

# King's Counsel\*

## IT Governance

### Steering Point

The King Committee on governance issued the *King Report on Governance for South Africa – 2009 (the “Report”)* and the *King Code of Governance Principles – 2009 (the “Code”)* together referred to as “King III” on 1 September 2009.

The issuance of King III was necessitated by the new Companies Act of South Africa and the changes in international governance trends that have emerged since the release of the second King Report on Corporate Governance for South Africa (King II) in 2002.

King III recognises that information technology (IT) has become an integral part of modern business

and is fundamental to the support, sustainability and growth of organisations. IT now cuts across all aspects, components and processes in business and is therefore not only an operational enabler, but also a significant source of risk. It is for this reason that King III proposes that IT should be governed from board level to ensure that it supports the strategic objectives of the organisation.



#### Inside

Content	Page
IT governance in the context of King III	1
Summary of principles, recommendations and practical considerations	1
Putting principles into practice	4
Added benefits of sound IT governance	6
Critical factors for a successful implementation	6
Our services	8
Contacts	8
IT Publications	9

The Companies Act, 2008 (which constitutes the redraft of the Companies Act, 1973) was assented to and signed by the President on 8 April 2009. The Act will come into operation on a date which is yet to be fixed by the President.

## IT governance in the context of King III

Since information and communication technology have come to dominate the business operating environment, sound corporate governance now requires active consideration of IT governance. In contrast to King I (1994) and King II (2002), King III recognises this important development and has dedicated an entire chapter of the Report to the governance of information technology. King III essentially provides that in exercising their duty of care, directors should ensure that prudent and reasonable steps have been taken with respect to IT governance. Due to the critical nature of IT in enabling business processes, and the intellectual and other information resources that are exposed through technology channels, IT governance now represents an essential component in ensuring the efficient and secure operation of the business.

### Summary of principles, recommendations and practical considerations

5.1 The board should be responsible for information technology (IT) governance	
Recommendations	Practical considerations
<ul style="list-style-type: none"> <li>The board should understand the strategic importance of IT, assume responsibility for the governance of IT and place it on the board agenda.</li> <li>IT should be directed and controlled effectively by the board through the establishment of an IT governance framework.</li> <li>The IT governance framework's function is to support effective and efficient management and decision making around the utilisation of IT resources to facilitate the achievement of the company's objectives and the management of IT-related risk.</li> <li>The IT governance framework includes a charter, policies, decision-making structures, accountability framework, IT reporting and an IT internal control framework.</li> <li>Within the IT governance framework, the board should ensure that an IT charter and policies are established and implemented.</li> <li>The board should ensure that an IT internal control framework is adopted and implemented and it should receive independent assurance on the effectiveness thereof.</li> <li>The board should also ensure promotion of an ethical IT governance culture and awareness of a common IT language.</li> </ul>	<p>An IT governance framework should be in place covering both strategic and operational IT aspects, including:</p> <ul style="list-style-type: none"> <li>Charter;</li> <li>Policies;</li> <li>Decision-making rights and structures;</li> <li>Accountability framework;</li> <li>IT reporting; and</li> <li>IT internal control framework.</li> </ul>
5.2 IT should be aligned with the performance and sustainability objectives of the company	
Recommendations	Practical considerations
<ul style="list-style-type: none"> <li>The board should ensure that the IT strategy is integrated with the company's strategic and business processes.</li> <li>This requires the integration of business and IT plans, defining the IT value proposition and aligning IT operations with business operations.</li> <li>The board should ensure that there is a process in place to identify and exploit opportunities to improve the performance and sustainability of the company through the use of IT.</li> <li>The negative impact of IT on the environment should be considered.</li> </ul>	<ul style="list-style-type: none"> <li>IT should be considered within the business budgeting and planning cycle.</li> <li>An IT strategy should be in place which is aligned with the business strategy and which clearly stipulates the IT value propositions, the IT sustainability plan, other IT initiatives and how they are aligned with the business' requirements.</li> <li>The use of emerging technologies for the benefit of business should be considered within the IT strategy, while the compilation of or changes to business strategy should consider the impact of IT.</li> <li>An IT sustainability plan should be considered that is aligned with the overall business sustainability objectives.</li> <li>Reporting back to the board on IT achievements against the IT strategy and sustainability plan.</li> </ul>

