

Definition

Enterprise Risk Management enhances an organization's ability to effectively manage uncertainty. It is a comprehensive, systematic approach for helping all organizations, regardless of size or mission, to identify events, and measure, prioritize and respond to the risks challenging its most critical objectives and related projects, initiatives and day-to-day operating practices.

ENTERPRISE RISK MANAGEMENT POLICY

Corporate-wide Vision

XYZ is committed to its vision, which is to be the most preferred and successful telecommunications group. In achieving this vision, XYZ will face risks to its business strategy, operational risks and risks associated with the protection of its people, property and reputation. This document describes the policies by which the entire spectrum of these risk are to be effectively managed.

Enterprise Risk Management Policy

XYZ defines risk as any potential event which could prevent the achievement of an objective. It is measured in terms of impact and likelihood. Risks arise as much from the likelihood that an opportunity will not happen, as it does from the threat or uncertainty that something bad will happen.

XYZ's policy is to identify, analyse and respond appropriately to all risks. The risk responses selected are determined by the appetites and tolerances for risks. These will vary over time according to the specific business objectives, for example strategic, operational or asset protection.

The effectiveness of risk management and control measures will be regularly reported to and acted upon by the Board. In addition, periodic independent review on the effectiveness will be conducted.

Responsibilities

The Board is responsible for the Enterprise Risk Management Framework . The Senior Leadership Team under the leadership of the Chief Executive Officer is responsible for implementing the strategy, culture, people, processes, technology and structures which constitute the Enterprise Risk Management Framework.

Review of policy

This policy and underlying principles will be reviewed annually by the Board, to ensure its continued application and relevance.

Key Principles on Managing Risk

- In order to achieve XYZ's business objectives, risks must be considered and managed enterprise-wide;
- Risk management is integral to the strategic planning process, business decision making and day-to-day operations;
- Risks are identified, analysed, responded to, monitored and reported on, in accordance with XYZ's policies and procedures;
- Risk responses must be tailored to each particular business circumstance;
- Management must regularly assess the status of risks and risk responses; and
- Compliance with the Enterprise Risk Management Framework must be monitored and reported.

XYZ's ENTERPRISE RISK MANAGEMENT APPROACH

XYZ has adopted the **ORCA Approach** to ensure consistent application of risk management by all staff, in the:

- execution of strategy,
- achievement of business objectives, and
- day-to-day operations.

ORCA represents:

O OBJECTIVES

Goals and results that XYZ aims to achieve

R RISKS

Any potential event which could prevent the achievement of an objective

C CONTROL

Management's response to risks

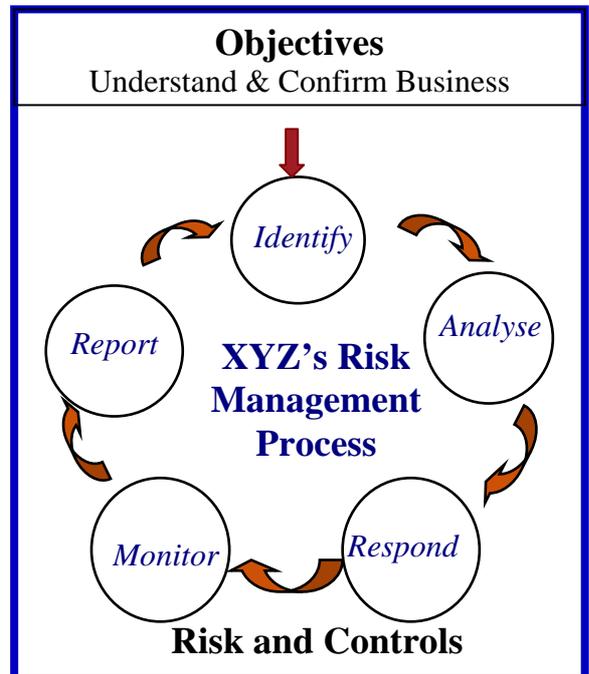
A ALIGNMENT

Alignment of XYZ's objectives, risks and controls across the enterprise determined by its appetites and tolerances for risks

XYZ's ENTERPRISE RISK MANAGEMENT PROCESS

The XYZ Enterprise Risk Management process comprises the following steps:

- 1 **IDENTIFY** key risks
- 2 **ANALYSE** the potential impact and likelihood of risks
- 3 **RESPOND** to risks by considering existing controls as well as selecting, prioritising and implementing appropriate actions
- 4 **MONITOR** the internal and external environment for potential changes to risks and ensure that risk responses continue to operate effectively
- 5 **REPORT** on risks and the status of risk responses adopted



OBJECTIVES

What we are trying to achieve in our business?

