

Marymia Ltd – Vendor Risk Treatment & Management Summary

Prepared by: Ikuomola Adedeji – Third-Party Risk Analyst
Date: 20 July 2024
Version: 1.0
Next Review: 20 January 2025

Purpose
This document outlines Marymia Ltd's approach to identifying, evaluating, treating, and monitoring risks associated with third-party vendors based on the due-diligence and contract review phases. It forms part of the organisation's ISO 27001-aligned Third-Party Risk Management (TPRM) framework.

1. Risk Treatment Approach

Treatment Option	Description	When to Apply	Example
Mitigate	Enhance controls to reduce risk to acceptable level	When vendor supports critical data systems	Add encryption, access controls, MFA.
Transfer	Shift risk to another party via contract	When vendor holds sensitive data	Add liability clauses or cyber insurance.
Avoid	Discontinue engagement or use alternative vendor	When risk exceeds acceptable threshold	Stop high-risk vendor contract.
Accept	Tolerate risk if low and monitored	For non-critical services with compensating controls	Accept minor process delay.

2. Vendor Risk Treatment Plan

Vendor	Risk	Key Issue	Treatment	Mitigation Actions	Owner
DHL Logistics	High	No incident plan, no audit rights	Mitigate / Transfer	Require IR plan and audit clause	Legal / Compliance
Zoom Communications	Medium	Expired ISO certificate	Mitigate	Request updated certificate	Risk Analyst
FedEx Delivery	Medium	No breach clause	Mitigate / Transfer	Add 72-hour clause and DPA	Legal
AWS Cloud Services	Low	None identified	Accept	Maintain annual review	Compliance
QuickBooks (Intuit)	Low	Minor BCP clause gaps	Mitigate	Request DR test summary	Procurement

3. Vendor Risk Register

Risk ID	Vendor	Description	Likelihood	Impact	Score	Level	Action	Status
R01	DHL	Missing incident plan	High	High	9	High	Mitigate	In progress
R02	Zoom	Outdated ISO certificate	Medium	Medium	6	Medium	Mitigate	Open
R03	FedEx	Missing DPA & clause	Medium	High	8	High	Transfer	Open
R04	QuickBooks	Missing BCP evidence	Low	Medium	4	Low	Mitigate	In progress
R05	AWS	Minor process delay	Low	Low	2	Low	Accept	Closed

4. Management Summary

Total Vendors Reviewed: 30
High-Risk Vendors: 2
Medium-Risk Vendors: 3
Low-Risk Vendors: 25
Treatment Completion: **80%** (24/30 vendors remediated or accepted)

Next Review: **20 January 2025**

Observations:

- Most High-Risk vendors are in logistics and communication sectors.
- Compliance and Legal are leading contractual mitigations.
- All residual risks are within Marymia Ltd's accepted risk appetite.

Recommendations:

1. Continue quarterly vendor risk reviews for critical suppliers.
2. Enforce updated security clauses upon contract renewal.
3. Maintain TPRM dashboard for continuous monitoring.
4. Integrate scoring and risk trend data into Power BI reporting.