

Third-Party Vendor Management Process

1. Introduction

As The Open College of the Arts (OCA) engages and works with a number of third-party vendors, it is important that the security risks associated with working with vendors of technology or information related products and services are identified and managed with a consistent approach, prior to any access to the OCA's information and information systems. This process sets out the required actions to be taken by the OCA to ensure vendors collaborating with, or providing products or services to the College, do so securely and in-line with the requirements of the Third-Party Vendor Management Policy.

The Third-Party Vendor Management Process comprises of several stages:

- A high-level triage risk assessment of a new vendor, done internally by the OCA as part of due diligence before onboarding that vendor (Stage 1).
- Depending on the outcomes of the risk assessment, a self-assessment questionnaire (Stage 2).
- Depending on the outcomes of the previous stage(s), a remediation stage (Stage 3).

The Third-party Vendor Management process shall also be applied to existing vendors in any of the following cases:

- When there is a significant change or extension of the services provided by an existing vendor.
- When the contract with an existing vendor is reaching its end, and the vendor has not been subject to the Third-party Vendor Management Process before.

In the case where a given vendor provides the same service to two or more business units of the OCA, this Third-party Vendor Management Process can be applied globally across the relevant business units.

2. New or Changing Vendors

To ensure that the Third-party Vendor Management Process is initiated in a timely fashion, the Vendor Sponsor must inform the IT Manager when:

- Engaging any potential new vendor, including as part of a tender evaluation process;
- There are changes to an existing vendor's service; or
- An existing vendor's contract is coming to an end.

It is then the responsibility of the IT Manager to carry out the risk assessment (stage 1) of the vendor in collaboration with the Vendor Sponsor.

3. Stage 1: Triage Risk Assessment

A triage risk assessment shall be carried out on all vendors that could affect information security, irrespective of the value of the contract.

The Vendor Sponsor, in collaboration with the IT Department, is responsible for carrying out the initial vendor triage assessment to determine the inherent level of risk.

Further guidance on how to conduct a risk assessment can be found within the [Risk Management Process](#).

3.1. About the Vendor, Service and Data

All details of the vendor should be captured before performing the risk assessment. These key questions should be asked to the vendor during the initial procurement phase and documented in as much detail as possible.

Responses to the volume and classification of data the vendor may be handling can be selected through drop-down lists. The selections available are colour coded to provide an indication of the potential risk levels associated and provide further context for the risk assessment. The risk levels are represented as follows: **High**, **Medium** and **Low**.

About the Vendor	
Vendor Name	
Vendor Website	
Vendor Contact Name	
Vendor Contact Email Address	
Vendor Operating Locations - Offices; Datacentres	
Vendor Outsourcing	
Vendors Information Security Certifications	
About the Service	
Service description	
Data flow information between the Vendor and the OCA	
How often is the information exchanged?	
Location where OCA data will be stored and processed	
About the Data	
Description of the data	
Is the data regulated?	Yes / No
Does the data include personal details of staff, students or customers? If yes, what is the volume of data shared?	Small Number of Records (0-1000)
Does the data include credit card or debit card details? If yes, what is the volume of data shared?	
What is the data classification?	Highly Confidential

3.2. Recording Inherent Risk

It is the responsibility of the IT Manager to review and approve the completed triage risk assessment, decide whether further due diligence is required, and communicate their findings and recommendations to the Vendor Sponsor.

Results of the triage risk assessment should be recorded within the Third-Party Vendor Risk Register as the Inherent Risk.

Where the OCA obtains confirmation that a vendor is certified against relevant information security standard(s) during the triage process, this may be considered as sufficient assurance regarding the level of risk posed by using the vendor's services. In this case, the certification should be verified and approved by the IT Manager, and the certification documented within the Third-Party Vendor Risk Register. No further due diligence shall be required. The vendor risk should be recorded as Tolerated (accepted) and no further actions required.

4. Stage 2: Vendor Self-Assessment

Following the triage risk assessment (Stage 1), all vendors that the IT Manager has assessed to represent a **Medium** or **High** risk to the OCA shall undergo further due diligence. This involves the vendor answering a self-assessment questionnaire to evaluate its information security controls and maturity. The Vendor Sponsor is responsible for ensuring the vendor completes the Third-Party Vendor Information Security Questionnaire.

4.1. Reviewer Response and Rating

The IT Manager is responsible for reviewing the responses that the vendor has provided, assessing the rating, response narrative and evidence for each control question. Evidence should be carefully analysed to ensure that any documentation provided is accurate and is the current approved version. During the review stage, the vendor's response ratings should be assessed as follows:

Implemented – The vendor has given an adequate response and provided sufficient evidence to demonstrate that they meet the control.

Partially Implemented - The vendor had provided a response that details how they meet some aspects of the control and provided sufficient evidence – Or – the response provided is adequate, but the evidence provided appears outdated, inaccurate or not applicable. For example:

	Control Question	Supplier Rating	Supplier Response	Supplier Evidence	Reviewer Response / Notes	Reviewer Rating	Action Required
1.1	Does your organisation have an information security policy and data protection privacy document which is defined, approved by management, published and communicated to all employees and relevant stakeholders?	Implemented	Yes	Information Security Policy.pdf Data Privacy Policy.pdf	The appropriate policies are in place, however they do not appear to be approved or signed off by management.	Partially Implemented	Ask the supplier if they have an approved version of the documents. Or can evidence an approvals process is in place.