XYZ's MISSION

To be the most preferred and successful communications group in Europe.

XYZ's VISION

To exceed customer, shareholder and employee expectations by providing superior customer and shareholder value and being the employer of choice

XYZ's BUSINESS OBJECTIVES

XYZ's business objectives drive its activities, and hence the business objectives should be clearly defined and communicated. The enterprise risk management framework starts with the understanding of the business objectives in ensuring that key risks are identified.

- Enhance Premium Brand;
- Sustain Operational Excellence;
- Continue Quality Customer Service;
- Develop Strategic Partnership;
- Improve human capital;
- Improve Product leadership and innovation;
- Develop Quality network;
- Improve Targeted and Profitable growth.



RISKS

What could affect your ability to meet objectives?

Risks are uncertain future events which could influence the achievement of XYZ business objectives and can be viewed from three perspectives:

Opportunity

Risk of lost opportunity or something good not happening

By viewing risks from the perspective of opportunity, XYZ recognises the inherent relationship between risk and return, i.e. the greater the risk, the greater the potential return or loss. In this context, XYZ must adopt suitable responses to maximise the upside opportunity within the constraints of its operating environment. Typically, strategic questions will involve consideration of this type of risks.

Uncertainty

Risk of not meeting expectations

When considering risks from the perspective of uncertainty, XYZ must determine how it can proactively prevent an uncertainty from having a negative impact. This will mainly be achieved through management of risks relating to operational performance.

Hazard

Risk of loss or something bad happening

While managing risk from the perspective of hazard, XYZ must mitigate the degree of damage to critical business assets (people, property, earning capacity and reputation) that would be caused if the hazard occurs.

Risk Appetite and Risk Tolerance

XYZ business objectives are integral to its appetites for, and tolerances of, risk. The risk appetites and tolerances dictate the nature and level of risks that are acceptable to XYZ.

Risk appetite is defined as *'the risks that XYZ is in business to take, based on its corporate goals and its strategic imperatives.'*

Risk tolerance represents *'the threshold of risk that XYZ considers acceptable, based on its capabilities to manage the identified risks'.*

Risk appetites and tolerances will vary according to the balance of opportunity, uncertainty or hazard which differing risks represent.

CONTROL

Which risk responses promote the achievement of objectives?

Control encompasses all of XYZ's possible responses to risk, whether viewed as opportunities, uncertainties or hazards. These controls are the responsibilities of all XYZ staff and are designed to provide reasonable assurance regarding the achievement of XYZ business objectives.

In determining risk responses, XYZ must first assess whether to accept, exploit, mitigate, transfer or avoid the risks. In the case of exploit, mitigate or avoid, controls will need to be put in place.

There are three main categories of controls:

Preventive Controls	Responses to stop undesirable transactions, events, errors or incidents occurring
Detective Controls	Responses to promptly reveal undesirable transactions, events, errors or incidents so that appropriate action can be taken
Corrective Controls	Responses to reduce the consequences or damage arising from crystallisation of a significant incident

In determining the types of controls to be implemented, the following factors are considered:

- XYZ's business objectives
- XYZ's capability and skills
- Appetite and tolerance for the type of risk
- Time horizon i.e. matching the duration of the exposure and the length of time required in implementing solutions to manage the risks
- Financing i.e. cost effectiveness
- Alignment with other initiatives within the organisation and overall business direction

In ensuring the effectiveness of controls, the following factors are essential:

- Control framework is the responsibility of the Board of Directors
- Integrity, ethical values and competencies of XYZ staff
- Management's philosophy and operating style
- Delegation of authority and responsibility
- Continuous staff development
- Incorporate in existing infrastructure, business processes and reporting as far as possible

