



THE Bidvest GROUP LIMITED

Information Technology ('IT') Governance Framework

1. INTRODUCTION

The Board of Directors of The Bidvest Group Limited ("the Company") acknowledges the need for an IT Governance Framework as recommended in the Code of Governance Principles for South Africa ("King III").

2. PURPOSE OF THE IT GOVERNANCE FRAMEWORK

*IT Governance Framework is created in order to "support the effective and efficient management of information resources (e.g. people, funding and information) to facilitate the achievement of the organisations objectives. The focus of this framework is on the measurement and management of IT performance to ensure that the risks and costs associated with IT are appropriately controlled."*ⁱ

King III says that "The Board should be responsible for IT governance and should ensure that an IT internal control framework is adopted and implemented". The responsibility for the implementation of this framework should be delegated to management. The Board should monitor and evaluate significant IT investments and expenditure, as well as ensuring that information assets are managed effectively. The risk and audit committee should assist the Board in carrying out its IT responsibilities. IT should form an integral part of the company's risk management.

3. FRAMEWORK ADOPTION

Good governance is largely driven by adopting a process model to use as a guide and establishing a common language for your organisation to manage IT activities.

The Company has adopted the ISACA and IT Governance Institute (ITGI) best practice COBIT standards for IT governance. COBIT provides a set of generally accepted governance measures, indicators, processes and best practices, to assist managers, auditors and IT users in maximising the benefits derived through effective and efficient use of information technology within your organisation.

When reviewing the role IT plays in your organisation, the following high level risk categories should be considered:

People risk: What is your level of reliance on IT personnel, considering both key reliance and level of skill?

Information risk: How is your management team securing data?

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

Integrity of data & availability risk:	How reliable are your IT systems (both applications and infrastructure?) Is your internal control environment such that audit can supply the audit committee with a level of assurance?
Legal risk:	What legislation / regulations are applicable to your IT environment? How can IT help your organisation comply with other relevant regulations / legislation?
Change control and project management risk:	Are you aware of all the changes to your IT system and are these changes monitored? How much change is being effected (and managed) on the IT structure of your organisation?
Outsourcing risk:	What is the level of dependency on IT managed by third parties and are you satisfied with how the third party is managing those risks? Are you satisfied with how your management team is managing that third party providing outsourced IT services?

4. IT dependency and maturity assessments

The decentralised and diversified nature of the Company recognises that IT plays a variety of roles throughout. The adoption and implementation of the COBIT standards should be customised and adapted to meet the needs of your business and/or divisional IT environment.

IT dependency needs analyses are to be performed by your business with the guidance and support of the Group IT Governance team. IT dependencies will be rated as follows:

IT dependency rating:	IT Usage:	What this means:
High	Key operational driver	- Ensure minimum IT policies are in place - Require a full COBIT Maturity assessment - Determine “current” maturity and “required” maturity - Create a plan on how to achieve required maturity level
Low	Administrative support tool	- Ensure minimum IT policies are in place - Plan an IT dependency assessment within the next 12 months

Following the dependency analyses, should your business / division IT dependency be rated 'High', an IT maturity assessment will be required. The *current* level of IT maturity will be assessed, as well as the *required* level of IT maturity to be achieved by your business / division.

The required level of IT maturity will be determined taking into account your business and IT strategy and the extent of exposure to risk as identified by your divisional risk committee. These assessments will be conducted by an independent Group IT Governance specialist.

The level of IT maturity determines the extent of adoption of the COBIT standards as depicted in the table below:

Maturity Levels:	1 Non-existent	2 Initial/ad hoc	3 Repeatable but intuitive	4 Defined	5 Managed & measured	6 Optimised
Status of the internal control environment	There is no need for internal control in this environment.	Some need for internal control – but is disorganised and ad hoc	Controls are in place but up to the individual to perform them. Not documented	Controls are in place and documented but not managed or measured.	Management depends on a robust system of internal control	Enterprise wide risk and control programme provides effective and continuous comfort.
Establishment of internal controls	No intent to establish internal controls	Internal control reviews performed ad hoc usually as a result of an incident	Controls established for specific IT processes as required by IT manager	Critical IT processes are defined and ownership attributed to key role players	IT criticality is regularly defined with full support and agreement from business owners.	Business changes consider the criticality of IT processes. For critical processes independent assurance reviews are performed

Once the current maturity level and the required IT maturity level has been determined, it will be necessary for the responsible officer from the business / division, with the assistance of the Group IT Governance team to create a plan detailing the timing and actions required to achieve the required level of IT maturity.

The rollout and completion of this plan is the responsibility of the business / divisional risk committee, with regular feedback to the boards.

The maturity levels and plan will need to be reviewed annually to ensure that the IT strategy and business strategy of the business / division continue to be aligned and supported through this process.

