Vendors / Suppliers Pre-procurement Minimum Cyber Security Standard

Table of Content

Introduction

Purpose

The purpose of this document is to provide self-serve guidance to Monash University Australia (MUA) staff on vendor tiering and the minimum cybersecurity requirements applicable for each tier during an evaluation of an IT procurement. This will ensure that all vendors and suppliers meet the necessary cyber security requirements to protect our data and services.

In Scope

This standard applies to all Monash University Australia staff and associates, and is applicable when selecting new suppliers and vendors accessing the University's Information Technology (IT) environments.
In scope of this document:

- Procurement of any new information assets, both internally and externally stored or handled.
- Procurement of virtual or physical systems supporting or storing Monash data.

Out of Scope

Out of scope of this standard:

- Detailed security requirements.
- System level Technical, Administrative and Operational Controls related to services or products under procurement.

Vendor Tiering Model

Monash University classifies vendors/suppliers into three (3) tiers based on the:

- Criticality and sensitivity of the data/ information they may have access to
- Availability requirements of the services or products provided to the University
- The data / information could be hosted by the University or the vendor(s)/supplier(s)

Table 1: Third Party Risk Tiering Model, provides the details of the criteria to allocate an appropriate tier to each new vendor or supplier.

Table 1. Third Party Risk Tiering Classification Criteria		
Vendor/ Suppliers Tier Classification	Classification Criteria	Risk Factor (refer to **Figure 1**)
Tier 1: High Risk Vendors/ Suppliers	Vendors with access to • Monash University's network (e.g., API, VPN, Direct/ Remote access, etc) AND/OR • Access to data/information classified as C3 and/or C4[1]	• Network Access OR • C4* data (Very Sensitive) OR • C3* data (Sensitive)
Tier 2 Medium Risk Vendors/ Suppliers	Vendors with no access to • Monash University network AND • Data/information classified as C3 and/or C4 but, have access to • Data/information classified as C2 AND/OR • where failure of the vendor service will significantly impact business operations.	• Access to C2 data (Restricted) only OR • Significant impact to operations if vendor has a service failure
Tier 3 Low Risk Vendors/ Suppliers	Vendors with no access to • Monash University network AND • Data/information classified as C2, C3 and/or C4 AND • where failure of the vendor service will not significantly impact business operations AND • Where vendors will only have access to C1 data.	• Access to C1 data (Public) only AND • No significant impact to operations if vendor has a service failure

[1] For details on Information Classification and Labelling such as C1, C2, C3 and C4 see Electronic Information Security Classification Procedure