ALIGNMENT

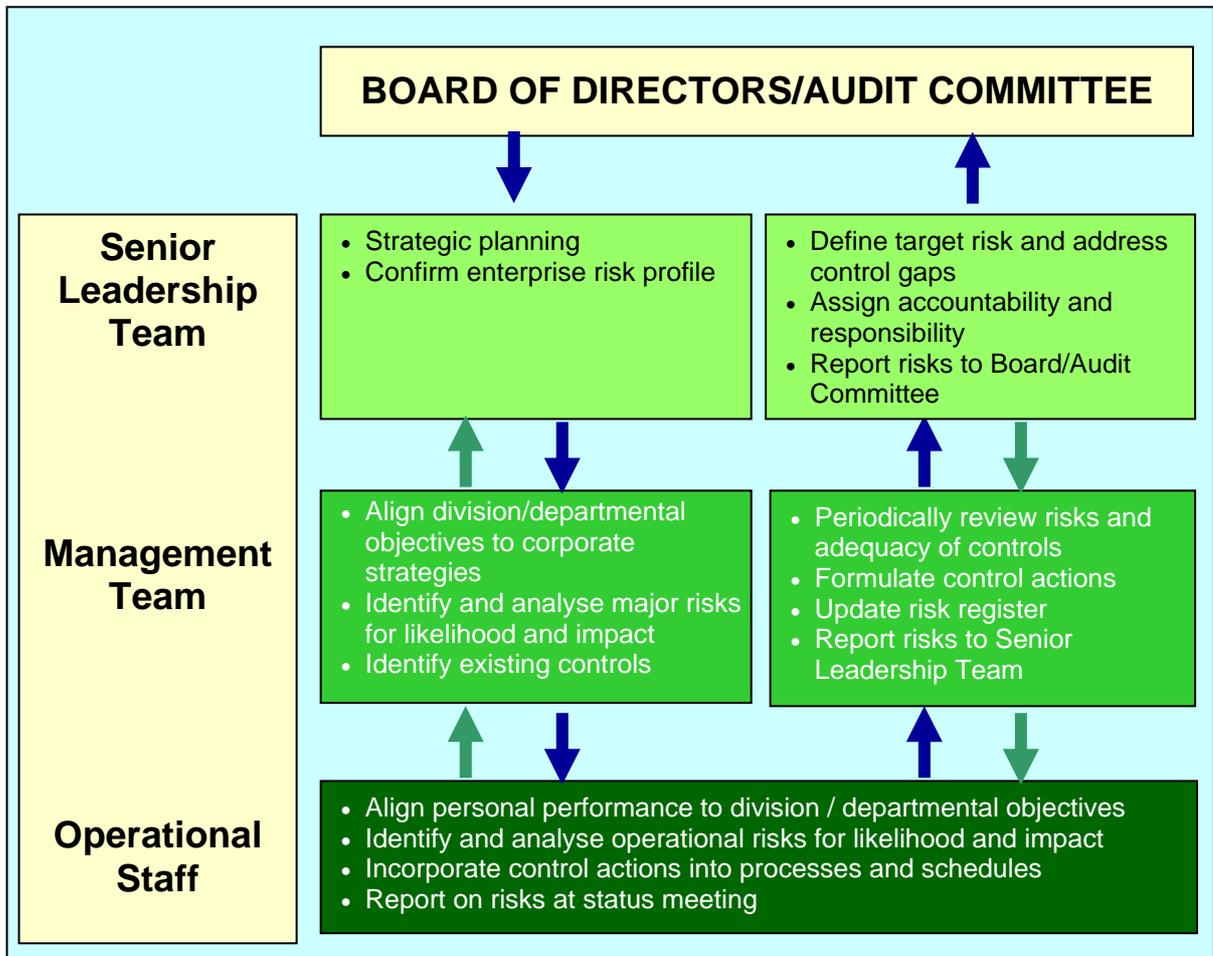
ALIGNMENT
Are objectives, risks and controls aligned enterprise-wide?

Alignment exists between the objectives, risks and controls at all levels within XYZ:

- Between strategies, operational objectives and individual job accountabilities
- Between the risks being taken and the XYZ's appetite and tolerance for risk
- Between the control and the desired level of investment in implementing such control

Given the fast and continuous change in today's business environment, XYZ's competitive advantage is dependent on the rapid deployment of new strategies, whilst remaining focused on existing strategies.

