

Waltzing with the Elephant:

A comprehensive guide to directing
and controlling information technology.



Mark Toomey

Information technology is the Elephant in the Room – especially the boardroom. Organizations depend on it for routine operations and future performance, and IT problems can have serious consequences. Yet many organizations lack effective oversight of IT, and are at risk of surprises. This book aims to help build shared understanding that leads to a well-integrated system for governance of IT from the boardroom to the coalface, framed around the guidance in ISO/IEC 38500.



Infonomics,
Melbourne,
Australia

Promotional Extract

Waltzing with the Elephant:

A comprehensive guide to directing
and controlling information technology.

Mark Toomey

Foreword by Adela McMurray

Business Leader's Perspective by Ian Wightwick

Graphics and photography by Mark Toomey

This book is published by:

Infonomics Pty Ltd.
311 Ryans Rd
Belgrave South
Victoria 3160
Australia
www.infonomics.com.au



This is Edition 1, Print 1, 3rd August 2009.

Copyright

© 2009 Infonomics Pty. Ltd. All rights reserved.

No part of this publication may be reproduced, stored in an automated retrieval system, or published in any form or by any means, without the prior written permission of the copyright owners.

This book is sold in hard copy and in electronic format, as a PDF file. Each PDF is individually watermarked with details of the purchaser. Making and passing copies of this book, whether in hard copy or electronic format, to any person or organization for any purpose whatsoever is expressly prohibited.

If you have received this book in any format other than as a bound hard copy volume, please either inform Infonomics immediately, at the above address, or purchase a copy for your own use at the Infonomics Shop, which is accessible from www.infonomics.com.au.

This book reproduces certain definitions and a model for governance of information technology taken from ISO/IEC 38500: 2008 – Corporate Governance of Information Technology. These definitions and diagram are reproduced with the permission of the International Organization for Standardization, ISO. The ISO/IEC 38500 standard can be obtained from any ISO member and from the Web site of the ISO Central Secretariat at www.iso.org. Copyright for the material reproduced from ISO/IEC 38500 remains with ISO.

Product and company names used in this book are for identification and reference purposes only, and their use does not in any way indicate a claim by the author or the publisher of ownership of corresponding trademarks.

National Library of Australia Cataloguing in Publication Data

CIP Registration pending.

ISBN: 978-0-9806830-0-4

Disclaimer

This book was written to provide general guidance and stimulate debate. It should not be construed as providing professional advice and services for any particular or specific situation. Accordingly, it should not be used as a substitute for consultation with expert advisers. Before making any decision or taking any action you should consult with Infonomics Pty Ltd or other competent professionals.

Cover photograph

The ancient Nuffield tractor on a Southern New South Wales Riverina farm has seen better days. After years of sterling service, it's gone the way of all machinery that has passed its use-by date. Overtaken by larger, more powerful, more reliable, more economical, more flexible and safer machines, the Nuffield moved quickly from work-horse to spare parts, and eventually, complete disuse. Now it awaits the interest of collectors who will one day refurbish it to its former glory, and demonstrate to future generations what life was like in days gone by.

The Nuffield's story is easy to comprehend, because it is a real, tangible machine. One glance tells us that it is old and tired, and our general knowledge tells us that it has been supplanted by much more modern appliances.

How so would we depict the fate of computer systems of similar age? We cannot see much of what comprises our oldest operational computer systems – so we have little in the way of tangible cues to trigger our thoughts about their effectiveness, value, reliability and safety.

Perhaps this book will help us to develop much needed perspective, and become more effective in asking questions and making decisions about how our organizations use information technology.

Photograph by Mark Toomey, using a Sony Alpha digital SLR, with a Sony 35-70 lens in auto mode.

Promotional Extract

This work is dedicated to the memory of

Brian Minchin, CMC¹

Without Brian's encouragement, this book may never have been written.

Brian's boundless energy and enthusiasm were snuffed out by cancer in December 2008.

His work was not finished.

Just one year earlier, at Brian's lakeside cabin north of Toronto, the idea for this book was born.

He never read a page of it, but he was committed to the ideals that it presents.

We seek a better world – a world of peace and prosperity.

Information Technology, well used, can contribute greatly to our achievement of such ideals.

Through better, more responsible, and effective decision making and control, we can make better use of information technology, and we can improve the world.

This book aims to improve the success of all the world's business and government organizations in their use of IT. But the change does not come from my writing the text. It comes from you, critically assessing what you do, and improving it where appropriate. All I can do, with the encouragement of my friends, is share with you some ideas.

¹ Certified Management Consultant – a qualification administered by the Canadian Association of Management Consultants.

Promotional Extract

This promotional extract may be circulated freely

Standards are generally required
when excessive diversity creates
inefficiencies or impedes
effectiveness.

Edward W. Hammond and James J. Cimino,
Standards in Medical Informatics (Springer, 2001)

Promotional Extract

This promotional extract may be circulated freely

Acknowledgements

How does one thank the people who contribute to a work such as this? How does one even identify them all?

Waltzing with the Elephant expresses the learnings of a fortunate career – one that has enabled me to experience many situations and many points of view. From the early days at Management Information Systems, where we pioneered the use of what were then called mini computers in medium sized businesses (my telephone has vastly more power than the machines we used in those days), to more than ten years at DMR, where wonderfully skilled and generous people helped organisations all over the world build and realise their dreams, and on to the firms with which I have worked as an independent consultant, there have been countless individuals and organisations who have through their deeds and misdeeds created the colour in my experience and provided most of the anecdotes expressed herein.

This book may never have happened had it not been for the unstinting efforts of my colleagues in development of the standards to which it refers. I particularly thank John Graham, Max Shanahan and Raymond Young for the many hours of discussion, Alison Holt for the encouragement, and Chris Jones for the early reviews.

Adela McMurray, Associate Professor and Assistant Dean Research & Innovation at RMIT University has been an enthusiastic supporter who never stopped encouraging me even though I kept sending her more drafts for comment.

Chris Gillies, Chris Ogden and John Thorp, all long time friends and experts in effective use of information technology have been sounding boards who gave freely of their own ideas and experience.

My beloved partner Leonie has endured long periods of solitude while I pounded the keyboard, and rewarded me with her precise and perceptive eye during the proof-reading stage.

Peter Cross and his colleagues at itSMF Australia have been generous in their support as hosts of the international launch of the book at their 2009 annual conference in Sydney.

Alistair Urquhart and his team at Affairs of State have been equally generous with the follow-up launch for the business and government communities in Melbourne.

Promotional Extract

This promotional extract may be circulated freely

Foreword

Governance of IT is at times afflicted by alarmingly contagious outbreaks of insanity and is subservient to a proliferation of academic theories and practical solutions - many of which claim to possess the IT Governance panacea and yet these are often seen at odds.

Expeditious technological change punctuates modern business in Australia and abroad yet the implications and outcomes of its impact on an organization's IT enabled change and re-invention are yet to be demonstrated through research intelligence. As a senior academic and consultant working with a multitude of practitioners riding the high and low tidal waves of rapid change in their organizations I see two core variables impacting on sustainability of how organizations Govern their use of IT. These core variables are organizational climate and culture which reside on the same continuum. Climate is more grounded in individual consciousness (perceptions) and culture is largely preconscious or more to do with tacitly held values, attitudes and beliefs. There is congruence between culture and climate where the key behaviours for Governance of IT requires embedding within both of these key concepts across the various organizational layers.²

Waltzing with the Elephant is the first authoritative book providing insight into Governance of IT that is pitched across organizational layers from CEO to shop floor level in both industry and academic contexts. Thus, this unique feature fast-tracks the transportability and understanding of IT Governance values, attitudes and perceptions that may be implemented across an organization's climate and culture levels.

This timely book provides an integrated approach to the conceptualization and application of IT Governance leadership, accessible to one and all, where the IT Governance dance is performed with others thereby facilitating the recognition and appreciation of its value. – Don't be shy: take the lead; for the experienced 'Toomey Band' is playing!

Adela J McMurray, PhD
Assistant Dean, Research & Innovation
College of Business, RMIT Business Melbourne.
Email: Adela.McMurray@rmit.edu.au

² McMurray, A.J. (2003) The Relationship Between Organizational Climate and Organizational Culture. The Journal of American Academy of Business, Vol 3, No 1).

Promotional Extract

This promotional extract may be circulated freely

Business leader's perspective: Ian Wightwick

Today, as a non-executive public company director, and previously as CEO of a large listed international company, the effective control and efficient use of IT systems has been a critical "top-of-the-mind" issue for me.

Why? Since I first became seriously involved with IT in 1967, I have been involved in the fantastic benefits of successful IT projects, but also exposed to some classic failures.

What continues to amaze me is the extent of major IT failures. Indeed I would go so far as to say most large IT projects which have come to my attention have had major problems involving one or more of significant cost over-runs, extremely late delivery, and failure to meet original project scope objectives.

Given this prevalence of failures, and the often near catastrophic impact on businesses, I have been intrigued as to why IT governance never seems to get the same prominence at board level (and sometimes even at CEO level) as financial systems management and reporting, remuneration and HR reporting, etc. Even with the current emphasis on risk analysis and reporting, IT is often mentioned only in terms of "What if IT systems failed?"

Yet, paradoxically, I would contend every CEO and every director now accepts the criticality of IT systems to the very core activities of all business transactions and financial reporting.

I can only conclude there is a mystique, maybe fear, surrounding IT that sees many boards being satisfied with simple assurances from the CIO or CEO, and auditors. It may be the jargon ("techno-babble" according to Mark Toomey) being overwhelmingly confusing, or the fear of being seen to ask dumb questions or just plain ignorance of the real risks.

Whatever the reason, there is a desperate need for more thorough and effective IT governance in each and every organization dependent on IT systems.

Probably the worst IT catastrophe of which I have first-hand knowledge involved a top 50 listed company in which I worked. Newly appointed top management had decided the 60 strong IT department (who had been running a hitherto very successful IT department), were "too old-fashioned" to bring the company into the "new IT age". They contracted the IT development group of a now non-existent international accounting firm to write a completely new sales and accounting system. A relatively low-level steering group was to regularly review the project, but not one person from the IT Department was involved in the project design or control.

The project team from the accounting firm were relatively young, and no one with extensive experience had any hands-on involvement. Worse, the external team kept changing "due to other customers' project needs".

Before long, it began to be recognized by a few of us not on the steering committee, that the project was going out of control. Eventually, after over 12 months of work, the code for the project to-date, with not one word of documentation, had to be (embarrassingly) handed over to the company's IT department's chief. He and his team were left to complete the work and get it up and running. Needless to say, bitter recriminations and bad feelings abounded, apart from the impact of the huge time and cost over-run.

One more recent significant IT experience was when I was CEO of a large listed international company. We embarked on a 2+ year, A\$70M project to replace all financial, sales, manufacturing, warehousing and distribution systems with a selected proprietary software package. Based on extensive business experience with major IT project experiences since the

early 1970's, and a short period of "hands-on" restructuring and directing of a large IT department, I was convinced that the CEO should chair the Steering Committee for this pervasive IT Project.

I was certain it was necessary to elevate control to this level to ensure a sufficiently detailed scope was conducted, a thorough software supplier selection procedure was followed, an experienced and disciplined project manager was appointed (with major non-IT capital project experience in this case), and importantly major milestones were achieved on time and within budget. By far the biggest danger was recognized as the lack of control over proposed variations to project scope, with the consequent danger of cost and time blow-out.

A major international software supplier's package was selected and, from the outset, we specified the least possible "customization" of the package to keep future software upgrade costs to a minimum. Mid-project scope variations were subject to such a high level and rigorous review that it was soon realized only those absolutely critical to project success should ever be proposed.

Even with this level of control, the project ran into big hurdles, mainly due to a couple of key modules of the software supplier's systems not performing as specified. There was much confrontation, but with the high level of governance via the CEO and the steering committee, the supplier was simply forced to meet their contract obligations without cost penalty.

The project came in on time, to budget, and, importantly, performed satisfactorily.

During this time, the board of directors also appointed one of their number who, fortunately, had IT experience, to review the project throughout the whole process. This director attended regular steering committee meetings, and independently reported back to the board.

The example quoted emphasizes IT governance as it relates to projects. Of equal board and CEO concern is the governance of existing IT systems. The board and CEO must keep informed of the currency, capacity and support of hardware and software and respond to systemic inadequacies identified by auditors.

Boards should devote close attention to the IT strategic plan, assigning similar weight to that of other strategic business plans (for markets, products, production, etc.). This may encompass such critical issues as future IT development, more effective use of data and systems to enhance competitiveness, IT back-up adequacy and whether to outsource IT in whole or in part.

Clearly the purpose of Mark Toomey's text is to promote the need for adequate IT governance. It is commendable in this regard, but is only the beginning.

Company director (including CEO) education courses and regular director briefings will need appropriate attention with provision of simplified explanatory material and check-lists, as well as encouraging the de-mystifying of the whole business-critical IT issue.

Ian Wightwick, 3 July 2009.

Ian Wightwick is Chairman of Plantic Technologies. Until February 2003 he was Managing Director and Chief Executive Officer of PaperlinX Ltd, which went public under his stewardship in 2000, became a top 100 public company in Australia and went on to become the largest international paper merchant. His 50-year career spans technical, marketing, production, consulting, general management and chief executive roles in the oil, chemical, food and paper and packaging industries. His current activities include investment management, consulting and mentoring (both at national and international level).

Preface

Information Technology is “The Elephant in the Room” – especially the boardroom. During the past few years, veterans of the boardroom have said, with absolute conviction: “IT should only be discussed regularly by boards of banks and airlines – as those businesses clearly depend on it”; and “IT should only be discussed in the boardroom when it has become a problem”.

By contrast, advisors, researchers, professional bodies and now even peak boardroom organizations (the King III report from the Institute of Directors in South Africa contains specific guidance regarding directors duties in respect of IT) are saying the directors should have effective oversight of their organization’s IT.

Recent experience of serious problems with IT in numerous organizations, large and small, in all fields of endeavour, makes it clear that IT is critical to both daily business activity and to future performance. The boards of many such organizations may well wish that they had been better equipped to understand and control the situation with IT well before the problems became disruptive, debilitating and in some cases, absolutely destructive.

Directors are in a very difficult situation. How do they understand, direct and control their organization’s use of IT when so often the discussion is laced with technobabble, impossible to understand and encased in vague assurances of value that might be delivered? Directors the world over struggle to know how to control IT. But, knowing that their organizations may be at risk of IT failures, and that an enormous percentage of all IT investment projects fail, how do directors fulfil their obligations to shareholders and the law, when information technology involves so many unknowns?

