BIDVEST

RISK MANAGEMENT FRAMEWORK

INDEX

1. Introduction

The Bidvest Group Ltd ("Bidvest" or "Group") identified the COSO (Committee of Sponsoring Organisations of the Treadway Committee) Enterprise Management framework, an update from the previously used COSO Internal control model, as an appropriate risk management tool to embed the risk management culture and structures whilst also achieving consistency of the application of the risk assessment process within the Group.

2. Purpose and objectives

All organisations face risks that may affect the achievement of their strategic objectives. These risks must be managed to minimize the unfavorable impact and maximise opportunities. Effective risk management should result in added value for stakeholders through the successful execution of strategy whilst assuming acceptable residual risk.

The Risk Management Framework ("Framework") aims to achieve the following:

- Management accountability for designing, implementing and monitoring the process of risk management;
- Management responsibility for integrating the risk management process into the day-to-day activities of the Group; and
- Assist the board in discharging its risk management oversight responsibilities.

3. Risk management philosophy and policy statement

Bidvest's principle-based approach extends to risk management which allows for scalability and agility. There are no policies or procedures stipulated but rather a Framework that sets out management's responsibility and accountability with regards to risk management and the reporting thereof to assist the Board in discharging its responsibilities.

Based on our values, the Bidvest Code of Ethics sets out day-to-day standards of conduct and behavior which is a key component of our all-encompassing enterprise risk management.

4. Scope of Enterprise Risk Management Framework

Bidvest's Risk Management Framework provides guidance on the principles, components, categories, tools, management and reporting of risks. The application of this is left to divisional and operational management to apply in a fit-for-purpose manner, taking cognisance of the appropriate risk maturity level, on a bottom-up basis. Ultimately, the diverse nature of Bidvest is its most effective risk mitigant.

This Framework builds on the current level of risk management that exists in the normal course of business, across all subsidiaries of Bidvest, and it demonstrates how integrating enterprise risk management practices throughout an entity helps to accelerate growth and enhance performance. The Framework also incorporates important considerations, including governance and culture; strategy and objective-setting; performance; information, communications and reporting; and the review and revision of practices to enhance entity performance.

5. Custodians of risk

Bidvest is a decentralised group whose success is, in part attributable, to allowing managers to run the businesses as if they are their own. Cluster, divisional and corporate office layers provide oversight, guidance, strategic direction and consolidated reporting.

Based on our values, the Bidvest Code of Ethics sets out day-to-day standards of conduct and behavior which are key components of our all-encompassing enterprise risk management. The entrepreneurial and decentralised model demands that all MDs are custodians of risk and that risk management must be integrated in daily activities. Corporate office integrates and augments this bottom-up approach with top-down macro and thematic risk considerations. The divisional CEOs are the custodians of risk per division.

Risk management and the oversight thereof, is a group-effort. The CEO ultimately assures the board that all risks at strategic and operational levels have been considered.

6. Lines of defence and assurance

Material business processes, controls and risks are monitored and assessed through a combined assurance model. Combined assurance continually receives deliberate and focused attention in deriving the IA Plans from the perspective of all assurance functions. Optimisation of combined assurance avoids duplicative efforts, rationalises collaboration efforts upstream and effectively manages assurance costs, ultimately translating into an increased maturity level of the assurance functions as a whole.

Risk	Exco	Finance	Legal (either in-house or external)	Human Capital	Operations	IT	Risk (either an internal department or Group RMS)	Compliance	Respective Committees (company, divisional or Group level)	Internal Audit	ISO Audit	External Audit	ALICE	Ethics Facility
	Management 1st Line						Monitoring 2nd Line			Independent Assurance 3rd Line				
Strategic	●	●	●	●		●			●	●				
Financial		●				●	●	●	●	●		●		
Operational - IT						●	●	●	●	●			●	
Operational - People				●			●	●	●	●		●	●	●
Operational - Commercial	●				●		●	●	●	●	●	●		
Cyber Risk	●					●	●	●	●	●			●	
Business Resilience	●	●	●	●	●	●	●	●	●	●				
Fraud Risk	●	●					●	●	●	●		●	●	●
Regulatory & Compliance Risk			●				●	●	●	●		●		●
Sustainability	●	●			●	●	●	●	●	●		●		

