Enterprise Risk Management Framework

PHX021

Contents

Copyright Notice

Disclaimer

The material and information contained in the document is for general information purposes only, and as specified through the nature of the topics covered. While we endeavour to keep the information up to date and correct, Phoenix Software Ltd makes no representations or warranties of any kind, express or implied about the completeness, accuracy, reliability, suitability, or availability of information with respect to the policy, and any reliance placed on such material is therefore strictly at your own risk.

Phoenix Software: Ethics Statement

Phoenix Software Ltd ("Phoenix") adheres to the highest levels of lawful, ethical, and responsible business conduct and it requires its suppliers, customers, and stakeholders of Phoenix, in their interaction with the business, to adhere to similar principles.

The complete company polices will be provided on request and are also available at www.phoenixs.co.uk

INTRODUCTION

Phoenix Software Ltd ("Phoenix") operates within ICT sector in the UK. Phoenix is therefore exposed to financial, political, regulatory, technology and legal events that could potentially adversely affect the achievement of its strategic, operational, compliance or reporting objectives.

Phoenix is an operating company within Bytes Technology Group PLC, Bytes House, Leatherhead, Surrey, KT22 7DW

The Enterprise Risk Management (ERM) framework represents Bytes Technology Group's coordinated plan for risk management across the business. The Phoenix ERM supports that framework and where working practices with Phoenix influence a change of practice to the Group ERM process this is highlighted.

The Board of directors of Phoenix has committed the organisation to a process of risk management that is aligned to the principles of the UK Corporate Governance Code, COSO and the ISO31000 Integrated Enterprise Risk Management Framework. The ERM methodologies are also defined through continued research and development as well as being benchmarked against international best practice. In defining these specifics, it is necessary to understand the specific requirements from a Board and management perspective as emphasised by the UK Corporate Governance Code. These principles can be highlighted as follows:

The Role of the Bytes Technology Board (in respect of)

C2: Risk Management and Internal Control

Main Principle

The board is responsible for determining the nature and extend of the principal risk it is willing to take in achieving its strategic objectives. The board should maintain sound risk management and internal control systems.

Code Provisions

C.2.1 The directors should confirm in the annual report that they have carried out a robust assessment of the principal risks facing the company, including those that would threaten its business model, future performance, solvency, or liquidity. The directors should describe those risks and explain how they are being managed or mitigated.

C.2.2 Taking account of the company's current position and principal risks, the directors should explain in the annual report how they have assessed the prospects of the company, over what period they have done so and why they consider that period to be appropriate. The directors should state whether they have a reasonable expectation that the company will be able to continue in operation and meet its liabilities as they fall due over the period of their assessment, drawing attention to any qualifications or assumptions as necessary.

C.2.3 The board should monitor the company's risk management and internal control systems and, at least annually, carry out a review of their effectiveness, and report on that review in the annual report. The monitoring and review should cover all material controls, including financial, operational and compliance controls.

1. Components of the Enterprise Risk Management Process

Enterprise risk management consists of interrelated components as per COSO and ISO31000 Frameworks. These are derived from the way management runs the enterprise and are integrated with the management process. These components are:

COMPONENTS OF COSO 2004

Internal environment

- Objective setting
- Event identification
- Risk assessment
- Risk response
- Control activities
- Information and communication
- Monitoring

Objective consideration

- Strategic
- Operational
- Compliance
- Reporting

COMPONENTS OF ISO31000 2010

Establish the content

- Risk assessment
- Risk identification
- Risk evaluation
- Risk response
  - tolerate
  - treat
  - transfer
  - terminate

Risk treatment

- Monitoring and control

Communication and consultation

2. Objectives Of Enterprise Risk Management

2.1 Objectives

Enterprise Risk Management (ERM) is about managing risk across the enterprise and should serve as a key enabler in the deliverance of Phoenix's strategy. To break it down further, ERM is about:

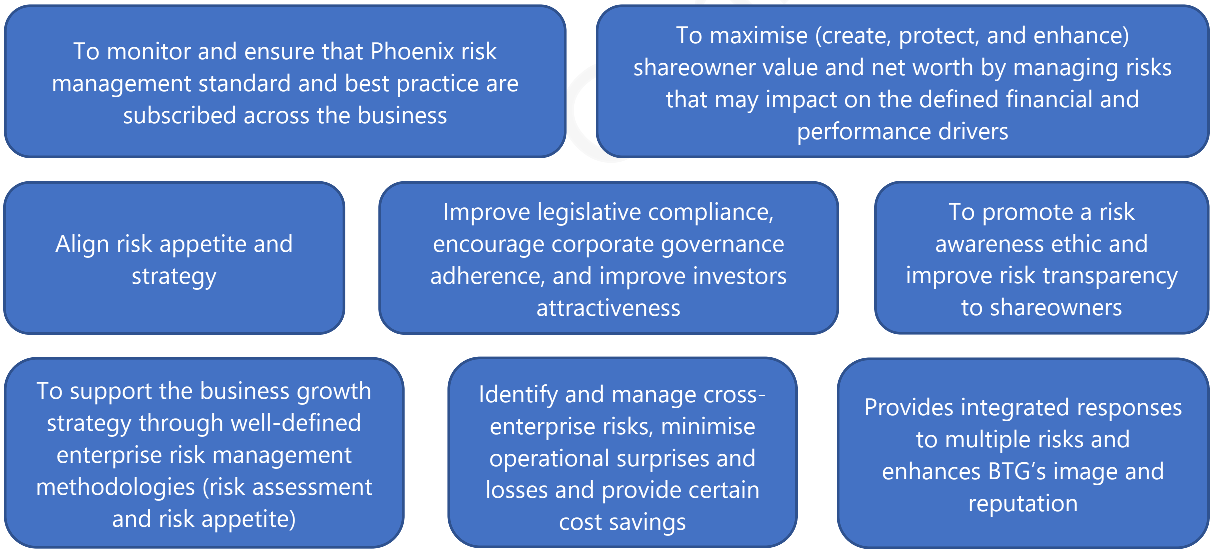
- Identifying negative and positive risk circumstances
- Assessing risks in terms of likelihood and magnitude of impact
- Creating a response strategy and monitoring it
- Creating value for its stakeholders, shareholders, employees, and customers
- To assist business in achieving their objectives by proactively de-risking their business plans

Phoenix's Enterprise Risk Management is a function within Phoenix that sets out to achieve the following key objectives:

- **Oversight:** All critical risks are identified group-wide and are managed and monitored under a holistic approach consistent with the approved risk appetite statement.
- **Ownership and Responsibility:** The ownership of risk is assigned to management individuals who are responsible for identifying, evaluating, mitigating, and reporting risk exposures.
- **Assurance:** The Board and its sub-committees, Group Exco and management have reasonable assurance that the risk is being appropriately managed within defined levels to bring value to the organisation.

2.2 Benefits

The overall benefits of enterprise risk management give effect to a risk management programme that supports Phoenix's vision and objectives as defined by Phoenix's strategy. Specific benefits of effective risk management include the following:



To monitor and ensure that Phoenix risk management standard and best practice are subscribed across the business

To maximise (create, protect, and enhance) shareowner value and net worth by managing risks that may impact on the defined financial and performance drivers

Align risk appetite and strategy

Improve legislative compliance, encourage corporate governance adherence, and improve investors attractiveness

To promote a risk awareness ethic and improve risk transparency to shareowners

To support the business growth strategy through well-defined enterprise risk management methodologies (risk assessment and risk appetite)

Identify and manage cross-enterprise risks, minimise operational surprises and losses and provide certain cost savings

Provides integrated responses to multiple risks and enhances BTG's image and reputation

3. Phoenix's Enterprise Risk Management Strategic Process

The strategy of ERM is to assist management of Phoenix in ensuring that its strategy and business plans are not negatively affected by various risks. To achieve this, the enterprise risk management process is followed.

The ERM process is driven by a series of activities and events designed to integrate ERM within business processes across the enterprise and ensure that there is standardisation and common elements across all these occurrences. Enterprise risk management is not strictly a serial process, where one component affects only the next. It is a multidirectional, iterative process in which almost any component can and does influence another.