Cyber Risk and Resilience

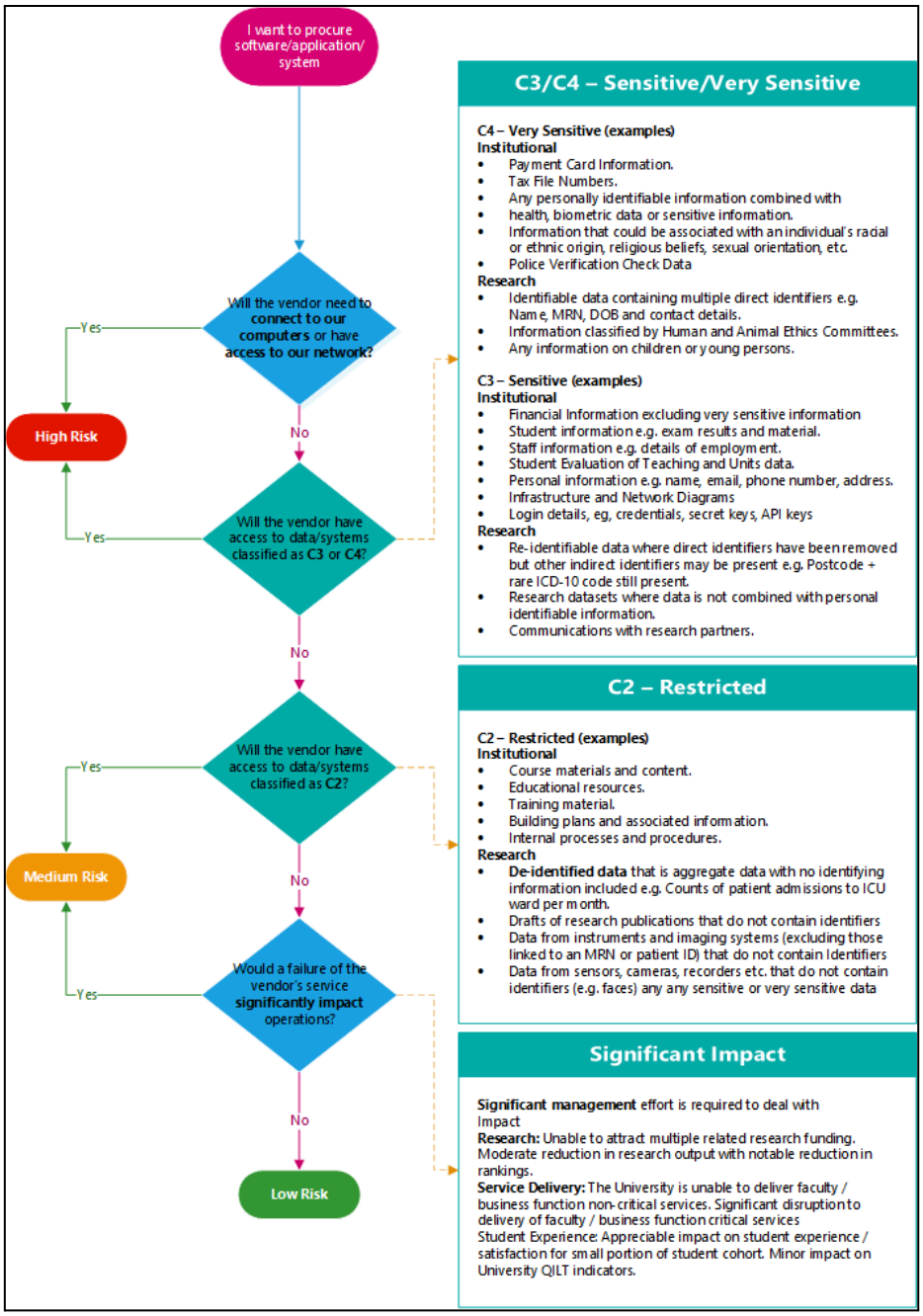

***Figure 1: Third-Party Risk** Tiering Model*

Minimum Cybersecurity Requirements

Vendor/ Suppliers Risk Tiers	Minimum Cyber Security Key Controls
Tier 1: High Risk	Vendors and suppliers must: • Have the ability to support Monash Single-Sign On (SSO). AND • Hold industry certification equivalent to ISO27001, SOC2 Type II, and are able to provide evidence when requested. AND • Agree to adhere to Monash University specific cybersecurity clauses within contracts. AND • Demonstrate evidence of Cyber Insurance with appropriate level of third party coverage, including service(s) provided to Monash University. Other recommended documents: • Higher Education Community Vendor Assessment Toolkit (HECVAT) Lite or Full • Other independent assessment/certification based on a common security framework.
Tier 2: Medium Risk	Vendors and suppliers must: • Have the ability to support Monash Single-Sign On (SSO) AND • Hold industry certification equivalent to ISO27001,SOC 2 Type 1, and are able to provide evidence when requested. AND • Agree to adhere to Monash University specific cybersecurity clauses within contracts.
Tier 3: Low Risk	• Service Owner led risk management. All requirements for Tier 2 are strongly recommended.

Table 2: Minimum Cyber Security Controls for Third Party Risk Tiers

Next Steps

A cyber security vendor review process will need to be undertaken on the shortlisted vendor. The business owner must:

- Log an Information Security Risk Assessment (ISRA) and refer to the ISRA webpage for further guidance if required.
- The ISRA will be reviewed by the Cyber Risk and Resilience Team to understand the context and identify and prioritise risks so that the business can make an informed decision to determine if the risk is acceptable to Monash University. This may require the vendor /third-party and / or the business to implement additional controls and / or a remediation plan.

If you require further information about this, please contact Cyber Risk and Resilience team via cyberteam-risk-l@monash.edu.

Reference

- NIST 800-61 rev 1 Standard
- FIPS-199 Standard
- Monash University Cyber Security Architecture Principles
- Monash University Cyber Security Standards
- Information Classification Standard

Version and Update History

Version	Date	Author/ Reviewer	Summary of Change
1.0 Final	4/11/2024	Cyber Key Stakeholders	Review with Cyber LT