### 5.3 The board should delegate to management the responsibility for the implementation of an IT governance framework

Recommendations	Practical considerations
<ul style="list-style-type: none"> <li>• Management should be responsible for the implementation of the structures, processes and mechanisms for the IT governance framework.</li> <li>• The board may appoint an IT steering committee of similar function to assist with its governance of IT.</li> <li>• The CEO should appoint a chief information officer (CIO) responsible for the management of IT.</li> <li>• The CIO should be a suitably qualified and experienced person who should have access and interact regularly on strategic IT matters with the board and/or appropriate board committee and executive management.</li> <li>• IT should report to the board on whether:               <ul style="list-style-type: none"> <li>– IT objectives are met</li> <li>– IT is resilient and agile to adapt to strategic needs</li> <li>– IT is protected against risks; and</li> <li>– Technology opportunities are exploited.</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>• An appropriately qualified CIO or IT manager (depending on the criticality of IT for the business) with business, IT and IT risk management knowledge should interact with the board or IT subcommittee and executive management on strategic IT matters.</li> <li>• The CIO needs to agree with the board or IT subcommittee on what needs to be reported internally and externally via the integrated report.</li> <li>• Performance metrics should be derived from the IT strategy and IT governance frameworks and be embedded within the KPIs of the CIO and IT management.</li> </ul>

### 5.4 The board should monitor and evaluate significant IT investments and expenditure

Recommendations	Practical considerations
<ul style="list-style-type: none"> <li>• The board should oversee the value delivery of IT and monitor the return on investment (ROI) from significant IT projects.</li> <li>• The board should ensure that intellectual property contained in information systems is protected.</li> <li>• The board should obtain independent assurance on the IT governance and controls supporting any outsourced IT services.</li> <li>• Appropriate project management should be applied to all IT projects.</li> <li>• If responsibility for the provision of IT has been delegated to another party (or division), all parties (including the board) remain accountable for enforcing and monitoring IT governance.</li> <li>• The board is responsible for ensuring good governance principles are in place for the acquisition and disposal of IT goods and services.</li> </ul>	<ul style="list-style-type: none"> <li>• Effective project management (incorporating benefits management and independent quality assurance) to ensure that project benefits are measured and monitored as part of IT projects.</li> <li>• Data classification exercise to determine the sensitivity of data and what protection measures should be applied to different classes of data.</li> <li>• Use of auditors to provide independent assurance on outsourced IT services e.g. ISAE 3402 (previously SAS 70).</li> <li>• Measuring and reporting on the IT spend and the value derived from IT via standard reporting templates. Value derived from IT can be measured in quantitative terms, but also in qualitative terms and with the utilisation of industry benchmarks.</li> <li>• IT procurement and disposal policies, standards and procedures to be put in place.</li> </ul>

### 5.5 IT should form an integral part of the company's risk management

Recommendations	Practical considerations
<ul style="list-style-type: none"> <li>• The board should ensure that IT risk is considered as part of the company's risk management activities.</li> <li>• The board should evaluate how IT can be used to aid the company in managing its risk and compliance requirements.</li> <li>• Management should regularly demonstrate to the board that the company has adequate business resilience arrangements in place for disaster recovery.</li> <li>• IT risk management should cover IT legal risks, compliance to laws, rules codes and standards</li> </ul>	<ul style="list-style-type: none"> <li>• IT risks should be managed as part of the enterprise risk management (ERM) activities of the organisation.</li> <li>• Management is responsible for ensuring adequate disaster recovery plans are in place – these should be aligned to the company's business continuity plan and reported on regularly.</li> <li>• Ensuring awareness of IT-related laws and regulations either through the compliance officer or through an individual within IT who is given this responsibility.</li> <li>• Appropriate software licence management should be in place.</li> </ul>

