GDPR RISK MANAGEMENT PROCEDURE

Policy no:	8.8
Version no. & date:	V23.3
Next review due:	September 2024
Responsible Committee:	SMT
Approved by & date:	April 2023
Linked policies:	Other GDPR Policies Risk Management Policy
External references	GDPR, Data Protection Act 2018
Audience:	Internal

Contents

1. **Introduction**

At Oxford Business College (OBC), we are dedicated to safeguarding the privacy and integrity of personal data entrusted to us. In accordance with the General Data Protection Regulation (GDPR), we have implemented a comprehensive risk management policy designed to identify, assess, mitigate, and monitor information security risks associated with the handling of personal data

2. **Purpose**

The purpose of this document is to provide a risk management framework which will be used by OBC to identify, assess, treat and monitor information security risks, and support our commitment to protecting personal data. It includes a breakdown of what risk is, how OBC approaches risk management and instructions for managing the internal risk register.

3. **Scope**

Protecting company data and the systems that collect, process, and maintain personal information is of critical importance and requires a security and risk framework. OBC framework involves the participation and support of every employee or representative who interacts with the company's data and systems. Therefore, this procedure apples to all who fall within that definition.

4. **Aims and Objectives**

This Policy aims to:

- Identify, assess, and mitigate potential data protection risks associated with the organization's data processing activities, ensuring compliance with GDPR requirements.
- Foster a proactive approach to GDPR risk management within the organization, promoting a culture of data protection awareness, responsibility, and continuous improvement.
- Implement an effective and structured GDPR risk management process that enables the organization to monitor and address data protection risks in a timely and efficient manner, safeguarding the privacy rights of individuals and maintaining the organization's reputation.

5. **Responsibilities**

- Risk Owners/Process Owners/Asset Owners are responsible for identifying business and information security risks, recording risks, assessing the risks and for the development, testing and maintenance of plans to manage those risks.
- The Senior Management Team is responsible for ensuring that all business and information security risks have been included in the risk register and appropriately treated.

- All staff and/or representative who interacts with the company's data and systems is responsible for identifying risks and bringing these to the attention of their line manager
- Line Managers are responsible for reporting risks to the Process Owners/Asset Owners

6. Risk Assessment

Identified risks will be assessed according to the likelihood of the risk occurring and the impact if it did. The company has defined likelihood and impact as follows:

Defining Likelihood

Assumptions based on likelihood may come from various internal and external sources, depending on the specific circumstances. As with potential impact, assessors need to document the justification for the value that was determined, including the facts and assumptions used in the decision-making process. The five (5) categories of potential likelihood are:

Very Low:	Low	Medium	High	Very High:

Defining Impact

TOBC has defined potential impact into five (5) categories. These categories allow a more granular understanding of risk and broken down by differing types of impact as per the grid below:

Description	Financial Impact	Operational Impact	Reputational Impact
Insignificant	Loss/breach equivalent to £1K or less	Minor problems in one area of service delivery affecting fewer than 10 students	Internal Matter
Minor	Loss/breach equivalent to between £1K and £5K	Disruption to specific areas of service delivery affecting between 10 and 20 students	Adverse attention from fewer than 5 students
Moderate	Loss/breach equivalent to between £5K and £10K	Widespread disruption to business operations affecting over 50% of students	Adverse attention in local press

Major	Loss/breach equivalent to between £10K and £100K	Major disruption to business operations affecting the majority of students	Major adverse industry media attention
Severe	Loss/breach equivalent to more than £100K	Unable to provide service to students	Significant national/international adverse media attention

The impact (insignificant, minor, severe etc) will be determined by the greatest of the three areas under consideration (financial, operational, reputational). So, for example, if the financial impact is insignificant, but the reputational impact is major, the impact rating would be major.

7. Risk Acceptance Criteria

Deciding on how and or if to mitigate a risk is always a senior management team decision.

Risk Levels

OBC has four (4) levels of risk categorisations. They are:

- Low
- Medium
- High
- Severe

8. Risk Calculation

The following assessment chart (also found in the risk register) should be used to understand the overall risk level.

