



# IT Governance

## Developing a successful governance strategy

A Best Practice guide for decision makers in IT



---

# IT Governance

## Developing a successful governance strategy

A Best Practice guide for decision makers in IT

The effective use of information technology is now an accepted organisational imperative - for all businesses, across all sectors - and the primary motivation; improved communications and commercial effectiveness. The swift pace of change in these technologies has consigned many established best practice approaches to the past. Today's IT decision makers and business managers face uncertainty - characterised by a lack of relevant, practical, advice and standards to guide them through this new business revolution.

Recognising the lack of available best practice guidance, the National Computing Centre has created the Best Practice Series to capture and define best practice across the key aspects of successful business.

### Other Titles in the NCC Best Practice series:

|   |                           |
|---|---------------------------|
| <b>IT Skills</b> - Recruitment and Retention                              | <b>ISBN 0-85012-867-6</b> |
| <b>The New UK Data Protection Law</b>                                     | <b>ISBN 0-85012-868-4</b> |
| <b>Open Source</b> - the UK opportunity                                   | <b>ISBN 0-85012-874-9</b> |
| <b>Intellectual Property Rights</b> - protecting your intellectual assets | <b>ISBN 0-85012-872-2</b> |
| <b>Aligning IT with Business Strategy</b>                                 | <b>ISBN 0-85012-889-7</b> |
| <b>Enterprise Architecture</b> - understanding the bigger picture         | <b>ISBN 0-85012-884-6</b> |
| <b>IT Governance</b> - developing a successful governance strategy        | <b>ISBN 0-85012-897-8</b> |
| <b>Security Management</b> - implementing ISO 27000                       | <b>ISBN 0-85012-885-4</b> |

All titles are available from NCC see the website for further details [www.ncc.co.uk](http://www.ncc.co.uk)

The National Computing Centre - generating best practice

---

# ***IT Governance***

## Developing a Successful Governance Strategy

A Best Practice Guide for Decision Makers in IT

# Foreword

For organisational investment in IT to deliver full value, it is recognised that IT has to be fully aligned to business strategies and direction, key risks have to be identified and controlled, and legislative and regulatory compliance demonstrated. IT Governance covers this and more, and in light of recent corporate failures, scandals and failure, enjoys a higher profile today than ever before.

Back in 2003, IMPACT launched an IT Governance Specialist Development Group (SDG) to identify the issues that need to be addressed and to share and further develop the practical approaches to IT governance used in their organisations.

Over the past two years, heads of IT governance from Abbey, Aon, Avis, Barclays, BOC, DfES, Eli Lilly, Learning & Skills Council, Legal & General, NOMS, Royal Mail and TUI Group have examined what they identified as the key topics and, with the guidance of IT governance expert Gary Hardy, have defined the good practices captured in this guide.

For further information on the IMPACT Programme, its Professional Development Programme and the IT Governance and CobiT Specialist Development Group, please contact Elisabetta Bucciarelli on 0207 842 7900 or email [elisabetta.bucciarelli@impact-sharing.com](mailto:elisabetta.bucciarelli@impact-sharing.com). The IMPACT Programme is a division of the National Computing Centre.

## IMPACT

The IMPACT Programme  
International Press Centre  
76 Shoe Lane  
London EC4A 3JB

### **IT Governance**

Developing a successful governance strategy  
A Best Practice Guide for decision makers in IT

### **Published by**

The National Computing Centre  
Oxford House  
Oxford Road  
Manchester  
M1 7ED

**Website:** [www.ncc.co.uk](http://www.ncc.co.uk)

**Tel:** 0161 242 2121

**Fax:** 0161 242 2499

First published November 2005

Copyright © National Computing Centre 2005

**ISBN:** 0-85012-877-8

British Cataloguing in Publication  
A CIP catalogue record for this book is available from the British Library

Printed and bound in the UK

All rights reserved: no part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording or otherwise without either the prior written permission of the authors and Publisher or as permitted by the Copyright, Designs and Patents Act 1988. Enquiries for such permissions should be made to the Publisher.

### **Disclaimer**

Every care has been taken by the authors, and by the National Computing Centre, and associated working groups, in the preparation of this publication, but no liability whatsoever can be accepted by the authors or by National Computing Centre, or associated NCC working groups, for actions taken based on information contained in this document.

All trademarks acknowledged.

# Contents

|          |   |           |           |  |           |
|----------|---|-----------|-----------|--|-----------|
| <b>1</b> | <b>IT Governance – The Business Case</b>                                | <b>4</b>  | <b>7</b>  | <b>Supplier Governance</b>                             | <b>37</b> |
| 1.1      | Why is IT Governance important?   | 5         | 7.1       | Why is supplier governance important?                  | 37        |
| 1.2      | What does IT Governance cover?  | 6         | 7.2       | The customer's role                                    | 38        |
| 1.3      | What are the benefits?  | 6         | 7.3       | How best to select a supplier                          | 40        |
| 1.4      | What is IT Governance best practice?                                    | 7         | 7.4       | The customer/supplier relationship                     | 40        |
| <b>2</b> | <b>Performance Measurement</b>  | <b>9</b>  | 7.5       | Service management techniques and SLAS                 | 41        |
| 2.1      | Why is performance measurement important?                               | 9         | 7.6       | The supplier/outsourcing governance lifecycle          | 42        |
| 2.2      | What does performance measurement cover?                                | 10        | <b>8</b>  | <b>IT &amp; Audit Working Together and Using CobiT</b> | <b>43</b> |
| 2.3      | Who are the stakeholders and what are their requirements?               | 11        | 8.1       | Introduction to CobiT                                  | 43        |
| 2.4      | What should we measure?   | 12        | 8.2       | How is CobiT being used?                               | 44        |
| 2.5      | What is best practice?  | 12        | 8.3       | What are the roles of IT and audit for IT Governance?  | 45        |
| <b>3</b> | <b>Implementation Roadmap</b>   | <b>14</b> | 8.4       | How can IT and internal audit work better together?    | 45        |
| 3.1      | Goals and success criteria  | 14        | <b>9</b>  | <b>Information Security Governance</b>                 | <b>48</b> |
| 3.2      | How to get started  | 15        | 9.1       | Background   | 48        |
| 3.3      | Who needs to be involved and what are their roles and responsibilities? | 16        | 9.2       | What is information security?                          | 49        |
| <b>4</b> | <b>Communication Strategy &amp; Culture</b>                             | <b>18</b> | 9.3       | Where to focus   | 50        |
| 4.1      | Who do we need to influence?  | 18        | 9.4       | Roles and responsibilities                             | 50        |
| 4.2      | What are the key messages?  | 19        | 9.5       | Action planning and best practice                      | 52        |
| 4.3      | Communication best practices  | 20        | <b>10</b> | <b>Legal &amp; Regulatory Aspects of IT Governance</b> | <b>53</b> |
| 4.4      | Developing an influencing strategy                                      | 20        | 10.1      | Legal and regulatory factors affecting IT Governance   | 53        |
| 4.5      | Change roadmap  | 22        | 10.2      | Roles and responsibilities                             | 54        |
| <b>5</b> | <b>Capability Maturity &amp; Assessment</b>                             | <b>23</b> | 10.3      | Best approach to compliance                            | 55        |
| 5.1      | Why IT capability is important  | 23        | 10.4      | What IT has to do                                      | 56        |
| 5.2      | How to measure IT capability  | 24        | 10.5      | Dealing with third parties                             | 58        |
| 5.3      | Setting maturity targets and considering improvements                   | 25        | 10.6      | Critical success factors                               | 59        |
| 5.4      | Roadmap for sustaining the approach                                     | 25        | <b>11</b> | <b>Architecture Governance</b>                         | <b>60</b> |
| 5.5      | Self assessment tool  | 26        | 11.1      | Why is architecture governance important?              | 60        |
| <b>6</b> | <b>Risk Management</b>  | <b>28</b> | 11.2      | What are the objectives of architecture governance?    | 61        |
| 6.1      | What are the risks?   | 28        | <b>12</b> | <b>Managing the IT Investment</b>                      | <b>63</b> |
| 6.2      | What is the best approach for risk analysis and management?             | 29        | 12.1      | Why is managing the IT investment important?           | 63        |
| 6.3      | Using standards and best practices – is certification useful?           | 30        | 12.2      | Portfolio management                                   | 64        |
| 6.4      | What are the roles of management, staff and auditors?                   | 31        | 12.3      | Benefits management                                    | 65        |
| 6.5      | Who needs to be competent?  | 31        | 12.4      | Measuring investment performance                       | 65        |
| 6.6      | What competence is required?  | 32        | 12.5      | Improve value delivery and ROI                         | 66        |
| 6.7      | How to obtain, develop, retain and verify competence                    | 33        | 12.6      | Measuring and controlling IT operational costs         | 66        |
| 6.8      | When to source competence from outside                                  | 35        | 12.7      | Project risk management                                | 66        |
| 6.9      | Key learning points   | 35        | <b>13</b> | <b>Success Factors</b>                                 | <b>67</b> |

# 1 IT Governance – The Business Case

---

|  |   |
|--|---|
| 1.1 Why is IT Governance important? .....      | 5 |
| 1.2 What does IT Governance cover? .....       | 6 |
| 1.3 What are the benefits? .....               | 6 |
| 1.4 What is IT Governance best practice? ..... | 7 |

---

▼ The guide focuses on 12 key topics selected by the group because of their importance to effective IT governance:

- ▶ *The business case – The organisation needs to understand the value proposition*
- ▶ *Performance measurement – Is the ship “on course”?*
- ▶ *Implementation roadmap – How to start – What path to follow*
- ▶ *Communications – How to explain the objectives and change the culture*
- ▶ *Capability assessment – Finding out the true current state of IT governance*
- ▶ *Risk management – What risks exist and how to make sure they are dealt with*
- ▶ *Supplier governance – External parties play a big role and must be included*
- ▶ *IT and audit working together – How to co-operate for a common goal*
- ▶ *Information security – A key topic in today’s networked environment*
- ▶ *Legal and regulatory aspects – Compliance is a global concern*
- ▶ *Architectures – The foundation for effective technical solutions*
- ▶ *Managing investments – Ensuring value is delivered and benefits realised*

Implementation of this guidance, or indeed any IT best practice, should be consistent with your organisation’s management style and the way your organisation deals with risk management and delivery of IT value. Please share these ideas with your business users, external service providers, and auditors, since to realise their full value, all stakeholders of IT services should be involved.

All analysts currently agree that probably the biggest risk and concern to top management today is failing to align IT to real business needs, and a failure to deliver, or be seen to be delivering, value to the business. Since IT can have such a dramatic effect on business performance and competitiveness, a failure to manage IT effectively can have a very serious impact on the business as a whole.

Corporate Governance generally has taken on even greater significance. It is being recognised that IT has a pivotal role to play in improving corporate governance practices, because critical business processes are usually automated and directors rely on information provided by IT systems for their decision making. With the growth of direct connection between organisations and their suppliers and customers, and more and more focus on how IT can be used to add value to business strategy, the need to effectively manage IT resources and avoid IT failures and poor performance has never been greater.

The current climate of cost reduction and budget restriction has resulted in new norm – there is an expectation that IT resources should always be used as efficiently as possible and that steps are taken to organise these IT resources ready for the next cycle of growth and new IT developments. A key aspect of these factors is the increasing use of third party service providers and the need to manage these suppliers properly to avoid costly and damaging service failures.

▼ This briefing provides a high level set of business arguments for IT Governance. It also explains how an IT Governance initiative can enable business and IT executives to:

- ▶ *Be sure that they are aware of all IT related risks likely to have an impact on their organisation;*
- ▶ *Know how to improve the management processes within IT to manage these risks;*
- ▶ *Ensure there are manageable relationships with suppliers, service providers and with the business (customers);*
- ▶ *Ensure there is a transparent and understandable communication of these IT activities and management processes to satisfy the Board and other interested stakeholders.*

IT Governance covers the culture, organisation, policies and practices that provide this kind of oversight and transparency of IT – IT Governance is part of a wider Corporate Governance activity but with its own specific focus. The benefits of good IT risk management, oversight and clear communication not only reduce the cost and damage caused by IT failures – but also engenders greater trust, teamwork and confidence in the use of IT itself and the people trusted with IT services.

## 1.1 Why is IT Governance important?

▼ IT Governance has become very topical for a number of reasons:

- ▶ *In the wake of Enron and other corporate scandals, “Governance” generally has taken on even greater significance. IT has a pivotal role to play in improving corporate governance practices.*
- ▶ *Management’s awareness of IT related risks has increased.*
- ▶ *There is a focus on IT costs in all organisations.*
- ▶ *There is a growing realisation that more management commitment is needed to improve the management and control of IT activities.*

▼ IMPACT’s IT Governance Special Interest Group (SIG) has examined these trends and found that the following issues drive the need for IT Governance:

- ▶ *There is a general lack of accountability and not enough shared ownership and clarity of responsibilities for IT services and projects. The communication between customers (IT users) and providers has to improve and be based on joint accountability for IT initiatives.*
- ▶ *There is a potentially widening gap between what IT departments think the business requires and what the business thinks the IT department is able to deliver.*
- ▶ *Organisations need to obtain a better understanding of the value delivered by IT, both internally and from external suppliers. Measures are required in business (the customer’s) terms to achieve this end.*
- ▶ *Top management wants to understand “how is my organisation doing with IT in comparison with other peer groups?”*
- ▶ *Management needs to understand whether the infrastructure underpinning today’s and tomorrow’s IT (technology, people, processes) is capable of supporting expected business needs.*
- ▶ *Because organisations are relying more and more on IT, management needs to be more aware of critical IT risks and whether they are being managed. Furthermore, if there is a lack of clarity and transparency when taking significant IT decisions, this can lead to reluctance to take risks and a failure to seize technology opportunities.*
- ▶ *And finally, there is a realisation that because IT is complex and has its own fast changing and unique conditions, the need to apply sound management disciplines and controls is even greater.*

▼ Stakeholders include:

- ▶ *Top level business leaders such as the Board, Executive, non-Execs, and especially heads of Finance, Operations and IT.*
- ▶ *Those that have a responsibility for investor and public relations.*
- ▶ *Internal and external auditors and regulators.*
- ▶ *Middle level business and IT management.*
- ▶ *Key business partners and suppliers.*
- ▶ *Shareholders.*
- ▶ *Customers.*

▼ Concerns they typically have include:

- ▶ *Availability, security and continuity of IT services.*
- ▶ *Costs and measurable returns on investments.*
- ▶ *Quality and reliability of service – no embarrassments.*
- ▶ *IT not appearing to respond to the real needs of the business.*
- ▶ *Identification and management of IT related risks to the business.*

- ▶ *Capability and skills of human resources.*
- ▶ *Compliance to legal, regulatory and contractual requirements.*
- ▶ *Responsiveness and nimbleness to changing conditions.*

## 1.2 What does IT Governance cover?

IT Governance is a relatively new concept as a defined discipline and is still evolving.

IT Governance is not just an IT issue or only of interest to the IT function. In its broadest sense it is a part of the overall governance of an entity, but with a specific focus on improving the management and control of Information Technology for the benefit of the primary stakeholders. Ultimately it is the responsibility of the Board of Directors to ensure that IT along with other critical activities is adequately governed. Although the principles are not new, actual implementation requires new thinking because of the special nature of IT.

▼ IT Governance spans the culture, organisation, policy and practices that provide for IT management and control across five key areas<sup>1</sup>:

- ▶ **Alignment** – *Provide for strategic direction of IT and the alignment of IT and the business with respect to services and projects.*
- ▶ **Value Delivery** – *Confirm that the IT/Business organisation is designed to drive maximum business value from IT. Oversee the delivery of value by IT to the business, and assess ROI.*
- ▶ **Risk Management** – *Ascertain that processes are in place to ensure that risks have been adequately managed. Include assessment of the risk aspects of IT investments.*
- ▶ **Resource Management** – *Provide high-level direction for sourcing and use of IT resources. Oversee the aggregate funding of IT at enterprise level. Ensure there is an adequate IT capability and infrastructure to support current and expected future business requirements.*
- ▶ **Performance Measurement** – *Verify strategic compliance, i.e. achievement of strategic IT objectives. Review the measurement of IT performance and the contribution of IT to the business (i.e. delivery of promised business value).*

IT Governance is not a one-time exercise or something achieved by a mandate or setting of rules. It requires a commitment from the top of the organisation to instil a better way of dealing with the management and control of IT. IT Governance is an ongoing activity that requires a continuous improvement mentality and responsiveness to the fast changing IT environment. IT Governance can be integrated within a wider Enterprise Governance approach, and support the increasing legal and regulatory requirements of Corporate Governance.

## 1.3 What are the benefits?

Investments are likely to be needed to improve and develop the IT Governance areas that need attention. It is important therefore, to begin with as good a definition as possible of the potential benefits from such an initiative to help build a viable business case. The expected benefits can then become the project success criteria and be subsequently monitored.

The IMPACT IT Governance SIG has identified the following main areas of benefit likely to arise from good IT Governance:

▼ Transparency and Accountability

- ▶ *Improved transparency of IT costs, IT process, IT portfolio (projects and services).*
- ▶ *Clarified decision-making accountabilities and definition of user and provider relationships.*

▼ Return on Investment/Stakeholder Value

- ▶ *Improved understanding of overall IT costs and their input to ROI cases.*
- ▶ *Combining focused cost-cutting with an ability to reason for investment.*
- ▶ *Stakeholders allowed to see IT risk/returns.*
- ▶ *Improved contribution to stakeholder returns.*



- ▶ *Enhancement and protection of reputation and image.*

#### ▼ Opportunities and Partnerships

- ▶ *Provide route to realise opportunities that might not receive attention or sponsorship.*
- ▶ *Positioning of IT as a business partner (and clarifying what sort of business partner IT is).*
- ▶ *Facilitate joint ventures with other companies.*
- ▶ *Facilitate more businesslike relationships with key IT partners (vendors and suppliers).*
- ▶ *Achieve a consistent approach to taking risks.*
- ▶ *Enables IT participation in business strategy (which is then reflected in IT strategy) and vice versa.*
- ▶ *Improve responsiveness to market challenges and opportunities.*

#### ▼ Performance Improvement

- ▶ *Achieve clear identification of whether an IT service or project supports “business as usual” or is intended to provide future added value.*
- ▶ *Increased transparency will raise the bar for performance, and advertise that the bar should be continuously raised.*
- ▶ *A focus on performance improvement will lead to attainment of best practices.*
- ▶ *Avoid unnecessary expenditures – expenditures are demonstrably matched to business goals.*
- ▶ *Increase ability to benchmark.*

#### ▼ External Compliance

- ▶ *Enables an integrated approach to meeting external legal and regulatory requirements.*

## ▶▶ 1.4 What is IT Governance best practice?

Experiences gained by IMPACT SIG members have identified a number of practical organisational and process issues that need to be addressed when implementing IT Governance. This has enabled the Group to recommend the following best practices (critical success factors) when planning IT Governance initiatives:

#### ▼ An enterprise wide approach should be adopted

- ▶ *The business and IT must work together to define and control requirements.*
- ▶ *IT will need to develop a control model applicable to all business units/divisions.*
- ▶ *A committee approach is recommended for setting, agreeing, and monitoring direction/policy etc.*
- ▶ *A shared, cohesive view of IT Governance is needed across the enterprise based on a common language.*
- ▶ *There should be a clear understanding (and approval) by stakeholders of what is within the scope of IT Governance.*

#### ▼ Top level commitment backed up by clear accountability is a necessity

- ▶ *IT Governance needs a mandate and direction from Board/Executive level management if it is to succeed in practice.*
- ▶ *Make sure management responsibilities and accountabilities in the business as well as IT have been defined.*

#### ▼ An agreed IT Governance and control framework is required

- ▶ *Although it may generate challenges and pushback, and will require a consensus, an agreed framework for defining IT processes and the controls required to manage them must be defined for IT Governance to function effectively.*
  - ▶ *The processes for IT Governance need to be integrated with other enterprise wide governance practices so that IT Governance does not become just an IT owned process.*
  - ▶ *The framework needs to be supported by an effective communication and awareness campaign so that objectives are understood and the practices are complied with.*
  - ▶ *Incentives should be considered to motivate adherence to the framework.*
  - ▶ *Pay attention to devolved decentralised IT organisations to ensure a good balance between centrally driven policy and locally implemented practices.*
  - ▶ *Avoid too much bureaucracy.*
- ▼ Trust needs to be gained for the IT function (in house and/or external)
- ▶ *For IT Governance to work the suppliers of IT services and know-how need to be seen as professional, expert and aligned to customer requirements. Trust has to be developed by whatever means including awareness programmes, joint workshops, and the IT Director acting as a bridge between the business and IT.*
- ▼ Measurement systems will ensure objectives are owned and monitored
- ▶ *Creation of an IT scorecard will underpin and reinforce achievement of IT Governance objectives.*
  - ▶ *Creation of an initial set of measures can be a very good way to raise awareness and initiate an IT Governance programme.*
  - ▶ *The measures used must be in business terms and be approved by stakeholders.*
- ▼ Focus on costs
- ▶ *It is likely that there will be opportunities to make financial savings as a consequence of implementing improved IT Governance. These will help to gain support for improvement initiatives.*

# 2 Performance Measurement

|  |    |
|--|----|
| <b>2.1</b> Why is performance measurement important? .....                 | 9  |
| <b>2.2</b> What does performance measurement cover? .....                  | 10 |
| <b>2.3</b> Who are the stakeholders and what are their requirements? ..... | 11 |
| <b>2.4</b> What should we measure? .....                                   | 12 |
| <b>2.5</b> What's best practice? .....                                     | 12 |

One of the greatest challenges faced by those trying to manage IT in today's fast moving economy and complex technical environment is knowing whether the "ship is on course" and being able to predict and anticipate failures before it is too late. Like driving a car or steering a ship, good instruments are essential. The use of measures to help steer the IT function has for many years been a challenge that few appear to have successfully addressed, which is why the expression "it's like driving a car with a blacked out windscreen and no instruments" is often used. If it is difficult for those literate in technology and relatively close to the IT function, then it is even worse for the end customer who finds technical jargon a smokescreen and lack of information relevant to his business a major headache.

There is no doubt that a practical and effective way to measure IT performance is an essential part of any IT Governance programme, just as transparency and reliability of financial results is a Corporate Governance necessity. Performance management is important because it verifies the achievement of strategic IT objectives and provides for a review of IT performance and the contribution of IT to the business (i.e. delivery of promised business value). It is also important in providing a transparent assessment of IT's capability and an early warning system for risks and pitfalls that might otherwise have been missed. Performance measurement provides transparency of IT related costs, which increasingly account for a very significant proportion of most organisations' operating expenses.

Stakeholders play a key part in IT Governance, since at the heart of the governance responsibilities of setting strategy, managing risks, allocating resources, delivering value and measuring performance, are the stakeholder values, which drive the enterprise and IT strategy.

For performance measurement to be successful, it is important to understand who the stakeholders are and what their specific requirements and drivers are so that the performance measurements will be meaningful to them. An IT Governance best practice is the approval of measures by stakeholders. A performance measurement system is only effective if it serves to communicate to all who need to know what is important and then motivates positive action and alignment to common objectives. The measures are not an end in themselves but a means to take corrective action and to learn from real experiences. Concise and understandable communication and clear accountabilities are therefore critical success factors if measures are to be turned into effective actions.

"If you can't measure it, you can't manage it"

## 2.1 Why is performance measurement important?

*"Teams that don't keep score are only practising."*  
Tom Malone, President Milliken & Company

Performance measurement is a key component of IT Governance. It verifies the achievement of strategic IT objectives and provides for a review of IT performance and the contribution of IT to the business (i.e. delivery of promised business value).

▼ Performance measurement supports the other key elements<sup>2</sup> of IT Governance by:

- ▶ *Alignment – monitoring the strategic direction of IT and the alignment of IT and the business.*
- ▶ *Value Delivery – assessing whether the IT/Business organisation is providing business value from IT and assessing ROI.*
- ▶ *Risk Management – monitoring whether risks are being identified and managed and measuring the cost and benefit of risk management investments.*

- ▶ *Resource Management – measuring the effectiveness of sourcing and use of IT resources, the aggregate funding of IT at enterprise level, and measuring IT capability and infrastructure compared to current and expected future business requirements.*

Performance measures are required to ensure that the outcomes of IT activities are aligned to the customer's goals. Internal IT process measures are required to ensure that the processes are capable of delivering the intended outcomes cost-effectively. Advanced performance measurement enables the measurement of key aspects of IT capability such as creativity and agility (new ideas, speed of delivery and success of a change programme), development of new solutions, ability to operate reliable and secure services in an increasingly demanding IT technical environment, and the development of human resources and skills.

Performance measurement may also be a vital tool when assessing mergers and acquisitions to allow earlier insight into IT strengths and gaps. The introduction of a performance measurement system focused on a few key measures can be an excellent way to kick-start an IT Governance initiative, providing, perhaps for the first time, transparency of critical activities and a way to bridge the communication gap between IT and its customers.