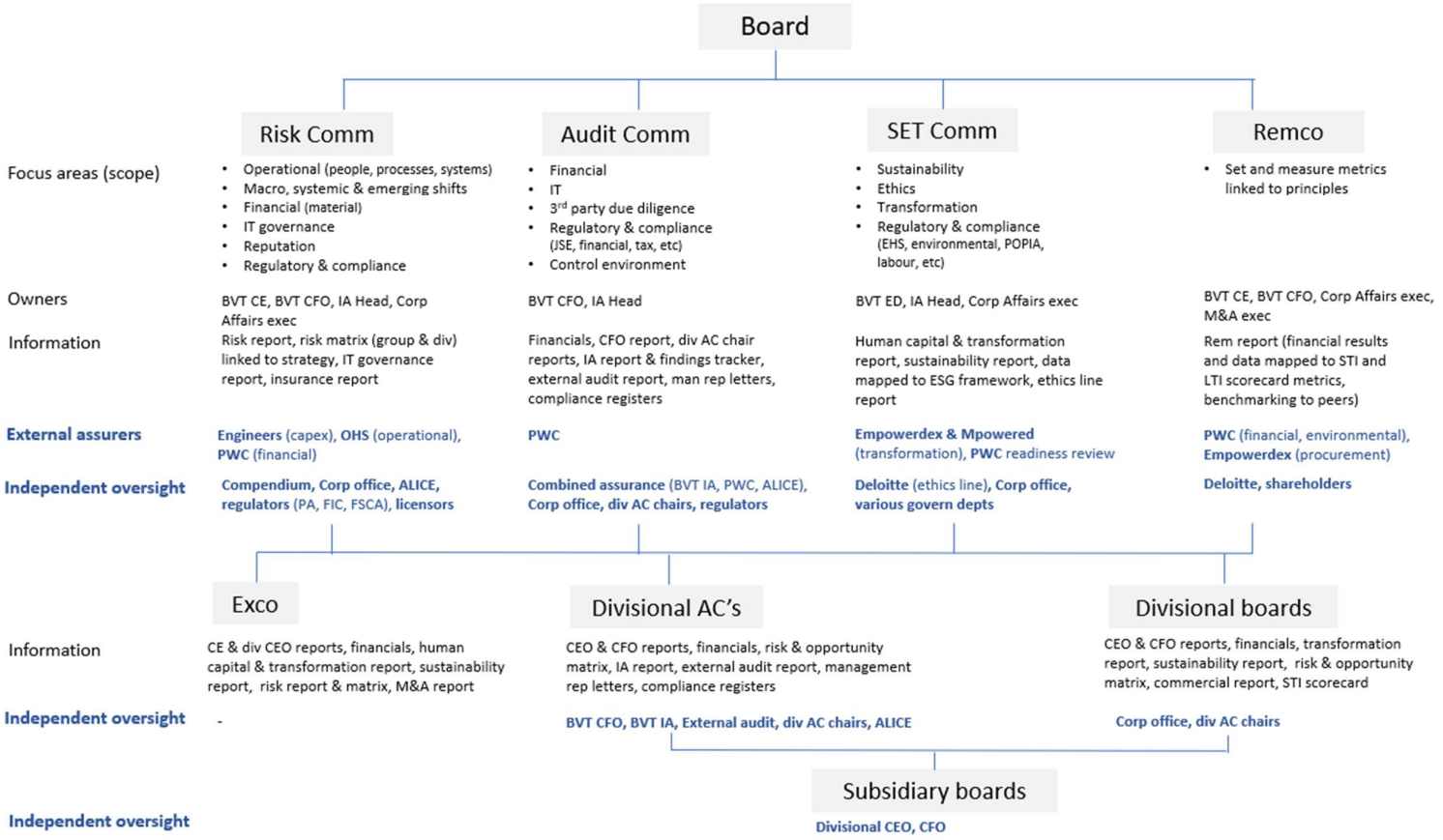
Management, Internal Audit (IA) and external audit, ALICE as well as non-executive directors all play a role.