Likelihood	Impact				
	Insignificant	Minor	Moderate	Major	Severe
Very Low	LOW	LOW	MEDIUM	MEDIUM	HIGH
Low	LOW	LOW	MEDIUM	HIGH	HIGH
Medium	LOW	MEDIUM	MEDIUM	HIGH	SEVERE
High	MEDIUM	MEDIUM	HIGH	SEVERE	SEVERE

Very High	MEDIUM	MEDIUM	HIGH	SEVERE	SEVERE

Risk Management decisions have been separated into two tiers to support where certain risks require escalation for senior sign-off. Tiers have been established that allow for escalation on risk greater than Low. These tiers provide the organisation with the appropriate level of management oversight, based on the level of risk:

TIER 1 – Automatic Acceptance

- Risks which are defined as **LOW** and MEDIUM will be automatically accepted by the organisation. However, they must still be recorded and reviewed. If, despite the outcome of the assessment, the person completing the risk assessment believes it needs to be brought to the attention of senior management, then it should.

TIER 2 – Senior Management

- Must decide on a risk treatment plan or decide to accept HIGH and SEVERE risks.
- A member of senior management should be made the risk owner
- That owner should develop a plan to incorporate remediation actions within a reasonable period of time and review the risk after compensating controls have been put in place.

9. **Risk Register**

Identified risks should be recorded in the company information security risk register. The asset owner/process owner should record the risk and assess it.

The risk registers for OBC includes a risk assessment. If the risk is considered HIGH or SEVERE it will be investigated immediately by the senior management team. Any LOW or MEDIUM risks will be added to the register and be part of the registers regular review unless it is deemed a higher priority based on its context.

Step one Recording the Risk:

- Date Identified – Enter the date that the risk was identified e.g. 21/01/2023
- Risk Category – Select the most appropriate risk category from the drop down
- Risk ID – Enter the risk ID – this should be sequential e.g. if the previous risk is RISK001 then the next is RISK002
- Risk Description – Enter A paragraph describing the risk. As much detail as possible is advised. E.g. There is a risk that, if software patches are not applied quickly, a hacker will be able to exploit the vulnerabilities that the patch addresses, which could lead to exfiltration of personal data

Step two Assess the risk:

- Likelihood – Select from the drop down based on the likelihood table, the appropriate likelihood
- Impact – Select from the drop down based on the impact table the most appropriate impact
- Risk Rating – using the 5X5 risk calculation matrix shown above (and in the risk register), select the risk rating from the drop down.
- CIA – identify whether the risk impacts confidentiality, integrity or availability (or any combination of)
- Notes – add any additional notes about the risk. E.g. it may be that at this point further investigations are needed to establish how best to address the risk.

Step three decide on risk decision:

- Next Steps – Identify and record what the next steps are going to be to address the risk
- Risk owner – enter the name of the risk owner
- Risk decision – Select from the dropdown to either accept, treat, terminate or transfer – the decision here will depend on what the options are to deal with the risk and the level of risk. There may be some debate, decision making that will go on before this can be recorded.
- Details of the decision – Enter as much detail as possible as to how the risk is going to be addressed

Step four – residual risk assessment

- Residual Likelihood – Select from the drop down based on the likelihood table, taking into consideration the effect any risk treatment will have on this
- Residual Impact - Select from the drop down based on the impact table, taking into consideration the effect any risk treatment will have on this
- Residual Risk Rating – using the 5X5 risk calculation matrix shown above (and in the risk register), select the residual risk rating from the drop down

Step five – approval and monitoring

- Approval – Enter the name of the person approving the residual risk (according to the tiers above, low and medium residual risks can be approved by the business i.e. the risk owner, high and severe residual risks will need approval from senior management)
- Date Approved – Enter the date that the approver approved
- Status – Select either open or closed from the drop down menu – an item is closed if the risk has been addressed, controls have been put in place. If the risk has yet to be addressed e.g. if you are installing some new software to help address the risk, the status will remain open until the controls are in place.

- Last review date – Enter the date when the risk was last reviewed as part of either the original assessment or when there was a review of risks. Enter the next review date in accordance with the Risk review schedule table below:

Risk Rating	Frequency of review
LOW	6 months
MEDIUM	3 months
HIGH	1 month
SEVERE	1 month

Information security is all about protecting the confidentiality, integrity, and availability (CIA) of data. These three terms are defined as:

- Confidentiality
    - Confidentiality addresses preserving restrictions on information access and disclosure so that access is restricted to only authorised users and services.