Business executives often face similar problems. With no direct background in the IT space, how do business leaders ensure that they are using IT in the most appropriate way, extracting the full benefit of new IT investments, maintaining the operational viability of the business, and providing the board with the right information about IT to enable the directors to discharge their duties?

The answer was supposed to be “IT Governance”. But increasingly, experts in the field are suggesting that “IT Governance” has failed. Despite substantial investment, there has been little, if any, tangible increase in success of projects, or reduction in business-damaging failures of established IT systems.

Why has “IT Governance” failed? I suggest that the most fundamental reason is that it has dealt only with one side of the problem – the supply of IT. It has been focused on controlling the IT supply function, and has not given enough attention to the way that demand for IT is controlled, from the top of the organization. In language terms, it has been fairly simple: “IT Governance” has operated in the space of IT – disenfranchising the business leaders it was supposed to help.

That’s why ISO/IEC 38500 was developed. The standard addresses the problem differently – not from a supply perspective, but from the perspective of how the organization uses IT. Use, or demand, should drive supply – not the other way around.

From its release on 5 June 2008, ISO/IEC 38500 has been hailed by observers as a landmark, if for no other reason than its clear definition for governance of IT.

But ISO/IEC 38500 is very different to previous treatments of “IT Governance”. It is brief – only 15 pages long, and devoid of any instructions about how to organise and run IT. How can it then be used to achieve its goals – to help organizations achieve effective, efficient and

acceptable use of IT and thus to both reduce the waste of failed projects and increase the value of projects that do succeed?

Considered in isolation, and in the hands of those who have limited experience at the top of organizations, ISO/IEC 38500 may seem superficial and narrow. But the years of work that went into developing the standard were not aimed at emasculating it. Rather, by driving to condense it into the foundation concepts that it presents, the authors of ISO/IEC 38500 created an immensely powerful frame of reference in which to consider all aspects of how organizations use, and make decisions about their information technology.

Effective governance of IT will rarely be achieved by simply following a generic framework – any more than a basic accounting system alone is sufficient for monitoring and controlling an organization's finances. Rather, it requires fundamental thinking about the issues that are important, and it requires that the leaders of the organization behave in ways that maximise the value and contain the risks in their current and future use of IT.

Effective governance of IT would also be unlikely if the various parties in an organization were deriving their expectations from diverse guides. *Waltzing with the Elephant* is specifically designed to eliminate that problem. It is written for a wide spectrum of audience – from the non-executive chair of a large listed corporation, to the permanent head of a government agency, to top executives, business managers, IT professionals and consultants, researchers, academics and students. Its language is not bland, but it does avoid needless jargon. Its anecdotes are not synthetic – they are drawn from the author's real life experience.

Waltzing with the Elephant helps those who want to identify the issues that are important in their organizations and understand the critical elements of governing IT in the organizations for which they are responsible. It bridges the gap between the boardroom and those responsible for the detail by explaining the nature of a system of governance, spanning seamlessly from the top of the organization to the coalface.

For directors and senior executives, *Waltzing with the Elephant* give new insight to what should be happening in respect for future planning, delivery and operational use of IT – equipping them to ask pertinent and timely questions, and to cut through the babble to the core issues of concern to them.

For managers, whether senior or junior, responsible for business or technology issues, *Waltzing with the Elephant* aims to expand awareness and understanding – to help them think about what things should be happening and how they should be happening. It should be seen as an essential companion to frameworks for directing and controlling their organization's use of IT – to be used when establishing the frameworks and again when evaluating and improving them.

For technology specialists, *Waltzing with the Elephant* lays bare the role of the business in defining how it will use information technology in pursuit of the organization's objectives, and provides the hooks for designing and implementing an effective approach to controlling and directing IT use that goes beyond engaging the business, to putting the business in its vitally important role of leadership.

Waltzing with an Elephant requires a very clear and shared understanding of who is doing what, and the absolute engagement of all who are participating in the dance. So does governing information technology.

Mark Toomey
August, 2009.

Contents

How to use this book.....	1
1 The problem with information technology	3
1.1 The risks inherent	3
1.2 The IT management improvement industry	5
1.3 Impact of improvement.....	6
2 The standard for governance of IT	9
2.1 The requirement	9
2.2 Australian Standard AS 8015	10
2.3 ISO/IEC 38500	11
2.3.1 Development and adoption.....	11
2.3.2 Subsequent developments	12
2.3.3 A synopsis of ISO/IEC 38500	13
3 Understanding governance of IT.....	15
3.1 The fundamental equations.....	15
3.1.1 Supply ↔ demand	15
3.1.2 The business system	17
3.2 The system of governance.....	23
3.2.1 Defining governance of IT	23
3.2.2 Distinguishing governance and management	25
3.2.3 Putting governance of IT into context.....	26
3.2.4 The system perspective	29
3.2.5 Responsibility for information technology	30
3.2.6 Board oversight of IT	30
3.2.7 In summary.....	31
4 The key messages in ISO/IEC 38500	33
4.1 Directors should govern the use of information technology	33
4.2 Governance and management are separate concepts.....	34
4.3 The standard is applicable to every organization.....	37
4.3.1 Organizations that use information technology.....	38
4.3.2 Ownership structure and profit motivation	39
4.4 The people who should most use the standard are the managers	40
4.5 Good governance of IT is a desirable attribute for stakeholders.....	41
4.6 Behaviour is key.....	43
4.7 Implementation is the responsibility of each organization	45
5 The ISO/IEC 38500 model for governance of IT	49
5.1 Fundamental topics in governance of IT	50
5.1.1 Business processes	50
5.1.2 Proposals	50
5.1.3 Projects	51
5.1.4 Operations	52
5.2 The tasks for governance of IT.....	52

5.3	The principles for governance of IT	53
5.3.1	Principles and organization behaviour	54
5.3.2	Applying principles through policy	56
5.3.3	Completeness of the ISO/IEC 38500 principles	59
6	The integrated system for governance and management of IT	61
6.1	Governance and management: the relationship	63
6.2	The nature of a proposal	69
6.2.1	Vision.....	70
6.2.2	Strategy	71
6.2.3	Planning	71
6.2.4	Projects	72
6.2.5	Operation.....	72
6.2.6	Governance system	73
6.2.7	In summary	74
6.3	What does "evaluate" really mean?	74
6.3.1	The director's role in evaluation	74
6.3.2	Evaluating current use of IT – the business systems perspective	75
6.3.3	Evaluating current use of IT – the technology perspective	76
6.3.4	Evaluating future use of IT – strategy	77
6.3.5	Evaluating proposed initiatives – and the competing priorities.....	81
6.3.6	Evaluating supply	85
6.3.7	Evaluating governance	90
6.4	The task of giving direction.....	93
6.4.1	Constitution.....	93
6.4.2	Delegations.....	94
6.4.3	Strategy	95
6.4.4	Specific plans	96
6.4.5	Policies.....	96
6.4.6	Key decisions.....	97
6.4.7	ISO/IEC 38500 expectations of direction	99
6.5	Monitoring – ensuring that intentions are realised	101
6.5.1	Some problems with monitoring.....	102
6.5.2	Monitoring in the system of governance	104
6.5.3	The role of audit.....	104
6.5.4	The safety valve.....	105
6.5.5	Monitoring responsibility.....	106
6.5.6	Monitoring performance.....	108
6.5.7	Operational objectives.....	109
6.5.8	Future operations.....	110
6.5.9	Current investments	112
6.5.10	Capacity to implement	114
6.5.11	Monitoring conformance	114
7	The responsibility principle.....	119
7.1	Who is responsible for IT?	119
7.2	Responsibility assignment and the system of governance	121
7.3	Desirable behaviours	123
8	The strategy principle	127
8.1	Elements of strategy and planning.....	128

8.2	Planning disciplines.....	130
8.2.1	Strategy	130
8.2.2	Enterprise architecture	131
8.2.3	Portfolio, program and project	135
8.2.4	Portfolio	136
8.2.5	Program.....	138
8.2.6	Project.....	139
8.2.7	Operation.....	141
8.2.8	Asset.....	142
8.2.9	Security	145
8.3	Desirable behaviours	147
8.4	Responsibility for strategy and planning	151
9	The acquisition principle	153
9.1	Appropriate analysis	153
9.1.1	Objective: what is the intended outcome?.....	155
9.1.2	Value: why is the outcome important?	155
9.1.3	Approach: how will the outcome be achieved?	156
9.1.4	Performance: how will progress and success be made visible?	158
9.1.5	Risk: how will the things that could go wrong be detected and controlled?.....	159
9.2	Continuing an initiative	159
9.3	The living system – business as usual	160
9.3.1	Business-as-usual elements.....	162
9.3.2	Retirement decisions.....	166
9.4	The evolving economics of outsourcing	168
9.4.1	Traditional outsourcing	169
9.4.2	New wave outsourcing.....	170
9.4.3	Outsourcing in a business as usual context	171
9.4.4	Disengaging an outsourcing arrangement	171
9.5	The decision making framework	172
9.6	Cutting to the core	173
9.7	Responsibility in acquisitions.....	173
10	The performance principle.....	175
10.1	Planning.....	177
10.1.1	Business plans	178
10.1.2	Information technology plans.....	179
10.2	Projects	181
10.2.1	Technology projects	182
10.2.2	Benefits realisation	182
10.2.3	Project selection	184
10.2.4	Project management	185
10.2.5	Project reporting	186
10.2.6	Delivery capacity and capability	188
10.2.7	Oversight capability	189
10.3	Operations	194
10.3.1	Workload	194
10.3.2	Efficiency	196
10.3.3	Integrity	197
10.3.4	Reliability	199
10.3.5	Continuity	200

10.3.6	Security	202
10.3.7	Problems	203
10.3.8	Maintenance and changes	204
10.4	Risk	205
10.5	Responsibility for performance	207
11	The conformance principle	211
11.1	External obligations	211
11.1.1	Sources	212
11.1.2	Conformance behaviours	212
11.2	Internal controls	214
11.2.1	The system for governance of IT	214
11.2.2	Policy and conformance framework	216
11.2.3	Strategic policies	217
11.2.4	Operating policies	219
11.2.5	Usage policies	221
11.2.6	Elements of an IT controls and conformance policy	221
11.3	Responsibility for conformance	222
11.3.1	External conformance	222
11.3.2	Internal conformance	222
12	The human behaviour principle	225
12.1	Scope of human behaviour – the people perspective	226
12.2	Scope of human behaviour – the behaviour perspective	227
12.3	The human communities	230
12.4	Elements of a human behaviour policy	232
12.5	Responsibility for human behaviour	233
	Bibliography	235

Figures

Figure 1: The demand ↔ supply equation	16
Figure 2: Key elements of the business system.....	17
Figure 3: Models of change.	19
Figure 4: The role of corporate governance	26
Figure 5: Tricker's model of corporate governance	27
Figure 6: The governance system.....	29
Figure 7: Corporate governance of information technology model (ISO/IEC, 2008 p. 7)	49
Figure 8: Steering use of IT.....	53
Figure 9: Framing common issues with principles	60
Figure 10: Corporate governance of information	62
Figure 11: Juxtaposing of governance and management tasks.....	63
Figure 12: Primary management systems	64
Figure 13: Thorp's strategic governance framework, extended	65
Figure 14: IT management disciplines in business management model	66
Figure 15: The system for governance of information technology	67
Figure 16: Governance – management engagement	68
Figure 17: Resources underpinning business operations	87
Figure 18: Omnibus organizational change: resource requirement.....	89
Figure 19: Framework for evaluating governance of IT.....	92
Figure 20: Notional conformance management matrix	117
Figure 21: Notional conformance summary report linked to management framework.	118
Figure 22: Ranking chart for comparing proposed initiatives.....	137
Figure 23: Illustrating the work required for a project.....	140
Figure 24: Three points of focus for performance	176
Figure 25: Diagram used to anchor status report	187
Figure 26: The hierarchy of policies	216
Figure 27: The people in the process	226
Figure 28: Communities of Interest	230

Promotional Extract

This promotional extract may be circulated freely

How to use this book

Dancing with the Elephant was written with a single goal – to improve governance of information technology use in all organizations.

It is a book for everybody, because in most organizations, everybody is involved, to some extent, in the use of IT.

It is particularly a book for those who have significant responsibility for the success of IT use – including especially those who may not have been aware of, or understood their responsibility.

It is written to build a shared and consistent understanding of concepts that have been, in many cases, poorly understood and greatly confused. It is designed to progressively build a consistent understanding of the topic – directing and controlling the use of IT in most organizations.

Skim the book to gain a first impression of the breadth and depth of subject matter it explores. While ISO/IEC 38500 condenses governance of IT into just 15 pages, that first scan should leave you convinced that a comprehensive approach to governance of IT should deal with many topics.

Read the book from cover to cover, to gain a comprehensive picture of what can be important in governing an organization's use of IT. Don't skip the parts that you think you know. It will help you in later conversation with others to have a common frame of reference. Even if you do know the core concepts, it should be useful for you to see how they are explained to others who are not so well informed. Remember, one of the greatest barriers to communication is the absence of common language, and one purpose of both this book and ISO/IEC 38500 is to establish that common language.

Mark up the parts that are significant for you and explore them further. These may be matters that you have not considered in the past and now seek to understand better, or they may be new ways of looking at and understanding issues that have caused you concern.

Raise questions for topics on which you think there may not be sufficiently answers or adequate attention in your organization, and follow through on those questions. Get answers and decide from there whether further action is required.

Compare the way that your organization plans, implements and operates its use of IT with the practices and behaviours described. Consider whether and to what extent there are differences, and evaluate the potential consequences of those differences.

Refer back to the book regularly to reinforce and challenge your thinking on aspects of governing IT that are significant for you at the time. At different stages of your job, you can be sure that different topics will be important.

Build checklists for yourself to help in your role, whatever it is, to help you confirm that you have done the important things, asked the relevant questions, and addressed the relevant issues.

Buy ISO/IEC 38500. Obviously, this book cannot reproduce the standard, and nor should it replace the standard. The standard presents the formal guidance. This book is here to help you understand that guidance and work out how to apply it in your situation. Read the relevant sections of the standard in conjunction with the corresponding chapters in Waltzing with the Elephant, to ensure that you get the connection.

Promotional Extract

This promotional extract may be circulated freely

1 The problem with information technology

Whether we like it or not, information technology has become ubiquitous and essential in both ongoing operation and strategic development of almost all organizations. But information technology is troublesome – it can and frequently does go wrong and the consequences of failure can be serious.