## 2.2 What does performance measurement cover?

Performance measures are the “vital signs” of an organisation. They quantify how well the activities within a process or the outputs of a process achieve a specific goal. The measures tell people what and how they're doing as part of the whole. They communicate what's important throughout the organisation: strategy from top management down, process results from the lower levels up, and control and improvement within the process. Only with a consistent view of the “vital signs” can everyone work toward implementing the strategy, achieving the goals, and improving the organisation (Vital Signs, by Steven M. Hronec).

▼ An IT performance measurement system should help to:

- ▶ *Focus on the customer to increase customer satisfaction*
- ▶ *Improve processes so problems are anticipated and prevented*
- ▶ *Understand and reduce costs*
- ▶ *Encourage and facilitate change by obtaining facts about current state, desired state and the gap that needs to be met*
- ▶ *Set realistic benchmarks for comparison*

▼ Effective performance measurement of IT will enable management and other stakeholders to know whether or not IT is meeting its objectives. It provides a transparent and objective communication mechanism, as long as the measures are understandable by both the customers and the service providers. The measures should address two aspects (The IT Governance Institute's CobiT Management Guidelines provides example metrics for all IT processes and explains the difference between Goal Indicators (KGIs) and Process Indicators (KPIs)):

- ▶ *Outcome focused – is IT meeting the objectives set by the customer?*
- ▶ *Process focused – are the IT processes operating effectively and likely to lead to the customer objectives being met?*

▼ The IT Governance SIG recommends that performance measures meet the following requirements to be successful:

- ▶ *Defined using a common language appropriate and understandable for the audience*
- ▶ *Approved by the stakeholders*
- ▶ *In keeping with the culture and style of the organisation*
- ▶ *Based on targets derived from IT's objectives*
- ▶ *Contain a mix of objective and subjective measures*
- ▶ *Flexible and responsive to changing priorities and requirements*
- ▶ *Based on easy to collect actual measurement results*
- ▶ *Include both positive measures (to motivate) and negative measures (to correct)*
- ▶ *Balanced, i.e. measuring more than just financial results. The Balance Scorecard is recommended as an effective approach providing financial, customer, internal and learning dimensions (The Balanced Scorecard, Kaplan & Norton)*
- ▶ *Limited in number and focused only on priority areas but sufficient to support decision making (passes the “so-what?” test)*

- ▶ *Easy to interpret (e.g. reporting should be visual using RAG or heat map techniques) and permit drilling down for more detail and examination of root causes. A scorecard is sometimes not appropriate, e.g. for project review and prioritisation or detailed analysis (where aggregation distorts or confuses)*
- ▶ *Show trends to enable backward examination and forward extrapolation*
- ▶ *Consolidated for hierarchical reporting*
- ▶ *Support benchmarking internally between peer groups and externally with best practice*
- ▶ *Integrated if possible with any existing business level performance measurement system*

## 2.3 Who are the stakeholders and what are their requirements?

Stakeholders play a key part in IT Governance. At the heart of the governance responsibilities of setting strategy, managing risks, allocating resources, delivering value and measuring performance, are the stakeholder values, which drive the enterprise and IT strategy. For performance measurement to be successful, it is important to understand who the stakeholders are and what their specific requirements and drivers are so that the performance measurements will be meaningful to them. An IT Governance best practice is the approval of measures by stakeholders (IT Governance Institute – Board Briefing on IT Governance).

For the purposes of performance measurement, we have classified stakeholders into three groups: investors, controllers and deliverers/providers with specific measurement interests and requirements as follows:

### ▼ Investors – (business management, business partners and IT management)

- ▶ **Interests** – *they provide the funding and want to see a return on their investment and alignment with their strategic objectives*
- ▶ **Requirements**
  - *Financial – ROI, cost v. budget, productivity, benefits realisation*
  - *Customer – surveys and feedback (subjective as well as objective), strategic objectives v. actual projects/activities*
  - *Process – capability benchmark, performance exceptions, transformation capability and tactical agility*
  - **Learning** – *attrition, retention, skill profile, resource short fall, training and development*

### ▼ Controllers – (internal and external audit, risk and compliance officers, finance, human resources, industry specific regulators)

- ▶ **Interests** – *they monitor risk and compliance and have an interest in due process, regulatory and legal requirements, evidence of governance and risk management, amount of rework/repeat effort, and compliance with strategy*
- ▶ **Requirements**
  - *Financial – losses, investments in control improvements*
  - *Customer – exceptions/breaches, risk management, compliance with legislation and regulations*
  - *Process – control effectiveness, compliance*
  - *Learning – risk identification, risk prevention*

### ▼ Deliverers/Providers – (IT service and product suppliers, in-house and outsourced, contract and procurement management and staff involved in IT delivery and support)

- ▶ **Interests** – *they need to meet customer expectations, and deliver in an efficient and effective way, preserving and enhancing reputation*
- ▶ **Requirements**
  - *Financial – operational and project costs, cost allocation/recovery, service credits, cost optimisation*
  - *Customer – performance against SLAs, satisfaction feedback e.g. survey responses, customer retention and growth statistics, effectiveness of dealing with business churn*

- *Process – internal improvement in efficiency and risk reduction, internal v. outsource decision support*
- *Learning – capability to deliver, readiness for new requirements, time to market for new initiatives*

## 2.4 What should we measure?

The ownership of measures and accountability for achieving targets should be clear. Furthermore, ownership and the collection of measurement data will not always be an IT responsibility, e.g. measurement of customer-focused outcomes. It should therefore also be clear whose responsibility collection is. Where appropriate, measures should be formalised in Service Level Agreements (SLAs) based on service descriptions written in a language and using terms meaningful to the customer. For third party service providers an SLA should form part of the contractual agreement so that performance measurement can be backed up with contractual recourse in the event of performance failure. To support IT Governance the following top fifteen areas to measure are recommended, with an indication of who has a primary interest and therefore who should approve the measures (figure 2.4)

| Area  | Investors | Controllers | Providers |
|---|-----------|-------------|-----------|
| Business & IT alignment   | √         |             |           |
| Major project delivery performance (objectives, time and budget)              | √         |             | √         |
| Overall financial performance (costs v. budgets)                              | √         | √           | √         |
| ROI for IT investments (business benefit)                                     | √         |             |           |
| Status of critical risks  | √         | √           | √         |
| Performance with respect to reliability and availability of critical services | √         |             | √         |
| Complaints (QOS) and customer perception                                      | √         |             |           |
| Number of significant reactive fixes to errors                                |           |             | √         |
| SLA performance by third parties  | √         |             | √         |
| Relationships with suppliers (quality & value)                                | √         |             | √         |
| Capability e.g. process maturity  |           |             | √         |
| HR measures for people involved in IT activities                              |           |             | √         |
| Internal and external benchmarks  | √         |             | √         |
| Audit weaknesses  |           | √           | √         |
| Business continuity status  | √         | √           | √         |

**Figure 2.4**

## 2.5 What is best practice?

Experiences gained by the IMPACT SIG members have identified a number of enablers and inhibitors that will assist in the achievement of Performance Measurement best practices when supporting IT Governance. Since the Interest Group is not primarily focused on performance measurement techniques we are not attempting to provide best practice guidance on measurement methods and/or tools.

In general, performance measurement should support this classic control model (figure 2.5)

▼ Enablers

- ▶ *Support and ownership of performance measurement by Stakeholders*
- ▶ *Measures that are approved by and meaningful to the Stakeholders*
- ▶ *Measures that align with agreed IT objectives*
- ▶ *Measures that focus on processes critical to the success of IT objectives*
- ▶ *Measures that are easy to collect and understand*
- ▶ *Targets that are challenging but also achievable*
- ▶ *Measures that are balanced e.g. based on the Balanced Scorecard technique*
- ▶ *Measurement reports and scorecards that are easy to interpret, with explanations of exceptions*
- ▶ *Where possible, measures should be automated*

▼ Inhibitors

- ▶ *Too much focus on technical measures (especially if they are not aligned to IT objectives)*
- ▶ *Lack of ownership and accountability*
- ▶ *Measures which are not straightforward to interpret or encourage counter-productive behaviour (cf. National Health Waiting List targets)*
- ▶ *Measures which are expensive to collect or not focused on priority areas*
- ▶ *Too many measures obscuring relevant and important information*

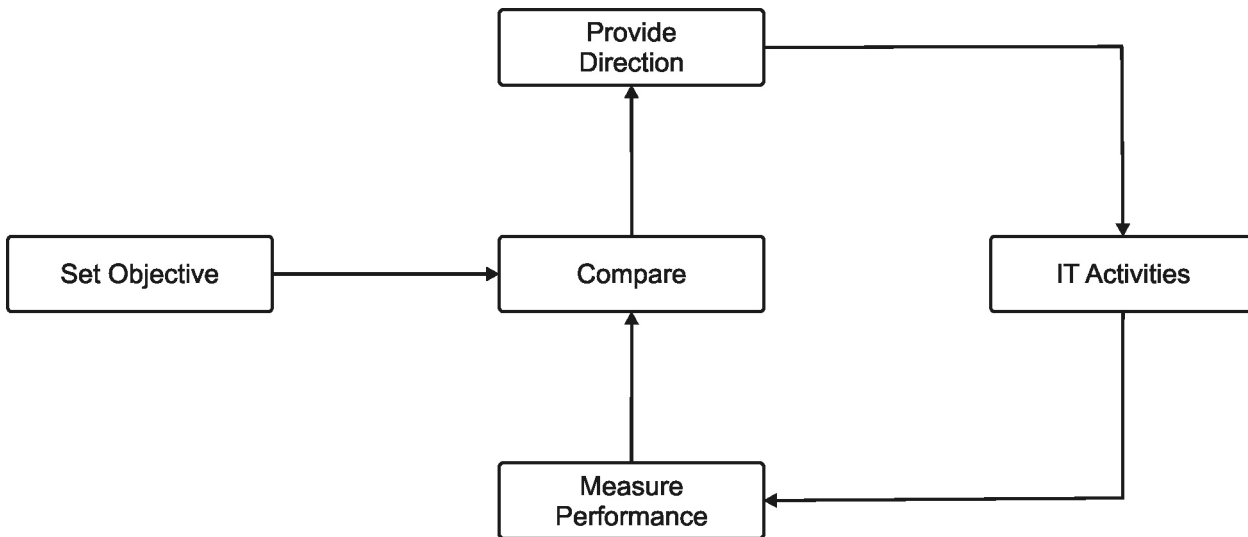


Figure 2.5<sup>3</sup>

# 3 Implementation Roadmap

|  |    |
|--|----|
| <b>3.1</b> What are the goals and success criteria? .....                                | 14 |
| <b>3.2</b> How to get started – the key initial activities .....                         | 15 |
| <b>3.3</b> Who needs to be involved and what are their roles and responsibilities? ..... | 16 |

This chapter describes an “Implementation Roadmap” for activating an effective IT Governance programme to deliver the above benefits, and is based on the practical implementation experiences gained by the IMPACT IT Governance SIG members.

The roadmap begins with establishing clear goals and objectives in order to align effort with the real needs of the enterprise, to manage expectations, and to ensure continual focus. The roadmap then consists of activities to get started, followed by the key implementation tasks with suggested roles and responsibilities. IT Governance is an ongoing task and therefore this roadmap is only the initial phase of what needs to become an iterative sustainable approach.

## ▶▶ 3.1 What are the goals and success criteria?

Implementing IT Governance for many organisations will mean major changes. It is important therefore to not only have high-level sponsorship but also the active involvement of key stakeholders. The roadmap is an iterative lifecycle that begins with an initial phase to define overall goals and to gain the support and commitment of top management which then leads to the ongoing effective governance of IT activities.

A generic set of initial objectives has been identified by the SIG and is shown in Figure 3.1. Figure 3.1.1 suggests some success criteria for this initial phase of IT Governance.

| Typical objectives of the initial implementation phase   | “Agreed” ✓ |
|--|------------|
| Define the meaning of governance in your organisation and where/if IT Governance fits  |            |
| Identify any organisational/environmental/cultural constraints and enablers  |            |
| Achieve a broad understanding of IT Governance issues and benefits across all stakeholders   |            |
| Agree, publish and gain acceptance of an initial IT Governance framework, tools and processes  |            |
| Completion of an initial gap analysis against best practice – to demonstrate where IT Governance is already in place and to highlight areas of focus for the roadmap |            |
| Creation of a Project Initiation Document (PID) and/or Terms of Reference (ToR) that has the support of stakeholders   |            |
| Creation of a Project Plan with definition and prioritisation of the initial ITG project deliverables  |            |
| Identification and commitment of the resources required to deliver this initial project  |            |
| Identification and sign-off of Key Performance Indicators and Critical Success Factors for this project  |            |
| Documented estimated timescales and resource (£s and FTE) implications as well as expected ROI   |            |
| Alignment of the ITG Initiative with business objectives/strategy  |            |

Figure 3.1



| Success criteria for the initial implementation phase   | “Done” ✓ |
|---|----------|
| Key stakeholders identified, engaged and actively involved  |          |
| Key stakeholders contributing towards and able to explain and support the business case for ITG           |          |
| Stakeholders have an understanding of the expectations of the IT Governance initiative                    |          |
| Some initial ‘quick wins’ have been identified and implemented – to make governance “real”                |          |
| Acceptance of the published IT Governance framework by those responsible for implementation               |          |
| An effective communication plan – who to, what, when etc. to overcome any barriers and to motivate change |          |
| Current key IT projects mapped against ITG plan, to look for easy fit/implications                        |          |
| Changes are sustainable and institutionalised, i.e. they become Business as Usual practices               |          |

**Figure 3.1.1**

## 3.2 How to get started – the key initial activities

Having set the goals, and gained support, activation consists of two steps – planning, based on analysis of the current environment, followed by implementation itself.

### Planning

These are recommended implementation planning activities together with some critical success factors:

| Activities  | CSFs  |
|---|---|
| <ul style="list-style-type: none"> <li>• Identify champions                             <ul style="list-style-type: none"> <li>- Stakeholders (including partners), Input providers, IT strategy committee (council) members</li> </ul> </li> <li>• Establish IT strategy committee (council)</li> <li>• Identify IT “hotspots” in the organisation, and where governance could enable ‘hotspot’ resolution:                             <ul style="list-style-type: none"> <li>- Strategy? Delivery? IT Cost? Architecture?</li> <li>- Where current approaches have not worked or caused serious failures</li> </ul> </li> <li>• Identify skill set and capabilities needed from people involved</li> <li>• Identify existing good practice (‘pseudo governance’) or successes that could be built on or shared</li> <li>• Identify cost/benefit arguments – why do we need to do anything?</li> <li>• Identify inconsistencies in process/practice</li> <li>• Identify opportunities for “rest of business” to get involved in IT</li> <li>• Explore opportunity to adopt industry best practice model, or standards framework</li> <li>• Utilise external influences</li> <li>• Create a measurement approach for an area or activity to expose actual evidence of problems</li> <li>• Do some gap analysis against industry best practice</li> </ul> | <ul style="list-style-type: none"> <li>✓ Authoritative and articulate champions</li> <li>✓ Available skills and capabilities</li> <li>✓ Well prepared business cases approved by stakeholders</li> <li>✓ Real opportunities for the business to see the benefit of participating</li> <li>✓ Practical and useful governance approaches</li> <li>✓ Effective and useful measures</li> <li>✓ Expose the truth /whole picture, warts and all, about project success /failure, showing how governance can be helpful</li> </ul> |

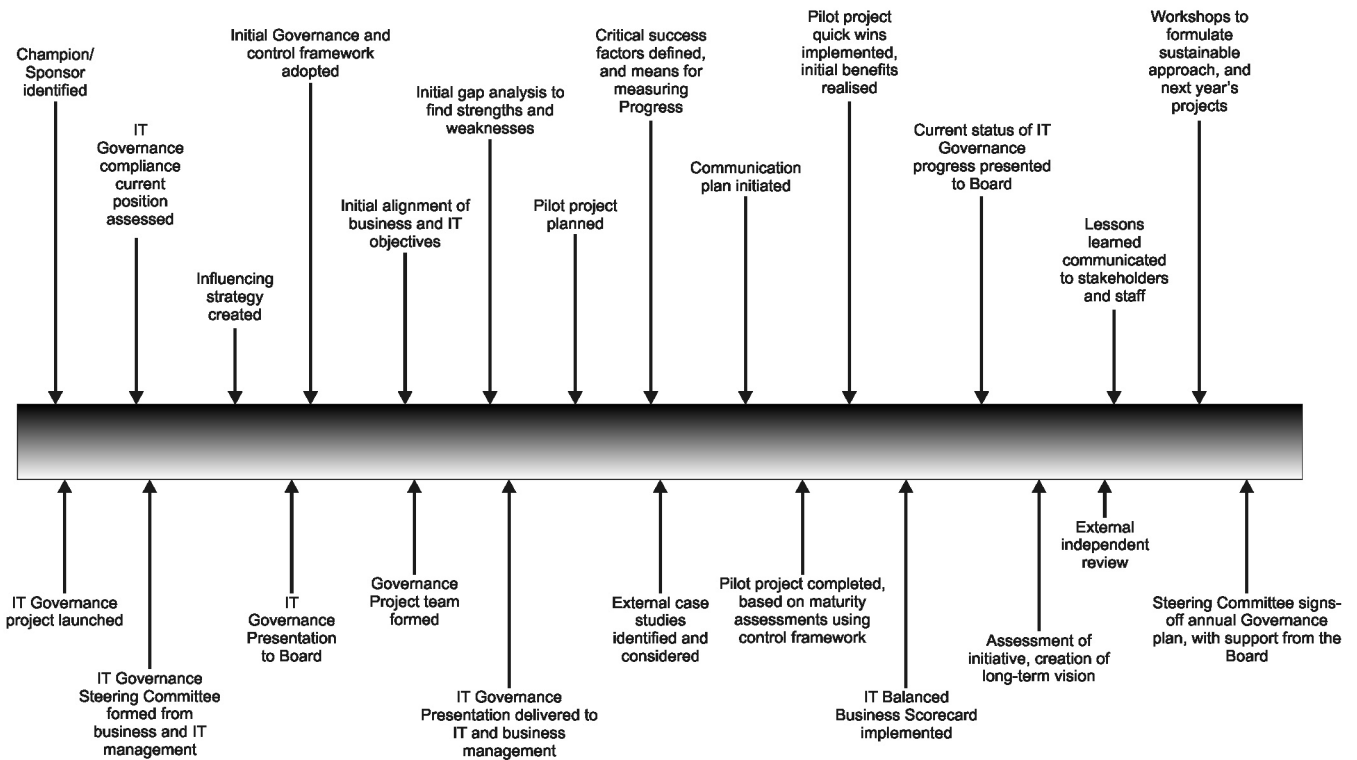
**Implementation**

These are the recommended activities to start up the implementation roadmap, together with some critical success factors:

| Activities  | CSFs  |
|---|---|
| <ul style="list-style-type: none"> <li>• Create a sound project structure                             <ul style="list-style-type: none"> <li>- Define scope (what is included/excluded) and deliverables</li> <li>- Agree success criteria/quality criteria</li> <li>- Set realistic timeframes</li> <li>- Allocate suitable resources and roles</li> <li>- Identify risks and a risk mitigation strategy</li> </ul> </li> <li>• Gain approval from Senior Management (the higher the better within the Enterprise)</li> <li>• Find reference site, or external examples to learn from</li> <li>• Build communication plan to gain buy-in, and break down barriers                             <ul style="list-style-type: none"> <li>- Who/what/how frequent/purpose</li> </ul> </li> <li>• Do a pilot activity (demonstrate the business case) to show how it would work and demonstrate potential benefits</li> <li>• Follow a phased introduction, e.g.                             <ul style="list-style-type: none"> <li>- Focus on critical but easier to address areas</li> <li>- Assess projects first</li> <li>- Build up operational performance improvement progressively based on prioritising maximum return for lowest cost</li> <li>- Consider one business area first, others later</li> <li>- Aim to establish some successes while learning how to be effective</li> </ul> </li> </ul> | <ul style="list-style-type: none"> <li>✓ Good project management (set the governance tone)</li> <li>✓ Expectations set correctly</li> <li>✓ Approved business case</li> <li>✓ Manage IT like you manage the rest of the business</li> <li>✓ Convincing reference sites</li> <li>✓ Successful pilot</li> <li>✓ Address quick wins first to demonstrate results and realise benefits before attempting any major changes</li> </ul> |

**3.3 Who needs to be involved and what are their roles and responsibilities?**

All three generic groups of stakeholders, and their interests, should be involved in an IT Governance initiative. A key characteristic of any successful IT Governance initiative is the establishment of an enterprise-wide approach that clearly sets out roles and responsibilities, emphasising that everyone has a part to play in enabling successful IT outcomes.



**Figure 3.3: This timeline is generic and intended only to be an example – it is based on the SIG's experience. Thanks to Legal and General for the concept.**

It may also be helpful to include an external, or internal, facilitator to provide an objective and neutral position. The suggested generic roles and responsibilities of the three main groups are shown in Figure 3.3.1.

| Investors   | Providers   | Controllers   |
|---|---|---|
| <p><b>Management board (authority to make things happen)</b></p> <ul style="list-style-type: none"> <li>• Give direction backed up with adequate support and sponsorship</li> <li>• Balance requirements with available resources, making available additional resources if required</li> <li>• Insist on and seek measurable benefit realisation</li> <li>• Coordinate overseas/satellite parts of the enterprise to ensure their interests and constraints have been considered</li> <li>• Create organisation and structure to ensure board involvement in the governance process – by forming committees, establishing reporting processes</li> <li>• Monitor performance, monitor risks, correct deviations</li> </ul> <p><b>Business and IT senior managers, business partners and project sponsors</b></p> <ul style="list-style-type: none"> <li>• Implement organisation and necessary infrastructure</li> <li>• Take ownership of requirements</li> <li>• Champion and collaborate in IT governance activities</li> <li>• Ensure business strategy and objectives are set and communicated and aligned with IT</li> <li>• Assess business risks and impacts</li> <li>• Establish reporting processes meaningful to stakeholders</li> <li>• Communicate any business concerns in a balanced and reasoned way</li> <li>• Provide project champions, creating the seeds of change</li> </ul> <p><b>User representatives</b></p> <ul style="list-style-type: none"> <li>• Take responsibility for Quality Assurance programme (design and output)</li> <li>• Regularly check actual results against original (or changed) goals</li> <li>• Provide service feedback to providers</li> </ul> | <p><b>IT management (internal and external), with support from business management</b></p> <ul style="list-style-type: none"> <li>• Take ownership and set direction of IT Governance activities</li> <li>• Build and achieve a pilot business case</li> </ul> <p><b>IT management</b></p> <ul style="list-style-type: none"> <li>• Set IT objectives</li> <li>• Define IT governance and control framework</li> <li>• Identify critical IT processes</li> <li>• Assess risks, identify concerns</li> <li>• Assess IT capability, identify gaps</li> <li>• Initiate a continuous improvement programme</li> <li>• Develop business cases for improvements</li> <li>• Design and implement solutions</li> <li>• Commit skilled resources</li> <li>• Establish performance measurement system</li> <li>• Report to senior management</li> <li>• Respond to QA feedback from customers</li> </ul> <p><b>Suppliers/business partners</b></p> <ul style="list-style-type: none"> <li>• Integrate any own existing or planned governance practices with customer's</li> <li>• Support and contribute to customer's governance approach</li> <li>• Agree service definitions, incentives, measures and contracts/agreements</li> </ul> <p><b>Training and Development</b></p> <ul style="list-style-type: none"> <li>• Ensure adequate education and communication</li> </ul> <p><b>HR function</b></p> <ul style="list-style-type: none"> <li>• Incorporate governance principles into induction and performance measurement process</li> </ul> <p><b>Core team</b></p> <ul style="list-style-type: none"> <li>• Define plan and deliverables</li> <li>• Organise team and roles (architects, senior responsible officer, facilitator, project manager, process owners)</li> <li>• Undertake core tasks</li> <li>• Report progress to plan</li> </ul> | <p><b>Internal and External Audit</b></p> <ul style="list-style-type: none"> <li>• Scope audits in coordination with governance strategy</li> <li>• Provide assurance on the control over IT</li> <li>• Provide assurance on the control over the IT performance management system</li> </ul> <p><b>Risk Management</b></p> <ul style="list-style-type: none"> <li>• Ensure that new risks are timely identified, provide advice</li> </ul> <p><b>Compliance officers</b></p> <ul style="list-style-type: none"> <li>• Ensure that IT complies with policy, laws and regulations</li> </ul> <p><b>Finance</b></p> <ul style="list-style-type: none"> <li>• Advise on and monitor IT costs and benefits</li> <li>• Provide support for management information reporting</li> <li>• Incorporate governance requirements into purchasing/contract process</li> </ul> |

Figure 3.3.1

# 4 Communication Strategy & Culture

---

|  |    |
|--|----|
| 4.1 Who do we need to influence? .....       | 18 |
| 4.2 What are the key messages? .....         | 19 |
| 4.3 Communication best practices .....       | 20 |
| 4.4 Developing an influencing strategy ..... | 20 |
| 4.5 Change roadmap .....                     | 22 |

---

IT Governance and risk management is about improving the management and control of IT activities and enabling top management to exercise proper oversight. To achieve this, better processes, controls, best practices and management techniques are required. However all of these improvements will only have a chance of succeeding in a sustainable way if the culture of the organisation is changed to drive and support the desired new management approach.

