Group Risk Management Policy

CountPlus Limited (ACN 126 990 832)
As adopted by the Board

Revised as at June 2022

1. Introduction

1.1 This Group Risk Management Policy describes the CountPlus (Company) risk management framework with respect to the operation of the Company, comprised of the head entity CountPlus Limited; and its subsidiary companies (within the meaning of section 46 of the Corporations Act) and non-subsidiary companies in which it has an equity interest and into which each party has entered into a Shareholders' Agreement (each a Partner Firm).

1.2 The Company is committed to ensuring that effective risk management is embedded throughout the Company and its Partner Firms as an integral part of its organisational culture, its business operations, and a core Board and management responsibility. Effective risk management allows the Company and its Partner Firms to take full advantage of business opportunities through informed decision making based on a rigorous assessment of risks and benefits. Further, risk management considerations are incorporated into planning, approval and implementation of new products, services, business processes and systems, acquisitions and outsourcing arrangements.

1.3 CountPlus is committed to continuously improving its risk management practices and ensuring that its monitoring and reporting processes allow the early identification of new risks. It seeks to anticipate and minimise risks before they occur and is committed to fully investigating any unexpected consequences from risk exposures.

1.4 CountPlus recognises that risk is an essential part of doing business and that managing risk appropriately is critical to its immediate and future success.

1.5 CountPlus has implemented an Enterprise Risk Management Solution (ERMS) which systematises risk management practices allowing Partner Firms to manage and monitor their own risks, while providing consolidated risk information to Management and Board.

1.6 This Policy is based upon AS/NZS ISO 31000:2018 Risk Management – Guidelines and relates to all risk management activities conducted in the Group.

2. Policy Statement

2.1 The Board of Directors of the Company (Board) is committed to ensuring the effectiveness of the risk management framework and that risks are adequately and appropriately addressed in a timely manner. To meet this commitment, risk is to be everyone's business. All employees are required to be responsible and accountable for managing risk in so far as is reasonably practicable within their area of responsibility.

2.2 This Policy must be adhered to at all times. Partner Firms are required to adopt this Policy and Framework subject to such adaptation as is required, taking into account their business functions.

3. Policy Principles

3.1 CountPlus is committed to the following risk management principles as detailed in AS/NZS ISO 31000:2018:

(a) **Integrated** - risk management is an integral part of all organisational activities.

(b) **Structured and comprehensive** - structured and comprehensive approach to risk management contributes to consistent and comparable results.

(c) **Customised** – the risk management framework and processes are customised and proportionate to the organisation's external and internal context related to its objectives.

(d) **Inclusive** - appropriate and timely involvement of stakeholders enables their knowledge, views and perceptions to be considered. This results in improved awareness and informed risk management.

(e) **Dynamic** – risks can emerge, change or disappear as an organisation's external and internal context changes. Risk management anticipates, detects, acknowledges and responds to those changes and events in an appropriate and timely manner.

(f) **Best available information** – the inputs to risk management are based on historical and current information, as well as on future expectations. Risk management explicitly takes into account any limitations and uncertainties associated with such information and expectations. Information should be timely, clear and available to relevant stakeholders.

4. Risk Management Framework

4.1 Essential elements of the Risk Management Framework are:

(a) Group Risk Management Policy;

(b) Risk Appetite and tolerances;

(c) Risk Management Methodology;

(d) Risk Management Plan and Risk Registers (contained within the ERMS);

(e) Clear roles and responsibilities for:

i. The Board;

ii. Chief Executive Officer;

iii. Partner Firms;

iv. Partner Firm Boards

v. Audit and Risk Committee;

vi. Management; and

vii. All Employees.

(f) Risk management methodology and procedures;

(g) Company policies and procedures aligned with relevant compliance obligations and incorporating appropriate risk management controls;

(h) Risk management training and awareness program (including where relevant, Continuous Professional Development ("CPD");

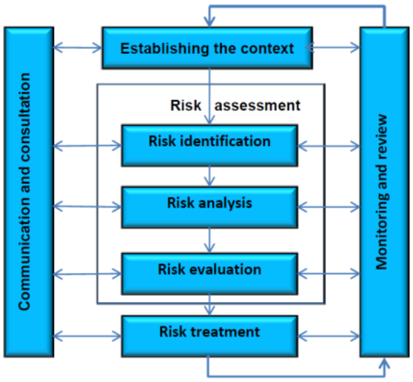
(i) Risk management incorporated into all personnel and Partner Firms' KPI's;

(j) Risk monitoring program including controls self-assessment program, independent assurance testing, and alignment with compliance monitoring program; and

(k) Risk and compliance incident and breach reporting, assessment and rectification process.