The schematic overleaf illustrates the various levels of reporting, focus areas, oversight, etc.

Given the decentralised nature of Bidvest and the autonomous manner in which businesses are run, as the reporting moves from business level to Group level, there are various layers of (operationally) independent and external oversight. To strengthen this further, each Divisional Audit committee, who's mandate includes risk and certain sustainability elements, is chaired by independent non-executive chairperson.

The IA function also mirrors the corporate structure of the Group. Divisional IA teams, report to both divisional management as well as the Group IA head. Divisional IA is independent of businesses while Group IA is independent of divisions, thereby providing independent oversight on various financial, control and risk elements. The in-house developed AI tool, ALICE, provides further automated continuous oversight.

Annual IA plans incorporate operational, financial and information technology risk monitoring and assessment. The outcome of work conducted is reported to Divisional Audit committees and upwards.


Board
Risk Comm
Audit Comm
SET Comm
Remco
Focus areas (scope)
• Operational (people, processes, systems)
• Macro, systemic & emerging shifts
• Financial (material)
• IT governance
• Reputation
• Regulatory & compliance
• Financial
• IT
• 3rd party due diligence
• Regulatory & compliance (JSE, financial, tax, etc)
• Control environment
• Sustainability
• Ethics
• Transformation
• Regulatory & compliance (EHS, environmental, POPIA, labour, etc)
• Set and measure metrics linked to principles
Owners
BVT CE, BVT CFO, IA Head, Corp Affairs exec
BVT CFO, IA Head
BVT ED, IA Head, Corp Affairs exec
BVT CE, BVT CFO, Corp Affairs exec, M&A exec
Information
Risk report, risk matrix (group & div) linked to strategy, IT governance report, insurance report
Financials, CFO report, div AC chair reports, IA report & findings tracker, external audit report, man rep letters, compliance registers
Human capital & transformation report, sustainability report, data mapped to ESG framework, ethics line report
Rem report (financial results and data mapped to STI and LTI scorecard metrics, benchmarking to peers)
External assurers
Engineers (capex), OHS (operational), PWC (financial)
PWC
Empowerdex & Mpowered (transformation), PWC readiness review
PWC (financial, environmental), Empowerdex (procurement)
Independent oversight
Compendium, Corp office, ALICE, regulators (PA, FIC, FSCA), licensors
Combined assurance (BVT IA, PWC, ALICE), Corp office, div AC chairs, regulators
Deloitte (ethics line), Corp office, various govern depts
Deloitte, shareholders
Exco
Divisional AC's
Divisional boards
Information
CE & div CEO reports, financials, human capital & transformation report, sustainability report, risk report & matrix, M&A report
CEO & CFO reports, financials, risk & opportunity matrix, IA report, external audit report, management rep letters, compliance registers
CEO & CFO reports, financials, transformation report, sustainability report, risk & opportunity matrix, commercial report, STI scorecard
Independent oversight
-
BVT CFO, BVT IA, External audit, div AC chairs, ALICE
Corp office, div AC chairs
Subsidiary boards
Independent oversight
Divisional CEO, CFO

7. Enterprise Risk Management Framework

The Framework itself is supported by a set of principles organized into five interrelated components. These principles cover everything from governance to monitoring. They're manageable in size, and they describe practices that can be applied in different ways regardless of size, type, or sector. Adhering to these principles can provide management and the board with a reasonable expectation that the organization understands and strives to manage the risks associated with its strategy and business objectives.

Governance and Culture: Governance sets the organization's tone, reinforcing the importance of, and establishing oversight responsibilities for, enterprise risk management. Culture pertains to ethical values, desired behaviours, and understanding of risk in the entity.

Strategy and Objective-Setting: Enterprise risk management, strategy, and objective-setting work together in the strategic-planning process. A risk appetite is established and aligned with strategy; business objectives put strategy into practice while serving as a basis for identifying, assessing, and responding to risk.

Performance: Risks that may impact the achievement of strategy and business objectives need to be identified and assessed. Risks are prioritized by severity in the context of risk appetite. The organization then selects risk responses and takes a portfolio view of the amount of risk it has assumed.

