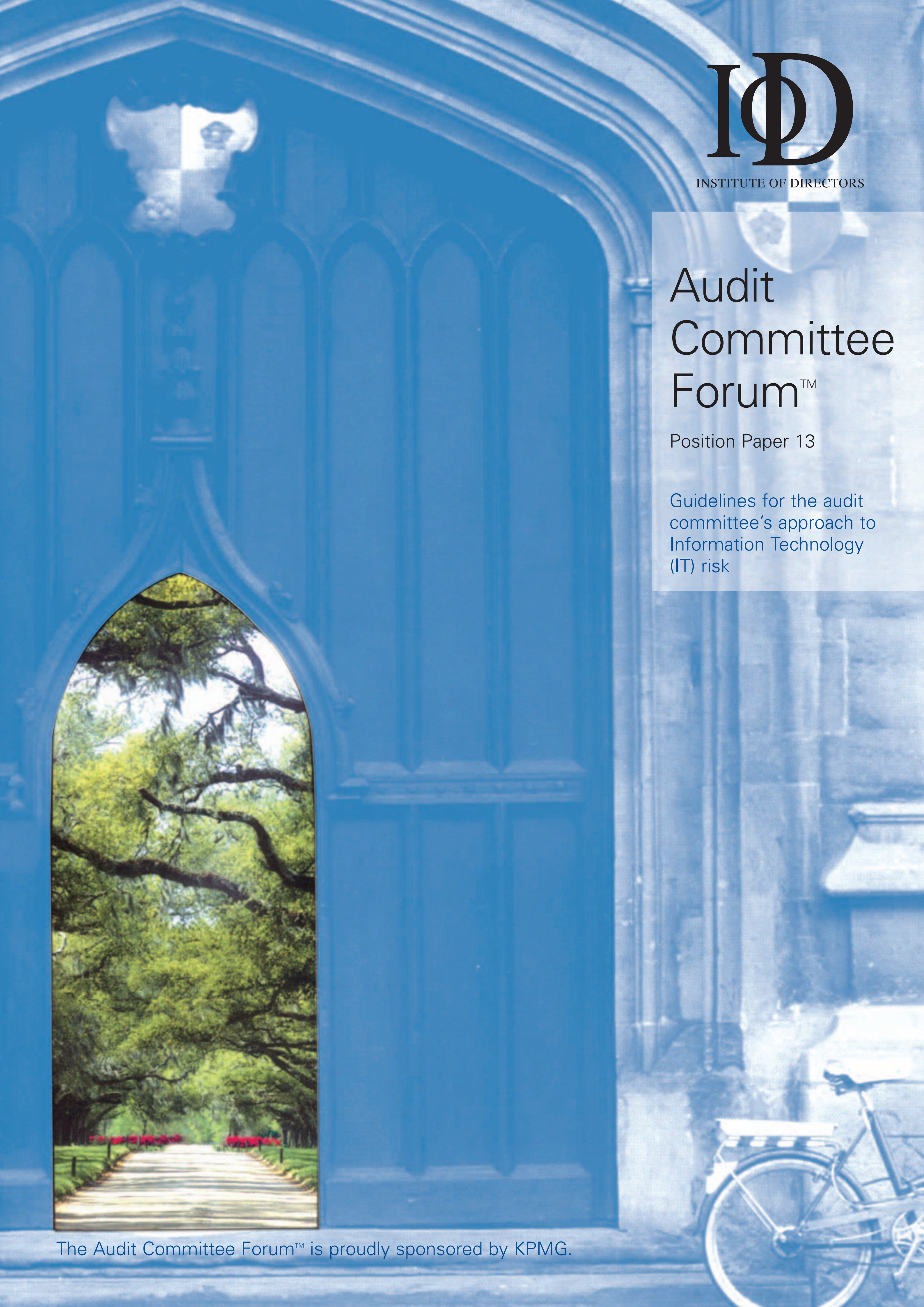


IoD

INSTITUTE OF DIRECTORS

Audit Committee Forum™

Position Paper 13

Guidelines for the audit committee's approach to Information Technology (IT) risk

The Audit Committee Forum™ is proudly sponsored by KPMG.

Guidelines for the audit committee's approach to Information Technology (IT) risk.

The information contained in Position Papers disseminated by the Audit Committee Forum™ is of a general nature and is not intended to address the circumstances of any particular individual or entity. The views and opinions of the Forum do not necessarily represent the views and opinions of KPMG, the Institute of Directors and/or individual members. These guidelines are for discussion purposes only and in considering these issues the culture of each entity should be taken into account as must the charter for each entity's audit committee. Although every endeavour is made to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No reliance should be placed on these guidelines, nor should any action be taken without first obtaining appropriate professional advice. The Audit Committee Forum™ shall not be liable for any loss or damage, whether direct, indirect, consequential or otherwise which may be suffered, arising from any cause in connection with anything done or not done pursuant to the information presented herein.

