Ethics, Risk, Governance and Fraud Workshop

November 2019

Delegate Workbook

Facilitated by Pro-Active College (Pty) Ltd

FASSET

The views expressed in this workbook are not necessarily reflective of the official views of Fasset.

Contents

Chapter 1: Growing need for risk assessment

1. Risk management principles

During the last five years several public and private sector enterprises failed. The question that can be asked is whether risk management could have prevented such failures. Why is it that some enterprises can survive tough economic decisions and others fail? This training would attempt to answer some of the questions. Some examples of failures are included below:

Gupta sanctions put state capture specialists KPMG, PwC, McKinsey back in spotlight

11th October 2019 by Jackie Cameron

As tangible action against state capture masterminds, the Gupta brothers and Salim Essa, is taken by US authorities, the world spotlight is back on corporation that have aided and abetted the corrupt in South Africa.

FEATURES / COVER STORY

Scandal of the year: VBS — a most unsophisticated bank heist

VBS Mutual Bank collapsed this year after being fleeced by the very people entrusted with looking after depositors' money

21 DECEMBER 2018 - 05:00 · By SIKONATHI MANTSHANTSHA

R100m lost as Limpopo suspends two officials ov borehole 'scams'

Alex Matlala

A set of guiding principles is indispensable for risk management to be effective in an organization. According to the ISO 31000 Standards for Risk Management, these principles would include:

Risk management creates and protects value	Risk management contributes to the demonstrable achievement of objectives and improvement of performance in, at all levels in the organization, and across all functions and processes, for example, human health and safety, security, legal and regulatory compliance, public acceptance, environmental protection, product quality, project management, efficiency in operations, governance and reputation.
Risk management is an integral part of all organizational processes	Risk management is not a stand-alone activity that is separate from the main activities and processes of the organization. Risk management is part of the responsibilities of, not only management, but of all organizational personnel and an integral part of all organizational processes, including strategic planning and all project and change management processes.

Risk management is part of decision making	Risk management helps decision makers make informed choices, prioritize actions and distinguish among alternative courses of action, especially where there is a level of uncertainty associated with the achievement of objectives, and projected outcomes, and the risk reward ratios vary for the different decision options.
Risk management explicitly addresses uncertainty	Risk management explicitly takes account of uncertainty, the nature of that uncertainty, and how it can best addressed to either optimise value creation or minimise value destruction.
Risk management is systematic, structured and timely	A systematic, timely and structured approach to risk management contributes to efficiency and to consistent, comparable and reliable results
Risk management facilitates continual improvement of the organization	Organizations should develop and implement strategies to improve their risk management maturity alongside all other growth and performance activities of their organization.

2. Introduction

Risk management is a management discipline with its own set of techniques and principles. It is a recognised management science and has been formalised by international and national codes of practice, standards, regulations and legislation.

Risk management forms part of management's core responsibilities and is an integral part of the internal processes of an organization. Worldwide managers are simplifying the processes and practices of to optimise the cost-benefit thereof, with a greater shift away from compliance for the sake of compliance, to a greater focus on the pursuit of value creation opportunities, the achievement of objectives, and the mitigation of potential value destruction.

3. Best practices

Risk management is a systematic process to identify, evaluate and address risks pro-actively and continuously before such risks can impact negatively on the organization's service delivery.

When properly executed, risk management provides reasonable, although not absolute assurance, that the organization will be successful in achieving its goals and objectives. The ISO 31000 [1] standards and COSO [2] risk management frameworks are recognised as providing the best available practice guidance on risk management - this framework is based on many of the principles contained in these frameworks.

Locally the South African King codes on corporate governance[3] has been breaking ground in this space and is observed as one of the leading governance codes competing favourably with other international codes, also regarding its reference to risk management and how it should be dealt with within organizations.

[1]Risk Management Principles and Guidelines, SANS 31000:2009 Edition 1 / ISO31000:2009 Edition 1, all pages.

[2]COSO Enterprise Risk Management – Integrated Framework, Executive Summary, September 2004.

[3]The King Code of Corporate Governance, chapter 6, Institute of Directors of Southern Africa, 2009.

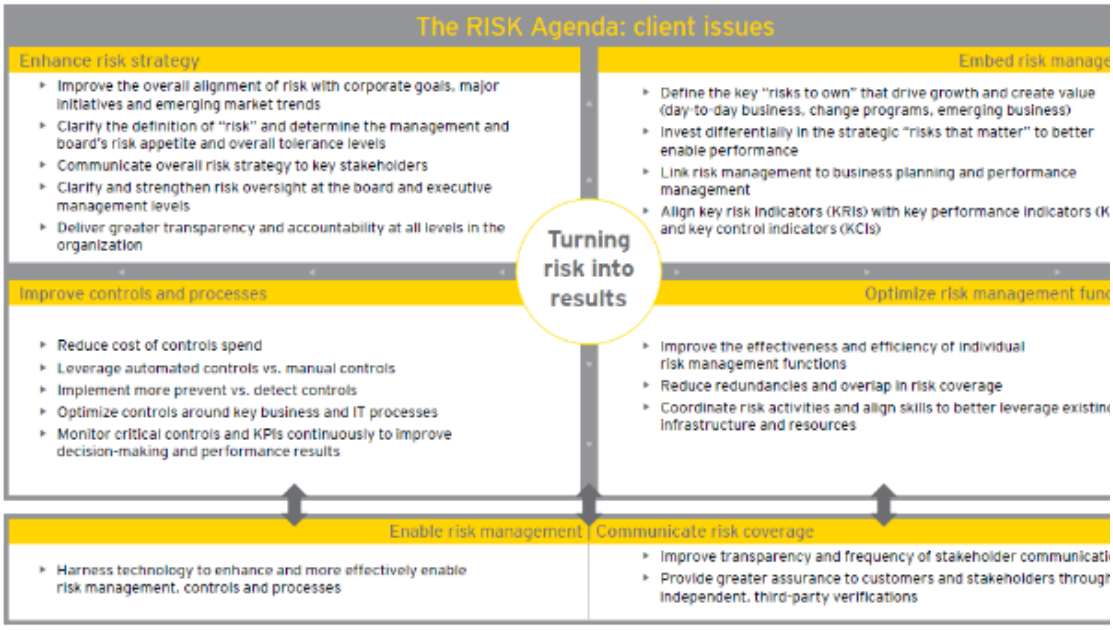


Figure 1: Risk agenda

King III principles address the responsibility of risk, mostly as these pertain to the board and its subcommittees. Boards should:

a. Be responsible for the governance of risk;
b. Determine the levels of risk tolerance/appetite;
c. Establish a risk committee or audit committee to assist the board in carrying out its risk responsibilities; and
d. Delegate to management the responsibility to design, implement and monitor the risk management plan.

King III principles also address the management of risk, whereby the board should ensure that:

a. Risk assessments are performed on a continual basis;
b. Frameworks and methodologies are implemented to increase the probability of anticipating unpredictable risks; and
c. Management considers and implements appropriate risk responses.

King III principles address the monitoring, assurance and disclosure of risk, whereby the board should:

a. Ensure continuous risk monitoring by management;
b. Receive assurance regarding the effectiveness of risk management processes; and
c. Ensure that there are processes in place enabling complete, timely, relevant, accurate and accessible risk disclosure to stakeholders.

King IV recommends that the board should appreciate that the core purpose of the organization, its risks and opportunities, strategy, business model, performance and sustainable development are all inseparable elements of the value creation process. Board should:

a. Assume responsibility for organizational performance by steering and setting the direction for the realisation of the core purpose and values through its strategy;
b. Delegate the formulation and development of short, medium and long term strategy to management;
c. Approve the strategy by considering:
    i. The timelines and parameters of the short, medium and long term;
    ii. The risks and opportunities relating to the organizational environment; and
    iii. The various forms of capital supporting the strategy.
d. Oversee whether the organization frequently and continuously assess the negative consequences of its activities and outputs; and
e. Be alert to the general viability of the organization with regard to its capital resources, its solvency and liquidity and its status as a going concern.

4. Glossary of terms

Audit Committee	An independent committee constituted to review the effectiveness of control, governance and risk management within the organization.
Chief Audit Executive	A senior official within the organization responsible for internal audit activities
Chief Risk Officer	A senior official who is the head of the risk management unit.
Combined assurance	Integrating and optimising all assurance services and functions, so that taken as a whole, these enable an effective control environment, support the integrity of the information used for decision-making by management, the business and it's committees to maximise risk and governance oversight and control efficiencies, and optimise overall assurance to the audit and risk committee, within the organization's risk appetite.
Compliance risks	**Compliance risks** include the risk that laws, regulations, policies, procedures and contractual obligations will be breached. This would typically include risks associated with legal and regulatory obligations.

External risks	**External** risks are related to requirements or forces imposed on an organization from outside. The organization cannot control the likelihood they will occur; it can only prepare for and respond to them. It includes legal/regulatory, natural hazard, economic, technological, social and demographic risks.
Financial risks	**Financial risks** include the risk of loss of revenue and / or earnings as a result of price volatility, the inability to secure funding capital, increase in bad debts, etc. This would typically include risks associated with the market, credit; liquidity, solvency and capital availability.
Governance	The act of directing, controlling and evaluating the culture, policies, processes, laws, and mechanisms that define the structure by which organizations are directed and managed.
Inherent Risk	The exposure arising from risk factors in the absence of deliberate management intervention(s) to exercise control over such factors.
Integrated risk management	A continuous, pro-active and systematic process to understand, manage and communicate risk from a organizational-wide perspective in a cohesive and consistent manner. It requires an ongoing assessment at every level and in every sector of the organization, aggregating these results at the executive level, communicating them and ensuring adequate monitoring and review.
Internal Audit	An independent, objective assurance and advisory activity designed to add value and improve an organization's operations. It helps an organization accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes.
King IV report	King 4 report on corporate governance in South Africa, 2016, and specifically part 6.2: Supplement for organizations.
Operational risks	**Operational risks** could include the risk of loss resulting from inadequate or failed internal processes, people and systems, or from external events. This would typically include risks associated with business continuity; fraud; people; processes and systems.

Residual Risk	The remaining exposure after the mitigating effects of deliberate management intervention(s) to control such exposure (the remaining risk after management has put in place measures to control the inherent risk). However risk can also be reduced by transferring (outsourcing, sharing) of the management of that risk. This is extremely important in the business environment where outsourcing is a viable alternative to poor service delivery.
Risk	Risk is about the uncertainty of events, including the likelihood of such events occurring and its effects, both positive and negative, on the achievement of the organization's objectives. Risks include uncertain events with a potential positive effect on the organization (i.e. value creation opportunity) not being captured or not materialising.
Risk Appetite	Risk appetite can be defined as the amount and type of risk that an organization is willing to take in order to meet their strategic objectives. Organizations will have different risk appetites depending on their maturity, location, culture and objectives. A range of appetites exist for different risks and these may change over time.
Risk Management	Systematic and formalised processes to identify, assess, manage and monitor risks.
Risk Policy	The statement of the overall intentions and direction of an organization related to risk management.
Risk Tolerance	The amount of risk the organization is capable of bearing (as opposed to the amount of risk it is willing to take)
Strategic risk	**Strategic risks** are those internal and external events and scenarios that can inhibit an organization's ability to achieve its strategic objectives. This would typically include risks associated with governance, the business model and the industry/ economic environment.
Technology	Comprises the infrastructure, devices, systems and software that is used to record, analyse, report and maintain risk management information, to enable risk management decision-making.

5. Background

Organizations are bound by their strategic mandate to provide services or products in the interest of the public good. No organization has the luxury of functioning in a

risk-free environment and organizations are especially vulnerable to risks associated with fulfilling their mandates.

a. Risk management is a valuable management tool which increases an organization's prospects of success through minimising negative outcomes and optimising opportunities. Local and international trends confirm that risk management is a strategic imperative rather than an option within high performing organizations.

b. High performing organizations set clear and realistic objectives, develop appropriate strategies aligned to the objectives, understand the intrinsic risks associated therewith and direct resources towards managing such risks on the basis of cost-benefit principles.

c. Organizations should, in accordance with the previously mentioned prescripts under 6(a), implement and maintain effective, efficient and transparent systems of risk management and internal control.

d. The underlying intention of (d) above is that organizations should through the risk management process achieve, among other things, the following outcomes needed to underpin and enhance performance:

    - More sustainable and reliable delivery of services;
    - Informed decisions underpinned by appropriate rigour and analysis;
    - Innovation;
    - Reduced waste;
    - Prevention of fraud and corruption, unauthorised, fruitless and irregular expenditure;
    - Better value for money through more efficient and effective use of resources; and
    - Better outputs and outcomes through improved project and program management.

e. Risk management enables an organization to:

    - Increase the likelihood of achieving service delivery objectives;
    - Encourage proactive management;
    - Be continuously aware of the need to identify and treat risk throughout the organization;
    - Improve the identification of both opportunities and threats;
    - Comply with relevant legislative and regulatory requirements;
    - Improve stakeholder confidence and trust;
    - Improve governance on business, organizational manager and senior management level by:

i. Establishing a reliable basis for strategic and operational decision making and planning;
ii. Efficiently allocating and using resources for risk treatment;
iii. Improving operational effectiveness and efficiency;

- Enhance health and safety performance, as well as environmental protection;
- Improve controls and loss prevention and incident management; and
- Improve organizational learning.

6. Why organizations need risk management

Risk management provides a dedicated focus on risk for the following reasons:

6.1 Corporate governance

Corporate governance codes such as King IV expects an organization to implement a risk management plan. As a result of organization failures in the past, stakeholders do not want to be caught unawares by risk events. They expect that internal control and other risk mitigation mechanisms to be based on a thorough assessment of organization wide risks.

Stakeholders require assurance that management has taken the necessary steps to protect their interests. Board members, managers and stakeholders now want to know more about the risks facing an organization. This is understandable in an environment of complex and challenging service delivery expectations.

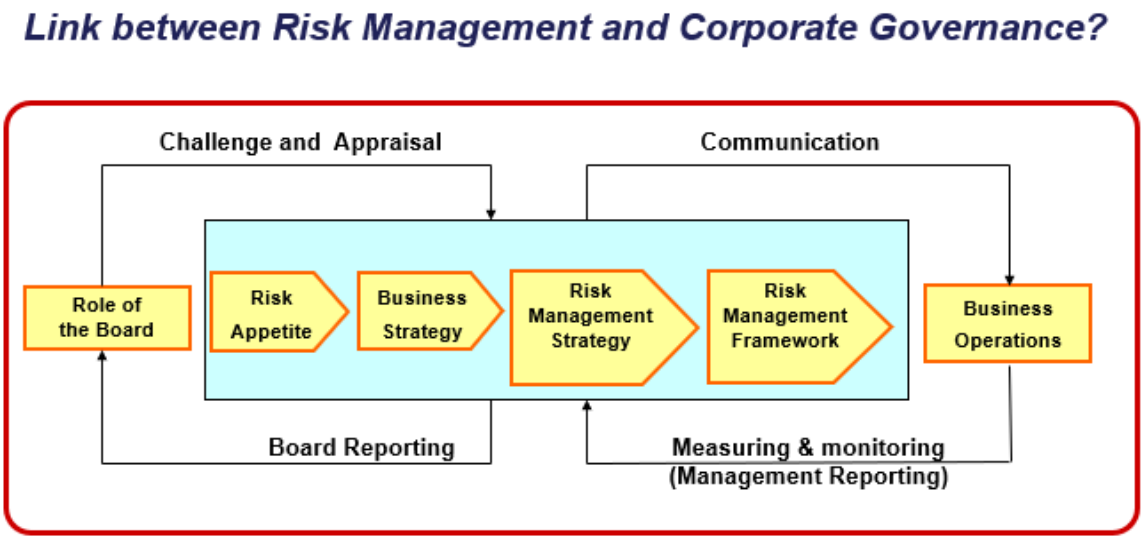


Figure 2: Risk management and corporate governance

6.2 Planning and organisation

The value of risk management is best leveraged when its principles and techniques are applied during organizational planning processes and organisation. Given the increased levels of volatility and uncertainty, it is vital that plans, particularly multiple year plans, take into consideration a thorough assessment of risks and mitigation strategies.

Hence, it becomes clear that planning and risk management are inter-dependent.

6.3 Continuous risk assessment

The risk profile of an organization is changing on an on-going basis. Some risks are created by changes initiated by the organization. *An example would be where a new CFO has been appointed or where the supplier master-file has been centralised.* Other risks are the result of changes in society, business, legislation or communities. *An example is where the credit rating of the country deteriorates, which has a significant impact on the interest rates, and eventually on the cost of servicing debt*. A once a year risk assessment will not elevate this to the decision-making level.

Even the best management teams will struggle to keep an accurate perspective of changing risks when risk management is approached on an informal basis.

The risk management plan must provide the organization with the ability to systematically identify new and emerging risks, and the assurance that existing risks are being addressed in the best possible way given current resource constraints and other challenges.

Change is often beyond the control of management, however, the risks it creates need to be managed as effectively as possible.

Figure 3 below illustrates continuous monitoring in the form of a robot, changing colours as risks materialise.