The 11 risk management principles on which the ERM framework is based consist of the following:

1. **Risk strategy** – A strategy must be in place for managing risk across the Group which includes the consideration of the inter-relationships and correlations between risks.
2. **Risk governance structures** - Risk governance structures must be in place to ensure that all applicable statutory and regulatory requirements and risk management standards are met.
3. **Responsibility and accountability** - Responsibility and accountability for risk management must be clearly assigned, documented, and communicated throughout the Group with the aim of fostering an open and transparent risk culture that encourages best practice risk management behaviour.
4. **Risk appetite and risk tolerance** - Risk appetite statements must reflect the nature and level of risk the Group is willing to take to achieve specific business objectives.
5. **Objective identification** – Objective identification for any risk management assessment is important. It requires a thorough understanding of the environment in which an organisation exists and operates.
6. **Risk management processes** - Risk management processes and procedures must be in place to ensure risks are identified, measured, managed, monitored, and reported on a consistent basis.
7. **Risk response and mitigation** - Risk-specific response and mitigation plans, including business continuity and crisis management plans, must always be in place with clear criteria set for when such plans are invoked.
8. **Risk monitoring** - The level of risk exposure must be actively monitored (key risk indicators, key control indicators and key performance indicators) against the limits set and/or the capital available.
9. **Risk incidents / Internal loss management** - Processes must be in place to ensure that unexpected internal losses are identified, escalated, and remedied promptly.
10. **Stress and scenario analysis** - The resilience of the business to risk incidents must be tested under both normal and stressed conditions, including developing an understanding of the severity of an incident that would cause the business to breach its risk appetite and tolerance limits.
11. **Risk reporting** - Risk reporting must be accurate, relevant, and timely to support the management of risks, meet the needs of all relevant internal and external stakeholders and, where required, meet the specific reporting needs of separate legal entities.

4. Risk Strategy

The risk strategy provides a high-level perspective of the nature of the risks that the business is willing to participate in as well as provides guidance on Phoenix's approach to measuring and managing risk and return. Phoenix's risk strategy will be reviewed in line with the changes in its business strategy.

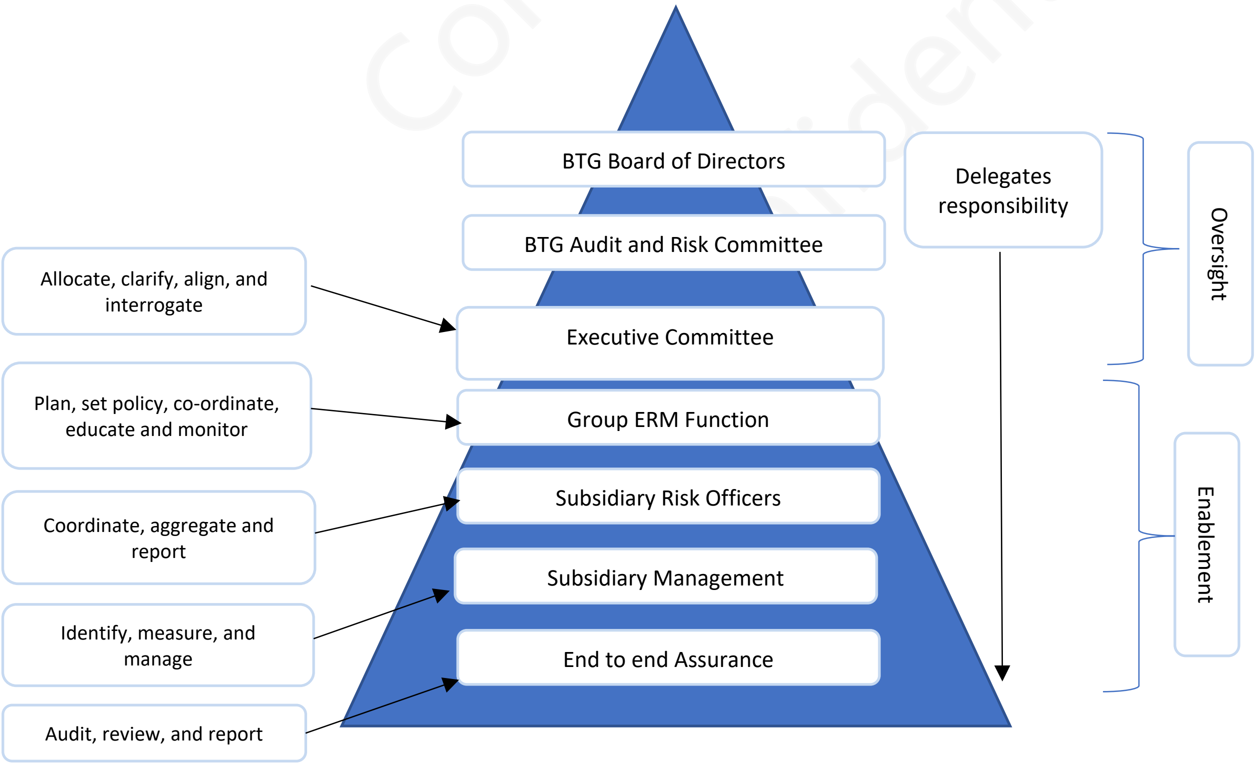
5. Risk Governance Structures

The Board of Directors of BTG through the BTG Audit and Risk Committee are responsible for the total process of risk management. The Managing Director, part of the Executive Committee, is responsible for implementing and reporting on the policies, frameworks, and requirements to align with the Group's Enterprise Risk Management Function. The Executive Committee comprises of the BTG CEO, BTG CFO, BSS MD, Phoenix MD.

The Subsidiary Risk officer for Phoenix is Operations Director, who along with the Subsidiary Executive Management, performs ongoing risk exposure analysis and produces a risk profile report, demonstrating the management of key risks and opportunities identified.

The Enterprise Risk Management Function results are presented at the Phoenix Software Board Meeting on a six-monthly basis.

Essential to the achievement of the ERM objectives is the implementation of a governance structure to support the achievement of the objectives. The following diagram depicts the ERM governance structure to include Bytes Technology Group PLC:


BTG Board of Directors
BTG Audit and Risk Committee
Executive Committee
Group ERM Function
Subsidiary Risk Officers
Subsidiary Management
End to end Assurance
Allocate, clarify, align, and interrogate
Plan, set policy, co-ordinate, educate and monitor
Coordinate, aggregate and report
Identify, measure, and manage
Audit, review, and report
Delegates responsibility
Oversight
Enablement

6. Responsibility and Accountability

6.1 Commitment and Mandate

Phoenix is committed to the optimal management of risk in order to achieve our vision, our principal tasks, and key objectives and to protect our core values.

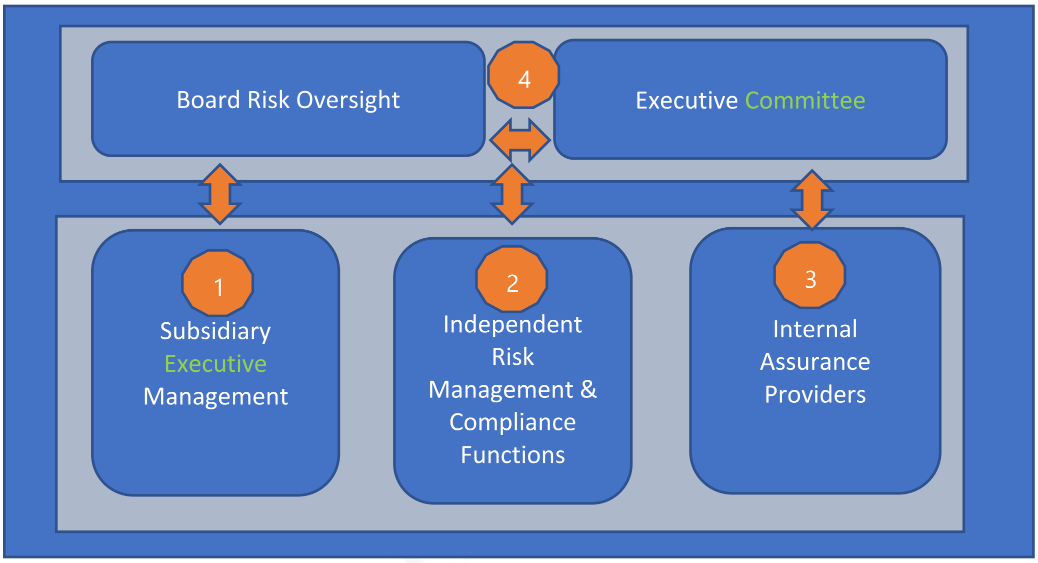
The Board of Directors of Phoenix has committed the organisation to a process of risk management that is aligned to the principles of the UK Corporate Governance Code, COSO and the ISO31000 Integrated Enterprise Risk Management Framework.
Effective risk management is imperative to Phoenix with reference to our risk profile. The realisation of our strategy depends on us being able to take calculated risks in a manner that does not jeopardise the direct interests of stakeholders and interested parties. Sound management of risk will enable us to anticipate and respond to changes in our environment, as well as to enable us to make informed decisions under conditions of uncertainty. An organisation wide approach to risk management will be adopted by Phoenix, which means that every key risk in each part of the organisation will be included in a structured and systematic process of risk management. All key risks will be managed within a unitary framework that is aligned to Phoenix's corporate governance responsibilities.