1.1 The risks inherent

A Special Report in the Financial Times (Tieman, 28 May 2008) leads with an article titled "Sweeping away a sector's chaos". The article reports on the extreme dependence of the banking system on information technology, but points out that in some instances, the critical systems at the core are ancient and a source of unacceptable risk. It says that one major UK bank's systems still calculate in the old sterling currency of pounds, shillings and pence, 37 years after the nation converted to decimal currency.

But it is not merely the age of the systems that worries the Financial Times. The article goes on to say that while technology has enabled banks to process ever-increasing volumes of transactions, and to introduce more complex and sophisticated products, the lack of comprehensive coverage in systems means that new areas of risk are emerging. Specifically, it suggests that the 2007/8 credit crisis may be in part attributed to weakness in risk management, where exposure to risk has become remote from the risk itself and is thus both poorly understood and virtually impossible to monitor.

National Australia Bank has first-hand experience of the risks inherent in using information technology. In 2003, the bank experienced substantial losses as a result of "irregular currency options trading". While four currency traders subsequently faced criminal proceedings, the consequences for the bank were far-reaching, climaxing in the resignation of the Chief Executive and a complete, though progressive, spill of the entire board of directors. The bank was subject to increased supervision by the government regulator, and was required to undertake a number of mandatory improvement programmes. The role played by IT in this situation was remarkable not merely because the irregular trades were facilitated by weak controls in the IT systems, but also because of a lack of adequate controls in the processes for controlling change to the IT systems. An investigation (Australian Prudential Regulatory Authority, 2004) found that the traders requested, and were given, new features in their systems that enabled them to bypass standard review procedures and to extend the depth of their irregular trades while avoiding detection. They called this feature "Deal Surrender", and it seems that nobody thought to ask what it was for, or why it was needed.

There are many examples, in all markets, of the risks that are contained within information systems used in all sectors of government and industry. The range of risk clearly extends beyond the mere possibility that an anticipated benefit will not be attained. As examples cited above, and numerous other well-documented and comprehensively researched situations have demonstrated, the current and future use of information technology includes significant risks for individuals, communities, corporations and governments. It is arguable that the scope of risk today extends to the environment and the entire world.

One does not need to go to specialised press to find examples of IT disasters:

- ❖ British Gas sued Accenture for £182 Million (Daley, 2008). Reports say that a failed project to develop a new billing system resulted in the company losing a million customers and having to employ 2,500 additional staff for two years;

- ❖ British Sky Broadcasting (BSkyB) sued EDS for £709Million (Songini, 2004), following failure of its Customer Relationship Management (CRM) initiative;
- ❖ A listed pharmaceuticals and retailing company was suspended from trading for eight weeks, and lost over 27% of its market capitalisation (Australian Pharmaceutical Industries Limited, 2006) when, after installing a new Enterprise Resource Planning (ERP) system, it was unable to reconcile accounts and unable to produce statutory reports;
- ❖ In 2005, the Australian Customs Service introduced a new system for clearing imports into Australia. The changeover experienced major problems from the outset and the prior system was reinstated three weeks later. A subsequent review (Australian National Audit Office, 2006) stated bluntly: *"the implementation of the imports component of the ICS caused substantial disruption to the movement of cargo at Australia's major ports and airports"*;
- ❖ The Royal Bank of Canada installed routine maintenance changes to its accounting applications (Luciw, 2004) and was unable to calculate balances for five days;
- ❖ A problem with the boarding gate system at Los Angeles airport (AAP, 2003) resulted in a Qantas flight to Melbourne carrying a passenger who was supposed to be flying Cathay Pacific to Hong Kong, just 18 months after the attack on the World Trade Centre, at a time when airline security was supposed to be at an intensive level.

This small selection of disasters shows clearly that significant damage can arise for any organization that depends on IT, through both project failure and operational failure. And the damage is often not confined to loss of up-front investment. BSKyB is claiming that the company has lost significant anticipated benefits. For British Gas, the consequences of problems include loss of customers and increased operational costs. In many cases, the reputational damage from IT problems is as significant, if not more significant, than the cost of the problem itself.

Industry researchers such as Standish, Butler, Forrester, Gartner and KPMG have confirmed in diverse reports, that the problem with IT breakdown continues to be substantial. Indeed, as IT becomes more and more integral to the operations of organizations, the consequences of failure are increased and the likelihood of failure arising out of complexity is increasing.

The challenge for organizations is, clearly, to improve their success with IT. By doing so, they stand to gain substantial benefits such as:

- ❖ Reduced risk of failure of projects;
- ❖ Reduced risk of business interruption;
- ❖ Lower cost of projects;
- ❖ Greater benefits and earlier access to benefits from successful projects;
- ❖ Better and more sustained business performance through more effective use of IT;
- ❖ Improved competitive advantage from established and future IT assets.

While there is little comprehensive research on the total potential gain to be made from significantly improved success with IT, one study (Young, 2006) which analysed a variety of authoritative literature concluded that in Australia, improved governance of IT projects alone has the potential to lift national Gross Domestic Product (GDP) by 1.6% to 3.1%.

Clearly, there is a compelling reason to improve the performance of IT use within many organizations.

1.2 The IT management improvement industry

The cost of Information Technology, the relentless demand for more and more IT capability, the increasing dependence of organizations and communities on IT, and the desire to avoid project and operational problems as described above has resulted in many, diverse efforts to improve the controls and disciplines surrounding Information Technology. The IT Management Improvement Industry really came into existence in the early days of computing, but emerged as a significant force during the 1990's, as more and more organizations invested in developing and adopting methodologies and management tools.

Nobody would suggest that either the IT industry or IT organizations have not been trying to improve their performance. Although IT is a young discipline by comparison with accounting, its novelty, technical complexity, growth and importance has resulted in enormous investment in development of techniques for making IT more predictable, reliable, efficient, and effective.

Proprietary project methodologies and operational management frameworks have been available for at least some computer users since the earliest use of computers in business. Many organizations have moved through generations of such tools in an effort to improve their performance. During the 1980's as proprietary computing platforms began ceding ground to more generic platforms, there was an initial trend to discarding these frameworks because their proprietary basis was seen as "not fitting" the new world. Well established and mature approaches to management of information technology were abandoned in pursuit of lower cost and greater flexibility. This dismantling of controls became the breeding ground for countless operational and project failures, fuelled by a lack of comprehension of risk and responsibility. But, over time, the resulting vacuum has driven creation of new, more universal frameworks, the development of which has been sponsored by both government and independent industry bodies.

Nowadays, organizations can obtain frameworks, guidelines and tools from diverse public and commercial sources. In many cases, these are supplemented by extensive training and certification schemes that address the needs of individuals and organizations. In some disciplines, obtaining professional employment is increasingly dependent on having acquired a relevant individual qualification. Some of the more widely known organizations that have been contributing to improvement of IT include:

- ❖ ISACA – the Information Systems Audit and Control Association, and its affiliated organization, the Information Technology Governance Institute (ITGI), through which it publishes the CobiT and ValIT frameworks;
- ❖ PMI – the Project Management Institute, which is the custodian of the Project Management Body of Knowledge (PMBok);
- ❖ The United Kingdom Office of Government Computing (OGC), which is the creator of many frameworks and methodologies, including Prince2 (for projects), Gateway (for investment control), ITIL (for IT Operations and Service Management);
- ❖ itSMF – the IT Service Management Foundation, which promotes the business benefits of IT Service Management best practice and the adoption of relevant standards by the IT industry as well as other non-IT related organizations that provide products and services to their customers. itSMF engages with the international standards community to contribute to the ongoing development of the ISO/IEC 20000 series of standards, and co-operates with OGC on the continuing development of ITIL and associated resources;

- ❖ IPMA – the International Project Management Association, which works through national affiliates to provide professional context and development for people involved in organising and managing projects of all kinds, including IT projects.

Governments have been active as well. While the UK OGC (cited above) has been a leading provider of public domain intellectual property, many other governments have sought to minimise the sovereign and economic risk inherent in IT use through various levels of informal and formal guidance, and in many cases through explicit regulation and legislation.

Probably the most widely known of the legislative frameworks is the US Sarbanes Oxley (SOx) legislation. This law is widely documented and has spawned its own industry of consultants and advisors. While addressing a much wider range of issues than IT, SOx also mandates a number of specific controls around IT that have required substantial investment for organizations that are listed or traded on US financial markets. Other nations, seeking similar levels of assurance to that envisioned by the architects of SOx have established similar legislation, and we have seen the emergence of legislation such as JSOX (Japan) and KSOx (Korea).

But direct legislation is not the only vehicle by which governments are demanding rigour and control over the use of IT in key areas of their economies. In some national jurisdictions, legislation and regulation have been used to mandate use of selected frameworks. For example, in May 2006 the Banking Regulation and Supervision Agency of Turkey mandated that all banks operating in Turkey must adopt COBIT's best practices when managing IT-related processes (ISACA).

The IT Improvement Industry is of course not limited to the public domain resources and legislative demands mentioned above. There are many IT software vendors and consultants who offer proprietary product and services all ostensibly designed to assist their clients to improve performance, avoid risk, understand their current situation, and make better decisions. It is not the purpose of this book to detail them. Indeed, anybody who wants to explore this angle would need to do little more than enter "IT Governance" into any internet search engine, and then wade through the tens of thousands of results that will inevitably be returned.

So, has the IT Improvement Industry made a difference?

1.3 Impact of improvement

It's important to say that it is not the purpose of this book to present an exhaustive, or even a comprehensive analysis of the efficacy of IT Governance investments that have been made by organizations over the past ten to twenty years.

But, it is fair to say that the anecdotal evidence – the evidence that is reported in the press and that which circulates along the informal industry grapevines – is generally saying that we still have too many problems. After several years of effort by IT organizations implementing improvements with frameworks and tools, the rate of problems with IT projects and operations has, arguably, not improved. People in the IT industry are asking questions like "Why has IT Governance Failed³?"

The long running Standish Chaos Report does tell us that there is a trend for projects to meet budget and time estimates more accurately. This may be a consequence of better project

³ A discussion on an international web based forum at <http://itgovernance.groupsie.com/> in March 2009 focused on "Why has first generation of IT governance framework failed?" drew a wide range of responses, all offering explanations, but none disputing the premise that the early investments in "IT Governance" have failed to deliver the certainty that has been desired.

planning and management methods. But it is also being increasingly recognised that time and budget are not the most useful determinants of success for projects.

Increasingly, the real measure of success for projects is seen as the extent to which the project delivers intended business outcomes and sustainable operation of the business. But, surprisingly, few organizations measure at this level, and only 13% of organizations surveyed (KPMG, 2005) track benefits until they are realised and formally reported on. KPMG said that only 41% of organizations have any formal approach to benefits realisation at all. No subsequent reports have suggested any significant shift from these results.

So IT Governance investments may have improved project performance somewhat, in terms of basic management measures like time and budget. But, with the continuing lack of emphasis on the important measures – business outcomes and their achievement, it seems that there has not been a great deal of progress.

Certainly, when one considers the continuing examples of project failures that are discussed in the press (and remember – these are generally only the really big failures that simply cannot be hidden), there is a fairly strong case for arguing that the investment in IT improvement has not delivered the desired rate of improvement.

But use of IT is not just about projects. In fact, many analyses of IT spending show that the vast majority of IT spend is operational – and often considered non-discretionary. There's little doubt that operational dependence on IT is significant for many organizations, and the consequences of operational failure in IT can be severe. This is particularly so when one considers that the domain of operational use includes the continuing maintenance and evolution of systems once they have passed through the initial project that created them. Of the problems listed earlier in this chapter, we can see that the Qantas, Royal Bank of Canada and the National Australia Bank experiences were associated with operational management rather than with projects.

Some researchers (Kim, Milne, Phelps and Castner, 2006), (Cater-Steel and Tan, 2005) have looked at the factors that influence operational performance (in its broadest sense) of IT, and some have looked at the contribution of frameworks to the improvement of IT performance, but to date, there appears to be no substantial and rigorous research that establishes a broad baseline of the overall performance of IT as it is used to enable day to day business operations. Generally, their work appears to indicate that robust management frameworks and controls are significant contributors to good internal performance of IT as a service supplier. However, there does not seem to be any insight regarding trends. We don't seem to have any evidence of whether business overall is experiencing more or less disruption as a result of something happening to its operational use of IT.

In essence, what we are seeing from the researchers, whether in projects or operations, are conclusions that the IT components of those two fields are improving. That is, IT Projects that create new technology capability for the organization, and IT Operations that provide IT services to the organization are slowly, but surely, becoming better. But, there is no convincing evidence that following any of the IT Governance guidelines will lead to superior business performance (Young, 2006).

But despite these improvements, we continue to see major IT initiatives going wrong, and we continue to see business suffering financial and reputational damage because of operational problems.

So what are we missing?

Promotional Extract

This promotional extract may be circulated freely

2 The standard for governance of IT

2.1 The requirement

With the money that has been invested in improving the management and delivery of IT, any reasonable observer would expect that failure of IT projects and operational disruption to business would be a thing of the past. But the reality is that the problems continue. Organizations still suffer major embarrassment and damage because IT related activities go off track.

It is not difficult to conclude that the risks inherent in the use (or non-use) of information technology must be controlled, and this is a fundamental aspect of the discipline we have in the past known as "IT Governance". And it is true that organizations have been investing, for several years, in improving their "IT Governance".

Frameworks, software and consulting advice regarding how to manage IT have been in abundance for several years. Terms such as CobiT and ITIL are familiar to most IT leaders, and there are global communities of professionals who are well versed in these frameworks, as well as in many other frameworks, methodologies and tools. These frameworks are complemented by standards such as the ISO/IEC 20000 (IT Service Management) series and ISO/IEC 27000 (Information Security) series. But careful examination of failures that have occurred often reveals problems that cannot be ascribed to poor process or lack of suitable management systems and tools.

Some of these frameworks and standards have been described as being the means to achieving effective "IT Governance". But organizations that have used them still encounter problems. Indeed, the research presented by Standish in the Chaos report clearly indicates that improved management techniques may be improving time and budget performance but is making little impression on overall success.

All of the frameworks available to date in the IT industry are, in reality, management frameworks, and the vast majority of them are primarily oriented to the management processes for supply of IT. Indeed, the core thinking that underpins the notion of IT Service Management and the ISO 20000 family of standards is of encapsulating IT as a supply provided to its (internal and external) customers.