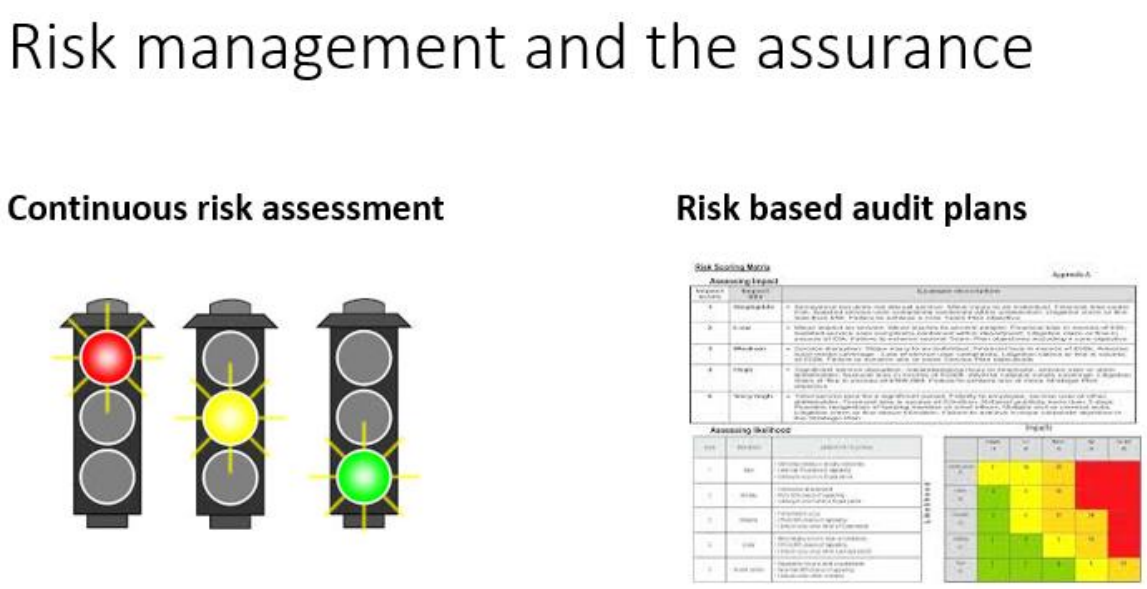


Figure 3: Continuous risk assessment and link to the risk based audit plan

6.4 Risk-based internal audit plans

Internal audit plans are now based on the outcomes of risk assessments. Internal auditors are increasingly basing their priorities on the risk management plan and give priority to high-risk assets and processes.

Internal audit is well-placed to independently evaluate the adequacy and effectiveness of key controls. The frameworks of internal control used by auditors are useful contributions to the risk management plan.

Internal audit is a key role player in providing assurance with regards to the effectiveness of risk management.

Figure 3 above illustrates the linkage between continuous risk assessment and the risk based audit plan.

6.5 Cultural adjustment

The essential behaviours of officials charged with responsibility for various activities of risk management must change. This requires a shift in the cultural dynamics insofar as it concerns risk management, which can be achieved through awareness and advocacy, communication, coaching, training and linking risk management to performance measures. Risk management must be a catalyst for change in behaviour of managers. Managers need to develop competencies to ensure that they make conscious risk-based decisions. Rather than viewing risk management and its associated activities as mere bureaucracy, managers need to look at it as a powerful driver of service delivery excellence.

7. Five lines of assurance

Every organization has objectives it strives to achieve. In pursuit of these objectives, the organization will encounter events and circumstances which may threaten the achievement of these objectives. These potential events and circumstances create risks an organization must identify, analyse, assess, and treat. Some risks may be accepted (in whole or in part) and some may be fully or partially mitigated to a point where they are at a level acceptable to the organization.

The Five lines of Assurance (5 LOA) [4], as illustrated below, addresses how specific duties related to risk and control could be assigned and coordinated within an organization, regardless of its size or complexity. Board members and management should understand the critical differences in roles and responsibilities of these duties and how they should be optimally assigned for the organization to have an increased likelihood of achieving its objectives. In particular, 5 LOA clarifies the difference and relationship between organizations' assurance and other monitoring activities - activities which can be misunderstood if not clearly defined.

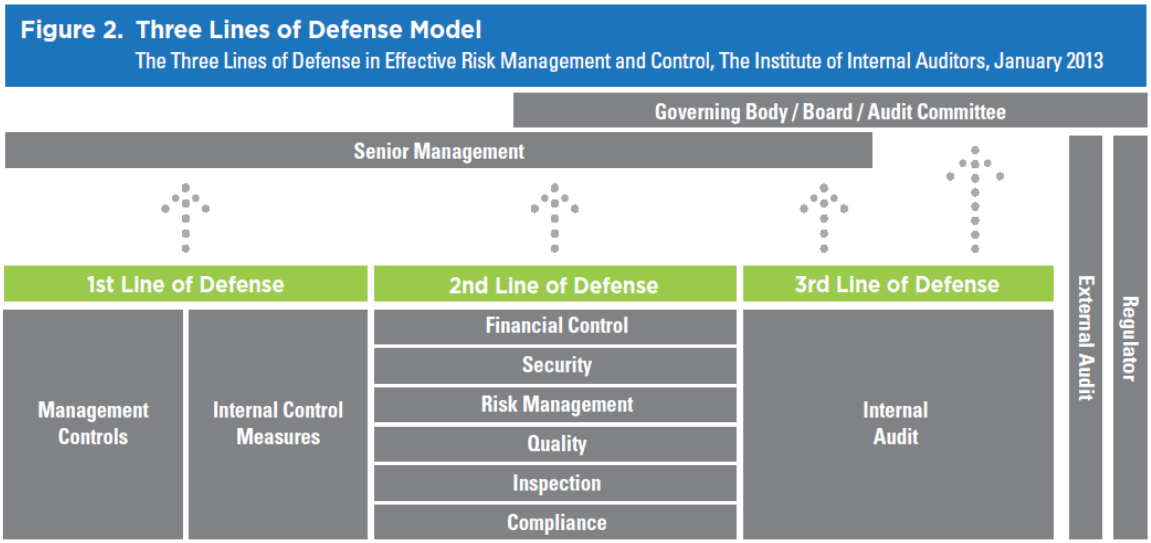


Diagram 1: Layers of the five lines of assurance

5 LOA enhances the understanding of risk management and control by clarifying roles and duties. Its underlying premise is that, under the oversight and direction of board and the organizational manager, three separate groups (or lines of assurance) within the organization are necessary for effective management of risk and control. The responsibilities of each of the groups (or 'lines') are:

[4]www.riskoversightsolutions.com

a. The **Board** who should steer and set strategic direction, approve policy and planning, oversee, monitor and ensure accountability;
b. The **Accounting Officer** who executes the strategic direction, policies and oversight responsibilities;
c. **Risk Owners** who manage risk and control (front line operating management);
d. **Risk Management** who monitors risk and control in support of management (risk, control, and compliance functions put in place by management); and
e. **Independent assurance provided by Internal and External Audit** to the Board through its Audit Committee and senior management concerning the effectiveness of the management of risk and control.

Each of the five lines plays a distinct role within the organization's wider governance framework. When each performs its assigned role effectively, it is more likely the organization will be successful in achieving its overall objectives. When an organization has properly structured its 5 LOA, and they operate effectively, there should be:

a. No gaps in risk and control coverage;
b. No unnecessary duplication of effort; and
c. A higher probably of risks and controls being effectively managed.

Regardless of how a particular organization structures its five lines of assurance, there are a few critical principles implicit in 5 LOA:

a. **<u>The first line of assurance</u>** lies with the process and risk owners whose activities create and/or manage the risks that can facilitate or prevent an organization's objectives from being achieved. This includes taking the right risks. The first line owns the risk, as well as the design and execution of the organization's controls to respond to those risks.

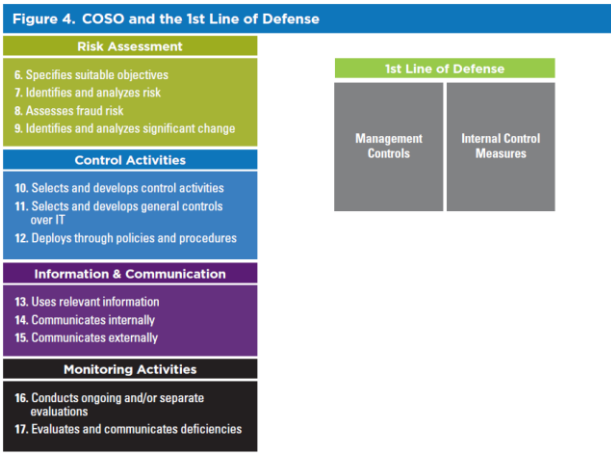


Diagram 2: First line of assurance

These include internal control processes designed to identify and assess significant risks, execute activities as intended, highlight inadequate processes, address control breakdowns, and communicate to key stakeholders of the activity. Operational managers must be adequately skilled to perform these tasks within their area of operations. Senior management has overall responsibility for all first line activities. For certain high-risk areas, senior management may also

provide direct oversight of front-line and mid-line management, even to the extent of performing some of the first line responsibilities themselves.

b. **<u>The second line</u>** is established to support management through particular expertise and process excellence, and management monitoring alongside the first line to help ensure that risks and controls are effectively managed.

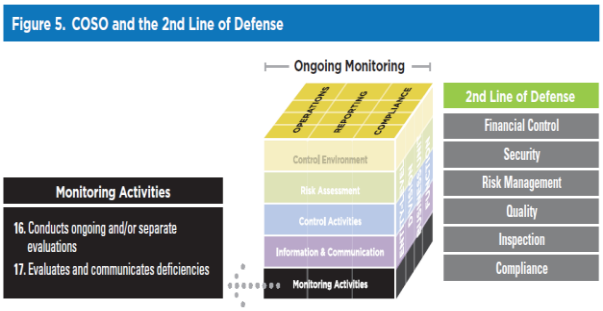


Diagram 3: Second line of assurance

These second line of assurance support functions are essentially advisory and oversight functions of their expertise applied to management processes, for example Risk Management 'owns' the Risk Management process methodology and provides both guidance and oversight to management (Risk Owners).

The second line of assurance includes various risk management and compliance functions to help ensure controls and risk management processes implemented by the first line of assurance are designed appropriately and operating as intended. These are management functions, separate from first-line operating management, but still under the control and direction of senior management.

Functions in the second line are typically responsible for <u>ongoing monitoring of risk and control.</u> They often work closely with operating management to help define risk management implementation strategy, provide expertise in risk management, guide the implementation of policies and procedures, and collate information to create an enterprise-wide view of risk and control.

The duties of the second line may also be retained by managers within the first line of assurance in smaller organizations. Typical second-line functions include specialised groups such as risk management, information security, financial control, physical security, quality, health and safety, inspection, compliance, and legal and environmental experts.

Under the oversight of senior management, second-line specialists monitor specific controls to determine whether the controls are functioning as intended. Monitoring activities performed by the second line typically cover all three categories of objectives, namely operational, reporting, and compliance.

The responsibilities of individuals within the second line of assurance vary widely but typically include:

- Assisting management in design and development of processes and controls to manage risks;
- Defining activities on how to monitor and measure success as compared to management expectations;
- Monitoring the adequacy and effectiveness of internal control activities;
- Escalating critical issues, emerging risks and outliers;
- Providing risk management frameworks;
- Identifying and monitoring known and emerging issues affecting the organization's risks and controls;
- Identifying shifts in the organization's implicit risk appetite and risk tolerance; and
- Providing guidance and training related to risk management and control processes.

c. **<u>The third line</u>** provides assurance to senior management and board over both the first and second lines' efforts consistent with the expectations of board and senior management. The third line of assurance is typically not permitted to perform management functions to protect its objectivity and organizational independence.

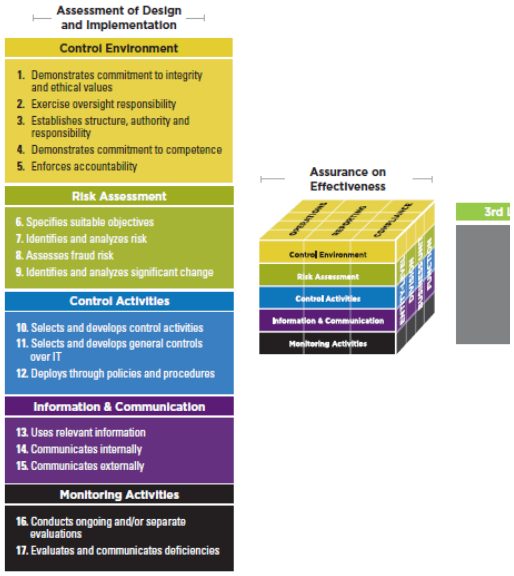


Diagram 4: Third line of assurance

In addition, the third line has a primary reporting line to the board by reporting to the audit committee. As such, the third line is purely an assurance function and not a management function, which separates it from the second line of assurance. Internal auditors serve as an organization's third line of assurance

The IIA defines internal auditing as "*an independent, objective assurance and consulting activity designed to add value and improve an organization's operations. It helps an organization accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes*." Among other roles, internal audit provides assurance regarding the efficiency and effectiveness of governance, risk management, and internal control.

Establishing a professional internal audit activity should therefore be a priority for all organizations. This is important not just for larger organizations but also for smaller entities. Smaller organizations may face equally complex environments with a less formal, robust organizational structure to ensure the effectiveness of governance and risk management processes, and may lack an effective second line of assurance.

d. **In the fourth line of assurance** senior management (represented in this model by die accounting officer) is accountable for the selection, development, and evaluation of the system of internal control with oversight by the board.

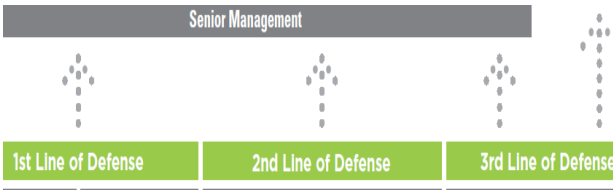


Diagram 5: Senior management's role

Senior management must fully support strong governance, risk management and control. In addition, they have ultimate responsibility for the activities of the first and second lines of assurance. Their engagement is critical for success of the overall model. COSO clearly identifies the responsibilities of the senior management to design and implement processes that:

i. Demonstrate commitment to integrity and ethical values;
ii. Exercise oversight responsibility;
iii. Establish structure, authority and responsibility;
iv. Demonstrate commitment to competence; and
v. Enforce accountability.

e. **Fifth line of assurance**

The Board and the Audit Committee fulfils the fifth line of assurance.

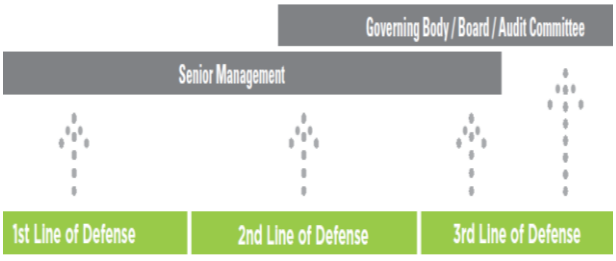


Diagram 6: Board and its committees

Senior management and the board collectively have responsibility for establishing an organization's objectives, defining high-level strategies to achieve those objectives, and establishing governance structures to best

manage risk. They are also the parties best positioned to ascertain the optimal organizational structure for roles and responsibilities related to risk and control.

King IV outlines the key principles that the board should endorse. The Board should:

i. Lead ethically and effectively and should govern the ethics of an organization in a way that supports an ethical culture;
ii. Appreciate that the organization's core purpose, its risks and opportunities, strategy, business model, performance and sustainable development are all inseparable elements of the value creation process;
iii. Comprise an appropriate balance of knowledge, skills and experience, diversity and independence to discharge it governance role and responsibilities objectively and effectively;
iv. Ensure that its arrangement for delegation within its own structures promote independent judgment, and assist with the balance of power and the effective discharge of its duties;
v. Govern risk in such a way to support the organization in setting and achieving its strategic objectives;
vi. Govern technology and information in a way that supports the organization in setting and achieving its strategic objectives;
vii. Govern compliance with applicable laws and adopted non-binding rules, codes and standards in a way that supports the organization being ethical and a good corporate citizen;
viii. 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 organization's external reports.

Chapter 2: Control environment and tone at the top

8. Introduction

An organization is as strong as its tone at the top, and as such the control environment should be evaluated as the first step. King IV recommends 16 principles that should embody the aspirations towards good governance. King IV has specific guidance for organizations, included in *Part 6.2 – Supplement for organizations* which includes that the board should ensure that assurance services enable an effective control environment and that these support the integrity of information for decision-making purposes.

9. Applicability

Evaluating the control environment requires a solid understanding of risk, the roles of the first three lines of assurance, and correlation between the different assurance providers.

The COSO ERM framework defined the elements of a strong tone at the top. It comprises elements that should be implemented and applied to ensure **that risk and controls are managed effectively**. COSO[5] has five elements which are supported by 17 principles. Compliance with the principles is tested by assessing supporting guidelines for these principles. As with most assessments, a matrix is applied to perform the assessment, which in line with this framework, is published as a control environment risk assessment.