It is expected that risk management processes will become embedded in all the organisation's systems and processes, to ensure that Phoenix's responses to risk remain current and dynamic. All key risks associated with major changes and significant actions by Phoenix will also fall within the processes of risk management.

Phoenix has structured a risk appetite statement which sets the tone for the levels of risk that the company is willing to accept in the pursuit of business targets. Risk appetite is the amount of risk that Phoenix is willing to take in the pursuit of value.

6.2 Roles and Responsibilities

In defining the specific accountabilities, roles, and responsibilities, it is necessary to understand the specific requirements in terms of the lines of defence as emphasised by the UK Corporate Governance Code, which states that the Board is ultimately accountable for risk management.


Board Risk Oversight
4
Executive Committee
1
Subsidiary Executive Management
2
Independent Risk Management & Compliance Functions
3
Internal Assurance Providers

1 The first line of defence consists of the subsidiary management They are responsible for the implementation of risk frameworks, inclusive of risk identification, assessment, and response, as defined by the second line of defence. They must design capabilities for managing risk in accordance with the selected risk response and consistent with the risk appetite.

2 The second line of defence consist of risk management, compliance, and other independent functions, that establish risk management policies, set standards for managing risk, enforce risk appetite and provide appropriate oversight. These functions ensure that appropriate frameworks for managing risk have been implemented by the subsidiary management consistently.

3 The third line of defence consist of the internal assurance providers. Internal assurance providers review controls, risk management procedures, identify issues and improvement opportunities, makes recommendations, and keeps the Board and Executive management informed of the status of risk management. Internal assurance provides have a high level of independence and objectivity.

4 The Board's risk oversight plays an important role in ensuring executive management appropriately handles escalated risk issues and involved the appropriate Board committee in a timely manner. Executive management and the Board are the last line of defence when significant issues are escalated upward.

The roles and responsibilities are defined as follows:

a) BTG Board of Directors

- Is accountable for the risk management process.
- Approves the Phoenix risk philosophy.
- Approves the risk management plan.
- Approves the ERM policy and framework.
- Approves the risk appetite framework and tolerance levels.
- Reports on the effectiveness of risk management.

- Ensure that the company's reputational risk is protected; and
- Determine the extent to which risks relating to sustainability are addressed and reported on.

b) Executive Committee – BTG CEO, COO, Phoenix MD, Bytes MD

- Recommends the ERM policy and framework for approval.
- Recommends the ERM plan for approval; and
- Recommends the risk appetite and tolerance levels for approval.
- Monitors the implementation of the ERM policy, framework, and plan.
- Monitors risk appetite; and
- Monitor to ensure that key risks are quantified and are responded to appropriately.

c) Subsidiary Executive management – Phoenix Board Members

- Implementation of ERM plan.
- Implementation of risk appetite framework.
- Implements and maintains risk registers.
- Identification of mitigating controls; and
- Implementation of action plans.

d) Subsidiary Risk Officers are responsible for: Operations Director

Each subsidiary is to nominate a Risk Officer. The Risk Officer shall be a member of Senior Management within the subsidiary and their responsibilities include:

- Facilitating the implementation of the Group ERM policy and framework.
- Creating risk awareness within the subsidiary.
- Facilitation of workshops for risk identification and assessment to develop risk registers for the subsidiary.
- Development and monitoring of the subsidiary risk appetite framework.
- Continuous monitoring and maintenance of risk registers.
- Key risk indicator analysis and action plan monitoring.
- Risk reporting of the consolidated subsidiary risks and action plans to Subsidiary Executives and to the Group Risk Management Function.

e) Internal Assurance Providers - Governance Manager

To provide assurance to the company's stakeholders that the company operates in a responsible manner by performing the following functions:

- Evaluating Phoenix's governance processes including ethics, especially the 'tone at the top';
- Performing an objective assessment of the effectiveness of risk management and the internal control framework.
- Systematically analysing and evaluating business processes and associated controls; and

- Providing a source of information, as appropriate, regarding instances of fraud, corruption, unethical behaviour, and irregularities.

Internal Audit ensure that it is subjected to an independent quality review, either in line with IIA standards or as and when the Audit Committee determines it appropriate, as a measure to ensure the function remains effective.

6.3 Communication and Training

An effective ERM communications programme is a primary management tool for reducing risks within the organisation. The Enterprise Risk Management Function shall champion the risk awareness initiative with the support of management and ensure that risk management saturates at all levels of the company. The function shall develop, establish, and implement infrastructure to ensure that managing risk becomes an integral part of planning, management processes and the overall culture of the organisation.

This shall include:

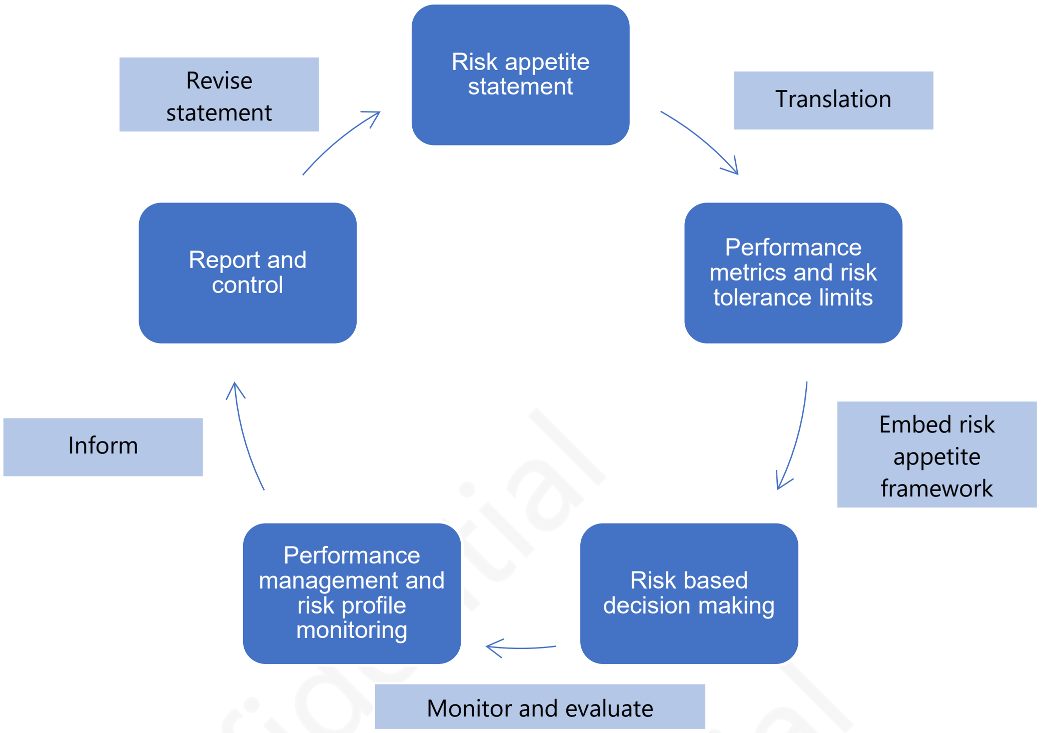
- Establishing a team consisting of management personnel to be responsible for the communication of risk issues.
- Raising awareness about managing risks.
- Communication/dialogue throughout the organisation about managing risk.
- Acquiring risk management skills through risk specialists (internal and external); and
- Ensuring appropriate levels of recognition and rewards.

