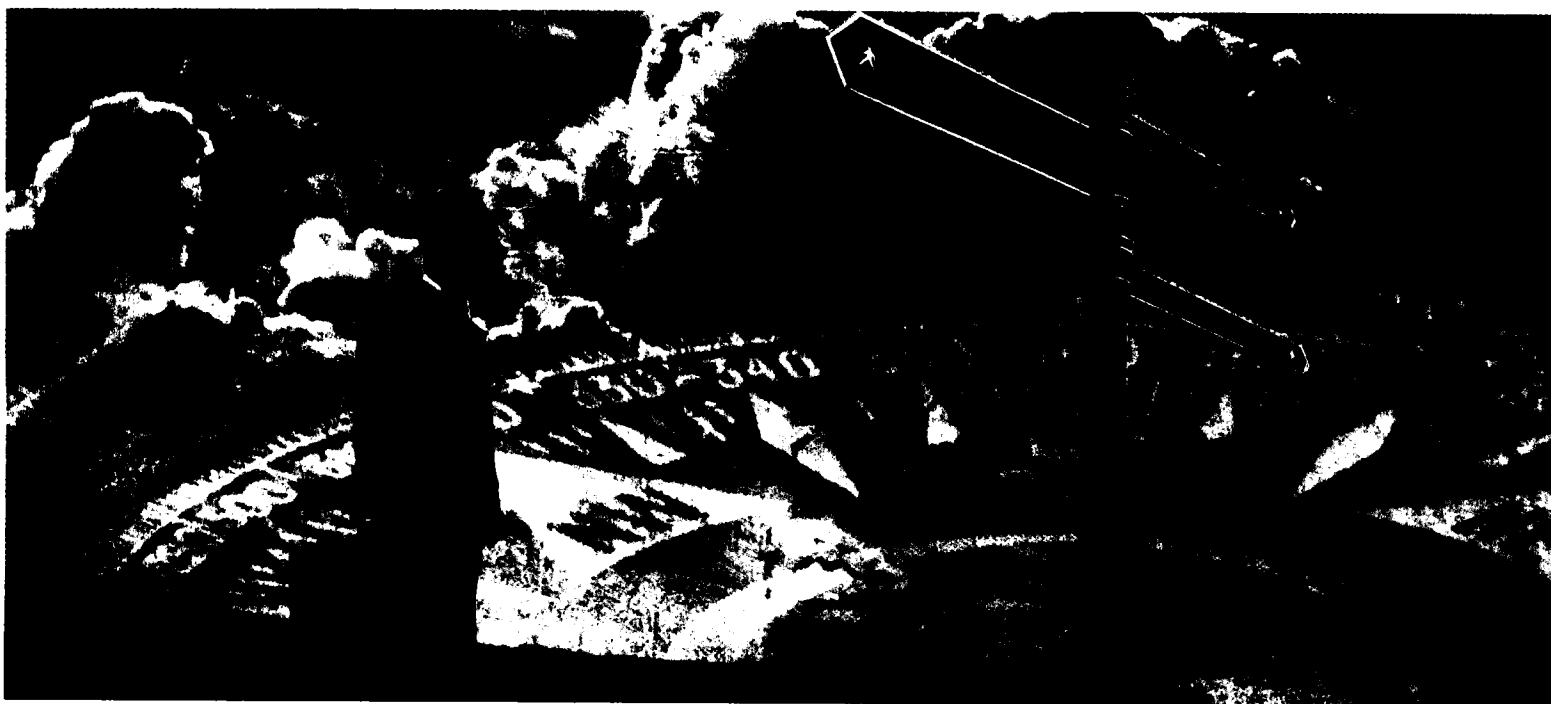For IT leaders – strategy, people, processes and projects

Management

ComputerWeekly
40th
anniversary year

GOVERNANCE There's no need for wrong turns on the road to achieving effective IT governance. Frameworks can offer a clear path to better risk management and value

A helping hand with IT governance

Showing the way: a mixture of frameworks such as Cobit, ITIL, CMM and ISO 17799 can help organisations with their IT governance implementations

Paul Williams
Opinion

> It is surprising that relatively few organisations to date have started to use existing IT governance frameworks to help them in their endeavours

KEY POINTS
▶ Fewer than 20% of firms using IT governance frameworks, says study
▶ Frameworks can be used collectively, depending on specific needs
▶ Cobit framework is globally accepted and promoted as an open standard
▶ Must be proper balance between operational needs of IT and compliance

Within many organisations IT governance is up there with military intelligence and rap music as one of the great oxymorons of our time. To more enlightened organisations, however, IT governance is a central component of their business culture, leading to enhanced management of risk and the delivery of measurable and sustainable stakeholder value from IT-related investments.

