GDPR RISK MANAGEMENT PROCEDURE

Policy no:	6.7
Version no.	V24.11
Next review due:	September 2025
Last review date:	November 2024
Responsible Board:	Corporate and Planning Board
Approved by & date:	SMT April 2023
Linked policies and documents:	Risk Management Policy
External references	GDPR, Data Protection Act 2018
Audience:	Internal

Table of 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's 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

4.1 This Policy aims to:

4.1.1 Identify, assess, and mitigate potential data protection risks associated with the organisation's data processing activities, ensuring compliance with GDPR requirements.

4.1.2 Foster a proactive approach to GDPR risk management within the organisation, promoting a culture of data protection awareness, responsibility, and continuous improvement.

4.1.3 Implement an effective and structured GDPR risk management process that enables the organisation to monitor and address data protection risks in a timely and efficient manner, safeguarding the privacy rights of individuals and maintaining the organisation's reputation.

5 Responsibilities

5.1 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.

5.2 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.

5.3 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.
5.4 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:

6.1 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:
1-5	6-10	11-15	16-20	21-25

6.2 Defining Impact

OBC 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 1% of students	Internal Matter
Minor	Loss/breach equivalent to between £1K and £5K	Disruption to specific areas of service delivery affecting between 3% students	Adverse attention from fewer than 3% students
Moderate	Loss/breach equivalent to between £5K and £10K	Widespread disruption to business operations affecting over 10% 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	Unable to provide service to	Significant

	equivalent to more than £100K	students	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.

7.1 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:

8.1 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.

8.2 TIER 2 – Senior Management

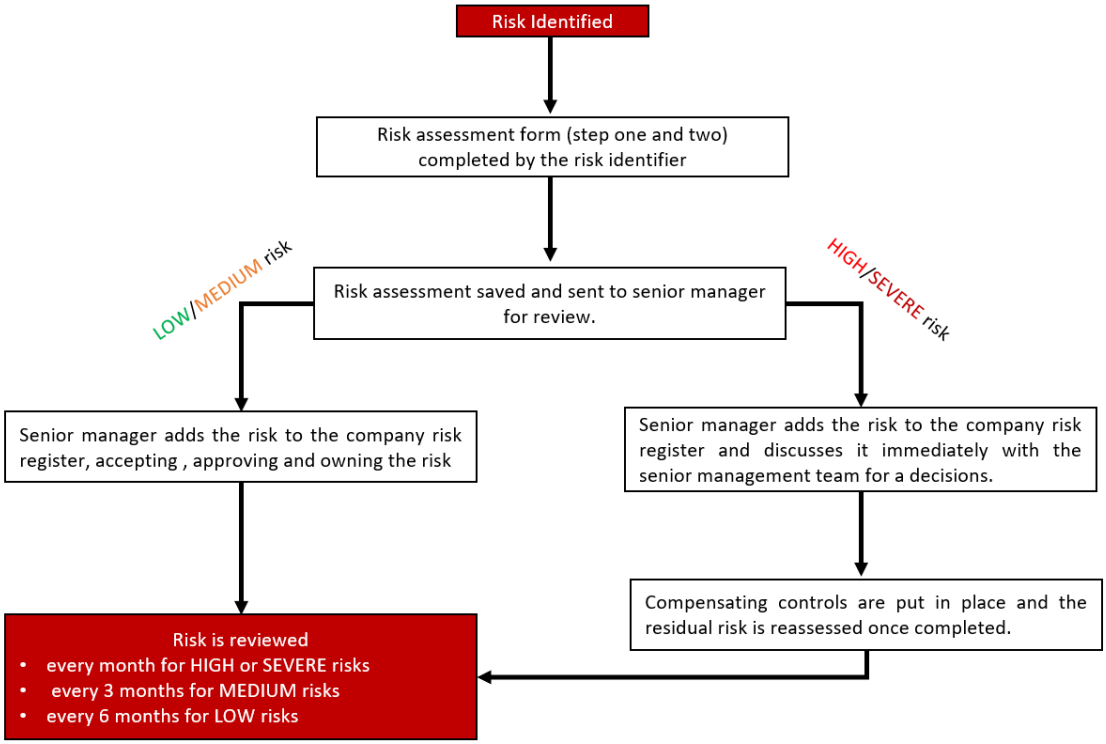
8.2.1 Must decide on a risk treatment plan or decide to accept HIGH and SEVERE risks.

8.2.2 A member of senior management should be made the risk owner

8.2.3 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.

8.2.4 These risks will be added to the institutional risk register.

9 GDPR Risk Management Process



9.1 Institutional Risk Management Procedure

The following steps describe the process of Risk Management at the College throughout the annual review cycle:

9.1.1 All risks on the Risk Register undergo assessment every quarter.

9.1.2 Each risk on the Risk Register is assigned a risk owner who is responsible for identifying, updating, and managing the risk(s) they are accountable for.

9.1.3 If any member of the Board of Governors (BoG) or Corporate Planning Board (CPB) identifies a new risk and the corresponding risk owner, they inform the Head of Quality Compliance & Legal Affairs to assign the risk and include it in the Risk Register.

9.1.4 The Head of QualPliance & Legal Affairs forwards each identified risk to the respective risk owner for assessment.

9.1.5 Following input from risk owners, the Head of QualPliance& Legal Affairs update the risk register and included the new risk in institutional monitoring.

9.1.6 CPB members monitor and evaluate each risk along with the implementation of mitigation plans to address threats and leverage opportunities.

9.1.7 The Risk Register, along with its monitoring and review process, is presented to the BoG by the Head of Quality Compliance & Legal Affairs.

9.1.8 Mitigation plans are scrutinised and revised during the subsequent CPB meeting.

9.1.9 The CPB has the authority to designate new risk owners as and when new risks are identified, ensuring a proactive approach to risk management and mitigation.