## 5.6 The board should ensure that information assets are managed effectively

Recommendations	Practical considerations
<ul style="list-style-type: none"> <li>The board should ensure that a formal information security management system is developed and implemented, incorporating confidentiality, integrity and availability of information.</li> <li>Sensitive information (personal, private, confidential or secret) should be identified and classified with appropriate handling and monitoring procedures put in place.</li> <li>Processes should be put in place to monitor the quality of data.</li> <li>The board should ensure that all personal information is identified and treated by the company as an important business asset.</li> <li>The board should oversee and approve the information security strategy and delegate and empower management to implement the strategy.</li> </ul>	<ul style="list-style-type: none"> <li>A comprehensive security management policy should be approved by the board and implemented throughout the organisation incorporating:               <ul style="list-style-type: none"> <li>– Security governance;</li> <li>– Incident monitoring;</li> <li>– Technical security;</li> <li>– Identity management; and</li> <li>– Data classification and protection.</li> </ul> </li> <li>Independent assurance of the information security management system.</li> <li>Data management policy, standard and procedure to be put in place.</li> <li>Security strategy to be developed and approved by the board.</li> </ul>

## 5.7 A risk committee and audit committee should assist the board in carrying out its IT responsibilities

Recommendations	Practical considerations
<ul style="list-style-type: none"> <li>The risk committee should ensure that IT risks are adequately addressed.</li> <li>The risk committee should obtain appropriate assurance that controls are in place and are effective in addressing IT risks in areas that are highly dependent on IT.</li> <li>The audit committee should consider IT as it relates to financial reporting and the going concern status of the company.</li> <li>The audit committee should consider the use of IT to improve audit coverage and efficiency.</li> </ul>	<ul style="list-style-type: none"> <li>IT risks should be covered as part of the ERM process.</li> <li>IT should be on the agenda of both the risk and audit committee meetings.</li> <li>Continuous auditing techniques to obtain assurance throughout the year should be considered.</li> </ul>

## Putting principles into practice

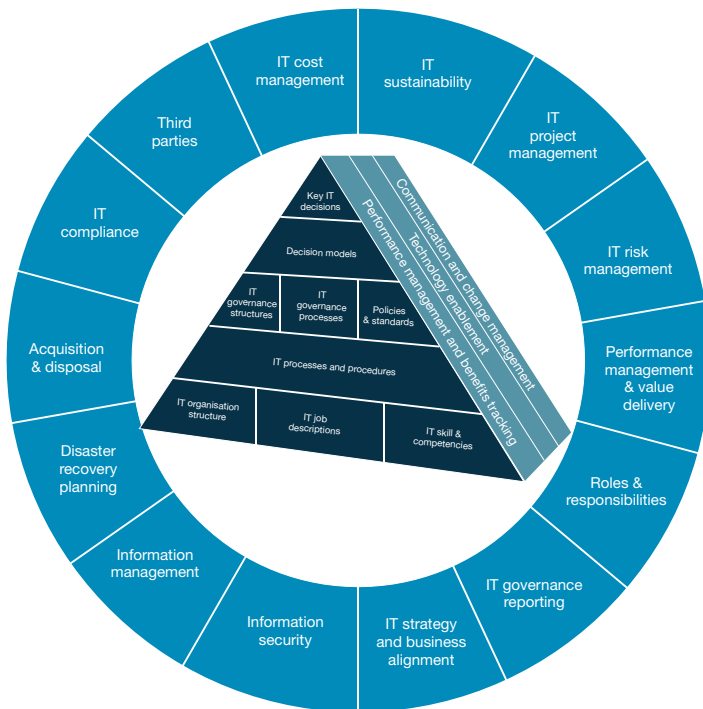
While King III sets out a number of principles, the immediate challenge is to implement them in a practical and efficient way.

Fortunately, King III recognises that every organisation is different and the Code's governance framework encourages entities to tailor application of its principles to the size, nature and complexity of the organisation. From this perspective, it is up to each organisation to determine, for example, what an IT governance framework is, how it is implemented and how it is monitored.

Nevertheless, there are a number of common areas that should be focussed on within every organisation and the appropriate structures, processes, policies and standards put in place for these.

PricewaterhouseCoopers (PwC) has developed a framework for IT governance and controls that reflects these core focus areas, which are illustrated below.

### PwC IT governance and control framework



Each one of the areas depicted in the diagram can be linked back to the principles and recommendations of King III. They therefore provide a handy checklist of priority issues to be addressed.

## IT governance and control framework

An IT governance and control framework should provide the structure, processes and controls required to govern IT. It should also provide overall policies as well as guidance over how IT is run and managed (as without being able to effectively manage, the organisation won't be able to govern).