A KPMG study on IT governance from 2004 contained references from a number of CIOs of major UK companies with quotes such as "the potential benefits of governance include the significant elimination of waste and improved strategic focus", and "improved communication is one of the most important achievements of governance".

Studies such as this are not short of ringing endorsements for the value that a positive approach to IT governance can bring. Few such studies, however, concentrate on the difficulties that many organisations experience in developing, implementing, maintaining and monitoring effective IT governance structures and processes.

Many organisations embarking on the road of IT governance seek assistance from other, perhaps more mature, organisations among their peers or from external advisers. Such help can be invaluable in helping to avoid the pitfalls and in enhancing their ability to achieve success in the shortest time.

However, external help will never be low cost, and peer group assistance will always be inhibited by competitive pressures. Equally, a fully independent approach can be a lonely and unpredictable course,

prone to blind alleys, self doubt and frustration.

Set against this background, therefore, it is surprising that relatively few organisations to date have started to use existing IT governance frameworks to help them in their endeavours.

Indeed, the same KPMG study identified that fewer than 20% of organisations were using frameworks such as the Control Objectives for Information and Related Technology (Cobit), the Capability Maturity Model (CMM), ISO 17799 and the IT Infrastructure Library (ITIL) to assist with their IT governance implementation. Why is this?

Of course, with the possible exception of Cobit, there is no non-proprietary framework that comprehensively covers the total
→ continued on p28

Management

spectrum of structures and processes relevant to IT governance. And Cobit itself is often in danger of being regarded as the "all-purpose miracle cleaner" of IT governance frameworks in the way it has been promoted as an IT governance, process and management control and IT audit tool.

The existence of these (and other) standards has often caused some confusion with IT and business managers who often ask which of these they should use, or which is the most appropriate for their environment.

Of course it is not a simple matter of selecting the right one for your organisation. The fact is that all of these frameworks are potentially useful and, depending on your specific needs, they may be used collectively but in a practical and selective way.

Due to the confusion, the recently published management briefing from the IT Governance Institute (ITGI), which is responsible for Cobit, and the UK Office of Government Commerce (OGC) – the sponsor of ITIL – is to be welcomed. The IT Service Management Forum (itSMF) has also endorsed its content.

This joint briefing paper makes the point that to achieve alignment of best practices to business requirements, Cobit should be used at the highest level. This will provide an overall control framework based on an IT process model that should generically suit most organisations, regardless of industry or whether private or public sector.

Specific practices and standards such as ITIL and ISO 17799 cover discrete areas and can be mapped up to the Cobit framework, thus providing a hierarchy of guidance materials.

