

Effective risk management is fundamental to the success of modernization in national statistical organisations (NSOs), in that it concerns both organisation and production processes. Actually, Risk management, on the one hand, points at strengthening organization governance on the whole by supporting the decision-making process when selecting priorities; on the other hand, it points at identifying, analysing and removing the uncertainties that can put obstacles in the way of change and development.

The UN Guidelines on Risk Management in Statistical Organizations give NSOs, interested in internally implementing a risk management system, a reference based on the practices developed within the UNECE organizations and containing some key features: effective development, sustainability (in terms of resources and complexity), alignment with change management processes.

This training module supports the implementation of the Guidelines and is structured consistently with the ISO 31000:2018 standard architecture; this standard is widely accepted internationally as well as used by most public organisations when implementing Risk management systems.

Module 1: The Concept of Risk Management

- 1) *an unwanted event which may or may not occur.*
- 2) *the cause of an unwanted event which may or may not occur.*
- 3) *the probability of an unwanted event which may or may not occur'*

The Definition of Risk

According to the ISO risk definition, **risk** is "effect of uncertainty on objectives".
 "An effect is a deviation from the expected. It can be positive, negative or both, and can address, create or result in opportunities and threats".
 Uncertainty is "the lack of information about the understanding or knowledge of an event, its consequences and likelihood".
 "Objectives can have different aspects and categories, and can be applied at different levels".
 Risk is often expressed in terms of a combination of the consequences of an event (including changes in circumstances) and the associated likelihood of occurrence"




Risk: Combination of the likelihood of an event and its effects

Inherent Risk: Risk without any intervention

Residual risk: Risk remaining after the treatment, possibly containing risks not identified

Risk treatment: Selection and implementation of interventions on risk

Before any risk treatment is put in place, the event involves an **"inherent risk"**, ontologically related to the activity that could determine the event itself

Once the mitigating action has been put in action, all that's left is the **"residual risk"**, whose value can be equal to, greater or less than the "inherent risk".

Risk management is an organizational model aimed at developing the quality of management processes; it stands out by analysing the events that have not materialized within the organization. Unlike most managerial systems, risk management doesn't overlap with other internal controls because it represents a different perspective that cuts across planning and control, performance evaluation system, audit, quality and so on.

Therefore, risk management helps the organizations bring about a higher level of quality of services and products because it supports the decision-making processes, preparing for the difficulties that could hinder the achievement of the strategic goals. In a few words, the main objective of risk management concerns protecting and strengthening:

- Values, ethics and sense of belonging
- The entity's tangible and intangible assets
- Growth of organizational culture
- Leadership and relationship
- Effectiveness and efficiency of processes
- Resources for strategic priorities
- Stakeholder's satisfaction

That means that risk management is a tool to effectively manage an organization; in fact, it deals with risks and opportunities affecting the creation or the preservation of an entity's value. risk management is defined as: *"a process, effected by an entity's board of directors, management and other personnel, applied in a strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives"*.

Continued on Next Page >>>>>>>


The Definition of Risk

When defining a risk, some issues should be taken into consideration:

- A risk statement should be a **clear, meaningful and concise statement** that describes the risk.

Example: "Increased difficulties in reaching household survey respondents could adversely impact the quality of our data".

- The statement should **describe the event**, and the **potential impact** of that event on the achievement of the organization's objectives.
Example: There is a risk that (event)...and the consequences are (impact)...
- A good risk statement should also include the **possible causes** (drivers).
Examples: There is a risk that (event)...because of (cause)...and the consequences would be (impact)... Given that...there is a risk that...with the potential impact of...



The definition reflects certain fundamental concepts; in particular, risk management is:

- A process, ongoing and flowing through an entity
- Effected by people at every level of an organization
- Applied in strategy setting
- Applied across the enterprise, at every level and unit, and includes taking an entity level portfolio view of risk
- Designed to identify potential events that, if they occur, will affect the entity and to manage risk within its risk appetite
- Able to provide reasonable assurance to an entity's management and board of directors
- Geared to achievement of objectives in one or more separate but overlapping categories

This definition is purposefully broad. It captures key concepts fundamental to how companies and other organizations manage risk, providing a basis for application across organizations, industries, and sectors. It focuses directly on achievement of objectives established by a particular entity and provides a basis for defining enterprise risk management effectiveness.

