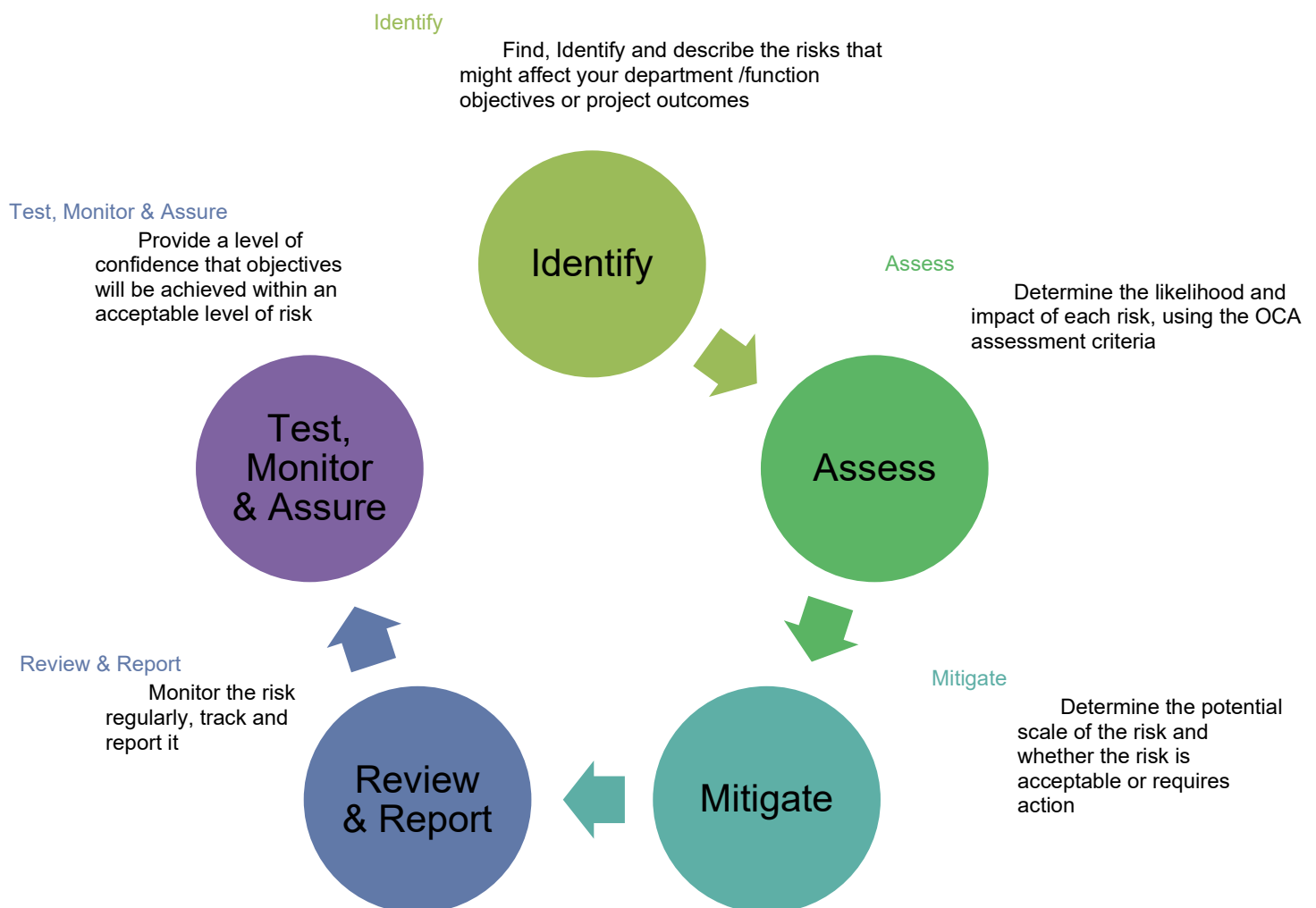


Risk Management Process

Purpose

The Risk Management Process outlines the various stages we need to undertake to fully understand our risks and identify the best ways to manage them.

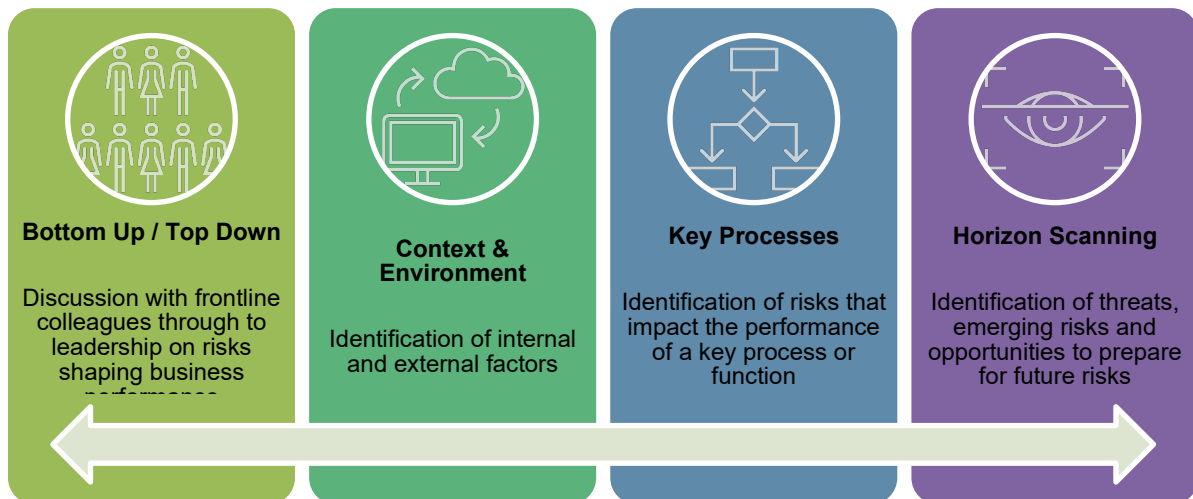
This process applies to all departments across The Open College of the Arts (OCA), ensuring a consistent approach to Risk Management.