Effective communications are a key enabler of these changes, just as poor communications can create a legacy of misunderstanding, lack of trust, and technical mystique and hype in many organisations. As we said earlier, if it is difficult for those literate in technology and relatively close to the IT function, then it is even worse for the end customer who finds technical jargon a smokescreen and lack of information relevant to his business a major headache. Communication and cultural behaviour, based on appropriate influencing strategies are therefore key ingredients of any IT Governance improvement programme. In order to best influence stakeholders, and communicate the major objectives and benefits of IT Governance throughout the organisation, the right language must be used. Given the significance of IT both in terms of investment and potential impact on the business – the risks of IT and of failing to exploit IT for strategic advantage must be stressed in any communication about IT Governance. Wake-up calls are sometimes required at the highest levels. Stakeholders must understand and feel responsible for safeguarding against IT risks.

Effective communications will ensure that “everyone is on the same page” – that key issues have been grasped, objectives have been positively accepted by management and staff, and everyone understands their role. Every organisation will have its own existing culture and choice of IT Governance approach that it wishes to adopt. The roadmap to follow for cultural change and effective communication will therefore be unique to each organisation, however there may be common elements.

## 4.1 Who do we need to influence?

A fundamental element of IT Governance is change. When considering who needs to be influenced for successful IT Governance, it is important to remember that different messages are needed for different stakeholders. Whatever the topic is about, the language used must be understandable, relevant to the intended audience, and motivate positive attitudes towards change.

Identifying and gaining the support of key influencers of success and failure help enable successful communications strategies. It is also vital to recognise the main stakeholders impacted by the change, identify why we want to influence a particular stakeholder, and identify any resistance that needs to be overcome. Positive attitudes need to be promoted and used to influence others.

All three generic groups of stakeholders, and their interests, should be involved in an IT Governance initiative. It is critical to influence these groups positively so that they understand the objectives and benefits of IT Governance and are able to communicate consistently to each other and within their groups (Figure 4.1).

| <b>Who needs to be influenced?</b>   |  |   |
|--|--|---|
| <b>Investors</b>   | <b>Providers</b>   | <b>Controllers</b>  |
| <ul style="list-style-type: none"> <li>• The Board</li> <li>• IT Council/Management Team</li> <li>• Senior business unit managers e.g. key customers of IT services</li> <li>• Business Partners</li> <li>• External investors/shareholders – as part of corporate governance</li> </ul> | <ul style="list-style-type: none"> <li>• Project and change managers (IT and Business)</li> <li>• Programme managers</li> <li>• Business managers and users</li> <li>• Technical delivery and support teams</li> <li>• Key players e.g. business sponsors, project champions</li> <li>• Relationship managers and internal communications teams</li> <li>• Suppliers (especially outsourced service providers)</li> <li>• Contract and procurement management</li> <li>• Peripheral players/influencers/policy owners e.g. HR, Facilities Management, Legal</li> </ul> | <ul style="list-style-type: none"> <li>• Internal audit and external audit (due diligence)</li> <li>• External regulators</li> <li>• Corporate governance coordinator</li> <li>• Risk managers</li> <li>• Compliance – regulatory and internal</li> <li>• Finance/Project Managers/IT and business managers – reviewers of benefits/ROI</li> <li>• Post investment appraisal/post project review teams</li> </ul> |
| <b>Key Messages</b>  |  |   |
| <ul style="list-style-type: none"> <li>• Benefits of governance</li> <li>• Why we need to do it</li> <li>• Impact on the business strategy</li> <li>• Commitment to support action plans</li> </ul>  | <ul style="list-style-type: none"> <li>• Benefits of governance</li> <li>• Why we need to change</li> <li>• Your role and responsibility</li> <li>• How you need to change</li> </ul>  | <ul style="list-style-type: none"> <li>• Need for independent assessment and assurance</li> <li>• Relate to real business risks and impacts</li> <li>• Work positively with management to address control needs</li> </ul>  |

Figure 4.1

## 4.2 What are the key messages?

In order to best influence stakeholders, and communicate the major objectives and benefits of IT Governance, the right language must be used. An inability to communicate effectively has been one of the major causes of IT failures, with too much technical jargon, lack of business understanding and poor appreciation of the other party's requirements and issues. Ideally, a common language is required, and a balance has to be found between the business trying to understand IT and IT trying to understand the business. Communications will improve if the business views the technology provider not as a simple enabler but as a valued business partner and if IT presents benefits in the language that the business understands. The following are examples of some of the key messages that need to be communicated, based on three primary IT Governance objectives and the related benefits that can be realised (Figure 4.2).

| <b>Ability to address these Objectives</b>   | <b>will realise these Benefits</b>   |
|--|--|
| <p><b>IT and Business strategic and operational alignment</b></p> <ul style="list-style-type: none"> <li>• IT and business working towards the same corporate goals</li> <li>• Architecture and other technology approaches seen as relevant and value adding to the business</li> </ul>                                   | <p><b>Roi/Stakeholder Value, Transparency and Accountability</b></p> <ul style="list-style-type: none"> <li>+ Shareholder Value</li> <li>+ Leveraging investments for greatest return</li> <li>+ Better use of IT capabilities</li> <li>+ Cost effective IT solutions</li> </ul>   |
| <p><b>Effective Relationship Management (internal and external)</b></p> <ul style="list-style-type: none"> <li>• Mutual understanding of goals</li> <li>• Shared language and terminology</li> <li>• Working in partnership – equal investment and responsibility</li> <li>• Clear accountabilities</li> </ul>             | <p><b>Opportunities and Partnerships</b></p> <ul style="list-style-type: none"> <li>+ Increased synergies</li> <li>+ Improved speed to market</li> <li>+ Improved efficiencies, particularly with third parties</li> <li>+ Agility to respond to change</li> </ul>                 |
| <p><b>Management Control/Quality Management</b></p> <ul style="list-style-type: none"> <li>• Standardised processes</li> <li>• Consistent approaches</li> <li>• Comparison/adoption of external best practices (e.g. ISO, CMMi, CobiT, ITIL)</li> <li>• Professional IT services</li> <li>• Management of risks</li> </ul> | <p><b>Performance Improvement</b></p> <ul style="list-style-type: none"> <li>+ Risk mitigation</li> <li>+ Continuous efficiency and quality improvements</li> <li>+ Increased assurance that controls are working</li> <li>+ Transparency and confidence about measures</li> </ul> |

Figure 4.2

## 4.3 Communication best practices

The experiences of the IT Governance SIG have shown that it is best practice to emphasise the importance of controlling IT related risks when communicating the need for IT Governance. In particular, make sure stakeholders understand and feel responsible for safeguarding against risks that would not exist if they had put in place effective IT Governance controls:

- a) The “downside” business risks associated with the use and function of IT, i.e. financial losses, damage to reputation, loss of service etc.
- b) The “upside” business risks of not exploiting IT effectively, i.e. loss of competitive advantage, inefficiencies, failure to respond to changing markets etc.

### Recommended approaches

▼ If IT risks are not communicated effectively, and instead are surrounded by hype and complexity, then stakeholders will not appreciate their real impact, take the issues seriously, or be motivated to insist on better controls. The following approaches are recommended to ensure risks have been properly appreciated:

- ▶ *Emphasise the business impact of risks associated with misaligned IT strategies, misuse of technology, badly managed operations and ineffective project management. Show how these risks can be mitigated by effective controls.*
  - Use case studies that have impacted the business or other businesses (e.g. virus attacks, critical service outages, projects with “unexpected outcomes”) to illustrate how issues might arise.
- ▶ *Identify relevant examples of governance providing business benefits beyond the basic requirement of evidencing control.*
  - Use case studies to illustrate how effective governance has identified risk to the business, its objectives and strategy, and brokered an alternative solution.
  - Use case studies to illustrate business benefits as a direct result of effective governance, e.g. reduced costs, improved quality, productivity, reputation and marketing advantages.
- ▶ *Scenario modelling with risk assessment and mitigation:*
  - Consider known and new risks across both business and IT (e.g. external audit requirements)
  - How governance can help mitigate the risk
  - Calculate a risk factor = likelihood x impact
  - Consider options – accept, mitigate or assign
- ▶ *Using common business language:*
  - Technological risk in financial/economic/business terms
  - Legal/regulatory, contractual implications

▼ Critical Success Factors

- ▶ *Involve all relevant stakeholders in a facilitated workshop environment*
- ▶ *Get clear ownership and funding commitment for risk mitigating actions*
- ▶ *Monitor/track all actions*

## 4.4 Developing an influencing strategy

Critical to the success of any IT Governance initiative is an effective communications plan. The communications plan should be based on a well-defined influencing strategy. Behaviours will need to be changed and care should therefore be taken to ensure that participants will be motivated and see the benefits of the new approaches, as well as understanding the consequences of accepting responsibility. If this is not positively communicated, then IT Governance will not be perceived as part of the corporate mission with Board level support. Management will resist it as a barrier to getting the job done, a deviation from current priorities, or another management fad.

The strategy should identify opportunities for the active involvement of stakeholders in developing the governance approach, planning and implementing IT management changes, and ideally building specific change objectives/targets into personal performance plans. The stakeholders are likely themselves to be the targets of change and should be involved in discussing/evolving responses to the change via collaborative workshops, focus groups etc.

| Influencing style examples   |   |   |   |
|--|---|---|---|
| Asserting  | Persuading  | Bridging  | Attracting  |
| <ul style="list-style-type: none"> <li>Stating expectations of improved IT Governance and consequences of not adopting the new control model</li> <li>Evaluating current capability, risk management, delivery quality etc. and exposing unacceptable performance</li> <li>Creating incentives by setting clear IT Governance objectives, based on business priorities, backed up by the personal reward scheme</li> </ul> | <ul style="list-style-type: none"> <li>Proposing new management approaches, best practices, standards for IT activities, based on development workshops</li> <li>Reasoning that changes are needed, by educating top management about the key IT issues and the benefits IT Governance can provide, e.g. more ownership in the business of IT projects</li> </ul> | <ul style="list-style-type: none"> <li>Involving the business in IT decision making, by breaking down technical barriers and encouraging shared responsibility for IT outcomes</li> <li>Listening to user feedback about IT services and encouraging suggestions via satisfaction surveys</li> <li>Disclosing IT problems and incidents seeking workable solutions instead of covering them up</li> </ul> | <ul style="list-style-type: none"> <li>Finding Common Ground by developing corporate mission statements and policies about IT Governance with support from the Board</li> <li>Visioning by IT and the business developing shared strategies and action plans, backed up by measurable and accountable objectives and targets</li> </ul> |



**Figure 4.4**

The influencing strategies need to be designed to work in specific situations with the individual influence targets identified. The following table shows four typical influencing styles, examples of the communications involved and the associated leadership styles. It is important to select the most appropriate style taking into account who needs to be influenced and on what topic.

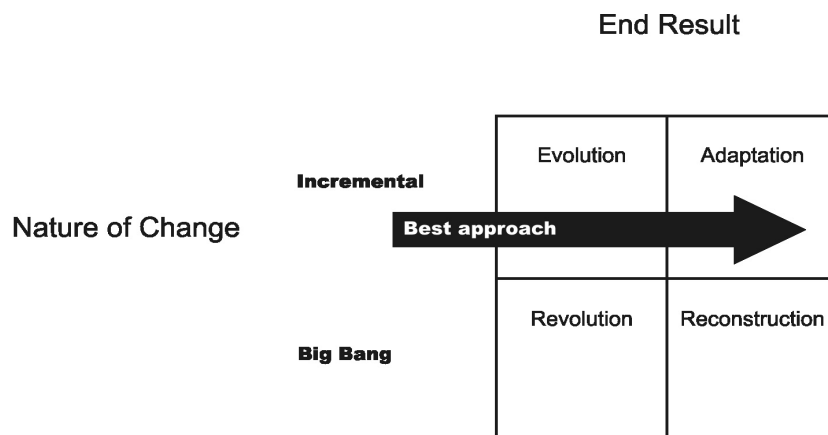
▼ Focus on Roles and Responsibilities

- ▶ *Identify an overall sponsor and steering group with specific tasks and responsibilities for leading the change*
- ▶ *Ensure there is a complete structure of cascaded sponsorship down to team/line manager level*

▼ Focus on individual situations

- ▶ *Identify champions (those high on interest and/or influence)*
- ▶ *Use successes as benchmarks*
- ▶ *Disseminate across teams and support formation of new teams*

Figure 4.4.1 shows different change approaches that can be used. For IT Governance initiatives experience shows that the best approach is incremental change evolving and adapting of current practices to a new collaborative IT management approach.



**Figure 4.4.1**

## 4.5 Change roadmap

Every organisation will have its own existing culture and choice of IT Governance paradigm that it wishes to adopt. The roadmap to follow for cultural change and effective communication will therefore be unique to your specific situation.

▼ The following techniques (Exploring Strategic, Change Veronica Hope-Hailey, Julia Balogun, Gerry Johnson, Kevan Scholes, Cranfield University) can help guide the best path to follow, and can be used to assess how your organisational culture and management style currently deals with the governance of its IT activities and what cultural style it desires. To do this you must:

- ▶ Analyse the existing state
- ▶ Define the desired state

Cultural style and paradigms are formed from several characteristics which can generally be illustrated as shown in Figure 4.5.

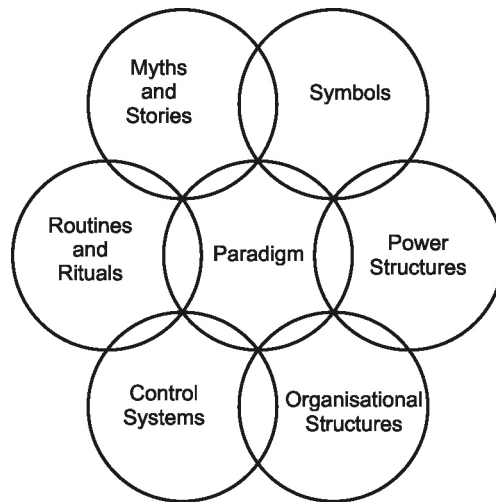


Figure 4.5

Figure 4.5.1 illustrates some of the typical current and desired IT Governance behaviours found in many organisations today.

| Characteristic                   | Current   | Desired   |
|----------------------------------|---|---|
| <b>Myths and Stories</b>         | Poor business and IT alignment: Project failures; budget overruns; poor service, failure to meet business needs.    | Effective business and IT alignment: Demonstrable RoI, project success stories, user satisfaction, business driving IT. |
| <b>Symbols</b>                   | Mystique and technical jargon, lack of business terms.  | Common language based on customer needs. Business literate in IT issues and opportunities.                              |
| <b>Power Structures</b>          | Them and us attitudes.  | Collaboration.  |
| <b>Organisational Structures</b> | Divisive. IT seen as overhead function.   | Partnerships. IT seen as business enabler.  |
| <b>Control System</b>            | Based on departmental units and who knows the most.   | Based on defined processes, standards and best practices owned by the organisation.                                     |
| <b>Routines and Rituals</b>      | Hidden agendas, measures in provider's terms and a general lack of transparency leaving top management in the dark. | Joint forums for monitoring progress, measures in customer's terms, transparent reporting to top management.            |

Figure 4.5.1



# 5 Capability Maturity Assessment

|  |    |
|--|----|
| <b>5.1</b> Why IT capability is important .....                        | 23 |
| <b>5.2</b> How to measure IT capability .....                          | 23 |
| <b>5.3</b> Setting maturity targets and considering improvements ..... | 24 |
| <b>5.4</b> Roadmap for sustaining the approach .....                   | 25 |
| <b>5.5</b> Self-assessment tools .....                                 | 26 |

**M**onitoring and assessing the adequacy of IT Resources (people, applications, technology, facilities, data) to ensure that they are capable of supporting the current and proposed IT strategy is a key aspect of IT Governance. In many organisations board level management have a very unclear view of their IT capability, and find it very difficult to understand the technical and organisational IT environment upon which they increasingly depend. Often inadequacies only manifest themselves when projects fail, costs spiral, operational systems crash, or service providers fail to deliver the value promised. To exercise sufficient governance and oversight, senior management should insist on objective and regular assessments of their internal and externally provided IT services to ensure any inadequate capabilities are exposed before serious problems occur, and then take the necessary action to rectify weaknesses. In recent years, surveys and assessments carried out around the world have shown that in general IT capabilities have not kept pace with increasing IT complexities and the growing demands for reliable, secure and flexible services. Cost control and reducing inefficiencies are also important reasons for reviewing technical and organisational capability.

**Improving the maturity of IT capability both reduces risks and increases efficiency – cost saving is often a justification.**

Capability Maturity Modelling (CMM) techniques (CMM was created by the Software Engineering Institute with Carnegie Mellon) are increasingly being adopted by many organisations for assessing IT capability. This technique focuses on the IT management processes that control IT resources, and assessments usually reveal significant weaknesses and an IT capability disproportionate to the high dependency organisations have on their IT service providers. Using the CMM scale it is rare to find even a defined (level 3) process in many organisations.

Management should insist on objective and transparent assessments, and carry out these analyses as part of any due diligence review, or request third party certifications when considering outsourcing or during mergers and acquisitions. Agreement then must be reached regarding where and how to address inadequacies, by either investing in the internal infrastructure or seeking externally provided outsourced resources, or accepting the risks.

## ▶▶ 5.1 Why IT capability is important

A key to successful IT performance is the optimal investment, use and allocation of IT resources (people, applications, technology, facilities, data) in servicing the needs of the enterprise. Most enterprises fail to maximise the efficiency of their IT assets and optimise the costs relating to these assets. In addition, the biggest challenge in recent years has been to know where and how to outsource and then to know how to manage the outsourced services in a way that delivers the values promised at an acceptable price.

▼ Boards need to address appropriate investments in infrastructure and capabilities by ensuring that:

- ▶ *The responsibilities with respect to IT system and services procurement are understood and applied.*
- ▶ *Appropriate methods and adequate skills exist to manage and support IT projects and systems.*
- ▶ *Improved workforce planning and investment to ensure recruitment and more importantly, retention, of skilled IT staff.*
- ▶ *IT education, training and development needs are fully identified and addressed for all staff.*
- ▶ *Appropriate facilities are provided and time is available for staff to develop the skills they need.*

- ▼ Boards needs to ensure that IT resources are used and managed wisely by ensuring that:
  - ▶ *Appropriate methods and adequate skills exist in the organisation to manage IT projects.*
  - ▶ *The benefits accruing from any service procurement are real and achievable.*

IT assets are complex to manage and continually change due to the nature of technology, and changing business requirements. Effective management of the lifecycle of hardware, software licences, service contracts, and permanent and contracted human resources is a critical success factor in not only optimising the IT cost base, but also for managing changes, minimising service incidents, and assuring a reliable quality of service.

Of all the IT assets, human resources represent the biggest part of the cost base and on a unit basis the one most likely to increase. Identifying and anticipating the required core competencies in the workforce is essential. When these are understood, an effective recruitment, retention and training programme is necessary to ensure that the organisation has the skills to utilise IT effectively to achieve the stated objectives.”<sup>8</sup>

## 5.2 How to measure IT capability

- ▼ To ensure IT resources are managed effectively, IT capability should be assessed on a regular basis and whenever resources are critical to strategic IT decisions. The capability assessment should be:

- ▶ *Based on alignment of IT goals with business goals*
- ▶ *Targeted at the IT processes critical to business success by,*
  - *Assessing the current capability of these IT processes*
  - *Determining the required capability*
  - *Analysing any gaps in capability*
  - *Providing transparent visibility of the capability position*
  - *Defining and justifying necessary improvement projects or*
  - *Re-adjusting the IT strategy*
- ▶ *Adjusting goals*
- ▶ *Improving capability*
- ▶ *Outsourcing when cost-effective*

The measurement of IT capability should be an objective assessment oriented towards business requirements. This will ensure that the current “as-is” and required “to-be” capabilities are realistic and measurable enabling any gaps to be identified and a plan to be drawn up to rectify any shortcomings.

The Capability Maturity Model (CMM) approach first developed by the Software Engineering Institute for measuring software delivery capability is increasingly being adopted as the basis for assessing overall IT capability. This model provides a standard scale for assessing the maturity of any IT process on a five-point scale (figure 5.2).

- ▼ The following principles are recommended when carrying out an assessment:

- ▶ *Set Scope*
- ▶ *Select a reference model based on standards and best practices most suitable for your business, e.g. CobiT, ITIL, SEI-CCM, SixSigma, ISO9000/9001, PMBOK – perhaps considering weighting measures*
- ▶ *Use an acceptable measurement methodology agreed with the stakeholders which is defined and transparent*
- ▶ *Set a baseline in the context of 1 and 2 above and present the current state assessment using a scale or rating system*
- ▶ *Set reasonable objectives for the targeted level of capability*
- ▶ *Define measures which relate both to “the journey” as well as the “end goal” (e.g. the KPIs and KGIs recommended by CobiT)*
- ▶ *Ensure simplicity and flexibility*
- ▶ *Limit the number of measures, minimise measurement overhead, and avoid information overload*

- ▼ Consider the following critical success factors:

- ▶ *Appropriate level of ownership*
- ▶ *Avoid complexity and be flexible*

- ▶ *Embed measures into business as usual processes*
- ▶ *Ensure staff have adequate skills, training and tools*
- ▶ *Create a repeatable process and agree frequency of reporting*
- ▶ *Where possible automate measurement and reporting*
- ▶ *Assess achievement against targets alongside other business as usual targets*

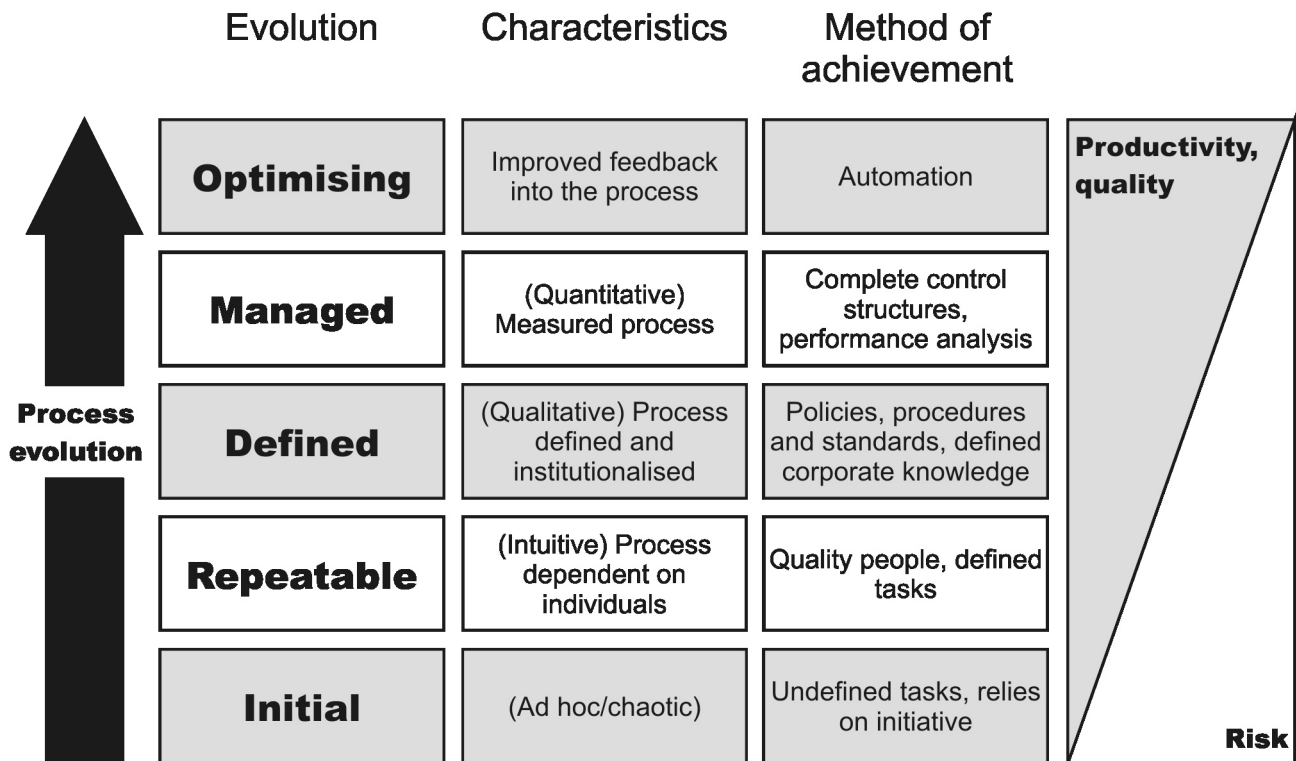


Figure 5.2

### 5.3 Setting maturity targets and considering improvements

The real value of a capability assessment comes from the identification and implementation of cost effective improvements. A realistic and practical approach is required to ensure that the proposed improvements are based on business priorities, will be supported and funded by management, and will be successfully implemented.