Introduction

IT governance is a "framework that supports the effective and efficient management of information resources (e.g. people, funding and information) to facilitate the achievement of corporate objectives. The focus is on the measurement and management of IT performance to ensure that the risks and costs associated with IT are appropriately controlled."[1]

"IT governance is the responsibility of the board of directors and executive management. It is an integral part of corporate governance and consists of the leadership and organisational structures and process that ensures that the organisation's IT sustains and extends the organisation's strategies and objectives."[2]

The Audit Committee Forum™ is aware that corporate governance structures are not the same in every entity. Governance principles should be applied and structured to best suit the size and complexity of the entity, including IT governance. This position paper is written on the basis that the audit committee is responsible for the oversight of risk management and that a separate risk committee does not exist (please refer to position paper 6 for *The Role of the audit committee in respect of Risk Monitoring* for more detail on this topic).

The audit committee, however, is always responsible for oversight of internal controls, including IT general and application controls. This oversight function involves ensuring the entity has an appropriate controls framework in place, the controls are appropriately documented and that systems are in place to ensure the controls operate effectively.

The role of the audit committee

Information Technology (IT) plays an ever-increasingly important role in supporting business processes and enabling entities to differentiate themselves in the marketplace.
In addition, increasing reliance is being placed on systems and other automated control processes to manage risk. Questions have been raised regarding the role of the audit committee in monitoring increased IT risks.

In most governance structures the board of directors is responsible for the strategic direction and decisions regarding IT and the audit committee is responsible for the oversight of certain strategic and operational aspects of IT, particularly IT risks.

The results of the Second Annual Audit Committee Institute[3] survey showed that the 1 343 respondents across the globe were of the view that audit committees today are overseeing various aspects of their company's Information Technology but that audit committees and boards should be doing more in this area.

[1] Ken Doughty and Frank Grieco, "IT Governance: Pass or Fail?" Information Systems Control Journal 2, 2005.

[2] Board Briefing on IT Governance, 2nd Edition, IT Governance Institute

[3] Audit Committee Institute Annual Survey November 2006.

Following the introduction of the review requirements of Sarbanes-Oxley Act in the United States the majority of governance failures related to IT.

The audit committee should, in the case of all entities, determine whether IT plays a critical role. The aspects in which audit committees play an oversight role as per the responses include:

- IT risks and controls: 66% of audit committee members responded that they have oversight of IT risks and controls.
- Business continuity and data recovery related to IT: more than 50% of respondents overall and 80% in South Africa stated the oversight of business continuity as a role of the audit committee.
- Information security and privacy: 48% audit committee members stated that information security and privacy was part of their IT governance role.

IT risks and controls

Audit committees should consider IT risk as a crucial element of the effective oversight of risk management of the entity. However, audit committee members should assess if they are adequately equipped with the specialist technical know-how necessary to review and analyse the effectiveness of systems and systems controls. In many cases the audit committee may need to rely on expert advice from within or outside the entity.

In understanding and measuring IT risks the members of the audit committee should understand the entity's overall exposure to IT risks from a business perspective including the areas of the business which are most dependent on IT for their effective and continual operation.

Areas that are highly dependent on IT are more exposed if IT risks are not appropriately governed and the audit committee would need to obtain appropriate assurance that controls are adequate to address these risks.

The most widely adopted framework audit committees use in the oversight of IT risks and controls is the COBIT (Control Objectives over Information Technology) model. This model focuses on 34 control objectives to ensure that IT controls satisfy business requirements. Please refer to Appendix A for an overview of the COBIT control objectives.

Some of the main IT risks facing entities are listed below.

- IT outsourcing: Increasingly, entities are outsourcing their IT structures and systems. This in turn creates additional concerns for effective IT risk management. Questions the audit committee can ask to assess the risk include:
  - Does the entity have an appropriate Service Level Agreement (SLA) with the service organisation?

- Has the SLA been interrogated sufficiently and reviewed by relevant specialists, including legal?
- Is the SLA sufficiently comprehensive and being complied with? (Often audit committees request a compliance audit of the SLA for this purpose).
- Has the entity requested a report from the service organisation's auditors confirming the effective operation of IT controls at the service organisation (a 'SAS70-type' report)?