5. Risk Management Methodology

5.1 The key elements of the Risk Management Methodology are based on AS/NZS ISO 31000:2018 and are summarised below:



6. Organisational Context

6.1 CountPlus is an aggregation of Partner Firms and their subsidiaries across Australia. Risk to CountPlus is mitigated by the fact that its Partner Firms operate independently and are geographically diversified. As such, a risk event faced by one Partner Firm is generally not expected to have a significant impact on the Group as a whole. However, a material risk event may have a significant reputational impact on the Group and therefore each Partner Firm must always manage its risks in a way that minimises the likelihood that it may damage the reputation of the Group as a whole.

7. Legislative Context

7.1 In addition to CountPlus meeting high standards in the management of risks, there are legal and regulatory obligations regarding risk management including:

(a) *Corporations Act 2001 section 912A(1)(h)* which requires all holders of an Australian Financial Services Licence to have adequate risk management systems in place;

(b) *ASX Corporate Governance Principles and Recommendations* require listed entities to establish a sound risk management framework and periodically review the effectiveness of that framework (see Principle 7);

(c) *ASIC Regulatory Guide 104* which provides guidance on how AFSL licensees should meet their general obligations as set out in section 912A(1) of the Corporations Act;

(d) *APES 325 Risk Management for Firms* which requires members who are principals in firms to implement, document and monitor a risk management framework.

8. Risk Categories

8.1 The Board has identified the following risk categories as being applicable to the Company and Partner Firms:

(a) **Operational Risk** – covers a vast number of business areas and can include issues such as business processes and controls, service delivery, document management, physical security and overall business continuity. Business continuity is the ability of an organisation to maintain essential functions during as well as after a serious incident disaster has occurred and the organisations ability to resume normal operations within a reasonably short period. The organisation also needs to recognise the need to ensure that personnel and assets are protected.

(b) **Regulatory and Compliance Risk** – is exposure to legal penalties, financial forfeiture and material loss an organisation faces when it fails to act in accordance with industry laws and regulations, internal policies and/or prescribed best practices. This may include codes of conduct and member organisations' standards of practice (e.g. CAANZ,CPA, or via an AFSL).

(c) **Financial Risk** – refers to the Company's ability to maintain solvency at all times and to meet the financial requirements of an Australian Financial Service Licence. It also addresses the risks faced by the Company in failing to adequately plan its business operations resulting in revenue loss.

(d) **Governance Risk** – Governance is the ethical management of a company by its Board, executives and management through the establishment of policies and the continuous monitoring or the proper implementation by the members of a governing body. It is the system by which an organisation is controlled and operates, and the mechanism by which it and its people are held to account. Governance risk is the risk of not having a regulatory and compliance management system in place (and oversight of this system) that covers both ethics and regulatory issues.

(e) **Information Technology Risk** – is any risk related to information technology that can cause adverse impacts on the organisation's business processes. This can include but is not limited to; hardware and software failure, human error, spam, viruses and malicious attacks.

(f) **Mergers and Acquisitions** – a combination of Investment and Transaction risk and derived from a number of sources, including market risk (e.g. equity, interest rate and foreign exchange risk), credit risk, counterparty risk and investment concentration risk. Credit exposures can increase the risk profile of a Partner Firm and adversely affect its financial viability. Credit exposure in this context includes both on-balance sheet and off-balance sheet exposures (including guarantees, derivative financial instruments and performance related obligations) to single and related counterparties.

(g) **Complaints and Client Risk** – matters such as litigation involving the Company and a client can affect the ability to attain adequate insurance coverage and increase insurance premiums. Inadequate handling of client complaints can significantly impact business reputation and client referral business that is detailed in the separate risk of Contagion and Reputation.

(h) **People and Culture Risk** – refers to the issues impacting the Company's employees and culture. Culture is the sum of the shared values and behaviours including the Company's people as they relate to various dimensions such as risk. Culture is a key determinant in the performance of an organisation and its capacity to achieve its own objectives. Some key risk indicators will include issues such as WHS, staff retention, ethics, training, development and onboarding.