- Integrity
    - Integrity addresses ensuring that sensitive data has not been modified or deleted in an unauthorized and undetected manner.

- Availability
    - Availability addresses ensuring timely and reliable access to and use of information.

Step two of the Risk Assessment Sheet:

In step two, risk identifiers would need to use the drop-down options and define the likelihood and Impact of said risk (using the table at the bottom of the sheet). Once the likelihood and impact has been defined, the risk rating will be automatically calculated as per in built risk matrix. **NOTE**: Do not edit the raw data of this sheet. Only fill in the boxes.

Next, treatment plan suggestions should be made by the risk reporter or reviewing manager to reduce said risk to an acceptable level.

Step three of the Risk Assessment Sheet:

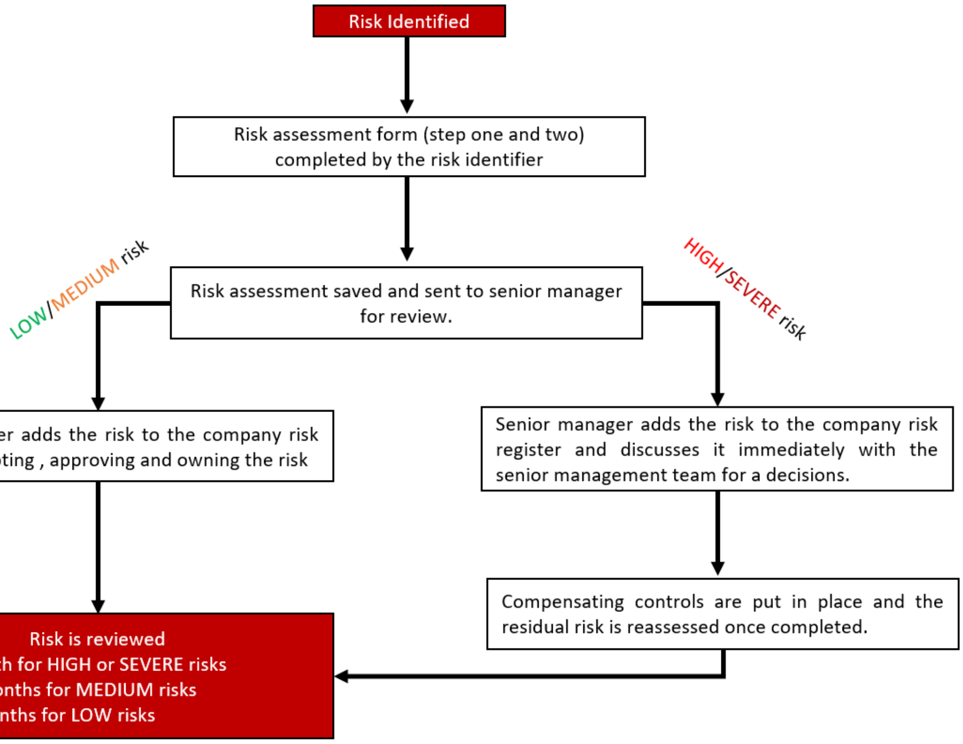
This section must only be completed by senior management!

A Senior Management representative needs to review all the information from steps one and two. If the risk is deemed HIGH or SEVERE it should immediately be discussed with the rest of the senior management team to determine if they are going to accept, transfer, avoid or treat the risk. Once discussed the Risk treatment option can be entered using the drop-down box. If the risk was deemed to be LOW or MEDIUM, the risk can be automatically accepted and approved by the senior management representative if they agree with the assessment.

Regardless of the rating, this risk assessment should then be added to the risk register and a review date assigned according to the review schedule below:

Risk Rating	Frequency of review
LOW	6 months
MEDIUM	3 months
HIGH	1 month
SEVERE	1 month

10. **Risk Management Process**


Risk Identified
Risk assessment form (step one and two) completed by the risk identifier
Risk assessment saved and sent to senior manager for review.
LOW/MEDIUM risk
HIGH/SEVERE risk
Senior manager adds the risk to the company risk register, accepting , approving and owning the risk
Senior manager adds the risk to the company risk register and discusses it immediately with the senior management team for a decisions.
Compensating controls are put in place and the residual risk is reassessed once completed.
Risk is reviewed
• every month for HIGH or SEVERE risks
• every 3 months for MEDIUM risks
• every 6 months for LOW risks