The following approach is recommended:

1. *Understand the environment*
2. *Establish capability improvement framework*
3. *Set realistic targets and respond to environment changes*
4. *Identify gaps – prioritise improvements*
5. *Propose achievable solutions*

### 5.4 Roadmap for sustaining the approach

Having initiated a capability assessment approach, and perhaps performed a pilot project, a capability assessment process needs to be implemented as part of normal business procedures.

▼ The following practices are recommended to help ensure the process is sustainable

- ▶ *Articulate current capabilities in relation to an adopted framework*
- ▶ *Set current levels of capability in the context of external comparisons*

- ▶ *State the effect on the business of the current IT capability state of affairs. Describe the ramifications of NOT improving capability e.g. additional costs or risks, inability to realise opportunities, late or non-delivery of the strategic development programme, redundant effort*
- ▶ *Describe the benefits of implementing improvements in specific areas*
- ▶ *Describe the projected effect on the business after delivery of enhancements*

▼ Initiating and sustaining capability enhancements

- ▶ *Agree steering and review mechanism, sponsorship etc.*
- ▶ *Agree on prioritised programme of improvements*
- ▶ *Look for continuous improvement opportunities where improvement is relevant or necessary*
- ▶ *Follow the 80:20 rule, i.e. don't implement more than is necessary*
- ▶ *Embed all improvements as "business as usual", not a one-off initiative*
- ▶ *All improvements should be achievable, sustainable, relevant*
- ▶ *Motivate everyone involved by publishing and celebrating successes*
- ▶ *Agree key measures around implementation of improvements and measures of resultant business benefit – make part of a wider IT balanced scorecard*
- ▶ *Agree communication to targets, stakeholders and sponsors as well as the wider community where there is likely to be a general interest in outcomes*
- ▶ *Periodically review the objectives and reset goals if necessary, checking validity of goals against business strategy*

## 5.5 Self-assessment tool

The simple self-assessment diagnostic in figure 5.5 can be used to help show overall capability at a high level. It is based on the four domains of CobiT, broken down into the 34 CobiT sub-processes. The extent of the analysis depends on how precise you wish to be. A management workshop can be used to arrive at an approximate initial assessment without extensive analysis.

| <b>IT Process/Maturity</b>                                 | <b>Importance</b> | <b>Ad hoc</b> | <b>Repeatable</b> | <b>Defined</b> | <b>Managed</b> | <b>Optimised</b> |
|--|-------------------|---------------|-------------------|----------------|----------------|------------------|
| <b>Planning &amp; Organisation</b>                         |                   |               |                   |                |                |                  |
| PO1 Define a Strategic Information Technology Plan         | H                 |               |                   |                |                |                  |
| PO2 Define the Information Architecture                    | M                 |               |                   |                |                |                  |
| PO3 Determine the Technology Direction                     | M                 |               |                   |                |                |                  |
| PO4 Define the IT Organisation and Relationships           | M                 |               |                   |                |                |                  |
| PO5 Manage the Investment in Information Technology        | M                 |               |                   |                |                |                  |
| PO6 Communicate Management Aims and Direction              | L                 |               |                   |                |                |                  |
| PO7 Manage Human Resources                                 | L                 |               |                   |                |                |                  |
| PO8 Ensure Compliance with External Requirements           | M                 |               |                   |                |                |                  |
| PO9 Assess Risks   | M                 |               |                   |                |                |                  |
| PO10 Manage Projects                                       | L                 |               |                   |                |                |                  |
| PO11 Manage Quality  | L                 |               |                   |                |                |                  |
| <b>Acquisition &amp; Implementation</b>                    |                   |               |                   |                |                |                  |
| AI1 Identify Solutions                                     | L                 |               |                   |                |                |                  |
| AI2 Acquire and Maintain Application Software              | M                 |               |                   |                |                |                  |
| AI3 Acquire and Maintain Technology Architecture           | M                 |               |                   |                |                |                  |
| AI4 Develop and Maintain Information Technology Procedures | M                 |               |                   |                |                |                  |
| AI5 Install and Accredite Systems                          | L                 |               |                   |                |                |                  |
| AI6 Manage Changes   | M                 |               |                   |                |                |                  |
| <b>Delivery &amp; Support</b>                              |                   |               |                   |                |                |                  |
| DS1 Define Service Levels                                  | M                 |               |                   |                |                |                  |
| DS2 Manage Third-Party Services                            | H                 |               |                   |                |                |                  |
| DS3 Manage Performance and Capacity                        | M                 |               |                   |                |                |                  |
| DS4 Ensure Continuous Service                              | L                 |               |                   |                |                |                  |
| DS5 Ensure Systems Security                                | M                 |               |                   |                |                |                  |
| DS6 Identify and Allocate Costs                            | L                 |               |                   |                |                |                  |
| DS7 Educate and Train Users                                | L                 |               |                   |                |                |                  |
| DS8 Assist and Advise Information Technology Customers     | L                 |               |                   |                |                |                  |
| DS9 Manage the Configuration                               | M                 |               |                   |                |                |                  |
| DS10 Manage Problems and Incidents                         | H                 |               |                   |                |                |                  |
| DS11 Manage Data   | H                 |               |                   |                |                |                  |
| DS12 Manage Facilities                                     | L                 |               |                   |                |                |                  |
| DS13 Manage Operations                                     | M                 |               |                   |                |                |                  |
| <b>Monitoring</b>  |                   |               |                   |                |                |                  |
| M1 Monitor the Process                                     | M                 |               |                   |                |                |                  |
| M2 Assess Internal Control Adequacy                        | M                 |               |                   |                |                |                  |
| M3 Obtain Independent Assurance                            | M                 |               |                   |                |                |                  |
| M4 Provide for Independent Audit                           | M                 |               |                   |                |                |                  |

Figure 5.5

# 6 Risk Management

|  |    |
|--|----|
| <b>6.1</b> What are the risks? .....   | 28 |
| <b>6.2</b> What is the best approach for risk analysis and management? .....             | 29 |
| <b>6.3</b> How can standards and best practices be used – is certification useful? ..... | 30 |
| <b>6.4</b> What are the roles of management, staff and auditors? .....                   | 31 |
| <b>6.5</b> Who needs to be competent? .....  | 31 |
| <b>6.6</b> What competence is required? .....  | 32 |
| <b>6.7</b> How to obtain, develop, retain and verify competence .....                    | 33 |
| <b>6.8</b> When to source competence from outside .....                                  | 35 |
| <b>6.9</b> Key learning points .....   | 35 |

The management of risks is a cornerstone of IT Governance, ensuring that the strategic objectives of the business are not jeopardised by IT failures. IT related risks are increasingly a Board level issue as the impact on the business of an IT failure, be it an operational crash, security breach or a failed project, can have devastating consequences. However, managing IT risks and exercising proper governance is a challenging experience for business managers faced with technical complexity, a dependence on an increasing number of service providers, and limited reliable risk monitoring information. As a consequence, management are often concerned whether risks are being cost effectively addressed, and they need assurance that risks are under control.

The universal need to demonstrate good enterprise governance to shareholders and customers is the driver for increased risk management activities in large organisations. Enterprise risk comes in many varieties, not only financial risk. Regulators are specifically concerned about operational and systemic risk, within which technology risk and information security issues are prominent. The Bank for International Settlements, for example, supports that view because all major past risk issues studied in the financial industry were caused by breakdowns in internal control, oversight and IT. Infrastructure protection initiatives in the US and the UK point to the utter dependence of all enterprises on IT infrastructures and the vulnerability to new technology risks. The first recommendation these initiatives make is for risk awareness of senior corporate officers.

▼ Therefore, the board should manage enterprise risk by<sup>4</sup>:

- ▶ *Ascertaining that there is transparency about the significant risks to the enterprise and clarifying the risk-taking or risk-avoidance policies of the enterprise.*
- ▶ *Being aware that the final responsibility for risk management rests with the board so, when delegating to executive management, making sure the constraints of that delegation are communicated and clearly understood.*
- ▶ *Being conscious that the system of internal control put in place to manage risks often has the capacity to generate cost-efficiency.*
- ▶ *Considering that a transparent and proactive risk management approach can create competitive advantage that can be exploited.*
- ▶ *Insisting that risk management is embedded in the operation of the enterprise, responds quickly to changing risks and reports immediately to appropriate levels of management, supported by agreed principles of escalation (what to report, when, where and how).*

We must be conscious though that risk taking is an essential element of business today. Success will come to those organisations that identify and manage risks most effectively. Risk is as much about failing to grasp an opportunity as it is about doing something badly or incorrectly.

## ▶▶ 6.1 What are the risks?

To enable effective Governance, IT risks should always be expressed in the business context rather than in the technical language favoured by IT risk experts. The following generic structure for expressing IT risks in any organisation is suggested:

**Business specific risk** (e.g. Operational risk of orders not being received)

**Generic common IT risk** (e.g. IT availability risk)

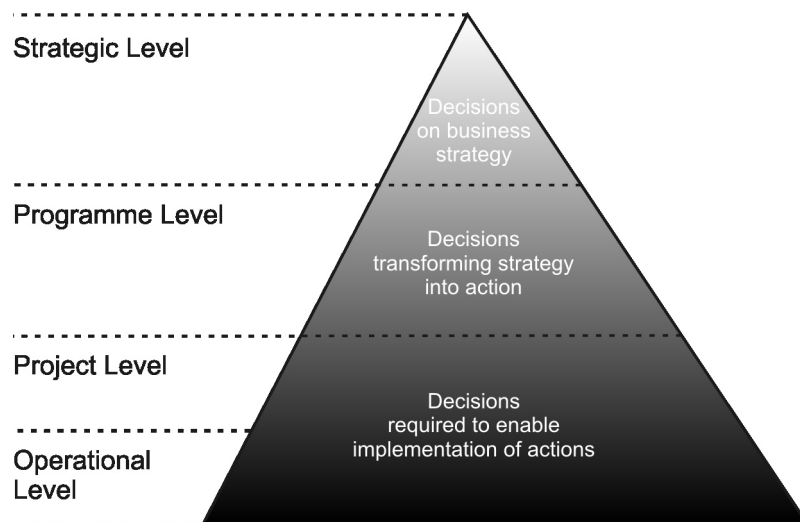
**Specific IT risk** (e.g. Denial of service attack on Internet customer order system)

Business risks are affected by the business environment (management style, culture, risk appetite, industry sector factors such as competition, reputation etc., national and international regulations). IT risks can be similarly affected.

▼ There is no single accepted set of generic IT risk definitions, but these headings can be used as a guide (Taken from a global study by the Economist Intelligence Unit in 2002):

- ▶ *Investment or expense risk*
- ▶ *Access or security risk*
- ▶ *Integrity risk*
- ▶ *Relevance risk*
- ▶ *Availability risk*
- ▶ *Infrastructure risk*
- ▶ *Project ownership risk*

The OGC's M\_o\_R framework visualises four levels of risks in a pyramid with appropriate escalation to higher levels for significant risks (Figure 6.1).



**Figure 6.1**

For IT to be effectively governed, top management must be able to recognise IT risks and ensure that significant risks are managed. Significance of an IT risk is based on the combination of impact (what effect the risk would have on the organisation if it occurred) and likelihood (the probability of the risk occurring). Because of the complexity and fast changing nature of IT, education and awareness is essential to ensure risks are recognised – not just at the top management level but at all levels throughout the organisation. It is increasingly common for a dedicated risk management function to be established or for external advice to be obtained on a regular basis to ensure that risks are monitored and the rest of the organisation is kept informed. Maintenance of a risk catalogue or risk register can be helpful to ensure that a thorough review of all IT related risks takes place on a periodic basis and for providing assurance to management that risks are being addressed.

## 6.2 What is the best approach for risk analysis and management?

▼ Risk management consists of two main elements:

- ▶ *Risk Analysis*
- ▶ *Risk Management*

▼ Having defined risk appetite and identified risk exposure, strategies for managing risk can be set and responsibilities clarified. Dependent on the type of risk and its significance to the business, management and the board may choose to:

- ▶ Mitigate, by implementing controls
- ▶ Transfer, by sharing risk
- ▶ Accept, by formally acknowledging that the risk exists and monitoring it

The following framework for managing risk in Figure 6.2 is suggested by the OGC (OGC Risk Management Framework [www.ogc.gov.uk](http://www.ogc.gov.uk)).

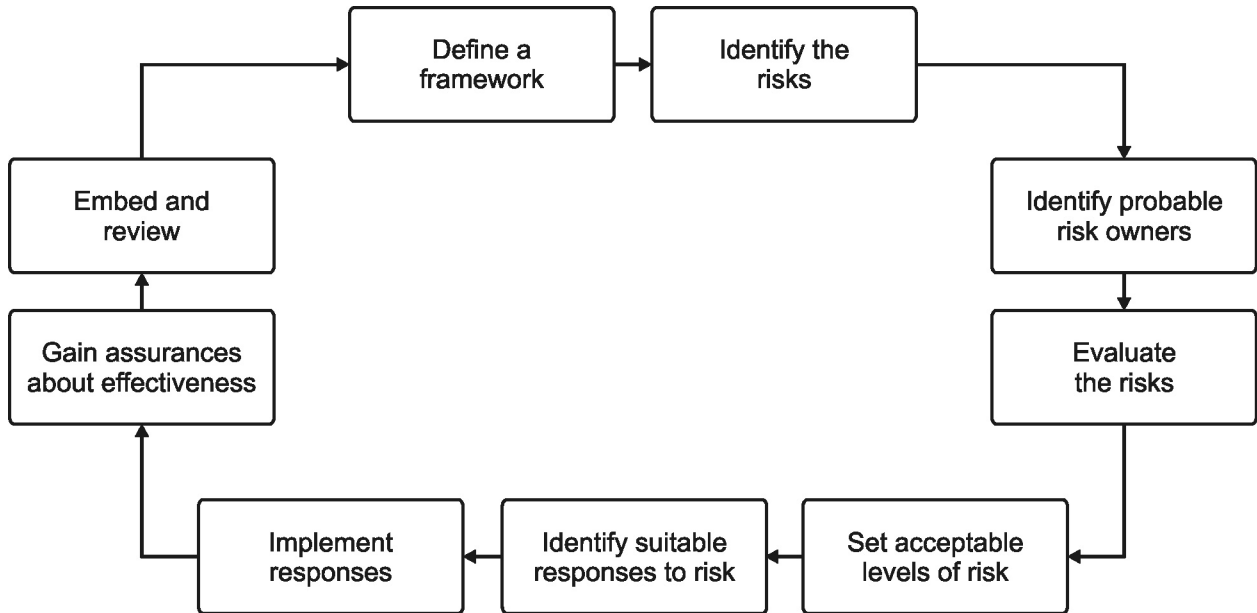


Figure 6.2

The analysis of IT risks can be very time-consuming and there is a danger of “analysis paralysis”. To ensure effective and timely identification of risk, management workshops involving knowledgeable and interested representatives from the business, IT, audit and, if necessary external advisors, can help to rapidly pinpoint key risks requiring attention, as well as prioritising risk management actions. It is also important to identify the benefits of managing a risk as they can help to justify the business case for taking action. Benefits can include financial savings such as reduced losses and improved efficiencies as well as intangibles such as improved reputation and image.

Risk management checklists are useful for raising awareness and reminding everyone of typical risk related issues. Regular self-assessments, internal audits and external audits/assessments are also helpful to ensure objectivity, and a thorough approach. For technical areas such as Internet security, the advice of an expert is likely to be required to ensure any technical vulnerabilities have been identified.

### 6.3 Using standards and best practices – is certification useful?

There is no doubt that effective management policies and procedures help to ensure that risks are identified and managed as a routine part of everyday activities. Adoption of standards and best practices will help to enable quick implementation of good procedures and avoid lengthy delays re-inventing wheels and agreeing approaches.

The best practices adopted have, however, to be consistent with the risk management framework and be appropriate for the organisation, and be integrated with other methods and practices that are being used. Standards and best practices are not a panacea and their effectiveness will depend on how they have been actually implemented and kept up to date. They are most useful when applied as a set of principles and as a starting point for tailoring specific procedures. To avoid practices becoming “shelf-ware”, change enablement is required, so that management and staff understand what to do, how to do it, and why it is important. For risk management to be effective, the use of a common language and a standardised approach oriented towards real business requirements is best – making sure everyone follows the same set of objectives, issues and priorities.

Benchmarking is another very useful way to compare how risk management is being addressed within the organisation in relation to best practice, industry peer groups and other organisations. Conformance to generally accepted standards and practices can be very helpful when managing risks relating to outsourced services and third party suppliers. Certification



against a standard may be important for helping to establish trust with trading partners, or for raising significance within the organisation. However, there is a danger that acquiring a certificate becomes more important as a marketing tool, than operating effective management itself. Certification may also only mean conformance with a baseline and may in itself not be sufficient to address all the risks in the organisation. In the IT environment there is no specific standard relating to risk management, but there are standards and best practices covering specific areas. Of these CobiT, ISO17799, ITIL, ISO9000, PMBOK and Prince2 are the most widely used.

## 6.4 What are the roles of management, staff and auditors?

The ownership of IT risks, and giving direction for managing key risks is a fundamental aspect of IT Governance. An absence of top management responsibility and accountability for risk management can result in serious risks being ignored, potentially misguided actions, and even costly investments being wasted. Ultimately it is the business – the user of IT services – who must own business related risks including those related to the use of IT. They should set the mandate for risk management, provide the resources and funding to support any necessary risk management plan designed to protect their business interests, and monitor whether risks are being managed. In practice, due to the complex and technical nature of IT, the IT service provider will need to provide guidance and work with business management to ensure adequate safeguards are in place. IT management will then have a responsibility to endorse, establish and monitor the agreed risk management framework including key principles and mitigation strategies. IT and user staff have a responsibility to implement the framework, assessing, escalating and delivering mitigating actions.

Auditors can provide initial momentum by highlighting to senior management inadequate risk management practices or specific risks that are not being adequately addressed. Audit should also align audits with key business risks and known areas of weakness, and provide independent assurance to management, make sure that appropriate risk management plans are in place and are being followed in all key areas or provide improvement recommendations.

▼ The OGC make the following suggestions regarding risk ownership:

- ▶ *Allocate responsibility at a senior level for managing key risks*
- ▶ *Ensure that every risk has an owner; there may be separate owners for the actions to mitigate the risks*
- ▶ *Ensure anyone allocated ownership has the authority to take on the responsibility and that they are aware that they are the designated owner*
- ▶ *Adopt a mechanism for reporting issues – ultimately to the individual who has to retain overall responsibility*

## 6.5 Who needs to be competent?

A key characteristic of any successful IT Governance initiative is the establishment of an enterprise-wide approach that clearly sets out roles and responsibilities, emphasising that everyone has a part to play in enabling successful IT outcomes. Implementation of effective IT Governance therefore depends on everyone having adequate and appropriate skills to fulfil their specific role. In most organisations, Investors and Controllers will have a good understanding of governance principles but they usually have a very poor understanding of how to apply these principles in the world of IT. Providers, who are usually IT specialists, conversely understand IT but have a poor appreciation of governance and control principles.

Most IT Governance initiatives begin with the establishment of an IT Governance project team and the appointment of an IT Governance project manager. The team is likely to be made up of people with some existing skills and relevant experiences, sometimes supported by external advisors, but usually even these teams will require training to improve their competence in IT Governance concepts and implementation approaches.

Over time the project team will become the specialists, guiding and mentoring all role players. For IT Governance to be successful and sustainable, skills must be transferred from the specialists to the rest of the organisation.

## 6.6 What competence is required?

Each group of role players will require different sets of skills to support IT Governance effectively (Figures 6.6-6.6.2).

| Investors Role & Responsibilities  | Competence Required   |
|--|---|
| <p><b>Management board (authority to make things happen)</b></p> <ul style="list-style-type: none"> <li>• Give direction backed up with adequate support and sponsorship</li> <li>• Balance requirements with available resources, making available additional resources if required</li> <li>• Insist on and seek measurable benefit realisation</li> <li>• Coordinate overseas/satellite parts of the enterprise to ensure their interests and constraints have been considered</li> <li>• Create organisation and structure to ensure board involvement in the governance process – by forming committees, establishing reporting processes</li> <li>• Monitor performance, monitor risks, correct deviations</li> </ul> <p><b>Business and IT senior managers, business partners and project sponsors:</b></p> <ul style="list-style-type: none"> <li>• Implement organisation and necessary infrastructure</li> <li>• Take ownership of requirements</li> <li>• Champion and collaborate in IT governance activities</li> <li>• Ensure business strategy and objectives are set and communicated and aligned with IT</li> <li>• Assess business risks and impacts</li> <li>• Establish reporting processes meaningful to stakeholders</li> <li>• Communicate any business concerns in a balanced and reasoned way</li> <li>• Provide project champions, creating the seeds of change</li> </ul> <p><b>User representatives</b></p> <ul style="list-style-type: none"> <li>• Take responsibility for Quality Assurance programme (design and output)</li> <li>• Regularly check actual results against original (or changed) goals</li> <li>• Provide service feedback to providers</li> </ul> | <p><b>General executive leadership skills:</b></p> <ul style="list-style-type: none"> <li>- Ability to understand the big picture and how IT plays a part</li> <li>- Ability to think strategically – how can IT make a positive difference to enterprise strategy?</li> <li>- Ability to make strong decisions relating to IT, and be able to direct and challenge IT approaches</li> </ul> <p><b>Ability to challenge:</b></p> <ul style="list-style-type: none"> <li>- Uncover IT related issues</li> <li>- Probe business cases</li> <li>- Assess concerns</li> <li>- Assess performance</li> </ul> <p><b>IT awareness and understanding:</b></p> <ul style="list-style-type: none"> <li>- Ability to demonstrate value of IT to the business, including return on investment</li> <li>- Ability to understand how the business can use IT profitably</li> <li>- Ability to appreciate the impact of IT on the business, from a value perspective but also from a risk perspective</li> <li>- Be able to link the IT and business strategy, and show how IT supports and enables the overall strategic approach</li> </ul> <p><b>Ability to challenge:</b></p> <ul style="list-style-type: none"> <li>- Uncover IT related issues</li> <li>- Assess accuracy of requirements</li> <li>- Assess and prioritise concerns</li> <li>- Assess performance</li> <li>- Assess impacts of risks and poor performance</li> </ul> <p><b>Ability to articulate requirements and monitor delivery:</b></p> <ul style="list-style-type: none"> <li>- Understand how to express IT related requirements, test deliverables and provide constructive feedback</li> </ul> |

Figure 6.6

| Providers Role & Responsibilities  | Competence Required   |
|--|---|
| <p><b>IT management (internal and external), with support from business management</b></p> <ul style="list-style-type: none"> <li>• Take ownership and set direction of IT Governance activities</li> <li>• Build and achieve a pilot business case</li> </ul> <p><b>IT management</b></p> <ul style="list-style-type: none"> <li>• Set IT objectives</li> <li>• Define IT governance and control framework</li> <li>• Identify critical IT processes</li> <li>• Assess risks, identify concerns</li> <li>• Assess IT capability, identify gaps</li> <li>• Initiate a continuous improvement programme</li> <li>• Develop business cases for improvements</li> <li>• Design and implement solutions</li> <li>• Commit skilled resources</li> <li>• Establish performance measurement system</li> <li>• Report to senior management</li> <li>• Respond to QA feedback from customers</li> </ul> | <p><b>Ability to manage overall IT activities:</b></p> <ul style="list-style-type: none"> <li>- Ability to communicate well in business language</li> <li>- Influencing skills – particularly, able to influence the Investors</li> <li>- Knowledge of the IT organisation and the wider business organisation</li> <li>- Awareness of overall business and IT strategy</li> <li>- Ability to take a high level view and understand the rationales</li> <li>- Aggregate assessment – be able to appreciate the whole IT picture, identify and prioritise key issues and actions</li> <li>- Ability to justify improvement actions</li> <li>- Understand the principles of regulation</li> </ul> <p><b>Supplier management skills:</b></p> <ul style="list-style-type: none"> <li>- Contract and commercial management</li> <li>- Risk management</li> <li>- Stakeholder management – who should be involved and why</li> <li>- Portfolio management</li> <li>- Budget management</li> </ul> |

|  |  |
|--|--|
| <p><b>Suppliers/business partners</b></p> <ul style="list-style-type: none"> <li>Integrate any own existing or planned governance practices with customer</li> <li>Support and contribute to customer's governance approach</li> <li>Agree service definitions, incentives, measures and contracts/agreements</li> </ul> <p><b>Training and Development</b></p> <ul style="list-style-type: none"> <li>Ensure adequate education and communication</li> </ul> <p><b>HR function</b></p> <ul style="list-style-type: none"> <li>Incorporate governance principles into induction and performance measurement process</li> </ul> <p><b>Core team</b></p> <ul style="list-style-type: none"> <li>Define plan and deliverables</li> <li>Organise team and roles (architects, senior responsible officer, facilitator, project manager, process owners)</li> <li>Undertake core tasks</li> <li>Report progress to plan</li> </ul> | <p><b>People related IT Governance skills:</b></p> <ul style="list-style-type: none"> <li>Understanding of roles</li> <li>Understanding of competencies required</li> <li>Understanding of sources of expertise</li> </ul> <p><b>Delivery management skills:</b></p> <ul style="list-style-type: none"> <li>Familiarity with best practices</li> <li>Understanding of IT processes, how they should be controlled, and how to monitor performance</li> <li>Knowledge of corporate standards and policies affecting IT</li> <li>Ability to provide cost estimates</li> <li>Engagement and project management</li> </ul> |
|--|--|

Figure 6.6.1

| Controllers Role & Responsibilities   | Competence Required  |
|---|--|
| <p><b>Internal and external audit</b></p> <ul style="list-style-type: none"> <li>Scope audits in coordination with governance strategy</li> <li>Provide assurance on the control over IT</li> <li>Provide assurance on the control over the IT performance management system</li> </ul> <p><b>Risk management</b></p> <ul style="list-style-type: none"> <li>Ensure that new risks are identified in a timely manner, provide advice</li> </ul> <p><b>Compliance officers</b></p> <ul style="list-style-type: none"> <li>Ensure that IT complies with policy, laws and regulations</li> </ul> <p><b>Finance</b></p> <ul style="list-style-type: none"> <li>Advise on and monitor IT costs and benefits</li> <li>Provide support for management information reporting</li> <li>Incorporate governance requirements into purchasing/contract process</li> </ul> | <p><b>How to apply good Governance practices effectively in IT:</b></p> <ul style="list-style-type: none"> <li>Understand the business environment and its impact on IT</li> <li>Awareness of the business impact, the need for and justification of IT control</li> <li>Ability to be practical and pragmatic</li> <li>Ability to communicate and explain the context of need for control, regulations etc. and the benefits of taking action</li> <li>Analysis ability – root cause determination</li> <li>Able to put theory into practice, be knowledgeable of real world examples</li> <li>Objectivity and independence</li> <li>Coaching, mentoring and skills transfer competence so that others learn control theory</li> <li>Negotiating skills to persuade others</li> </ul> |

Figure 6.6.2

## 6.7 How to obtain, develop, retain and verify competence

### Recruitment

▼ When considering who to place in IT Governance lead positions, especially when creating an initial project team, staff in a number of existing positions may be excellent candidates. The IMPACT IT Governance SIG members have found that the following roles often provide people who would be effective in IT Governance roles.