5. RESPONSIBILITIES

RESPONSIBILITIES	RESPONSIBLE	FREQUENCY
------------------	-------------	-----------

PERSON		
Bidvest Board and Divisional Board responsibilities: • To appoint a group / divisional officer responsible for the management of IT • Ensure alignment of business and IT strategies and clarify the role of IT in achieving these strategies • Approving the IT governance framework • Delegate responsibility for implementing the IT framework to the divisional risk committees • Ensure IT is placed on the group and divisional risk committee agendas and regular feedback is provided to the boards • Review and assign accountability for the organisational changes needed for IT to succeed • The boards must further conclude and report to their stakeholders an assessment regarding the effectiveness of IT governance and management activities, as well as how the boards have achieved this assurance	Chairperson of the board	Annually
Bidvest Group Risk Committee • To assist the boards in the function of IT governance • Determine and communicate levels of IT risk tolerance / appetite • The group risk committee will review the material IT risks as profiled by divisional risk committees and apply its own mind to the completeness of the risks facing the Company • To ensure the IT Maturity assessment has been performed throughout the Company to assess IT maturity levels - both current levels and required levels • To ensure that compliance with the adopted IT standards has been achieved within their assessed maturity requirements	Group risk committee chair	Quarterly
Divisional Risk Committee • To assist the group risk committee in the function of IT governance • Each division / business should appoint a full time or part time IT manager, depending on the needs of the business • In businesses with a complex IT environment, the appointment of an IT Steering Committee should be considered to act as an effective oversight body responsible for IT governance • To review the material IT risks as profiled by the business'	Divisional risk committee chair	Quarterly

IT managers and apply its own mind to the completeness of the risks facing the division

- To review the assessment of the IT dependency within each business and of the division
- To ensure the IT Maturity assessment has been performed and to review the assessed IT maturity levels, both current and required within the business and the division
- To review the identified gap analysis between current and required maturity levels and ensure an appropriate and acceptable plan is in place
- To annually review the IT dependency, IT maturity requirements and monitor progress against the execution of the IT maturity plan

Divisional / business IT manager (as appropriate)

IT manager

Monthly

- Ensure the divisional/ business IT strategy is aligned with the business strategy and objectives
 - Monitor the current levels of IT dependency and maturity
 - Design and implement an action plan to achieve desired / required levels of IT maturity
 - Monitor and evaluate the acquisition and appropriate use of technology processes and people
 - Determine IT's resilience within the business to learn, adapt and respond
 - Assess IT's response to inherent risks in the organisation such as disaster recovery
 - To challenge whether IT has recognised potential opportunities and responded appropriately
 - To report back regularly to the divisional risk committee on the progress against the IT maturity plan highlighting milestones achieved, challenges experienced or misalignment of the plan against current requirements
-

6. MINIMUM REQUIREMENTS

Regardless of the level of IT dependencies or maturity within the division / business the following basic IT guidelines should be implemented. These policies may exist as a single policy or as separate policies, however the twelve requirements below should be implemented within each business in order to comply with the minimum requirements for an IT environment per ISO 27002:

Policy name	Policy objectives
i. Information Security Policy	Information is an asset to the business just like any other business asset. Therefore information security is the protection of all company information in any form it may exist (i.e. printed or written on paper, electronic files, or spoken in conversations) from a wide range of threats in order to ensure business continuity, minimise business risk and maximise return on investments.
ii. Organisation of Information Security Policy	To manage information security within a business and to maintain the security of this business asset including information and information processing facilities that are accessed, processed, communicated to, or managed by third parties.
iii. Asset Management Policy	To manage asset classification and controls is to maintain appropriate protection of these business assets. All information assets should be accounted for and have an owner. Accountability for assets assist to ensure that appropriate protection is maintained. Information needs to be classified to ensure that the information asset get the correct level of protection.
iv. Human Resources Security Policy	To set guidelines on how to reduce the risks of human error, theft, fraud or misuse of the business' facilities as well as to ensure that users are aware of information security threats and concerns and are adequately equipped to support the security policy during their everyday work. Personnel need to be informed with regards to how they should handle security threats in order to minimise the damage caused by such threats.
v. Physical and Environmental Security Policy	To prevent unauthorised access, damage and interference to business premises and information; loss, damage or compromise of assets and interruption to business activities, and compromise or theft of information and information processing facilities.
vi. Computer Telecom Usage Policy	To ensure the proper use of computer and telecommunication resources and services by its employees, independent contractors and other users, require that all users commit themselves to the responsible use of the computer and telecommunications resources for the benefit only of the business and in an efficient, ethical, and lawful manner.

vii.	Communication and Operations Management Policy	To ensure the correct and secure operation of information processing facilities; to minimise the risk of system failures; to document all current system processes; to appropriately control any changes made to the systems by way of change management; to ensure any new system that is implemented is properly introduced into the new business environment so as to limit the exposure of system failure to the business.
vii	Access Control Policy	To prevent unauthorised logical and physical access to the business' information and information processing facilities through controlling of user access, password controls etc
ix.	Backup and Recovery Policy	To maintain integrity and availability of the business' information, through guiding back up procedures; frequency of backups; rotation of backup media; storage of backups; restoration from backup media etc
x.	Monitoring Policy	To detect any unauthorised information processing activities through the use of audit logging and error logging mechanisms
xi.	Business Continuity Management Policy	To counteract interruptions to business and to protect critical business processes from the effects of major failures of information systems or disasters and to ensure their timely resumption.
xii	Information Security Incident Management Policy	To ensure information security events and weaknesses associated with information systems are communicated in a manner allowing timely corrective action to be taken as well as to ensure a consistent and effective approach is applied to the management of information security incidents.

7. EVALUATION

The evaluation of this framework and related policies should be performed annually.

8. APPROVAL OF THIS FRAMEWORK

This framework was approved by the board on _____ and will be due for review on _____.

[name]
Chairman

Appendix A: COBIT Framework

The overall COBIT framework, as depicted in the graphic below, shows COBIT's process model of four domains containing 34 generic processes, managing the IT resources to deliver information to the business according to business and governance requirements.