7. Risk Appetite and Risk Tolerance

Enterprise Risk Management (ERM) ensures a structured and consistent approach to risk management, aligning risk appetite to strategy, processes, people, and technology. The approach to ERM and determining and setting risk appetite provides Phoenix with the information and knowledge to evaluate and manage the uncertainties faced in creating shareholder value.

The UK Corporate Governance Code and international risk management standards requires a Board of Directors to approve the ERM framework and risk appetite.

The Risk Appetite Framework is therefore a key business performance tool and is central to strategic planning, delegation of authority and establishment of aligned roles and responsibilities within Phoenix.


Risk appetite statement
Translation
Performance metrics and risk tolerance limits
Embed risk appetite framework
Risk based decision making
Monitor and evaluate
Performance management and risk profile monitoring
Inform
Report and control
Revise statement

7.1 Risk Appetite Statement

The risk appetite statement and tolerance levels are calibrated against Phoenix's broad financial targets and is prepared each year, as part of the planning process, combining a top-down view of the company's risk capacity with a bottom-up view of the risk profile. Phoenix's risk appetite statement has been defined in the Risk Appetite Framework.

7.2 Risk Tolerance (Limits)

Risk tolerance levels monitor that the actual risk exposure does not deviate too much within an organisation's risk appetite and risk bearing capacity. Exceeding risk limits will typically act as a trigger for management action.

While risk appetite is broad, risk tolerance is tactical and operational. Risk tolerance must be expressed in such a way that it can be:

- Mapped into the same metrics the organisation uses to measure success.
- Applied to categories of impact factors or objectives (people, financial, regulatory, legal, customers, reputational, and business interruptions); and
- Implemented by operational personnel throughout the organisation.

Because risk tolerance/escalation is defined within the context of objectives/impact and risk appetite, it should be communicated using the metrics in place to measure performance. In that way, risk tolerance sets the boundaries of acceptable performance variability.

7.3 Performance Management and Risk Monitoring

Once an organisation's risk appetite is developed and communicated, management with Board support must revisit and reinforce it. Risk appetite cannot be set once and then left alone for extended periods. Rather, it should be reviewed and incorporated into decisions about how the organisation operates. This is especially important if the organisation's business model begins to change.

Management should monitor the organisation's activities for consistency with risk appetite through the specifics identified with risk tolerances. Business Units should have key risk metrics that they use to measure performance. It is easy to integrate risk tolerances into the monitoring process used to evaluate performance.

7.4 Report and Control

For many organisations, monitoring risk tolerances requires a culture that is aware of risks and risk appetite. Management, by revisiting and reinforcing risk appetite, can create a culture whose organisational goals are consistent with the Board's, and to hold those responsible for implementing risk management within the risk appetite parameters.

Creating a culture is one way of reinforcing overall risk appetite. The approach is best used when the organisation has a well-communicated risk appetite and associated risk tolerances, to the point at which the following outcomes exist:

- Consistent implementation across the business
- Effective monitoring and communication of risk and changes in risk appetite
- Consistent understanding of risk appetite and related tolerances for each business activity
- Consistency between risk appetite, objectives, and relevant reward systems.

This approach draws on ongoing and separate evaluations conducted as part of the organisation's monitoring. Any variation from the stated (or desired) risk appetite is then reported to management and the Board as part of the normal internal reporting process.

8. Objective Identification

Establishing objectives which are aligned to Phoenix's mission, vision, goals, and values, is the reference point for identifying and assessing risks. Thus, objective setting is a pre-condition to any risk management process.

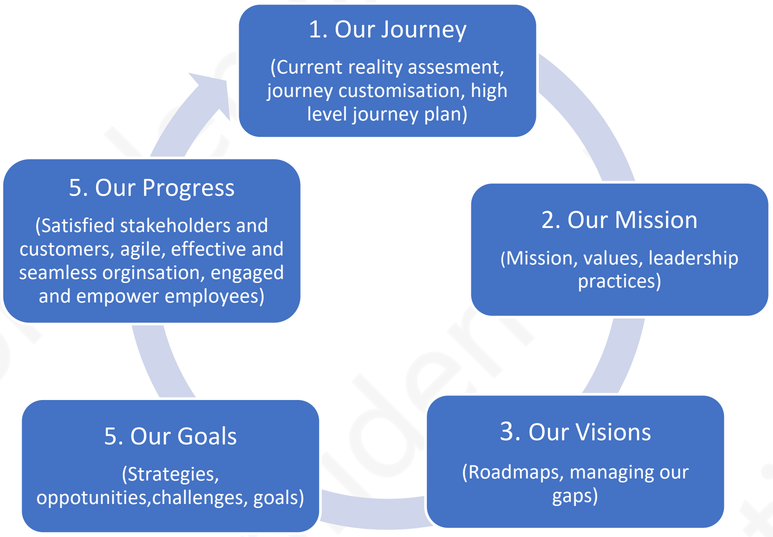
Every entity faces a variety of risks from external and internal sources, and a precondition to effective event identification, risk assessment and risk response is establishment of objectives.

Objectives are aligned with the organisation risk appetite, which drives the risk tolerance levels for the entity.

Phoenix has established an enterprise-wide risk management approach that enables an informed response to opportunities and threats in the business environment. On an annual basis, or upon changes within the business environment, Phoenix's Enterprise Risk Management Function will facilitate the alignment of the business strategic objectives for the particular financial year.

8.1 Benefits of Objective Setting

- It provides a sense of direction.
- It motivates the leaders and service organisations to aim for specific targets to attain the set objectives, which are linked to the strategy and business plans.
- It supports the evaluation of Phoenix's performance; and
- It serves as a control device to ensure that objectives are met.

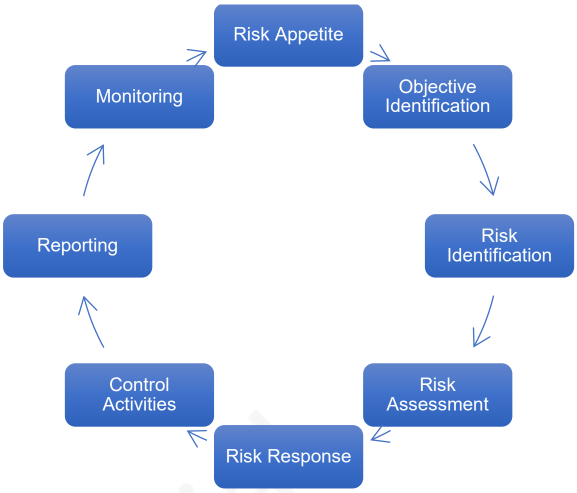

1. Our Journey
(Current reality assesment, journey customisation, high level journey plan)
2. Our Mission
(Mission, values, leadership practices)
3. Our Visions
(Roadmaps, managing our gaps)
5. Our Goals
(Strategies, oppotunities,challenges, goals)
5. Our Progress
(Satisfied stakeholders and customers, agile, effective and seamless orginsation, engaged and empower employees)

9. Risk Management Processes

The ERM process is driven by a series of activities and events designed to integrate ERM within business processes across the enterprise and ensure that there is standardisation and common elements across all these occurrences.

Enterprise risk management is not strictly a serial process, where one component affects only the next. It is a multidirectional, iterative process in which almost any component can and does influence another. It is also important to ensure that ERM process and risks are re-evaluated and updated on an on-going basis to reflect new information and experiences so that all significant risks are appropriately identified and addressed and that any material opportunities are not overlooked.

The following cyclical flow depicts the critical enterprise functional risk management activities undertaken on an on-going basis.



9.1 Risk Identification

The risk identification phase of enterprise risk management is critical to ensure that uncertain events and opportunities that may impact the objectives are identified.

