Form

Risk Assessment

Why is this important?

The identification and management of risks are central to achieving our strategic objectives. It protects us against downside risk, enables us to take risks for strategic reward, and improves our resilience against emerging risks.

Document control
This document is uncontrolled when printed or downloaded and should be discarded after use. Always source the most recent version from the White Rose *Governance Fundamentals Library* and share only the document link.

Document title	**Quick Investigation**	Verbatim of above
Identification	**FORM002**	A unique identification number: letters followed by three digits.
Status	**Published**	The lifecycle status: draft/published.
Version	**1**	Major number only (0=draft; 1; 2; etc)
Approval Date	**26 February 2026**	The date this version of the document was approved
Revalidation Date	**26 February 2028**	The date the document is due for review. A maximum of two years after the approval date.
Approver	**Lee Mason**	Title of the person who owns and is responsible for the document

Revision History		
Revised by	Revisions/changes/comments	Date re-published
Lee Mason	**First drafting**	

Table of Contents

1. Risk Management

Minimum requirements for Bowtie

Minimum requirements for Bowtie	
Risk Ref	Unique reference number for the risk
Identified	Date risk was identified.
Reviewed	Date of the latest review.
Name	Risk Name/Type
Risk Owner	Identify the individual(s) who own/accept the risk
Risk Event	The "risk" is being assessed. Gives rise to an action or condition; makes something happen, which may result in the Risk Event.
Risk Category	Type of risk
Uncontrolled Risk Rating	A, B, C, or D, assessed from the Risk Rating Matrix *(below)*
Mitigation Activity/Control	An actionable endeavour that protects reduces, limits, or regulates downside risk. An actionable endeavour that enables strategic reward.
Controlled Risk Rating	A, B, C, or D, assessed from the Risk Rating Matrix *(below)*
Implemented	Has the control(s) been implemented, yes or no?

Risk Rating Matrix

Based on the likelihood and impact of each risk, place each risk into an Uncontrolled Risk Rating category:

			Impact			
			0	1	2	3
			Acceptable	Tolerable	Unacceptable	Intolerable
			Little or No Effect on the Business	Effects are Felt but Not Critical; do not seriously effect the Business	Serious Impact to Course of Action; causes major disruption to Business Outcome	Could result in Disaster; Business may not recover
Likelihood	Improbable	Risk unlikely to occur; small chance of happening	A	B	B	C
	Possible	Risk will likely occur; some chance of happening	A	B	C	D
	Probable	Risk will occur; very likely to happen	B	C	C	D

*Uncontrolled Risk Rating = the size/measure of the Risk Event before any controls are implemented. Controls should be designed to reduce the likelihood and impact of the Risk Event (or enable the strategic reward in the case of Upside risks).

2. Risk Assessment

Risk Ref	Identified	Review	Name	Risk Owner (name / Position)	Risk Description	Causal Factors	Consequences	Risk Category	Pre-mitigation Risk Assessment			Mitigation Activity	Post-mitigation Risk Assessment			Implemented
									Pre Mit Likelihood	Pre Mit Impact	Pre Mit Risk Index		Post Mit Likelihood	Post Mit Impact	Post Mit Risk Index	
					There is a chance that ...	because of ...	with the consequences ...									
WRLP-001	20-Jul-22	20-Jul-23	Fraud	Samantha Mason - Director/Founder	There is a chance that WRLP will be subject to a fraudulent event	Because of: 1. Employees	With the consequence that: 1. Risk to WRLP 2. Risk to Clients 3. Certification	Human Controls	Possible	Intolerable	D	1. Employ people we know (referrals). 2. Every employee is security/background checked.	Improbable	Unacceptable	B	Yes
WRLP-002	20-Jul-22	20-Jul-23	Data Loss	Samantha Mason - Director/Founder	There is a chance that WRLP will be subject to a data loss event	Because of: 1. Employees 2. Premise break-ins 3. WRLP procedures 4. Cyberattack	With the consequence that: 1. Risk to WRLP 2. Risk to Clients 3. Certification	Human/Procedural /Techncial Controls	Possible	Unacceptable	C	1. Induct, train and retain staff members and promote awareness of the consequences of data loss. Enforce complex user passwords for IT hardware and software logins. Restrict access to data-sharing websites/platforms and high-risk websites and promote authorised SaaS platforms. 2. WRLP premises to be alarmed and monitored to reduce the risk of break-ins. 3. Operate 100% paperless to prevent the risk of paper-based data loss and to ensure standardised work procedures are in place. 4. Conduct regular system and compliance audits/updates, separate guest web access network, conduct regular data security risk assessments, and enforce EndPoint protection and workstation hard-drive encryption.	Improbable	Unacceptable	B	Yes