The frameworks do not cover all the bases when we move from the narrow focus of how IT is supplied, to consider the broader question of how organizations actually use IT. When we look at this broader question, we discover that other factors go wrong. Ultimately, the failures come down to ineffective management decisions and the failure of management to do its job properly. It's not just in supply that IT can go wrong – problems are frequently found in the demand and usage side of the equation.

Oversight of management, to guide it in terms of the decisions that it makes, and to monitor its performance, is one of the fundamental roles of governance in an organization context. Therefore, a complete examination of the problem of IT failure leads to the inevitable conclusion that better governance in respect of an organizations use of IT should lead to better performance. But governance of IT is not management of IT, and the frameworks that have sometimes been referred to as governance frameworks are in reality management frameworks.

The requirement, clearly, is not for more management frameworks. Rather, it is for guidance on directing and monitoring the behaviour and performance of the organization and its management in determining and extracting the value from its use of IT – dealing equally with the demand aspects and the supply aspects.

2.2 Australian Standard AS 8015

Australian Standard AS 8015 was launched in Sydney on 31 January 2005. The AS 8015 launch event included speeches by the Chief Executive of Standards Australia, and, notably, the Chief Executive of the Australian Institute of Company Directors (AICD), who said:

The tasks in the standard we are launching today that relate to directors are quite specific: Directors should govern Information and Communications Technology through three main tasks:

- 1. Evaluate the use of Information and Communications Technology;*
- 2. Direct preparation and implementations of plans and policies;*
- 3. Monitor conformance to policies, and performance against the plans.*

This is a sensible framework... Obviously this closely links into the long established and crucial director obligation to understand and manage the risks of the business properly. From the directors' perspective, risk management is a duty that is taken seriously. It is closely aligned with determining the correct strategy for the company.

The proposal to develop AS8015 came initially from a Chief Information Officer who was frustrated by the failure of his attempts to improve the success rates of IT projects in his company. Following a preliminary conference of experts sponsored by Standards Australia, the opportunity was confirmed to research and develop new thinking on how to ensure that projects were successful. Standards Australia established a Technical Committee, known as IT-030, and charged it with the task of developing the first of a new family of standards. Under the leadership of Dr Ed Lewis, of the University of New South Wales and the Australian Defence Force Academy, experts from diverse backgrounds researched failures and developed theories regarding the issues behind IT failures.

IT-030 recognised that, unlike the other major disciplines in Corporate Governance, Information Technology was frequently given insufficient attention in the boardroom. In some organizations, it was seen as being of low importance compared with other strategic issues and the ever-present need to monitor both financial performance and conformance. In others, IT was seen as too esoteric, too complex and too time-consuming for directors to give it time – even when it was known that the risk of problems was quite significant. Directors often felt that they were poorly equipped to ask questions about things they did not understand, and they were at the same time in despair of the babble that they would hear when IT was presented to them.

IT-030 recognised that the problem was because the boardroom discussions of IT were frequently at the wrong level. They talked of technology, rather than the use of technology. They talked of problems, not opportunities. They were all about supply, rather than demand. Too often, the discussion of IT was lead by technology specialists rather than by business leaders who could focus on the way the technology would be used to further the business goals. In some cases it was also seen that business leaders would adopt (and frequently misuse) the jargon of the technology specialists, leading to even greater confusion.

So the challenge for IT-030 in AS8015 was to re-engage the board of directors, and provide organizations with new guidance on how to ensure that IT use is always effective, efficient and acceptable. IT-030 addressed this challenge by identifying that governance of IT needs to address both the creation of future capability (projects) and the reality of day to day business dependence on IT (Operations). It established a new model for the Governance Cycle, where needs and opportunities are evaluated, direction is given, projects are delivered, business

operations are conducted and the entire system of IT use is monitored for performance and conformance. This straight-forward Governance Cycle was complemented by six profoundly simple, yet fundamental principles for governing IT – principles that could be considered at each point in the Governance Cycle. This book will, of course, explain more about this governance cycle and the system of governance that it predicates.

2.3 ISO/IEC 38500

2.3.1 Development and adoption

ISO/IEC 38500 was announced (ISO, 2008) to the international market on 5th June 2008. This event marked a seminal milestone in a journey that started with the first discussions of AS 8015 in Sydney, during the latter half of 2002.

Soon after the Australian Launch of AS8015, the body responsible for development of international standards relating to information technology (Joint Technical Committee 1 of ISO and the International Electrotechnical Commission – commonly known as ISO/IEC JTC1), through its Systems and Software Subcommittee (SC7) surveyed the market for standards that would guide the world's IT users in improving their operational and strategic success. This survey resulted in international adoption of BS15000 as ISO/IEC 20000 (Information Technology Service Management), and a subsequent invitation to Australia to submit AS8015 for processing via fast-track procedures to an ISO standard. The fast-track process began in mid 2006, and reached its climax at a meeting of SC7 in Montreal, Canada in October 2007.

The fast-track process for ISO/IEC 38500 was facilitated by a special Study Group set up within SC7. More than 20 nations were represented in the Study Group, which reaffirmed the learnings of IT-030, that a new perspective on governance of IT was most certainly desirable, and that AS8015 provided a new line of thinking that should help improve success in the use of IT for many organizations.

Fast-track processing of any standard involves the origin document (in this case AS8015) being circulated to and voted on by JTC1 member nations. Complex voting rules ensure that any draft standard must enjoy significant acceptance before it is deemed successful, and in this case all required margins were comfortably exceeded.

The fast-track voting process allows for comments to be submitted with both Yes and No votes, and AS8015 attracted 153 comments from voting nations. While some were editorial in nature, pointing out changes that would have to be made in transitioning the standard from the Australian context to the international context, many of the comments provided constructive suggestions on how the standard might be improved. A revised draft of the standard was reviewed by the voting nations, and particularly those who voted in the negative, in Montreal in October 2007. Over a four day period, the amendments were debated and refined, with all nations that had initially voted against adoption of AS8015 changing their votes and accepting the revised document. Thus, ISO/IEC 38500 was accorded the honour of unanimous acceptance (excluding those nations that, for whatever reason, did not cast a vote) by the voting nations in the final record of the fast-track process.

ISO/IEC 38500 improves on AS8015 in several important ways. It is not the purpose of this book to explore those differences – though perhaps a student may wish to do so in pursuit of a doctoral thesis. However, it is worth noting the key changes.

First – the introductory material in section one has been tidied and clarified. The audience for the standard is better defined, and the reasons why the standard should be applied are both clearer and more universally relevant. Importantly, the definitions have been expanded and

refined. For the first time, there is a definition of “management”, which is most important in developing distinction between the concepts of governance and management.

Second – the definition and explanation of the principles has been restructured and made clearer. The principles now have a single word name, rather than a sentence. While they are no longer expressed as an imperative (which some may have seen as an auditable instruction), they do now set out the desirable characteristics of organizations that have good behaviour and good governance. It is easier to judge, just on reading the standard, whether or not your organization has some alignment with the principal.

Experience has shown that the principles are extremely powerful. But they do not relate just to the role of the directors. They in fact relate to the entire organization, and provide a frame of reference for considering and guiding the behaviour of the organization. It is not difficult to understand that an organization that behaves well, according to the principles, has a much better chance of success than an organization that behaves badly. The author’s own experience in assessing organizations reinforces this point – those organizations that consistently have trouble with IT also consistently behave poorly when evaluated through the lens of ISO/IEC 38500. Examination of many IT problems, with both projects and operations shows that in every case, at least one and often, several of the principles has been violated.

Third – the guidance on good governance practices has been markedly improved. It is clearer, more consistent and more comprehensive. It should be more meaningful for those who are embarking on their first assessment of whether their governance of IT is effective. A cursory examination by a member of the ISO JTC1 Study Group of the globally notorious Heathrow Terminal Five debacle suggests that every one of the six principles was violated. The reputation damage suffered by British Airways and BAA should thus be no surprise at all. How could the executives and directors of these organizations have recognised the reality that they were driving headlong into a disaster? Perhaps they might have benefited from the guidance in the standard regarding good governance practices.

What has not changed in ISO/IEC 38500 is the way it applies to all organizations, regardless of scale, structure and purpose. It does this by avoiding any suggestion of requirement for structure and process. It does not tell any organization what to do – rather it encourages all organizations to think about what they need to do, and how they go about doing it.

Some may be frustrated by this aspect of ISO/IEC 38500. It is not a recipe book. It is not a “one size fits all” answer to the great dilemma of how to keep IT under control. But neither is it a panacea. ISO/IEC 38500 guides organizational behaviour, and provides the board or other governing body with a lens through which to check that management is doing the job of managing IT properly. It does not replace established frameworks, such as CobiT and ITIL, and does not obviate the need for tools to assist with managing portfolios of projects or IT Service Delivery. Instead, it complements these established resources, and provides a much-needed additional focus on the demand side of IT use – where the organization as a business is responsible for determining the extent and manner in which it uses IT as an enabling tool.

2.3.2 Subsequent developments

Following international adoption of ISO/IEC 38500, JTC1 undertook a further international study to determine whether there is a demand for, and how it should manage further standards relating to governance of IT. In November 2008, JTC1 acted on recommendations of this study to establish a new Working Group that would focus on further developments. This Working Group, now known as JTC1 WG6, met for the first time on London in May 2009 and immediately began work on clarifying a most important issue – the relationship between governance and management of information technology. Over time, JTC1 WG6 can be expected to advance on

several tasks, including updating of ISO/IEC 38500 and development of further, more specific standards for governance of IT use. The need for further development has been already realised in Australia, where work is under way on more detailed standards covering the two main subjects overviewed in ISO/IEC 38500 – Projects and Operations.

2.3.3 A synopsis of ISO/IEC 38500

It is extremely challenging to summarise the 15 pages of ISO/IEC 38500 in this book without reproducing the entire standard and violating a raft of intellectual property laws. For that reason, this extremely brief synopsis is taken from the original press announcement (ISO, 2008) of the standard:

"Because inadequate information technology (IT) systems can hinder the performance and competitiveness of organizations or expose them to the risk of not complying with legislation, the new ISO/IEC 38500 standard provides broad guidance on the role of top management in relation to the corporate governance of IT.

François Coallier chair of the ISO subcommittee, Software and systems engineering, that developed the standard comments: "Most organizations use IT as a fundamental business tool and few can function without it. IT is also a significant enabler in the future business plans of many organizations. ISO/IEC 38500 will help the governing body to evaluate, direct and monitor the use of IT.

"It will assist directors in assuming conformance with obligations – regularly, legislation, common law, contractual – concerning the acceptable use of IT and to have a proper corporate governance of IT."

ISO/IEC 38500:2008, Corporate governance of information technology, is applicable to organizations of all sizes, including public and private companies, government entities, and not-for-profit organizations. This standard provides a framework for effective governance of IT to assist those at the highest level of organizations to understand and fulfil their legal, regulatory, and ethical obligations in respect of their organizations' use of IT.

The framework comprises definitions, principles and a model. It sets out six principles for good corporate governance of IT that express preferred behaviour to guide decision making:

- ❖ *responsibility;*
- ❖ *strategy;*
- ❖ *acquisition;*
- ❖ *performance;*
- ❖ *conformance;*
- ❖ *human behaviour.*

The purpose of the standard is to promote effective, efficient, and acceptable use of IT in all organizations by:

- ❖ *assuring stakeholders that, if the standard is followed, they can have confidence in the organization's corporate governance of IT;*
- ❖ *informing and guiding directors in governing the use of IT in their organization; and*
- ❖ *providing a basis for objective evaluation of the corporate governance of IT".*

The model for governance of IT provided in ISO/IEC 38500 defines three fundamental governance tasks – Evaluate, Direct and Monitor, which are applied to the proposals for use of IT, the projects that implement use of IT and the operations that are dependent on IT.

All readers of Waltzing with the Elephant should read and use ISO/IEC 38500. By doing so, they will be able to correlate the in-depth discussions with the expectations defined in the standard.

Promotional Extract

This promotional extract may be circulated freely

3 Understanding governance of IT

3.1 The fundamental equations

To fully understand the scope of governance of IT and the effectiveness of contemporary investment in "IT Governance", and to fully understand the position of ISO/IEC 38500, requires clear and consistent understanding of some fundamentals of IT use in any organization.

It's important to recognise that the fundamentals we will discuss in this chapter are intuitive common sense. But we all know that common sense is remarkably uncommon, and so we should not be surprised to realise that when we look at how organizations control their IT, they often display symptoms of not understanding these fundamental equations.

There are two fundamental equations that we need to consider:

- ❖ Supply ↔ Demand – the fact that business demand drives the supply of IT which in turn provides business capability that demands IT service;
- ❖ Business Systems = (People + Process + Structure + Technology) – the fact that information technology alone does not actually do anything; results only occur when IT is combined with three other vital ingredients to make a business system.

3.1.1 Supply ↔ demand

Exactly why do organizations invest in IT? Surely it is to achieve a business result that is consistent with its purpose! Can anybody today imagine an organization other than an IT vendor doing R&D investing in IT merely for the sake of experimentation?

IT has a business purpose. This notion is intrinsic to any investment in or application of IT. The business purpose must be identifiable in business terms, and should fit into one of three classifications:

- ❖ Strategic capability – enabling the organization to do something that it was previously unable to do;
- ❖ Operational capacity – enabling the organization to efficiently and effectively conduct its current business;
- ❖ Regulatory conformance – enabling the organization to meet the requirements of external regulators.

Regulatory Conformance is in effect the organization's license to continue in business. It must be considered, and the necessary capabilities created when planning and implementing strategic capability. And it must be an integral, and effective, part of the ongoing operational capacity. In reality, while regulatory conformance may be cited as a reason (and entirely validly) for spending on IT, it is a subset of the other two – the main reasons for investing in IT.

We can classify the use of IT by an organization as "Demand". If the organization were not in its chosen business, or not following its chosen strategic development path, or not operating in its selected regulated environment(s), the use of IT would be different. The demand made of IT by the business is specifically driven by the choices of the business leaders regarding what the business is, how and where it operates, how it competes, and how it evolves.

Similarly, we can classify the provision of IT to the organization as "Supply". It would seem sensible that the supply of IT should meet the demand – that it enables the organization to conduct its intended business, following its chosen strategic development path, and operating in its selected regulated environments.