The focus of ERM is on integrating risk management into strategy setting. The emphasis is on identifying potential future events that can/have both positive and negative effects and evaluating affective strategies for managing the organisation's exposure to those future events.

The following risk identification techniques are used by management:

a) Workshops

Risk assessment workshops and advisory sessions are held by management on quarterly basis to identify potential events that my result in the non-achievement of their business objectives.

b) Management information

Data analysis, review of performance indicators, economic information, loss data, and the like can produce important risk information. The following reports and documents are used to identify risks:

- Management/Board reports.
- Incident reports.
- Benchmarking data.
- Customer NPS scores
- Market analysis.
- Budget/actual variances.
- External and internal audit reports; and
- Business plan incorporating risk information

c) One-on-one Meetings

One-on-one meetings are held to help identify and update existing risks and controls. Meetings can be in person or virtual

d) Emerging risks

To be pro-active in the identification of risk, it is important that Phoenix also considers those risks that are on the horizon.

A variety of information and reports are generated in Phoenix and subsidiaries that are used to highlight emerging risks. Management and ERM plays a key role in placing this information into context.

Data originates from:

- PEST studies of the external environment (Political, Economic, Social and Technological Factors).
    - PEST analysis describes a framework of macro environmental factors used in the environmental scanning component of strategic management.
- SWOT analysis of the internal environment.
    - SWOT analysis is a strategic planning method used to evaluate the Strengths, Weaknesses, Opportunities, and Threats involved in a project or in a business venture.
    - Identification of SWOTs is essential because subsequent steps in the process of planning for achievement of the selected objective may be derived from the SWOTs.
- Benchmarking the organisation to competitors.

9.2 Loss Event and Risk Experience

Should the historical exposure and impact of the risk be known in monetary value, this should be recorded. Note that it should not just be limited to a loss event but also in the case of a gain which can be defined as upside or opportunity. (Examples are fines for non-compliance, market growth due to expansion, etc.).

9.3 Risk Classification / Categories

Phoenix's risk categorisation or classification is aimed at determining the nature and type of the risk, which assists in identifying similar risks. The risk categories will be reviewed annually by Bytes Technology Group and updated to Phoenix.

9.4 Risk Assessment

Risks are measured to determine the impact (criticality) and likelihood of occurrence levels. The main objective of a risk assessment exercise is to assist management in prioritising identified risks. This enables management to spend more time, effort, and resources to manage risks of higher priority.

The assessment is performed based on the approved enterprise risk management methodology. Risks are assessed based on impact of occurrence and likelihood of the risk occurring at that level of impact. (Risk = Impact x Likelihood).

a) Impact / consequences

Key causes and potential consequences of risks are identified. This is the potential magnitude of the impact on the business operations should the risk/threat occur. This is assessed on the basis that management has no specific/focused controls in place to address the risk/threat (therefore before any controls). The Impact Risk Ranking Table as defined in the Risk Appetite Framework must be used to assist management in quantifying the potential impact that a risk exposure may have on the business.

Impact Category	Category Definition	Factor
Catastrophic	A disaster with a potential to lead to the collapse of the company and is fundamental to the achievement of objectives.	5
Severe	An event which can be endured but which may have a prolonged negative impact and extensive consequences to the company.	4
Material	Major events, which can be managed but that require additional resources and management effort.	3
Moderate	Consequences can be absorbed under normal operating conditions.	2
Minor	The impact is minor and can easily be contained.	1

b) Probability / likelihood

This is the likelihood that the identified risks will occur within a specified period on the basis that management has no controls in place (inherent level). The following table represents the Likelihood Risk Ranking Table used to assess Inherent Risk Exposure.

Likelihood category	Category definition	Likelihood % total instances	Likelihood - Historical and future risk views	Factor
Confidently Expected	The event is confidently expected to occur in most circumstances.	>75%	• Occurred in last 3 months • May occur in 3-6 months	**5**
Probable	The event will probably occur in most circumstances.	50% - 75%	• Occurred in last 6 months • May occur in 6-12 months	**4**
Possible	There is a moderate chance that the event will occur.	25% - 50%	• Occurred in last 12 months • May occur in 12-24 months	**3**
Unlikely	The event is unlikely to occur.	10% - 25%	• Occurred in last 2 year • May occur in 2-3 years	**2**
Remote	The event is extremely unlikely and may occur only in exceptional circumstances.	< 10%	• Occurred in last 3 years • May occur in >3 years	**1**

i. Inherent risk exposure (Impact x Likelihood)

Inherent risk considers the "worst case" scenario. This involves considering the impact and likelihood of the risk in the absence of any management control interventions. The actual risk exposure is calculated using the following formula: Impact x Likelihood = Inherent Risk Exposure. This level of assessment provides a perspective of the consequences of the risk to Phoenix in its unmanaged state. The table below should be used to categorise the various levels of inherent risk.

			LIKELIHOOD				
			Remote < 10%	Unlikely 10% - 25%	Possible 25% - 50%	Probable 50% - 75%	Confidently Expected >75%
			1	**2**	**3**	**4**	**5**
IMPACT	Catastrophic	**5**	Low	Medium	High	Very High	Catastrophic
	Severe	**4**	Low	Medium	High	Very High	Very High
	Material	**3**	Low	Medium	Medium	High	High
	Moderate	**2**	Low	Low	Medium	Medium	Medium
	Minor	**1**	Low	Low	Low	Low	Low

10. Risk Response and Mitigation

10.1 Risk Response

Implementing risk responses could involve expenditure of additional time, cost, or resources. Clearly it is important that Phoenix should be prepared to spend the required time, money, or effort in responding to identified risks, otherwise the process will be ineffective.

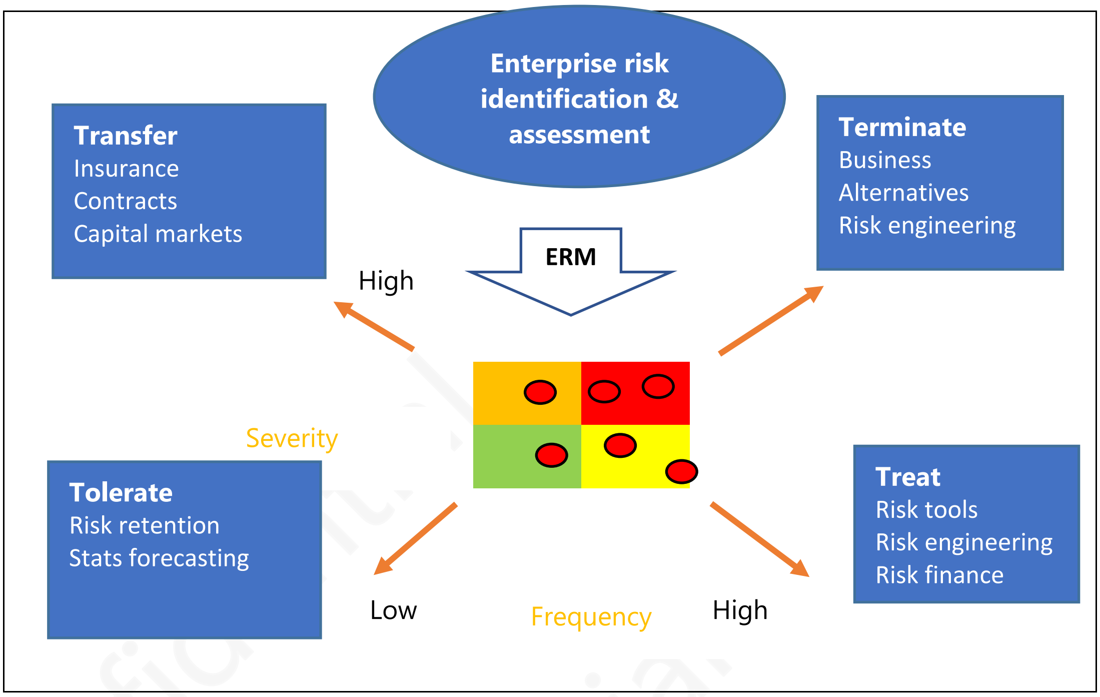
Identification and assessment of risk will be worthless unless responses are developed and implemented which optimises the risk response approach to the identified risks.