- ▶ *Auditors*
- ▶ *Project Managers*
- ▶ *Risk Managers*
- ▶ *Business Analysts*
- ▶ *Infrastructure Management*
- ▶ *Procurement/Contract Management*
- ▶ *IS Strategy – alignment with the business*
- ▶ *Quality Management*
- ▶ *Business Relationship Management*
- ▶ *Programme Managers*

However, there is a need for breadth of business and IT knowledge rather than too narrow a specialisation.

## Developing Skills

Demonstrating commitment by senior management for the importance of IT Governance and the value of being competent, removing cultural barriers and improving communications are all critical success factors for improving competence. Suggested techniques for improving skills by each group of role players are shown below:

### ▼ Investors

- ▶ *Obtain external experiences to help position and challenge internal activities*
- ▶ *Obtain "360 degree feedback"*
- ▶ *Consider appointing Executive mentoring advisors*
- ▶ *Obtain and read Executive briefings*
- ▶ *Seek non-executive challenges to the Board*
- ▶ *Consider external Executive IT awareness courses*
- ▶ *Foster cultural change activities*
- ▶ *Foster collaborative working and co-location*
- ▶ *Enable job exchanges to improve awareness*

### ▼ Providers

- ▶ *Formalise documentation of governance, standards and best practices*
- ▶ *When training, focus on specialised and relevant areas*
- ▶ *Organise internal events to raise awareness*
- ▶ *Rotate involvement in governance meetings to improve understanding*
- ▶ *Use the results of assessments and maturity modelling to raise awareness of governance issues, gaps in capability, and impact on the business of IT weaknesses*
- ▶ *Ensure management and control of IT is taken seriously*
- ▶ *Manage the transfer of skills from the specialists to the organisation*

The sequence of events should be:

1. *Training*
2. *Establish an environment which fosters governance*
3. *Roll out the processes and skills*
4. *Measure compliance with standards and reinforce*

### ▼ Controllers

- ▶ *Skills development is often more about learning on the job than about training courses*
- ▶ *Understand the business, how IT affects the business, the IT related business risks, and why IT needs to be controlled*
- ▶ *Focus on Professional training in IT Governance and consider certification in relevant skills*
- ▶ *Maintain continuing professional development*
- ▶ *Consider `soft` skills training to improve communication and influencing skills*

## Retention of Skills

▼ The most effective way to retain IT Governance skills is by establishing standards and practices within the organisation rather than only within individuals. This reduces reliance on key individuals and ensures sustainable processes are put into place. In addition:

- ▶ *At all levels there will be a need to refresh skills continually because of the changing nature of IT*
- ▶ *Skills transfer should always be encouraged, especially from experts to operational staff*
- ▶ *Providers must be valued for their governance skills and encouraged to invest in them. This is especially true of external service providers.*
- ▶ *Induction training is required for new joiners, especially those holding key positions in controller functions.*

If there is institutionalised, sustained implementation of IT governance then the environment will support continual skills growth.

### Verifying Skills

▼ The best way to verify competence is to include governance skills in the appraisal process. This should be based on performance on the job:

- ▶ *Clear job objectives and role definition for IT Governance*
- ▶ *IT Governance competencies required for role*
- ▶ *Review of competency performance*

In addition, surveys can be carried out periodically to measure the level of awareness in key competencies. This technique can also be a valuable awareness raising and reinforcing technique. Another approach to verifying competence is to measure the maturity of IT Processes, focusing on competency aspects. The chart below shows generically how this could be done based on guidance from CobiT's Management Guidelines (Figure 6.7).

| <b>Generic Maturity Model for Governance Competence (CobIT)</b> | <b>Understanding &amp; Awareness</b>     | <b>Training &amp; Communication</b>   | <b>Expertise</b>  |
|---|--|---|---|
| 1 Initial/Ad Hoc  | Recognition                              | Sporadic communication on issues  |   |
| 2 Repeatable but Intuitive                                      | Awareness                                | Communication on the overall issues and needs   |   |
| 3 Defined Process   | Understanding of need to act             | Informal training supports individual initiatives   | IT Governance expertise exists within the Process owner and team                        |
| 4 Managed & Measurable  | Understand full requirements             | Formal training supports a managed programme  | IT Governance expertise is monitored and measured outside the Process                   |
| 5 Optimised   | Advanced, forward-looking, understanding | Training and communications support external best practices and use leading edge concepts | Use of external experts and industry leaders for guidance, comparison to best practices |

Figure 6.7

## 6.8 When to source competence from outside

▼ Acquiring IT Governance competence from outside the organisation will be driven by two different objectives:

- ▶ *When it is more cost-effective to outsource skills that are not available in-house*
- ▶ *When outside input of expertise is beneficial in its own right*

However, if implementation of IT Governance is to be successful and sustainable, competence will have to be developed within the organisation, since management of IT must be owned within the organisation. In many organisations where all or significant parts of the IT service have been outsourced, responsibility and competence for controlling use of these services should still be retained internally. It is essential to retain sufficient skills internally to be able to sustain the business – and to understand and manage what is being outsourced.

## 6.9 Key learning points

▼ The following list of key points have been identified by the IMPACT IT Governance SIG and should be considered when developing IT Governance skills:

- ▶ *Skills optimisation*
- ▶ *Governance skills are normally found at the top level, but are typically not understood in the context of IT*
- ▶ *The appointment of an IT Governance manager and team should not be permanent because governance practice should become business as usual*

- ▶ *People must understand why governance is important*
- ▶ *Governance skills need to be transferred from the specialists to the organisation as a whole*
- ▶ *The best approach to training is learning by doing and being part of the process*

The sequence of events should be:

- 1.** *Specialised training*
- 2.** *Establish an environment which fosters governance*
- 3.** *Roll out the processes and skills*
- 4.** *Measure compliance with standards and re-enforce*

# 7 Supplier Governance

|  |    |
|--|----|
| <b>7.1</b> Why is Supplier Governance important? .....         | 37 |
| <b>7.2</b> The customer's role .....                           | 38 |
| <b>7.3</b> How best to select a supplier .....                 | 40 |
| <b>7.4</b> The customer/supplier relationship .....            | 40 |
| <b>7.5</b> Service management techniques and SLAs .....        | 41 |
| <b>7.6</b> The supplier/outsourcing governance lifecycle ..... | 42 |

Every organisation relies on numerous suppliers to support their business and IT strategy. It is not unusual for external organisations to provide critical IT infrastructure (such as telecommunications networks, hosted data centres, and software applications) used by critical business processes, and increasingly the trend is to outsource significant parts of the internal IT function.

Effective governance of IT suppliers is therefore a key component of IT Governance, to make sure that risks are managed and value is delivered from the investment in supplier products and services. Most organisations are highly dependent on a limited number of key suppliers, and so governance should be focused on those relationships with the greatest risk and investment. For supplier governance to be effective the role of the customer is crucial. The customer should take ownership of the whole transaction from defining requirements and selection all the way through to engagement, operation and termination. Even when the bulk of IT is outsourced, several key functions should be retained because they supply continuity for clients of IT, provide for the oversight of the outsourcer, are highly specific to the way the business operates, and are strategic to the organisation. To some extent, the mix will vary with the reason(s) for outsourcing and which functions have been outsourced. However, all organisations will need to retain some expertise in strategic functions, such as project oversight, architecture, planning, vendor management, and security.

▼ One of the best ways to establish effective supplier governance is to focus on the relationship

- ▶ *The correct form of the relationship (commodity provision, 'market relationship' allows clearly definable boundaries between client and supplier, while the 'partnership' end of the scale requires an ongoing and close cooperation)*
- ▶ *How both parties engage with each other*
- ▶ *Commitment by both parties at a senior level*
- ▶ *Responsibility and accountability by senior decision makers on both sides*
- ▶ *Specification of governance responsibilities in a "governance schedule" within the contract*

Try to create a win/win partnership so that both parties are motivated for success – beating down the supplier is generally seen as poor practice, while cooperation, considered openness and mutuality of benefit defines the basis for better working relationships.

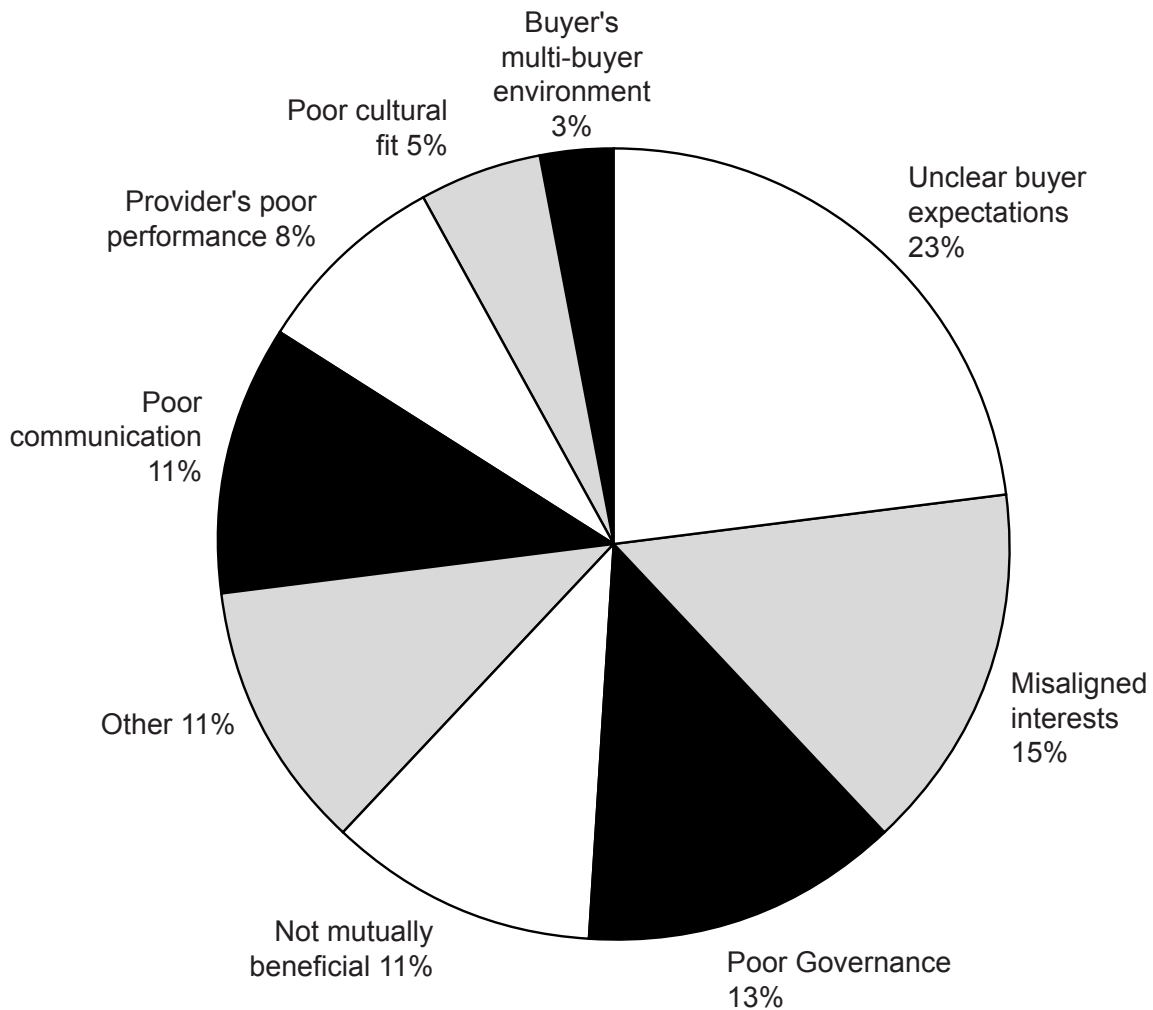
Underpinning the customer/supplier relationship should be formal service level agreements which define **objectives and measures in customer relevant terms**, managed according to service management best practices such as ITIL.

## 7.1 Why is Supplier Governance important?

"Because organisations are relying more and more on IT, management needs to be more aware of critical IT risks and whether they are being managed. Furthermore, if there is a lack of clarity and transparency when taking significant IT decisions, this can lead to reluctance to take risks and a failure to seize technology opportunities. There is a realisation that because IT is complex and has its own fast changing and unique conditions, the need to apply sound management disciplines and controls is even greater." (IT Governance – The Business Case)

Most organisations are highly dependent on a limited number of key suppliers, and so governance should to be focused on those relationships with the greatest risk and investment. The outsourcing of a function or service is likely to be a major

strategic decision which should be governed carefully. Outsourcing is also a huge global commercial business opportunity for the service providers who will compete fiercely for market share. In such a complex technical and commercial situation, proper governance is crucial to help avoid potential service failures and large financial losses.



**Figure 7.1: Causes of outsourcing failures – source Outsourcing Center 2004**

## 7.2 The customer's role

For supplier governance to be effective, the role of the customer is crucial. The customer should take ownership of the whole transaction from defining requirements and selection all the way through to engagement, operation and termination. It is essential that what is outsourced by the customer is NOT its core competency as this is what defines what the organisation is, how customers perceive it and how it retains its position in the marketplace. Only under a limited set of circumstances, one example being technology catch-up, should core competencies be outsourced. The supplier is of course also a stakeholder and will want to ensure the relationship is properly managed, and that the financial and operational requirements are acceptable. It will be in the customer's interest to balance the supplier's needs with his own in order to arrive at a solution that provides reasonable incentives for the supplier while properly meeting the customer's needs.

- ▼ If the relationship is critical in support of the customer's business strategy (which will be the case if significant outsourcing is planned, or if critical infrastructure needs to be supported), then the customer's role in ensuring effective governance will be particularly important and should address:



- ▶ *Discipline over managing the transaction and transparency of the results*
- ▶ *Independence from the supplier*
- ▶ *Accountability and responsibility for key decisions*
- ▶ *Increasing stakeholder value (both internal and for the supplier)*
- ▶ *Key governance steps at each stage, best defined in a governance schedule in the contract, and in a shared procedure manual where key responsibilities and escalation procedures are defined.*

## How to be an effective customer

### ▼ Organisation

- ▶ *Focus on what's critical*
- ▶ *Have the right capability to manage IT suppliers*
- ▶ *Ensure there are clear roles and responsibilities on the customer's side of the relationship*
- ▶ *Ensure there is an Executive level sponsor who will be responsible and accountable for all significant decisions regarding key suppliers*
- ▶ *Commit long-term*
- ▶ *Establish relationships at multiple levels*
- ▶ *Organise suppliers according to criticality and roles*

### ▼ Technical

- ▶ *Manage technical IT issues to ensure conformance where necessary and compatibility with in-house technical standards*
- ▶ *Ensure all relevant legal and regulatory requirements have been considered*
- ▶ *Standardise and commoditise solutions wherever possible*
- ▶ *Set realistic expectations regarding service delivery*
- ▶ *Take time to understand product and service offerings*
- ▶ *Understand how your own IT assets may be affected by supply of external products or service*
- ▶ *Ensure there is good control of the internal environment affected by the external supply*

### ▼ Project Approach

- ▶ *Take care to manage all staff related issues*
- ▶ *Set up a co-ordination committee of senior customer representatives*
- ▶ *Make sure there is a process for both parties to follow*
- ▶ *Build into the requirements and contract plans for transition/transformation from the current state to an outsourced service*
- ▶ *Approach contracts and relationships in a balanced way ensuring risks have been considered in the context of the value expected from the supplier*
- ▶ *Avoid the danger of mixed messages coming from different parts of the customer organisation*
- ▶ *Make sure there is top-down management commitment to support all key decisions*

## How to monitor and measure

### 1. Identify a limited range of meaningful and measurable key measures e.g.:

- ▶ *Performance*
- ▶ *Financial*
- ▶ *Risks*
- ▶ *Compliance*
- ▶ *Relationship*
- ▶ *Value added*
- ▶ *Delivery*

### 2. Take ownership and define and obtain agreement for all measures

### 3. Supplier senior management should:

- ▶ *Provide data for all measures he is responsible for*
- ▶ *Monitor delivery performance*
- ▶ *Agree remedial action with customer*
- ▶ *Commit remedial actions*

**4.** Customer IT service management should:

- ▶ *Be responsible for monitoring and reporting*
- ▶ *Prioritise and recommend actions*

**5.** Customer should:

- ▶ *Provide customer satisfaction measurement data*
- ▶ *Consider benchmarking to other organisations and other services*

**What functions should be retained by the customer?**

(Reference Forrester Research "Functions to Retain when Outsourcing, July 2004)

Even when the bulk of IT is outsourced, several key functions should be retained because they supply continuity for clients of IT, provide for the oversight of the outsourcer, are highly specific to the way the business operates, and are strategic to the organisation. To some extent, the mix will vary with the reason for outsourcing. However, all organisations will need to retain some expertise in strategic functions.

## **7.3** How best to select a supplier

The following steps are suggested:

- 1.** *Research the markets to identify preferred suppliers*
- 2.** *Consider the size of supplier compared to your organisation and your requirements*
- 3.** *Consider the need to integrate several suppliers*
- 4.** *Do due diligence reviews*
- 5.** *Prepare an effective RFP*
- 6.** *See key people*
- 7.** *Consider pilots and pre-project trials*
- 8.** *Check track record*
- 9.** *Consider impact of any off-shore situations*

## **7.4** The customer/supplier relationship

▼ One of the best ways to establish effective supplier governance is to focus on the relationship:

- ▶ *How both parties engage with each other*
- ▶ *Commitment by both parties at a senior level*
- ▶ *Responsibility and accountability by senior decision makers on both sides*
- ▶ *Specification of governance responsibilities in a "governance schedule" within the contract*

Make sure each party understands its role. Figure 7.4 summarises how IMPACT SIG members believe each group of stakeholders should focus in the customer/supplier relationship.

| Party                     | Stakeholder | Focus                                       |
|---------------------------|-------------|---|
| Customer                  | Investors   | Define outsourcing and procurement strategy |
|                           |             | Define supplier governance framework        |
|                           |             | Provide supplier with strategic direction   |
|                           |             | Approve contracts and any changes           |
|                           |             | Consider future business requirements       |
|                           |             | Define business objectives                  |
|                           |             | Evaluate performance                        |
|                           | Providers   | Specify architecture                        |
|                           |             | Define business requirements                |
|                           |             | Manage relationship                         |
|                           |             | Manage projects                             |
|                           |             | Monitor service                             |
|                           | Controllers | Verify financial ROI                        |
|                           |             | Manage contract                             |
|                           |             | Assess and monitor risk                     |
|                           |             | Ensure legal/regulatory compliance          |
|                           |             | Perform financial analysis                  |
|                           |             | Ensure supplier service audit               |
| Establish security policy |             |   |
| Supplier                  | Investors   | Define business objectives                  |
|                           |             | Protect supplier and customer investments   |
|                           |             | Commit resources for delivery               |
|                           |             | Define service strategy                     |
|                           |             | Define governance framework                 |
|                           | Providers   | Define services                             |
|                           |             | Define service levels                       |
|                           |             | Monitor service quality                     |
|                           | Controllers | Measure financial performance               |
|                           |             | Monitor risk management                     |
|                           |             | Manage contracts                            |
|                           |             |   |

Figure 7.4

## 7.5 Service management techniques and SLAs

Underpinning the customer/supplier relationship should be formal service level agreements, managed according to service management best practices. ITIL is recommended as the best source of guidance in this area, and the IMPACT SIG members recommended the following techniques:

- ▶ Use a supplier governance framework to drive service management practices (figure 7.5).
- ▶ Create a service management board to oversee service delivery
- ▶ Create a service code of practice “how to engage”
- ▶ Adopt standard processes for managing the services
- ▶ Develop a common language and common understanding of service objectives
- ▶ Ensure there is a clear definition of service scope
- ▶ Define the scope of the retained IT function
- ▶ Maintain the contract as a result of service changes
- ▶ Create a policy and procedure manual for both parties to follow
- ▶ Where possible define a service credit regime – this describes how ‘overs and unders’ on the service provision are handled without recourse to hard, fixed penalties

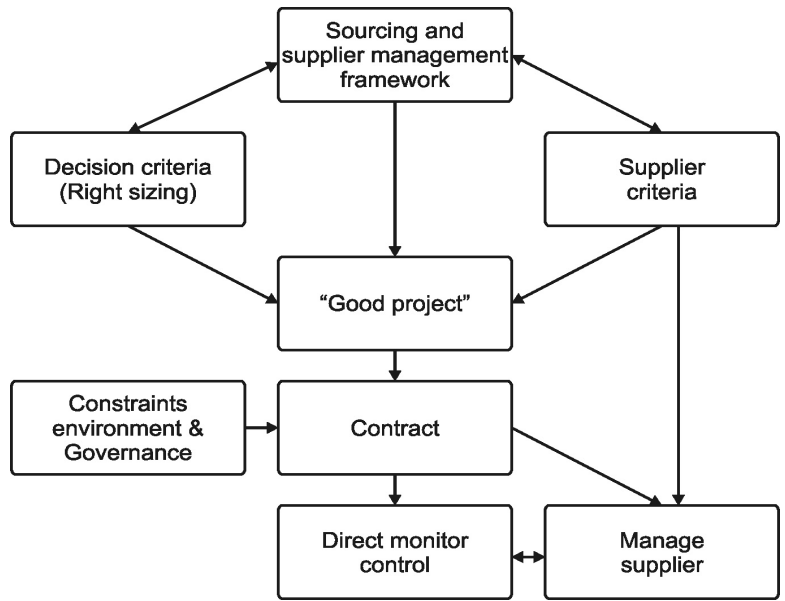
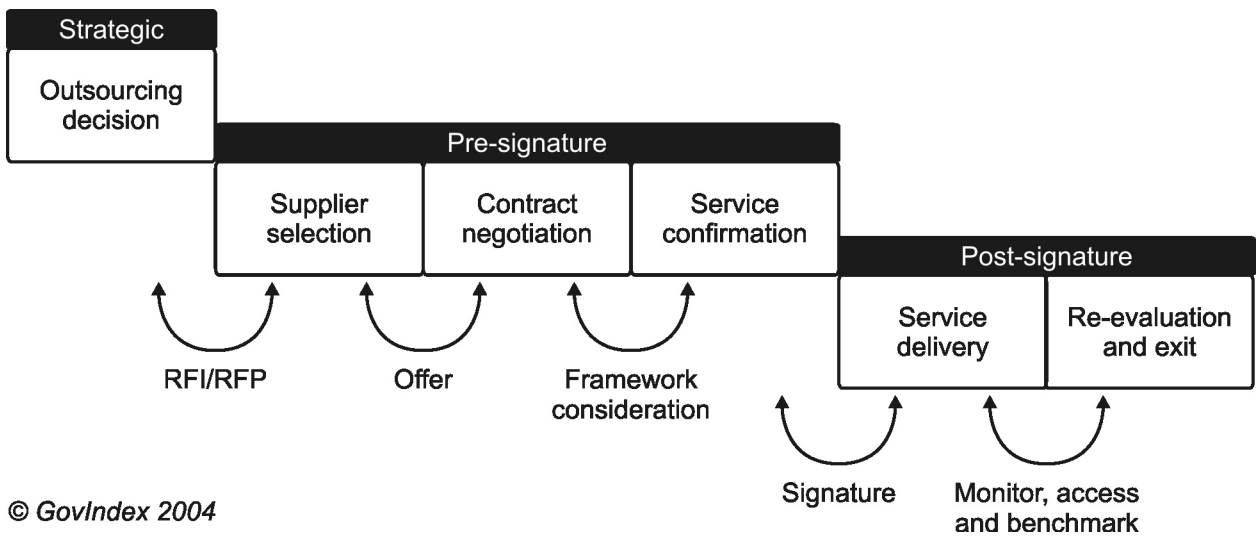


Figure 7.5

## 7.6 The supplier/outsourcing governance lifecycle

The outsourcing lifecycle is useful in determining major points for governance throughout the contract, but more importantly ensures a common understanding of the major processes (Figure 7.6).



