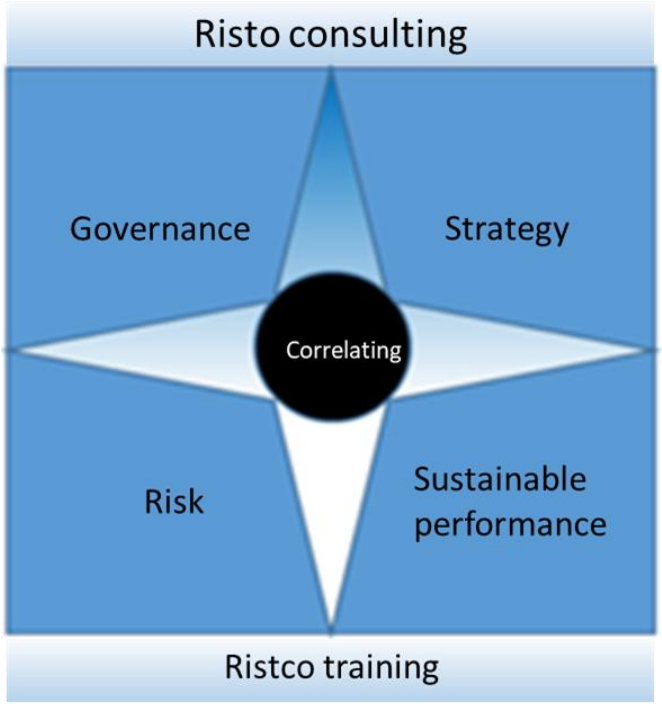
RELATION BETWEEN GOVERNANCE AND RISK – ACCORDING TO ISO 31000:2018

The relationship between governance and risk management has been a discussion point for a long time. Many a time it is based on the view of a specific individual and even to the extent that governance has to be tolerated as it is enforced upon people.



I have highlighted the high level relationship between risk and governance as it is reflected in ISO 3100:18 below. Interestingly it paints a totally different view and also touches on their correlation with strategy and performance management.

One of the major changes associated with the 2018 version update is bigger emphasis on leadership and the integration of risk management in business processes – starting with governance of the organisation. (Foreword)

- ISO 31000 is clear that managing of risk is part of governance and leadership and it is fundamental to how organisations are managed on all levels. It also contributes to the management of all management systems. (Introduction)

- Governance is regarded as a critical success factor as it is clearly stated that the effectiveness of risk management will depend on its integration into governance of the organisation, including decision-making. This requires the support of all stakeholders, especially the board of directors and top management. (Par 5.1 in the context of the Framework discussion)

- ISO 31000 recognises that governance guides the course of the organisation, its external and internal relationships and the rules,

processes and practices needed to fulfil its purpose. (Par 5.3 – Integration). This will typically include the purpose of the organisation.

- The Board / top management translate the governance direction into the strategy and the associated objectives required to achieve desired level of sustainable performance and long-term viability. (Par 5.3 – Integration). Risk is defined as the effect of uncertainty on objectives and therefore linked to the effective governance / company direction, which also may contain risk to be considered.

- Determining risk management accountability and oversight roles within the organisation is an integral part of the organisation's governance. (Par 5.3 – Integration).

- ISO 31000 requires that the integration of risk management into an organisation be a dynamic and iterative process and that it should be customised to the organsiation's needs and culture. Risk management should be part of, and not separate from, the organisational purpose, leadership and commitment, strategy, objectives and operations. (Par 5.3 – Integration). So, it is clear that it does not only refer to individual decisions, but the holistic risk program in support of well considered objectives.

- The internal and external context, inclusive of a stakeholder analysis are core elements to adequately shape the risk framework and program. Examining the governance of the organisation is important input to the organisations internal context analysis / consideration. (Par 5.4.1 – Understanding the organsiation and its context).

The above makes the point that there is a lot of value in deeply understanding the international risk management standard. Contact us at info@ristco.co.za or johan.opperman@ristco.co.za for additional information or to arrange for an obligation free virtual meeting with Johan Opperman (+27 83 233 4630) to discuss how risk management and governance could be optimally correlated in your organisation. Such a discussion could also touch on the correlation with strategy and sustainable performance and potential training needs.

About Ristco: Ristco is a management consulting firm specialising in corporate and IT governance, strategy, risk and risk type management as

well as sustainable performance management via the optimised operation and correlation of the mentioned disciplines. Ristco is a PECB partner to provide internationally accredited ISO standard certification training. Ristco also adds value via customised Board / Exco or risk personnel training interventions.