The purpose of risk response or control strategy planning is to reduce the "size" of the risk exposure to below a threshold of "risk acceptability. The "size" of a risk can be reduced by addressing either its probability to make it less likely, or its impact to make it less severe or both. Best practices are of a preventative nature rather than a corrective nature.

10.1.1 Elements of Risk Response

- Review risk information
- Identify risk response strategies
- Evaluate risk response strategies
- Select responses
- Risk profile / portfolio view

10.1.2 Identifying Risk Responses



In considering its response, management considers costs and benefits and select a response that brings expected likelihood and impact within the desired risk tolerance thus reducing the inherent risk to an acceptable level of residual risk. Refer to the diagram above illustrating the concepts.

a) Terminate risk

The first and best option to consider is whether a risk exposure can be terminated. Action is taken to avoid the activities giving rise to the risk.

This option is chosen when the cost of managing the risk is higher than eliminating the risk e.g. - Disposing of a business unit or a product line. Deciding not to engage in new initiatives/activities that would give rise to risks exceeding the appetite.

b) Treat the risk

Treating the risk implies reducing the risk to an acceptable level according to the criteria. Action is taken to reduce the likelihood and/or impact. This may be achieved through everyday business decisions.

Treatment involves a response to reduce a residual risk to a level that is in line with a business unit's risk tolerance. Examples could include the following:

- Implementation of processes and procedures that is cost effective.
- Enhancing management involvement in decision making, monitoring; and
- Reallocation of capital among operating units.

c) Transfer risk

Action is taken to reduce risk likelihood or impact by transferring or sharing a portion of the risk e.g., purchasing insurance products or outsourcing an activity to contractors/vendors.

Transfer responses, as in the case with reduction, reduces the residual risk to a level that is in line with Phoenix's risk tolerance.

Transferring risk has a cost: contractual risk, insurance premiums and excesses. For example:

- Insuring significant unexpected losses
- Enter joint venture/partnership
- Outsourcing business processes
- Sharing risk through contractual agreements with customers, vendors/other business
- Partners

d) Tolerate risk

For some risks, further action may not be justifiable or possible to reduce the risk, so a decision is made to tolerate/accept the risk. For example:

- "Self-insuring" against losses
- Accepting risk as already conforming to risk tolerance

Sometimes it may be more expensive to control a risk than the potential loss that it may produce. Tolerating a risk may suggest that the risk is in line with the company's risk tolerance. (If the loss incurred over a period is less than the mitigating cost.)

10.1.3 Select Risk Responses

- Once the effects of alternative risk responses have been evaluated, Management, the Executive Committee and the Risk Committee decide HOW to manage the risk by instituting controls.
- ERM requires that management select a response or combination of responses that brings anticipated risk likelihood and impact WITHIN the set enterprise' risk tolerance.
- A selected risk response may need an implementation plan to execute the response and recalibrate the risk on a residual basis.
- Internal audits could be applied to measure the effectiveness of the anticipated controls.
- It is recognised that some level of residual risk will always exist, not only because responses are limited, but also because of inherent future uncertainty and limitations in all activities.

- On a quarterly basis, the Risk Committee will assess the adequacy of the risk mitigation strategies and responses implemented and where appropriate make recommendations to both management and the Executive Committee of alternate options for implementation.

All the stakeholders should be consulted regarding the identified risks, this ensures that the risk is identified correctly, defined correctly, brings the expertise together in analysing the risk and ensures that all views are taken into consideration when formulating risk treatment plans.

10.2 Control Activities

Risks and risk categories are mapped to core business processes and controls. Controls are the management activities / policies / procedures/ processes / functions / departments / physical controls that the Board and management have put in place, and rely upon, to manage the strategic and operational key risks of Phoenix. Controls are designed to address risks that could prevent Phoenix from achieving its stated objectives.

10.2.1 Control Types

Management considers various control types as options to better manage the risks exposures to an acceptable level of residual risk:

a) Preventative controls

These controls are designed to prevent an undesired event from occurring e.g., a manager's review of purchases prior to approval prevents inappropriate expenditures of funds; or a computer application asking for a password prevents unauthorised access to information. If properly enforced, these controls are usually the most effective type of controls.

b) Detective controls

These controls are designed to detect errors that may have occurred. (e.g., performance of reconciliations, utilisation, and investigation of exception reports).

c) Corrective controls

These controls are designed to correct failures of detective and preventative controls; these controls are usually the least effective type of controls as the risk event has already materialised; and indicate a failure in the pro-active design of an effective control environment/activities.

10.2.2 Evaluation Of Current Adequacy

Controls are assessed based on design adequacy which involves evaluating whether the controls identified are suitably designed to prevent or detect errors on a timely basis. Controls will not be designed adequately if a key control is omitted; or if implemented controls do not ensure that the appropriate control objectives are achieved i.e., risks are mitigated. When assessing the design adequacy, the frequency and automation of the control are taken into consideration.

Once the controls have been identified and documented for each risk, their level of adequacy is determined by using the criteria listed in the table below. The design of controls is assessed to determine if the design of controls will detect, prevent, and correct or respond to risks taken.

The following criteria should be utilised when evaluating the adequacy of controls.

Ranking	Category	Adequacy Factor
No controls	Key controls are absent or vague. Prompt corrective action is required. Immediate action is required by management to implement effective controls. The overall system of internal control is materially impaired.	**0%**
Weak	Pervasive weaknesses (Critical) in the control and/or instances of non-compliance (gaps in the treatment)	**20%**
Additional Controls Required	Unsatisfactory controls or significant weakness in the control and/or instances of non-compliance (potential gaps in treatment)	**40%**
Satisfactory	Isolated areas of weakness (Less Significant) and/or instances of non-compliance with internal controls identified (treatment in place adequate with minor improvement required)	**60%**
Good	No significant weaknesses (Housekeeping) in the control and/or insignificant instances of non-compliance identified (No noticeable weakness)	**80%**
Excellent	No weakness (Housekeeping) in the control and no instances of non-compliance identified (No noticeable weakness)	**100%**

10.3 Residual Risk Exposure

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

Controls may reduce the likelihood of occurrence of a potential risk, the impact of such a risk, or both. Residual risk will therefore inform management of the actual level of control effectiveness.

Management may determine a target residual risk level (is a desired optimal level of risk) by defining actions/additional controls to get to a desired level.

Green Within Appetite	Minor	The level of risk is acceptable The risk is within defined risk appetite No further action or additional controls required Risk monitoring is required, and Internal audit may perform effectiveness review
	Moderate	The level of risk is acceptable The risk is within defined risk limits, however existing controls should be considered of adjusted. Risk monitoring is required, and Internal audit may perform effectiveness review
	Material	The risk level is acceptable The risk is within defined risk limits; however, controls should be adjusted, and senior management intervention is required. Escalation required for action to achieve an acceptable level of residual risk.
Defined limit / Appetite		
Risk Appetite Breached but Within Risk Tolerance	Severe	The risk level is not acceptable The risk has breached the risk appetite and approaching the tolerance level High level of controls, senior management intervention required. Immediate escalation required for to executive and board members for deliberation and action. Defined action plan with timeline and monitoring required
Risk Tolerance Breached but Within Risk Bearing Capacity		
Risk Tolerance Breached and Within Risk Bearing Capacity	**Catastrophic**	The risk level is not acceptable The risk level may have detriment consequences to the Group. Immediate escalation to the Executive and Board and shareholders. The risk may impact the risk bearing capacity for the Group
Risk Bearing Capacity		

Phoenix's risk tolerance levels act as a guide to what, how and the extent to which risk is managed.

10.3.1 Targeted Residual Risk Exposure

The targeted residual risk exposure is determined considering the effectiveness of the stated action plans, and their associated impact on the effectiveness of controls once implemented.

10.3.2 Residual Risk Trend

The business should assess the trend of the risk exposure by considering the current risk trend versus the exposure at the last review. This is performed to assess whether the risk exposure has increased, remained stable, or decreased relative to the previous assessment. The following criteria should be used to assess the trend of the residual risk exposure:

Trend	
Stable	↔
Increasing	↑
Decreasing	↓

10.4 Management Action Plans

Management action plans are different to controls, in that the completion of the actions may result in a change to an existing control or the creation of new controls. These controls are assessed for the design adequacy and operational effectiveness as part of the ongoing risk assessment process. Management must ensure that actions are tracked and communicated within the ISO quarterly reviews, and they are fully implemented so that maximum benefit is derived from the process.