[5] Leveraging COSO across the three lines of defence – IIA-INC – July 2015

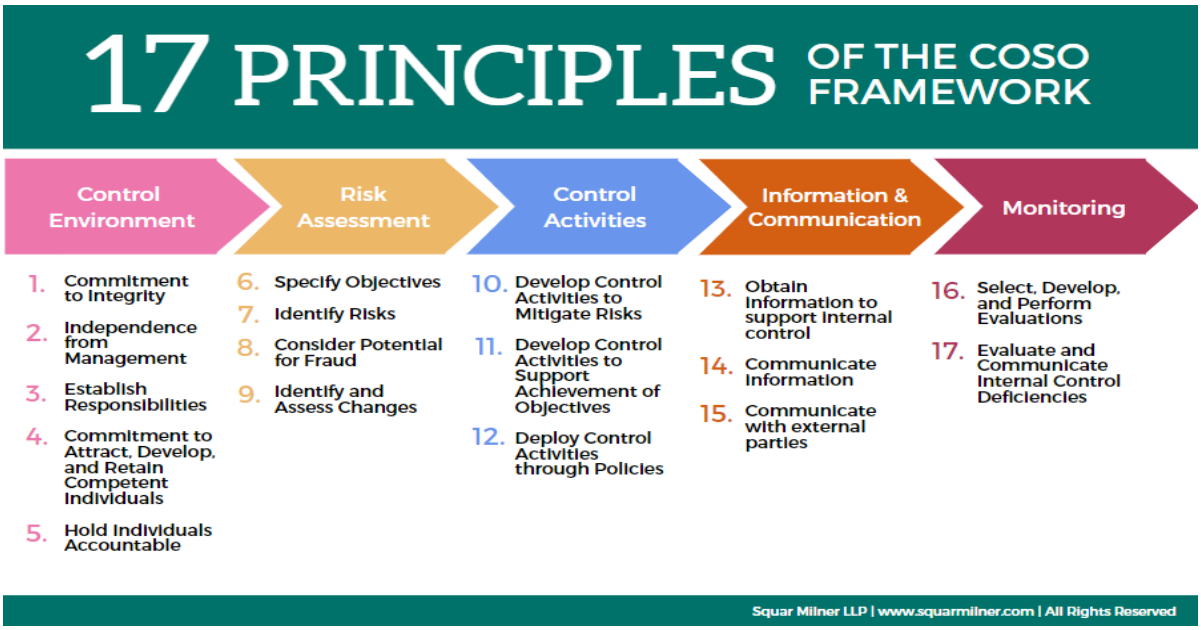


Figure 4: 17 principles of the COSO framework

Chapter 3: The risk universe

The risk (or event) identification process precedes risk assessment and produces a comprehensive list of risks (and often opportunities as well), organized by risk category (financial, operational, strategic, compliance) and sub-category (market, credit, liquidity, etc.) for business units, corporate functions, and capital projects. At this stage, a wide net is cast to understand the ***universe of risks*** making up the enterprise's risk profile. While each risk captured may be important to management at the function and business unit level, the list requires prioritization to focus senior management and board attention on key risks. This prioritization is accomplished by performing the risk assessment.

Figure 5 below indicates one example of a risk universe.

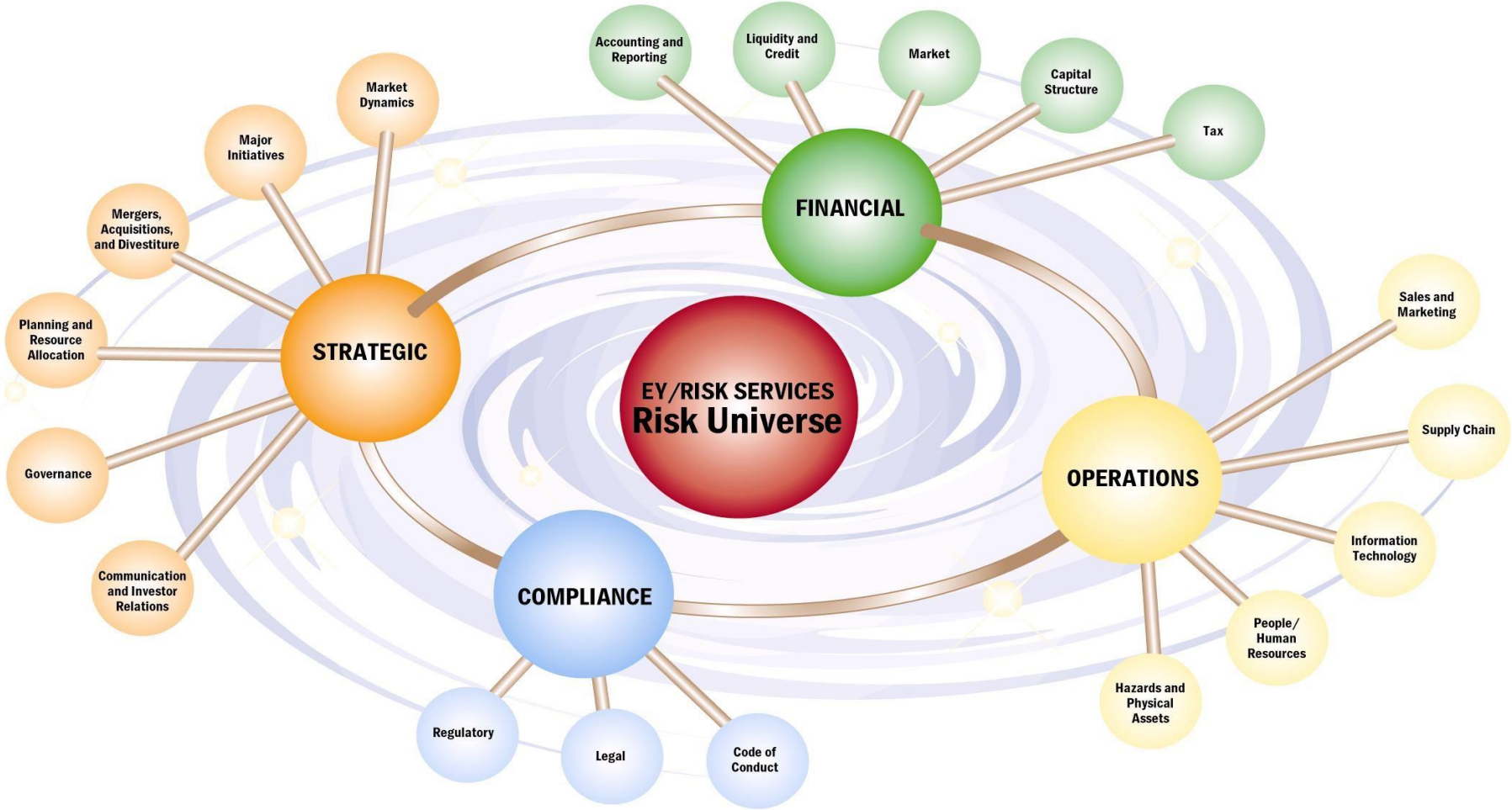

EY/RISK SERVICES
Risk Universe
FINANCIAL
Accounting and Reporting
Liquidity and Credit
Market
Capital Structure
Tax
STRATEGIC
Market Dynamics
Major Initiatives
Mergers, Acquisitions, and Divestiture
Planning and Resource Allocation
Governance
Communication and Investor Relations
OPERATIONS
Sales and Marketing
Supply Chain
Information Technology
People/ Human Resources
Hazards and Physical Assets
COMPLIANCE
Regulatory
Legal
Code of Conduct

Figure 5: Risk universe

Chapter 4: Aligning risk management to strategic planning processes

10. Introduction

In organizational strategy, whether defined in terms of a mission, vision and/or purpose, management sets out (with Business oversight) what the organization aspires to achieve – explicitly establishing the organization's broad-based reason for being.

Management then sets strategic objectives, formulates strategy, and establishes related operational implications, performance criteria, compliance requirements and reporting objectives for the organization.

While an organization's mission and strategic objectives are generally stable, its strategy and many related objectives are more dynamic and adjusted for changing internal and external conditions, and emerging risk scenarios. As they change, strategy and related objectives are realigned with strategic objectives.

Strategic objectives reflect management's choice as to how the organization will seek to create value for its stakeholders. In considering alternative ways to achieve its strategic objectives, management identifies and assesses risks associated with a range of strategy choices and consideration of their implications. This would be more evident in risk intelligent organizations.

11. Defining risk management strategy

The right place for an organization to start the design of its risk management strategy is to focus on the identification and management of strategic risks - those risks that are most consequential to a organizations ability to execute its strategy, achieve its operational objectives, and build and protect value.

12. Alignment between risk management and organizational objectives

Considering the definition above, an appropriate process of objective setting is a critical component of risk management. Risk management focuses primarily on:

a. Developing consistency of objectives and goals throughout the organization;
b. Identifying key success factors and associated key risk indicators and risks;
c. Assessing the risks and making informed responses;
d. Implementing appropriate risk responses, and establishing needed controls; and
e. Timely reporting of performance and expectations

Effective risk management provides reasonable assurance that an organization's reporting objectives are being achieved. Achieving reporting and compliance objectives is largely within the organization's control. But there is a difference when it comes to strategic and operational objectives, because their achievement is not solely within the organization's control. It is exposed to external events – such as change in government, mother of nature conditions, exchange rate fluctuations and oil prices – where an occurrence is beyond its control.

Management must ensure that the organization's objectives align with the organization's risk appetite. Misalignment could result in not accepting enough risk to achieve the objectives, or conversely, putting the organization's survival at risk by accepting too much risk.

13. Strategic risk assessment (SRA)

SRA is a systematic and continual process for assessing significant risks facing an organisation. In drafting a risk management strategy and implementation methodology, the right place to start is to focus on the identification and management of strategic risks – those risks that are most consequential to an organization's ability to execute its strategy, achieve its business objectives, and build and protect value.

The six steps for conducting a Strategic Risk Assessment can be summarised as follows:

a. Achieve a deep understanding of the strategic direction of the organization;
b. Gather views and data on strategic risks;
c. Prepare a preliminary risk strategy;
d. Validate and finalise the risk strategy;
e. Develop a Strategic Risk Management Implementation plan; and
f. Communicate and implement the risk strategy and strategic risk implementation plan.

The following table provides one layout of a strategic risk register. Strategic risk registers should rather be produced on excel spreadsheet in a horizontal format (fragmented risk management units). If an organization is already using software tools like BarnOwl or Teammate, it will be easier as the templates are part of the standardised design of the risk management software.

Elements of SRR	Strategic risk 1	Explanations
Strategic outcome	Financially sustainable organization, well maintained assets	Obtained from the strategic plan
Risk description	Irregular expenditure	
Risk category	Financial	Financial, operational or compliance - risk categories under the risk identification module
Root causes – internal	Over-riding of financial controls No second line of assurance No internal audit unit	Use the fishbone diagram to determine the potential root causes for the risk
Root causes – external	Political interference	Use the fishbone diagram to determine the potential root causes for the risk
Consequence	Cash flow pressure, Weak current ratio, Inability to borrow	Brainstorm the consequences should the risk materialise
Likelihood	5	Rate the likelihood of risk materialising on a level of 1 - 5
Impact	4	Rate the impact if risk materialises on a level of 1 - 5
Rating	20	Likelihood x impact and rate risk according to the assessment scale
Risk response	Mitigation	Identify risk response – mitigate, avoid, accept or transfer
Control processes	Bid evaluation and adjudication processes.	Identify current processes in place
Control effectiveness	Ineffective	Rate the effectiveness of the risk
Residual risk	20	Calculate the remaining risk
Risk appetite	Zero tolerance for irregular expenditure	Measure the residual risk against the risk appetite
Action plan	Implement accountability controls Establishing risk management/ internal audit unit.	

Table 1: Strategic risk register layout

Chapter 5: Risk Management Policy

14. Introduction

A formal risk management policy is intended to set out the organization's approach to risk. It introduces a common language and understanding of risk, demonstrates management ownership and endorsement of an approach and helps ensure that all employees have a sound basis for risk management decision-making and application. This policy needs to be worded in a way that contemplates all forms of risk. The policy should reflect the organization's overall goals and operating environment.

15. Policy

The risk management policy is a brief statement about the organization's commitment to risk management. The practical implications thereof can be replicated in the risk management plan. It is advisable to publish and circulate the risk management policy to existing and new staff as part of the risk awareness strategy.

The objectives of the risk management policy must be clearly defined such so that is is possible to determine and report on the extent of compliance against the policy. It could typically include the following:

a. Alignment of risk-taking behaviour with strategic business objectives;
b. Promote a risk management culture across the organization and improve risk transparency to the stakeholders;
c. Maximise stakeholders value and net worth by managing risks that may impact the defined financial and performance drivers;
d. The way in which conflicts of interest regarding risk management roles are dealt with;
e. The way in which risk management performance will be measured and reported;
f. A commitment to review and improve the risk management system periodically
g. Assist the Organization in enhancing and protecting those opportunities that represents the greatest service delivery benefits.

16. Focus areas of a risk management policy

The risk management policy acts as the primary internal risk governance mechanism, and as such it should provide all the guidance required for the broader organization to practice sound risk management, therefore enabling the successful drafting of a risk management plan to implement risk management at the operational business level. In practical terms this should guide:

a. Risk management and internal control objectives (governance);
b. Statement of the attitude of the organization to risk (risk philosophy and strategy);
c. Description of the risk culture or the control environment;
d. Level and nature of risk that is acceptable (risk appetite);
e. Risk management structure and arrangements (risk architecture);

f. Details of procedures for risk recognition and ranking (risk assessment);
g. List of documentation for analysing and reporting risk (risk protocols);
h. Risk mitigation requirements and control mechanisms (risk response);
i. Allocation of risk management roles and responsibilities;
j. Risk management training topics and priorities;
k. Criteria for monitoring and benchmarking of risks;
l. Allocation of appropriate resources to risk management; and
m. Risk activities and risk priorities for the coming year.

17. Risk categories

Risks originate from internal sources or from external sources. The table below provides guidance on typical risk categories of an organization, which would also be reflected in its Risk Universe (see Chapter 4 section 6 for an example of a business risk universe).

Tools such as PESTLE and STEEP are typically used to determine the key internal and external drivers of risk, which could be used to determine and draft the risk categories of an organization.

Internal risks **Risk Category**	**Description**
Human resources	Risks that relate to human resources of organization. These risks can have an effect on an organization's human capital with regard to: • Integrity & Honesty; • Recruitment; • Skills & competence; • Employee wellness; • Employee relations; • Retention; and • Occupational health & safety.
Knowledge and information management	Risks relating to an organization's management of knowledge and information. The following aspects relate to knowledge and information management: • Availability of information; • Stability of the information; • Reliability and integrity of information data; • Relevance of the information; • Retention; and • Safeguarding of data and information.
Litigation	Risks that the organization might suffer losses due to litigation and lawsuits against it. Losses from litigation can possibly emanate from:

	• Claims by employees, the public, service providers and other third parties; and • Failure by an organization to exercise certain right that is to its advantage.
Loss \ theft of assets	Risks that an organization might suffer losses due to either theft or loss of an asset of the organization.
Material resources (procurement risk)	Risks relating to an organization's material resources. Possible aspects to consider include: • Availability of material; • Costs and means of acquiring \ procuring resources; and • The wastage of material resources.
Information Technology	The risks relating specifically to the organization's IT objectives, infrastructure requirement, etc. Possible considerations could include the following when identifying applicable risks: • Security concerns; • Technology availability (uptime) • Applicability of IT infrastructure; • Integration / interface of the systems; • Effectiveness of technology; and • Obsolescence of technology.
Third party performance	Risks related to an organization's dependence on the performance of a third party. Risk in this regard could be that there is the likelihood that a service provider might not perform according to the service level agreement entered into with an organization. Non-performance could include: • Outright failure to perform • Not rendering the required service in time; • Not rendering the correct service; and • Inadequate / poor quality of performance.
Health & Safety	Risks from occupational health and safety issues e.g. injury on duty; outbreak of disease within the organization.
Disaster recovery and business continuity	Risks related to an organization's preparedness or absence thereto to disasters that could impact the normal functioning of the organization e.g. natural disasters, act of terrorism etc. This would lead to the disruption of processes and service delivery and could include the possible disruption of operations at the onset of a crisis to the resumption of critical activities. Factors to consider include: • Disaster management procedures; and • Contingency planning.

Compliance \ Regulatory	Risks related to the compliance requirements that an organization has to meet. Aspects to consider in this regard are: • Failure to monitor or enforce compliance; • Monitoring and enforcement mechanisms; • Consequences of non-compliance; and • Fines and penalties paid.
Fraud and corruption	These risks relate to illegal or improper acts by employees resulting in a loss of the organization's assets or resources and irregular expenditure.
Financial	Risks encompassing the entire scope of general financial management. Potential factors to consider include: • Cash flow adequacy and management thereof; • Liquidity and solvency; • Financial losses; • Fruitless and wasteful expenditure; • Budget allocations; • Financial statement integrity; • Revenue collection; and • Increasing operational expenditure.
Cultural	Risks relating to an organization's overall culture and control environment. The various factors related to organization culture include: • Communication channels and its effectiveness; • Cultural integration; • Entrenchment of ethics and values; • Goal alignment; and • Management operating style.
Reputation	Factors that could result in the tarnishing of an organization's reputation, public perception and image.

External risks	
Risk category	**Description**
Economic Environment	Risks related to the organization's economic environment. Factors to consider include: • Credit downgrade; • Inflation; • Foreign exchange fluctuations; and • Interest rates
Political Environment	Risks emanating from political factors and decisions that have an impact on the organization's mandate and operations. Possible factors to consider include: • Political unrest; • Local, Provincial and National elections; and • Changes in key office bearers.
Social environment	Risks related to the organization's social environment. Possible factors to consider include: • Unemployment; and • Migration of workers.
Natural environment	Risks relating to the organization's natural environment and its impact on normal operations. Consider factors such as: • Depletion of natural resources; • Environmental degradation; • Spillage; and • Pollution.
Technological environment	Risks emanating from the effects of advancements and changes in technology.
Legislative environment	Risks related to the organization's legislative environment e.g. changes in legislation, conflicting legislation.