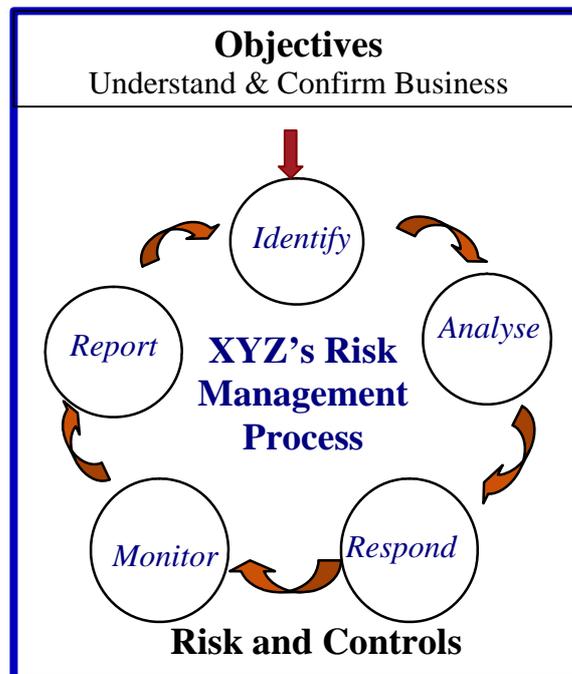
In order to achieve the above, XYZ must therefore streamline the actions of all staff, individually and collectively towards achieving its business objectives. This entails the alignment of the objectives, risks and controls throughout the enterprise. It should encompass the respective business processes and operational activities undertaken by all levels of staff. The diagram below depicts how this alignment may be achieved.



ENTERPRISE RISK MANAGEMENT PROCESS

OVERVIEW

The basis of the XYZ Enterprise Risk Management Process is a continuous cycle anchored in the five steps of identify, analyse, respond, monitor and report as shown below. Within each step of the process, regular and meaningful communication is essential to improve the likelihood of success. By viewing this cycle as a continual loop, managers are reminded of the need for thoughtful and regular feedback, as improvement is critical to successful risk management.



ENTERPRISE RISK MANAGEMENT PROCESS

STEP 1: IDENTIFY

Systematically and continuously identify risks faced in meeting objectives

For each business objective, it is necessary to identify the key risks that might impede the achievement of the respective business objectives. Risk identification should be performed as part of all major decision making processes, as shown below:

Each major decision level

- Group strategy planning
- Business Unit operating plans
- Core processes
- Project plans
- Investment (Buy/Sell) decisions
- Personal plans

Collective and individual assessment of risks

- By individuals in groups using techniques such as brainstorming, internal and external input e.g. project sub-contractor presentations

New Projects

- Project team planning
- Project paper presentation and discussions

Process or system changes

- Change requests

Identifying the current risk profile is a separate and discreet exercise when Enterprise Risk Management framework is first adopted. Thereafter, risks can be updated on an ongoing basis by integrating the identify step with core business management processes.

XYZ SOURCES OF RISK

Risks identified are categorised by sources to facilitate the determination of root cause and subsequently to assign responsibility for responses. The following list represents XYZ key sources of risk.

- Direction and Decision Making
- Political Influence
- Human Capital
- Management Information systems
- Fraud, Theft and Malicious Acts
- Economic
- Regulatory/Licence
- Natural Events
- Environmental Health and Safety
- Suppliers
- Product
- Finance
- Network
- Location
- Technology
- Distribution Channels
- Competition