The central philosophy of King III concerns leadership, sustainability and corporate citizenship. In the area of IT governance, this requires ensuring that decisions are being made by the right people, with access to the right information and the right processes, and with appropriate structures in place to support decision making in order to ensure that IT:

- Delivers value;
- Complies to laws, rules and regulations;
- Risk are managed; and
- Resources are managed efficiently (do not result in unnecessary cost).

PwC's IT governance and control framework outlines the decision makers (and their accountabilities and responsibilities), processes, structures and underlying policies, controls and standards which support this framework. In order to provide confidence to the board that IT is being properly governed, we believe it is essential to understand, evaluate and account for activities within every area of the framework.

The starting point of an IT governance and control framework is the determination of the key IT decisions that need to be made within the organisation, considering requirements from the perspective of both the internal and external environment (such as stakeholder requirements, legislation, market factors etc).

These key IT decisions could include, amongst others, decisions relating to:

- IT Strategy;
- IT Architecture;
- Sourcing;
- Applications;
- Infrastructure;
- Security; and
- Projects.

Once the key IT decisions have been identified, the involvement of various stakeholders and entities has to be determined. This is necessary to ensure that all decisions are 'owned' by relevant stakeholders. Examples of these stakeholders include the board, executive management, business process owners, heads of business units and IT management.

IT governance structures should facilitate the optimal involvement of the right stakeholders (such as board, board committees etc) in the decision-making process and should be dependent on the way in which an organisation is structured (centralised or decentralised). These structures could include the establishment of, for example, centralised and decentralised steering committees, investment committees and their charters.

Essential IT governance processes, such as how IT risks are managed, how investment appraisals are determined and how architecture exceptions are handled, can be defined by these stakeholder groups.

One of the key mechanisms for enforcing IT governance compliance is to have the right IT rules – policies and standards – in place. These policies and standards will include various security and end-user policies as well technical and product standards.

A holistic IT governance view should include an interface with more operational IT aspects, such as IT processes, procedures and controls, IT organisational structures and required roles, skills and competencies. These operational IT aspects are mostly covered by best practices, such as CobiT, CMMI, ITIL, ISO17799, and ISO27001. Without alignment of IT governance decision structures and the operational IT environment, IT cannot be managed and governed effectively.

By adopting a holistic IT governance framework, organisations will not only establish a solid foundation from which to meet the provisions of King III, but also tangible benefits that extend way beyond proving compliance.

## IT governance reporting

King III notes in a number of recommendations that IT needs to report to the board and/or that the board is responsible for the governance of IT, in which case reporting to the board is required. The CIO or similar type of function (dependent on the criticality of IT to the business), should prepare regular reports to the board, which should as a minimum cover:

- Value derived from IT, measured in a quantitative and qualitative way;
- IT risks;
- IT security and continuity, including data protection;
- IT projects;
- IT cost and major investments;
- IT strategy and progress on IT strategy plan; and
- IT governance and controls.

## Information security

From the perspective of King III, it is important to ensure that sensitive information is properly secured and that security is being utilised in order to comply with rules and regulations. Sensitive information might be related to company-specific data, which is critical for business purposes, but also customer and personal data. While sensitive information might reside on IT systems, it should also not be overlooked that a lot of information may also be kept or stored outside the systems.

Firstly, information security requires the identification of two important elements:

- What data needs to be protected ; and
- How much protection is required.

Information classification combined with a risk and vulnerability assessment is therefore advisable.

Secondly, the appropriate way to protect the company information needs to be identified. Mechanisms to secure information can, for example, be a combination of the following:

- Identity and access management;
- Application security;
- Information and database security;
- Physical security;
- Remote access and internet security;
- Internet security;
- Security policies, standards and guidelines; and
- Security governance structures.

Thirdly, once security mechanisms have been put in place, it is very important to monitor the effectiveness of these and to ensure processes have been put in place to handle security incidents and to continuously improve security and amend security requirements to meet new legal, regulatory, vulnerability and business needs.

A strategy should be compiled to determine the organisation's long-term security requirements, taking into account ever-changing business requirements and demands. Procedures to report to the board or appropriate committees will also need to be put in place.