Chapter 6: Risk identification and assessment

18. Introduction

Risk assessment is a systematic process to quantify or qualify the level of risk associated with a specific threat or event, to enrich the value of risk information available to the organization. The main purpose of risk assessment is to help the organization to prioritise the most important risks as the Organization is not expected to have the capacity to deal with all risks in an equal manner.

Risk assessment provides an understanding of risks, their causes, consequences and their probabilities. This provides input to decisions about:

a. whether an activity should be undertaken;
b. how to maximise opportunities;
c. whether risks need to be treated;
d. choosing between options with different risks;
e. prioritising risk treatment options; and
f. the most appropriate selection of risk treatment strategies that will bring adverse risks to a tolerable level

19. The purpose of a risk assessment

The purpose of risk assessment is to provide evidence-based information and analysis to make informed decisions on how to treat particular risks and how to select between options. Some of the principal benefits of performing risk assessment include:

a. understanding the risk and its potential impact upon objectives;
b. providing information for decision makers;
c. understanding of risks, in order to assist in selection of treatment options;
d. identifying the contributors to risks and weak links in systems and organization;
e. comparing of risks in alternative systems, technologies or approaches;
f. communicating risks and uncertainties;
g. assisting with establishing priorities;
h. contributing towards incident prevention through post-incident investigation;
i. selecting different forms of risk treatment;
j. meeting regulatory requirements;
k. providing information that will help evaluate whether the risk should be accepted when compared with pre-defined criteria.

20. The risk assessment process

Risks should be assessed on the basis of the likelihood of the risk occurring and the impact of its occurrence on the particular objective(s) it is likely to affect. Risks should be expressed in the same unit of measure used for the key performance indicator(s) concerned. In simplified terms, there should be high correlation between key performance indicators and key risk indicators.

Risk assessment should be performed through a three stage process:

a. Firstly, the inherent risk should be assessed to establish the level of exposure in the absence of deliberate management actions to influence the risk;
b. Secondly, a residual risk assessment should be performed to determine the actual remaining level of risk after the mitigating effects of management actions to influence the risk; and
c. Thirdly, the residual risk should be benchmarked against the Organization's risk appetite to determine the need for further management intervention, if any.

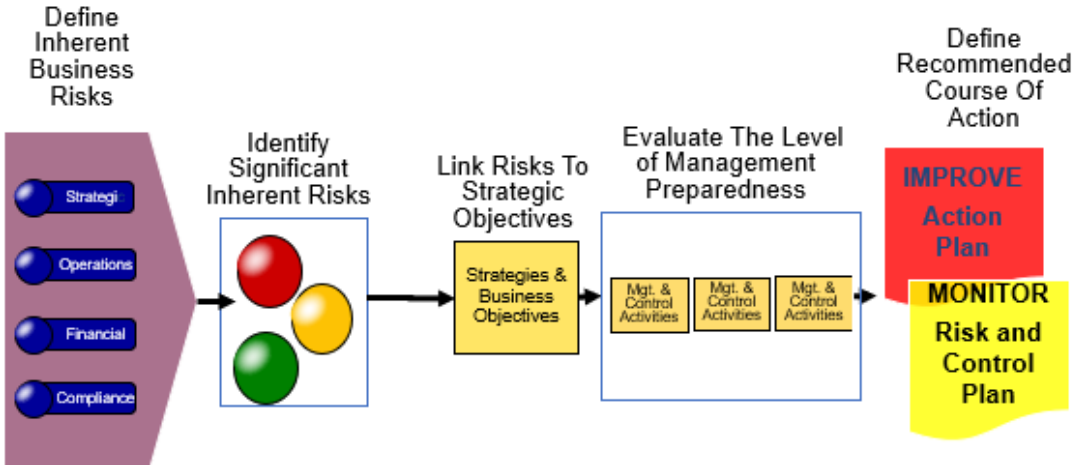


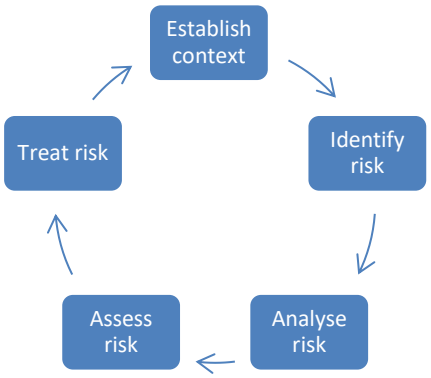
Figure 6: Risk assessment process

Risk assessment should be strengthened by supplementing management's perceptions of risks, inter alia, with:

a. review of the reports to the Audit Committee;
b. financial analyses, inclusive of liquidity and solvency analysis;
c. historic data analyses, which might include audit reports and incident reports and actual loss data;
d. interrogation of trends in key performance indicators;
e. benchmarking against organization of the same nature and size;
f. market and economic sector information;
g. scenario analyses; and
h. forecasting and stress testing.

Risk assessments should be re-performed for the key risks in response to significant environmental and/or organizational changes, but at least once a year, to ascertain the shift in the magnitude of risk and the need for further management action as a result thereof.

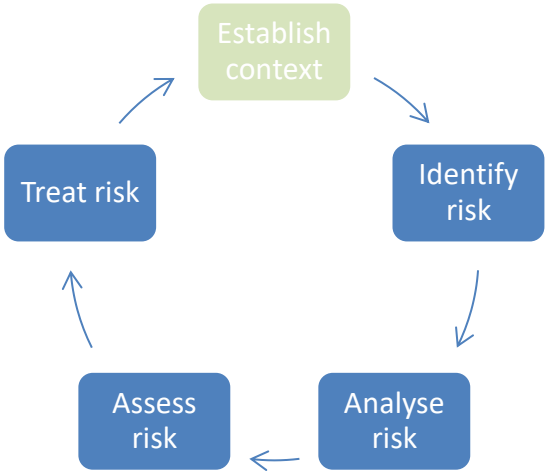
The outline below summarises the steps of the risk management process. It normally comprises of five phases.



Establish the context	Establishing context is about setting the parameters or boundaries around risk appetite and risk management activities. It requires consideration of external factors such as social, cultural, political and economic and alignment with internal factors such as strategy, resources and capabilities. The risk manager will need to establish context of the risk management processes which includes establishing a risk management policy, processes, methodologies, plans, risk rating criteria, training and reporting processes.
Identify the risk	Comprises of the processes for identifying, analysing and evaluating risks. Ideally, the organization will utilise a range of risk identification techniques including brainstorming, work breakdown analysis, and expert facilitation.
Analyse the risk	Risk analysis considers possible causes, sources, likelihood and consequences to establish the inherent risk. Existing management controls should be identified and effectiveness assessed to determine the level of residual risk.
Assess the risk	After this analysis, an evaluation of the level of risk is required to makes decisions about further risk treatment.
Treat the risk	Where the level of risk remains intolerable, risk treatment is necessary. Risk owners can treat risks by avoiding the risk, treating the risk sources, modifying likelihood, changing consequences or sharing elements of the risk. The remaining level of risk retained should be within risk appetite.

21. Risk context

Risk analysis requires a thorough understanding of the risk context, including its internal and external environment and the purpose of risk management activity. It also includes assigning roles and responsibilities of various parts of the organization participating in the risk management process. Understanding the external environment of an organization involves looking at the impact of the social, cultural, regulatory and political activities when developing risk management criteria. In this way it is possible to prepare for external threats and take advantage of externally generated opportunities.



The internal context highlights an organization's culture, its internal stakeholders, organization structure, and its human resource capabilities. It also looks at an organization's strategic goals, and its operational functions and processes involved in achieving its objectives. It further includes:

a. Policies, objectives, and the strategies that are in place to achieve them;
b. Capabilities, understood in terms of resources and knowledge (e.g. capital, time, people, processes, systems and technologies);
c. Inter-dependencies of the various management systems, functions and activities of the organization;
d. Information systems, information flows and decision-making processes (both formal and informal);
e. Relationships with, and perceptions and values of, internal stakeholders;
f. The organization's culture;
g. Standards, guidelines and models adopted by the organization; and
h. Form and extent of contractual relationships.

This helps an organization to set a strategic direction for risk management as a key component of the entire organization's operations. Establishing the context is not a once off step. It is ongoing as it ensures adaptability of organizational risk management to an ever changing internal and external environment.

22. Risk management context

Establishing the Risk Management Context involves determining the objectives, strategies, scope and parameters of the activities of the organization. The management of risk should be undertaken with full consideration of the need to justify the resources used in carrying out risk

management. The resources required, responsibilities and authorities, and the records to be kept should also be specified as part of the risk management context.

The risk management context will vary according to the needs of the organization and can involve:

a. Defining the goals and objectives of the risk management activities;
b. Defining responsibilities for and within the risk management process;
c. Defining the scope, as well as the depth and breadth of the risk management activities to be carried out, including specific inclusions and exclusions;
d. Defining the activity, process, function, project, product, service or asset in terms of time and location;
e. Defining the relationships between a particular project, process or activity and other projects, processes or activities of the organization ;
f. Defining the risk assessment methodologies;
g. Defining the way performance and effectiveness is evaluated in the management of risk;
h. Identifying and specifying the decisions that have to be made; and
i. Identifying, scoping or framing studies needed, their extent and objectives, and the resources required for such studies.

23. Risk criteria

An organization should define criteria to be used to evaluate the significance of risk. The risk criteria should reflect the organization's values, objectives and resources, and key measures of success, i.e. how an organization will know that it is performing.

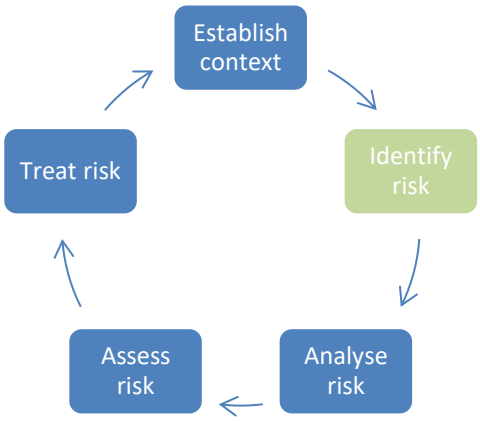
Some criteria can be imposed by, or derived from, legal and regulatory requirements and other requirements to which the organization subscribes. Risk criteria should be consistent with the organization's risk management policy, be defined at the beginning of any risk management process and be continually reviewed throughout the process.

When defining risk criteria, factors to be considered should include the following:

a. The nature and types of causes and consequences that can occur and how they will be measured (consequence/severity levels in the risk rating methodology);
b. How likelihood will be defined (likelihood levels in the risk rating methodology);
c. The timeframes of the likelihood and/or consequences;
d. How the level of risk is to be determined (risk rating);
e. The views of stakeholders;
f. The level at which risk becomes acceptable or tolerable; and
g. Whether combinations of multiple risks should be taken into account (interdependency) and, if so, how and which combinations should be considered.

24. Risk Identification

Risk identification is a deliberate and systematic effort to identify and document the Organization's key risks. The objective of risk identification is to understand what is at risk within the context of the organization's explicit and implicit objectives and to generate a comprehensive inventory of risks based on the threats and events that might prevent, degrade, delay or enhance the achievement of the objectives. This necessitated the development of risk identification guidelines to ensure that organizations manage risk effectively and efficiently.



25. The risk identification process

Comprehensive identification and recording of risks are critical, because a risk that is not identified at this stage may be excluded from further analysis. In order to manage risks effectively, an organization should know what risks they are faced with. The risk identification process should cover all risks, regardless of whether or not such risks are within the direct control of the organization. The organization should adopt a rigorous and on-going process of risk identification that also includes mechanisms to identify new and emerging risks timeously.

Risk identification should be inclusive, not overly rely on the inputs of a few senior officials and should also draw as much as possible on unbiased independent sources, including the perspectives of important stakeholders.

26. Risk workshops and interviews

Risk workshops and interviews are useful for identifying, filtering and screening risks but it is important that these judgment-based techniques be supplemented by more robust and sophisticated methods where required, including quantitative techniques.

Risk identification should be strengthened by supplementing management's perceptions of risks, inter alia, with:

- Review of external and internal audit reports;
- Financial analyses;
- Historic data analyses;
- Actual loss data;
- Interrogation of trends in key performance indicators;
- Benchmarking against peer group or quasi peer group;

- Market and sector information;
- Scenario analyses; and
- Forecasting and stress testing.

27. Focus points of risk identification

To ensure comprehensiveness of risk identification the organization should identify risk factors through considering both internal and external factors, through appropriate processes of:

Strategic risk identification

Strategic risk identification to identify risks emanating from the strategic choices made by the organization, specifically with regard to whether such choices weaken or strengthen the organization's ability to execute its Constitutional mandate:

- Strategic risk identification should precede the finalization of strategic choices to ensure that potential risk issues are factored into the decision making process for selecting the strategic options;
- Risks inherent to the selected strategic choices should be documented, assessed and managed through the normal functioning of the system of risk management; and
- Strategic risks should be formally reviewed concurrently with changes in strategy, or at least once a year to consider new and emerging risks.

Operational risk identification

Operational risk identification to identify risks concerned with the Organization’s operations:

- Operational risk identification should seek to establish vulnerabilities introduced by employees, internal processes and systems, contractors, regulatory authorities and external events;
- Operational risk identification should be an embedded continuous process to identify new and emerging risks and consider shifts in known risks through mechanisms such as management and committee meetings, environmental scanning, process reviews and the like; and
- Operational risk identification should be repeated when changes occur, or at least once a year, to identify new and emerging risks.

Project risk identification

Project risk identification to identify risks inherent to particular projects:

- Project risks should be identified for all major projects, covering the whole lifecycle of each project; and

- For long term projects, the project risk register should be reviewed on a regular basis, such as quarterly and annually to identify new and emerging risks.

Although some projects may be multi-year projects, it remains important to continuously identify emerging issues that could have an impact on project objectives – either positive or negative. This could include internal risks such as a change in available resources, and external implications such as national policy or legislative changes that may have an impact on the project outcomes.

28. How to perform risk identification

It is crucial to have knowledge of the institutional environment before commencing with risk identification process. It is also important to learn from both past experience and experience of others when considering the risks to which an organization may be exposed and the best strategy available for responding to those risks.

Risk identification starts with understanding the Organizational objectives, both implicit and explicit. The risk identification process must identify unwanted events, undesirable outcomes, emerging threats, as well as existing and emerging opportunities. By virtue of an organization's existence, risks will always prevail, whether the organization has controls or not.

When identifying risks, it is also important to bear in mind that "risk" also has an opportunity component. This means that there should also be a deliberate attention to identifying potential opportunities that could be exploited to improve organizational performance. In identifying risks, consideration should be given to risks associated with not pursuing an opportunity, e.g. failure to implement an IT system to collect organizational rates.

Risk identification exercise should not get bogged down in conceptual or theoretical detail. It should also not limit itself to a fixed list of risk categories, although such a list may be helpful.

The following are key steps necessary to effectively identify risks from across the organization:

- Understand what to consider when identifying risks;
- Gather information from different sources to identify risks;
- Apply risk identification tools and techniques;
- Document the risks;
- Document the risk identification process; and
- Assess the effectiveness of the risk identification process.

29. Understand what to consider when identifying risks

In order to develop a comprehensive list of risks, a systematic process should be used that starts with defining objectives and key success factors for their achievement. This can help provide confidence that the process of risk identification is complete and major issues have not been missed.

30. Gather information from different sources to identify risks

Good quality information is important in identifying risks. The starting point for risk identification may be historical information about this or a similar organization. Discussions with a wide range of stakeholders about historical, current and evolving issues, data analysis, review of performance indicators, economic information, loss data, scenario planning and the like can produce important risk information.

Furthermore, processes used during strategic planning like Strength Weakness Opportunity and Threat (SWOT) Analysis, Political Economic Social Technological Environment & Legal. (PESTLE) Analysis and benchmarking will have revealed important risks and opportunities that should not be ignored, i.e. they should be included in the risk register.

Certain disciplines like IT, Strategic Management, Health and Safety, etc. already have in place established risk identification methodologies as informed by their professional norms and standards. The risk identification process should recognize and utilize the outputs of these techniques in order not to "re-invent the wheel".

31. Apply risk identification tools and techniques

An organization should apply a set of risk identification tools and techniques that are suited to its objectives and capabilities, and to the risk the Organization faces. Relevant and up-to-date information is important in identifying risks. This should include suitable background information where possible. People with appropriate knowledge should be involved in identifying risks.

Approaches used to identify risks could include the use of checklists, judgments based on experience and records, flow charts, brainstorming, systems analysis, scenario analysis, and system engineering techniques.

- The approach used will depend on the nature of the activities under review, types of risks, the Organizational context, and the purpose of the risk management exercise.
- Team-based brainstorming for example, where facilitated workshops are used, is a preferred approach as it encourages commitment, considers different perspectives and incorporates differing experiences.
- Structured techniques such as flow charting, system design review, systems analysis, Hazard and Operability (HAZOP) studies and operational modelling should be used

where the potential consequences are catastrophic and the use of such intensive techniques are cost effective.