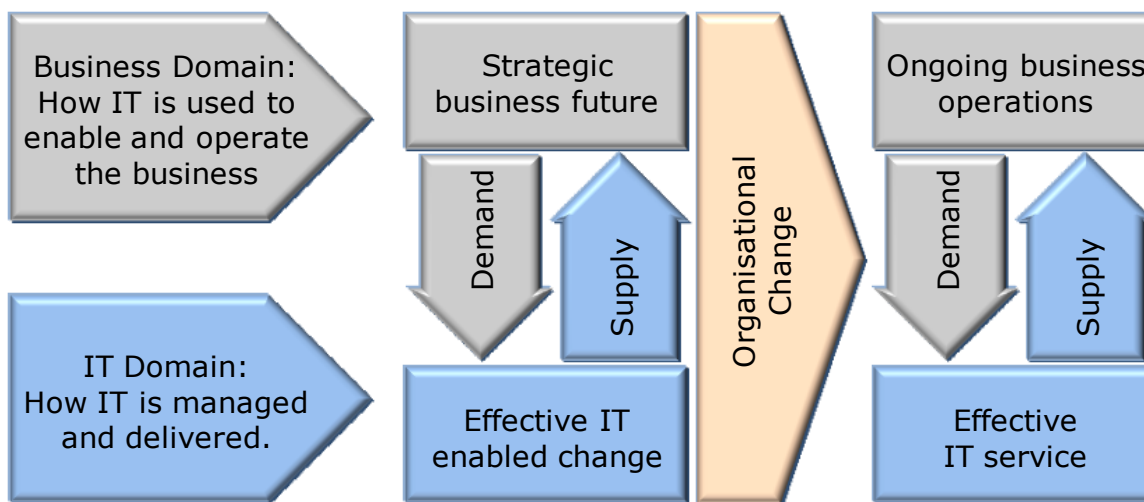


Figure 1: The demand ↔ supply equation

The model presented in figure 1 highlights that demand and supply involves a symbiotic relationship between two “domains” – the Business Domain and the IT Domain. Each domain has its own set of responsibilities and issues, but neither can, or should, exist and operate effectively without the other also being effective. Simply:

- ❖ The business domain is responsible for demand. Demand is a product of planning and running the business. It includes determining what the business is, and how it operates. To plan virtually any business in the 21st century demands an understanding of how information technology (among others) can influence and enable the business. Any organization that does not take information technology into account as part of its strategic and operational planning is likely to miss opportunities, and to be beaten by its competitors.
- ❖ The IT domain is responsible for supply. Supply involves planning, organising, implementing and running the IT that is needed to enable the business – to underpin its strategic intent, and to make its day to day operations reliable and effective.

The model also introduces the notion of “Organizational Change”. This is the process by which the intended strategic future of the organization becomes its day to day reality. We will explore Organizational Change further when we discuss “The Business System”.

For a moment, think again about the relationship between the business (demand) domain and the IT (supply) domain. Consider the focus of the IT Improvement Industry that we discussed in the previous chapter. Is there a problem here?

The vast majority of the IT Improvement Industry has focused on the supply domain. The frameworks and standards have been developed largely by IT specialists, and are predominantly sold to IT specialists, with a view to making the IT Supply function as effective as it can possibly be.

Of course, there was plenty of room for improvement in the IT supply domain, and anecdotal evidence suggests that there is plenty of further room for improvement yet. But there has been comparatively little attention given to the business demand domain, and in many cases, what attention has been given is focused through the perspective of IT supply. It may be the case that, by focusing on the demand side a little more, we may be able to improve the way, and the success with which organizations use IT.

Focusing on the demand side involves understanding that IT is in fact nothing more or less than a tool of business, and it is ultimately the business that determines how effectively it uses that tool. IT can no more be separated from and run independently of the business than can Human

Resources or Finance. Responsibility for the successful use of IT can not be ascribed only to the IT team any more than responsibility for successful sales performance can be assigned purely to the head of finance. The reality of contemporary business is that demand for and supply of IT are so closely linked, and so fundamental to business performance, that true success in use of IT can only come from a highly integrated approach to planning and directing the use of IT that involves both the demand and supply sides of the equation.

It's not just a matter of IT specialists understanding business demand and tailoring supply to suit. For organizations to be effective, business must understand the capability and opportunity in use of IT, and the risks associated with decisions to use, or not use IT.

Thus, recognition of the need to be clear about demand for IT is one of the key attributes of ISO/IEC 38500, and the primary reason why its focus is on the use of IT.

3.1.2 The business system

The operations of any business can be described as a system. In effective organizations, it is likely that the system, or set of interrelated systems that make up the business are organised, coherent, well understood, and evolving to adapt to changing internal and external circumstances. In less effective organizations, the converse is often evident – the business systems are not so well organised (perhaps to the point of being chaotic), are not well understood and do not evolve.

For most organizations, the overall business system is made up of subsystems that integrate at key points to ensure effective overall operation. There are many ways of identifying the business systems, but it is not the purpose of this discussion to go into that topic in detail. It should suffice to say that common domains for business systems include supply, production, distribution, sales, marketing and finance.

To better understand what makes up a business system, we can adapt the diamond model of organizational change (Leavitt, 1964). Leavitt's model proposes that a business system is comprised of four interacting elements, as depicted in figure 2.

To remain consistent with contemporary nomenclature, what Leavitt referred to as "Task" is now called "Process". The point of Leavitt's model is that the four elements interact to make a business system operate. Changing a business system generally involves changing more than one element.

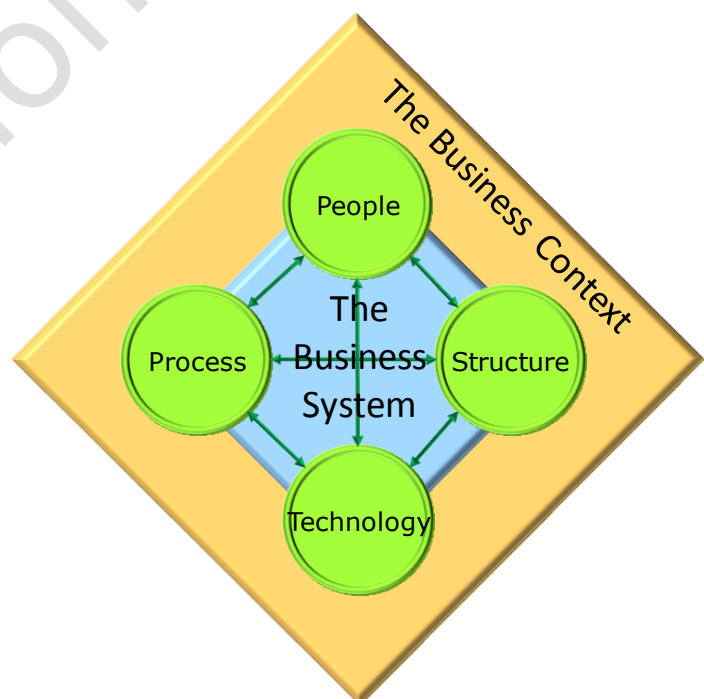


Figure 2: Key elements of the business system

Generally speaking, changing one of the interacting elements will have a consequence for the other elements. However, it does not follow that changing one element will have a desired

impact on the others, and to maintain the system in equilibrium, it is necessary to be explicit in making the required change in each.

We can further extend Leavitt's model by recognising that every business system operates in the context of its external business environment (business context), over which it has relatively little direct control and to which it must adapt over time. The context for a business system includes other organizations and individuals – its suppliers, competitors, customers, labour market, educators, regulators and so on. It is within this context that business systems are designed and implemented, using four basic building blocks:

- ❖ People, who work in the system and provide the "glue" that is essential when dealing with uncertainty;
- ❖ Process, which is the set of tasks that are undertaken in achieving the outcomes, regardless of the extent to which they are automated and how they are sourced;
- ❖ Structure, which provides boundaries on operation (such as geography and time) and which provides authority for decision making (including for escalation and delegation);
- ❖ Technology, which provides enabling capabilities, throughput, performance, control and numerous other features that are essential for any contemporary business.

These four building blocks interact to make a business system operate. By tuning the individual building blocks and adjusting their interactions, business systems can be adjusted in many dimensions, such as throughput, speed, reliability, cost and adaptability.

Understanding the nature of the business system is key to understanding the role of IT in support of the business. Organizations use IT to enable people, process and structure to be arranged in new, more effective and more reliable ways, with greater capacity, greater reach and greater availability.

Application of IT alone does not automatically result in improved business systems.

In the early days of IT, where automation was focused on speed and volume, especially in background tasks like accounting, there was little impact of the IT on either the process or the structure. And the impact on people was straight-forward to understand as well – for a given volume of work, less people were required. But there is a limit to the opportunity for mere speeding up and increasing capacity of routine processes, and it is quite arguable that that boundary was passed quite some years ago.

With increasing capability in information technology, and increasing sophistication of IT use by market leaders and innovators, it has become clear that the speed and volume opportunity presented by IT is trivial by comparison to the new opportunities in respect of process, people and structure. Organizations can now do things that were previously not possible. People can perform tasks that they previously could not perform. And organizations can expand beyond their old boundaries of time, geography and scale. Information Technology has become the enabler of remarkable transformation in organizations, and clever use of technology has resulted in enormous transformation of some organizations and even markets.

But, refer to the model in figure 2 again. Think about the transformations that have been made by organizations that have been successful in their efforts to gain advantage through use of IT. Now consider the models presented overleaf in Figure 3.

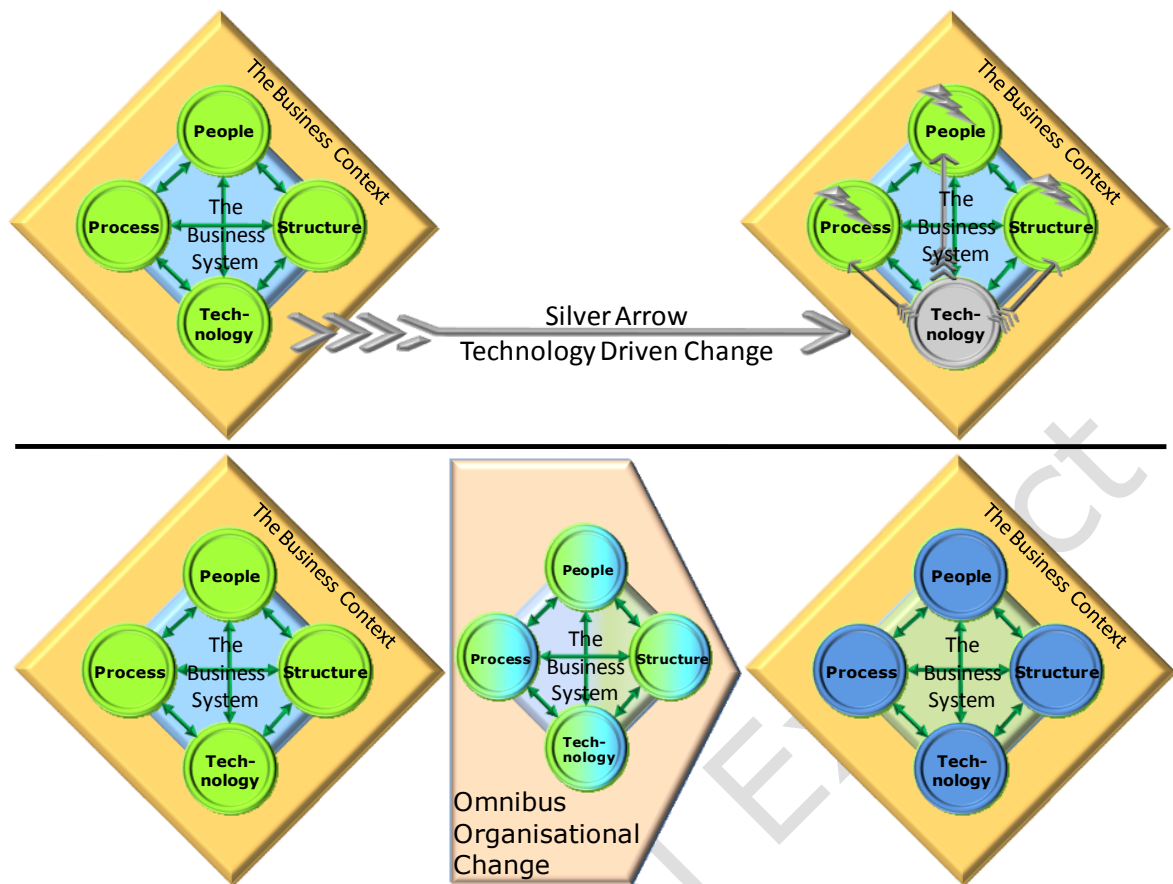


Figure 3: Models of change.

Figure 3 presents two common models of change. Some (perhaps many) organizations, often without realising it, use the top model – where the “Silver Arrow” of information technology is the lever through which change is driven into the business system. Other organizations use the model at bottom – where the “Omnibus of Change” works on all four elements of the business system to integrate and progressively transform the system.

Silver Arrow scenarios occur when organizations treat information technology as the driving force of change. What happens is that the majority of the attention goes to the IT component, and an expectation (often subconscious) develops that the people, process and structure elements of the system will adapt to the new technology, thus realising the benefits that have been postulated. Compounding the problem with silver arrow scenarios is the tendency of IT organizations, both internal and external, to strongly believe and sell the proposition that they can successfully drive the change from the IT perspective. And because change is, in many cases, a difficult and challenging task for business managers, they can be all too willing to hand over responsibility and avoid becoming involved.

Not surprisingly, many Silver Arrow initiatives fail. And they fail even when those driving the projects attempt to give some recognition to the people, process and structure elements. Some IT projects have “business readiness” teams, which will go forth before the project is delivered, to train the people to use the new system, and perhaps even to perform the new processes that are being introduced as part of the system. But the problem in these situations is that Silver Arrow initiatives invariably take an IT centric approach to change, rather than a whole-of-business system approach. They miss the opportunity to comprehensively assess and refine the business system in terms of process, people and structure as well as technology.

That doesn’t mean that many IT initiatives are not started for good reasons, and it doesn’t mean that there is always comprehensive failure to consider other aspects (non IT) of the

system. Indeed, more than one IT Silver Arrow has originated in a comprehensive organization review that has proposed new processes and structures, but then as the initiative moves forward the focus narrows to the IT component and the opportunity to effectively manage change is lost.

RMIT University's Academic Management System project of 1999 – 2002 is one example of a major project that started with the intent of transforming business systems, but then became an IT initiative operating with little linkage to the business. A report (Auditor General Victoria, Feb 2003) said: "There appeared to be a general lack of communication and consultation between the AMS Project Team and business users during the implementation of the project".