© GovIndex 2004

Figure 7.6

# 8 IT & Audit Working Together & Using CobiT

|  |    |
|--|----|
| <b>8.1</b> Introduction to CobiT .....                                 | 43 |
| <b>8.2</b> How is CobiT being used? .....                              | 44 |
| <b>8.3</b> What are the roles of IT and Audit for IT Governance? ..... | 45 |
| <b>8.4</b> How can IT and internal audit work better together? .....   | 45 |

**T**he growing interest in IT Governance and increasing pressure to deal with regulatory compliance (e.g. Sarbanes Oxley), and a continuing focus on security, has made IT management much more involved in risk management and control activities. There is therefore a need for IT management to work more closely with IT auditors.

For many years there have been barriers between auditors (both internal and external) and auditees (IT functions and business units). This can be due to communication gaps, hidden checklists, and a failure to collaborate on control assessment and control improvement. A more effective approach requires better recognition of one another's role and alignment to a mutually accepted and understood control framework, so that everyone is "on the same page".

CobiT is an IT Control and Governance Framework that is increasingly being adopted by organisations around the world as a common reference model for IT Control. CobiT has historically been mostly used by IT auditors but the trend now is for IT management to use CobiT as a basis for IT process ownership, a reference model for good controls and as a way to integrate other best practices under one "umbrella" aligned to business needs. More advanced users make use of CobiT's maturity modelling and metrics to measure performance and drive improvement initiatives.

As a consequence, many IT functions and IT service providers are adopting CobiT as part of their operational control framework.

## 8.1 Introduction to CobiT

Business orientation is the main theme of CobiT. It is designed to be employed not only by users and auditors, but also, and more importantly, as comprehensive guidance for management and business process owners. Increasingly, business practice involves the full empowerment of business process owners so they have total responsibility for all aspects of the business process. In particular, this includes providing adequate controls. The CobiT Framework provides a tool for the business process owner that facilitates the discharge of this responsibility. The Framework starts from a simple and pragmatic premise:

**In order to provide the information that the organisation needs to achieve its objectives, IT resources need to be managed by a set of naturally grouped processes.**

The Framework continues with a set of 34 high-level Control Objectives, one for each of the IT processes, grouped into four domains: planning and organisation, acquisition and implementation, delivery and support, and monitoring. This structure covers all aspects of information and the technology that supports it. By addressing these 34 high-level control objectives, the business process owner can ensure that an adequate control system is provided for the IT environment.

IT Governance guidance is also provided in the CobiT framework. IT Governance provides the structure that links IT processes, IT resources and information to enterprise strategies and objectives. IT Governance integrates optimal ways of planning and organising, acquiring and implementing, delivering and supporting, and monitoring IT performance. IT Governance enables the enterprise to take full advantage of its information, thereby maximising benefits, capitalising on opportunities and gaining competitive advantage.

In addition, corresponding to each of the 34 high-level control objectives is an Audit Guideline to enable the review of IT processes against CobiT's 318 recommended detailed control objectives to provide management assurance and/or advice for improvement.

The Management Guidelines further enhances and enables enterprise management to deal more effectively with the needs and requirements of IT governance. The guidelines are action oriented and generic and provide management direction for getting the enterprise's information and related processes under control, for monitoring achievement of organisational goals, for monitoring performance within each IT process and for benchmarking organisational achievement. CobiT's Management Guidelines are generic and action oriented for the purpose of answering the following types of management questions: How far should we go, and is the cost justified by the benefit? What are the indicators of good performance? What are the critical success factors? What are the risks of not achieving our objectives? What do others do? How do we measure and compare?" (CobiT Framework 2000, www.itgi.org)

ISACA recognised in the early 1990's that auditors, who had their own checklists for assessing IT controls, were talking a different language to business managers and IT practitioners. In response to this communication gap, CobiT was created as an IT control framework for business managers, IT managers and auditors, based on a generic set of IT processes meaningful to IT people. The best practices in CobiT are a common approach to good IT control – implemented by business and IT managers, and assessed on the same basis by auditors. Over the years CobiT has been developed as an open standard and is now increasingly being adopted as the control model for implementing and demonstrating effective IT Governance.

▼ Today, as every organisation tries to deliver value from IT while managing an increasingly complex range of IT related risks, the effective use of best practices can help to avoid re-inventing wheels, optimise use of scarce IT resources, and reduce the occurrence of major IT risks such as:

- ▶ *Project failures*
- ▶ *Wasted investments*
- ▶ *Security breaches*
- ▶ *System crashes*
- ▶ *Failures by service providers to understand and meet customer requirements*

Due to its high level and broad coverage, and because it has been based on many existing practices, CobiT is often referred to as the "integrator", bringing disparate practices under one "umbrella" and just as importantly, helping to link these various IT practices to business requirements.

## 8.2 How is CobiT being used?

Although the long-term aim of CobiT was to be a common framework used by management and auditors, it began as an Audit reference. This was largely due to its origins within ISACA and its early adoption by ISACA members who are mostly from the computer audit profession. Over the years its usage has widened out into the IT community and nowadays this is the fastest growing user segment. Whereas auditors have been using CobiT mostly as a controls checklist, IT managers see it more as a "best practice" framework for performance measurement and improvement planning. With increasing regulatory requirements such as Sarbanes-Oxley in the US, both auditors and IT managers are adopting CobiT as the compliance framework for IT controls. The CobiT IT Process model has helped convey a view of IT understandable to business management, auditors and IT, and at the same time provide a basis for IT functions to organise themselves into a process structure with accountable process owners.

The maturity modelling and metrics concepts within CobiT are probably the most popular for IT managers, providing an easy and powerful technique for positioning IT control gaps in the context of business requirements. The profiles and scorecards that results are a powerful tool for communicating with senior management and demonstrating the reality of current IT capability in relation to what the business might have expected.

As organisations have adopted the CobiT approach, it has driven the professional Audit firms to follow similar approaches, and to integrate CobiT into their internal proprietary methodologies. This has helped to break down communication barriers and improve the mutual understanding of IT controls. There is also a trend among service providers to use CobiT and other best practices to improve their market image and quality of service. This is also helping to improve communication of control issues and make it easier to manage and audit IT activities against a commonly accepted basis. Because CobiT is open and independent of any specific vendor all parties can use it freely. It is not a "standard" as such but a "best practice" framework and set of guidance materials to be tailored for each specific situation.

There is currently a great deal of focus on the Sarbanes-Oxley Act in the US, and the reporting requirements that this legislation requires for Company Directors. Many companies are using CobiT as the framework for reporting the status of IT systems and controls, and consequently a massive CobiT-based controls documentation effort is underway. While Sarbanes-Oxley has been very useful for putting IT governance and control on the Board's agenda, there is a danger that the effort will be limited to a documentation exercise to achieve compliance. The real value from any control evaluation, especially when based on CobiT, is the identification of control gaps and the implementation of a sustainable improvement programme. There

is an analogy with the Y2K experience in that Sarbanes-Oxley should not be a one off exercise but an ongoing programme for improving management control and establishing governance.

## 8.3 What are the roles of IT and Audit for IT Governance?

### ▼ Role of IT Audit

- ▶ *IT Governance is a management responsibility, and therefore not the sole responsibility of an Audit function. The Audit function should remain independent, but this can provide an excellent position to influence and recommend change. Independence should not inhibit provision of advice, so long as management take full responsibility and accountability for implementation and operation of controls. Taking responsibility for enabling an IT Governance initiative or for initiating governance projects should not compromise Audit.*
- ▶ *IT Governance requires management commitment and ownership within IT and the business in order to make it happen. Audit can then determine if it is happening, and provide assurance to the board.*
- ▶ *When reviewing Governance, Audit must do more than just identify problems. They need to identify root causes and make constructive recommendations.*
- ▶ *Audit can test controls especially where control is critical and assurance is required. But increasingly there is a trend for IT to “test themselves” by performing self-assessments.*
- ▶ *Audit can play a part in setting standards, and providing control criteria and control benchmarks, particularly in respect of external regulation.*
- ▶ *Given the speed of IT change and the high cost of development projects, it makes sense to involve auditors in projects. To be effective auditors must:*
  - *Be credible and confident to gain the respect of IT*
  - *Not wait until the end of a phase to critique – but give pro-active guidance on what should be done*

### ▼ Role of IT

- ▶ *IT has to be responsible for changing the culture of the IT organisation, for managing the IT processes, and adopting a focus on controls.*
- ▶ *IT professionals often have a poor understanding of what controls are and why they are needed. Education in control principles may be needed, and audit can help with this by working together with IT, and by providing training, workshops and staff secondments.*
- ▶ *A common framework and understanding is needed in order to ensure that IT Management is exercising IT Governance. Using a common framework for control such as CobiT, will help to ensure that everyone is “on the same page”.*
- ▶ *The CIO and Head of Internal Audit should work together to drive change.*
- ▶ *IT should take a lead on governance; audit can “sow the seeds”.*
- ▶ *If IT (as so often) is in ‘fire fighting’ mode it is harder for them to drive governance.*
- ▶ *Executive management may point to historic data as showing no problems- so why should they worry about governance? However, the problems can usually be identified by IT digging into process failures – e.g. project delay and excess cost. IT management have to be confident of their position to draw attention to internal weaknesses.*

## 8.4 How can IT and internal audit work better together?

Increasingly, control self-assessments are being performed by IT functions because it is more efficient than relying on limited IT audit resources, and more likely to motivate corrective action.

### ▼ Typical examples using self-assessments are:

- ▶ *Risk assessments*
- ▶ *Compliance with specific standards (ISO 17799)*
- ▶ *Compliance with regulatory requirements such as Sarbanes-Oxley*
- ▶ *Quality of service assessments*

| IT contribution   | Governance Phase                          | Audit contribution  |
|---|---|---|
| <b>Common approach – culture, charter, communication and language, clear ownership</b>  |   |   |
| <ul style="list-style-type: none"> <li>• Get CIO commitment.</li> <li>• Know your audience when explaining IT Governance, controls adoption and CobiT.</li> <li>• Get ownership from the business side, using business language, RAG charts and scorecards. Demonstrate strengths and weaknesses.</li> <li>• Influence the business and the board about IT management issues (use ITGI Board Briefing) (<a href="http://www.itgi.org">www.itgi.org</a>).</li> <li>• Achieve a balance between regulation and improvement planning. Leverage regulations for positive effect.</li> <li>• Coordinate with service providers who may be a trigger and may be using CobiT.</li> </ul> | <b>Building Awareness &amp; Ownership</b> | <ul style="list-style-type: none"> <li>• Provide thought leadership.</li> <li>• Influence the Board and Audit Committee to take issues seriously and mandate change.</li> <li>• Use objective and independent position to recommend organisational change.</li> <li>• Don't just make general recommendations – point to root causes.</li> <li>• Provide independent view of the risk profile.</li> <li>• Regulations like Sarbanes-Oxley can be an enabler of change – encourage response to be more than just a documentation exercise.</li> <li>• Demonstrate benefits.</li> </ul> |
| <ul style="list-style-type: none"> <li>• Adopt a Framework e.g. CobiT.</li> <li>• Appoint process owners.</li> <li>• Liaise with 3rd parties and service providers.</li> <li>• Integrate existing and other best practices.</li> </ul>  | <b>Framework Approaches</b>               | <ul style="list-style-type: none"> <li>• Provide thought leadership on available techniques.</li> <li>• Perform “open book” audits (no hidden checklists or issues).</li> <li>• Ensure business and IT orientation to audit approach and recommendations.</li> <li>• Share audit information and documentation.</li> </ul>  |
| <ul style="list-style-type: none"> <li>• Perform risk self assessment.</li> <li>• Perform business impact analysis with business units.</li> <li>• Define business requirements for IT Governance together with business units.</li> <li>• Understand impact of regulatory and compliance issues.</li> <li>• Perform a maturity self assessment on critical IT processes.</li> <li>• Understand risk appetite.</li> </ul>   | <b>Focus</b>                              | <ul style="list-style-type: none"> <li>• Ensure scope alignment (audits versus governance).</li> <li>• Identify key risks.</li> <li>• Analyse audit history and use to prioritise.</li> <li>• Share planning approach.</li> <li>• Identify key control weaknesses.</li> <li>• Define regulatory compliance requirements.</li> <li>• Coordinate with external auditors.</li> </ul>   |
| <ul style="list-style-type: none"> <li>• Do internal/external benchmarking.</li> <li>• Internal/external analysis.</li> <li>• Perform controls self-assessments.</li> <li>• Perform detailed self maturity assessments.</li> </ul>  | <b>Assess</b>                             | <ul style="list-style-type: none"> <li>• Provide assurance of IT self –assessments.</li> <li>• Provide positive statements where appropriate.</li> <li>• Provide independent control evaluations for critical areas.</li> </ul>   |
| <ul style="list-style-type: none"> <li>• Produce scorecards and RAG charts for IT performance in business terms.</li> <li>• Provide explanations for deviations, successes and significant trends.</li> </ul>   | <b>Scorecard</b>                          | <ul style="list-style-type: none"> <li>• Review and assure measures.</li> <li>• Provide “Audit scorecards” showing performance against past audit reports.</li> <li>• Provide where appropriate independent scorecards of IT performance.</li> </ul>  |
| <ul style="list-style-type: none"> <li>• Define HOW improvements can be made.</li> <li>• Create business case for changes.</li> <li>• Create implementation action plan.</li> <li>• Provide Project Control and QA.</li> <li>• Facilitate job rotation/seconddees.</li> </ul>   | <b>Improvement</b>                        | <ul style="list-style-type: none"> <li>• Advise on WHAT should be improved.</li> <li>• Provide training in controls.</li> <li>• Provide workshops to improve understanding.</li> <li>• Organise shared events.</li> <li>• Facilitate job rotation/seconddees.</li> </ul>  |

Figure 8.5

▶ IT Process Maturity assessments (e.g. CobiT)

▼ The methods used vary from formal schemes, perhaps based on IIA (Institute of Internal Auditors) or Internal Audit guidance to less formal approaches. All approaches can provide value e.g.:

- ▶ Questionnaires – based on policy (e.g. security) How do you consider you have addressed each objective?
- ▶ Self certification by management e.g. Sarbanes-Oxley
- ▶ Face-to-face interviews and workshops
- ▶ Pre-defined checklists



The effectiveness of a self-assessment depends on the quality, objectivity, skill and experience of the people performing the review. Using an alternative means of checking to supplement the questionnaire can help as can obtaining Internal audit input in an educating/reviewing role.

▼ There are a number of constraints and challenges relating to self-assessments:

- ▶ *Level of maturity*
- ▶ *Number/volume of testing*
- ▶ *Reliance on the results*
  - *Objectivity*
  - *Completeness and Rigour*
- ▶ *Resources – IT is typically overloaded with day to day pressures*
- ▶ *Political issues need to be addressed – how to get management buy-in, and there may be a reticence to identify and quantify risks*
- ▶ *Cultural aspects should be considered – e.g. the need to balance positive messages with weaknesses*
- ▶ *Avoid routine ticking boxes exercises which are much less valuable*

▼ The following are some practical requirements for self-assessments:

- ▶ *Individuals performing assessments recognise accountability*
- ▶ *There will be a need framework/objectives/policy to self assess against (e.g. based on CobiT)*
- ▶ *Well designed questionnaires – keep them simple with no ambiguity, and examples to aid interpretation*
- ▶ *Coaching/training may be needed if using a web-based questionnaire*
- ▶ *Require supporting evidence to be documented*
- ▶ *Training may be needed on risk identification, definition, and quantification*

# 9 Information Security Governance

|                                       |    |
|---------------------------------------|----|
| 9.1 Background                        | 48 |
| 9.2 What is information security?     | 49 |
| 9.3 Where to focus                    | 50 |
| 9.4 Roles and Responsibilities        | 50 |
| 9.5 Action planning and best practice | 52 |

**E**xecutive management has a responsibility to ensure that the organisation provides all users with a secure information systems environment. Sound security is fundamental to achieving this assurance.

Information systems can generate many direct and indirect benefits, and as many direct and indirect risks. These risks have led to a gap between the need to protect systems and the degree of protection applied. Although awareness of these security issues has increased significantly at board levels, most senior business managers are uncertain about actions they should take and rely heavily on technical advisors. Proper governance of security, like any other aspect of IT, requires top management to be more involved in setting direction and overseeing the management of risk. Faced with the fear of unknown risks, and uncertainty regarding the effectiveness of existing controls, top management naturally wonder where to focus attention and set priorities. A risk assessment is usually the best place to start. A complimentary approach is to focus on establishing a security baseline irrespective of the risks – i.e. ensure that all the basic measures are in place.

Managing investments in the implementation and operation of controls is critical, since security can be an expensive and time-consuming task, and experience has shown that large sums of money can be wasted on ineffective or inadequately implemented technical solutions. However, proving security ROI can be difficult since actual reductions in losses or incidents must be shown, and it is sometimes impossible to know if a risk has been prevented.

There is no doubt though, that the easiest way to demonstrate cash return is by showing the cost of incidents and wherever possible this should be done even if the examples are based on assumptions rather than actual figures. Increasingly, the benefits of good security are being recognised by management who understand that security is needed to enable e-business and that a reputation for good security can enhance customer loyalty, sales and ultimately share price. These benefits should be considered when building the business case for security investments. Given that IT security is a specialised topic and there is a shortage of skills, organisations will often seek support from third parties. Information security specialists can play a key role although governance and final decision-making must remain in-house.

## 9.1 Background

“In a global information society, where information travels through cyberspace on a routine basis, the significance of information is widely accepted. In addition, information and the information systems and communications that deliver the information are truly pervasive throughout organisations—from the user’s platform to local and wide area networks to servers to mainframe computers. Accordingly, executive management has a responsibility to ensure that the organisation provides all users with a secure information systems environment. Furthermore, there is a need for organisations to protect themselves against the risks inherent with the use of information systems while simultaneously recognising the benefits that can accrue from having secure information systems. Thus, as dependence on information systems increases, security is universally recognised as a pervasive, critically needed, quality.” (International Federation of Accounts (IFAC) Statement on Managing Security of Information 1998)

Because new technology provides the potential for dramatically enhanced business performance, improved and demonstrated information security can add real value to the organisation by contributing to interaction with trading partners, closer customer relationships, improved competitive advantage and protected reputation. It can also enable new and easier ways to process electronic transactions and generate trust.”<sup>5</sup>

▼ The view of the IMPACT IT Governance SIG is that Information security concerns have increased due to:

5. Information Security Governance: Guidance for Boards of Directors and Executive Management, the IT Governance Institute®.

- ▶ *Technical complexity*
- ▶ *Hackers and virus spreaders*
- ▶ *Increasing ease of use, and the accessibility of IT systems*
- ▶ *Anywhere/anytime access*

Although awareness of these security issues has increased significantly at board levels, most senior business managers are uncertain about actions they should take and rely heavily on technical advisors. Proper governance of security, like any other aspect of IT, requires top management to be more involved in setting direction and overseeing the management of risk.

▼ It is essential therefore for executive management to understand why information security is important and take action to ensure that:

- ▶ *The importance of information security is communicated to all and that a policy exists to underpin activities in a changing environment.*
- ▶ *The ownership and responsibility for information security is accepted by senior management in the business as well as in IT.*
- ▶ *Everyone understands that security will not be satisfied simply by the appointment of a security manager – the security function is there to assist management and security is ultimately the responsibility of everyone.*
- ▶ *Any shortage of skilled resource in this area is addressed, as it may be impossible to retain all the necessary skills and functions in-house.*
- ▶ *Responsibility for any security aspects of corporate compliance is accepted by the Board.*

▼ Management concerns are focused on:

- ▶ *Gaps – what and where are the significant and specific weaknesses in security?*
- ▶ *Are these weaknesses being addressed?*
- ▶ *Are resources and money being wisely invested and are the right controls being implemented in the areas most vulnerable to threat?*

## ▶▶ 9.2 What is information security?

One of the causes of poor information security and ineffective governance of information security is a misunderstanding of what it actually covers and how it should be addressed. The ITGI publication, Information Security Governance: Guidance for Boards of Directors and Executive Management, describes information security as follows:

“Security relates to the protection of valuable assets against loss, misuse, disclosure or damage. In this context, “valuable assets” are the information recorded on, processed by, stored in, shared by, transmitted or retrieved from an electronic medium. The information must be protected against harm from threats leading to different types of vulnerabilities such as loss, inaccessibility, alteration or wrongful disclosure. Threats include errors and omissions, fraud, accidents and intentional damage. The objective of information security is “protecting the interests of those relying on information, and the systems and communications that deliver the information, from harm resulting from failures of availability, confidentiality and integrity.”

|   |   |
|---|---|
| <b>Policy Development</b>                   | The security objective and core principles provide a framework for the first critical step for any organisation – developing a security policy.   |
| <b>Roles &amp; Responsibilities</b>         | For security to be effective, it is imperative that individual roles, responsibilities, and authority are clearly communicated and understood by all.   |
| <b>Design</b>                               | Once a policy has been approved by the governing body of the organisation and related roles and responsibilities assigned, it is necessary to develop a security and control framework that consists of standards, measures, practices, and procedures.   |
| <b>Implementation</b>                       | Once the design of the security standards, measures, practices, and procedures has been approved, the solution should be implemented on a timely basis, and then maintained.  |
| <b>Monitoring</b>                           | Monitoring measures need to be established to detect and ensure correction of security breaches, such that all actual and suspected breaches are promptly identified, investigated, and acted upon, and to ensure ongoing compliance with policy, standards, and minimum acceptable security practices. |
| <b>Awareness, Training, &amp; Education</b> | Awareness of the need to protect information, training in the skills needed to operate information systems securely, and education in security measures and practices are of critical importance for the success of an organisation’s security program.   |

**Figure 9.2**

According to the IFAC guidance, the major activities associated with Information Security management relate to the items in Figure 9.2.

### 9.3 Where to focus

Faced with the fear of unknown risks, and uncertainty regarding the effectiveness of existing controls, top management naturally wonder where to focus attention and set priorities. A risk assessment is usually the best place to start and this should be based on analysis of the likelihood of different threats, vulnerability and impact. Consideration of the impact of security threats should always be the responsibility of business management, who should ultimately sign-off acceptance of the risk management plan. In practice, this is an area where the business needs to be more involved.

It will be helpful if the risk assessment can be converted to a financial value derived from the impact – even if this is only approximate and based on rough estimates or scales – since decisions to improve security will usually be made based on financial parameters.

A complimentary approach is to focus on establishing a security baseline irrespective of the risks – i.e. ensure that all the basic measures are in place. This can be based on standard guidance such as the ISO17799 ([www.iso.org](http://www.iso.org)) standard or freely available guidance such as the CobiT Security Baseline ([www.itgi.org](http://www.itgi.org)). A key element of this approach is to create security within the infrastructure, rather than on a piecemeal basis.

### 9.4 Roles and Responsibilities

“Executive management, information systems security professionals, data owners, process owners, technology providers, users, and information systems auditors all have roles and responsibilities in ensuring the effectiveness of information security. Due diligence must be exercised by all individuals involved in the management, use, design, development, maintenance, operation, or monitoring of information systems.” (International Federation of Accounts (IFAC) Statement on Managing Security of Information, 1998)

“Too often information security has been dealt with as a technology issue only, with little consideration given to enterprise priorities and requirements. Responsibility for governing and managing the improvement of security has consequently been limited to operational and technical managers.

However, for information security to be properly addressed, greater involvement of boards of directors, executive management and business process owners is required. For information security to be properly implemented, skilled resources such as information systems auditors, security professionals and technology providers need to be utilised. All interested parties should be involved in the process.”<sup>6</sup>

#### Specific roles:

A **Forum or Council** should be established to set policy, ensure that consensus is reached on where security investments should be made, and for approving and overseeing execution of the risk management plan. The Forum should share knowledge of IT and risks, be focused on business objectives not technical solutions and include representatives from key business units, IT, internal audit and outsource suppliers. It should report into a governance board (or group IT board).

An **IT Security Manager** should be in place as an advisor to management and the project owner of security action plan. However, care must be taken to avoid implying that security has now been dealt with by hiring such a person (when it is everyone’s responsibility) or that this role relieves top management of their overall governance responsibilities. The role can be part time and is often supported by external advisors. It is often part of a **Risk Management function**.

An **Operational Team** will be needed to maintain and monitor security processes and operate administrative procedures. This is usually a technical function and it is increasingly being outsourced.