## IT compliance

Depending on the industries and geographies a company operates in, different legislative and regulatory requirements will need to be adhered to. The impact of these on the IT environment needs to be assessed and systems developed in order to ensure and monitor compliance.

Some of the laws and regulations that have an impact on IT governance include:

- Financial Intelligence Centre Act (FICA);
- Regulation of Interception of Communications Act (RICA);
- Protection of Personal Information Bill;
- The South African Electronic Communications and Transactions Act, 2002 (ECT Act);
- The Payment Card Industry (PCI) Data Security Standard
- The Sarbanes-Oxley Act (SOX)

After determining compliance requirements, it should also be determined in what ways IT can support compliance. Compliance mechanisms, controls and monitoring activities will need to be determined and reported upon. In the end, IT compliance will never be a once-off action, but an ongoing process which should be embedded into the organisation's procedures and operations.

## Added benefits of sound IT governance

King III is concerned not just with IT governance, risks and controls, but with effective IT management. While this may appear daunting to some, it offers tangible benefits that extend well beyond proving compliance. These include:

- Clarified decision making and accountability;
- Improved understanding of overall IT costs and their input to ROI cases;
- Improved risk management, security, efficiency and effectiveness of IT and making this visible (i.e. IT will deliver value);
- Enhancement and protection of reputation and image;
- Positioning of IT as a business partner and clarifying IT's role in the business;
- Improved and more professional relationships with key IT partners (vendors and suppliers);
- Improved responsiveness to market challenges and opportunities;
- Clear identification of whether an IT service or project supports 'business as usual' or is intended to provide future added value;
- A focus on performance improvement that will lead to the attainment of best practices;
- Avoidance of unnecessary expenditure as spending can be demonstrably matched to business goals; and
- Enabling an integrated approach to meeting external legal and regulatory requirements.

## Critical factors for a successful implementation

Once an organisation has recognised the all-encompassing function of IT governance, the challenge will be to follow a roadmap which provides a flexible approach to achieve its IT governance ambitions, and to use this step-by-step approach to achieve quick wins where possible.

There are several levels of maturity of an IT governance implementation and each organisation's necessary level of maturity will depend on the internal and external requirements of that organisation.

While implementing an IT governance programme, it is important to keep in mind that the definition of decision models, decision structures and decision processes should be aligned to the culture and function of the IT function within the organisation. If these are not aligned, implementation will be a time-consuming process as it inherently necessitates changes in operational IT processes. Adequate change management is of vital importance to the success of an IT governance implementation.

In our experience, a 'big bang' approach to implementation will in all likelihood fail and will not deliver the required benefits of IT governance. We recommend a number of general implementation guidelines, which should be adjusted depending on the organisation's specific requirements:

- Ensure senior management commitment and vision;
- Set achievable targets and expectations;
- Define a benefit management system;
- Identify your current maturity level;
- Value communication as a critical success factor;
- Focus, execute, enforce;
- Link IT governance to key business themes; and
- Don't over-engineer IT governance.

## Ensure senior management commitment and vision

Before starting to implement areas of the IT governance framework, an organisation should ensure that there is broad senior management commitment and vision, including a company-specific definition of IT governance. IT governance initiatives should be initiated by top management in the organisation. It is important that this support is sustained and that IT governance is part of the strategic vision of all senior managers to ensure the adequate availability of resources and the support for good IT governance practices during conflict situations.

## Set achievable targets and expectations

Once IT governance has been established as an important initiative driven by an organisation's senior management, an organisation needs to broaden its vision for the expected outcomes of its IT governance activities. It is absolutely crucial to set achievable targets and expectations that are well understood by senior management and all stakeholders.

## Define a benefit management system

Besides defining the objectives of an IT governance programme, an organisation should also define a benefit management system that can be used to measure the new IT governance targets. Don't forget that IT governance is about improving the value of IT to the organisation and reducing risk. Introducing IT governance practices without putting in place a system that includes the definition of expected benefits and how they will be measured is a contradiction in terms.

## Identify your current maturity level

An 'as-is' analysis is required to measure how IT currently provides the leadership, organisational structures and processes to enable business strategy. This maturity assessment covers all relevant aspects of the governance framework, so it is vital that the organisation honestly outlines its real maturity status. It is crucial to get the right

people from the business involved in this analysis phase. Remember, IT governance is not an IT issue; it is a business issue with implications for the entire organisation. The maturity assessment should set a target maturity level that an organisation intends to achieve through its IT governance activities.

