RISK

Philosophy

2014 has seen the JSE risk function further mature as well an improvement in the interaction between the risk and internal audit functions as a result of changing the reporting structure. The risk and internal audit functions maintain independence to ensure appropriate lines of defence, but information sharing is benefiting both functions. JSE enterprise risk now forms part of the Governance, Risk and Compliance division.

Risk management is not about eliminating risk but rather about managing of how much risk the entity is prepared to and does accept as it strives to create value.

The JSE enterprise risk function supports enterprise objectives by evaluating itself against the JSE enterprise risk philosophy, outlined in six principles:

SUPPORTS ENTERPRISE OBJECTIVES AND INCORPORATES OPPORTUNITIES

A risk view must be provided in the context of achieving business goals and objectives. Risk must not only be seen as a hazard (possibility of a negative event) but must also incorporate the context of recognising the inherent relationship between risk and return through opportunities.

APPROPRIATE FOR THE JSE

Only applicable components will be used from best practices to ensure that its risk practices are fit for purpose for the JSE while still meeting any legal and regulatory requirements. All risk management activities will be within the context of the JSE risk appetite.

OPERATES EFFECTIVELY

The measure of a risk process lies in its ability to focus on and execute the appropriate risk response strategy (transfer, mitigate, accept or avoid) for every major exposure. Risk management must also be embedded into the way the JSE operates.

IS CONSISTENT AND VALIDATED

Risk processes incorporate not only management perspectives but also the judgement of risk management and independent assurance (audit) views.

MUST ADD VALUE

Risk management must not simply be a function that exists to meet governance, legal and regulatory requirements and provide reporting, but must add value, where appropriate, to the enterprise through the application of insight and skills.

ACCOUNTABILITY MUST BE CLEARLY DEFINED

Because risk management operates across governance, compliance and specialist risk and business management functions, clear accountability areas must be defined in order to avoid duplication of effort or unmanaged areas.

Roles and responsibilities

JSE Board and Risk Management Committee

King III indicates, and the JSE subscribes to the fact, that the Board should:

- be responsible for the governance of risk;
- determine the levels of risk tolerance;
- delegate to management the responsibility to design, implement and monitor risk management;
- ensure that risk assessments are performed continually;
- ensure that frameworks and methodologies are implemented to increase the probability of anticipating unpredictable risks;
- ensure continual risk monitoring by management;
- receive assurance regarding the effectiveness of the risk management process; and
- ensure that there are processes in place enabling complete, timely, relevant, accurate and accessible risk disclosure to stakeholders.

The JSE Board has constituted the Risk Management Committee to assist with the discharging of its duties and responsibilities with regard to risk management. Enterprise risk management oversight is provided by the JSE Risk Management Committee by monitoring the implementation of the JSE risk framework and driving corrective actions.

Approach

Enterprise risk reporting has been enhanced to align with enterprise objectives by tracking risk areas in relation to the JSE strategic vision and reporting them in that format to the JSE Board Risk Management Committee. This report is compiled using the existing JSE risk profile supported by underlying risk methodologies that incorporate ISO 31000 principles. Risk reporting has been emphasised to ensure the right focus and discussions at the JSE Board Risk Management Committee as well as continuing to ensure that the business drives risk management in its operations.

Current risk profile

Seven key strategic and business risk focus areas were noted at the most recent JSE Board Risk Management Committee meeting. These areas were drawn from interactions with management, a review of the enterprise risk register, and the application of judgment by the enterprise risk management (ERM) team. The areas were:

1. Risk caused by operational vulnerabilities
2. Delivery of the T+3 project (phase 2)
3. Delivery of the ITaC project
4. Impact of regulatory trends
5. Digestibility risk: the ability of the JSE and its clients to deal with the required change
6. Responding appropriately to the changing strategic landscape
7. An internal and external view of the JSE's compliance profile.

These areas are actively managed by the JSE and tracked formally by the JSE risk team.