Sample Enterprise Risk Management Framework

ENTERPRISE RISK MANAGEMENT PROCESS

STEP 2: ANALYSE

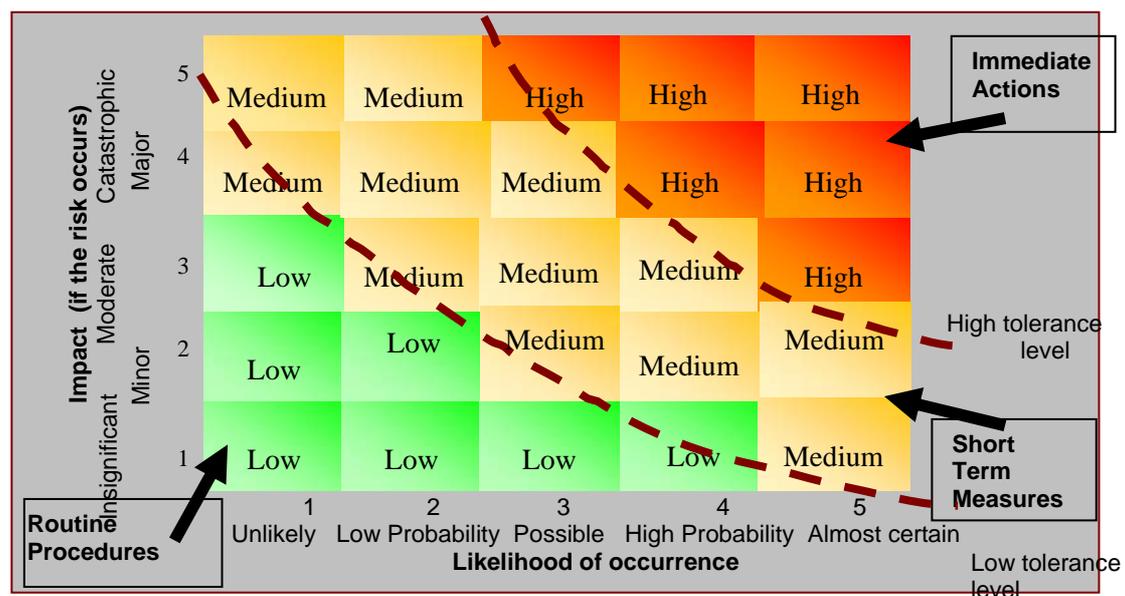
Assess the significance of risks to enable the development of Risk Responses

Once the risks have been identified, the **likelihood** of the risk occurring and the potential **impact** if the risk does occur are assessed using the risk rating table below.

Likelihood Rating				
5	4	3	2	1
Almost certain	High probability	Possible	Low probability	Unlikely

Risk Impact Rating				
5	4	3	2	1
Financial – direct loss or opportunity costs of:				
>100m	>50m – 100m	>25m – 50m	>10mil-25mil	1mil - 10 mil
Operational - missed milestone by:				
>6months	>3-6 months	1-3 months	1-4 weeks	<1 week
Regulatory				
Large scale action, material breach of legislation with very significant financial or reputational consequences	Regulatory breach with material consequences but which cannot be readily rectified	Regulatory breach with material consequences but which can be readily rectified	Regulatory breach with minimal consequences but which cannot be readily rectified	Regulatory breach with minimal consequences and readily rectified
Strategic / Organisation-wide				
Failure to meet key strategic objective; organisational viability threatened; major financial overrun	Major impact on strategy; major reputational sensitivity	Moderate impact on strategy; moderate reputational sensitivity	Minor impact on strategy; minor reputational sensitivity	Minimal impact on strategy. Minimal reputational sensitivity
Personnel - Loss of managerial staff in 1 year:				
>40	21-30	11-20	6-10	<5

The risks are depicted in a 5x5 **Risk Map**, which represents XYZ's risk profile:

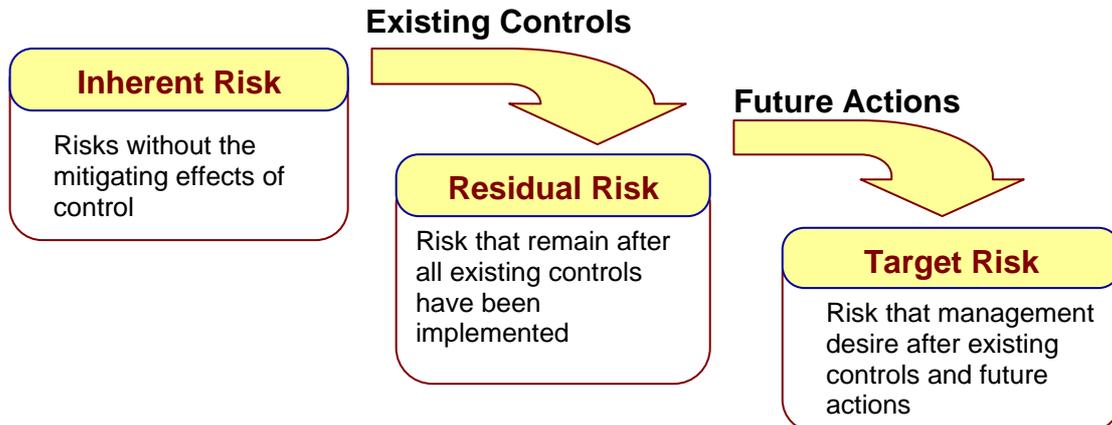


ENTERPRISE RISK MANAGEMENT PROCESS

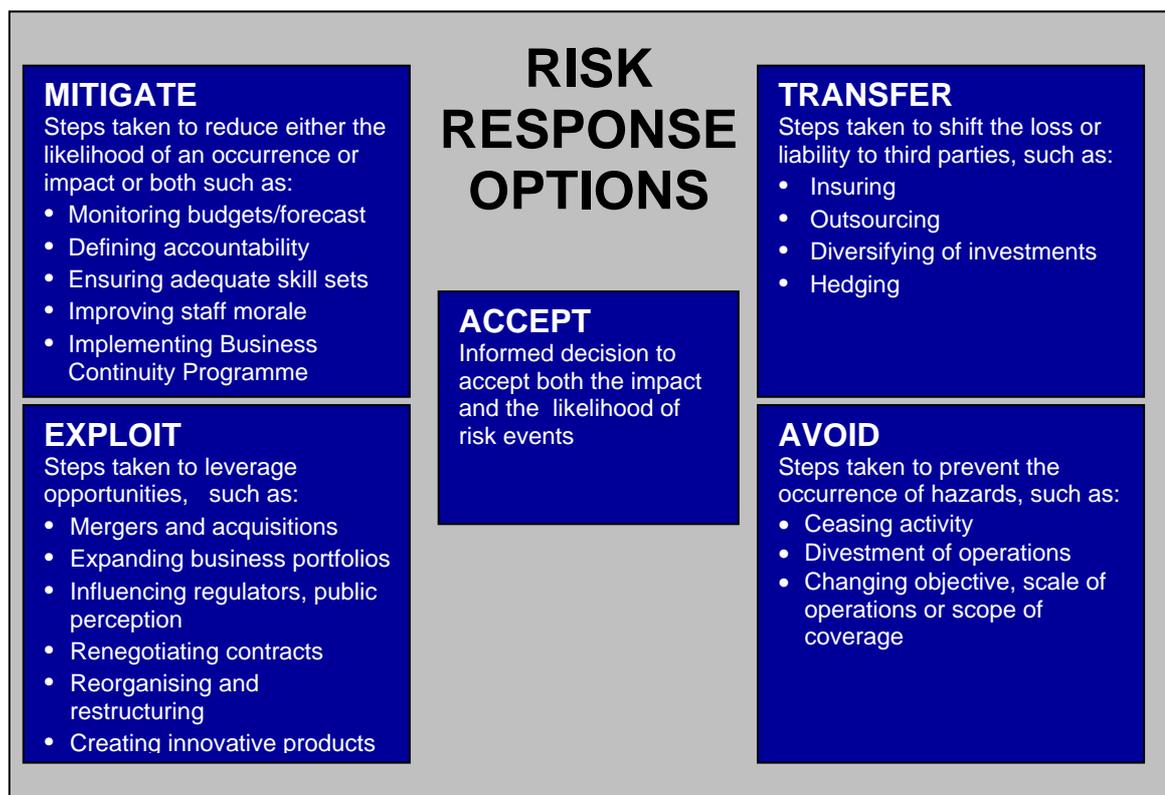
STEP 3: RESPOND

Decide and formulate effective risk response strategies and plans

Once risks have been analysed, appropriate risk responses can be determined to mitigate risk to an acceptable level within reasonable costs. XYZ's inherent and residual risk profile presented on the Risk Map are monitored against the target risk profile.