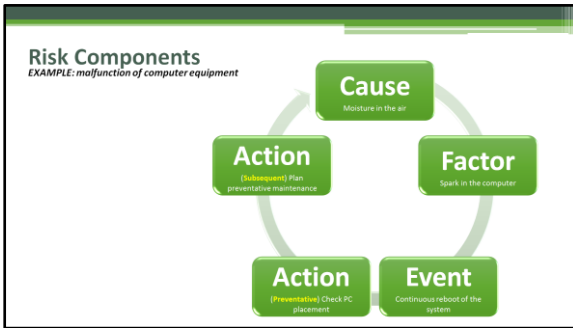
Risk management examines the events that have negative impact; they represent the risks which can prevent value creation or erode existing value. There are many risk definitions in the literature and in the standards most recognized at the international level; the standard ISO 31000:2018 defines risk as: "the effect of uncertainty on objectives", where "an effect is a deviation from what is expected (positive and/or negative), often expressed in terms of a combination of the consequences of an event (including changes in circumstances) and the associated likelihood of occurrence" and the uncertainty is "the lack of information about the understanding or knowledge of an event, its consequences and likelihood".



The concept of risk is more complex than the combination of likelihood and effect; it comprises some issues considered by the cognitive analysis relating to the organization, including:

- **Risk Profile:** set of risks that may affect all or part of an organization;
- **Risk Appetite:** total amount and type of risks that an organization decides to pursue, maintain or adopt
- **Risk Perception**, which describes how people perceive risks according to their values and interests
- **Risk Attitude.** (Existing Risk Profile). If an organization is particularly effective in managing certain types of risks, it may be willing to take on more risk in that category, conversely, it may not have any appetite in that area.
- **Risk Acceptance**, which refers to the maximum potential impact of a risk event that an organization could withstand. Often, appetite will be well below acceptance.
- **Risk Capacity**, which is the maximum level of risk that an organization can assume without violating the regulatory burden;
- **Risk Retention**, which considers stakeholders' conservative return expectations and a very low appetite for risk-taking.
- **Risk Tolerance**, which is the level of variation that the entity is willing to accept around specific objectives.

All of these issues should be considered to assess the overall risk level of the organization



The identification of the "enabling factors" and the "causes" related to a risk, could contribute significantly to specifying the context in which the risk can occur, allowing risk owners, to adopt the necessary preventive measures.

While the enabling factor represents an organizational/social/environmental circumstance which facilitates a behaviour that could result in a risk, the cause is the reason why the action has been undertaken. Therefore, the root-cause analysis can help organizations distinguish risks that could be effectively tackled from those which can only be partially dealt with.

What is or isn't a Risk?

- The risks must be linked to the objectives
- You must pay attention to the risks with generic impact on the objectives, but not relevant for the results
- In identifying the risks, you should not confuse them with the impacts
- You must avoid defining risks with assertions that are only the opposite of the objectives
- The definition of a risk should understand the cause and consequence

Objective: Travelling by train from A to B to arrive on time for a meeting

| | | |
|---|---|--|
| Not being able to get from A to B in time for the meeting | ✗ | This is only the opposite of the objective |
| Be late & miss the meeting | ✗ | This is the impact of the risk not the risk itself |
| There isn't a dining car so I'm hungry | ✗ | This does not impact on the objective |
| I miss the train (so I'm late & I cannot attend the meeting) | ✓ | This is a risk that I can control making sure that I will arrive early |
| The bad weather conditions prevent the train from leaving the station | ✓ | This is a risk that I cannot control but I can manage with an emergency plan |




Are you a Risk Seeker or Risk Averse?
 Read the excerpts that follow and decide which option you would choose.