■ Enterprise Resource Planning systems: These planning systems are increasingly becoming more complex and costly to implement. The key risks include:

- overall project failure;
- projects running over budget and time;
- failure to deliver the expected return on investment; and
- insufficient administrative and management skills.

■ System changes and implementation: Often the process of software changes and implementation of new systems result in increased IT-related risks. These risks include the selection of the appropriate software, the appropriate implementation process and the integrity of information. The audit committee, although not responsible for the decision for system changes and implementation, should ensure that the process for establishing the needs assessment is rigorous and that adequate planning is undertaken for the change or conversion.

Refer to Appendix B for detailed questions the audit committee can use to evaluate the risks of system changes and implementation.

■ Tailor-made software increases the risk to the entity significantly, as the entity ordinarily does not have access to the source codes, i.e. subsequent changes cannot be made or the initial developer no longer exists. A practical solution to this issue is to place the codes in escrow to ensure that access to the source codes will be maintained.

It is also vital that internal audit be involved before and after implementing a new system or changing an existing system.

■ Access is one of the most problematic areas in a modern business environment driven by and highly dependent on IT. Some of the areas of concern include:

- Lack of discipline in changing and protecting passwords;
- Inappropriate access levels assigned to staff which allows for abuse of information;

- Lack of discipline in removing access of previous employees;
- Remote access to information through Wi-Fi and Broadband networks;
- Inappropriate access and authority of super-users. Companies should maintain an updated register of all super-users with the various access levels assigned to them.

Business continuity related to IT

The reliance on IT has raised the stakes in terms of disaster recovery planning. It is important that the audit committee question management with regards to the business continuity plan as part of the oversight role. Some of the questions audit committees can ask management include:

- How critical is the IT system to the business?
- What is the plan for dealing with a significant business interruption?
- What types of interruptions does the business continuity plan cater for?
- When last was the business continuity plan tested under normal operating conditions?
- Which areas of the plan did not work as expected and what alternative plans were made?
- Is the backup capacity sufficient?
- What is the cost of redundancy of the system?
- How long will the recovery take and what will the cost to the entity be?
- Does the entity have adequate insurance in cases of disaster and loss of information?
- Is there confirmation of business continuity at least annually, either through external or internal audit?

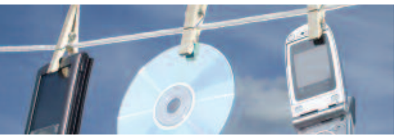
Information security and privacy

Rapid technological advances have led to instantaneous availability of information, often across several geographical locations. The uses of removable storage devices and mobile e-mail solutions have increased the risk of unauthorised access to sensitive and confidential company information.

Questions the audit committee may ask of management to assess the entity' security levels include:

- Does the audit committee receive regular feedback regarding network violations?
  - When was the last occasion a network violation was reported?
  - What was the nature of the last network violation?
  - What was the impact of the last violation?
  - What measures were implemented to secure the network after the last violation?

> "The reliance on IT has raised the stakes in terms of disaster recovery planning."



- Has the entity used outside providers to perform security testing and what has changed as a result?
- Do all electronic messages contain a disclaimer policy?
- Has the entity developed and communicated policies regarding the use of non-entity specific software?
- Is there appropriate and timely cleansing of data prior to staff exiting?
- Does the entity abide by licensing agreements and are the agreements reviewed on a regular basis and confirmed independently?
- How much critical information if derived directly from the system and how much rework is required?

Action plan for audit committees

Management is responsible for identifying risks and subsequently developing, assessing and monitoring appropriate internal controls. The Chief Financial Officer, Chief Executive Officer and Chief Information Officer should provide the relevant assurance regarding IT risks and controls to the audit committee. If the audit committee has been charged with oversight of risks it should ensure that management is performing ongoing assessments of all IT risks. If the audit committee is not charged with the oversight of IT risks, it should satisfy itself that these risks are adequately addressed in light of the risk management structures in place at the entity.

The audit committee's oversight of IT risks can be facilitated through the following steps:

Updating the audit committee charter

Audit committees and boards need to align their oversight responsibilities for IT governance and agree on an arrangement that makes the most sense for culture and governance structure of the company. This should clearly be addressed in the charter of the board and the audit committee.

Utilise direct access to the Chief Information Officer

Through presentations by the business unit heads and the Chief Information Officer (CIO), or equivalent IT executive, it is possible for the audit committee to understand from a business perspective how IT is being utilised in the business, how it could be utilised in other areas of the business and what the potential exposure to the whole business is from IT.