Risks can be dealt with in various ways. The risk response options encompass all possible management response to risk, whether viewed as opportunities, uncertainties or hazards. The risk response options and examples of activities under each option are outlined below:



ENTERPRISE RISK MANAGEMENT PROCESS

STEP 4: MONITOR

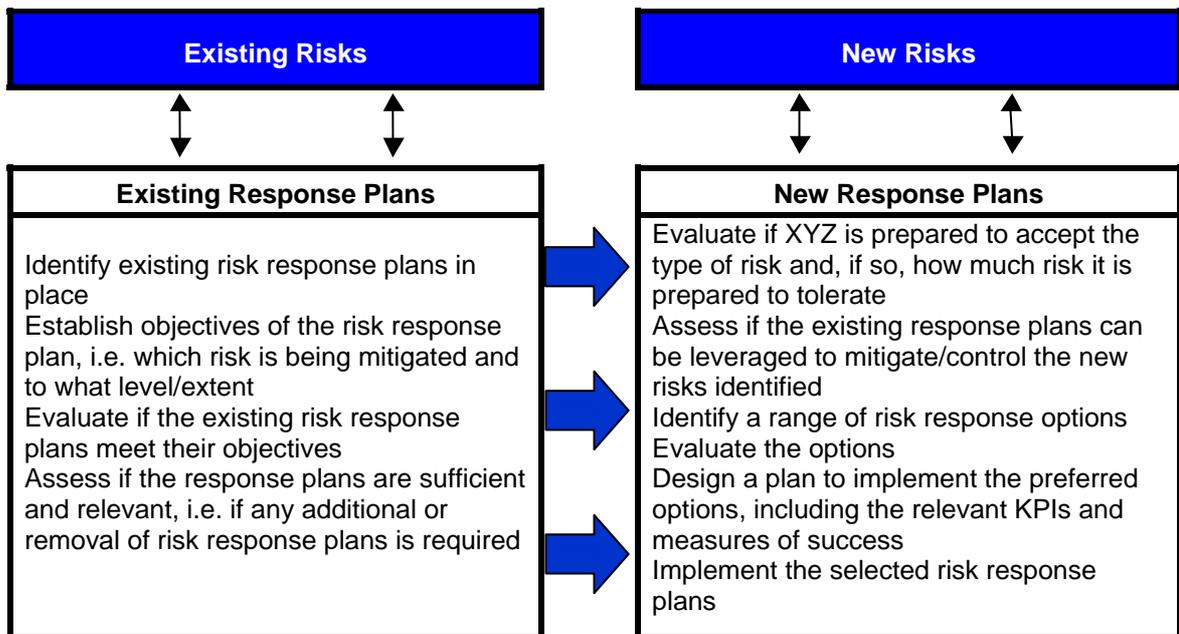
Continuously ensure that the risk response plans are operational and relevant

The monitoring and review of the risk profile and the risk response plans is a continuous process. The purpose of the review is to:

- provide assurance that risks are being managed as expected;
- assess whether the risk response plans remain relevant; and
- ensure that the risk profile anticipates and reflects changed circumstances and new exposures.

Risk monitoring consists of a combination of regular communication, periodic reviews or audits and evaluation by independent executives at appropriate levels at XYZ. Assurance techniques include:

- periodic or random testing of controls, risks and control environment
- quality assurance reviews
- post-implementation reviews
- performance appraisals



Risk response should be measured in terms of efficiency and effectiveness. Efficiency measures the cost of implementing risk management responses in terms of time, money and resources, whereas effectiveness measures the relative degree to which the responses reduce the impact or likelihood of the risk occurring.

To maximise efficiency and effectiveness of risk responses, monitoring and reporting should be integrated with existing business processes and reporting as far as possible.

ENTERPRISE RISK MANAGEMENT PROCESS

STEP 5: REPORT

Determine risk owner and report the status of risks and associated responses

While everyone in XYZ is responsible for enterprise risk management in their respective areas, some staff have specific responsibilities. The policy, design and framework for enterprise risk management is driven by the Board and managed by the enterprise risk management team.

The reporting structure ensures that risk response gaps are addressed and the risk responses are operating effectively under changing conditions. Enterprise risk management activities should be monitored and reported upwards throughout XYZ as illustrated in the following diagram.