A manager is sourcing equipment for a new IT project. The project has to choose between two vendors, **Best Retailer IT** and **New Retailer IT**. To simplify the problem, the project manager decides to estimate the potential profit of these vendors on the basis of product reliability.

- Through research, the manager finds that **Best Retailer IT** has a **60%** chance of providing reliable equipment, and its parts cost **£300,000** (this includes costs of installations and maintenance).
- There is, a **40%** chance that the equipment will fail – in which case, costs can increase to **£850,000**.
- If **New Retailer IT** is chosen, there is an **80%** chance of high reliability at a cost of **£750,000** and a **20%** chance of failure.
- **New Retailer IT** provides lifelong guarantees and maintenance services.

Would you choose
Best Retailer IT or **New Retailer IT**?



Participant Feedback

If you choose Best Retailer IT, you can consider yourself to be a **risk seeker**, and if you chose New Retailer IT, you could be considered **averse to risk**.

Risk seekers will choose the option with the most at stake (40% chance that costs can increase to £850,000) but the most favorable outcome (£300,000 cost).

Risk averse individuals will choose the safest option (80% chance of high reliability at a cost of £750,000) with a life-long guarantee. However, this is the costly option.

As a risk seeker would the following scenario change your mind?

Given the competition from New Retailer IT, Best Retailer IT has proposed the following incentive: a 70% guarantee of providing reliable equipment and parts at a cost of £300,000. There is still however a 30% chance that the equipment will fail – in which case, the costs can increase to \$850,000.

Would this change your choice of retailer?

As Best Retailer IT's guarantees increase, its offer becomes attractive to even the most risk-averse individuals because of the massive savings it offers compared with New Retailer IT.

The Risk Management System

According to the ISO 31000:2018, Risk Management refers to the architecture used to manage risks. This architecture includes Principles, Framework, and Process.

A risk management framework (system) provides the infrastructure for delivering, maintaining and governing risk management throughout the organization. As a part of this framework, an organization should set up:

A risk management mandate, that is the board's statement for setting the direction and priorities for risk management, and through which "who does what" is established, and the proper authorization and necessary resources are given. This is the main expression of the governance of risk, through which the organization's board engages stakeholders in locating the different responsibilities for managing risks.

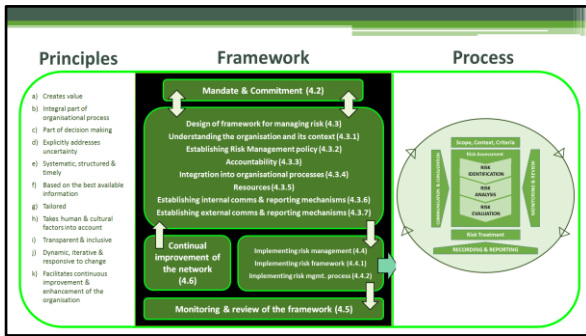
A risk strategy, that points out how risk management supports the organization's overall strategy and related objectives. It takes into consideration the external and internal context, focusing in particular on key stakeholders' demands.

A risk policy that provides a clear and concise outline of the organization's requirements for risk management within the organization's overall approach to governance. It includes the risk appetite statement, the human resources training program for supporting the risk management process, as well as a definition of risk assessment criteria.

An integrated risk approach supports quality management in improving statistical data integrity and quality, through identification, analysis and treatment of risks inherent to statistical and over-arching processes.

The framework assists in managing risks effectively through the application of the risk management process at varying levels and within specific contexts of the organization.

- ❑ The framework ensures that information about risk derived from the risk management process is adequately reported and used as a basis for decision making and accountability at all relevant organizational levels.
- ❑ The framework is not intended to prescribe a management system, but rather to assist the organization to integrate risk management into its overall management system.
- ❑ If an organization's existing management practices and processes include components of risk management or if the organization has already adopted a formal risk management process for particular types of risk or situations, then these should be critically reviewed and assessed



A risk management framework is a set of components that support and sustain risk management throughout an organization.

