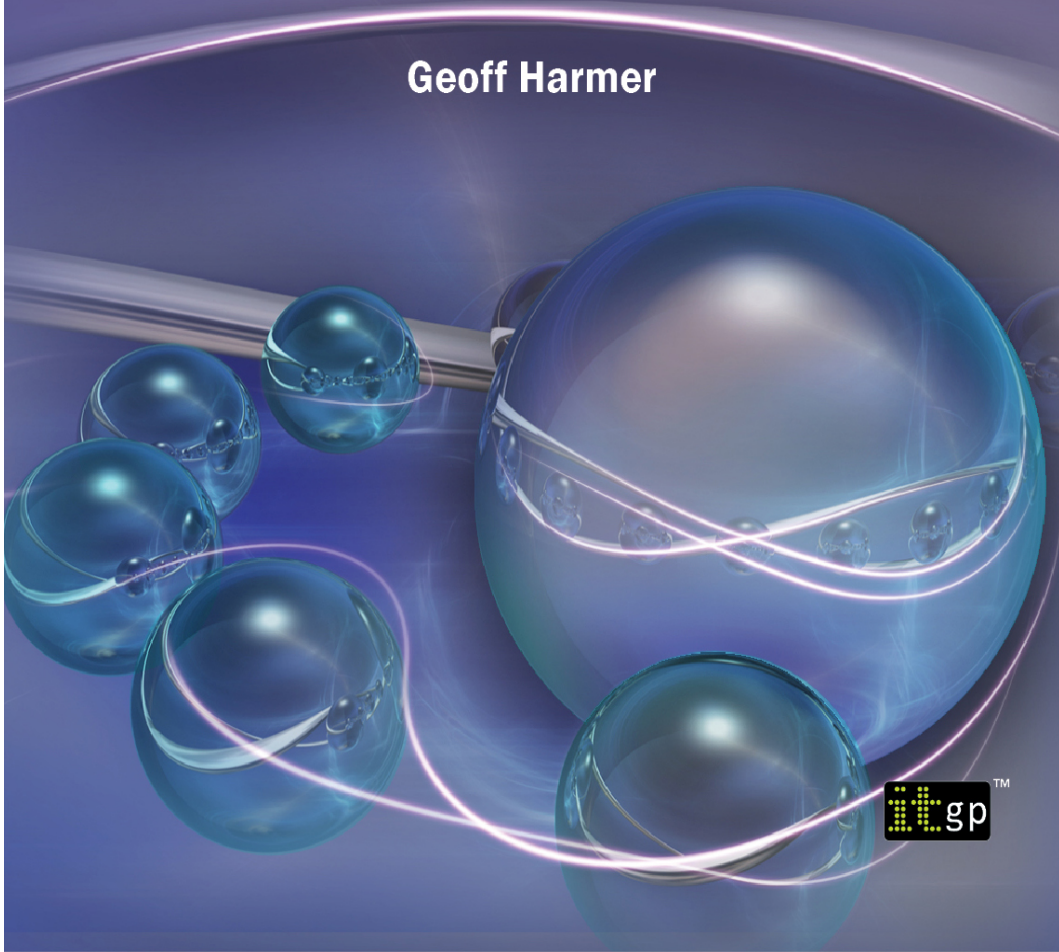
Governance of Enterprise IT based on COBIT® 5

A management guide

Geoff Harmer



itgp™

Governance of Enterprise IT based on COBIT®5

A management guide

Governance of Enterprise IT based on COBIT®5

A management guide

GEOFF HARMER

IT Governance Publishing

IT Governance Publishing
IT Governance Limited
Unit 3, Clive Court
Bartholomew's Walk
Cambridgeshire Business Park
Ely, Cambridgeshire
CB7 4EA
United Kingdom
www.itgovernance.co.uk

First published in the United Kingdom in 2013
by IT Governance Publishing.

ISBN 978-1-84928-520-9

ABOUT THE AUTHOR

Geoff Harmer lives in the UK and is the Director of Maat Consulting Ltd, an independent provider of education and consultancy on best practices for IT governance and IT service management.

He has more than 30 years' experience in the IT industry and is a Chartered Engineer (CEng), Fellow of the British Computer Society (FBCS), Chartered Information Technology Professional (CITP) and is Certified in the Governance of Enterprise IT (CGEIT®).