Management action plans should be proportional to the risks that they are trying to address and should be generated when:

- A control failure/ weakness has been identified (i.e. the control, when assessed, was inadequate or ineffective).
- A Key Risk Indicator (KRI) is reaching or has breached its limit.
- A risk incident has occurred.
- An audit finding (internal or external) has been reported.
- The residual risk exposure is rated as high, very high, catastrophic

11. Risk Monitoring

The level of risk exposure must be actively monitored against the limits set and/or the capital available. Risk monitoring and review forms an integral part of the risk management process.

The monitoring and review process encompass all aspects of the risk management process for the purposes of:

- Analysing and learning lessons from risks, incidents, changes, and trends,
- Detecting changes in the external and internal environment, including changes to the risk itself which can require revision of risk mitigation strategies and priorities,
- Ensuring that the risk and control treatment measures are effective in both design and operating effectiveness,
- Identifying emerging risks and promulgating risk reassessments, and
- Controls identified not to be effective by other assurance providers might require control redesign or risk assessment to ensure that the risk is mitigated.

Actual progress in implementing risk treatment plans provides a performance measure and is incorporated into the Group's performance management, measurement, and internal and external reporting activities.

11.1 Risk Re-Assessment

Monitoring involves the regular review of what is already present, this can be either periodic or ad hoc, both aspects must be planned. The results of the monitoring process are recorded and will be used as an input to the review of the risk management profile. The risk profile or risk type rating will be re-assessed if it is found to be ineffective when being reviewed by other assurance providers.

Some of the tools and mechanisms used for risk monitoring are Key Indicators and Risk Incidents, which are defined in further detail below.

11.2 Key Indicators

Key indicators play a critical role in the risk management framework. They provide tools for monitoring controls, risk drivers, risk exposures, risk incidents as well as early identification of emerging trends. Where the risk assessments are used to periodically identify risks and controls, key indicators monitor these risks in intervals. Key indicators also provide a means to express risk appetite as they often serve their most practical system in conjunction with a system of limits and boundaries. When a key indicator breaches its associated limit, it triggers a review, escalation, or management action.

Management must ensure that:

- Processes have been established for regular monitoring and updating of the risk profile,
- Adequate measures are in place to enable ongoing monitoring of the internal and external risk environment,
- Key risk information is reported via the governance structures,
- Risk analysis prompts appropriate modifications to the risk management system where necessary, and
- The risk profile is a key input in defining business objectives, policies, risk appetite and the internal control environment.

11.2.1 Lagging Indicators

Lagging indicators follow an event and are usually used to measure business performance against past experience. The benefit of lagging indicators is its ability to confirm that a pattern is occurring or about to occur and measure performance data that is already captured, e.g., returns on investments or a budget to plan variances.

11.2.2 Leading Indicators

Leading indicators change quickly and are generally seen as a precursor to the direction something is going. For example, interest rate changes will impact spending and investments, or aging baby boomers may indicate future stresses on the healthcare system. Because leading indicators come before a trend, they are considered business drivers. Identifying specific, focused leading indicators should be a part of each entity's strategic planning cycle.

11.2.3 Types Of Indicators

Indicators	Description
Key Control Indicator (KCI)	KCI's are measurable metrics that indicate the potential for a control to fail within an organisation. The role of KCI is to ensure that adequate responses and monitoring have been provided for an identified risk
Key Risk Indicator (KRI)	KRI's are metrics which provide early warning signal of the risk exposure. KRI also measuring the likelihood and impact of an event and its consequence will exceed the organization's acceptable threshold, resulting in negative impact to the goals. These act as a timely leading indicator for emerging risks
Key Performance Indicator (KPI)	KPI's enable the organisation to define its performance targets based on its goals as well as monitor its progress towards achieving these targets

11.2.4 Key Risk Indicator Methodology

KRIs facilitate the process of monitoring and controlling of key risks and can be used to support a range of risk management activities and processes including:

- risk identification,
- risk assessments,
- control assessments, and
- risk appetite.

The key attributes of KRIs include:

- Defining current risk levels by providing a measure of the status, of the identified risk and the effectiveness of its control.
- Highlighting trends and changes in risk levels by monitoring changes in risks arising during the risk assessment process.
- Provide early warning signals through predictive risk indicators which highlight changes in the risk environment, control effectiveness and risks before they materialise and result in loss or other exposure.

When creating KRIs, a risk-based approach must be followed. The number of indicators should be considered including the size, complexity and nature of the business, department, or team.

By monitoring a set of KRIs, and by examining their actual values and trends against agreed limits, it is easier to assess whether the risk exposure remains within the defined risk tolerance.

a) Identify metrics

KRIs are created, where necessary, as a direct output of a risk assessment and used to monitor key risks and risk incident experiences.

The first step in the KRI process is to identify existing metrics for all residually high risks.

To ensure efficient tracking, a KRI owner is identified and the frequency of the data to be produced is articulated. The KRI owner ensures that the objective of the KRI is clearly understood and documented in relation to the risk which is being monitored.

An entity should establish new or additional KRI's to identify new metrics, where the existing metrics are not suitable or inadequate.

b) Determine risk limits/thresholds

Once the list of KRIs have been established, risk limits, boundaries and tracking frequencies are set. The concept of a risk limit is to establish boundaries that, when exceeded, management will be notified of a significant change in the risk exposure. Therefore, defined risk limits provide management with the ability to identify areas within business where the level of risk may become unacceptable. KRIs are assessed against a set of predefined risk limits which is aligned with the risk appetite and tolerance framework defined.

c) Design a dashboard/report

The KRI dashboard should be designed to report on critical metrics to the entity's senior management and Exco. The dashboard can be useful on a standalone basis or as part of another management process. The dashboards generally include graphs and tables to provide concise and comprehensive risk picture highlighting KRIs that are approaching or have breached the defined risk limits. The dashboard should also include actions taken to bring the risk exposure within the defined limits.

d) Define action plans

Action plans are defined when a KRI is approaching or has breached a risk limit. Senior management should focus on monitoring the KRIs related to these action plans, especially those KRIs that have consistently breached the limit for over 3 months.

12. Risk Incidents

An incident is an event that has occurred which may result from a failure of people, processes, systems, or external events that gave rise to one or more losses, accidental gains or near misses. An incident may occur due no control being put in place or failed controls. This often has the potential to cause, an adverse financial and/or non-financial impact (e.g., reputational, regulatory, operational, or legal). For more detail refer to Phoenix Risk Management Policy. Risk incidents that have breached the risk appetite and tolerance limits must be reported as per the escalation matrix.

13. Stress and Scenario Analysis

The resilience of the business to risk incidents must be tested under both normal and stressed conditions, including developing an understanding of the severity of an incident that would cause the business to breach its risk appetite and tolerance limits.

For the purposes of stress and scenario analysis the following terminology is defined:

- **Stress test** – A stress test is a severe change in a single risk factor or a limited number of risk factors. It is typically conducted over a short time horizon, for example an instantaneous shock.
- **Scenario analysis** - Scenario analysis uses a hypothetical future or relevant historical state of the world to define changes in risk factors. This will normally involve changes in several risk factors, as well as the ripple effects and other impacts that follow logically from these changes and related management actions. Scenario testing is typically conducted over the time horizon appropriate for the business plan and risks being tested.
- **Reverse stress test** - A reverse stress test considers a scenario that could challenge the viability of the Group. A reverse stress test typically starts with a specified outcome that challenges the viability of the Group.

13.1 Stress And Scenario Exercises

On an annual basis, each entity is required to perform the following:

- **A Stress Test Exercise** – This involves evaluating a range of stresses to the business. This exercise will typically inform management of the key risk exposures and assist to validate the risk management process and capital models.
- **A Scenario Analysis Exercise** – This involves identifying and evaluating a small number (e.g. 2 or 3) of plausible adverse scenarios to the business plan. This exercise will typically be used to inform the robustness and vulnerabilities of the business plan.
- **A Reverse Stress Test Exercise** – This involves specifying when the business's viability is challenged and through identifying a relevant scenario. This exercise will typically be used to inform the range of possible management actions in an extreme scenario.