There are two types of components: foundations and organizational arrangements.

Foundations include your risk management policy, objectives, mandate, and commitment.

And **organizational** arrangements include the plans, relationships, accountabilities, resources, processes, and activities you use to manage your organization’s risk.

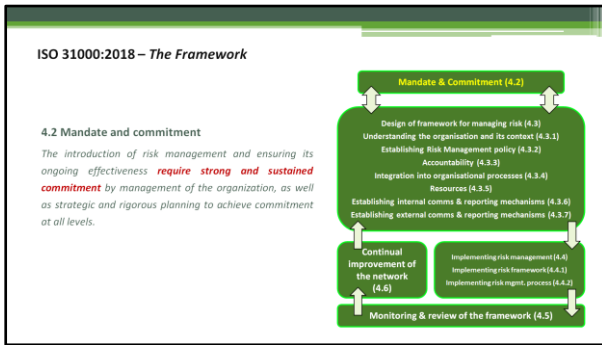
It is **not intended to prescribe** a management system, but rather to assist the organization **to integrate RM** into its overall management system.

The Principles

1. Consider culture, values & human behaviors
2. Use common language and update information
3. Build Tailor-made tools
4. Address to real risks
5. Be Systematic and structured
6. Promote transparency and staff involvement
7. Be embedded in decision-making processes
8. Protect and preserve every asset
9. Become dynamic and responsive

The Framework

1. Consists of: 1. Mandate & Commitment; 2. Design of framework for managing risk; 3. Implementing Risk Management; 4. Monitoring and review of the framework; 5. Continual Improvement of the framework
2. Is a set of 2 types of components supporting and sustaining risk management throughout an organization: a) foundations (policy, objectives, mandate, and commitment); b) organizational arrangements (plans, relationships, accountabilities, resources, processes) Build Tailor-made tools
3. assists in managing risks effectively through the application of the RM process at varying levels and within specific contexts of the organization Be Systematic and structured
6. ensures that information about risk coming from the risk management process is adequately reported and used as a basis for decision making and accountability at all relevant levels



Risk management mandate and strategy

A risk management strategy includes definition of the risk management scope and plan, as well as the discussion of risk management philosophy.

Risk philosophy

A risk management philosophy is the set of shared beliefs and attitudes that characterise how risk is considered in any organisation. It affects how risk management components are applied, including how risks are identified, accepted, and how they are managed.

When the risk management philosophy is not developed, understood, or fully embraced by the staff, an uneven application of risk management across business units, or departments is likely. Even when the philosophy is well developed, cultural differences among units resulting in variation in enterprise risk management application may still be found. Therefore, risk philosophy, risk appetite & risk strategy should always be kept aligned, as one reflects the other. To this purpose it's necessary to “measure” risk perception by the management staff – as some may be prepared to take more risk, than others – as well as the risk maturity of organizational context, since this latter could be more or less resilient in facing risk.

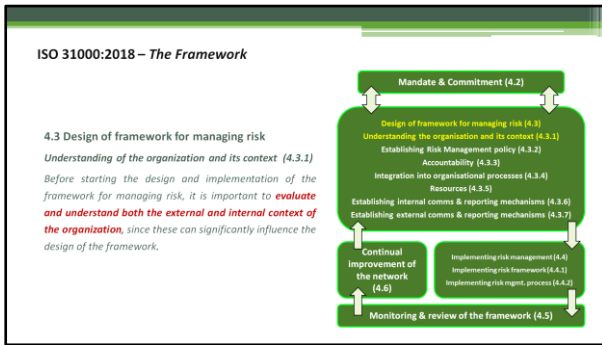
Mandate

A mandate in risk management expresses itself through an official document that clearly indicates the risk strategy & objectives, the people accountable for them, and authorizes such people to use proper resources for achieving their objectives. Defining and communicating this statement testifies a commitment to implement a risk management system.