(i) **Contagion and Reputation Risk** – this is a risk of possible damage to the Company's or Partner Firm's brand and reputation and the associated risk to earnings, capital or liquidity from any association, action or inaction which could be perceived by stakeholders to be inappropriate, unethical or inconsistent with the Company's values and beliefs.

(j) **Strategic Risk** – Strategic risk arises where the current and future direction of the Company or any of the Partner Firms is not well planned, leading to loss of competitive advantage and market share. Risk of loss of earnings and/or capital could arise from poor business decisions or improper strategic implementations. Strategic risk may be high when there is misalignment of organisational goals, decisions, deployment of resources and strategic implementation.

(k) **Fraud and Corruption Risk** – can arise from dishonest or fraudulent behaviour and the Company takes a very serious approach to cases, or suspected cases, of fraud or corruption perpetrated by staff and Partner Firms.

(l) **Supplier Risk** – refers to the risks associated with reliance on third party suppliers for the delivery of business-critical services, advice and systems.

9. Risk Appetite Statement

9.1 The CountPlus appetite for risk and relevant risk tolerances are approved by the Board annually and are set out in the Risk Appetite Statement ("RAS"). Partner Firms are required to operate within this RAS however may set their own Partner Firm RAS providing it does not exceed the parameters of the CountPlus RAS.

9.2 CountPlus accepts that taking risks is a fundamental part of being a provider of accounting and financial planning services. To that end it will tolerate a level of risk that allows it to exploit commercial opportunities and maximise the returns to its shareholders while not:

(a) prejudicing its abilities or those of its Partner Firms, to provide its services within the highly regulated environment in which it operates;

(b) prejudicing its reputation; and

(c) prejudicing its capacity to absorb costs and its ability to deal with third parties.

9.3 Specifically, CountPlus has no tolerance for:

(a) fraud or deliberately dishonest or unethical behaviour;

(b) the provision of any accounting services, financial product advice or conduct of any dealing that is not in the best interest of a client and that is not appropriate to the needs of any client; and

(c) acceptance of risk where there is a high likelihood of jeopardising CountPlus' continuing ASX listing, its financial stability, and the continuity of services, and where reasonable and cost-effective measures will not reduce the risk to acceptable levels.

10. Risk Management Plan and Risk Registers

10.1 The Company and each Partner Firm must maintain Risk Management Plans and Risk Registers which will enable the effective identification, assessment, treating, monitoring and communication of risks, and to develop a residual risk profile of the Company and each Partner Firm.

10.2 The ERMS is provided to Partner Firms as the sole repository of Risk Management information. Associate Firms that choose not to use the Company ERMS must provide the Company with a copy of their Risk Register on a monthly basis to allow consolidated Risk reporting at a Group level.

10.3 The ERMS includes all the key elements for Risk Management including:

a) Risk Registers

b) Control Libraries

c) Risk Rating matrices

d) Email Notifications

e) Reporting and dashboards

In addition, the ERMS includes Incident/Breach and Complaints registers that provides the Partner Firms with a structured and automated process for capturing, managing and reporting.

11. Policy, Risk Appetite Statement and Framework Review and Reporting

11.1 The CEO must review this Policy annually to ensure it provides an adequate framework to monitor the operating circumstances, which may change from time to time, that may impact on the risk profile of the Company.

11.2 An annual review of the RAS is to be conducted by the Board, which will include the Board's consideration for its approval of any management recommendations to change the RAS.

11.3 The Partner Firms should review their risks on a regular basis (at least annually) or after any significant business event or risk incident, with the Risk Owners providing updates on the effectiveness of controls and other mitigations.

11.4 The Partner Firm Boards should include Risk Management as a standing Agenda item, with the Partner Firm providing updates to its Board from the ERMS.

11.5 A consolidated Risk Report will be tabled at every CountPlus Audit and Risk Committee meeting.

11.6 The Partner Firm is to immediately inform the Partner Firm Board and the Company of the following:

(a) Any Inherent Risk which receives a score of 15 or above in the Risk Matrix (Red);

(b) What controls and mitigations have been put in place; and

(c) The resulting Residual Risk rating.

11.7 It should be emphasised that the Risk Register is a dynamic tool and must be subject to continuous monitoring including for new risks, changes to risks, and effectiveness of the risk controls.