After gaining a PhD in neutron physics at the University of Sheffield and conducting programming for scientific research in optical design at the University of Reading, he worked for Digital Equipment Company (DEC), a major computer vendor, for 13 years then moved to several consultancy houses specialising in IT strategy and IT service management for a further ten years before setting up Maat Consulting in 2004.

Since 2001, he has specialised in communicating and developing ideas and approaches around standards and frameworks for information technology through courses, workshops, public lectures, consultancy and writing blog columns. He regularly presents a wide range of courses that include certification exams – COBIT®, CGEIT®, ISO20000 and ITIL®.

He has been an Associate Lecturer in Technology with the UK Open University since 1999.

As a physicist he is very interested in the linking of quantum mechanics to computing and so is currently studying Quantum Computation.

ACKNOWLEDGEMENTS

I first discovered COBIT® in 2004 when Gary Hardy ("father of COBIT®") visited the company I worked for in Reading, UK to discuss COBIT® and to explain that ISACA® was about to plan a COBIT® Foundation course. Unfortunately, as I was teaching an ITIL® course that day, I didn't get a chance to meet him, but I immediately downloaded COBIT®3 and was surprised to discover it had 34 processes compared to ITIL V2, which had just 10 processes. Gary had asked my manager, Sue Kilford, if someone who was an ITIL trainer with experience of Foundation course syllabi could attend a meeting at the University of Antwerp Management School (UAMS) to discuss the syllabus for a COBIT® Foundation Certification Course that ISACA® wished to create as an online course. I was delighted to be asked to attend that meeting.

At the two-day meeting, I met Erik Guldentops ("grandfather of COBIT®"), Gary Hardy ("father of COBIT®") and I was also introduced to Professor Wim van Grembergen, Chair of Information Systems Management at UAMS, a leading academic researcher in the field of IT governance whose textbooks written with Associate Professor Steven de Haes would later enlighten me. That meeting was when I became an IT governance enthusiast and I participated in further meetings to help define the COBIT® Foundation Certificate syllabus that came to life with an ISACA® online course and online exam in 2005.

I'd like to thank Sue Kilford for inviting me to get involved in COBIT® with its enthusiastic leaders Erik Guldentops and Gary Hardy, who have certainly educated me

continually about COBIT®. Another COBIT® expert who has helped me considerably is Roger Southgate, who not only regularly presented about COBIT® at ISACA® meetings I attended in London, but also with Gary Hardy taught an Implementing COBIT® Certificate course that I attended at an ISACA® conference in London in 2006, enabling me to become an ISACA® accredited trainer for COBIT® in 2006 when classroom-based courses started.

Key to my success in the area of COBIT® training and consultancy has been Alan Calder, CEO of IT Governance Ltd, Ely, UK who in 2007 agreed to schedule COBIT® Foundation and COBIT® Implementation training courses using my company, Maat Consulting, and created opportunities for me to develop and teach other IT governance courses including CGEIT®. I also thank IT Governance staff Donna Garner for organising and managing training events for COBIT® and Elizabeth Quashie for setting up my accreditations with APMG for COBIT® and keeping me informed of the continually changing world of APMG/ISACA® qualifications.

I was delighted to be contacted by Vicki Utting of IT Governance Publishing (ITGP) with a request to write this textbook, and I thank her and her team for their advice, waiting a long time for me to complete it and for their editorial reviews. I would like to thank the following reviewers for their helpful suggestions: Brian Johnson, CA; Mark Thomas CGEIT, President, Escoute Consulting and S. D. Van Hove, Ed.D., FSM® SED-IT, CEO & Founder.

I thank my mother, Connie, and my late father, Frank, for their continual encouragement while supporting me at school and university and Nigel Kermode who persuaded me to become an IT professional instead of a physicist by

recruiting me to Digital Equipment Company (DEC) in 1982.

CONTENTS

INTRODUCTION

This book is a guide to the governance of enterprise IT (GEIT) and how this may be implemented using COBIT®5.

It covers the key concepts of COBIT 5 in order that IT service management and IT governance, risk and compliance (IT-GRC) practitioners can readily understand COBIT 5 and see how to drive implementation of GEIT using COBIT 5 and how process assessment is conducted.

The chapters in the book are:

Chapter 1: Governance – a discussion of the concepts of enterprise and governance and an explanation of the path from corporate governance to the governance of enterprise IT.

Chapter 2: Key Frameworks and Standards Supporting GEIT – a summary of the large number of frameworks and standards that COBIT 5 is built on.

Chapter 3: COBIT®: From Audit to GEIT – a brief discussion of the origin and history of COBIT.