Risk management commitment

Risk management design should be mostly contributed to by top management with the assistance of middle/low management and technical staff particularly during the start-up phase, every organizational level should be involved in order to collect inputs and needs (for example, through *ad hoc* interviews). Employees know best the most typical risks in their area, and should be both encouraged and engaged to regularly give information about them.

Risk management goals should not only be clearly defined and communicated by top management, but also discussed within each of NSO's units. Each unit should have a contact person who is entitled to coordinate all the risk management activities, in cooperation with his/her colleagues, including the head of unit.



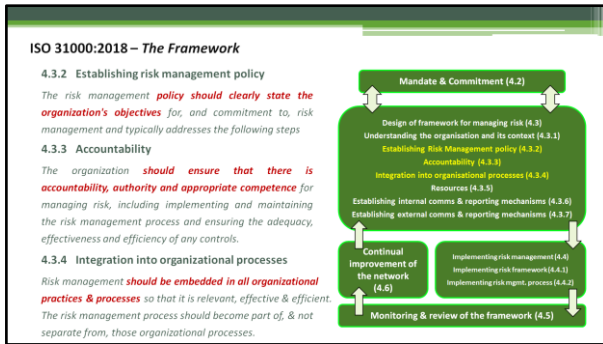
When designing the framework for managing risk, the organization should examine and understand its external and internal context.

Examining the organization's external context may include, but is not limited to:

- the social, cultural, political, legal, regulatory, financial, technological, economic and environmental factors, whether international, national, regional or local;
- key drivers and trends affecting the objectives of the organization;
- external stakeholders' relationships, perceptions, values, needs and expectations;
- contractual relationships and commitments;
- the complexity of networks and dependencies.

Examining the organization's internal context may include, but is not limited to:

- vision, mission and values;
- governance, organizational structure, roles and accountabilities;
- strategy, objectives and policies;
- the organization's culture;
- standards, guidelines and models adopted by the organization;
- capabilities, understood in terms of resources and knowledge (e.g. capital, time, people, intellectual property, processes, systems and technologies);
- data, information systems and information flows;
- relationships with internal stakeholders, taking into account their perceptions and values;
- contractual relationships and commitments;
- interdependencies and interconnections.



Establishing risk management policy

To achieve consistency in risk management activities across the organization, the policy should contain a high level overview and description of the risk management process.

The main features of the policy are:

- *Definition of corporate risk appetite: the board and senior managers set the risk tolerance level by identifying general boundaries against unacceptable exposure to risk. The corporate risk appetite is then used to shape tolerance levels down the organization*
- *Implementation of a risk management standardized process at all levels, to ensure that risk management is an inherent part of how core-business is run*
- *Top management involvement in risk management framework design*
- *Stakeholders' empowerment*
- *Definition of risk criteria*
- *Definition of a hierarchy of risks*
- *Implementation of a risk management unit/office*
- *Definition of human resource training policy to support risk management process*
- *Establishing a communication system*
- *Establishing a reporting system*

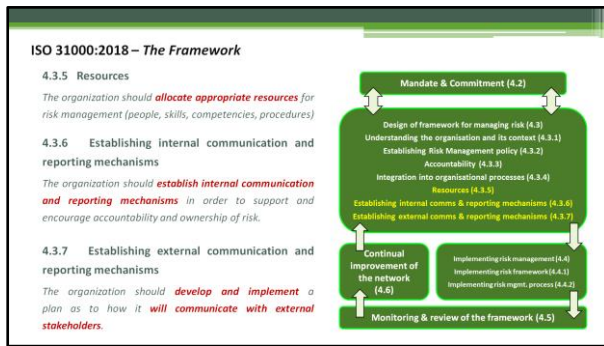
Risk Accountability

Need some narrative here

Integration into organizational processes

Risk management is essential to achieve the organization's strategic outcome, and such fulfilment can only be reached by ensuring that risk is included as a routine in all significant decision-making. This means that risk management should be part of the culture, embedded in every organizational process, including production and supporting processes.

This requires an agreed approach, integrated with corporate strategy, that outlines exposures, issues and problem areas: integrated risk management should result in a system that is a part of the regular organizational performance review, where the organization not only looks at performance and events, but systematically identifies important gaps, variations and exposures, in order to get ahead of (mitigate) their possible impact.