- Since risk workshops are useful only for filtering and screening of possible risks, it is important that the workshops are supplemented by more sophisticated or structured techniques described above.
- For less clearly defined situations, such as the identification of strategic risks, processes with a more general structure, such as 'what-if' and scenario analysis could be used.
- Where resources available for risk identification and analysis are constrained, the structure and approach may have to be adapted to achieve efficient outcomes within budget limitations. For example, where less time is available, a smaller number of key elements may be considered at a higher level, or a checklist may be used.

32. Document the risks identified

The risks identified during the risk identification are typically documented in a risk register that includes (at this stage):

- Risk description;
- How and why the risk can happen (i.e. causes and consequences); and
- The existing internal controls that may reduce the likelihood or consequences of the risks.

It is essential when identifying a risk to consider the following four elements:

- Description/event - an occurrence or a particular set of circumstances;
- Causes - the factors that may contribute to a risk occurring or increase;
- The likelihood of a risk occurring; and
- Consequences - the outcome(s) or impact(s) of an event.

It is the combination of these elements that make up a risk and this level of detail will enable an organization to better understand its risks.

33. Document your risk identification process

In addition to documenting identified risks, it is also necessary to document the risk identification process to help guide future risk identification exercises and to ensure good practices are maintained by drawing on lessons learned through previous exercises. Documentation of this step should include:

- The approach or method used for identifying risks;
- The scope covered by the identification;
- The participants in the risk identification; and
- The information sources consulted.

Experience has shown that management often disregards well controlled risks when documenting the risk profile of the Organization. It is stressed that a well-controlled risk must still be recorded in the risk profile of the Organization. The reason for this logic is that the processes for identifying risks should ignore at this point any mitigating factors (these will be considered when the risk is being assessed).

34. The outputs of risk identification

The document in which the risks are recorded is known as the "risk register" and it is the main output of a risk identification exercise.

A risk register is a comprehensive record of all risks across the organization or project depending on the purpose/context of the register. There is no single blueprint for the format of a risk register and organizations have a great degree of flexibility regarding how they lay out their documents.

The risk register serves three main purposes

- It is a source of information to report the key risks throughout the organization, as well as to key stakeholders.
- Management uses the risk register to focus their priority risks.
- It helps the auditors to focus their plans on the organization's top risks.

Once the risks have been identified, assessed and rated, and existing controls have been assessed, and it is has been established that controls are inadequate, a risk response strategy needs to be determined, i.e. an assessment, for example, of whether the risk is acceptable or whether it needs to be treated.

35. Risk Analysis

Risk analysis is a fundamental component of the risk management process. It helps to guide the evaluation of risks by defining the key parameters of the risk and how these may impact on the achievement of organization's objectives.

One of the key outcomes of the risk assessment process is determining levels of risk exposure for the organization. In addition, the data and related information collected during the risk assessment process can be used to assist in guiding risk response decisions.

36. Risk Analysis Methods

Methods used in analysing risks can be qualitative, semi-quantitative or quantitative. The degree of detail required will depend upon the particular application, the available data, the potential risks and the decision-making needs of the organization, or if prescribed by legislation.

a. **Qualitative assessment**: defines consequence, likelihood and level of risk by significance levels such as “high”, “medium” and “low”, may combine consequence and likelihood, and evaluates the resultant level of risk against qualitative criteria. In qualitative analysis there should be a clear explanation of all the terms employed and the basis for all criteria should be recorded.
b. **Semi-quantitative methods:** use numerical rating scales for consequence and likelihood descriptions and combine them to produce a level of risk using a formula. Scales may be linear or logarithmic, or have some other relationship and the formulae used can also vary.
c. **Quantitative analysis**: estimates numerical, practical values for consequences and their probabilities, and produces values of the level of risk in specific quantitative units. Full quantitative analysis may not always be possible due to insufficient data or information and often, due to the nature of the risk, the effort required of quantitative analysis is not warranted.

Even where full quantification has been carried out, it must be remembered that the calculations are estimates and they must not be attributed a level of accuracy and precision that is beyond the accuracy of the data and methods employed.

37. Risk analysis techniques

ISO 31010 lists several tools for risk analysis, but the more common ones are summarized below:

a. Root Cause Analysis

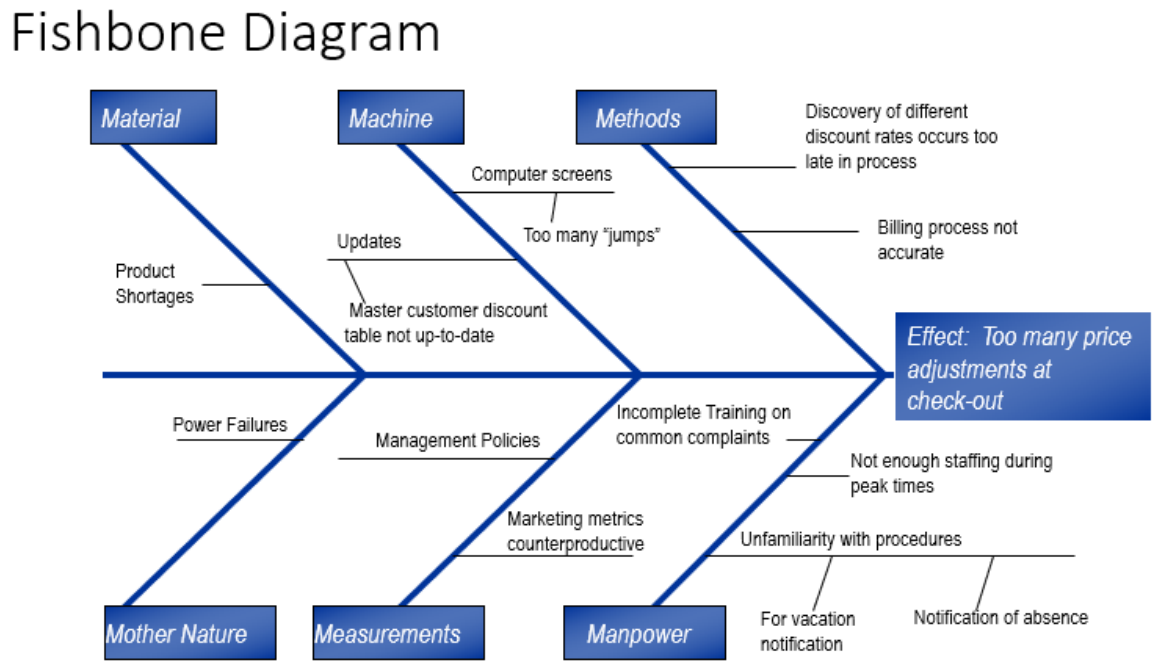
The analysis of a major loss to prevent its reoccurrence is referred to as Root Cause Analysis (RCA). It attempts to identify the root or original causes instead of dealing only with the immediately obvious symptoms. Corrective action may not always be entirely effective and continuous improvement may be required.

b. Cause-and-effect analysis

Cause-and-effect analysis identified possible causes of an undesirable event or problem and organises the contributory factors into broad categories so that all possible options can be considered. The information is organised in either a Fishbone (also called Ishikawa) or sometimes a tree diagram, and can be used as follows:

i. Provides a structured pictorial display of a list of causes of a specific effect. The effect may be positive (an objective) or negative (a problem) depending on context.
ii. Used consider all possible scenarios and causes generated by a team of experts and allows consensus to be established as to the most likely causes.
iii. It is most valuable at the beginning of an analysis to broaden thinking about possible causes that can be considered more formally late
iv. It allows for a structured way to identify root causes, and identifies six groups of root causes, namely:

- *Materials*, which includes lack of stock or medicines, lack of funding;
- *Machines*, which includes lack of equipment, or poorly designed application programs;
- *Methods*, which includes a lack of processes, or poorly designed processes;
- *Manpower*, which includes lack of staff or skills, management incompetence or high vacancy rates, poor ethical practices;
- *Measurements*, which include lack of dashboard, real-time monitoring of risks or lack of detection controls; and
- *Mother Nature*, which reflects on external risks or political interference.



c. Decision tree analysis

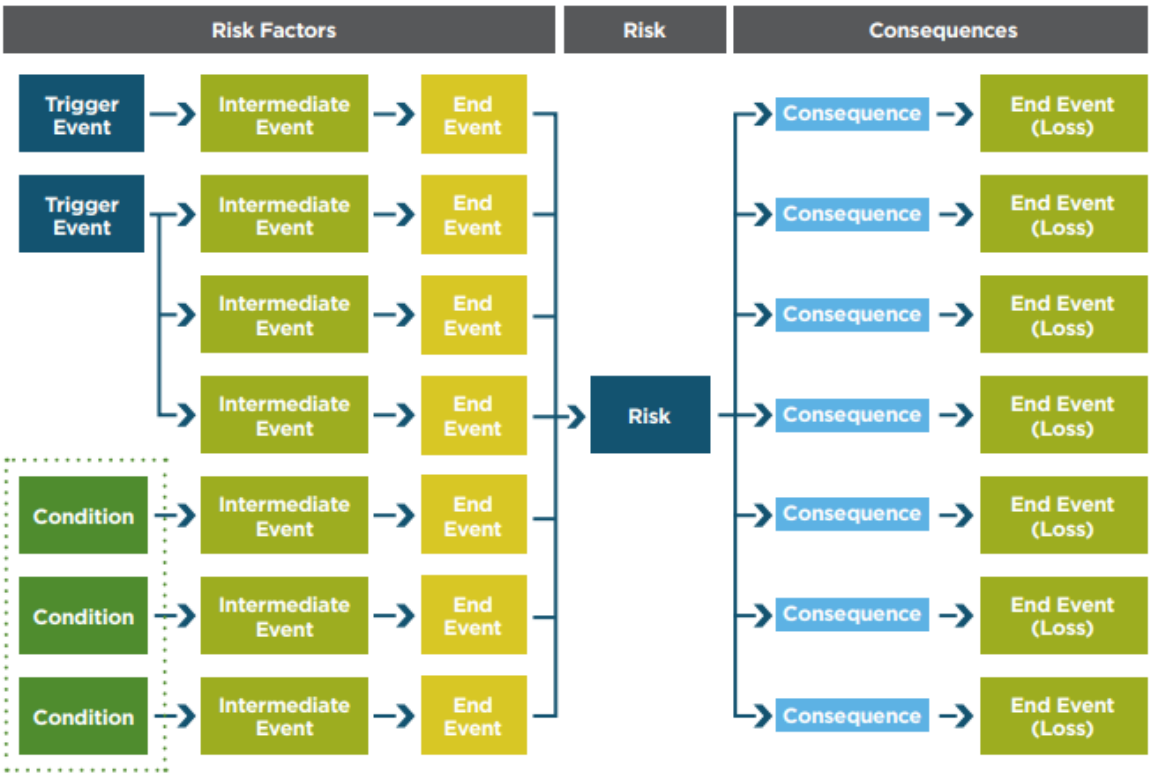
A decision tree represents decision alternatives and outcomes in a sequential manner which takes account of uncertain outcomes. It is similar to an event tree in that it starts from an initiating event or an initial decision and models different pathways and outcomes as a result of events that may occur and different decisions that may be made. It can be used as follows:

i. In managing project risks and to help select the best course of action where there is uncertainty; and
ii. For communicating decisions.

d. Bow Tie Analysis

Bow tie analysis is a simple diagrammatic way of describing and analysing the links within a risk from causes to consequences. A Bow Tie is similar to a combination of a fault tree analysing the causes of an event and an event tree analysing the consequences. It can be used as follows:

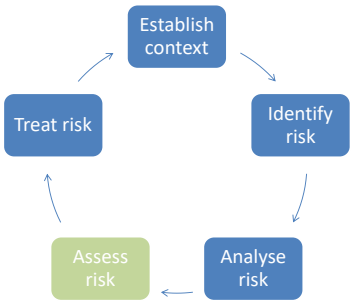
i. The focus of the bow tie is on the barriers between the causes and the risk, and the risk and consequences.
ii. Bow Ties show a range of possible causes and consequences.
iii. Bow tie analysis is often easier to understand than fault and event trees, and is a useful communication tool.



38. Risk assessment

Risk assessment involves interrogating risks at two levels, namely at the inherent risk level and the residual risk level, using the same rating criteria for each assessment.

Inherent risk considers the "worst case" scenario. This involves considering the likelihood and impact of the risk in the absence of any management control interventions. This level of assessment provides a perspective of the consequences of the risk to the organization in its unmanaged state.



The second tier of assessment concerns establishing the residual risk. Residual risk is the level of risk remaining after the mitigating influence of the existing control interventions is considered. Normally, management would introduce sufficient control to reduce the risk to within a pre-determined level, as informed by the optimal risk level. The residual risk is a critical indicator of whether the existing controls are effective in reducing the risk to an acceptable level.

When risks are assessed for the **fragmented** risk maturity status, the risks are assessed on a simplistic basis, as either high medium or low. When risk management has an **integrated** or **risk intelligent** status, risks are assessed on the basis of the likelihood of the risk occurring and the impact of its occurrence (Risk = Likelihood x Impact).

When assessing risk for risk intelligent organizations, additional risk criteria could be applied, such as the level of volatility of the risk (i.e. the rate at which the risk could change if not addressed and responded to). This will further facilitate decision-making regarding the urgency of addressing particular risks, i.e. including or excluding certain risks from a risk response strategy, depending on whether it will deteriorate of diminish over time.

The magnitude of the consequences of an event, should it occur, and the likelihood of the event and its associated consequences, should be assessed in the context of the effectiveness of the existing strategies and controls.

Consequences and likelihood may be estimated using statistical assessment and calculations. Where no reliable or relevant past data is available, subjective estimates may be made which reflect an individual's or Organization's degree of belief that a particular event or outcome will occur.

When rating the **impact** it is important to consider factors such as:

a. The value of transactions that pass through the process;
b. The importance of the activity in terms of the entity achieving its objective;
c. The impact this may have on other processes within the entity;
d. The geographical dispersion of operations;
e. Ethical climate and pressure on management to meet objectives;
f. Financial and economic conditions -frequency of losses;
g. Competency, adequacy and integrity of staff;
h. Management information - key measurable indicators; and
i. Degree of information being processed on computerised information systems.

Impact ratings can be defined as:

Impact	Description
Catastrophic	Loss of ability to sustain ongoing operations. A situation that would cause a standalone business to cease operation.
Major	Significant impact on achievement of strategic objectives and targets relating to the IDP of the organization.
Moderate	Disruption of normal operations with a limited effect on the achievement of strategic objectives or targets relating to the IDP.
Minor	No material impact on achievement of the organization's strategy or objectives.
Insignificant	Negligible impact.

Table 2: Inherent risk ratings

When rating the **likelihood** it is important to consider factors such as: -

a. Broad or vague legislative authority or regulations, missions, goals or objectives;
b. High degree of complexity;
c. Administration of contracts or grants;
d. Liquidity of assets;
e. Major restructuring of the organization;
f. Relationship with suppliers and customers;
g. Life expectancy of the internal control area;
h. Appropriateness of centralisation;
i. Classified or sensitive material;
j. Potential for conflict of interest; and
k. Management responsiveness.

The ratings can be defined as:

Likelihood	*Description*
Almost certain	*The risk is almost certain to occur more than once within the next 12 months. (Probability = 100% p.a.)*
Likely	*The risk is almost certain to occur once within the next 12 months. (Probability = 50 – 100% p.a.)*
Moderate	*The risk could occur at least once in the next 2 – 10 years. (Probability = 10 – 50% p.a.)*
Unlikely	*The risk could occur at least once in the next 10 - 100 years.*
Rare	*The risk will probably not occur, i.e. less than once in 100 years. (Probability = 0 – 1% p.a.)*

Table 3: Likelihood ratings

The most relevant sources of information and techniques should be used when analysing consequences and likelihood. Sources of information should include:

a. Past records, both financial and operational;
b. Audit reports from both internal and external auditors;
c. Current legislation;
d. Practice and relevant experience;
e. Relevant published literature;
f. Market research;

g. The results of public consultation;
h. Economic, engineering or other models; and
i. Specialist and expert judgments.

Techniques that can be utilised will include:

a. Structured interviews with experts in the area of interest;
b. Use of multi-disciplinary groups of experts;
c. Individual evaluations using questionnaires; and
d. Use of models and simulations.

Risk assessment should be performed in accordance with approved rating criteria for both likelihood and impact.

39. Determine the inherent risk rating

Once you have rated the likelihood and impact, combine the two to determine the overall risk rating.

Almost certain	5	10	15	20	25
Likely	4	8	12	16	20
Moderate	3	6	9	12	15
Unlikely	2	4	6	8	10
Rare	1	2	3	4	5
Likelihood	Insignificant	Minor	Moderate	Major	Catastrophic
	Impact				

RISK RATING: The colour coding will then lead to risk rating, which is reflected below:

Extreme	
High	
Moderate	
Low	

Table 4: Heatmap – risk rating

Based on the risk assessment, risks are classified by level to determine the appropriate level of response to those risks. Specific responses are defined at the "Risk Response" phase.

40. Identify and evaluate existing control effectiveness

Controls may reduce the likelihood of occurrence of a potential risk, the impact of such a risk, or both. Management then needs to assess the control effectiveness based on their understanding of the control environment currently in place. Residual risk will therefore inform management of the actual level of control effectiveness.