Chapter 4: Overview of COBIT 5 – GEIT – the key concepts of COBIT 5, the 5 principles, 7 enablers and the goals cascade.

Chapter 5: The 7 Enablers of COBIT 5 – a detailed look at all the concepts and features of all 7 enablers.

Chapter 6: Domains and Processes – the structure of the 37 COBIT 5 processes.

Chapter 7: Implementation of GEIT with COBIT 5 – the approach to implementation of GEIT using COBIT 5 and an implementation lifecycle.

Chapter 8: COBIT 5 Process Assessment Model (PAM) – the approach to process assessment of COBIT 5 processes based on international Standard ISO/IEC 15504.

Chapter 9: COBIT 5 Resources – a discussion of the official ISACA® documentation and training courses and certifications for COBIT 5.

This book covers all parts of the syllabus for the COBIT 5 Foundation course, so it is a useful and readable guide for those planning to take the exam. It has practical advice and guidance too, so it is also a valuable resource for implementing the governance of enterprise IT and fully understanding how process assessment is conducted.

CHAPTER 1: GOVERNANCE

'Corporate Governance began
In nineteen ninety-three
(which was rather late for me)
Between Robert Maxwell's fraud
And Cadbury's report to the LSE.'

after *Annus Mirabilis*[1] by Philip Larkin (1922-1985)

This chapter discusses the development path that has led from the introduction of corporate governance to IT governance to the governance of enterprise IT (GEIT).

Enterprise and Governance

First let's clarify two terms we are going to use extensively in this book: *enterprise* and *governance.*

Enterprise (n) is the term used to describe a range of different organisations: a commercial business (often called a corporation) that may, or may not, be quoted on a stock exchange; a public sector organisation such as a local or national government department, or a not-for-profit organisation such as a non-governmental organisation (NGO) or a charity. Enterprise is a more generic term than business since business often implies there is commercial interest. Perhaps the term organisation could also have been used since it, too, covers the full range of different enterprises just discussed and the term organisation chart is

[1] Larkin, P. A. (1967), Annus Mirabilis, in *High Windows*, (new edition 1979), London, Faber and Faber.

commonly used in all types of enterprises[2]. However, enterprise has become the term frequently used in the 21st century when discussing governance of organisations: that is, enterprise governance.

Governance (n) is 'the action, manner or fact of governing; controlling or regulating influence or good order[3]'.

Clearly, governance applied to enterprises is expressing the view that directors (or top management) of enterprises are tasked with governing, controlling and regulating their enterprise using best practices. Shareholders who appoint directors, as well as citizens who elect governments, expect this to take place but in some enterprises this has not happened and legal actions have had to be taken against many directors and top management over the centuries. Imprisonment and huge fines was not the only answer; what was needed was advice and guidance through regulations that must be obeyed – that is, corporate governance codes.

Emergence of Governance Codes

It was following Robert Maxwell's death in 1990 that a £4 billion fraud at Maxwell Communication Corporation and Mirror Group Newspapers was revealed. Maxwell was both chairman and chief executive – now considered not ideal and segregation of duties for these two roles is now best practice. Other frauds in enterprises quoted on the London Stock Exchange (LSE) around this time were Bank of

---

[2] A senior IT manager from a major UK government department confirmed that enterprise is a better term than organisation since the large government department where he works is broken into a number of *organisations*, so the government department is an *enterprise*.

[3] The New Shorter Oxford Dictionary (1993), Oxford, Oxford University Press.

Credit and Commerce International (BCCI) in 1991 and Polly Peck in 1990. These enterprises are all known in the UK as corporations – a word that implies stock market quoted enterprises. Consequently in 1991, the LSE and the accountancy profession appointed Sir Adrian Cadbury to chair a committee to recommend a code of best practice for corporate governance. The resulting Cadbury Report: *Financial Aspects of Corporate Governance* (December 1992)[4] is often seen as the point at which formally defined corporate governance emerged. The Cadbury Report identified the key responsibilities of boards of directors to be setting strategy, providing leadership, supervising management and reporting to shareholders about board stewardship (i.e. properly running the corporation in a fiduciary, i.e. trustworthy, way that the shareholders requested and expected).