The maturity assessment will identify all essential areas requiring improvement so that a roadmap for improvement can be developed. This roadmap should include all necessary activities, work packages, people and responsibilities required to move the organisation up the IT governance maturity scale. Success can only be achieved if focus is maintained and agreed practices are executed according to schedule.

### **Value communication as a critical success factor**

The roadmap defined for improving IT governance provides an integrated view of the activities that will need to be undertaken to achieve the agreed IT governance targets and augment the maturity of the organisation's IT governance. The improvement project itself should be accompanied by strong communication and change management activities. In most cases where more robust IT governance practices are introduced, some level of resistance will be encountered. We see successful clients as being those that recognise the importance of continued communication, especially where strong resistance is encountered or when exceptions need to be dealt with.

Sponsorship by senior management is required for all of these communication and change management activities. Once it is agreed to introduce or to improve IT governance, they will need to continue to drive the initiative forward in order to realise the expected results and benefits.

### **Focus, execute, enforce**

If technology standardisation is established as one of the cornerstones of IT governance, it is important to establish a strict exception management process for relevant deviations from standards. This provides a documented and structured mechanism for stakeholders (e.g. project sponsors or business unit management) to outline their case and request exceptions. At this stage of the project, various dimensions of IT governance will be approached in parallel, but focussing on the 'weakest link' or 'quick win' will show results and gain further project acceptance.

### **Link IT governance to key business themes**

The timeline for improving an organisation's IT governance maturity will differ depending on its current maturity level, the range of targets, the people who are able to contribute and how these activities are supported by senior management.

In our experience, realising IT governance improvements is a continuous process in which major improvements are established in the first couple of years. Taking this timeframe into account, it seems obvious that there will be many concurrent activities in an organisation which require commitment, people, budget etc. The easiest way to address these challenges is to link IT governance to the key business themes, such as cost reduction, innovation, agility, simplification, customer satisfaction, deal value, sourcing, compliance and risk management. Only then will the business and IT function be able to speak the same language. Both the IT function and the business should demonstrate that it is ready to align itself with the other. This will ensure that the business appreciates and provides active support to IT governance initiatives.

An organisation should also try to take advantage of other projects, like a merger or acquisition, corporate governance initiatives, establishment of a shared service centre or sourcing arrangement as an occasion to question the IT governance arrangements it has in place. Independent of whether the organisation is able or willing to link IT governance activities to business initiatives, it should be seen as a long journey rather than a short visit.

### **Don't over-engineer IT Governance**

We have advised a number of clients after the failure of their efforts to establish an IT governance programme. A major reason for failure has been that they tried to set up a structure that was too complex to achieve their targets. IT governance should not be over-engineered. While IT governance measures are key to the success of IT within the organisation, it is important not to overdo the effort with multiple committees or elaborate monitoring and reporting. A convoluted IT governance implementation will create more resistance in the organisation and ultimately be circumvented. In contrast, introducing IT governance practices wisely should enable rather than impede the flexibility of processes and procedures.

## Our Services

PricewaterhouseCoopers (PwC) has a global IT governance network with a strong presence in South Africa. The network develops and shares best practices (based on client experiences around the world), thought leadership, IT governance accelerators for implementation, assessment tools (against CobiT, ITIL, King III and PwC best practices) and implementation guidelines and approaches, which can be utilised in any client environment to accelerate the implementation of IT governance in a practical way.

Our South African experience includes:

- Our global leadership role in the development of the PricewaterhouseCoopers IT governance framework, methodologies, assessment tools and best practices;
- Our involvement in the development of King III;
- Our involvement in the global development of CobiT;
- Our tools and methodologies, which can accelerate the implementation of IT governance.
- PwC's extensive range of IT governance services includes:
  - IT governance assessment against King III and benchmarking against other organisations;
  - Practical implementations and improvements of IT governance utilising our extensive knowledge;
  - CobiT and ITIL assessments and implementations;
  - IT risk assessments, risk management design and implementations;
  - Security reviews and implementations;
  - IT value delivery, benefits tracking and cost management design and implementations;
  - IT performance assessments and benchmarking;
  - IT organisational design and implementations;
  - IT compliance assessments, design and implementations;
  - IT processes, policies, standards and control design and implementations;
  - Project management;
  - Project implementation assurance; and
  - Disaster recovery and business continuity management.