The business process method was identified as being the most widely used for application control review scoping. In today's world, many transactional applications are integrated into an ERP system. Because business transactions that flow through these ERP systems can touch several modules along their life cycle, the best way to perform the review is to use a business process or cycle approach (i.e., identifying the transactions that either create, change, or delete data within a business process and, at a minimum, testing the associated input, processing, and output application controls). The best way to approach the review is to break down the business processes using the fourlevel model:

a. Mega process (i.e., level 1): This refers to the complete end-to-end process, such as procure-to-pay.
b. Major process (i.e., level 2): This refers to the major components of the end-to-end process, such as procurement, receiving, and payment of goods.
c. Minor or subprocess (i.e., level 3): This level lists the minor or subprocess components of each of the major processes, such as requisitioning and purchase order creation.
d. Activity (i.e., level 4): This final level lists the system transactions that result in the creation, change, or deletion of data for each of the minor or subprocess components.

Mega Process (Level 1): Procure-to-Pay		
Major Process (Level 2)	**Subprocess (Level 3)**	**Activity (Level 4)**
Procurement	Requisition processing	Create, change, and delete
	Purchase order processing	Create, change, delete, approval, and release
Receiving	Goods receipt processing	Create, change, and delete
	Goods return processing	Create, change, and delete
Accounts Payable	Vendor management	Create, change, and delete
	Invoice processing	Create, change, and delete
	Credit memo processing	Create, change, and delete
	Process payments	Create, change, and delete
	Void payments	Create, change, and delete

Taking a business-centric view of application controls is essential to ensure that the review is comprehensive and meaningful to the organization. From this point forward, the review can be executed as a single engagement or as part of an integrated review.

Flowcharts are one of the most effective techniques used to capture the flow of transactions and their associated application and manual controls used within an end-to-end business process because they illustrate transaction flows. Figure 4 shows an example of a flowchart for a procure-to-pay process. Due to the difficulty of fitting the actual control descriptions on the flowchart, it is prudent to instead simply number the controls on the flowchart and have a separate document, such as a risk and controls matrix (see Figure 6, pg. 14-17), that contains the control descriptions and associated information. However, flowcharts may not be practical

for use all the time, and a process narrative would be more appropriate. This typically happens when an auditor is documenting the areas or work performed within the IT environment. In many cases, the work performed by IT and the related application controls do not flow in a linear manner as do business processes such as procure-to-pay.

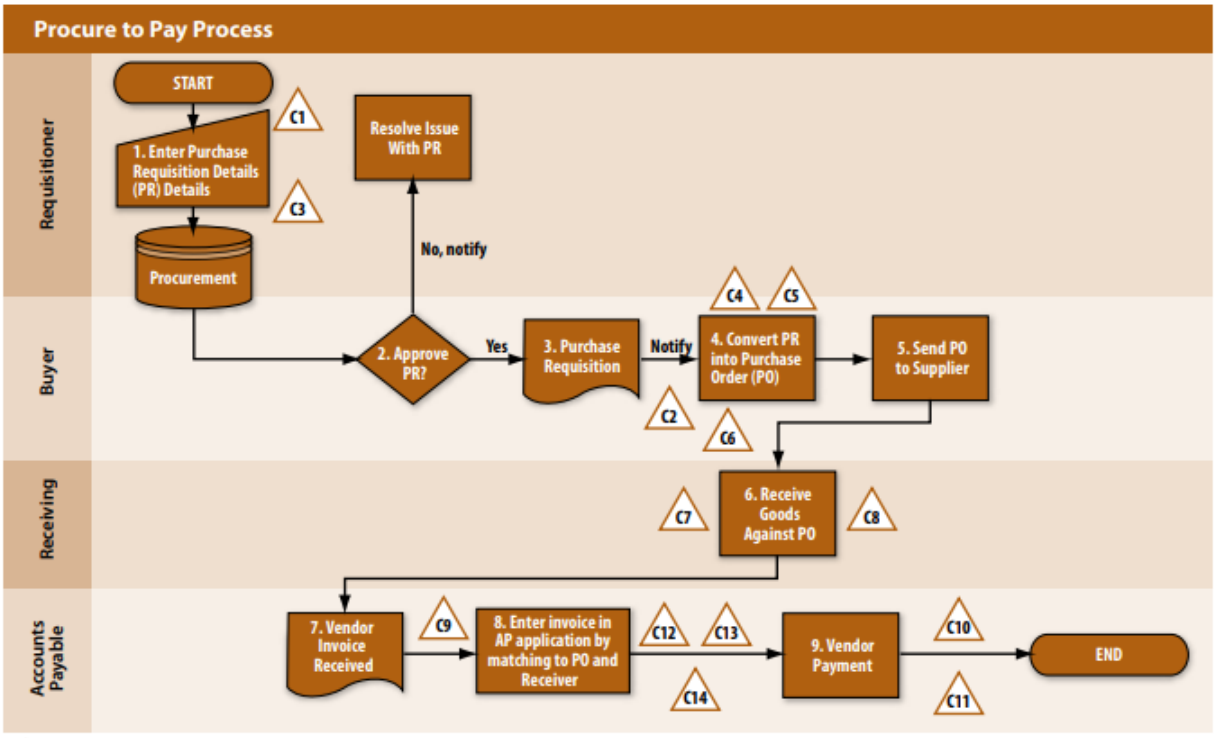


Figure 7: Process overview flowcharts

Controls should be considered on the basis of:

a. Design effectiveness - is the control "fit for purpose" in theory i.e. is the control designed appropriately for the function for which it is intended; and
b. Operational effectiveness - does the control work as practically intended. It is useful to involve staff with an understanding of the controls when rating them. Internal audit, business analysts and operational/ financial management can all provide input into control identification and assessment.

Risk and Control Matrix: Procure-to-Pay

	BUSINESS PROCESS & CONTROL OBJECTIVES	RISKS		CONTROL ACTIVITIES	COSO COMPONENTS					CONTROL ATTRIBUTES				CONTROL CLASSIFICATION						TESTING		
Number	Control Objectives	Risks	Impact/ Likelihood	Control Activities	CE	RA	CA	I/C	M	K (Y/N)	Man/Auto	Pre/Det	Frequency	Real	Recorded	Valued	Timely	Classified	Posted	Test Results	Operational Effectiveness (Y/N)	Notes

Figure 8: Risk and control Matrix

A well-designed and implemented control can often mitigate or reduce more than one risk or type of risk. Once effectiveness has been assessed, the residual risk rating can be calculated. Controls then need to be evaluated. The first step in the process of risk control evaluation is to

determine the adequacy of an individual control. This adequacy can be determined by asking questions around the control's design intent and purpose, its communication, whether performance parameters have been defined and whether the control requires continual maintenance.

The second step is to determine the effectiveness of the control, i.e. how well is it used, is the control available when required, is it used as intended, has it been checked/ validated?

Risk and Control Matrix: Procure-to-Pay

	BUSINESS PROCESS & CONTROL OBJECTIVES	RISKS		CONTROL ACTIVITIES	COSO COMPONENTS					CONTROL ATTRIBUTES				CONTROL CLASSIFICATION						TESTING		
Number	Control Objectives	Risks	Impact/ Likelihood	Control Activities	CE	RA	CA	I/C	M	K (Y/N)	Man/Auto	Pre/Det	Frequency	Real	Recorded	Valued	Timely	Classified	Posted	Test Results	Operational Effectiveness (Y/N)	Notes
	Major: Procurement																					
	Sub: Purchase Requisition Processing																					
	Activity: Create																					
C1	Controls provide reasonable assurance that purchase requisitions are created by authorized personnel completely and accurately.	Due to the lack of appropriate segregation of duties, a user is able to create, approve (i.e., release), assign, and convert a purchase requisition, resulting in the inappropriate rewarding of business to suppliers, overpayments, and excessive inventory levels.	H	Controls are such that access is granted only to those individuals with a business purpose for creating purchase requisitions.			X				A	P	Always	X	X	X		X	X			

Figure 9: Risk and control Matrix

For each control identified the risk control effectiveness value of the control must be established and rated. This can be done using the generic table below:

Risk Control Effectiveness	Interpretation
Fully effective	Controls are well designed for the risk - Review and monitor existing controls.
Partially effective	Most controls are designed adequately and operate effectively. Address control weaknesses or improve operational efficiency.
Ineffective	A number of controls are not being used as intended, or not designed to treat the root causes of the risk.
Totally ineffective	Significant weaknesses in control design, with many gaps. Redesign controls with focus on detection controls.
None	Inadequate design of controls/no controls in place to mitigate risk.

Table 4: Effectiveness ratings

41. Assessing of likelihood and consequence

The risk assessment allows for the identification of likelihood and impact of different risks, and the ability to integrate risks between different functions or responsibilities. Risk appetite is calculated, and residual risk is measured against the risk appetite. The future risk exposure is measured and reported to the 4th and 5th line of assurance as a matter of routine. The second line of assurance monitors risk exposure on an ongoing preventative basis and inform management timely when a risk might materialise. An example of such a risk register will have the following layout:

Elements of operational risk register	Operational risk 1	Explanations
Operational objective	Financially sustainable organization	Obtained from the strategic plan
Key performance indicator		
Risk description	Irregular expenditure	
Risk category	Financial	Financial, operational or compliance, etc
Root causes – internal	Over-riding of financial controls No second line of assurance	Use the fishbone diagram to determine the potential root causes for the risk
Root causes – external	Political interference	Use the fishbone diagram to determine the potential root causes for the risk
Consequence	Cash flow pressure Inability to borrow	Brainstorm the consequences should the risk materialise
Likelihood	5	Rate the likelihood of risk materialising on a level of 1 - 5
Impact	4	Rate the impact if risk materialises on a level of 1 - 5
Inherent risk rating	20	Multiply likelihood and impact and rate risk according to the assessment scale
Risk response	Mitigation	Identify risk response – mitigate, avoid, accept or transfer

Control processes implemented by management	Bid evaluation/ adjudication processes.	Identify current processes in place
Ongoing monitoring by risk management	Residual risk > risk appetite, automated aggregation and reporting to management, audit committee and internal audit	Ongoing monitoring by risk management
Control effectiveness	Effective	Rate the effectiveness of the risk. Combined assurance, inclusive of independent assurance by internal audit
Residual risk	9	Calculate the remaining risk
Risk appetite	Zero tolerance for irregular expenditure	Measure the residual risk against the risk appetite
Residual risk > risk appetite		Calculating the risk exposure
Continuous monitoring by management	Reported as a key risk indicator, measured against the key performance indicator above	Preventative reporting – risk is reported to management before it actually materialise
Ongoing monitoring		
Action plan	Implement accountability controls Allocate budget towards establishing risk management	
Responsible official	Organizational Manager	
Due date	June 2017	

Table 5: Operational risk register

42. Document risk assessment process

Documentation of the risk assessment process provides a record of how risks were analysed in previous periods, thereby informing future risk assessment exercises and providing consistency in how risks are identified, assessed and how decisions are made regarding how risks are responded to. A key outcome of documenting the risk assessment process is enabling accurate tracking of risks over time using historical reference data.

Documentation should include:

- Key assumptions and limitations;

- Sources of information used;
- Explanation of the assessment method, and the definitions of the terms used to specify the likelihood and consequences of each risk;
- Existing controls and their effectiveness;
- Description and severity of consequences;
- The likelihood of these specific occurrences; and
- Resulting level of risk.

Detailed documentation may not be required for very low risks; however a record should be kept of the rationale for initial screening of very low risks, for example, in a volatile environment where risks of low severity may change due to changing circumstances.

43. Risk assessment considerations

There are a number of other issues that must be considered in the context of risk assessment, which are noted below:

a. The risk assessment tables need to be consistently applied for all key risks in the organization.
b. Certain disciplines, for example, IT and Health and Safety, may utilise assessment methodologies that are informed by their professional norms and standards. In such circumstances, it would be prudent for the sake of the operational efficiency of these disciplines to allow them to use their preferred methodology. However, in order to maintain consistency at the organizational level the same risks should be re-assessed in terms of the organization-wide risk assessment methods.
c. The results of risk assessment could be represented in 'heat maps'. These are a simple graphical representation of each risk according to the two scales, namely likelihood and impact.
d. Assessment of likelihood more often than not imposes a challenge to management. Guidance in this respect can be obtained from the historical experience of the organization, as well as the experience of a similar organization.
e. The assessments must be considered together with the organization's risk appetite to determine whether the risk is acceptable or not. This in turn will inform whether additional interventions will be required.

44. Outputs

The output of risk assessment is a more sophisticated risk register which is enriched by the addition of ratings for each risk. This allows management to separate the more important risks from the less important ones and direct management attention accordingly.

45. Risk evaluation

The decision-making criteria should have been specified at the beginning of the risk management process and there may be other specific criteria mandated by legislation. Where risks are accepted ‘as is’ it is important to note any factors that may escalate them upwards, and hence require a response (consideration of the volatility of the risk and the risk environment).

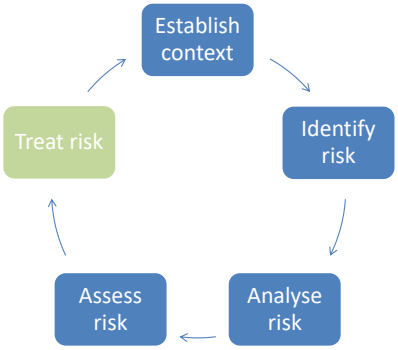
The decision about whether and how to treat the risk may depend on the costs and benefits of taking the risk and the costs and benefits of implementing improved controls. Following evaluation, risks can be divided into five bands as can be seen in the table below:

Risk index	Risk magnitude	Risk acceptability	Actions proposed
20 – 25		Unacceptable	Take action to reduce risk with highest priority
15 – 19			
10 – 14			Take action to reduce risk – inform management
5 – 9		Acceptable	Limited or no risk reduction, control and monitor, report to line manager.
1 – 4			

Table 6: Risk index

46. Treat the risk - risk response

A key outcome of the risk identification and assessment process is a detailed list of all key risks including those that require treatment as determined by the overall level of the risk against the organization's risk tolerance levels. However, not all risks will require treatment as some may be accepted by the organization and only require occasional monitoring throughout the period.



Although all key risks identified should be responded to, not all these risks will require treatment. The risks that fall outside of the organization's risk tolerance levels are those which pose a significant potential impact on the ability of the organization to achieve set objectives and therefore require treatment.

The purpose of responding to and treating risks is to minimize or eliminate the potential impact the risk may pose to the achievement of set objectives.

Risk response is concerned with developing strategies to reduce or eliminate the threats and events that create risks. Risk response should also make provision for the exploitation of opportunities to improve the performance of the organization. Responding to risk involves identifying and evaluating the range of possible options to mitigate risks and implementing the chosen option. Management should develop response strategies for all material risks, whether or not the management thereof is within the direct control of the organization, prioritising the risks exceeding or nearing the risk appetite level.

Where the management of the risk is within the control of the organization, the response strategies should consider:

a. Avoiding the risk by, for example, choosing a different strategy or terminating the activity that produces the risk;
b. Treating the risk by, for example, implementing or improving the internal control system;
c. Transferring the risk to another party more competent to manage it by, for example, contracting out services, establishing strategic partnerships or buying insurance;
d. Accepting the risk where cost and strategy considerations rule out alternative strategies; and
e. Exploiting the risk factors by implementing strategies to take advantage of the opportunities presented by such risk factors.

In instances where the management of risk is not within the control of the organization, the response strategies should consider measures such as forward planning and lobbying. Response strategies should be documented and the responsibilities and timelines attached thereto should be communicated to the relevant persons.

47. Developing a risk response strategy

Risk response plans identify responsibilities, schedules, the expected outcome of responses, budgets, performance measures and the review process to be set in place.

The risk response plan usually provides detail on:

a. Actions to be taken and the risks they address;
b. Who has responsibility for implementing the plan;
c. What resources are to be utilized;
d. The budget allocation;
e. The timetable for implementation; and
f. Details of the mechanism and frequency of review of the status of the response plan.

48. How to respond to risks?

Responding to risks involves the following key steps, each of which is covered in detail in this section:

a. Identify risk response options;
b. Select risk response options;
c. Assign risk ownership;
d. Prepare risk response plans; and
e. Identify risk response options.

Identify risk response options

Risk response design should be based on a comprehensive understanding of how risks arise. This includes understanding not only the immediate causes of an event but also the underlying factors that influence whether the proposed response will be effective.

Risk response options are not necessarily mutually exclusive or appropriate in all circumstances. They should include the following:

a. Avoiding risk – not engaging in the activity that creates risk exposure;
b. Mitigating risk – applying procedures that reduce the risk;
c. Transferring risks – transferring the risk exposure to other parties who may be better equipped or positioned to deal with it;
d. Exploiting risk – exploiting risks that represents an otherwise potential missed opportunity;
e. Accepting risk – accepting a risk with a low level of exposure;
f. Terminating risk – stopping the activity that gives rise to a risk higher than the acceptable level; and
g. Integrating some risks – applying some or all of the risk response to address a risk.

Select options for response

Once risks have been assessed and a level of risk rating has been assigned, an option for response is selected. Consideration should be given to the cost of the response option as compared to the likely risk reduction that will result.

For example, if the only available response option would cost in excess of R10m to implement and the cost impact of the risk is only R5m, it may not be advisable. It the risk volatility, however, is such that it may rapidly increase to exceed R10M, then this may become a viable decision.

In order to understand the costs and benefits associated with each risk response option, it is necessary to conduct a cost-benefit analysis.

