BID CORPORATION LIMITED

INFORMATION TECHNOLOGY ('IT') GOVERNANCE FRAMEWORK

The Board of Directors ('board') of Bid Corporation Ltd ('Bidcorp') acknowledges the need for an IT governance framework as recommended in the King IV Report on Corporate Governance for South Africa ('King IV').

1.   INTRODUCTION

King IV specifically recommends the following principles as providing the basis for the governance of IT and the establishment of a group wide IT governance framework:

1.1.   the board is responsible for the governance of IT;

1.2.   IT should be aligned with the performance and sustainability objectives of the company;

1.3.   the board should delegate to management the responsibility for the implementation of an IT governance framework;

1.4.   the board should monitor and evaluate significant IT investments and expenditure;

1.5.   IT should form an integral part of the company's risk management;

1.6.   the board should ensure that information assets are managed effectively; and

1.7.   the board may delegate to the audit and risk committee to assist in the carrying out of the board's IT responsibilities.

2.   PURPOSE OF THE IT GOVERNANCE FRAMEWORK

In addition to the seven principles stated above, King IV specifically states that the purpose of the IT governance framework is, ultimately, to 'support the effective and efficient management of IT resources to facilitate the achievement of a company's strategic objectives.'

The IT governance framework should also 'enable IT to deliver value to the business and mitigate IT risk', whilst remaining cognisant of 'the suitable strategy, structure and size of the company's IT function.'

In this context, and in light of the decentralised nature of Bidcorp, this IT governance framework is intended to serve as a group-wide baseline for the establishment of an IT governance framework within each operation.

3.   RESPONSIBILITIES

RESPONSIBILITIES	RESPONSIBLE PARTY	FREQUENCY
The board should: 3.1. Establish and approve the IT governance framework, including the IT control framework. 3.2. Ensure appropriate IT resource is appointed. 3.3. Delegate the responsibility for implementing the IT governance framework to the management teams. 3.4. Ensure the alignment of business and IT strategies. 3.5. Ensure IT is placed on the executive committee agendas and regular feedback is provided to the board. 3.6. Must conclude and report to the Bidcorp stakeholders an assessment regarding the effectiveness of IT governance and management activities.	Chairman of the board	Annually
The Bidcorp Audit & Risk Committee should: 3.7. Assist the board in the management and oversight of the function of IT governance. 3.8. Review the material IT risks as profiled by management teams and apply its own mind to the completeness of the risks and the appropriateness of the actions taken. 3.9. Ensure that compliance with the adopted IT governance standards has been achieved. 3.10. Review the material IT risks and apply its mind to the completeness of the risks facing the business and the appropriateness of the actions taken to address the risks. 3.11. Ensure the IT maturity assessment has been performed and to review the assessed IT maturity levels, both current and required, within each operation.	Bidcorp Audit & Risk Committee Chairman	Quarterly

|		
3.12. Review the identified gap analysis between current and required maturity levels and ensure an appropriate and acceptable plan is in place to reduce or eliminate the identified gap/s. 3.13. Monitor progress against the execution of the IT maturity plan.		
The IT management teams throughout the group should: 3.14. Ensure the alignment of the business strategy and IT strategy and the alignment of IT operations with the overall business operations. 3.15. Implement the IT solutions, structures, processes and mechanisms needed to execute the IT governance framework. 3.16. Identify material IT risks facing the business and institute appropriate actions to address the risks. 3.17. Review the results of the IT maturity analysis and implement an IT maturity plan to address any gaps identified between the current and required maturity levels. 3.18. Report the IT maturity plan and material risks to the Bidcorp Audit & Risk Committee.	Chief Information Officer / IT managers (as appropriate)	Ongoing basis

4.   FRAMEWORK DEVELOPMENT

Businesses within the group should, as appropriate, establish IT governance frameworks on the basis of the guidance in this baseline IT governance framework, whilst taking into account the following:

4.1.   the business strategy within the local entity; and

4.2.   the complexity of IT and the IT environment within this entity.

In addition to ensuring the appropriate alignment with business strategy, the various management teams should ensure that the following high-level risk categories are considered and addressed when developing the company-specific IT governance frameworks:

People risk:	**What is the level of reliance on IT personnel, considering both key personnel reliance and level of skill of the IT personnel?**
Information risk:	How is the management team securing data?
Integrity of data & availability risk:	How reliable are the IT systems (both applications and infrastructure)? Can management rely on the integrity of data when generating financial figures? Is the internal control environment such that audit can supply the Audit & Risk Committee with a level of assurance?
Legal risk:	What legislation / regulations are applicable to the IT environment? How can IT help the business comply with other relevant regulations / legislation?
Change control & project management risk:	Is there management level awareness of all the changes to the IT environment and how are these changes monitored?
Outsourcing risk:	What is the level of dependency on IT managed by third parties and how is the third party managing those risks? How is the third party providing outsourced IT services being managed?
IT investment risk:	How is the management team ensuring that investment in IT assets and systems is controlled and monitored?

