Marymia Ltd – Third-Party Security Due Diligence Programme

Prepared by: Ikuomola Adedeji – Third-Party Risk Analyst
Version: 1.0 **Issue Date:** 10 July 2024 **Next Review:** 10 July 2025

As part of Marymia Ltd's information security governance programme, a comprehensive **Third-Party Security Due Diligence and Risk Scoring Framework** was developed to evaluate the cybersecurity posture of thirty (30) strategic vendors. The project aimed to align supplier risk management with **ISO 27001**, **NIST SP 800-161**, and **GDPR** requirements. A **weighted scoring model** was designed to quantify risk across ten (10) security domains, including Governance, Data Protection, Access Control, Incident Response, and Business Continuity. Each domain was assigned a risk weight (5–15%) and assessed using an evidence-backed due diligence questionnaire containing over 100 control-based questions. All vendors completed the questionnaire by the reporting deadline (17 July 2024), achieving a 100% response rate. Results were consolidated into an automated Excel-based dashboard that calculates vendor risk using a **formula-driven SUMPRODUCT method** and visualises risk categories (Green / Amber / Red).

Key Outcomes

Total Vendors Assessed	30
Response Rate	100%
Low-Risk Vendors	10
Medium-Risk Vendors	14
High-Risk Vendors	6
Overall Portfolio Risk	Medium (Amber)

Key Observations & Impact:
Cloud and payment vendors demonstrated strong ISO and SOC 2 alignment. Several logistics and facilities suppliers lacked formal incident response plans. Contract clauses were updated to include breach notification and data retention obligations. Remediation trackers and audit evidence were stored in SharePoint for traceability. The programme enabled executive-level visibility into supply chain security risk.

This initiative delivered a **repeatable, auditable, and metrics-driven third-party security framework**, enhancing Marymia Ltd's visibility of supplier risk, improving decision-making, and strengthening compliance with data protection and business continuity standards.