Basic cost benefit analysis includes:

- Defining or breaking down the risk into its elements by drawing up a flowchart or list of inputs, outputs, activities and events;

- Calculating, researching or estimating the cost and benefit associated with each element. (Include, if possible, direct, indirect, financial and social costs and benefits); and
- Comparing the sum of the costs with the sum of the benefits.

Assign risk ownership

The Organizational Manager allocates responsibility for risk to an operational or functional area line manager.

Risk owners nominated by the Organizational Manager should assume responsibility for developing effective risk response plans. The risk owner (the person accountable for managing a particular risk) should be a manager with sufficient technical knowledge about the risk and/or risk area for which a response is required.

The risk owner will often delegate responsibility (but not accountability) to his/her direct reports or consultants for detailed plan development and implementation. Once the options have been brainstormed and assessed, a risk treatment plan will be developed. This can be a stand-alone plan, or additional columns on the risk register.

The process for developing the treatment plan is as follows:

a. Include the risk description and its risk rating in terms of consequence, likelihood and the overall rating.
b. List the treatment actions that were decided on following the risk treatment options discussion
c. Allocate a risk treatment owner who will take responsibility for the overall risk treatment.
d. Specific actions or tasks need to be determined to ensure the development of the Treatment Actions, i.e. the detailed steps.
e. Owners for the detailed actions or tasks need to be appointed
f. Resources that are required for achieving the tasks need to be determined, including financial, human and technical resources
g. The reporting requirements of progress with the completion of the tasks and actions need to be specified
h. Progress comments need to be made as part of the monitoring of the treatment action plan.

An example of a template is shown below:

Risk description:			Risk rating:			
Treatment action	Treatment owner	Actions	Action owners	Resources needed	Reporting	Progress

Prepare response plans

Once response options for individual risks have been selected, they should be consolidated into risk action plans and/or strategies.

As one risk response may impact on multiple risks, response actions for different risks need to be combined and compared so as to identify and resolve conflicts between plans and to reduce duplication of effort.

Response plans should:

- Identify responsibilities, schedules, the expected outcome of responses, budgets, performance measures and the review process to be set in place include mechanisms for assessing and monitoring response effectiveness, within the context of individual responsibilities;
- Determine processes for monitoring response plan progress against critical implementation milestones aligned with the organization's objectives. This information should all arise from the response design process; and
- Document how the chosen options will be implemented practically.

The successful implementation of the risk response plan requires an effective management system that specifies the methods chosen, assigns responsibilities and individual accountabilities for actions, and monitors them against specified criteria. Communication is a very important part of response plan implementation.

49. Opportunities versus threats

Measuring both the downsides and upsides of risk-taking provides a context that can be used to determine the type and amount of resources needed to support any project. Favourable outcomes, as projected by strategic planners and executive management, require a metric that is meaningful to the organization. For example, the risk should be measured in terms of its impact on service delivery.

A benefit of measuring risks as a group is that analysing the range of possible outcomes against what was actually achieved may also provide executive management with insights into individual operational performance capabilities.

To be sure, the benefits of identifying and assessing both risks and opportunities at the same time might seem obvious, yet it is rarely practiced. One reason is that the two most widely used tools currently employed in Enterprise Risk management (ERM) risk assessment are the risk register and risk heat map. The focus of both of these is only the perceived threats to an organization - they provide no consideration of the positive value that could be created by taking risks.

Risk registers and risk maps have value under certain circumstances. Based on our research and analysis, we conclude that:

- If the organizational goal is to respond only to known and identified threats, and the ERM process is viewed as an extension of audit and compliance, risk registers and risk heat maps can be useful.
- If the organizational goal is to respond to known threats and opportunities and gain risk intelligence about emerging perils on the horizon, traditional risk registers and risk heat maps fall short.
- If the organizational goal is to grow service delivery and create value for stakeholders, traditional risk registers and risk heat maps are useless.
- A new tool is required to measure both risks and opportunities. One example of such a tool is the Value Map – displayed below. Here both the threats and the opportunities are displayed.

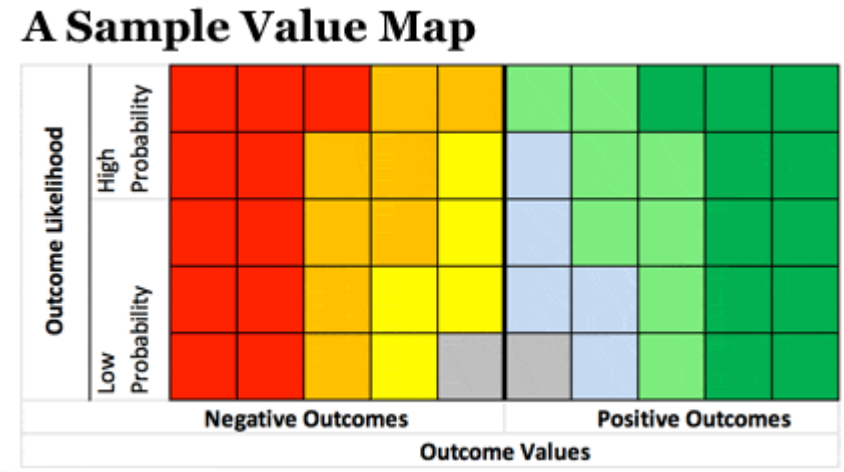


Diagram 3: A Sample Value Map

A Value Map is a graphical illustration of both threats and opportunities. Because threats and opportunities are two sides of the same coin, a value map also has two sides, as illustrated above. Threats (negative outcomes) are plotted on the left side of the map, while opportunities (positive outcomes) are located on the right side. Those outcome values may be measures of successful service delivery or a project's *net present value*, for example.

The vertical axis shows the relative likelihood of an event happening. Rather than plotting a single point on a risk map, the value map illustrates the range of the magnitude of each situation.

The net value of threat(s) versus opportunity(ies) could then be determined, for example, for pursuing a particular organizational strategy.

Chapter 7: Risk Appetite and Risk Tolerance

50. Introduction

Enterprise risk management enables management to identify, assess, and manage risks in the face of uncertainty, and is integral to value creation and preservation, which should lie at the core of an organization's strategy. All entities face uncertainty, and the challenge for management is to determine how much uncertainty it is prepared to accept as it strives to grow stakeholder value. This level of uncertainty an organization is prepared to accept, is termed it risk appetite. There is a distinct relationship between an entity's risk appetite and its strategy. An organization must consider its risk appetite at the same time it decides which goals or operational tactics to pursue. Usually any of a number of different strategies can be designed to achieve desired growth and return goals, each having different risks.

Risk intelligent organizations will apply and align both principles of risk appetite (strategic) and tolerance (operational), based on the organization's risk bearing capacity.

Organizations express risk appetite as the level of risk they will accept in providing value to their stakeholders. It is not always efficient or possible to manage risks to zero residual risk or a very low residual risk threshold because of the time, cost and effort that will be required, and which could result in the cost-benefit dynamics to become skewed. On the other hand it is also poor management practice to accept risks which create unnecessary exposure for the organization.

If an organization is making decisions regarding their credit control policy and the implementation of a *cut and collect* process, the risk appetite might be a collection rate of 85% and a current ratio of 1,5:1. This means that failing to collect 15% of outstanding debtors will still allow an organization to pay its short term creditors. Risk tolerance however, determines that if an organization only collects 78% of their debtors, the current ratios will deteriorate to 0,9:1, which is creating a material uncertainty to operate as a going concern.

The COSO ERM framework sets out five principles related to risk appetite:

a. It is a guidepost in strategy setting;
b. It influences resource allocation;
c. It aligns the organization with people, processes, and infrastructure;
d. It reflects the entity's risk management philosophy and influences the culture and operating style; and
e. It is considered in strategy setting so that strategy aligns with risk appetite.

When developing the risk appetite for an organization, there are a number of considerations that come into play, including:

a. The existing risk profile, as an indication of the risks it currently addresses;
b. The organization's capacity to take on extra risk in seeking its objectives;
c. The organization's attitude towards growth, risk and return; and
d. The acceptable level of variation an entity is willing to accept regarding the pursuit of its objectives.

Given the aforementioned dynamics it is important for the organization to make an informed decision on the amount of risk the organization is capable of bearing as part of normal management practice. This level of acceptable risk is known as a "tolerated risk" or "tolerance level" and establishes the benchmark for the organization's risk tolerance. This differs from risk appetite which is the amount of residual risk that an organization is willing accept. More often than not, risk appetite in an organization is set as the total impact of risk an organization is willing to accept regardless of whether it has the necessary capacity to recover from such impact. It would be more prudent and risk intelligent for an organization to define its risk appetite to remain within its risk bearing capacity. Risk appetite differs from organization to organization and can equally differ in terms of various categories of risk an organization may face at a point in time.

The aim of defining risk tolerance is to get people to think effectively about risk when they make important decisions. Performance management systems encourage officials to think about targets and rewards for meeting them. However the systems should equally tell officials about what management wants and what it does not want. In essence, effective risk taking that is aligned to overall organizational strategy should be a core skill and competency, especially in a risk intelligent organization.

Tolerance levels may vary by context and are influenced by the following:

- Ability and willingness of the Organizational Manager to take and manage risks;
- Size and type of organization;
- Skills and experience of officials;
- Maturity and sophistication of risk management processes and control environments;
- The current level of an organization's performance;
- The liquidity of an organization and its ability to pay short term liabilities and operational expenditure; and
- The solvency of the organization and its ability to withstand significant impact on its net asset value.

51. Approach

An organization's risk appetite should be reviewed annually to align it to new circumstances. The risk appetite should also be visited during the six-monthly adjustment budget process. Specific attention should be given to determine whether revenue collection estimates are still achievable, and to what extent under collection of revenue will influence liquidity and its effect on the risk appetite.

The risk tolerance levels should also be reviewed annually together with the organization's targets and the budget to determine the organization's risk bearing capacity. In addition it is important for management to be explicit about the bare minimum levels of performance. Failing to deliver on the bare minimum service requirements will affect the consumer's willingness to pay for services, and consequently might lead to non-payment and increased liquidity risk. Legal risk becomes more relevant in these cases and contingent liabilities normally increase as consumers and suppliers take legal action against the organization.

It is advisable to determine and communicate the level of unexpected losses that the organization is willing to accept in the event the risk materializes. These levels should be documented and communicated to all key stakeholders involved in the management of the risk. Zero tolerance risk exposures such as fraud and corruption, regulatory compliance unauthorised and irregular expenditure and health safety should be determined and communicated to all officials.

As management decisions are informed by targets being pursued, there should be a mechanism in place, which enables tracking of numbers involved to ensure that tolerance guidelines are complied with or applied as specified. This may require management to determine key risk drivers and to monitor performance in relation to actual risk event occurrences. Setting risk tolerance will assist management to monitor events and their impact against the stated risk appetite.

There is no "one-size fits all" approach to establishing the right risk tolerance levels. Practices will differ amongst organization based on the maturity of the risk management practice, available data, management expertise, sector specific dynamics and other pertinent factors. Thus it is advisable to rather follow certain guiding principles rather than "hard and fast" rules.

A risk appetite statement effectively sets the tone for risk management. The organization is more likely to meet its strategic goals when its appetite for risk is linked to operational, compliance and reporting objectives. A risk appetite statement is useful only if it is clear and can be communicated, interpreted and implemented across the organization. It therefore should:

a. Directly link to the organization's objectives;
b. Be stated precisely enough so that it can be communicated throughout the organization, can be monitored, and can be adjusted over time;
c. Help with setting acceptable tolerances for risk, thereby identifying the parameters of acceptable risk;
d. Facilitate alignment of people, processes, and infrastructure in pursuing organizational objectives within acceptable ranges of risk;
e. Facilitate monitoring of the competitive environment and considers shareholders' views in identifying the need to reassess or more fully communicate the risk appetite
f. Recognise that risk is temporal, volatile and relates to the time frame of the objectives being pursued;
g. Recognise that the organization has a portfolio of projects and objectives, as well as a portfolio of risks to manage, implying that risk appetite has meaning at the individual objective level and at the portfolio level.

Risk tolerance relates to risk appetite but differs in one fundamental way: risk tolerance represents the application of risk appetite to specific objectives. Risk tolerance can be defined as the acceptable levels of variation relative to the achievement of objectives.

While risk appetite is broad, risk tolerance is tactical and operational. Because risk tolerance is defined within the context of objectives and risk appetite, it should be communicated using the metrics in place to measure performance. Risk tolerance is best measured in the same units as

the related objectives, and associated performance criteria. In that way, risk tolerance sets the boundaries of acceptable performance variability.

The typical steps involved in establishing and implementing risk tolerance are:

- Complete an analysis of the organization's ability to physically and financially recover from a significant event (e.g. risk such as human influenza pandemic, inability to supply, credit crunch, etc.).
- The above analysis will highlight the need and importance of contingency plans, financial, physical and human resources and the importance of controls. From the analysis, determine the tolerance the organization can bear or accept.
- Management determines the level of tolerance which should then be endorsed by the Organizational Manager.
- The risk tolerance levels set by the organization will be reflected in the risk rating scales used to assess the risks:
    - An upper band where adverse risks are intolerable, whatever benefits the activity may bring, and risk reduction measures are essential whatever their cost.
    - A middle band (or 'grey' area) where costs and benefits are taken into account and opportunities balanced against potential adverse consequences.
    - A lower band where positive or negative risks are negligible, or the costs associated with implementing treatment actions outweigh the costs of the impact of the risk should it occur.

These levels of risk tolerance will help determine the type and extent of actions required to treat risks, and the level of management attention required in managing and monitoring the risks.

52. Calculating risk appetite

Risk appetite statements often start out broad and become more precise as they cascade into functions and operations across the organization. Some organizations find that broad qualitative statements crafted around terms such as “low”, “medium” and “high” appetite meet their requirements. Others are more precise, making more quantitative statements like “we are not comfortable with a current ratio of smaller than 2:1 as it will prevent us achieving our service delivery objectives”.

Quantitative approaches could be built on more sophisticated metrics like *economic value at risk* and/or *financial strength at risk*. Common methods for expressing risk appetite include:

a. Setting a boundary on a probability and impact grid;
b. Economic capital measures/balance sheet-based expressions;
c. Changes in credit ratings (headroom before a potential downgrade);
d. Profit and loss measures (e.g. tolerable level of annual loss);
e. Value based measures (based on probability of ruin or default);
f. Limits/targets or thresholds for key indicators (e.g. +/- 5% variation in profit or 1 - 2.5% variation in revenue);
g. Qualitative statements (e.g. zero tolerance for regulatory breaches or loss of life)

The table below indicates some of the metrics that can be used for different risk types:

Risk type	Metric	Risk tolerance range
Strategic	Going concern issues	Zero tolerance
	Minimum service delivery levels	80-90%
	Own revenue growth	10%
Financial, credit and liquidity risk	Current ratio	2.5 : 1
	Debt impairment	< 5%
	Debtors collection days	55 days
	Creditor payment days	60 days
Operational risk	Vacancy rate	< 10%
	% High risk control issues	<10%
	% Ineffective controls – assessed by both internal/external audit	<5%
	% cyber incidents with high impact	0
Compliance risk	Unauthorised expenditure	< 5%
	Fruitless and wasteful expenditure	< 5%
	Irregular expenditure	< 5%
	High impact non-compliance issues	0
	Assurance on effectiveness	90%
Reputational risk	Retention of key managers	>80%
	Customer satisfaction – delivery protests	>85%
	Legal, regulatory and ethical events	0

Table 7: Risk tolerance

Which type of statement is best for a particular entity is a management decision. As an organization become more experienced in risk management, they can start moving away from broad low, medium and high statements, to statements that are more precise.