The **Audit Function** plays a key independent role in monitoring and assessing the adequacy of security within the organisation.

A useful approach to improving the understanding, awareness and ownership of security within the business is to appoint **Information Security Coordinators**.

It is critical to influence the **Investors, Providers & Controllers** positively so that they understand the objectives and benefits of IT Governance and are able to communicate consistently to each other and within their groups. The table below

summarises how IMPACT SIG members believe each group of stakeholders should focus on their security responsibilities (Figure 9.4).

| Who needs to be involved?   |  |   |
|---|--|---|
| Investors   | Providers  | Controllers   |
| <ul style="list-style-type: none"> <li>The Board</li> <li>IT Council/Management Team</li> <li>Senior business unit managers e.g. key customers of IT services</li> <li>Business Partners</li> <li>External investors/shareholders – as part of corporate governance</li> </ul>  | <ul style="list-style-type: none"> <li>Project and change managers (IT and Business)</li> <li>Programme managers</li> <li>Business managers and users</li> <li>Technical delivery and support teams</li> <li>Key players e.g. Business sponsors, Project champions</li> <li>Relationship managers and internal communications teams</li> <li>Suppliers (especially outsourced service providers)</li> <li>Contract and procurement management</li> <li>Peripheral players/influencers/Policy owners e.g. HR, Facilities Management, Legal</li> </ul> | <ul style="list-style-type: none"> <li>Internal audit and external audit (due diligence)</li> <li>External regulators</li> <li>Corporate governance coordinator</li> <li>Risk managers</li> <li>Compliance – regulatory and internal</li> <li>Finance/Project Managers/IT and business managers – reviewers of benefits/ROI</li> <li>Post investment appraisal/Post project review teams</li> </ul> |
| Key Security Responsibilities   |  |   |
| <ul style="list-style-type: none"> <li>Risk sign-off</li> <li>Own the business case</li> <li>Set policy</li> <li>Define expectations and requirements</li> <li>Ensure legal and regulatory compliance</li> <li>Review performance</li> <li>Monitor delivery</li> <li>Quantify impact of risk</li> <li>Challenge the risk management plan</li> <li>Approve proposals and metrics</li> <li>Prioritise actions and investments</li> <li>Supply necessary resources</li> <li>Set culture and environment</li> </ul> | <ul style="list-style-type: none"> <li>Risk analysis</li> <li>Design and implementation</li> <li>Creation of business cases – cost and solution</li> <li>Security operations</li> <li>Security administration</li> <li>Monitoring security incidents</li> <li>Education and training (both IT and HR)</li> <li>Creation and maintenance of scorecards for performance measurement</li> </ul>   | <ul style="list-style-type: none"> <li>Understand impact of regulations</li> <li>Monitor adequacy and performance of controls (assessments and audits)</li> <li>Test actual performance of controls</li> <li>Monitor performance (execution of improvements)</li> <li>Provide independent assurance to management</li> </ul>  |

**Figure 9.4**

### Third party security providers

▼ Given that IT security is a specialised topic and there is a shortage of skills, organisations will often seek support from third parties.

Information security specialists can play a key advisory role although governance and final decision-making must remain in-house. There is also an opportunity for cost reduction compared with permanent in-house staff. Examples of outsourced security activities include:

- ▶ *Testing (e.g. following patches)*
- ▶ *Vulnerability testing (note: Penetration testing must be performed with care as it may crash the system)*
- ▶ *Incident management*

▼ Special care should be taken when dealing with outsourced suppliers:

- ▶ *Contractors need to be vetted for security purposes*
- ▶ *Suppliers do have a responsibility to manage security within their own activities – make sure this happens*
- ▶ *Although the supplier has to be trusted to carry out checks, the client must ensure that the necessary checks are in place*
- ▶ *Regulations such as Sarbanes-Oxley requires that governance responsibility remains in-house*

## **9.5 Action planning and best practice**

▼ IMPACT SIG members suggest the following action steps be considered:

1. Classify objectives and actions into technical and non-technical areas
2. Ensure that an effective security policy is in place
3. Establish a security baseline
4. Cover key vulnerabilities
5. Communicate management concerns for security to ensure staff awareness
6. Focus on changes – evaluate and test for security exposures
7. Ensure that Board presentations emphasise security as an enabler and not as a disabler

# 10 Legal & Regulatory Aspects of IT Governance

|  |    |
|--|----|
| <b>10.1</b> Legal and regulatory factors affecting IT Governance ..... | 53 |
| <b>10.2</b> Roles and responsibilities .....                           | 54 |
| <b>10.3</b> Best approach to compliance .....                          | 55 |
| <b>10.4</b> What IT has to do .....                                    | 56 |
| <b>10.5</b> Dealing with third parties .....                           | 58 |
| <b>10.6</b> Critical success factors .....                             | 59 |

In recent years there has been a general increase in the number of regulations affecting the use of IT and also the number of situations where legal measures need to be considered. This is due to the need to guard against a wide range of new IT related risks and from a general increase in corporate regulations.

▼ The impact of not taking sufficient care over legal or regulatory requirements can be considerable including:

- ▶ *Loss of reputation*
- ▶ *Inability to trade*
- ▶ *Financial penalties and losses*
- ▶ *Loss of competitive advantage*
- ▶ *Loss of opportunity*

▼ On the other hand the benefit of complying with regulatory requirements and using legal measures to protect commercial interests can be considerable, including:

- ▶ *General improvement in overall control of IT related activities*
- ▶ *Reduced losses and administrative costs*
- ▶ *More efficient and effective negotiation of commercial transactions*
- ▶ *A greater ability and confidence to take risks – because senior management feel more in control*

There are a wide range of laws and regulations, some specific to industry sectors that can have an impact on IT. Every organisation must identify the specific regulations affecting them and respond accordingly, and ensure that the roles and responsibilities for understanding legal and regulatory matters are properly defined for each group of stakeholder so that each group can apply its specific expertise effectively. External advice must be sought whenever the issues are sufficiently risky or complex.

Every organisation relies on a growing number of third parties for support of IT services. From a legal and regulatory perspective this means that there is potentially a complex hierarchy of responsibilities that combine to meet the legal and regulatory needs of the customer. Ultimately it is the customer's responsibility to ensure that all the right controls are in place with any third party that is relied upon for legal and regulatory compliance.

## ▶▶ 10.1 Legal and regulatory factors affecting IT Governance

▼ The recent increase in the number of regulations affecting the use of IT is due to a number of factors, including:

- ▶ *A greater interest by regulators in the operations of all organisations caused by major corporate financial failures and scandals, which is resulting in regulations like the US Sarbanes-Oxley Act forcing Boards of Directors to express opinions about their systems of control.*
- ▶ *Concerns about security and privacy fueled by the overall increase in use of computers and networks and the impact of the Internet.*
- ▶ *Laws to protect personal information and its potential misuse in electronic form.*
- ▶ *A growth in the use of computer systems and networks for criminal activity and terrorism, including viruses, hacking, money laundering and pornography etc.*
- ▶ *A growth in complex contractual relationships for IT services and products (outsourcing, managed services, product licenses etc.).*
- ▶ *The growth in all forms of electronic media and the potential for misuse of valuable information assets, resulting in copyright and intellectual property issues of concern to both vendors and users.*

What might appear to be an initial regulatory burden can become an opportunity to transform to better managed practices if the rules are used positively and applied productively. Corporate regulations like the Sarbanes-Oxley Act can be just a minimalist compliance procedure with no potential benefit to the business or be used as an opportunity to invest in better IT controls. Compliance with IT-related legal and regulatory requirements and the effective use of legal contracts are clearly part of the effective control and oversight of IT activities by senior management and therefore key aspects of IT Governance.

There are a wide range of laws and regulations, some specific to industry sectors, that can have an impact on IT. Every organisation must identify the specific regulations affecting them and respond accordingly.

▼ The IMPACT SIG has identified the following areas that ought to be considered:

- ▶ *Personal data and privacy*
- ▶ *Corporate Governance, financial reporting, stock market requirements*
- ▶ *Money laundering, and other criminal acts*
- ▶ *Intellectual Property, Trademarks and Copyright*
- ▶ *Electronic communication, signatures etc.*
- ▶ *Electronic commerce*
- ▶ *Email monitoring, appropriate use and confidentiality*
- ▶ *Email defamation*
- ▶ *Document and record retention*
- ▶ *IT products and services contracts*
- ▶ *Sector specific regulations e.g. financial, health, pharmaceutical etc.*

## 10.2 Roles and Responsibilities

Dealing with legal and regulatory requirements and knowing how best to use legal contracts can be challenging for IT experts who are not knowledgeable about legal matters, and for business managers who may not appreciate all the legal risks and issues associated with the use of advanced technology.

Organisations should therefore ensure that the roles and responsibilities for understanding legal and regulatory matters are properly defined for each group of stakeholder so that each group can apply its specific expertise effectively. External advice must be sought whenever the issues are sufficiently risky or complex.



| <b>Who needs to be involved?</b>  |  |  |
|---|--|--|
| <b>Investors</b>  | <b>Providers</b>   | <b>Controllers</b>   |
| <ul style="list-style-type: none"> <li>• The Board</li> <li>• IT Council/Management Team</li> <li>• Senior business unit managers e.g. key customers of IT services</li> <li>• Business Partners</li> <li>• External investors/shareholders – as part of corporate governance</li> </ul>  | <ul style="list-style-type: none"> <li>• Project and change managers (IT and Business)</li> <li>• Project and change managers (IT and Business)</li> <li>• Programme managers</li> <li>• Business managers and users</li> <li>• Technical delivery and support teams</li> <li>• Key players e.g. Business sponsors, Project champions</li> <li>• Relationship managers and internal communications teams</li> <li>• Suppliers (especially outsourced service providers)</li> <li>• Contract and procurement management</li> <li>• Peripheral players/influencers/Policy owners e.g. HR, Facilities Management, Legal</li> </ul>  | <ul style="list-style-type: none"> <li>• Internal audit and external audit (due diligence)</li> <li>• External regulators</li> <li>• Corporate governance coordinator</li> <li>• Risk managers</li> <li>• Compliance – regulatory and internal</li> <li>• Finance/Project Managers/IT and business managers – reviewers of benefits/ROI</li> <li>• Post investment appraisal/Post project review teams</li> </ul>  |
| <b>Legal and Regulatory Responsibilities</b>  |  |  |
| <ul style="list-style-type: none"> <li>• Understand requirements (what regulations are to be complied with)</li> <li>• Set the mandate</li> <li>• Set priorities and expectations</li> <li>• Establish and ensure the expected degree of compliance</li> <li>• Based on advice concerning risk and cost:</li> <li>• Assess impact on business</li> <li>• Provide resource and funding to ensure issues are addressed</li> <li>• Define who is accountable</li> <li>• Obtain internal or external assurance as required that issues have been addressed and controls established</li> <li>• Monitor and evaluate compliance programmes and significant commercial contracts</li> <li>• Sign off specific compliance programmes</li> <li>• Provide approvals when required for significant legal or regulatory decisions</li> </ul> | <ul style="list-style-type: none"> <li>• Advise on IT related technical and commercial risks that could impact legal and regulatory requirements</li> <li>• Provide proposals and business cases for legal and regulatory programmes, projects or action plans</li> <li>• Formulate solutions for compliance or commercial contracts</li> <li>• Identify best practices for ongoing good control of legal and regulatory requirements</li> <li>• Exploit technology and tools where appropriate for ensuring compliance (e.g. asset registers)</li> <li>• Execution of compliance and contractual processes, and operation of related controls</li> <li>• Provide compliance framework to ensure a sustainable “business as usual” approach to compliance</li> <li>• Provide evidence of compliance</li> <li>• Provide information relating to the cost of compliance and also cost of any incidents</li> <li>• Evaluate impact on business environment together with business units</li> <li>• Ensure vendors, service providers, and subcontractors are involved properly and integrated within the overall compliance approach</li> </ul> | <ul style="list-style-type: none"> <li>• Maintain awareness of current and emerging laws, and regulations affecting IT to assess their impact on the organisation’s business</li> <li>• Develop an understanding of their impact on the organisation and advise accordingly on “what is needed” - not necessarily “how”</li> <li>• Monitor adequacy of controls and compliance processes</li> <li>• Monitor the business and IT functions for performance in meeting legal and regulatory requirements and report back to management with advice regarding any shortcomings</li> <li>• Provide independent assurance to management that adequate controls are in place to deal with legal and regulatory requirements</li> </ul> |

**Table 10.2**

### **10.3 Best approach to compliance**

Ideally organisations should deal with legal and regulatory requirements on a “business as usual” basis instead of reacting on a case-by-case basis.

In practice, it is recommended that a framework for dealing with legal and regulatory issues be established. Because IT is fast changing and new regulations are also emerging, any such framework must be flexible and responsive to new requirements.

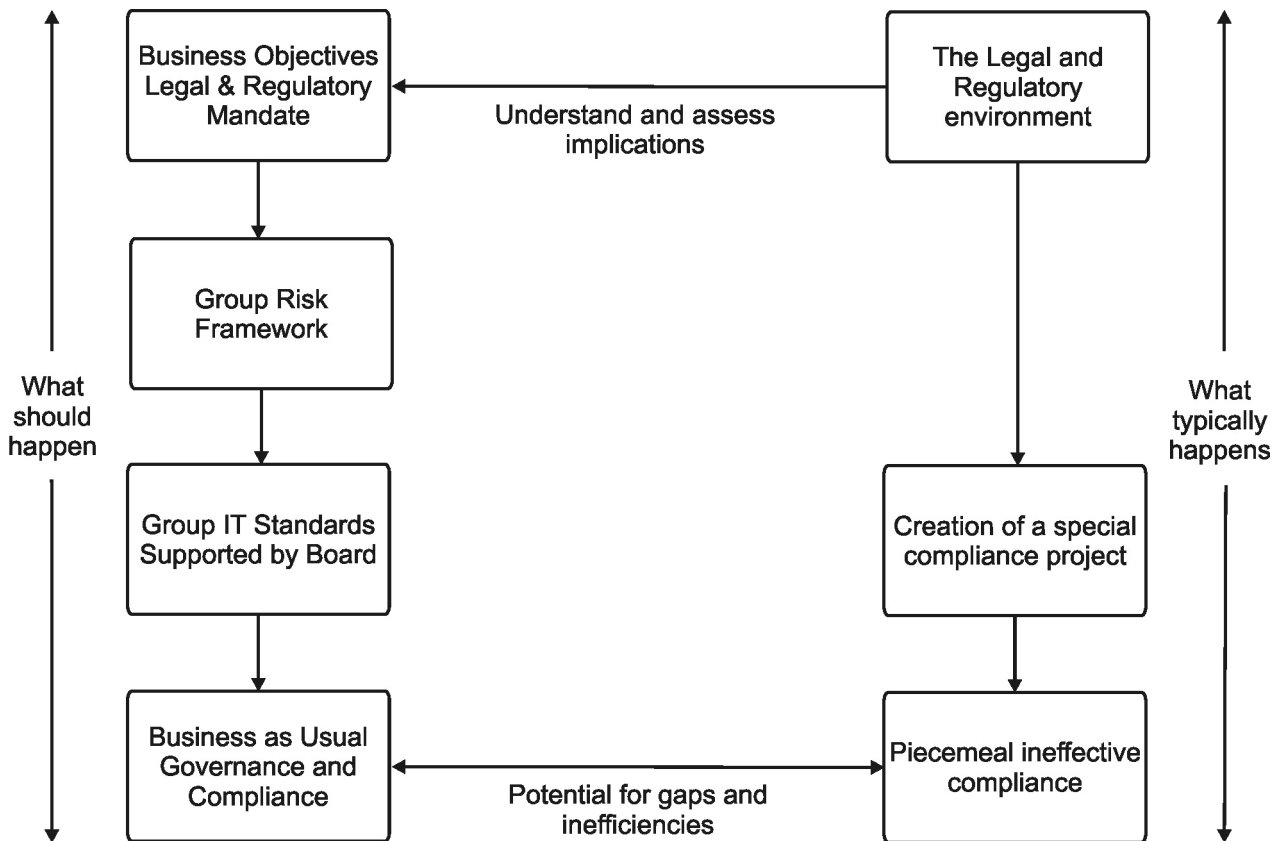


Figure 10.3

Figure 10.3 illustrates a common problem when new regulatory requirements are imposed. To be effectively handled the decisions concerning the regulation should be taken at the level at which business objectives are set and within the group or business risk framework. This is the necessary level at which priorities can be determined and the standards framework can be applied.

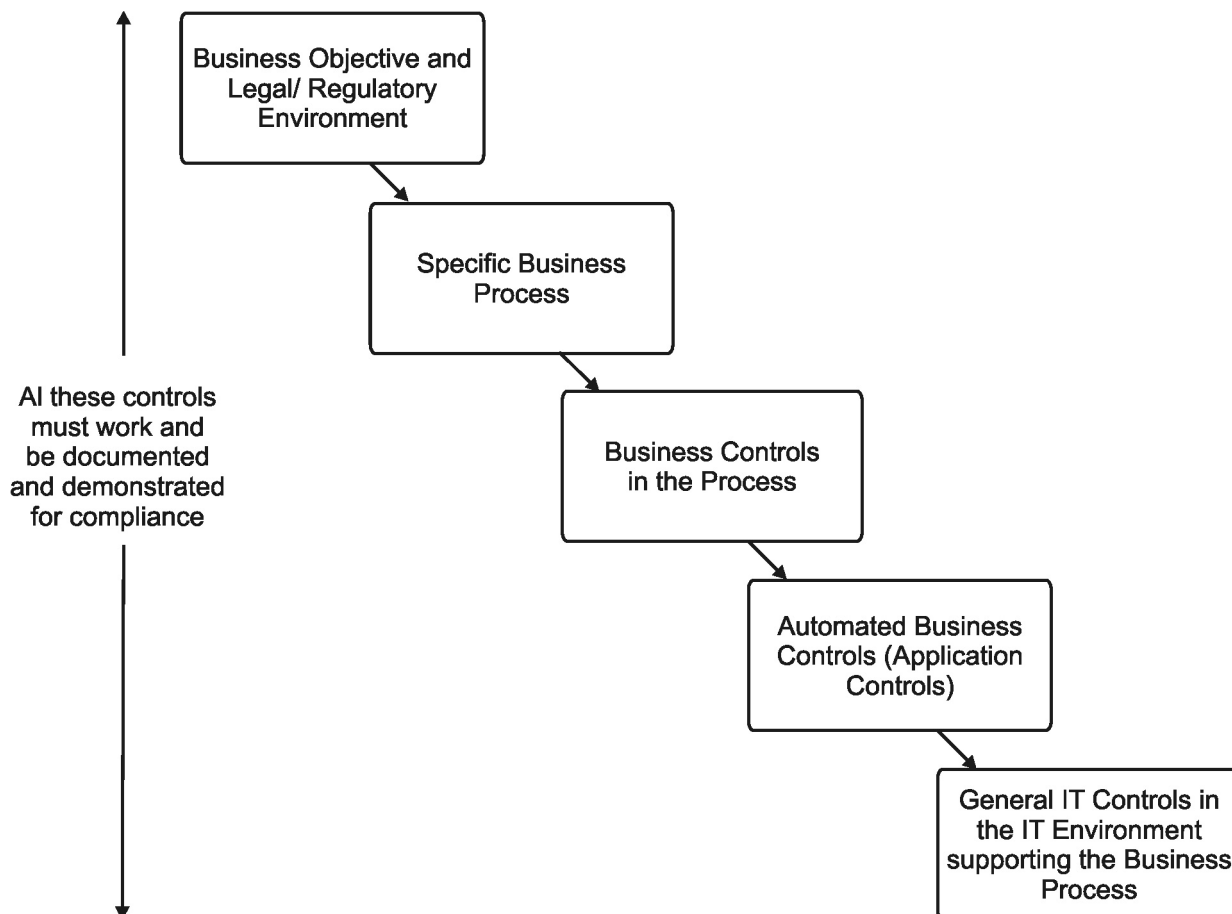
However, as illustrated, a special programme is frequently set up outside the remit of existing standards and governance in the hope that the new regulatory environment can be incorporated. This is usually unsuccessful or inefficient because outside of existing governance it is very difficult to allocate and establish responsibilities for monitoring and testing. Similarly, there can be no clear prioritisation or co-ordination among different regulatory requirements. Conversely, when the left-hand route is followed and a new regulation comes into force, it is possible to identify where there are already procedures in place that enable the new requirements to be met.

▼ For complex IT environments, the importance of the framework is emphasised by the need to understand which standards affect which systems. Then it becomes possible to address all the relevant systems when standards have to change:

- ▶ Consider regulatory issues together
- ▶ Do not set up separate projects which may conflict with the standard approach
- ▶ Decision making must rest with the business in terms of the extent and nature of compliance

## 10.4 What IT has to do

Historically, most IT people did not think about compliance- except in terms of good practice, because regulations rarely impacted the technical environment. Gradually this has changed, first with IT specific legislation like the Data Protection act, and most recently by the realisation that corporate level regulations like Sarbanes-Oxley must be inextricably linked to the IT systems because corporate information and financial reporting has become so automated.



**Figure 10.4**

In addition, due to the very significant cost of IT investments, and the complexity of customer and supplier relationships, legal contracts for IT services are being given much more careful attention. These contracts in turn demand greater controls be demonstrated by the parties to the contract, over many issues such as security, intellectual property, service availability, ownership of deliverables, support of products etc.

As a consequence, IT service providers, vendors, and internal IT functions are all realising that they must be better organised from a control and compliance perspective. It is only a relatively recent realisation that IT related controls should be documented and monitored by IT functions, increasingly driven by regulatory pressure.

Business objectives and processes should drive the system of internal control and therefore the documentation process. The flow should be:

For an efficient and effective compliance process, the documentation should be in a language that auditors would use, and therefore it is best to work with the audit community and adopt a common language and approach such as CobiT.

▼ IT functions increasingly need to be more involved in legal and regulatory requirements and should:

- ▶ *Work with the business users and risk management groups to identify critical systems and compliance priorities.*
- ▶ *Document architectures so that the overall environment is understood on a continuous basis.*
- ▶ *Define processes in IT in a logical well ordered fashion, meaningful to auditors and management (e.g. based on CobiT).*
- ▶ *Appoint process owners so there is accountability and responsibility.*
- ▶ *Understand control concepts, the need for IT controls, and how they relate to business level controls.*
- ▶ *Document these processes and controls (especially for compliance critical systems), and maintain the documentation as changes occur.*

- ▶ *Standardise wherever possible to avoid duplication of effort.*
- ▶ *Maintain evidence of controls being exercised to be better able to demonstrate compliance.*
- ▶ *Generate business benefits from the control and compliance projects by performing gap analyses to drive improvements and efficiencies as well as building good controls.*
- ▶ *Consider the whole infrastructure rather than tackling items on a piecemeal basis.*
- ▶ *Be responsible for diligent procurement and proper control and management of third parties.*

▼ To achieve these objectives:

- ▶ *IT should seek advice from HR, Legal, and Audit, and if necessary external experts.*
- ▶ *Adopt standard approaches and best practices – don't attempt to reinvent the wheel as it wastes time and makes working with partners and auditors much less effective (compare with accounting- standard procedures are essential).*
- ▶ *Build in the need for third party testing as required.*

## 10.5 Dealing with third parties

Every organisation relies on a growing number of third parties for support of IT services. From a legal and regulatory perspective this means that there is potentially a complex hierarchy of responsibilities that combine to meet the legal and regulatory needs of the customer. Ultimately it is the customer's responsibility to ensure that all the right controls are in place with any third party that is relied upon for legal and regulatory compliance.

▼ Conversely, service providers have their own corporate governance agenda, combined with the pressures of their business models – usually to provide a better service at a lower cost than the customer had previously experienced:

- ▶ *They have to work with differing governance models of business partners and clients.*
- ▶ *In theory they might use a standard model across all but in practice this is unlikely.*
  - *Large clients, in particular, are unwilling to change their own model.*
  - *Clients cannot be obliged to do business in a way specified by the provider.*

▼ The outsourcer or provider may not ensure full coverage of legal and regulatory requirements:

- ▶ *The customer may go to the provider and specify what is required or provide a questionnaire, but the provider may still not have taken action himself or know what is required.*
- ▶ *People who negotiate outsourcing contracts are usually at a commercial business level, not driven by controls and compliance issues.*

In order for both sides to be clear on responsibilities it is essential that sufficient in-house capability is retained. Most organisations actually get more rigour when they outsource but most contracts are built around existing operations with all their limitations. The onus should be on the provider to spell out the risks – but the provider will not improve controls unless paid to do so, or can see a commercial benefit in making the necessary investment.

Legally there is a standard reasonable expectation of basic service, and ultimately it is a question of negligence if controls were not operated properly.

The provider is unlikely to provide a higher level of control in specific situations (such as security) than the client had originally operated himself – but must have nevertheless an adequate set of controls. Special requirements such as vulnerability testing will not normally be seen as part of a contract unless formally requested and paid for.

