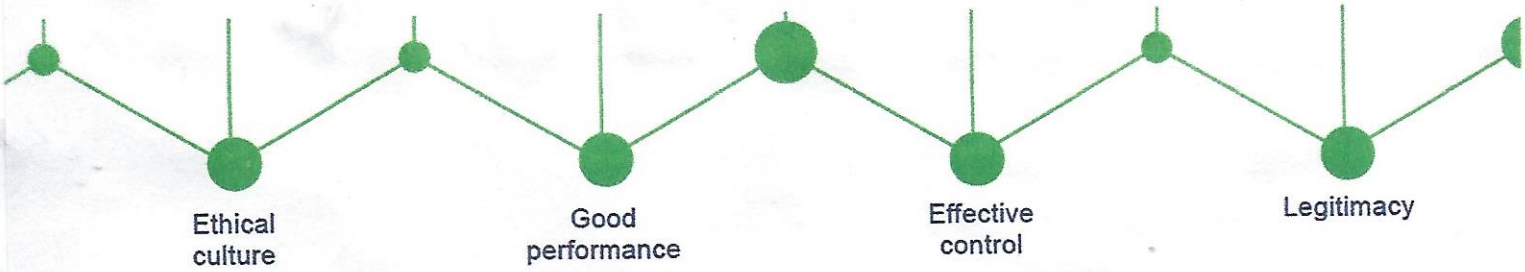

PART 5.4: GOVERNANCE FUNCTIONAL AREAS

Risk governance

Principle 11: The governing body should govern risk in a way that supports the organisation in setting and achieving its strategic objectives.

RECOMMENDED PRACTICES

1. The governing body should assume responsibility for the governance of risk by setting the direction for how risk should be approached and addressed in the organisation. Risk governance should encompass both:
   a. the opportunities and associated risks to be considered when developing strategy; and
   b. the potential positive and negative effects of the same risks on the achievement of organisational objectives.
2. The governing body should treat risk as integral to the way it makes decisions and executes its duties.
3. The governing body should approve policy that articulates and gives effect to its set direction on risk.
4. The governing body should evaluate and agree the nature and extent of the risks that the organisation should be willing to take in pursuit of its strategic objectives. It should approve in particular:
   a. the organisation's risk appetite, namely its propensity to take appropriate levels of risk; and
   b. the limit of the potential loss that the organisation has the capacity to tolerate.
5. The governing body should delegate to management the responsibility to implement and execute effective risk management.
6. The governing body should exercise ongoing oversight of risk management and, in particular, oversee that it results in the following:
   a. An assessment of risks and opportunities emanating from the triple context in which the organisation operates and the capitals that the organisation uses and affects.
   b. An assessment of the potential upside, or opportunity, presented by risks with potentially negative effects on achieving organisational objectives.
   c. An assessment of the organisation's dependence on resources and relationships as represented by the various forms of capital.
   d. The design and implementation of appropriate risk responses.
   e. The establishment and implementation of business continuity arrangements that allow the organisation to operate under conditions of volatility, and to withstand and recover from acute shocks.
   f. The integration and embedding of risk management in the business activities and culture of the organisation.
7. The governing body should consider the need to receive periodic independent assurance on the effectiveness of risk management.
8. The nature and extent of the risks and opportunities the organisation is willing to take should be disclosed without compromising sensitive information.
9. In addition, the following should be disclosed in relation to risk:
   a. An overview of the arrangements for governing and managing risk.
   b. Key areas of focus during the reporting period, including objectives, the key risks that the organisation faces, as well as undue, unexpected or unusual risks and risks taken outside of risk tolerance levels.
   c. Actions taken to monitor the effectiveness of risk management and how the outcomes were addressed.
   d. Planned areas of future focus.