Barger (2004)[5], *see Figure 1.1*, explained corporate governance very succinctly, stating there are three parts: ownership, governance and management. She indicated that shareholders had ownership of a corporation and appointed directors to govern the corporation. The directors' duty was to protect the shareholders' investment in the corporation by working with management to develop a corporate strategy and by directing management to run the corporation. Management's job was 'to develop business capabilities' and 'run business operations'. The directors would also request the management to provide reports so

[4] Cadbury Report (1992), *Financial Aspects of Corporate Governance.*

[5] Barger, T. (2004) Corporate Governance – A Working Definition, *International Corporate Governance Meeting*, Hanoi: IFC/World Bank Corporate Governance Department.

they could monitor whether their management was meeting directives.

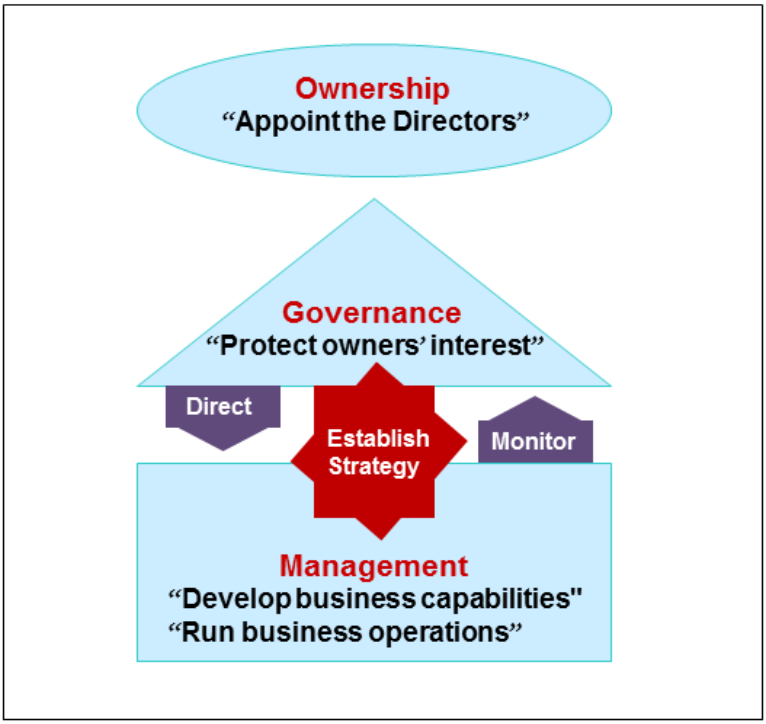


Figure 1.1 Corporate Governance (Based on Barger, 2004)

Corporate governance is now well established in the world, for example, all G-20 countries and, in total, more than 90 countries have their own corporate governance recommendations known as corporate governance codes (ECGI, 2013)[6].

[6] ECGI (2013) *www.ecgi.org/codes/all_codes.php.*

The International Federation of Accountants (IFAC, 2004)[7] used the term enterprise governance and indicated this includes two parts: Business Governance (i.e. performance) and Corporate Governance (i.e. conformance). Performance covers activities for value creation, resource utilisation and risk management. Conformance covers accountability and assurance. However, much earlier, Tricker, in his seminal textbook *Corporate Governance* – first written in 1984 when 'the term corporate governance was not then in use' (Tricker, 2008)[8] – indicated that corporate governance includes compliance (i.e. conformance) and performance. So enterprise governance means corporate governance. Interestingly, the Chartered Institute of Management Accountants (CIMA) who also used to say Enterprise Governance is made up of Corporate Governance and Business Governance has now removed both those terms and just talks about Enterprise Governance as performance and conformance (CIMA, 2010)[9].

When did IT Governance emerge?

As Weill and Ross, 2004[10], indicated in the preface to their seminal textbook, *IT Governance*, the point at which the importance of conducting IT Governance became clear is

---

[7] IFAC (2004) [online] Enterprise governance- getting the balance right, *www.ifac.org/sites/default/files/publications/files/enterprise-governance-gett-1.pdf* [accessed 30 Aug 2013].

[8] Tricker, R.I. (2008) *Corporate Governance: Principles, Policies and Practices*, Oxford, Oxford University Press.

[9] CIMA (2010) Enterprise governance – restoring boardroom leadership, [online], *www.cimaglobal.com/Documents/Thought_leadership_docs/Enterprise_governance.pdf*, [accessed 30 Aug 2013].