## 10.6 Critical success factors

▼ The IMPACT SIG identified the following success factors to enable effective ongoing legal and regulatory compliance and proper control of legal contracts:

- ▶ *Establish the right culture to encourage diligence and good controls*
- ▶ *Communication throughout the organisation based on a Board level mandate is essential to make sure everyone takes the issues seriously and uniformly*
- ▶ *Involve the right people as advisors but do not abdicate responsibility*
- ▶ *Retaining responsibility for control and compliance when using service providers*
- ▶ *Standardisation and a common approach is the most effective and efficient way to meet compliance requirements*
- ▶ *Use frameworks and accepted compliance models especially those accepted by auditors*
- ▶ *Integrate compliance objectives into the IT strategy*
- ▶ *Ensure management are actively involved – not just performing a sign-off at the end*
  - *Set the tone at the top*
- ▶ *Institutionalise compliance behaviour*
  - *Engage the governance and risk management groups (those who own the framework) as soon as possible*
  - *Provide a positive spin – good controls can be very beneficial*
  - *Make compliance normal business practice rather than a project*
- ▶ *Make compliance meaningful and relevant*
  - *Translate into normal language*
  - *Explain business context*
  - *Carry out awareness training*
- ▶ *Establish mechanisms for evidence and documentation*
- ▶ *Establish metrics for monitoring performance*
- ▶ *Create incentives and/or penalties as part of personal objectives*
- ▶ *Do regular compliance checking and tests*
- ▶ *Do regular review of risks (include 3rd parties)*
- ▶ *Have good incident management procedures to learn from legal and regulatory incidents*

# 11 Architecture Governance

---

|   |    |
|---|----|
| <b>11.1</b> Why is Architecture Governance important? .....           | 60 |
| <b>11.2</b> What are the objectives of Architecture Governance? ..... | 61 |

---

**G**iven the complexity and fast-changing nature of IT, architectures are important for defining technical direction, captured in a formal design that will support evolution and change, based on generally accepted standards as well as specific design standards. Architecture governance is therefore to do with ensuring that the principles of architectures are properly applied to the design and maintenance of information systems, meeting technical design standards as well as the business purpose and strategic objectives for IT.

- ▼ There are generally three overall end goals with respect to architecture governance:
  - ▶ *Business and IT Alignment (fit for purpose)*
  - ▶ *Risk Management (reduced likelihood of design failures)*
  - ▶ *Resource Management (cost effectiveness and value for money)*

The process of determining technological direction via an IT Architecture satisfies the business requirement to take advantage of available and emerging technology to drive and make possible the business strategy. This is enabled by creation and maintenance of a technological infrastructure plan that sets and manages clear and realistic expectations and standards, of what technology can offer in terms of products, services and delivery mechanisms. Given the significant amount of outsourcing of IT services, the effective governance of architectures in these situations is a key consideration. The business strategy may depend on an effective IT architecture, but who defines the architecture in the outsourced situation? The customer should always take control of his own requirements including architectural decisions even if the provider offers existing solutions and approaches. Senior management may assume that providers will develop technology to improve productivity – this is not always the case. A capability for setting the direction for technology improvement should be retained in house and often contracts will call for customers to control their own technical direction. Cost will usually be the driving factor in contractual arrangements – who will pay for architectural upgrades?

- ▼ The group identified the following critical success factors for achieving architectural governance:
  - ▶ *Ensure that the Architecture process and its governance is adequately funded*
  - ▶ *Ensure good communications among all the groups concerned*
  - ▶ *Align the architecture with the business strategy and the culture of the organisation*
  - ▶ *Recognise that persuasion is always needed for compliance and that this can be enhanced by active project involvement, technical consultancy, provision of readily-available, cost-effective tool-kits and components*
  - ▶ *Share all artefacts with outsource providers*

## ▶▶ 11.1 Why is Architecture Governance important?

Architecture (in Greek αρχή = first and τέχνη = craftsmanship) is the art and science of designing structures. In the context of computers, the term architecture is used to describe the technical design and interoperability of components that together make up the information system i.e. hardware, software and network components.

Given the complexity and fast-changing nature of IT, architectures are important for defining technical direction, captured in a formal design that will support evolution and change, based on generally accepted standards as well as specific design standards. There is an analogy with the original use of architectures for defining the design of buildings – providing the blueprint that demonstrates what the end product should look like, that it is formed on a solid foundation, that it is built according to defined design standards, and that it meets the purpose for which it was intended.

Architecture governance is therefore to do with ensuring that the principles of architectures are properly applied to the design and maintenance of information systems, meeting technical design standards as well as the business purpose and strategic objectives for IT. The IT Governance and Technical Architecture SIG members believe that in many organisations the

challenge is to commit to a properly funded and business driven architectural approach. Often it is treated as too technical an activity, with inadequate or insufficiently skilled resources, and with limited business and top management direction.

- ▼ The group assessed the maturity of Architectural activities based on the CobiT® maturity model (see Appendix). This assesses maturity on a scale from 0 to 5. An analysis of the maturity level of the organisations represented showed the following:
  - ▶ *Current maturity ranged from 1+ to 4*
    - *In larger organisations there was a spread (e.g. from 2 to 4) across the different parts of the organisation*
    - *The lowest maturity was in a business where IT had recently been outsourced*
  - ▶ *The maturity level aspired to was between 3+ and 4*
    - *No organisation saw level 5 as necessary*

## **11.2** What are the objectives of Architecture Governance?

The definitions CobiT® provides for setting technical direction were used to help define the purpose of Architecture Governance:

The process of determining technological direction via an IT Architecture satisfies the business requirement to take advantage of available and emerging technology to drive and make possible the business strategy. This is enabled by creation and maintenance of a technological infrastructure plan that sets and manages clear and realistic expectations and standards of what technology can offer in terms of products, services and delivery mechanisms.

- ▼ It considers:
  - ▶ *Capability of current infrastructure*
  - ▶ *Monitoring technology developments via reliable sources*
  - ▶ *Conducting proof-of-concepts*
  - ▶ *Risk, constraints and opportunities*
  - ▶ *Acquisition plans*
  - ▶ *Migration strategy and roadmaps*
  - ▶ *Vendor relationships*
  - ▶ *Independent technology reassessment*
  - ▶ *Hardware and software price/performance changes*
- ▼ Covering the following activities:
  - ▶ *Technological infrastructure planning*
  - ▶ *Monitoring future trends and regulations*
  - ▶ *Assessing technological contingency*
  - ▶ *Planning hardware and software acquisitions*
  - ▶ *Defining technology standards*

The group believe that measurement of these activities is difficult and may often rely on perception of trends.

- ▼ CobiT® suggests focusing on these key measurable outcomes:
  - ▶ *Number of technology solutions that are not aligned with the business strategy*
  - ▶ *Percent of non-compliant technology projects planned*
  - ▶ *Number of non-compatible technologies and platforms*
  - ▶ *Decreased number of technology platforms to maintain*
  - ▶ *Reduced applications deployment effort and time-to-market*
  - ▶ *Increased interoperability between systems and applications*
- ▼ And these performance measures:
  - ▶ *Percent of IT budget assigned to technology infrastructure and research*
  - ▶ *Number of months since the last technology infrastructure review*
  - ▶ *Business functions' satisfaction with the timely identification and analysis of technological opportunities*
  - ▶ *Percent of technological domains within the technology infrastructure plan that have sub-plans specifying current state, vision state and implementation roadmaps*
  - ▶ *Average length of time between the identification of potentially relevant new technology and the decision as to what to do with that technology*

- ▼ The Open Group ([www.opengroup.org](http://www.opengroup.org)) defines an Architecture Governance Framework which covers:

- ▶ *Governance processes*
- ▶ *Policy management*
- ▶ *Compliance assessments*
- ▶ *Dispensation procedures*
- ▶ *Monitoring and reporting*
- ▶ *Business control (compliance with the organisation's business policies)*
- ▶ *Environment management (the physical and logical repository management) and governance environment (administrative processes).*

Given the significant amount of outsourcing of IT services, the effective governance of architectures in these situations is a key consideration. The business strategy may depend on an effective IT architecture, but who defines the architecture in the outsourced situation? The customer should always take control of his own requirements including architectural decisions even if the provider offers existing solutions and approaches. Unfortunately, weaknesses and bad practices in outsourcing arrangements can lead to architectural misunderstandings or restrictions that can be costly or damaging to business performance. On the other hand the provider may enable a customer to adopt a proven, reliable architecture at much lower cost and in much faster timescales than agreeing and developing a solution in house (for example hosting services).

Senior management may assume that providers will develop technology to improve productivity – this is not always the case. A capability for setting the direction for technology improvement should be retained in house and often contracts will call for customers to control their own technical direction. Cost will usually be the driving factor in contractual arrangements – who will pay for architectural upgrades? Even when improvements are called for by the contract, they may not be provided.



# 12 Managing the IT investment

|  |    |
|--|----|
| <b>12.1</b> Why is managing the IT investment important? .....   | 63 |
| <b>12.2</b> Portfolio management .....                           | 64 |
| <b>12.3</b> Benefits management .....                            | 65 |
| <b>12.4</b> Measuring investment performance .....               | 65 |
| <b>12.5</b> Improving value delivery and ROI .....               | 66 |
| <b>12.6</b> Measuring and controlling IT operational costs ..... | 66 |
| <b>12.7</b> Project risk management .....                        | 66 |

**E**nsuring that value is obtained from investment in information technology is an essential component of IT governance. No investment, whether IT-related or not, should be undertaken without full knowledge of the expected cost and the anticipated return. Expected return should always be related to risk as, given the higher likelihood of failure, high-risk projects should always have an anticipation of a higher return. Ensuring that the right projects are approved in the first place implies a need for accurate predictive costing of the total project across its lifetime and robust predictions of the potential return, including quantification of the direct and indirect benefits. To ensure that the total process works and becomes part of the culture of the organisation, it is essential to establish proper tracking mechanisms to determine the actual value delivered and enable accountability.

Given the volatility of a portfolio of IT-related business projects, it is essential to embed active portfolio management into the organisation to maximise value creation and minimise the risk of value destruction. As with any aspect of IT governance, the process needs visibility, leadership and commitment from the top.

## 12.1 Why is managing the IT investment important?

“The basic principles of IT value are the on-time and within-budget delivery of appropriate quality, which achieves the benefits that were promised. In business terms, this is often translated into: competitive advantage, elapsed time for order/service fulfilment, customer satisfaction, customer wait time, employee productivity and profitability. Several of these elements are either subjective or difficult to measure, something all stakeholders need to understand. Often, top management and boards fear to start major IT investments because of the size of investment and the uncertainty of the outcome. For effective IT value delivery to be achieved, both the actual costs and the return on investment need to be managed” (ITGI Board Briefing V2 2004).

20% of all expenditure on IT is wasted<sup>7</sup>, representing, on a global basis, annual value destruction of US\$500bn according to a 2002 Gartner paper (Gartner, ‘The Elusive Business Value of IT’, August 2002). It is then no surprise that there is an increasing demand from boards and executive management for generally accepted guidelines for investment decision-making and benefit realisation. While particularly applicable to IT-enabled business investments, where IT is a means to an end, the need is equally applicable to all investment decisions. In the case of IT, the “end” is to contribute to the process of value creation in the enterprise.

IT-enabled business investments, when managed well within an effective governance framework, provide organisations with significant opportunities to create value. Without effective governance and good management, they provide an equally significant opportunity to destroy value. Horror stories abound around the value destruction suffered by major organisations through the failed implementation of IT enabled business investments. Nike reportedly lost more than US\$200m through difficulties experienced in implementing its supply chain software, failures in IT enabled logistics systems at MFI and Sainsbury in the UK led to multi-million pound write-offs, profit warnings and erosion of share price. Other organisations have suffered in a similar fashion.

On the other hand, many successful organisations have created value through selection of the right investments, and successfully managing them through implementation to realising the expected value. Examples include IBM who reportedly was able to save more than US\$12bn over two years by linking disparate pieces of its supply chain and thereby reducing inventory levels, and Southwest Airlines who were able to reduce procurement costs and increase service levels through their supply chain transformation project.

7. IT Governance Institute® research on IT Value.

The message is clear. IT-enabled business investments can bring huge rewards with the right governance and management processes and full commitment from all management levels. The process for managing IT investments can be summarised as developing, implementing, operating and maintaining financial controls over IT investments and expenditures in line with the IT strategic and tactical plans. Essential elements in this process are benefit and cost justification, budget ownership and accountability and control of actual spending. The process should enable the effective and efficient use of IT resources and provides transparency and accountability into the benefit realisation, total cost of ownership and return on investment of IT.

### **The role of IT Councils**

Organisations should establish an IT Council (or Strategy Committee or similar group) at board level to ensure that IT governance, as part of corporate governance, is adequately addressed. This committee reviews major investments on behalf of the full board and advises on strategic direction. Below this committee an IT steering committee (or equivalent) should be established to oversee the IT function and its activities and developing IT plans. The committee should determine prioritisation of IT resources and projects in line with business needs and should be composed of executive management, business and IT representatives. This committee structure will provide the oversight and direction of IT investments, ensuring accountability at senior level and proper involvement of all stakeholders.

## **12.2 Portfolio management**

▼ Portfolio management is a good practice for coordinating any group of investments and can be effectively applied to IT investments. It consists of:

- ▶ *Working with the business to establish and maintain a portfolio of new and existing IT-enabled investment programmes that are needed to achieve business goals and which, together with existing IT services and assets, form the basis of the IT budget.*
- ▶ *Building a portfolio that recognises that there will be a variety of categories of investment which will differ both in complexity and in the degree of freedom in allocating funds.*
- ▶ *Aligning the portfolio with the strategic direction of the enterprise in order to achieve the right balance of investments.*
- ▶ *Having evaluation criteria in place that should include, at a minimum: alignment with the enterprise's strategic objectives; financial worth (as determined by the practices of each enterprise); and risk, both delivery risk (the risk of not delivering a capability) and benefits risk (the risk of not realising the expected benefit from the capability).*
- ▶ *Implementing a decision-making process to prioritise the allocation of resources for IT operations, maintenance and systems development in order to manage and deliver an optimal return on the IT portfolio.*

Portfolio management is needed to balance and prioritise between new projects and the operating costs of existing systems. It can lead to possible savings on operating costs – e.g. via outsourcing or establishing shared services. Real portfolio management implies a group at the top with an overview of priorities and what is needed – otherwise decisions will be based on relationships and sometimes “who shouts loudest” rather than an objective analysis. Portfolio management should focus on the total ongoing commitment not only the cost of the initial implementation. Managing portfolios can be difficult and requires sound business judgment as well as disciplined management otherwise projects that may be significant to the business may be overlooked or missed in the detailed management processes. For example, projects that are significant to aligning with the business strategy or small initiatives that are critical opportunities may be overlooked. Like all governance activities decisions made at the top level regarding the portfolio investment approach must be communicated down to individual programmes and projects and be monitored.

### **Portfolio Monitoring**

Having created an investment portfolio approach, and approved individual investment programmes, there is a need to monitor (post sign-off) all active programmes, just as one would a financial investment portfolio of for example, equities or properties. Costs need to be monitored as well as cost reduction in business areas and revenue generating potential in the business. The portfolio should also be monitored to ensure continuous alignment with strategic business drivers which may be changing with time and with risk factors – both internal to projects and externally. Projects can be very hard to stop, although it is a good practice to review projects on a regular basis and cancel those that are not likely to deliver value. It is recommended that a project office be established working at the programme level, monitoring standards, targets and deliverables. It can be difficult to find and keep the appropriate people in place for this kind of work. Experience has shown that it can be effective to use bright, temporary people or contractors who will also be more likely to give objective assessments.

Acquisition programmes and procurement projects in the UK central civil government are subject to OGC Gateway Reviews. The OGC Gateway Process examines a programme or project at critical stages in its lifecycle to provide assurance that it can progress successfully to the next stage; the process is based on well-proven techniques that lead to more effective delivery of benefits together with more predictable costs and outcomes. It is designed to be applied to delivery programmes and procurement projects, including those that procure IT-enabled business change. The OGC Gateway Process provides assurance and support for Senior Responsible Owners (SROs) in discharging their responsibilities to achieve their business aims. For more guidance refer to [www.ogc.gov.uk](http://www.ogc.gov.uk).

## 12.3 Benefits management

Monitoring whether or not benefits are being delivered is a key aspect of investment management. Without it, it will be impossible to know whether a return on the investment has been realised. In practice though, it seems this is rarely done for IT investments.

- ▼ The objectives of benefits management should include:
  - ▶ *Implementation of a benefit monitoring process.*
  - ▶ *Identification of IT's expected contribution to business results, either as a component of IT-enabled investment programmes, or as part of regular operational support and then agreed, monitored and reported on.*
  - ▶ *Reporting opportunities to improve IT's contribution, appropriate actions should be defined and taken.*
  - ▶ *Updating the programme business case where changes in IT's contribution impact the programme, or where changes to other related projects impact the programme*

The IMPACT IT Governance SIG members believe that seldom does true benefit monitoring take place. Business sponsors should manage benefits but usually they do not. This may be because of job movement in the business, or because the business owner of change is often not the operational owner of the benefits. The main reason though is probably a lack of willingness for the senior business sponsor to take ownership and accountability for monitoring benefits. Investment oversight and the drive to apply discipline to the monitoring process should be directed by the IT Council or management team via a standard process.

## 12.4 Measuring investment performance

Management should establish a general monitoring framework and approach that defines the scope, the methodology and the process to be followed for monitoring IT's contribution to the results of the enterprise's portfolio management and programme management processes. The framework should be integrated with the corporate performance management system. The objective is to assess the overall performance of the portfolio of investments. Investment performance assessment should review how the products of IT activities are performing – not just IT as such but the whole process. Many lessons can be

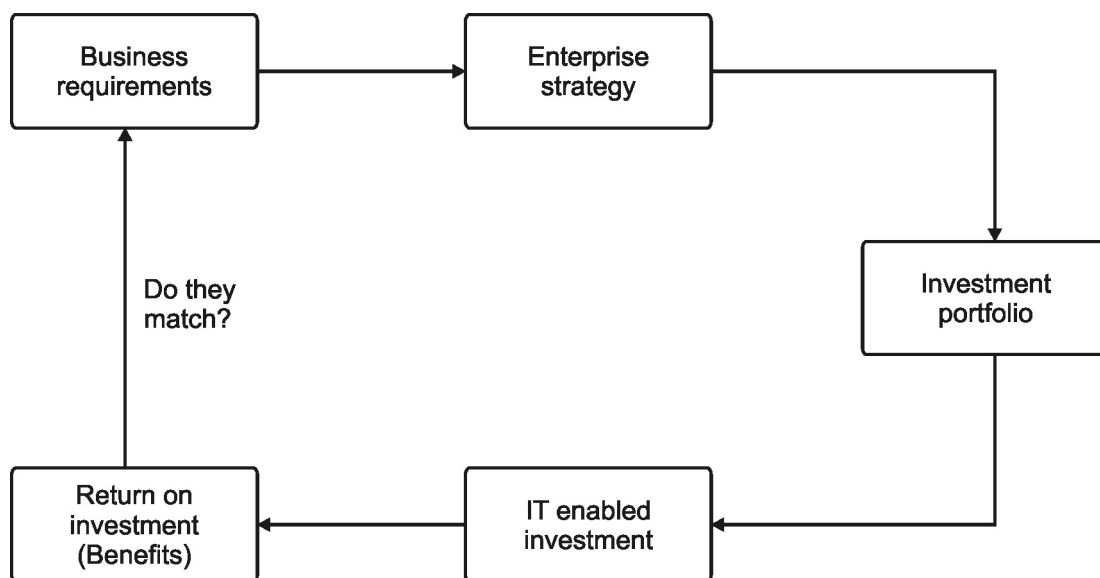


Figure 12.4

learnt from analysing why projects are successful or not successful. Setting actual targets and metrics should be driven by the stakeholders who should also approve and monitor them.

## 12.5 Improving value delivery and ROI

▼ To optimise the business value realised from IT-enabled investments it is recommended that<sup>8</sup>:

- ▶ *IT-enabled investments are managed as a portfolio of investments.*
- ▶ *IT-enabled investments include the full scope of activities that are required to achieve business value.*
- ▶ *IT-enabled investments are managed through their full economic life-cycle.*
- ▶ *Value delivery practices define and monitor key metrics and respond quickly to any changes or deviations.*
- ▶ *Value delivery practices engage the business and assign appropriate accountability for the delivery of capabilities and the realisation of business benefits.*
- ▶ *Value delivery practices are continually monitored, evaluated and improved.*
- ▶ *A disciplined approach is enforced to portfolio, programme and project management, insisting that the business takes ownership of all IT-enabled investments and that IT ensures optimisation of the costs of delivering IT capabilities and services.*
- ▶ *Technology investments are standardised to the greatest extent possible to avoid the increased cost and complexity of a proliferation of technical solutions.*

## 12.6 Measuring and controlling IT operational costs

When managing IT investments, there is a tendency to concentrate on new projects rather than ongoing operations. The operational budget is likely to be a much larger financial amount than new investments, and there are often opportunities to optimise these ongoing costs. It is therefore recommended that a cost management process be implemented comparing actual costs to budgets. Costs should be monitored and reported. Where there are deviations, these should be identified in a timely manner and the impact of those deviations on programmes should be assessed and, together with the business sponsor of those programmes, appropriate remedial action should be taken and, if necessary, the programme business case should be updated. If the costs are recorded and analysed down to the lowest “service” level, then the business can decide whether to use the service. Doing this may be costly – especially if carried to too low a level, so it is most effective to focus on significant services and cost areas.

## 12.7 Project risk management

▼ Project risk management is a very valuable process, providing an independent monitoring function. Its purpose is to eliminate or minimise specific risks associated with individual projects through a systematic process of planning, identifying, analysing, responding to, monitoring and controlling the areas or events that have the potential to cause unwanted change. It can include a focus on costs and benefit realisation. In this context project risk management should focus on the following:

- ▶ *Risk assessments that look beyond the internals of the project*
- ▶ *Identifying the factors to be considered in advance in a “risk register”*
- ▶ *Tracking these items on a continuous basis*
- ▶ *Understanding the proximity of the risk – when might it hit?*
- ▶ *Evaluating the severity of the risk to determine the frequency of monitoring needed*
- ▶ *Risks considered to be high should be closely monitored – by the steering committee if appropriate – and feedback should be obtained*
- ▶ *Project risks that relate to execution and delivery; examples of external business-related risk include:*
  - *Will the customer want it?*
  - *Need for market testing*
  - *Proof of concept needed?*

# 13 Success Factors

▼ Focus on the following success factors:

- ▶ *Treat IT governance initiatives as a project not a 'one-off' step. The goal is to make governance "business as usual".*
- ▶ *Obtain top management buy-in and ownership. This needs to be based on the principles of best managing the IT investment.*
- ▶ *Remember that implementation involves cultural change as well as new processes. Make sure you enable and motivate these changes.*
- ▶ *Manage expectations. In most enterprises, achieving successful oversight of IT takes some time and will involve continuous improvement.*



# IT Governance

## Developing a successful governance strategy

### A Best Practice guide for decision makers in IT

Throughout the past five years, we have witnessed unparalleled corporate scandals and failures in global businesses. The result; heightened focus on corporate governance, stricter regulations and new directors' responsibilities, all adding to the pressure on IT Directors and CIOs. They must now demonstrate to auditors that IT systems which support financial reporting, as well as monitor and manage business performance are based on sound management systems and controls.

Against this background, it has never been more important to ensure your organisation governs the use of IT properly. With corporate governance on every boardroom agenda - and increasing scrutiny of IT's performance - IT governance has become a hot topic around the world. For some many businesses, IT governance initiatives are already transforming the way their organisations take responsibility for IT. For others, it is a challenge just knowing where to start.

Recognising the challenges faced by CIOs in establishing effective IT governance, the NCCs IMPACT Programme launched an IT Governance Special Interest Group (SIG). Its aim was to identify not just the issues that need to be addressed, but also practical approaches for organisations to follow. Over the past two years, heads of IT governance from Abbey, Aon, Avis, Barclays, BOC, DfES, Eli Lilly, Learning & Skills Council, Legal & General, Marsh, NOMS, Royal Mail, and TUI Group examined the key challenges. They shared successful approaches and defined best practice.

This IT Governance Best Practice Guide is a comprehensive insight of the principles and practices that the group put together. It is presented in a form that should help you to understand better how to guide successful IT governance initiatives and make effective management and control of IT resources "business as usual".

This Guide forms part of the NCC 'Best Practice' Guides series and is intended to be of practical use for decision makers in IT. This guidance is achieved through industry consensus, managed by NCC, across the broadest range of professionals and experts.



#### National Computing Centre

Oxford House,  
Oxford Road,  
Manchester M1 7ED

**Tel:** 0161 242 2121

**Fax:** 0161 242 2499

**I M P A C T**  
Leading through Sharing

#### The IMPACT Programme

International Press Centre,  
76 Shoe Lane,  
London EC4A 3JB

**Tel:** 0207 842 7900

**Fax:** 0207 842 7979

ISBN 0-85012-897-8



9 780850 128970

ISBN 0-85012-897-8  
£35.00 NCC Members  
£50.00 Non NCC Members

**IMPACT**  
Leading through Sharing