At this point, some may be drawn to speculate on why the focus narrows to the IT component. Analysing that question is well beyond the reach of this book – but a couple of thoughts should help to keep the issue in perspective. Perhaps it is because the IT is perceived to be “big and complex” that it gets so much attention. Perhaps it is perceived as the first element that must be resolved, well in advance of the other work, which subsequently gets forgotten. Perhaps it is that the complexities of dealing with people in particular, and to a lesser extent process and structure, are too daunting, and avoidance behaviour results in an inordinate amount of attention to the IT. Or perhaps it is that there is a fundamental blindness to the need to attend to the non-technology dimensions, and a genuine, if misguided, expectation that delivering the technology will cause the people to adapt.

Delivering true and effective change to a business system requires direct, focused and skilled attention to the four parts of the system. The change must be planned and managed so that it is implemented in a logical progression, with all intermediate dependencies being properly resolved. We can call this Omnibus Organizational Change.

Again, it is not the purpose of this book to develop the subject of Omnibus Organizational Change comprehensively – indeed there are many books that address the subject of organization change from many points of view. But it is perhaps beneficial to briefly discuss a few aspects of the way that information technology enables and requires attention to complementary change in the other three elements:

- ❖ **Consider Process:** Business processes are the set of tasks or activities that a business undertakes in order to achieve its objectives. In a well-managed business, the processes would be well understood, clearly defined and optimised. As we said earlier, the early use of IT was principally focused on automating routine process, to increase speed and volume, and lower cost of repetitive work. But the capabilities of IT today mean that IT is being used to fundamentally redefine how processes work, and to enable entire new processes. Think of Amazon.com as a seminal example of how IT has been used to redefine a number of key business processes – and particularly the customer relationship and sales processes. Where the most traditional sales and relationship processes involve a face-to-face transactions and personal knowledge of customers, Amazon took the processes and fundamentally redefined how they operate. On a broader scale, it is important to understand that when an organization is investing in IT, it is doing so in order to improve its capability and therefore, it is almost certainly going to be adjusting its processes. To get the process adjustment right requires specific skills in designing and implementing business process – and these are different skills to those required for planning and implementing information technology.
- ❖ **Consider People** (unfortunately, it seems that in many cases, IT initiatives often fail to consider people): People take many roles in a business system. People may be workers

within the system, customers of the system, overseers of the system, suppliers to the system and perhaps mere observers of the system. For a system to be effective, it needs to be in harmony with the people who are part of that system – where the harmony is achieved through tuning of the relationship in all dimensions. Process, structure and technology should be designed with a thorough understanding of the people who are in the system, while the people in the system can be educated and developed so that they can play their part most effectively. Think of Amazon.com again: the development of that business demonstrates a very deep understanding of people – particularly people as customers. Amazon learned, through intensive research, how to engage customers in a new form of transaction – where there is not a face-to-face interaction, while retaining customer intimacy and subtly transferring what was traditionally an internal workload (processing the entire transaction) to the customer.

There are many other dimensions of the People element to consider in IT enabled change, and many more examples of how organizations have used IT to change the way that people operate within the business processes. Banks have moved their sales personnel out of branches and into their customer environments by giving them new technology that enables them to present products, tailor solutions and close deals while in direct contact with the customer. To enable the people to work in this way, however, has involved far more than merely providing the bankers with a new notebook PC and sending them forth. The bankers have needed to be equipped with appropriate personal and job skills to enable them to operate remotely, in less immediate contact with their supervisors, and in environments that are frequently most unlike the office to which they had been accustomed. Their working conditions have needed revision, to the extent that some bankers do not have an “office base”, spending most of their day on the road and completing their routine background work from home. Along with these changes in some banks have come significant changes to remuneration structures, supervision arrangements, and policies regarding dress and hours of work. Imagine what would have happened to a bank had its approach to implementing mobile banking been merely one of handing a sales rep a new notebook computer, and an instruction to “get out with the customers and start selling”! Clearly, using IT to enable a new form of selling, as with new approaches to many other business processes, can involve a substantial impact on the People, and this demands properly skilled attention in its own right.

It bears saying now that there is a new aspect of the People element emerging. With the emergence of what some commentators call the “Digital Era”, more and more people are familiar and comfortable with information technology, and are demanding greater use of, and access to IT enabled capability. Younger people in particular (the “Digital Generation” are exhibiting behaviours never before seen in workplace, commercial and social environments. They expect information technology to be available, to empower them and make their lives “easier”. They expect to be less beholden to hierarchy, to work in more flexible ways, and to not have to perform mundane tasks that can be automated. This characteristic, which needs to be dealt with in conjunction with the frequently opposite-pole behaviours of older generations, means that the People element must now be addressed not merely in terms of responding to an IT enabled change, but as a base driver of new approaches to using IT.

- ❖ **Finally, consider Structure:** Typically, when we think about structure, we think about organization – as represented in structure charts and so on. This is but one important aspect of structure when we consider a contemporary business. When IT is used to enable new business capability, there can be dramatic impact on structure in many ways. Refer once more to Amazon.com. From a single location, that business has achieved global reach – it can be accessed by prospective customers from any place that has an internet

connection. In the not too distant past, global reach could only have been achieved by a physical presence in every city, town and village, with the attendant costs of people and other infrastructure making such arrangements prohibitively expensive and impractical. But of course, reach is only one consideration in structure – Amazon also had to think about logistics and conformance with local laws and customs – factors that would have influenced its decision to operate not as a single entity, but as multiple entities in various locations. Amazon has balanced its structure taking advantage of technology but also taking into account a range of other considerations.

Not every organization is faced with structure decisions as significant as those for Amazon – but it is important to recognise that the use of IT to enable change in business systems is quite likely to have at least some ramification for the business structure. Go back to the bankers – a redesigned approach to loan sales probably needs a new approach to approval and verification. Instead of a paper document being passed through internal mail to a supervisor for approval, an electronic application can now be approved by the representative on the spot – because the IT behind the application has already performed the qualification checks that were done later under the paper system.

Thus, we have covered at a high level, the interaction between People, Process, Structure and IT. It is important that, for effective, efficient and acceptable use of IT, change enabled by IT is addressed from a “whole of system” perspective, giving equal attention to each of the elements, and ensuring that none are given “lip service”.

For another perspective on the point we are making here, consider a different change scenario. Consider the case of an airline which has made the decision to invest in a fleet of Airbus 380 aircraft. These gargantuan airliners “raise the bar” on many of the previous upper limits in the aviation industry. For an airline to use the A380 involves far more than merely being able to sell more seats on any given flight. Apart from the obvious issues like training pilots on the new aircraft, and establishing the engineering capabilities to maintain and support the new fleet, airlines have to work with airport authorities to upgrade infrastructure (wider runways with greater weight-bearing capacity, dual-level loading ramps, larger passenger lounges), develop new crewing structures, restructure routes and schedules, upgrade various IT systems (to accommodate increased passenger capacity and new seating configurations, and to provide correct flight information), and perhaps even upgrade the capacity of flight catering systems to cope with the higher point-in-time demand of provisioning an aircraft that perhaps doubles the previous peak load requirement. Imagine the chaos if an airline were to use the classical “Silver Arrow” approach to change when buying such a new aircraft. The new fleet would be initially unusable, and gradually adjustments would be made around the new fleet to enable it to become fully productive.

Don’t for one minute think that such scenarios never occur. A highly publicised case of a “Silver Arrow” is the disastrous opening of Heathrow’s much vaunted Terminal Five. By going directly to near-full load operations, with no transition or ramp-up period, British Airways and the British Airports Authority put an untested (as it turns out, comprehensively untested) system under full production stress and it immediately broke down. Perusal of the formal review (House of Commons Transport Committee, 2008) reveals that the problems with Terminal five include a failure to pay properly balanced attention to the four elements of change – People, Process, Structure and Technology. It seems that BA and BAA thought that what they were doing was opening a new passenger terminal. What they may not have realised was that they were reconstructing the entire business system for despatching and receiving airline travellers. The latter is, clearly, a much bigger job, of which building and opening a new passenger terminal is quite often an integral enabling element. It is also noteworthy that, under pressure of delays and looming deadlines, BA and BAA reduced the amount of testing. This course of action can be

found repeatedly in the assessments of many IT failures, and gives a clear pointer to a crucial decision factor in approving the live launch of any IT-enabled change: **Has the entire system been fully tested and demonstrated conclusively to be working correctly, to the complete satisfaction of all stakeholders?**

We won't go any further on exploring the relationship of the four elements of the business system. For the purposes of this book, it is sufficient to appreciate that:

- ❖ Information Technology is used to enable organizations to achieve specific outcomes. We would hope (though we know that it is often not the case), that the desired outcomes are clear, specific, measurable, appropriate and achievable.
- ❖ But Information Technology rarely, if ever, achieves specific outcomes on its own. There are aspects of the business system that IT cannot possibly deliver – even at the highest degree of automation.
- ❖ The reality is that information technology alone does not actually do anything – results only occur when IT is combined with three other vital ingredients to make a business system.
- ❖ The Business System = (People + Process + Structure + Technology). This is a vital and immovable concept that if forgotten, often leads to new IT investments being troublesome at best, and frequently being damaging failures.

3.2 The system of governance

There is one other matter that needs clarification before we can get into the standard in detail – though in this case we can explore some aspects of the standard as we go. That is: what do we mean when we talk about governance of information technology – or as many people put it: IT Governance.

3.2.1 Defining governance of IT

The term "IT Governance" has so many meanings, and people interpret it in so many different ways that any conversation about "IT Governance" is likely to suffer from the participants being "on different planets". It's not that we are intending to be difficult about it, but simply the reality that we have been conditioned to think about "IT Governance" from different points of view. For this reason, it may be best to avoid the term, and use better defined alternatives.

A stark, perhaps amusing and ultimately very unfortunate example of the diversity in understanding of the term "IT Governance" arose in the context of the disastrous implementation of the new Cargo Management System Imports Module, by the Australian Customs Service. During the period when the system was failing under extreme stress and the Australian economy was suffering severe disruption to its supply chain, the Customs CIO was addressing an IT industry event, explaining that Customs had extremely well developed and effective IT Governance. Of course, what he was referring to was the internal controls used by the IT department. These controls were far removed from the organization's overall set of controls for the entire project, which was fundamentally re-engineering the business system of importing goods into Australia. (Anecdote provided by a third party).

How did we get to this very interesting and challenging state of affairs, where such a seemingly straight-forward term is so confusing? It's probably a consequence of over-zealous IT industry marketing efforts, where a new term has been appropriated to maximise the selling attraction in diverse products. The IT industry is renowned for its techno-babble and jargon, and it has become de-rigueur for the industry to adopt and pervert words for its own purposes, making it

ever more difficult for outsiders to understand what is going on, and deepening the awful misconception that only IT people can control IT. It seems that, as weak Corporate Governance was identified as a key factor in globally visible corporate disasters such as Enron and WorldCom, so the problem associated with the continuing prevalence of IT problems – and particularly failed IT projects, must have been weak IT Governance. And in many ways, this is an appropriate conclusion.

But just as much of the popular press failed to understand the difference between corporate governance and corporate management (the press often castigates the board of directors for “failing to manage” organizations effectively), so it seems the IT industry did not understand the difference between IT Governance and IT Management. To all intents and purposes, the terms became synonymous, and the term IT Management was reserved for the lowest level of detail in the management system. The problem evolved to the point where most of the management disciplines in IT have been re-labelled, at some point in time and frequently by vendors of software and services with related product interests. Thus we have seen promotions for SOA Governance, Data Governance, Security Governance joining the more widely referenced Project Governance and Operations Governance. Look under the covers of these disciplines, and it is easy to see that they are in fact all management disciplines. The word “management” can replace the word “governance” and there is no loss of integrity in the concept at all.

It’s perhaps excusable in some ways that the confusion has emerged. The words “Governance” and “Management” come from different roots (Greek and Latin respectively) and their ancient predecessors have quite similar meanings. In strict language and dictionary terms, the words could be used almost interchangeably, particularly in the context of making decisions and achieving intended outcomes. But in modern business, other than when used in the IT context, the two terms have generally quite separate and clear meanings. Governing is about directing and controlling. Managing is about working within the established direction and being subject to the control of governance. A Chairman of a bank put the distinction most clearly when he said that “Governing is basically about making sure that management does its job properly”.

Given this confusion, it can hardly be surprising that boards of directors encounter problems when they begin to discuss IT in the boardroom. Because the distinction between governance and management is not clear, attempts to extend “IT Governance” into the director’s domain results in directors being asked to participate in management process – they are expected to operate at too low a level of detail and thus find the engagement both time consuming and technically complex. By the same token, people in IT management roles, even at a very senior level will become frustrated because their endeavours to engage the governing directors in what is a management level will be quite unsatisfactory. Further, such attempts to engage between board and management in what is ultimately a narrow conversation about IT management invariably focuses on the aspects most familiar and relevant to the IT supply domain. The demand side gets relatively little attention, mostly being considered as the driver of IT supply, rather than being addressed in the much more important context of how effectively the organization is using and advancing its capability to use information technology.

ISO/IEC 38500 recognises the problem of confusion in the terminology, and the existence of the plethora of definitions (some are well intentioned and some are quite well aligned to the true nature of governance, but unfortunately many are narrow and focused on an area of self-interest for the definer), and offers new and clear definition for both governance and management in the context of IT.

The ISO/IEC 38500 definition for governance of IT is no mere flight of fancy, nor a fresh definition for the sake of being different. It is in fact a very deliberate choice to reset and re-anchor the concepts of governance of IT in the foundations of Corporate Governance. In doing

so, ISO/IEC 38500 avoids creation of a new definition from the void. Instead, it draws on well established and very widely accepted precedent, adopting the definition of Corporate Governance that became virtually universal as a result of its presentation in the Cadbury Report (Cadbury et al, 1992). Quite simply, Corporate Governance is the system by which an organization is directed and controlled. It follows, most sensibly, that (corporate) governance of IT must be the system through which IT is directed and controlled.

But in writing the standard, its authors also recognised that the confusion created in the market by improper use of the term IT Governance had created for many the impression that governance of IT was all about governing the activities of the IT department or IT supplier. This narrow perspective is inappropriate, and in fact one of the key reasons that IT problems are experienced. As we have discussed in the chapter on the Fundamental Equations, it is not just the supply that has to be directed and controlled, but also the demand. To correct this bias, the authors chose to include the word "Use", thereby bringing focus to the demand side, without excluding the supply perspective. Thus, the formal definition provided says that Corporate governance of information technology is: "The system by which the current and future use of IT is directed and controlled" (ISO/IEC, 2008).

