Risk Management Policy

PHX029

Contents

Confidential Confidential Confidential

Please treat this information as private and confidential.

1. Document Control

1.1 Purpose of this Policy

To document and standardise the approach to risk management.

1.2 Scope

Applicable to all business, information, cyber and technical security processes within Phoenix and should be used as the overarching policy and procedure for risk management processes and risk acceptance criteria.

2. Policy Statement

2.1 Risk Management

Phoenix identifies, assesses, and mitigates risks where appropriate in relation to financial, strategic, operational, and technical risks, including monitoring and tracking risk mitigations and controls to ensure appropriate and proportionate to the identified risk throughout changing threat landscapes. The ERM Framework is governed by the Bytes Technology Board.

Risks are identified through day-to-day business activities; planning; monitoring; committee discussions and through the incidents and events. Identified risks must be escalated to the Senior Management Team or the Governance Manager for appropriate assessment.

Having regard for risk is the responsibility of all employees in course of carrying out their duties. The Senior Management Team have the accountability of managing risk within their work areas as subject matter experts.

It is the responsibility of the Governance team to ensure risk is appropriately assessed, reviewed, monitored, and managed through the risk and internal audit functions.

2.2 Risk Assessment

Risk Assessments identify the risks applicable to the company; probability these may occur; the impact of a realized risk and any mitigation action required to manage the risk. Risks are assessed by way of 5 x 5 risk analysis with assigned owners.

Please treat this information as private and confidential.

			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

The impact measurement of risk is determined by considerations such health and safety; legal obligations; cyber risk; business continuity risk; supplier and subcontractor risk; and the financial impact as a percentage of Annual Operating Profit.

An escalation route appropriate to risk scoring is in place to ensure proportionate response from the Senior Management Team to the Bytes Technology Board

The full Phoenix Risk Management Framework is set out in PHX021 Enterprise Risk Management Framework.

Confidential

Please treat this information as private and confidential.

Version Control

Author	Version	Date	Description
ISC	1.0	July 2015	Original Document
ISC	2.0	September 2018	Amended following annual review
ISC	3.0	November 2019	Amended following annual review
ISC	4.0	April 2020	Inclusion of ISO 14001 and ISO 20000 requirements
ISC	4.0	May 2021	Annual review – no changes
ISC	5.0	June 2021	Update to reflect holistic business approach to Risk. Alignment with Bytes.
ISC	6.0	01/02/2023	Update to align with ERM Framework

Document Approval

Name	Version	Date	Position
Sam Mudd	1.0	July 2015	Managing Director
ISC	2.0	September 2018	Information Security Committee
ISC	3.0	November 2019	Information Security Committee
ISC	4.0	April 2020	Information Security Committee
ISC	5.0	June 2021	Information Security Committee
Clare Metcalfe	6.0	February 2023	Operations Director

Signed:  Clare Metcalfe, Operations Director

Dated: 01/02/2023

Confidential Confidential Confidential

Please treat this information as private and confidential.