Review and Revision: By reviewing entity performance, an organization can consider how well the enterprise risk management components are functioning over time and in light of substantial changes, and what revisions are needed.

Information, Communication, and Reporting: Enterprise risk management requires a continual process of obtaining and sharing necessary information, from both internal and external sources, which flows up, down, and across the organization.

8. Risk appetite and tolerance

Bidvest accepts a calculated level of risk. We will accept risks in new product and/or service introduction, geographic expansion in our strategically chosen niches and support systems and processes. We will, however, not bear any risks that threaten financial stability, brand and/or company reputation, legal compliance or unchecked health and safety of people. Our risks management activities will prioritise these areas.

Commercial risk tolerance is equated to a material financial impact, in line with the financial materiality parameters of the Group's external auditors, on Bidvest and/or its businesses. IT risk tolerance is moderate given the varied IT infrastructure and landscape across the Group but conservative regarding cybersecurity at business level.

9. Risk management procedures

Executive management will ensure that it has in place the means to identify, analyse, control and monitor the strategic and operational risks faced across its diverse operations. Clear reporting lines will be established between business unit, divisional risk management committees and Group to implement an effective, enterprise-wide risk management process.

Risks shall be assessed and ranked according to their impact and their likelihood of occurrence. This shall principally be done at business unit and divisional levels with the main risks (at least top five) reported on as a standard agenda item at Divisional Board meetings. At Group-level, these and other global, country and Group risk considerations shall be overlaid for reporting to the Board on a quarterly basis.

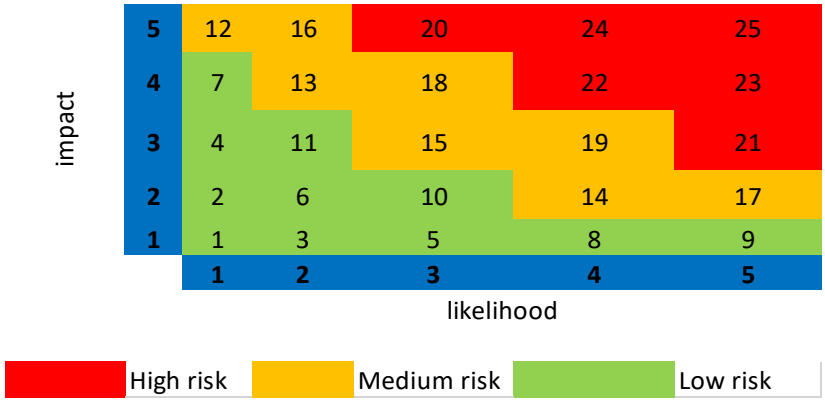
Risks shall be considered within the following categories:

- Reputational;
- Contractual;
- Economic and financial;
- Regulatory and compliance;
- Information technologies;
- Fraud and ethical conduct;
- Sustainability, including climate change;
- Human capital; and
- Systemic and emerging shifts.

IT Governance has been carved-out as a separate risk focus area, championed by Group IA, given the technical expertise, insight and vision required to access, monitor, remediate and manage the IT infrastructure to be fit-for-purpose. ALICE plays an integral oversight role in continuous monitoring across the diverse Group.

Each risk will be assessed as to its impact and likelihood to quantify, qualitatively and quantitatively, the inherent and residual risk. The impact shall be assessed using the Risk Assessment Matrix ("Matrix") below.

The Matrix used across Bidvest is not a numerically linear 5x5 matrix as it is skewed towards "likelihood" and medium risks. The Matrix is designed to take cognisance of the diverse and decentralised nature of the Group but also the aggregated impact of a similar risk across many operations. The assessment of risks is done on both quantitative and qualitative basis.


impact
5 12 16 20 24 25
4 7 13 18 22 23
3 4 11 15 19 21
2 2 6 10 14 17
1 1 3 5 8 9
1 2 3 4 5
likelihood
High risk
Medium risk
Low risk

The following guidelines accompany the risk matrix used across the Group:

IMPACT					
Level	**Non-Financial Impact Description**	**Quantitative**	**Reputation**	**Systems availability**	**SHE**
5. Severe	The impact is beyond the Stakeholders' ability to manage or resource and as such may threaten the survival of, for example, a particular project or the company itself.	>R100m	Suspension of business.	Systems unavailable for more than 2 days	• Fatality; • Multiple occupational health diseases directly attributable to Company's activities and irreversible; • Environmental disaster (evacuation of local community / significant irreversible pollution / prosecution by national government and local authorities)
4. Major	The impact would threaten the ability to achieve the Product and/or Organisational objectives in the medium term.	R20m-R100m	Adverse media comment that has a long-term impact on Company's image, significant brand damage.	Systems unavailable for more than 5 hours less than 2 days	• A number of disabling incidents; • Occupational health disease (irreversible and compensation claimed); • Major environmental incident (uncontrollable off site impacts /press coverage / fines and penalties / intervention by national government)
3. Significant	The impact may threaten the ability to achieve the Product and/or Organisational objectives in the short term.	R5m-R20m	Adverse media comment or regulatory action or fine that has a short-term reputational impact, requiring corrective action and dedicated additional resources to rectify and recover.	Systems unavailable for more than 30 minutes but less than 5 hours	• Lost time injury (lost work days); • Occupational health disease (lost work days but reversible; • Reportable environmental Incident (permit contravention or controllable off site impact / external complaint / intervention from local authority)

2. Minor	The impact can be absorbed within the day-to-day business running costs.	R500k-R5m	Adverse impact on some external customers, minor impact on objectives.	Systems unavailable for more than 5 minutes but less than 30 minutes	• Minor injury (no lost work days); • Ill health (reversible); • Minor environmental incident (contained and no off site impact)
1. Insignificant	The impact has little or no effect on the day to day running costs of the business		Breakdown in control but process performance unaffected.	Systems unavailable for less than 5 minutes	• First Aid Treatment; • Clinic Treatment; • Environmental near-miss

LIKELIHOOD		
Level	**Description**	**Probability of Occurrence in Next 12 Months**
5. Almost Certain	Expected to occur in most circumstances or occurs regularly	>70%
4. Likely	Occurrence is noticeable, starting to be of nuisance value	40% - 70%
3. Possible	Occurs occasionally	20%-40%
2. Unlikely	Occurs infrequently	5% - 20%
1. Rare	Only occurs in exceptional circumstances	<5%

Risks will be prioritised and mapped using the approach set out above. Where executive management choose a risk response other than “Accept”, risk treatment and response could include:

- Modify the risk / Mitigate – management may take actions to employ strategies to reduce the residual risk;
- Retain the risk / Accept – management may decide to accept and monitor the risk. This may be necessary for some risks that arise from external events;
- Share / Transfer the risk – management may decide to pass the risk on to another party through contractual terms or insurance cover, for example;
- Avoid the risk / Eliminate – the risk may be such that management decide to cease the activity or change it in such a way as to eliminate the risk.

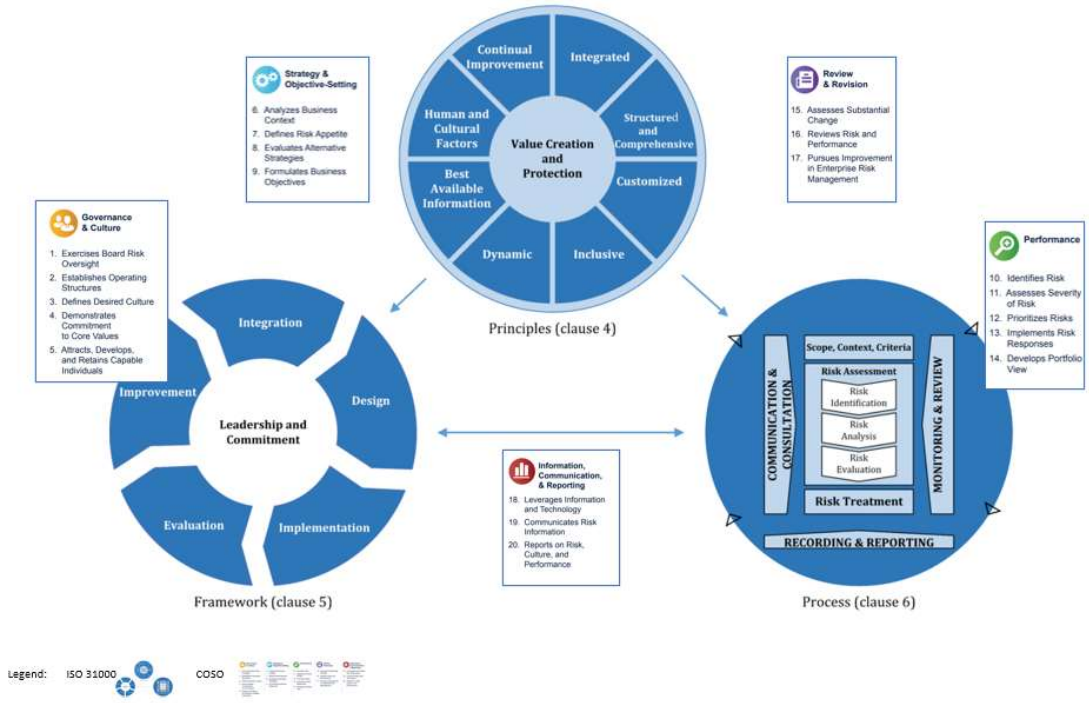
The procedure for managing risk will meet the following criteria:

- Bidvest Group and divisions will maintain risk registers, including risk treatment and responses;
- Inherent and residual risks will be scored based on the Matrix, determined through a combination of likelihood and impact;
- Risks may be valuated to estimate potential monetary loss, where practical, or may be considered on a qualitative basis;
- Management will respond to risks in a prioritised fashion. Remediation priority will consider the risk likelihood and impact, cost, work effort and availability of resources. Multiple remediations may be undertaken simultaneously;
- Management will consider the opportunities that identified risks pose and formulate an approach to capture, aligned to the Group strategy; and
- Quarterly reports will be made to executive management and the Board to ensure risks are being mitigated appropriately and in accordance with business priorities and objectives.

All of the above will be done bearing in mind the risk appetite of the Group and individual operations.

10. Alignment with ISO 31000

The three elements embedded in the leading practice guidance of ISO 31000 – leadership and commitment; value creation and protection principles; and risk management process – are integral to risk management at Bidvest. The COSO framework, as adopted by Bidvest, incorporates general corporate governance, internal controls and financial reporting into risk management embedded in organisational decision-making.



11. Corporate governance

King IV principles relevant to risk management are:

- *Principle 4 – The governing body should appreciate that the organisation's core purpose, its risks and opportunities, strategy, business model, performance and sustainable development are all inseparable elements of the value creation process.*
- *Principle 11 – The governing body should govern risk in a way that supports the organisation in setting and advancing its strategic objectives.*
- *Principle 13 – The governing body should govern compliance with applicable laws and adopted, non-binding rules, codes and standards in a way that supports the organisation being ethical and a good corporate citizen.*
- *Principle 15: the governing body should ensure that assurance services and functions enable an effective control environment, and that these support the integrity of information for internal decision-making and of the organisation's external reports.*
- At a Group level, independent non-executive oversight is multi-disciplinary as the Risk, Audit, Social, Ethics and Transformation as well as Remuneration committees all consider various elements of the risk categories (reputational, contractual, economic & financial, regulatory & compliance, information technology, fraud & ethical conduct, sustainability; human capital; and systemic and emerging shifts).

Quarterly the Board and its sub-committees are provided with data, information and report backs on all key risks, on a qualitative and quantitative basis. The process of gathering, evaluating and identifying key risks and the management thereof are depicted in the earlier schematic. Several layers of independent oversight, some external assurance and multiple committee reviews provide comfort with regards to completeness. Information sharing between the multiple committees is facilitated by the Group secretarial function through adding to relevant committee agenda's, quarterly sub-committee feedback to the Board, etc as appropriate.

Annually the maturity level of each business' risk management process is assessed as part of the combined assurance planning process. Enhancements, if required, are then implemented.

The periodic review of the Group purpose, strategy, ESG framework and key risks, together with the opportunities presented as a consequence, provide the Board with insight as to how these elements are integrated into daily activities to create value for all stakeholders. The annual reporting suite communicates this externally.

_____end_____