12. Continuous Risk Controls Monitoring and Reporting

12.1 The Company and Partner Firms are to administer a continuous risk controls monitoring and reporting program. That may consist of controls self-assessment programs, thematic risk reviews, and independent risk assurance reviews. The Company will provide guidance and, where appropriate, support such as templates and software solutions.

12.2 Independent risk assurance reviews might be conducted by internal audit or external risk specialists. It is recommended that the frequency of such monitoring will be a function of the last rated residual risk status for each risk, thus allowing for dynamic 'just in time' approach to allocating risk resources to monitoring tasks.

12.3 Where compliance monitoring and reporting are conducted separately, such as where Partner Firms operate under a third party AFSL, copies of any reports on the effectiveness of compliance management, etc. should be attached to the controls in the ERMS.

12.4 The results of controls monitoring are to be reported at each of the Partner Firm Board meetings.

13. Reporting and management of Risk Incidents (including where relevant, compliance breaches)

13.1 Risk incidents and breaches should be captured, monitored and reported via the ERMS Incident/Breach register. This register is structured to ensure that there is visibility over all incidents, with outstanding incidents being escalated as necessary.

13.2 Where a risk involves an actual or a potential compliance breach the Partner Firm should also record the breach in the ERMS Incident/Breach register and escalate it as necessary.

13.3 The ERMS Incident/Breach register sets out the requirements and procedures for the identification, reporting and ongoing management of incidents and breaches. This covers both compliance and risk management events.

13.4 The primary purpose of using the ERMS is to provide a consistent, rigorous and structured avenue for all personnel to raise any issues for treatment. In other words, reporting is a 'call for help'. It is also important to note that disciplinary action may follow where there has been deliberate or inappropriate behaviour leading to the incident or breach.

13.5 Reporting of all incidents and breaches should be provided to each Partner Firm's Board. Summary reports will also be provided to the CountPlus Audit and Risk Committee as deemed necessary.

14. Good Faith Reporting and Whistleblowing

14.1 In extreme circumstances an individual may be concerned that a serious breach has occurred but be in a position where he or she believes it would be personally damaging to pursue it through normal channels. For instance, they may have come into possession of information that indicates their manager or a close working colleague has knowingly caused a breach or suppressed the reporting of a breach. In such circumstances the individual should contact the 'Good Faith Reporting Manager', who will do all that is possible and practicable to deal with the matter in a way that protects the confidentiality of the person making the report.

14.2 Should the reporting individual subsequently be found to have been knowingly involved in the breach, the fact that they reported it will not protect them from subsequent action. However, the fact that the individual initiated the report may be taken into consideration in assessing disciplinary action.

14.3 The *Corporations Act* also protects certain whistleblowing activities and protects whistleblowers from persecution (see ss 1317AA – 1317AE). These protections are designed to encourage people within companies, or with special connections to companies, to alert ASIC and other authorities to illegal behaviour. To see how to whistleblow to ASIC and to do so in a way that ensures the protections that will be provided, see the information sheet on whistleblowing on ASIC's website: https://asic.gov.au/about-asic/asic-investigations-and-enforcement/whistleblowing/guidance-for-whistleblowers/

15. Communication and Reporting

15.1 Risk Management will be a standing agenda item at all Partner Firm Board and CountPlus Audit and Risk Committee meetings.

15.2 Partner Firms should ensure that all significant risks are notified to their Board and the CountPlus Audit and Risk Committee.

16. Roles and Responsibilities

16.1 **The Board** is responsible for the oversight of Risk Management within the CountPlus Group. It retains responsibility for assessing the effectiveness of the Company's systems for management of material business risks. That includes:

(a) reviewing and approving the Group Risk Management Policy and Framework and assessing the effectiveness of the Company's systems of risk management and internal control;

(b) approving the RAS, and any management recommendations to amend it, and risk tolerances; and

(c) understanding and monitoring the status of the significant risks facing the Company and Partner Firms.

16.2 **Chief Executive Officer** is responsible for ensuring the adequacy of risk management resources and for maintaining the risk management procedures that will assure the Board that major business risks are managed appropriately which includes:

(a) developing and implementing a Group Risk Management Policy and Framework to manage the Company's business risks;

(b) undertaking annually (as a minimum) a formal risk assessment which includes reviewing and updating the Company's Risk Management Plan and Risk Register;

(c) regular reporting to the Board and the Audit and Risk Committee on how effectively the organisation is managing its business risks; and

(d) providing leadership in respect to an effective risk culture.