## Contacts

### Gauteng

[Angeli Hoekstra](#)

Director

Global IT Governance Leader

+27 (0) 11 797 4162

[angeli.hoekstra@za.pwc.com](mailto:angeli.hoekstra@za.pwc.com)

### KwaZulu-Natal

[Binesh Rajkaran](#)

Director

+27 (0) 31 271 2016

[binesh.rajkaran@za.pwc.com](mailto:binesh.rajkaran@za.pwc.com)

### Western Cape

[John Wilkinson](#)

Director

+27 (0) 21 529 2086

[john.wilkinson@za.pwc.com](mailto:john.wilkinson@za.pwc.com)

### Eastern Cape

[Zahid Fakey](#)

Director

+27 (0) 31 271 2022

[zahid.fakey@za.pwc.com](mailto:zahid.fakey@za.pwc.com)

### Central Region

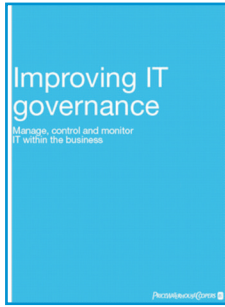
[Rudolph Laubscher](#)

Associate Director

+27 (0) 51 503 4100

[rudolph.laubscher@za.pwc.com](mailto:rudolph.laubscher@za.pwc.com)

## IT Publications



The pervasiveness of IT within most commercial and public organisations has placed increasing pressure on managing IT in order to reduce IT risks and enhance business value. The current IT organisation is embedded in the business environment and requires regulatory compliance, cost control, availability, risk management, business alignment of IT, timely project delivery, change and innovation in order to deliver stakeholder value.



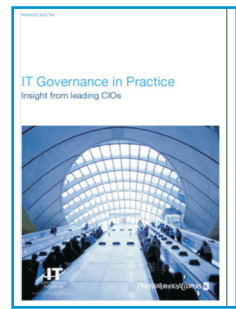
In 2007, PricewaterhouseCoopers was commissioned by the IT Governance Institute (ITGI) to conduct the third Global Survey on IT Governance, resulting in this report, which focuses on these objectives:

- Survey and analyse the degree to which the concept of IT governance is recognised, established and accepted within boardrooms and especially by chief information officers;
- Determine what level of IT governance expertise exists and which frameworks are known and are (or will be) adopted; and
- Measure the extent to which ITGI's own framework, Control Objectives for Information and related Technology (COBIT), is selected and how it is perceived.



This position paper explores two forces, generic IT and strategic value; and provides a framework for the design of a strategy to handle them. Every enterprise is different, so there is no one right strategy. But by understanding the forces themselves and their implications for the CIO, an organisation should be able to fashion an intelligent strategy.

PwC interviewed a number of CIOs around the world to obtain their views on IT governance, their experience in implementing IT governance programmes, and on what it takes to make IT governance work.



IT is gaining in importance for companies and becoming a real competitive success factor. However, as levels of utilisation and cost increase, this does not necessarily translate into a higher value contribution. This study investigate IT investment costs and the value orientation of IT in seven industries.



Managing your cost base is fundamental to managing through the downturn. In the majority of organisations, IT is a significant cost. As companies look to achieve significant, rapid reductions, the IT function is coming under increasing pressure. This paper explores our approach to cost reduction, which is underpinned by a framework that addresses strategy, structure, people, processes as well as technology. By looking at all five dimensions, we can help you to identify tangible, sustainable opportunities to reduce cost and support the delivery of an IT service which genuinely supports value creation and provides a flexible platform for supporting future growth.



Today, in the middle of the worst economic downturn in thirty years, information security has an enormously important role to play. What are the implications of these trends on how your business is addressing the challenges of the economic downturn? What expectations should you be placing on your information security function at this time? Which areas of focus offer the best opportunities for security to provide concrete business value – not just over the long run but right now, during an unusual economic period? Find out in this 2010 global state of information security survey.



For further information on these and other publications, please contact your engagement partner or the PricewaterhouseCoopers library at +27 (0) 11 797 5062.