Risk management resources

Risk management initiatives can promote employees' sense of belonging, as well as their own significance within the organization. It provides a systematic mechanism of internal control, that obliges all staff to come together to discuss, and identify issues and solve problems.

Risk management training

To effectively implement a risk management system, an organization should allocate **appropriate resources, suitable human capital** as well as ensure that those who are accountable can fulfil their role by providing them with the **training and skills** needed. All staff should be aware of the relevance of risk to achieve the objectives assigned and training to support staff in risk management should be available.

Roles & responsibilities

Risk management should work at any organizational level, as well as through participation by the entire staff, according to respective roles and functions.

The governing board is responsible for ensuring the setup of an effective risk management system throughout the organization

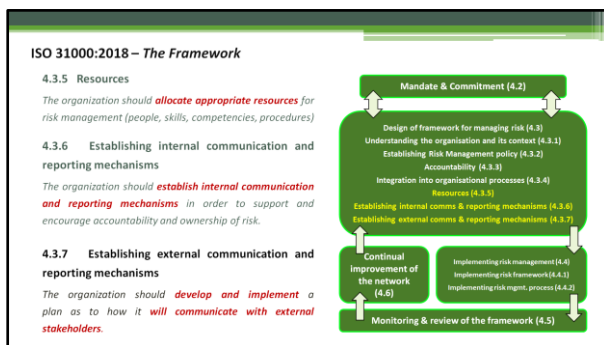
The risk committee/board entity is an oversight entity ruling the risk management system together with other strategic matters

The risk manager works under the guidance of the committee/board, and is skilled in risk management, and supported by sufficient staff for the size of the organization

Top management is responsible for: ensuring that there is a fit-for-purpose risk management framework, that processes are in place which are adequately resourced and financed

The Head of department/divisions/units must actively manage risks that are part of daily work through complying with the enterprise risk management framework

All staff must take risks into account when making decisions and are responsible for an effective management of risks, including identification of them. All staff are responsible for understanding and implementing risk management policies and processes.



Establishing reporting mechanisms

An organization should ensure that information about risks derived from the risk management process is adequately reported, and used as a basis for decision making at all relevant levels. For this, clear reporting line mechanisms and strong inter-department knowledge sharing should be established in order to encourage accountability of risk, and to ensure reports are delivered in an accurate, consistent and timely manner.

Internal Reporting

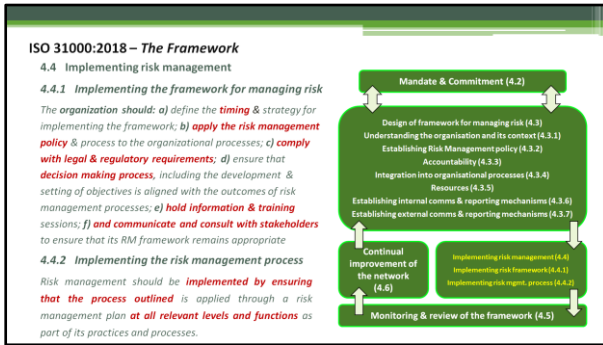
The organization should establish internal reporting mechanisms in order to support and encourage accountability and ownership of risk. These mechanisms should ensure that: key components of the risk management framework, its effectiveness and the outcomes and any subsequent modifications, are properly disseminated; relevant information derived from the application of risk management is available at appropriate levels and times; there are processes for consultation with internal stakeholders.

These mechanisms should, where appropriate, include processes to consolidate risk information from a variety of sources, and may need to consider the sensitivity of the information. Internal risk reports can either be real-time or periodic.

External reporting

Organizations are under increasing pressure for greater transparency, mandated or voluntary, and a **better alignment of externally reported information with that which is reported internally**. Stakeholders expect intensified corporate dissemination regarding risk, and awareness of the critical role of proper risk management.