Cobit has the major advantages of being globally accepted and promoted as an open standard which is available to be used by any organisation for their own IT governance and related purposes at no cost. If used intelligently, it has the flex-
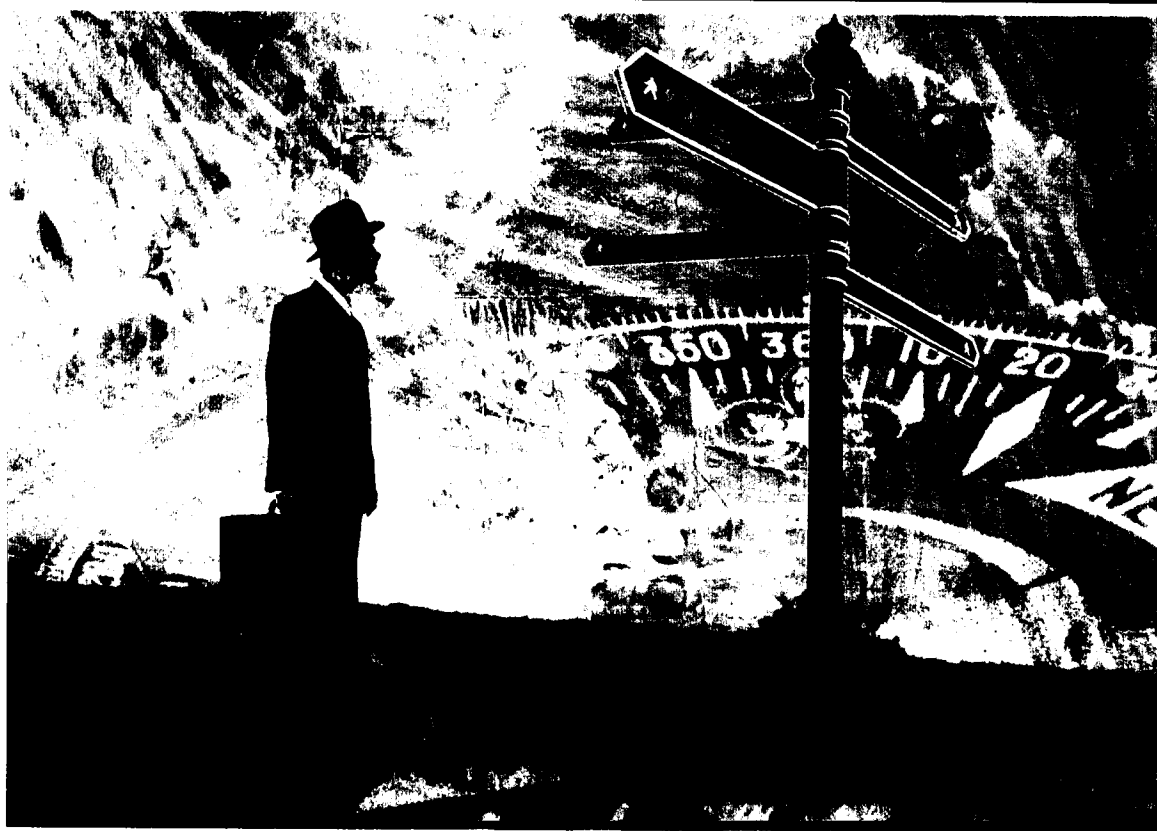
Guidance: although Cobit can appear complex, this can be overcome with an intitially selective implementation

ibility to be totally adaptable to the needs of each different organisation.

A 2005 survey carried out by PricewaterhouseCoopers on behalf of the ITGI has indicated that, of those entities currently using Cobit, 75% found it either very useful or somewhat useful, with 15% undecided and less than 10% showing a negative response. The main negative issue identified by the respondents was the perceived complexity of the framework.

Most users recognise that to cover the comprehensive ground that it does, a degree of complexity is unavoidable, but this can be overcome by an initially selective implementation leading towards full implementation over a sensible period of time.

To help with this there is a "lite" version of Cobit called Cobit Quickstart which, although originally de-

> **It is essential that there is a proper balance between the IT function's ability to operate in an entrepreneurial way, and seeking to comply with a set of rules and appropriate behaviours**

signed for small-to-medium-sized enterprises, can be used to support an initial implementation of Cobit in larger enterprises.

However, whichever framework is selected, if IT governance is going to be successful and deliver real value within your organisation, it is essential that there is a proper balance between the IT function's ability to operate in an entrepreneurial way, and seeking to comply with a set of rules and appropriate behaviours.

This is a key reason why the implementation of IT governance using a supporting framework has to be done using intelligence and discretion.

The solution has to be appropriate to the need, thus it requires a proper understanding of the business, its value drivers, its appetite for risk, the relevant regulatory framework and the corporate culture.

However, with the aid of such an understanding the use of a governance framework can significantly reduce the pain and effort required to ultimately reap the benefits of IT governance.

● *Paul Williams is an independent consultant specialising in IT governance, and a past international president of the IT Governance Institute*

WHAT IS COBIT?

The Control Objectives for Information and Related Technology (Cobit) is an IT governance framework and supporting toolset that allows IT managers to bridge the gap between control requirements, technical issues and business risks.

Created by the Information Systems Audit and Control Association (ISACA), and the IT Governance Institute (ITGI) in

1992, Cobit enables clear policy development and good practice for IT control throughout organisations.

Cobit provides IT managers, auditors and IT users with a set of generally accepted measures, indicators, processes and best practices to assist them in maximising the benefits derived from IT and developing appropriate IT governance and control in a company.