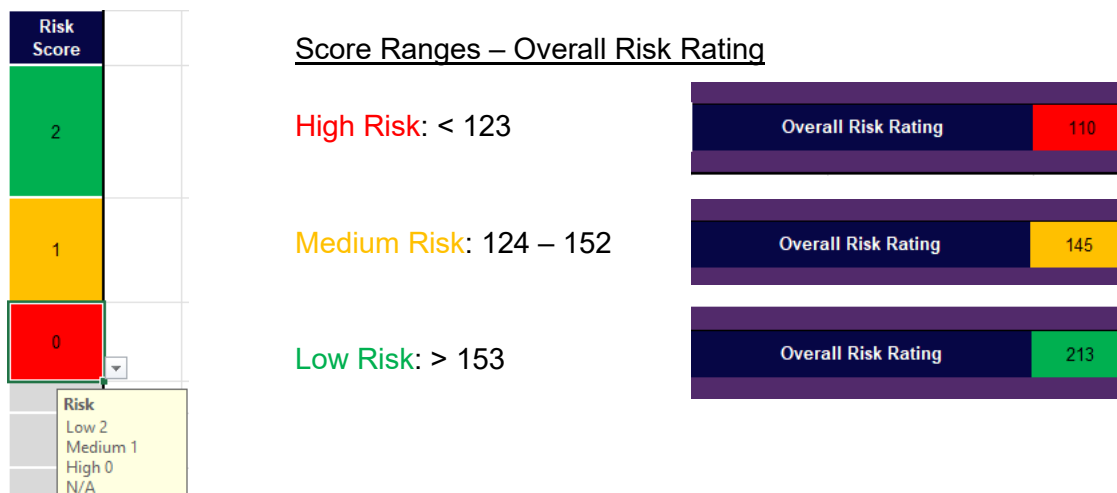
Not Implemented – The vendor has selected the rating ‘**Not Implemented**’ and does not meet the control – Or – no evidence has been provided.

Note* Guidance on how to select and detail the Vendor Rating, Vendor Response and Vendor Evidence for vendors completing the Information Security Questionnaire is contained within the document.

Where the vendor has selected a ‘**Implemented**’ or ‘**Partially Implemented**’ rating but provided no evidence. The initial ‘Action Required’ should first be a request for evidence.

4.2. Risk Score

The scoring mechanisms used within the Information Security Questionnaire for **Implemented**, **Partially Implemented** and **Not Implemented** ratings, align to the criteria of **Low (2)**, **Medium (1)** and **High (0)** risk ratings. With scoring ranges proportional to the risk criteria in the Information Security Risk Management Policy defining the level of risk. I.E., higher scores for implemented controls represent a lower overall risk rating and lower scores for not implemented controls representing a higher overall risk rating. The overall risk rating score acts as an indicator to inform the risk assessment process.



4.3. Recording Residual Risk and Action Required

After the initial review of the questionnaire, the residual risk of a vendor should be assessed, factoring in the results of the questionnaire, and recorded within the Residual Risk Section of the Third-Party Vendor Risk Register. The decision shall be made as to whether the OCA is exposed to a level of risk that is tolerable and the appropriate risk treatment option should be recorded. (Treat, Transfer, Terminate, Tolerate).

In order to ensure ‘Actions Required’ are appropriate, subject matter experts and relevant teams knowledgeable of the corresponding control within the OCA should be consulted. For example, the Data Protection Officer may be consulted to advise on GDPR requirements.

5. Stage 3: Remediation

Where there are any shortfalls in expected vendor controls that have been identified as part of the stage 2 assessment, these must be followed up with the relevant teams. The Vendor Sponsor, the IT Department and other stakeholders must agree 'Actions Required' and delivery dates with the vendor. The questionnaire should be linked within the Third-Party Vendor Risk Registers 'Further Actions Required' column to ensure all actions are captured and easily referenced.

The Target Risk should be assessed and recorded within the Third-Party Vendor Risk Register to ensure that remediation plans and 'Actions Required', once implemented, will bring the risk to a desired level that will be accepted by the OCA.

6. Third-party Vendor Review

It is the responsibility of the IT Manager to ensure every low-risk vendor undergoes a review at least every 24 months, and at least annually for medium-risk and high-risk vendors. If changing circumstances such as legislation, regulations, vendor disclosed incidents or contracts occur. Vendors will be required to undergo a more immediate review.

This is to confirm that:

- No changes have occurred to the services being provided that may require the vendor to undergo another risk assessment;
- OCA data and service availability are unaffected by any third-party activity or incident;
- No changes to the control coverage of the vendor have occurred that may require the vendor to undergo another self-assessment.

When a vendor has been reviewed, the Third-party Risk Register and Vendor Register shall be updated accordingly.

7. Document Control

Document Control	
Title:	Third-party Vendor Management Process
Version:	1.0
Date:	10/11/2025
Status:	Draft
Owner:	IT Manager
Classification:	Internal

Document Revision History

Version	Date	Author	Summary of changes
0.1			Initial draft
1.0	10/11/2025	Dean Humphreys	Re-numbered in line with OCA templates.