In view of this, an organization should provide accurate, timely and high quality reports to meet the external stakeholders' needs. Specifically, it should periodically conduct a review of the effectiveness of the risk management system and report to stakeholders on that, and a robust assessment of the principal risks, describing them and explaining how they are being managed or mitigated.



Implementing risk management

The coordination of the risk management process should be centralized: the risk office analyses and draws up information related to each process phase, and proceeds with strategic planning, in coordination with the organization’s board.

The risk committee sets up the criteria to select the most relevant information coming from the risk management information system. Significant risks in terms of impact or strategic level are reported by the office. The risk manager gives directions on translating strategies into risk management objectives, and monitors their achievement. The risk manager therefore finalizes the information received, by adapting it to the organizational context (down to the any single office level), in order to correct possible deviations from strategic priorities.

Implementing risk framework

The organization should implement the risk management framework by:

- developing an appropriate plan including time and resources;
- identifying where, when and how decisions are made across the organization,
- modifying the applicable decision-making processes where necessary;
- ensuring arrangements for managing risk are clearly understood and practised.

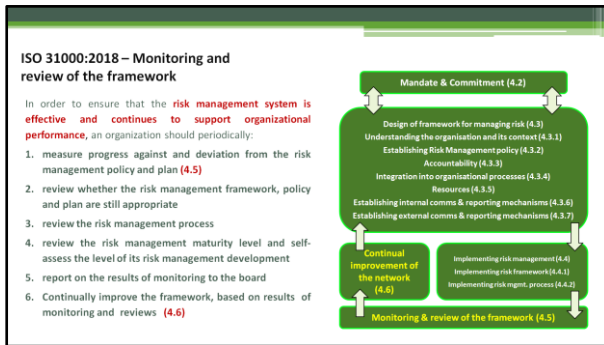
Successful implementation of the framework requires the engagement and awareness of stakeholders. This enables organizations to explicitly address uncertainty in decision-making.

Implementing risk management process

The risk management process is an element of the framework, and is derived from the risk management policy, which it operationalises. The risk management process is a systematic application of management policies, procedures and practices to the tasks of communicating, establishing the context of, assessing, monitoring and reviewing risks. It comprises the following activities:

- 1) Communication and consultation;
- 2) Context, Scope & Criteria;
- 3) Risk Assessment:
 - a. Identification;
 - b. Analysis;
 - c. Evaluation;
- 4) Risk treatment;
- 5) Monitoring and review.

The process should also concern the risk based audit & information system support in all phases.



Monitoring and review of the framework

In order to ensure that the risk management system is effective and continues to support organizational performance, an organization should:

- 1. Periodically measure progress against and deviation from the risk management policy and plan:** the framework and processes should be fit-for purpose, and aligned to the objectives/priorities of the organization, and relevant stakeholders should receive adequate reporting to fulfil their roles and responsibilities within the governance structure;
- 2. Periodically review whether the risk management framework, policy and plan are still appropriate, given the organization's external and internal context:** the organization should ensure that changes to the context, or changes to other factors affecting the suitability or cost of risk management, are identified and addressed;
- 3. Periodically review the risk management process:** the risk management resources should be sufficient, and people across the organization should have adequate skills, knowledge and competence, in line with the risk role they are required to perform on a daily basis;
- 4. Periodically review the risk management maturity level :** With a view to achieving continuous improvement, an organization should self-assess the level of its risk management development, to point out strengths and weaknesses and design and/or review a lasting path of growth for the risk management system itself;
- 5. Periodically report on the results of monitoring to the board:** based on the results from Guidelines on risk management practices in statistical organizations monitoring and review, decisions should be made to improve the organization's management of risk and its culture, ensuring that the organization is able to learn from risk events
- 6. Continually improve the framework, based on results of monitoring & reviews (4.6)**
The frequent monitoring and review of risk arrangements may identify areas which can be developed and improved. Any such improvement areas will be submitted to the risk committee where they will be discussed prior to being actioned and implemented, if it is believed that they will improve the organisation management of risk and risk management culture.