A key component in addressing the above IT risks within a business is the establishment and implementation of an appropriate IT General Controls ('ITGC') framework. The ITGC framework is constructed of six interlinked domains, represented below:
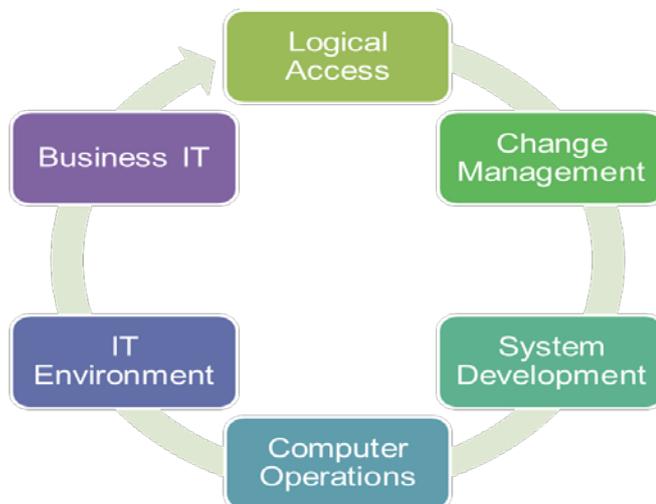
The ITGC framework and the six domains contain baseline policies, procedures and controls necessary in establishing the level IT maturity within each environment. The ITGC framework incorporates many of the concepts addressed by the following best practice standards and frameworks, including:

- Control Objectives for Information and related Technology ('COBIT');

- Information Technology Infrastructure Library ('ITIL'); and

- Information Technology - Code of Practice for Information Security Management (ISO/IEC 27002).

By detailing baseline policies, procedures and controls necessary for establishing the level of IT maturity within a business, the ITGC framework provides for a scalable and adaptable method of assessing IT maturity gaps. The IT maturity assessment will thus allow the identification, by management, of material IT risks and provide a basis for establishing actions to address the IT risks.

5. IMPLEMENTATION AND MAINTENANCE

The implementation of the IT governance framework requires a robust reporting structure within Bidcorp, at an entity level, focussing on the ITGC framework, and the associated policies, processes and controls within each business.

The internal audit function, and potentially external audit, should be used in assessing compliance to the IT governance framework, including the ITGC framework. The model below describes the implementation and maintenance of the ITGC framework.
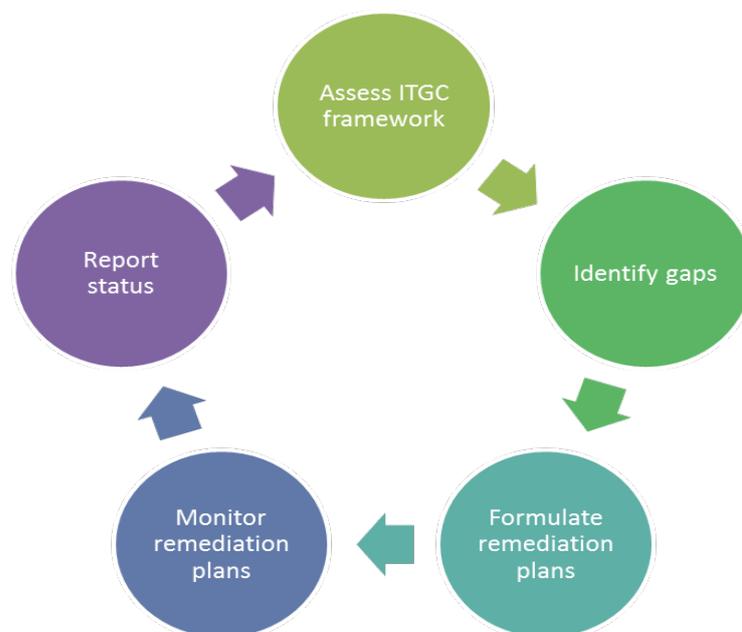
6. EVALUATION

The evaluation of this IT governance framework and the entity level IT governance frameworks should be performed annually.

7. APPROVAL OF THIS FRAMEWORK

On an annual basis this framework should be reviewed by the Bidcorp Audit & Risk Committee and recommended to the board for approval.