Within each entity management may appoint a senior person who would be accountable for the execution of the Stress and Scenario Exercises.

The results of the Stress and Scenario Exercises (and other documentation as required) will be submitted to Phoenix's Enterprise Risk Management Function for review and challenge.

13.2 Evaluating Stress and Scenarios

When undertaking a Stress and Scenario Exercise, consideration should be given to the current and projected (as appropriate) impact in the stress or scenario on the following (if relevant):

- Profit and loss and balance sheet
- Net present value of future profits
- Net assets
- Net current liquid assets
- Likely cash flow impacts
- Risk profile in the context of the risk appetite/risk methodology

13.3 Documentation

Adequate documentation should be maintained for each Stress and Scenario Exercise. This should include as a minimum the:

- Key assumptions and methodology used in the identification, selection, parameterisation and evaluation of a stress or scenario.
- Results of the Stress or Scenario Exercise

For the Scenario Analysis Exercise, Reverse Stress Test Exercise and Stress Test Exercise, the following additional information should be documented each time:

- The rationale for the scenario selection
- The scenario narrative, including the timing and interaction of risks
- Management actions assumed in the evaluation of the scenario

14. Risk Reporting

Risk reporting must be accurate, relevant, and timely to support the management of risks, meet the needs of all relevant internal and external stakeholders and, where required, meet the specific reporting needs of separate legal entities.

The risk reporting process enables the effective monitoring and reporting of risk and capital management issues across the Group and provides assurance that the ERM framework is operating as intended.

The risk monitoring and reporting processes are a critical factor in ensuring that the business proactively prevents risk incidents from occurring and implements corrective actions should a risk materialise.

Risk information obtained through various risk reporting processes must be validated.

All subsidiaries should ensure that all risks are identified and reported in time to the Phoenix Enterprise Risk Management Function.

All the subsidiaries are required to escalate all risk outside of appetite monthly to Phoenix Enterprise Risk Management Function.

Phoenix Enterprise Risk Management Function is responsible for risk aggregating in order to have a holistic view of the business risk exposures. This assists in ensuring that the business risk exposures remain within the specified appetite and tolerance levels. Phoenix Enterprise Risk Management Function is required to produce a 6 monthly consolidated risk report for the Phoenix Software Board Meetings.

Reporting of risk information will take place on an on-going basis as summarised below:

	Group Enterprise Risk Management	Subsidiary Risk Management
BTG Board of Directors	Every 6 months - Risk Report	-
Group Risk Committee	Quarterly Risk Report	-
Executive Committee	Quarterly Risk Report	Monthly Risk Report
Enterprise Risk Management Function	-	Monthly (risk outside of appetite)

The risk reporting process assists with strategic business decision making, facilitates risk challenge, and provides assurance that the risk framework and the risk and capital integration process are working effectively.

14.1 Risk Profile

This report is designed to provide its intended readers, the Board, and the Risk Committee, with sufficient oversight of the business's ERM Framework and risk exposures. Key components of the report include, but are not limited to:

- Overall ratings of each risk type for with detailed commentary for those risk types that have changed since the last rating.
- The principal risks faced by the business and its ratings, with further detail of rating rationale, and remedial actions for all high residual risk exposures. Details of all risks that have moved into, out of, or within the "High" and above risk rating.
- All high impact entity specific projects as well as cross company projects which have a significant impact to the business.
- Lastly, the report includes risk incidents reported to the Phoenix Enterprise Risk Management Function since the previous report.

Phoenix Enterprise Risk Management Function supports the requirement for the Group to have a holistic view of the Group's risk exposures. This assists in ensuring that the Group risk exposures remain within the specified appetite and tolerance levels.

15. Framework Governance

15.1 Framework Ownership

The Group CFO is the owner of this framework.

The framework shall be reviewed when changes are required, but at minimum on an annual basis.

New frameworks and changes to current frameworks will follow the Board approved “GRCS Policy Review Process”

16. Reference Policies and Guides

The following policies, guidelines, laws, regulations, and standards directly or indirectly impact this framework, and would need to be consulted as required:

- Enterprise Risk Management Framework
- UK Corporate Governance Code
- COSO Risk Management Framework (Committee of the Sponsoring Organisations of the Tredway Commission)
- Risk Management Standard ISO 31000
- The Companies Act, of 2006.

17. Definitions

TERM	DEFINITION OF TERM
BTG (or Group)	Bytes Technology Group , its divisions and subsidiaries, associate companies, entities that Phoenix has acquired or merged with, as well as entities in which the Phoenix has a controlling interest.
Board	Refers to the Board of directors within Phoenix Software Ltd
Consequence	That which follows from the occurrence of a risk, which results in a loss or gain. Also known as an impact.
Contractor	Refers to a natural person, business, or corporation that provides goods or services to the Group under terms specified in a contract.
Controls	Controls include, but are not limited to, any process, policy, device, practice, or other conditions and/or actions which maintain and/or modify risks.
Employee	Employee shall mean all permanent, contract and temporary employees appointed by Phoenix, its subsidiaries, divisions, and associate companies.
Event	An event can have one or more occurrences and can have several causes and several consequences/impacts.
Enterprise Risk Management	Refer to the Phoenix’s Enterprise Risk Management team that is responsible for oversight and facilitation of the risk management programme.

Impact	The magnitude of the potential risk or the outcome of an event/risk, expressed in a qualitative or quantitative manner. This can be seen as a positive or negative impact.
Inherent risk rating	The likelihood of the risk occurring and the severity of the impact if it does occur without considering the effectiveness of controls. This is the worst-case scenario, in the event that there are no controls in place, or the controls fail to take effect during a risk event.
Likelihood	A measure of probability or frequency. The frequency is a measure of the rate of occurrence of an event expressed as the number of occurrences of an event in a given time.
Management	Refers to a team of individuals at the highest level of management of an organisation who have the day-to-day tasks of managing that organisation.
Risk	Any uncertainty to a future event that might occur and have a positive or negative impact to a defined objective.
Risk Appetite (RA)	The level of risk the Group is willing to take in pursuit of its strategy, as defined by • the BTG Board (who approves the strategy and governs risks that threaten its achievement); and • the Phoenix Executives (who develop the strategy and are responsible for its successful implementation).
Risk Appetite Framework (RAF)	The framework that – • outlines BTG's specific risk appetite and risk tolerance levels as well as risk bearing capacity; and • articulates Phoenix's risk response, escalation, and reporting protocols to respond to risks that may affect the setting and achievement of its strategy and sustainability.
Risk Bearing Capacity (RBC)	The maximum level of risk that Phoenix can withstand, beyond which the Phoenix's status as a going concern and/or Phoenix's sustainable existence is under threat, i.e., the level at which shareholders and/or stakeholders are no longer willing and/or able to accept our existence.
Risk Tolerance (RT)	The level of risk Phoenix can take (even if implementation of the strategy may be affected), while Phoenix is able to exist for the purpose as defined by – • BTG's shareholders in the Company Memorandum of Incorporation (including performance); and • other relevant stakeholders, such as *inter alia* – ○ regulators, who determine the licencing conditions under which the Group operates. ○ customers, who agrees to buy Phoenix's products and services at sustainable levels; and ○ communities in which Phoenix operate, who grant our social licence to operate.
Risk management	It is coordinated activities to direct and control an organisation regarding risk
Risk owner	The managing of risk rests with the senior and line manager
Residual risk rating	The likelihood of the risk occurring and the severity of the impact if it does occur, this time taking into consideration the preventive and corrective controls.
Target residual risk	The level of acceptable risk that is desired. Action plans once implemented should improve the level of residual risk to the target level.

Version Control

Author	Version	Date	Description
Andrew Holden and Clare Metcalfe	1.0	19/10/2022	Original Document

Document Approval

Name	Version	Date	Position
Clare Metcalfe	1.0	21/10/2022	Operations Director

Signed: Clare Metcalfe Clare Metcalfe, Operations Director

Dated: 21/10/2022