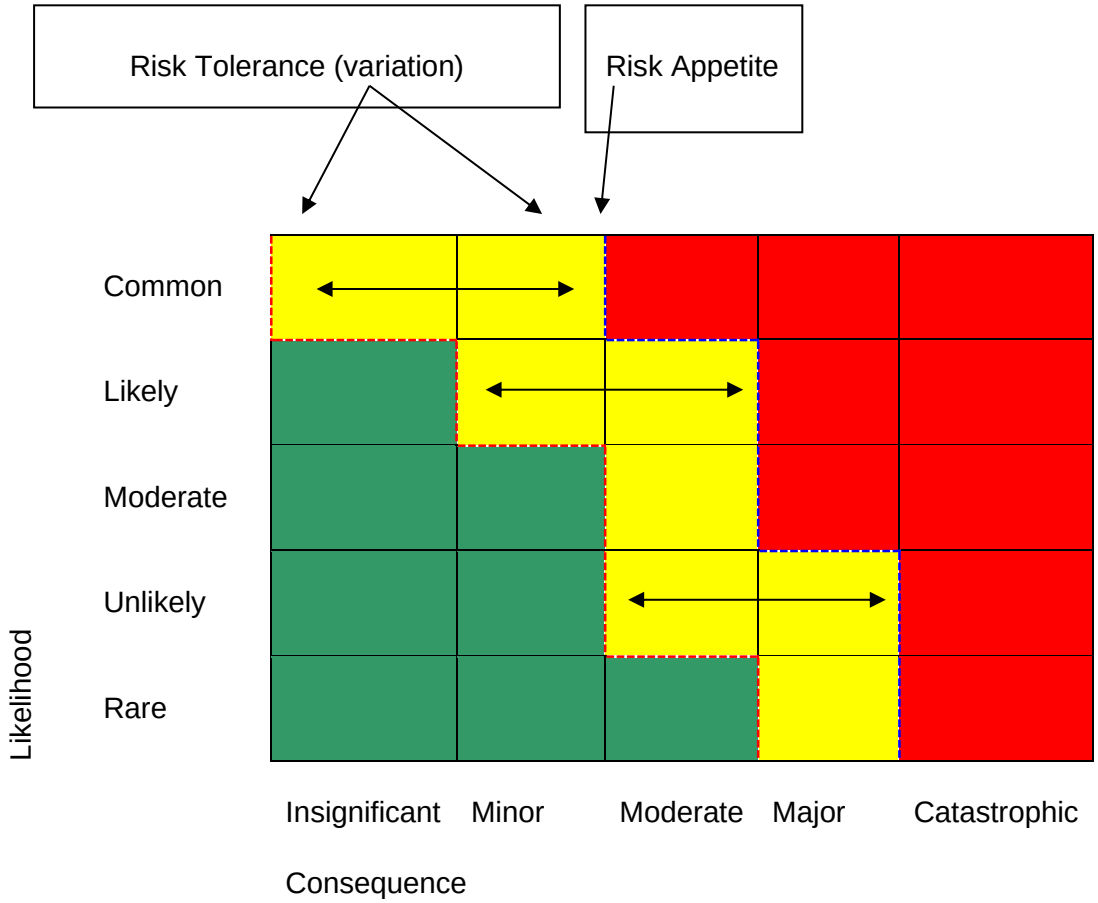
53. Risk tolerance statements

Some tolerances are easy to express in qualitative terms. For example, an organization may have a low risk appetite for non-compliance with laws and regulations and may communicate a similarly low tolerance for violations Or tolerance may be stated in quantitative terms. An organization could state that it relies on the reliability and disaster recovery of their computer systems so that the probability of computer failure is less than 0.01%. Other examples include:

a. An organization targets water leakage maintenance at 98% within 2 hours, with acceptable variation in the range of 97%-100% of the time;
b. It expects staff to respond to all customer complaints within 24 hours but accepts that up to 25% of complaints may receive a response within 24-36 hours.

54. Graphical depiction of risk appetite

Here is an example of a “Risk Heat Map” indicating Risk Appetite and Risk Tolerance levels.



The table below depicts how an organization may define risk appetite for various categories of risk. This is illustrated in the examples of a risk matrix or heat map.

Risk Rating Parameters (Product of Impact and Likelihood)	Risk Acceptance Guide	Risk Treatment Action Required
13 - 25	High	Risk exceeds the risk acceptance level and requires urgent and immediate management attention to bring it within the acceptable level. Controls require substantial redesign, or a greater emphasis on proper implementation
9 -12	Medium	Risk exceeds the tolerance level, but within the acceptable level and requires proactive management to bring it within tolerable level. Controls require some redesign or more emphasis on proper implementation
1 - 8	Low	Risks that are below the tolerance level and do not require active management, but require active monitoring. Controls are adequately designed and may require close monitoring to maintain the risk within a tolerable level

Table 14: Risk rating parameters

General guiding principles for development of risk tolerance:

a. Risk tolerance should be expressed in the same indicators as its related objectives;
b. In setting the risk tolerance management should consider the relative importance of the related objective;
c. Tolerance levels should not be out of line with the materiality framework of the Organization;
d. Without exception, all tolerance levels should be supported by rigorous analysis and expert management judgement;
e. Tolerances may be established for individual material risks, as well as aggregate tolerance for particular categories of risk;
f. Tolerances may also be established per individual business activity;
g. Risk tolerance levels should be revised as more reliable information becomes available;
h. Setting risk tolerance should be a collective senior management responsibility; and
i. Risk appetite is developed at the Organizational level by senior management and proposed to the Organizational Manager for approval. Once approved, it is communicated to all within the Organization, including staff and key stakeholders.

55. Communication of risk appetite

Three approaches for communicating risk appetite include:

a. Expressing overall risk appetite using broad statements;

b. Expressing risk appetite for each major class of organization objectives; and
c. Expressing risk appetite for different categories of risk. Some organizations use broad, generic risk categories, such as economic, environmental, political, staff, or technology, in their risk appetite statements. Others use more tailored risk categories that apply to their field.

56. Risk targets

Risk tolerances may be accompanied by a risk target. A risk target is a desired level of risk that the organization believes is optimal to meet its objectives. This often can be some level within the risk tolerance boundaries, possibly depicted along a risk/reward curve. Implicit in the risk tolerance and risk target concepts are reviews to determine the suitability, adequacy and effectiveness in operating within the boundaries at the desired target levels.

Monitoring changes from the expected outcomes is vital for risk tolerance statements to be meaningful. Unexpected or unacceptable deviations should trigger further analysis and action, including escalation to senior management.

As with appetite, an organization's risk tolerance generally is driven by its objectives and stakeholder expectations, ranging from value protection (generally lower tolerance levels) to value creation (generally higher tolerance levels). Tolerances are also highly dependent on how well capitalized or financed the organization is.

The output is a clearly defined tolerable level of risk established through a rigorous process of analysis and expert management judgement. Depending on the nature of risk, the tolerance may be expressed either in qualitative or quantitative terms.

In some instances, risks as assessed would exceed the tolerance level, but cannot be avoided (e.g. matter of national priority). In this case, these risks will have to be approved by Organizational Manager and regularly monitored.

The advantage of working within clearly defined risk tolerance levels assists with avoiding the danger of over controlling risks.

Chapter 8: The role of internal audit in combined assurance

57. Role of internal audit

Internal Audit or Risk Management are usually best placed to take on the combined assurance champion role. They have an overall understanding of the business, are familiar with the assurance concepts and have a strong vested interest in making sure the approach is effective. Other secondline-of-defence functions can take on the championing role, such as Compliance, the Company Secretary, and Legal. The on-going co-ordination of the combined assurance efforts can be achieved through a Combined Assurance Forum (CAF).

The diligence and effort in establishing an effective combined assurance approach must be matched by on-going efforts to ensure the approach provides the value it is designed to provide. Our practice has found that activating the assurance reporting on the risk management platform provides the lasting solution. Assurance providers plot their assurance activities planned against the risk profile. The risk and process owners can then assess the extent of disruption and overlap together with the Combined Assurance Forum. • The assurance assessment on residual risk status is recorded for the risks with a URL link to the assurance report s etc. • The assurance assessment can be compared to management assessment of residual risk. • Assurance findings are recorded as actions per the risk management system and remediated according to overall priority of all recorded remediation. Action tracking will apply equally to those findings. • Management and the Business then have access to “real time” assurance and do not have to wait for the audit process to be completed. • Assurance reporting is a couple of key strokes away at any time as required.

58. Ways of coordinating combined assurance

There can be different methods and ways of combining assurance, and the Standards does not offer a specific definition. When it comes to the type of coordination, variations depend on the specific requirements and the kind of integration of activities that individual organizations prefer

a. Integrated audits. Coordination takes place through audit activities; specifically, performing audits jointly with supporting functions and/or the external auditor.
b. Process integration. Coordination takes place through the planning and reporting processes. The risk-based audit plan is fully aligned with second-line governance functions. Integrated reporting can be internally or externally oriented. The International Integrated Reporting Board (IIRC) describes an integrated report that is externally oriented as: “An integrated report is a concise communication about how an organization’s strategy, governance, performance, and prospects, in the context of its external environment, lead to the creation of value in the short, medium, and long term.”*
c. Alignment through activities. Coordination takes place through alignment of activities, either on a structured or an ad hoc basis. For example, informing governance functions of the scope and outcome of internal audit activities allows these to be taken into account in their own activities (for example, control weaknesses identified by internal audit can be addressed by internal control).

d. Functional integration. Coordination takes place through hierarchical lines by combining internal audit and functions that support management, such as risk management, internal control, and compliance. Internal audit stays separate from other governance functions in the first three described ways of coordinating assurance—integrated audits, process integration, and alignment of activities. Consequently, these ways are not mutually exclusive but should be seen as complementary. Regarding the fourth way (functional integration), it should be noted that The IIA strongly promotes—from auditors' objectivity and independence point of view—to maintain a separate internal audit function. Therefore, functional integration is not a preferred option by The IIA. If functional integration occurs, it is preferably done on a temporary basis with the end goal of having fully separated functions (see The IIA Position Paper, The Three Lines of Defense in Effective Risk Management and Control). In such cases, safeguards and conditions should be put in place to minimize the negative impact on the auditor's objectivity and independence. Examples include situations where the maturity of the governance functions is not strong enough yet and internal audit plays a role in developing risk and compliance activities. For further discussion, see

59. IIA and 3 lines of defense

The IIA–Netherlands whitepaper about internal audit and the second lines of defense, released in 2014provides more details about different ways of combining assurance, including specific consideration of the role of the internal auditor, particularly with respect to safeguarding auditors' independence. References to the Standards are included. The IIA endorses the Three Lines of Defense Model. Each of the three "lines" plays a distinct role within the organization's governance framework.

Give assurance to management by reviewing the effectiveness of the so-called second line of defense functions. In the CBOK 2015 Global Internal Audit Practitioner Survey, of the respondents who are familiar with the Three Lines of Defense Model, between 45% and 64% indicated that internal audit operated as a fully separate independent function in the third line of defense in their organization (see exhibit 10). However, on average, 19% of the respondents who were familiar with the Three Lines of Defense Model, and whose organizations had adopted the model, indicated that the split between the second and third line was not clear, or internal audit operated as a second line of defense function (instead of being an independent third line assurance provider). There is a lack of familiarity with the model in certain regions, particularly South Asia, North America, and the Middle East & North

60. COSO recommendations

The Committee of Sponsoring Organizations of the Treadway Commission (COSO) recommends the following steps when implementing combined assurance:

a. Make the business case. Spell out the benefits of implementing combined assurance and estimate the project costs for doing so.
b. Inventory who provides assurance. Perform an inventory of all the players who assist management in providing assurance on risks and controls in the organization.

c. Map risks to assurance providers. Map the risks universe and relate this to the assurance providers who are monitoring those risks.
d. Design the combined assurance plan. Identify who will provide assurance across the risk universe, including the role of internal audit, specifying what assurance will be provided.
e. Create an implementation roadmap. Define a roadmap with key milestones. One of these must be to align the definitions and risks ratings used among the assurance providers to lay the foundation for implementing an effective combined assurance model.
f. Plan for continuous improvement. Evaluate the assurance model on a regular basis, identifying areas for improvement and deciding how information and assurance services to management could be further optimized.

By aligning and harmonizing assurance activities and ways of working across different functions, delivering assurance becomes increasingly efficient and effective, avoiding the pitfall of businesses becoming overloaded with information and eventually resulting in “assurance fatigue.” At the same time, care must be taken to ensure that combined assurance is implemented in a form that preserves the distinction between the three lines of defense. Clear benefits of implementing combined assurance among different assurance providers have been identified. However, understanding and implementation of the combined assurance concept is not yet widespread. There are different ways to combine assurance depending on the specific requirements and desired type of integration of activities in individual organizations. As the saying goes, all roads lead to Rome, and in-depth interviews with CAEs globally show that implementing combined assurance should be considered a journey, not something that can be put in place from day one.

Chapter 9: Communication and Reporting

61. Introduction

Risk management reporting is the regular provision of appropriate risk and risk management information to stakeholders and decision-makers within an organization in order to support understanding of risk management issues and to assist all officials in performing their duties within the organization.

Relevant information, properly and timeously communicated to and amongst relevant stakeholders, is essential in order to equip such stakeholders with the means to identify, assess and respond to risks, enabling decision-making at all levels.

Reporting on risk management performance will also provide the necessary confidence that the organization is managing its risks to a satisfactory level.

Stakeholders need to be informed of the level of performance of risk management through reporting on the extent to which:

a. the risk exposure of the organization is improving over time;
b. the organization is meeting its risk management compliance requirements;
c. the right balance of risk taking and risk mitigation is achieved;
d. the organization is operating within its risk bearing capacity; and
e. the risk management of the organization is adding value by impacting positively on service delivery.

62. Implementing an efficient and effective risk management reporting system

It is important that risk reporting demonstrates that the organization is managing its key risks and applying the most appropriate level of risk management maturity relevant to its exposure to threats, as well as its capacity, skills and budget for risk management.

This requires an organization to determine and communicate risk reporting arrangements to all stakeholders. A clearly defined risk reporting structure is essential to facilitate effective communication among stakeholders in the risk management process. Used effectively, risk reporting pinpoints key areas of concern of the organization which would require further attention.

An example would be a report highlighting where controls are:

- *Inadequate*, which in essence indicate a lack of or poorly designed controls;
- *Ineffective*, which indicates that staff and management is not applying the controls that have been designed; and

- *Excessive* and where they may be reduced to enable deviation of resources to areas where controls may be less adequate. Excessive controls are costly and add to the red-tape that prevent effective and efficient service delivery;

Common language, consistent form of reporting and collaboration among stakeholders are critical to ensuring that risk reports are effectively utilised to drive organizational performance. It is also crucial that risk reporting is not only a bottom up approach. While risk reporting is meant to aid managers to make risk-based decisions, it is equally important for such information and decisions to be communicated to operational staff.

Effective information and communication is intended to support enhanced decision making and accountability through:

a. Relevant, timely, accurate and complete information; and
b. Communicating responsibilities and actions.

When deciding on information and communication protocols, the following should be considered:

i. Understanding clearly the needs and requirements of each stakeholder group. This would include agreeing with them the manner, content and form in which the information should be communicated and the frequency of reporting;
ii. To what extent existing reporting channels can be utilised to transmit the required information rather than creating new channels.

Various internal and external data and information sources could be used to source information for reporting. Furthermore, this information could be in quantitative and qualitative form. The challenge for management is to process and refine large volumes of data into relevant and actionable information, and to keep historical records of analysis, trends and decisions. This challenge can be overcome by implementing an information system to source, capture, and process, analyse and report relevant information.

63. Types of risk management reports

In integrated and risk intelligent organizations, risk and risk management performance reporting should include the following broad categories of reporting:

a. **Risk profile reporting** to reflect risk profile improvement, indicating the extent to which the organization is:
    - Achieving the right balance between risk taking and risk mitigation;
    - Reducing its risk exposure, to ensure that the organization is operating within its risk bearing capacity.
b. **Risk management maturity reporting** to reflect risk management process improvement, indicating whether the organization is:
    - Making progress in moving towards a greater level of maturity;

- Achieving cost benefit of its risk management processes by embedding risk management as much as possible into all operational and decision-making processes
- Adding value through the achievement of its service delivery objectives.

c. **Risk management compliance reporting**, indicating:

- The extent to which the organization complies with the prescribed risk management processes as per the risk management policy;
- The extent to which the organization remains within its risk tolerance levels;
- Improvement of the organization's compliance to predetermined levels of performance.

The following summary illustrates the typical reports that might be used and the content, frequency, source information and impact of the reports:

Report name	Content	Frequency	Source	Desired impact
Annual Board Report	Assurance that the organization has risk management processes in place. Progress and status of Risk Management Maturity Business continuity and disaster recovery reports	Annually	Combined assurance report Risk Management Maturity Assessment Business continuity assessment Disaster recovery assessment	Assure that processes are effective in controlling risks to satisfactory level. Include information for external stakeholders about key risks within the organization and approaches to addressing these risks. Assurance on progress on risk management maturity.
Board Report	Disclosure of strategic and operational risks and the management thereof. Overview of risk management implementation progress	Quarterly	 Strategic risk register.xlsx  Operational risk register.xlsx	Stakeholder information and building of confidence in the management of risk.

Audit Committee Report	Risk Management Implementation New and emerging risks Assurance on management of existing risks Risk Management compliance report	Quarterly	 Strategic risk register.xlsx  Operational risk register.xlsx	Verifying progress of risk management. Provision of assurance that risks have been identified, are being managed, controls are in place to manage the risks and the effectiveness of the controls is understood. Provision of assurance on improvement of the organization's compliance to predetermined levels of performance. Provision of assurance on coordinated responsibility for assurance on risks and controls.
Exco Report	Significant changes in the risk profile (including "emerging" risks) since the last report and the reasons for the changes Consolidated risk profile showing the key risks and risk control effectiveness Results from monitoring activities	Quarterly	Strategic risk register Operational risk register	Ultimate Audit Committee and Board Assurance of risk management. Awareness, engagement and buy in of risk management.

	Performance against Risk KPIs			
Business process Report	New and emerging risks. Update on the management of existing risks Progress with treatment plans Results from monitoring activities Risk management implementation and performance in Business Unit	Monthly	Risk management implementation plan for business unit(s)	Awareness of new risks and update on existing risks. Demonstration of progress with actions and improvement in management of risks. Demonstration of improvements in control effectiveness. Understanding and awareness of risk management implementation and performance.
Risk Register Reports	New risks identified and existing risks remaining Changes to ratings and other information Results from monitoring activities	Monthly / Quarterly	Strategic risk register Operational risk registers Consolidated risk reports	Awareness of new risks and update on existing risks. Demonstration of progress with actions and improvement in management of risks. Demonstration of improvements in control effectiveness.

Risk and Control Owner Reports	Update on the management of existing risks Effectiveness of Controls	Monthly	Operational risk register	Demonstration of progress with actions and improvement in management of risks. Demonstration of improvements in control effectiveness.

Table 15: Types of reports to be generate