The audit committee should receive a comprehensive plan from the CIO, or equivalent, regarding his or her assessment of the IT function and any key weaknesses in IT controls. This assessment, together with independent assurance from internal and external audit, should provide the audit committee with assurance that IT is being properly managed that IT risks are being controlled. The audit committee may request the Chief Information Officer to sign a representation letter that IT risks within the entity are identified and adequately controlled.

Utilise internal audit support

The internal audit function normally has a degree of IT knowledge and sophistication consistent with the types of IT risks faced by the entity. The internal audit function should be utilised extensively in testing controls. Where the internal audit function does not comprise the necessary appropriate IT skills and knowledge, the audit committee should consider the need for outsourcing this assessment.

Internal audit could be utilised to answer the following questions for the audit committee:

- What is the level of reliance on IT personnel, considering both key reliance and level of skill? [People risk]
- How is the entity's management securing data? [Information risk]
- How reliable are the IT systems (both applications and infrastructure)? [Integrity of information and Availability risk]
- What is the level of dependency on IT managed by third parties and how is the entity managing those risks? [Outsourcing risk]
- What regulation/legislation applies to IT and how can IT help the entity comply with relevant regulations and legislation? [Legal risk]
- Are you aware of all changes to the IT system and are these conversions monitored? How much change is being effected (and managed) on the IT structure of the entity [Change and project management risk]
- Is the internal control environment such that internal audit can supply the audit committee with a representation?

Utilise external audit support

In the modern complex business environment, the external audit cannot be performed without an assessment of IT controls (both general and application). The audit committee should receive comfort from the external auditor regarding the IT risks and controls that were assessed as part of the external audit process. The audit committee should obtain an understanding of the extent of IT-related testing and evaluation performed by the external auditor as the criticality of IT should result in additional work in the area. Questions the audit committee may ask include:

- How much reliance is the external auditor placing on the IT system?
- How often has the external auditor defaulted to substantive testing to gather audit evidence?

Adopt a framework for assessing IT risks

As discussed in the preceding section, the COBIT model is one of the possibilities. The COBIT framework and other frameworks, allow for effective and efficient risk management with objective quantifiable assessment of all significant IT risks (as referred to in Appendix A).

Communication

Once management has assessed and mitigated the key IT risks by designing and implementing appropriate controls, the audit committee (with the help of internal audit or other independent services providers) should critically review the IT risk assessment and the designated controls. This broader perspective may be useful in identifying gaps in IT controls.

The audit committee should also receive feedback from both the internal and external audit processes with regards to IT risks and weaknesses in internal controls. The audit committee should review the coverage over IT controls by both internal and external audit and consider if this is sufficiently comprehensive and appropriate to provide the necessary assurance.

[4] The IT Governance Institute; COBIT 4.1; http://www.isaca.org/AMTemplate.cfm?Section=Downloads&Template=/ContentManagement/ContentDisplay.cfm&ContentID=34172

Appendix A[4]

The COBIT framework provides a reference process model and common language for everyone in an enterprise to view and manage IT activities. Incorporating an operational model and a common language for all parts of the business involved in IT is one of the most important and initial steps toward good governance. It also provides a framework for measuring and monitoring IT performance, communicating with service providers and integrating best management practices. A process model encourages process ownership, enabling responsibilities and accountability to be defined.

To govern IT effectively, it is important to appreciate the activities and risks within IT that need to be managed. They are usually ordered into the responsibility domains of plan, build, run and monitor.

Plan and Organise (PO)

This domain covers strategy and tactics, and concerns the identification of the way IT can best contribute to the achievement of the business objectives. The realisation of the strategic vision needs to be planned, communicated and managed for different perspectives. A proper organisation as well as technological infrastructure should be put in place. This domain typically addresses the following management questions:

- Are IT and the business strategy aligned?
- Is the enterprise achieving optimum use of its resources?
- Does everyone in the organisation understand the IT objectives?
- Are IT risks understood and being managed?
- Is the quality of IT systems appropriate for business needs?

Acquire and Implement (A)

To realise the IT strategy, IT solutions need to be identified, developed or acquired, as well as implemented and integrated into the business process. In addition, changes in and maintenance of existing systems are covered by this domain to make sure the solutions continue to meet business objectives. This domain typically addresses the following management questions:

- Are new projects likely to deliver solutions that meet business needs?
- Are new projects likely to be delivered on time and within budget?
- Will the new systems work properly when implemented?
- Will changes be made without upsetting current business operations?

Deliver and Support (DS)

This domain is concerned with the actual delivery of required services, which includes service delivery, management of security and continuity, service support for users, and management of data and operational facilities. It typically addresses the following management questions:

- Are IT services being delivered in line with business priorities?
- Are IT costs optimised?
- Is the workforce able to use the IT systems productively and safely?
- Are adequate confidentiality, integrity and availability in place for information security?