Risk-based compliance with laws, rules, codes and standards

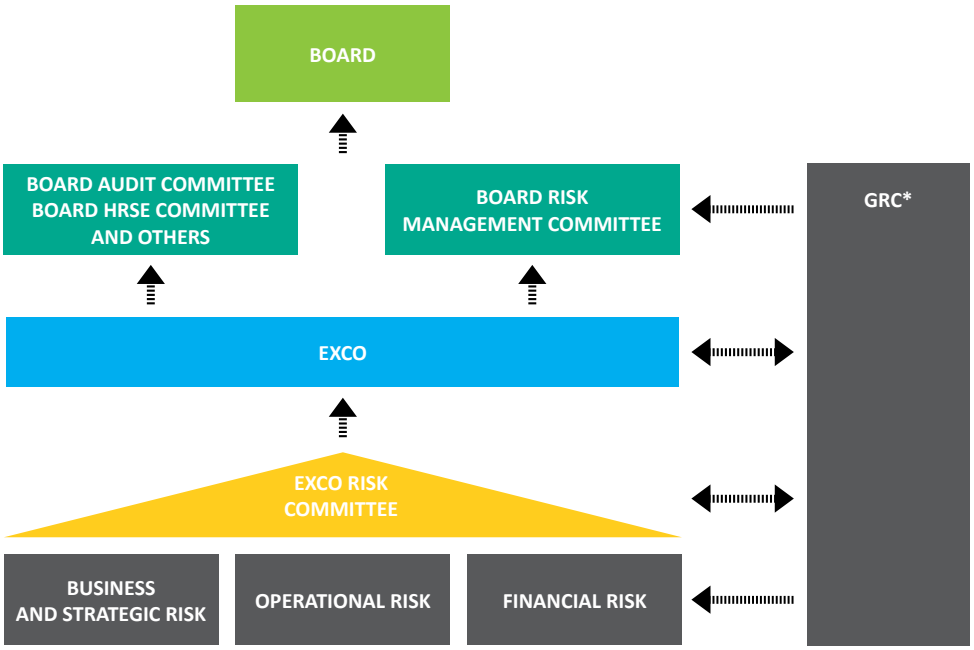
Compliance remains a focus area for the JSE. The JSE has continued with its risk based compliance approach. This will receive ongoing attention within the new JSE structure as well. Compliance is an ongoing focus for the JSE and inherently part of the JSE's DNA because of its regulatory culture. 2015 will see constant attention to this area, with some increased focus on formally maturing the JSE compliance profile.

JSE site management risk

JSE occupational health and safety requirements have been further embedded into the way the JSE operates after assessments carried out in 2013.

Information Security

In the previous annual report, it was noted that a formal information security office was established under the CIO. An approved information security programme now addresses the governance, risk, compliance, process, people and technology aspects of information security. A number of new technical and non-technical security controls have been implemented successfully during 2014 and more are planned for 2015. The security controls are being implemented to mitigate information risk and to improve the JSE's overall information security posture. The security controls are part of a defence-in-depth strategy to ensure the confidentiality, integrity and availability of our information assets. The status and efficiency of security controls are continuously managed, monitored and reported through an information security management system (ISMS) that provides ongoing assurance of an adequate security posture. The JSE information security programme is aligned with information security best practices, includes cybercrime defences and considers the efforts of our counterparts through participation in the WFE's Global Cyber Security Working Group.



**Governance, Risk and Compliance Division, including Enterprise Risk Management function and Internal Audit.*

Risk reporting

Risk reporting is submitted to the Exco Risk Committee. Exco receives risk reporting prior to it being submitted to the JSE Risk Management Committee. This reporting flows into Board reporting (including the Board receiving the JSE Risk Committee minutes). The reporting structure supports the specialist team's oversight function through allowing, in extreme cases, for independent escalation to the JSE Risk Management Committee on items where agreement on reporting could not be reached through the management reporting structures.

Oversight

The JSE enterprise risk team has also increased its oversight activities in order to bolster the risk lines of defence for the JSE. This is over and above risk reporting. The close cooperation with Internal Audit has also facilitated this.

Oversight areas include:

- Strategic projects;
- IT governance;
- Information security;
- Business continuity; and
- Information governance.