Notice that the standard also includes in the definition the words "current and future". Why did the authors do this? Again, if one looks at the market attention to "IT Governance", one sees a strong focus on the investment side. Indeed, much of the market attention to the topic focuses fairly narrowly on planning and monitoring of the IT investment program – which is of course only a minor portion of the real IT use for any organization. Clearly, as illustrate in the chapter "Why do we need another standard", organizations are as vulnerable to damage from operational breakdown as they are from project failure. The authors wanted to make it clear that governance of IT embraces both the present (operational aspects) as well as the future (investments).

3.2.2 Distinguishing governance and management

Knowing that there is widespread confusion in the IT industry about "Governance" and "Management", the team responsible for ISO/IEC 38500 considered it essential that both terms be defined in the standard. But where there is a readily identified line of authority from which to draw the governance definition, there is no straight-forward line of authority for the management definition. Indeed, when one considers the standards in existence today, it becomes clear that there has been a lack of consistency across those standards, as the concept of management has been locally defined to address the specific needs of those standards. And, as previously noted, the dictionary definitions are not all that useful either because, while they do provide definitions, they do not provide sufficient contextual separation from governance.

After an extensive search of available literature, the path chosen by the project editor was to break new ground, by creating a new definition of management, which would be consistent with the majority of available definitions, but which would also clearly establish the relationship between management and governance. After debate and some tuning during the final international reviews, this new definition of management was adopted: "The system of controls and processes required to achieve the strategic objectives set by the organization's governing body. Management is subject to the policy guidance and monitoring set through corporate governance" (ISO/IEC, 2008).

ISO/IEC 38500 does not limit the notion of management to "IT management". Indeed, management is, and should be, a consistent concept right throughout an organization and across all organizations, just as governance should be a consistent concept. Whether discussing financial management, production management, resource management or technology

management, the underlying understanding of what management is should be entirely consistent.

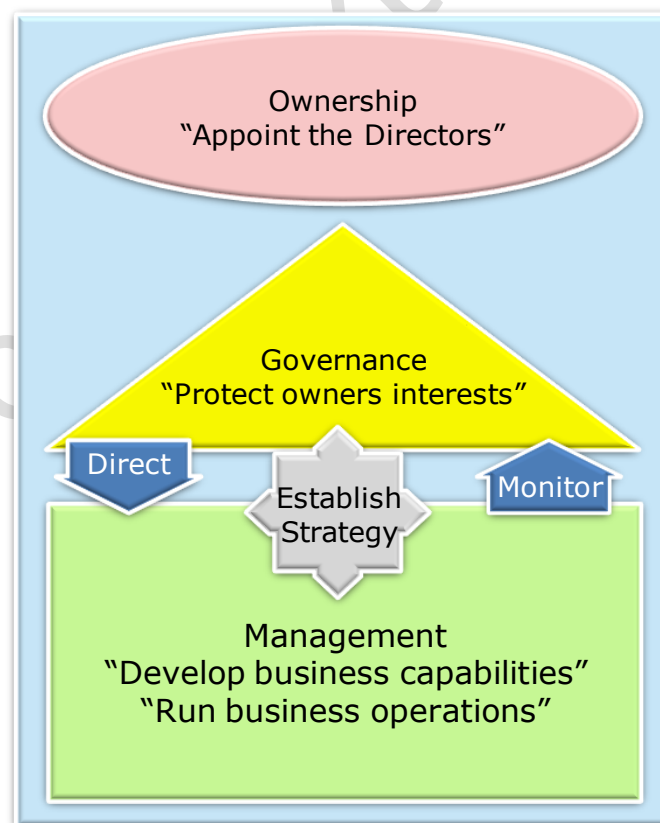
So how do we get a proper understanding of the distinction between governance and management, in the context of Information Technology? The solution lies in understanding that governance of IT is an important part of the overall governance framework for any organization, and that governance itself is a business system.

3.2.3 Putting governance of IT into context

To put governance of IT into context, we need to have a clear and consistent understanding of Corporate Governance. As noted earlier, ISO/IEC 38500 draws from the authority of the definition contained in the Cadbury Report (Cadbury et al, 1992), which says that "Corporate Governance is the system by which an organization is directed and controlled". But this definition alone may not convey a great deal of perspective, so we need to draw on additional sources to fully understand the purpose, practices and mechanisms of corporate governance.

Fortunately, there are many additional sources, for Corporate Governance is a very extensively researched discipline.

The United Nations provides, through the OECD (Organization for Economic Cooperation and Development), the International Finance Corporation and the World Bank, an extensive and expanding library of guidance on Corporate Governance, of which a centrepiece is the UN Principles of Corporate Governance. But it is not necessary to wade through this detail to understand the core concepts. A most useful introduction is provided in a paper prepared by the World Bank (Barger, 2004) and delivered to the government of Vietnam. This paper sets out very clearly the relationship between the owners and managers of an organization, and positions the governing body as the group that protects the owners' interests, by providing direction to, and monitoring the activities of management.



This promotional extract may be circulated freely

Figure 4: The role of corporate governance

Barger's paper makes it clear that the governing body and management are jointly responsible for developing the organization's strategy, within broad parameters established by the governing body, having due consideration to the wishes of the owners. The governing body then provides management with overall guidelines within which management should operate, and monitors the performance of the organization and its management, to ensure that the objectives set in the strategy are achieved, and that the organization conforms with all relevant regulatory requirements.

Barger's description of governance, and the model that derives from it, holds true for any type of organization. In the smallest possible business, a single individual is the owner, the governor and the manager. The disciplines and activities are relevant, and should be undertaken to

ensure that the business is performing well and sustainable into the future. They may not be highly visible, but they nonetheless exist and. As organizations grow, the distinction between the ownership, governance and management roles grows as well. For a small organization with employees, the owners tend to remain active as governors and managers. With further growth, additional managers are appointed, but the owners remain closely involved and in control at governance and senior management levels. With further growth, the owners will typically withdraw from management and focus on the governance roles, and then at the upper end of growth, as the organization transitions from private to public ownership, the owners become fully separated from the governing body, which is also separate from the management. Across a variety of different ownership scenarios (such as not-for-profit, and government) organizations, the model remains effective – with the concept of governance remaining unchanged.

While Barger's description provides a good understanding of the role and purpose of governance, it does not explain how governance is actually done. For an explanation of this, we look to one of the definitive works: *"International Corporate Governance"* (Tricker, 1994), which explains that Corporate Governance operates on a broad basis, and engages with management through the Chief Executive Officer.

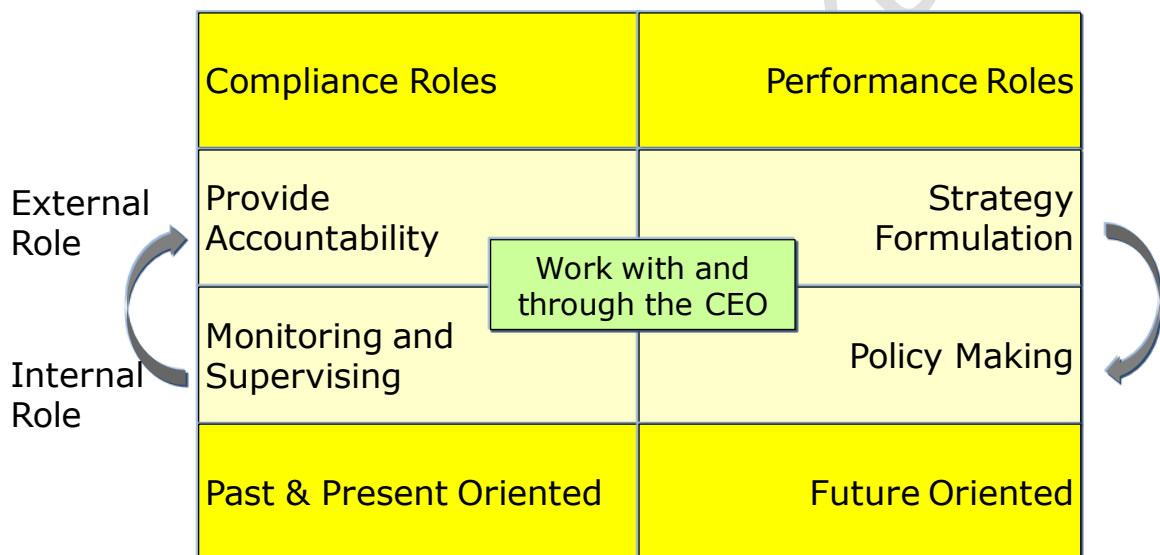


Figure 5: Tricker's model of corporate governance

Tricker's model of Corporate Governance presents several key concepts:

- ❖ Governance addresses current (past and present) and future timeframes;
- ❖ Governance takes into account the external environment as well as the internal situation of the organization;
- ❖ Governance deals with both compliance (meeting regulatory and legislative requirements) and performance (setting and achieving goals).

Working from the top right of the model in Figure 5, Tricker positions the governing body as having a key role in formulating strategy. At this level, strategy includes defining what the business is, and how it will develop. It is worth pointing out that, as development of a business almost always depends on, or creates requirement for information technology, the governing body's direction setting intrinsically sets the direction for IT as well. In larger organizations, strategy formulation typically involves significant management effort – but ownership and accountability for the strategy always remains with the governing body.

Policy is a key instrument through which the governing body provides instruction to management about how they, and through them, the organization will behave, both internally and as part of the overall business environment. Policy includes delegations and definitions of responsibility and authority, as well as rules for operation of the organization overall. The governing body may require management to prepare policy, but again, it is the governing body that makes policy effective, and requires that management conform to the policy as defined.

Strategy and policy, together with external drivers such as legislation and regulation, provide the anchors for the governing body's role in monitoring and supervision. The governing body should receive an appropriate flow of information, and make additional enquiries as necessary, to give it confidence that management is achieving the required performance (as established in the strategy) and conformance (to policy, regulation and legislation). Where performance and conformance are not as required, the governing body's supervision role includes providing additional direction to management.

The outcomes of monitoring and supervision should be that the organization meets the owner's objectives (as set out in strategy) and satisfies the requirements of regulators and legislation. The governing body has ultimate accountability for these outcomes, and takes action as necessary to discharge its accountability.

Tricker's model provides a broad view of the role and operation of the governing body. But for an organization to operate and achieve outcomes requires that it use its assets, and so directing and monitoring an organization effectively involves directing and monitoring how the organization develops and uses its assets. To understand the assets that any organization has, and thus the assets that should be governed, we turn to the work of Weill and Ross (P. Weill & J. Ross, 2004), and Broadbent (Broadbent, 2004). They identified six classes of asset:

- ❖ Human;
- ❖ Financial;
- ❖ Physical;
- ❖ Intellectual Property;
- ❖ Information;
- ❖ Relationships.

Broadbent says that these assets should be enhanced and managed, in a system of governance that involves both the governing body and the management of the organization. Again, it is not the purpose of this book to regurgitate the work of others, or to comprehensively develop thinking around that work. We simply want to draw some important leadership from it.

Information (and by common association, the systems and technology for managing information) is ranked as being an equally important asset for the organization as finance and human resources, both of which are almost universally considered important topics for the governing body, and are thus almost automatically on the agenda for every board meeting.

So, we have context: Governance is fundamentally the role of enhancing and protecting the interests of the organization's owners. It involves establishing strategy, enacting policy, monitoring and supervising management, and providing ultimate accountability. Governance involves enhancing and directing the use of six key asset classes, including Information. Governance operates as a system in which the governing body and management have clear and distinct roles, with the Chief Executive Officer providing the focal point for exchange between the board and management.

3.2.4 The system perspective

To complete our understanding of the "System of Governance", we need now to return to the system perspective. Much of the academic work cited in this chapter has referred more or less directly to the notion of the system, but what does it really mean?

To address this question, we need first to refer again to the discussion in chapter 3.1, where we built a generic model of a business system. Now, replace the word "business" with the word "governance".

Just as the Cadbury definition suggests, it makes sense to consider Governance as a system, in which people have clear roles and authorities, and in which they perform specific tasks, and for which, even at the highest level, technology plays a supporting role. And as we discussed earlier, where business systems can be considered to be collections of lower level, more detailed systems, the governance system should also be considered as an integrated collection of lower level, more detailed systems. For effective governance, which requires clear lines of authority and complete transparency, the governance system is necessarily integrated with the more detailed systems that we usually consider to be the domain of management.

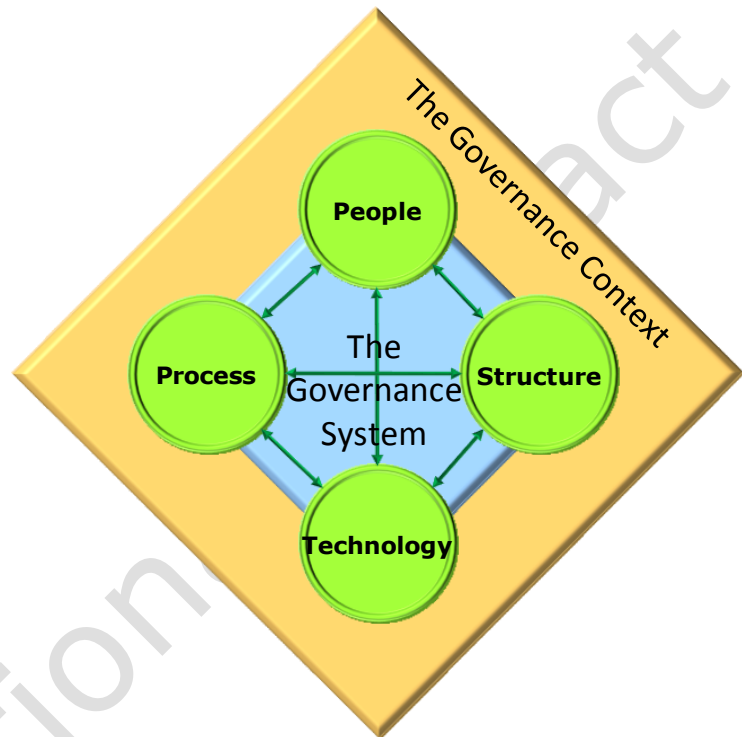


Figure 6: The governance system

A useful way to understand this point is to consider the financial controls that exist in most organizations. At the top level, the governing body is concerned with the use and performance of the organization's financial assets, and thus it pays considerable attention to the financial accounts. It has to ensure that the organization is solvent, and that it is achieving the intended return on both its investments and assets. To prepare the financial accounts, the chief financial officer needs to maintain detailed financial records, and ensure that they are both comprehensive and accurate. To ensure that the organizations financial assets are used appropriately, policies are established defining spending limits and controls. Often, these rules are visible throughout the organization, manifesting in matters like use of petty cash, and approval of expense claims. To ensure financial performance, executives and managers are made accountable for performance in areas like sales, production and purchasing. Clearly, the system for financial governance of an organization is vertically integrated into the management systems of the organization. The point where governance ends and management begins is somewhat indeterminate, considering that directors have the right to request more detailed information about the accounts they are asked to approve, and that the design of the governance system will vary from one organization to the next.