Monitor and Evaluate (ME)

All IT processes need to be regularly assessed over time for their quality and compliance with control requirements. This domain addresses performance management, monitoring of internal control, regulatory compliance and governance. It typically addresses the following management questions:

- Is IT's performance measured to detect problems before it is too late?
- Does management ensure that internal controls are effective and efficient?
- Can IT performance be linked back to business goals?
- Are adequate confidentiality, integrity and availability controls in place for information security?

Appendix B

The audit committee may request the internal audit department or CIO to use this questionnaire to ensure that IT risks are appropriately addressed. Feedback on these questions, and the questions listed in the position paper, should be provided to the audit committee to assist in its oversight responsibility.

1 Information systems

1.1 Computer controls (Group IT)

1.1.1 Is the disaster recovery plan for each site updated for all significant changes?

1.1.2 Is the DRP tested at least annually?

1.1.3 Does IT ensure that the backups at all sites are in fact up to date and tested?

1.1.4 Does IT check that the UPS's (uninterrupted power supply) are subject to regular services and logged?

1.1.5 Does IT check that the computer rooms meet the documented minimum standards?

1.1.6 Is the computer room temperature maintained at 20^{0}C or less?

1.1.7 Is virus-checking software loaded on all users that link to the internet?

1.1.8 Is the virus checking software loaded and maintained centrally and updated automatically daily?

1.2 Logical access

1.2.1 Are the password standards enforced using the operating system?

1.2.2 Is single sign-on used where possible?

1.2.3 Does each application enforce regular changes of passwords where they are unique to the application?

1.2.4 Does each application support the password standards?

1.2.5 Does the system enforce password changes when first logging on?

1.2.6 When users leave or are transferred, are the user profiles updated?

1.2.7 Is there an audit trail of all updates to user profiles?

1.2.8 Is this file backed up and archived?

1.3 Change control

1.3.1 Are there appropriate controls to prevent users from downloading software to the servers from the Internet, or introducing unauthorised software from CD's?

1.3.2 Are there controls to ensure that the most recent patches are updated immediately? (Unix, NT, applications, virus definitions, database)

1.3.3 Are there appropriate controls to ensure that only legal/authorised devices are added or linked to the network?

1.3.4 Are there adequate controls to ensure that only authorised persons have remote access to the company network?

1.3.5 Are there controls to ensure that old or inefficient devices are timeously removed or replaced?

1.3.6 Are requests responded to by the service organisation in terms of the relevant SLA?

1.4 Physical security and controls

1.4.1 Is the computer room adequately secured? Do the outsourcers keep the room locked?

1.4.2 Is the computer room accessed with the use of an access code?

1.4.3 Are the servers connected to a UPS?

1.4.4 Is the UPS serviced and tested at least twice annually?

1.4.5 Is the record of the service logged in a register in the computer room or on the UPS?

1.4.6 Is the room adequately protected against fire by either fire extinguishers or gas release devices?

1.4.7 Is the fire extinguishing service regularly serviced and a note made thereof?

1.4.8 Are back-ups made regularly at all sites in accordance with the documented standards?

1.4.9 Are the back ups properly labelled thus preventing overwriting?

1.4.10 Are the backups regularly tested and verified to ensure that the data is recoverable and complete?

1.4.11 Are the back-ups stored in fireproof safes in a building remoted from the computer room?

1.4.12 Is the backup register backed up and stored offsite with the appropriate version of the backup software?

1.4.13 Is the register of computers and IT devices up to date and properly maintained?

1.4.14 Is the asset register (IT Assets) adequately backed up and secured?

1.5 Logical access

1.5.1 Is there a documented standard for user profiles?

1.5.2 Do management review user profiles on a regular basis to ensure adequate segregation of incompatible functions?

1.5.3 Are passwords changed on a regular basis? Is this enforced by the system?

1.5.2 When users leave, or are transferred, are

a They removed from the system when leaving?

b User profiles updated and old functions removed when the users change roles?

1.6 Change control

1.6.1 Are all user problems logged with the Call Centre and a log number documented?

1.6.2 Are only changes that have been approved appropriately implemented?

1.6.3 Are you able to track the status of the change requests or help calls?

1.6.4 Are all open calls reviewed on a weekly basis?

1.6.5 Are there controls in place to ensure that all software changes are documented?

1.6.6 Are all changes loaded to a test system and fully tested by users before the change is implemented?

Contact details:

Lindie Engelbrecht
ACF National Co-ordinator
011 647 8778 or lindie.engelbrecht@kpmg.co.za