16.3 **Partner Firms** are responsible for implementing and monitoring the ERMS, and embedding Risk

Management processes in the day to day operations of their business including:

(a) allocating responsibility for the Risk Management process to a senior member of the Firm;

(b) ensuring systems and processes to manage risk are operating effectively in accordance with the Group Risk Management Policy and the Group RAS;

(c) regular reporting to their Board and the CountPlus Audit and Risk Committee on how effectively they are managing their business risks;

d) undertaking annually (as a minimum) a formal risk assessment which includes reviewing and updating the Partner Firm Risk Register;

(e) ensuring responsibility for Risk Management is included in all Managerial Position Descriptions and that Managers' Performance Reviews include KPI's for Risk Management; and

(f) ensuring the staff with Risk Management responsibilities receive the appropriate Risk Management training.

16.4 The **Audit and Risk Committee** assists the Board in discharging its responsibilities (as detailed in the Audit and Risk Committee Charter) by:

(a) reviewing and reporting on the efficiency, effectiveness and appropriateness of the Company's Risk Management Policy and Framework;

(b) monitoring and advising the Board on matters as they relate to risk management; and

(c) reviewing and assessing the appropriateness of the management of material risk incidents.

16.5 The **Partner Firm Board** is responsible for oversight of Risk Management within the Partner Firm including:

(a) understanding and monitoring the status of the significant risks facing the Partner Firm;

(b) reviewing the efficiency, effectiveness and appropriateness of the internal controls and risk mitigations; and

(c) escalating matters as appropriate to the CountPlus Board.

16.6 **Management** – all managers are accountable for day to day risk management in all activities and business processes within their area of responsibility. They are accountable to ensure all personnel are adequately competent, trained and equipped to perform their functions in a risk aware manner. They are accountable to ensure all processes and procedures are fit for purpose. They are accountable for the identification, reporting and appropriate management of risk incidents.

16.7 **Employees** – all employees, Authorised Representatives and contractors who act for or on behalf of CountPlus or a Partner Firm, are responsible to carry out their duties with due care and diligence; to know and apply risk controls pertaining to their functions; and to report all risk incidents and/or issues immediately upon discovery.

17. Risk Assessment and Evaluation Methodologies

17.1 The following risk assessment and evaluation methodologies and 'tools' are used in assessing the risk ratings and evaluating control effectiveness:

Attachment 1.a – Assessment Criteria Risk CountPlus (Consequence) - to be referred to in assessing the Company risks, risk incidents and breaches.

Attachment 1.b – Assessment Criteria Risk Partner Firms (Consequence) – to be referred to in assessing the Partner Firms' risks and of risk incidents and breaches.

Attachment 2 – Assessment Criteria Risk Likelihood

Attachment 3 – Risk Matrix (Inherent Risk) – the risk rating before the application of controls.

Attachment 4 – Assessment Criteria (Control Activity) – the criteria for assessing the effectiveness of a control activity.

Attachment 5 – Risk Matrix (Residual Risk) – the risk rating adjusted for the effectiveness of the Control Activity.

Attachment 6 – Risk Treatment Options – description of theoretical risk treatment options to assist management in determining optimal actions

Document control

Document number:	05
Effective from:	7 June 2022
Date approved:	7 June 2022
Approved by:	The Board
Last review date(s):	May 2022

ATTACHMENT 1.a

Assessment Criteria - CountPlus (Consequence)