3.2.5 Responsibility for information technology

Since IT is a tool of business which should be driven by, and planned to achieve business outcomes, the question arises: **Who should be responsible for realising the intended business result?**

The answer to this question unequivocally has to be the top executive responsible for the business area in which the result is to be delivered. No other individual will have either the focus of attention or the span of control to ensure that all inhibitors to value are resolved, and that results are both timely and optimal. Thus, the system of governance for IT must necessarily engage the business executive, in both setting the agenda and in assuring the results. Exactly how this engagement is implemented is one of the key issues for the organization in designing its specific system of governance.

In reality, as is the case for virtually every aspect of any organization's operations, it is the role of the top management – the executive – to prepare the detailed plans for the future and to oversee the day to day activities of the organization. Generally, the board should not be required to participate, or intervene in such activities. However, the role of the board is to ensure that the organization is performing as intended, while conforming to all required rules, and this requires ongoing monitoring. In effect, as has been stated by more than one non-executive board chair, the directors should be making sure that the managers are doing their jobs properly.

3.2.6 Board oversight of IT

The board can monitor the organization's use of IT and the performance of management in its stewardship of IT using similar means to those that apply in other aspects of the organization's activity – through regular, well-designed reporting, through direct questioning, and through systems of review (or audit) that should include periodic independent appraisal.

Often, board reporting of IT seems to focus on the technology. This is largely inappropriate. What is generally required is that board reporting of IT focus on the business systems and how they use IT – the operational business performance and capability that is available, and the planned outcomes and benefits of the investments that are under way.

When it comes to directly questioning aspects of IT, it is tempting to address all of the questions to the person most directly responsible for oversight of the IT systems and infrastructure (often known as the Chief Information Officer, or CIO). But this individual typically has no control, and no accountability for the business systems and the results they produce. Like the Chief Financial Officer, the CIO is the custodian of a system of control and the holder of key information, but is not the individual who determines the end result. In most cases, the individuals who most directly control whether or not the use of IT is effective are those who are responsible for the operations of the business – those responsible for marketing, sales, purchasing and production. In the ideal situation, these individuals and the CIO will work closely together to understand intimately how IT fits within the business system, and to optimise the business system through effective integration of its four elements – people, process, structure and technology. In any discussion with the board about effective use of IT, the conversation should be lead by the relevant business executive who would be closely supported by the CIO.

Systems of review, including independent appraisal, should give the board confidence at two levels. As has been the case for some time in many, particularly larger, organizations, periodic audit should check and confirm that the IT systems and infrastructure are in a satisfactory condition to meet the minimum requirements of reliability and integrity. Typical audits at this

level check that detailed management level controls are in place, that procedures are adequately defined, and that the procedures are being followed correctly.

A less common, but now very desirable form of review, is an assessment of the performance of the governance arrangements for IT. An assessment at this level checks not only that the low level controls are in place, but that these controls are being directed, monitored and actioned from the top level as and when necessary. It checks that the system of governance is keeping business leaders – the top managers and the directors – adequately informed of, and giving them the opportunity to control the organization's use of IT.

3.2.7 In summary

governance of information technology involves a system approach to directing and controlling the use of IT by the organization. The system should be specifically designed to suit the characteristics of the organization, ensuring that the directors and top executives are properly engaged in and able to perform their roles effectively. The focus of the system should be on the business use of IT, achieved through understanding of the organization's main business systems, and through this focus, the top executives should be jointly accountable, with the CIO, for the effective, efficient and acceptable use of IT.

Because the system of governance for IT is focused on business systems and outcomes, with appropriate summarisation in a properly designed regime of regular reporting, it should be feasible for board directors to monitor and assess the use of IT without requiring any specialised knowledge of technology. Through appropriate systems of review, the directors should obtain confidence that not only is the information technology itself secure and operating correctly, but also that the system of governance is operating correctly to set appropriate direction and to make essential decisions as and when necessary, with proper and effective engagement of the right people, at the right levels of the organization, in making those decisions.

Promotional Extract

This promotional extract may be circulated freely

Bibliography

AAP. 2003. Failure of computer system results in HK-bound passenger coming to Melbourne. *The Age*. Melbourne : s.n., 9 July 2003.

Auditor General Victoria. Feb 2003. *Report on Public Sector Agencies*. Melbourne : Victorian Government, Feb 2003. p. 61.

Auditor General, Victoria. 2008. Investing Smarter in Public Sector ICT - Launch speech. Melbourne, Victoria, Australia : s.n., 28 August 2008.

Australian National Audit Office. 2006. *ANAO Audit Report No.24 2006-07*. Canberra : Australian National Audit Office, 2006.

Australian Pharmaceutical Industries Limited. 2006. *Annual Report*. Melbourne : Australian Pharmaceutical Industries, 2006.

Australian Prudential Regulatory Authority. 2004. *REPORT INTO IRREGULAR CURRENCY OPTIONS TRADING AT THE NATIONAL AUSTRALIA BANK*. Melbourne : Australian Prudential Regulatory Authority, 2004.

Barger, Teresa. 2004. Corporate Governance – A Working Definition. *International Corporate Governance Meeting*. Hanoi : IFC/World Bank Corporate Governance Department, 2004.

Bellis, Mary. History of the Digital Camera. *About.com*. [Online] [Cited: 17 March 2009.] <http://inventors.about.com/library/inventors/bldigitalcamera.htm>.

Booz Allen Hamilton. 2006. *Review of the Integrated Cargo System*. 2006.

Broadbent, M. 2004. IT Governance: Who cares and does it matter? . *Australian Institute of Company Directors Annual Conference*. May 2004.

BusinessDictionary.com. management. *BusinessDictionary.com*. [Online] [Cited: 17 March 2009.] <http://www.businessdictionary.com/definition/management.html>.

Cadbury et al. 1992. *Report of the Committee on the Financial Aspects of Corporate Governance*. London : s.n., 1992.

Cater-Steel and Tan. 2005. *A survey of ITIL adoption and benefits*. Brisbane : University of South Queensland, 2005.

Construction Management Association of America. 2008. Application Definitions | CMAA. *Construction Management Association of America*. [Online] 2008. [Cited: 15 July 2009.] http://cmaanet.org/cmci/application_definitions.php.

Daley, James. 2008. Centrica launches £182m lawsuit against Accenture. *The Independent*. 12 May 2008.

Eastman Kodak Co. 2004. Kodak job losses and restructuring. *Digital Photography Review*. [Online] 6 October 2004. [Cited: 16 July 2008.] http://www.dpreview.com/news/0410/04100501kodak_joblosses.asp.

Gershon, Sir Peter. 2008. *Review of the Australian Government's Use of Information and Communication Technology*. Canberra : Australian Government Information Management Office, Department of Finance and Deregulation, 2008.

- House of Commons Transport Committee. 2008.** *The opening of Heathrow Terminal 5*. London : The Stationery Office Limited, 2008.
- IFEAD. 2009.** Institute For Enterprise Architecture Developments. [Online] 10 6 2009. [Cited: 16 6 2009.] <http://www.enterprise-architecture.info/>.
- ISACA. COBIT Mandated for Turkish Banks.** *www.isaca.org*. [Online] [Cited: 17 03 2009.] <http://www.isaca.org/Template.cfm?Section=Home&CONTENTID=38004&TEMPLATE=/ContentManagement/ContentDisplay.cfm>.
- ISO. 2008.** Press release: ISO/IEC standard for corporate governance of information technology. Geneva : s.n., 5 June 2008.
- ISO/IEC. 2008.** *ISO/IEC 38500:2008 Corporate Governance of Information Technology*. Geneva : ISO, 2008. p. v.
- Judge E, & Charles J. 2009.** HSBC fined \$6m in Britain for data loss. *The Australian*. 23 July 2009.
- Kim, Milne, Phelps and Castner. 2006.** *IT Controls Performance Study*. s.l. : Information Technology Process Institute, 2006.
- KPMG. 2005.** *Global IT Project Management Survey: How committed are you?* s.l. : KPMG, 2005.
- Leavitt, H. J. 1964.** Applied organizational change in industry: structural, technical and human approaches. [book auth.] J.G. March. *Handbook of organisations*. Chicago : Rand McNally, 1964, pp. 1144-1170.
- Luciw, Roma. 2004.** RBC extends bank hours. *Globe and Mail*. Toronto : s.n., 4 June 2004.
- McCrimmon, Mitch. 2007.** Organizational Culture and Climate: The Personality and Mood of Organizations. *Suite101.com*. [Online] 5 December 2007. [Cited: 26 July 2009.] http://businessmanagement.suite101.com/article.cfm/organizational_culture_and_climate.
- McMurray, Adela J. 1994.** *The Relationship between Organisational Culture and Organisational Climate with Reference to a University Setting*. Sydney : s.n., 1994.
- Mooney, Jed. 2007.** BSKyB versus EDS – the CRM battlefield. *DM Weekly*. [Online] 23 November 2007. [Cited: 17 March 2009.] <http://dmweekly.mad.co.uk>.
- P. Weill & J. Ross. 2004.** *Don't Just Lead, Govern!: Empowering Effective Enterprise Use of Information Technology*. s.l. : Harvard Business School Press, 2004.
- SearchCIO.com. 2009.** Whatis.com. *Technology management strategies for the enterprise CIO*. [Online] June 2009. [Cited: 12 June 2009.] <http://searchcio.techtarget.com/>.
- Shed, Mark. 2007.** Definition of Management. *Leadership 501*. [Online] 30 January 2007. [Cited: 19 March 2009.] <http://www.leadership501.com/definition-of-management/21/>.
- Songini, Marc. 2004.** Media giant BSKyB sues EDS over troubled CRM system. *Computerworld*. 17 August 2004.
- The Fred Hollows Foundation. 2009.** About Us. *The Fred Hollows Foundation*. [Online] 2009. [Cited: 2 July 2009.] http://www.hollows.org.au/About_Us/.
- Thorp, J. 2005.** *Rethinking IT Governance - Beyond Alignment to Integration*. s.l. : The Thorp Network, 2005.

Tieman, Ross. 28 May 2008. Sweeping away a sector's chaos. *Finnacial Times*. 28 May 2008, p. Special Report.

TOGAF. TOGAF Version 9. *The Open Group*. [Online] [Cited: 16 06 2009.] <http://www.opengroup.org/togaf/>.

Tricker, R. 1994. *International Corporate Governance*. 1994.

Various. 2008. Discussion topic: IT Governance or IT Good Governance? . *The IT Governance Group*. [Online] 2008. [Cited: 17 03 2009.] <http://itgovernance.collectivex.com/discussion/topic/show/57830>.

Weill, P and Ross, J. 2004. *IT Governance: How top performers manage IT Decision Rights for Superior Results*. s.l. : Harvard Business School Press, 2004.

Williams, Merran. 2003. The 156-tonne Gimli Glider. *Flight Safety Australia*. July-August, 2003.

Young, R and Jordan, E. 2008. Top management support: Mantra or necessity? 2008.

Young, Raymond C. 2006. What is the ROI for IT Project Governance? Establishing a benchmark. 2006.

Zhao, F, McMurray, AJ and Toomey, M. 2008. Effectiveness of Information Technology Governance: Perceptions of Board Directors and Senior Managers. [ed.] Fang Zhao. *Information Technology Entrepreneurship and Innovation*. Hershey. New York : s.n., 2008.

Promotional Extract

This promotional extract may be circulated freely

To Buy This Book

Waltzing with the Elephant: A comprehensive guide to directing and controlling information technology is available through the Infonomics Shop, at <http://infonomics.lookat.me.com.au/>.

Electronic download is priced at AUD\$60 per copy, plus applicable taxes for Australian residents.

Hard copy is priced at AUD\$100, plus shipping charges and applicable taxes for Australian residents.

Additional distribution channels can be found at the Infonomics web site at www.infonomics.com.au.

Promotional Extract

About the Author

Mark Toomey is an international leader in the vitally important field of known as governance of information technology.

He was deeply involved in development of Australian Standard AS 8015:2005 – Corporate Governance of Information and Communication Technology, and was subsequently appointed as Project Editor for ISO/IEC 38500:2008 – Corporate Governance of Information Technology.

Toomey continues his efforts to build worldwide understanding of the roles and disciplines required for effective governance and successful use of information technology as a founding member of the international standards working group on governance of information technology established under the auspices of ISO and the IEC.

Through his company, Infonomics Pty. Ltd., Toomey provides services to inform, assess and improve the way that individuals and organisations go about the task of directing and controlling the use of information technology. His portfolio of plain language literature, of which *Waltzing with the Elephant* has become the centrepiece, is complemented by an expanding array of education services delivered worldwide.

Mark Toomey completed his education at Marcellin College in Melbourne, and studied economics and information technology (computer science as it was then known) at La Trobe University in Melbourne. His working career began in 1977 as a trainee programmer with Management Information Systems, a pioneering company that brought information technology to medium sized companies using the then revolutionary Digital Equipment Corporation PDP-11 range. In 1985, Toomey joined the Melbourne office of DMR Group (now Fujitsu Consulting), which provided strategic advice and services to major organisations. After 11 years, he accepted the role of Chief Architect at the National Australia Bank, and late in 1997 was asked to manage one of the critical “Year-2000” projects at a major public corporation.

Having experienced first hand how the diverse and often colourful behaviour of people in leadership roles could contribute to, and more often detract from the success of information technology, Toomey moved into providing specialist board advisory services around information technology issues in 2000, and continues this work in parallel with his broader mission of improving understanding and practice in governance of information technology at all levels.

He is a Fellow of the Australian Institute of Company Directors and a Senior Member of the Australian Computer Society.

Mark lives on the edge of the Dandenong Ranges in Melbourne, Australia. He has two adult children and in his increasingly rare spare time maintains an interest in classic Jaguar cars, fine Australian wines and sustainable living.



www.infonomics.com.au



ISBN 978-0-9806830-0-4