[10] Weill, P. & Ross, J.W. (2004) *IT Governance*, Boston. Harvard Business School Press.

not well defined like that of corporate governance but emerged over a period of years from multiple research studies and discussions between managers. As early as 1998-9 Weill with Michael Vitale at the Melbourne Business School conducted an exploratory study of IT governance. Much of the work on business and IT alignment (BITA) in the 1990s contributed to IT governance, too. The earliest I have been able to find the term IT governance was in an article on strategic alignment of business and IT by Henderson and Venkatraman in 1992 in Chapter 7 of the book *Transforming Organisations* (Kochan and Useem)[11].

IT governance took off as a discipline once the COBIT framework evolved from an IT audit to an IT governance framework with the release of COBIT®3.0 in 2000. COBIT was, and still is, widely adopted as the *de facto* framework to meet the IT governance requirements of Section 404 of the Sarbanes-Oxley Act of 2002. It is worth pointing out that COBIT recognised that IT governance was concerned with ensuring both conformance and performance, that is, compliance and value delivery to the business.

In Australia between 2003 and 2005, Standards Australia developed Australian Standard AS 8015-2005 for the Corporate Governance of Information and Communication Technology. This complemented the set of Australian Corporate Governance Standards – the first of which had been published in 2003. AS 8015 was fast-tracked into an ISO Standard as ISO/IEC 38500, *Corporate Governance of IT*, published in May 2008. Unlike the free, comprehensive

[11] Kochan, T. A. and Useem, M (1997) *Transforming Organisation*, New York, Oxford University Press Inc.

resources within the COBIT framework, ISO/IEC 38500 was a slim, 12-page, easy-to-understand Standard aimed at directors of businesses to guide them in their governance in the use of IT – however, it has to be purchased at around $100.

Clearly COBIT needed to take on board the ISO/IEC 38500 Standard and this was to happen with COBIT 5.

Now people are starting to discuss Enterprise Governance of IT rather than IT Governance; notably Wim Van Grembergen and Steven De Haes at the University of Antwerp Management School (UAMS). They have been long-term researchers for ISACA/ITGI and advocates of approaches to implementation of IT governance that have contributed much to the development of the COBIT framework. In their book *Enterprise Governance of Information Technology*[12], published in 2009, they begin by pointing out that Enterprise Governance of IT is a relatively new term and they go on to explain that because of the 'IT' in the naming of IT governance, discussion did not generally reach the boardrooms of organisations. Clearly the involvement of business is crucial and they indicate there has been a shift of emphasis (largely due to the publication of ISO/IEC 38500, I feel) to focus on business involvement, that is, Enterprise Governance of IT. As they put it, 'Enterprise Governance of IT is an integral part of corporate governance and addresses the definition and implementation of processes, structures and relational mechanisms in the organisation that enables both business and IT people to execute their responsibilities in support of

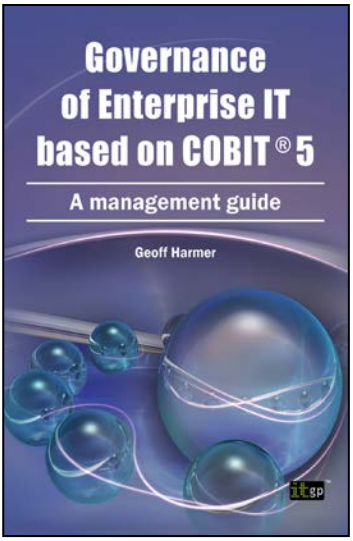
[12] Van Grembergen, W. & De Haes, S. (2009) *Enterprise Governance of Information Technology*, New York, Springer Science + Business Media LLC.

business/IT alignment and the creation of business value from IT-enabled investments.'

In 2009, ISACA created a new certificate called Certified in the Governance of Enterprise IT (CGEIT®) that is a person qualification based on passing an examination and having sufficient professional experience of the governance of enterprise IT. Notice that the term Governance of Enterprise IT (GEIT) is a rephrasing of Van Grembergen and De Haes' term 'Enterprise Governance of IT'. GEIT is now the conventional term for what earlier was, and still is, referred to as IT governance.

So from 2010, the COBIT 5 Task Force worked on COBIT®5 that was released in April 2012. It is aligned with ISO/IEC 38500 and it fully addresses the 'Governance of Enterprise IT'. That is the subject of this book.

WANT TO READ MORE?



YOU CAN BUY THE COMPLETE BOOK FROM OUR WEBSITES:

www.itgovernance.co.uk/shop/p-1509.aspx
www.itgovernanceusa.com/shop/p-1389.aspx

and from a wide range of booksellers including Amazon