Consequence									
Rating	**Impact**	**EBIT**	**Loss of Market Value**	**Operational**	**Compliance**	**WHS/Person**	**Reputational**	**Market Share**	**Strategy**
Catastrophic	Objectives not achieved	>50%	>50%	Inability to continue normal business operations across 4 or more Partner Firms	Regulatory sanctions Class Action	Potential Loss of Life situation	Loss of confidence in all stakeholder groups	Potentially irrecoverable (i.e.> 24 months)	Potential acquisition or bankruptcy
Major	Material Impact	30%-50%	<50%	Inability to continue normal business operations across 3 or more Partner Firms	Regulatory fines Large legal liability	Potential Hospitalisatio n situation	Loss of confidence by 3 or more stakeholder groups	Long term recovery (i.e.< 12-24 months)	2 or more changes in leadership Financial restructuring Significant change to strategy
Moderate	Noticeable impact	15%-30%	<25%	Inability to continue normal business operations across 2 or more Partner Firms	Investigation Legal reserves established	Potential to involve a Doctor visit	Loss of confidence by 2 or more stakeholder groups	Mid-term recovery (i.e.< 6-12 months)	1 or more changes in leadership Financial restructuring Significant change to strategy
Minor	Some impact	5%-15%	<10%	Inability to continue normal business operations across 1 or more Partner Firms	Regulatory attention Minimal liabilities	Potential First Aid situation	Loss of confidence by 1 or more stakeholder groups	Short term recovery (i.e.< 6 months)	Refinements or adjustment to operating plans and execution
Insignificant	Not visible	<5%	<5%	Limited interruption in 1 Partner Firm	Limited liability or Regulatory impact	No injury potential	Limited impact on 1 stakeholder group	Limited recovery (i.e.< 3 months)	Limited adjustment necessary

Assessment Criteria - Partner Firms (Consequence)

Consequence								
Rating	**Impact**	**EBIT**	**Operations**	**Compliance**	**WHS/Person**	**Reputational**	**Mgt Effort**	**Market Share**
Catastrophic	Objectives not achieved	>50%	Inability to operate	Regulatory sanctions	Potential Loss of Life situation	State / social media attention	Sustained MP/Board involvement	5+ clients lost 24-36 mths recovery
Major	Material Impact	30%-50%	Significant interruptions	Regulatory fines	Potential Hospitalisation situation	Regional / social media attention	Sustained MP/Snr Mgt involvement	4 clients lost 12-24 mths recovery
Moderate	Noticeable impact	15%-30%	Noticeable interruptions	Investigation	Potential to involve a Doctor visit	Local / social media attention	Moderate Snr Mgt effort and MP involved	3 clients lost 6-12 mths recovery
Minor	Some impact	5%-15%	Minor interruptions	Regulatory attention	Potential First Aid situation	Local media attention	Absorbed in BAU Snr Mgt involved	2 clients lost <6 mths recovery
Insignificant	Not visible	<5%	Insignificant interruptions	Limited Regulatory impact	No injury potential	No media attention	Absorbed in BAU no Snr Mgt effort	1 clients lost <3 mths recovery

ATTACHMENT 2

Assessment Criteria
(Likelihood)

Likelihood	
Rating	**Frequency**
Almost Certain	Several times a year
Likely	Once a year
Possible	Every few years
Unlikely	Once in 5 years
Rare	Once in 10 years

ATTACHMENT 3

RISK MATRIX (Inherent Risk)

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

Risk Rating
Low
Medium
High
Extreme

Assessment Criteria (Control Activity)

Consequence			
Rating	**Action**	**Risk**	**Control Effectiveness**
None	Critical improvement opportunity	Extreme Risk - Board intervention required	Controls do not exist
Weak	Significant improvement opportunity	High Risk - Senior Management attention required	No guarantee risks will be controlled
Needs Improvement	Moderate improvement opportunity	Medium Risk - Management needs to address improvements	Controls only address basic risks
Satisfactory	Limited improvement opportunity	Low Risk - limited improvement opportunities	Controls can be relied upon in most circumstances
Effective	Effective	Low Risk - manage through routine procedures	Controls can be relied upon

RISK MATRIX (Residual Risk)

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

Risk Rating
Low
Medium
High
Extreme

Risk Treatment Options

Depending on the type and nature of the risk, the following options are available:

OPTION	TREATMENT
AVOID	Deciding not to proceed with the activity that introduced the unacceptable risk, choosing an alternative more acceptable activity that meets business objectives, or choosing an alternative less risky approach or process.
REDUCE	Implementing a strategy that is designed to reduce the likelihood or consequence of the risk to an acceptable level, where elimination is considered to be excessive in terms of time or expense.
SHARE TRANSFER	Implementing a strategy that shares or transfers the risk to another party or parties, such as outsourcing the management of physical assets, developing contracts with service providers or insuring against the risk. The third-party accepting the risk should be aware of and agree to accept this obligation.
ACCEPT	Making an informed decision that the risk rating is at an acceptable level or that the cost of the treatment outweighs the benefit. This option may also be relevant in situations where a residual risk remains after other treatment options have been put in place. No further action is taken to treat the risk, however, ongoing monitoring is recommended.