Identifying Risks

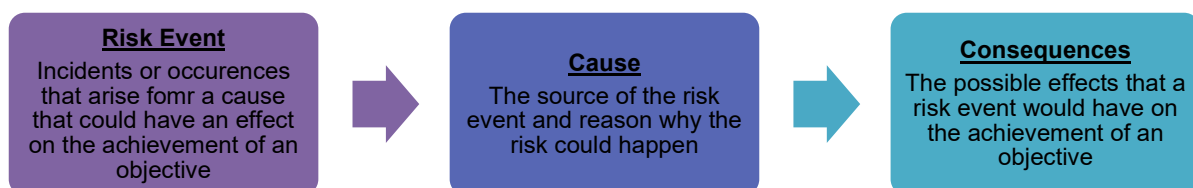
Identifying risks enables us to understand what could limit our ability to achieve our strategy objectives. Gaining clarity of the risks informs what actions can be taken to appropriately manage them.

The first stage of the Risk Management process is to identify and describe all significant risks that could impact our objectives. Here are some elements that should be considered when identifying risks:



Describing Risks

A key fundamental to identifying risk is to have an accurate description of the risk. Having properly defined risks allows us to understand the risk and ensure actions can be taken to manage it appropriately. The description of a risk should contain a single event, cause and consequence(s).

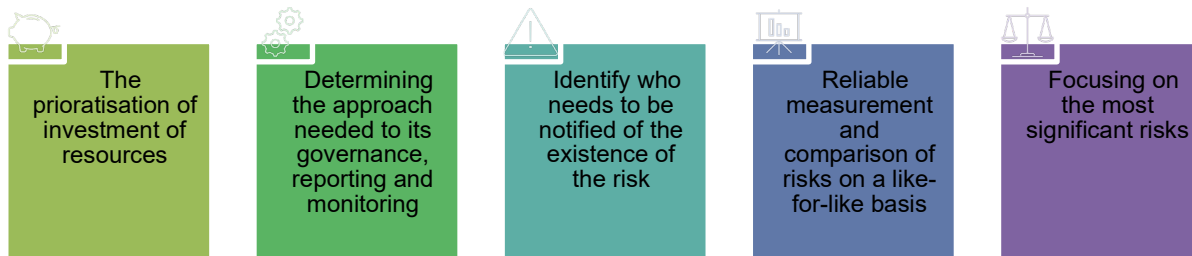


For example:

"Malicious external party gaining access to the organisation's cyber network due to poor cyber security controls may result in a potential loss of confidential information, damage to the organisation's reputation, loss of revenue and regulatory fines."

Risk Assessment

Following the identification of a risk, a **Risk Assessment Form** must be completed prior to the risk being recorded in the risk register. Carrying out risk assessments helps to integrate a consistent basis for reviewing risk and allows for:



Risk assessment determines the significance of a risk by assessing the severity of a risk. Severity can be determined by considering two factors, likelihood and impact:

Risk Assessment Criteria - Impact(s)

"The potential impact on objectives if the risk were to occur"

Consider and estimate the potential impact to the organisation should the risk occur, following the impact criteria.

Impact	Criteria by Type of Impact			
	Financial	Legal and Regulatory (Non-compliance)	Operational	Reputational
1: Insignificant	< £10k	Minor breaches managed locally	Negligible	Localised short-term media activity (press, TV, social media) resulting in negative comment by no more than 100 current and potential OCA students
2: Low	£10k-50k	Minor breaches resulting in communication from relevant body	Minor local operational issues on a daily basis affecting 10% or more of students and/or staff having limited effect on ability to complete study activities and / or routine work Or Failure to achieve a key Unit objective/ minor College objective by a due date	Localised media activity (press, TV, social media) lasting up to 2 weeks resulting in negative comment by no more than 200 current and potential OCA students with little impact on influencers/ government
3: Medium	£50k-100k	Significant breaches resulting in limited censure/ fine/ penalty but no	Minor local operational issues over a 1-week period affecting 10% or more of students and/or staff having some effect	National media activity (press, TV, social media) lasting more than 2 weeks resulting in negative comment by up to 600

		regulatory intervention	on ability to complete study activities and/or routine work Or Several key College objectives or core College activities not achieved by a due date	current and potential students and/or enquiries from influencers, MPs, funding bodies etc.
4: High	£100k-250k	Major breaches resulting in censure/ fines, intervention from relevant body and suspension of College autonomy	Extensive local operational issues for a period of one calendar month affecting 10% or more of students and/or staff having some effect on ability to complete required study components and/or critical work Or Failure to achieve the majority of key strategic objectives or to set fitting strategic objectives	Extended media activity (press, TV, social) resulting in negative comment by more than 800 current or potential students and widespread condemnation by influencers, MPs and challenges from funding bodies
5: Catastrophic	>£250k	Fundamental breaches likely to result in the College being unable to maintain income from the funding councils or continue as a going concern	Prolonged operational issues affecting over 80% staff having a sustained effect on ability to complete required study components and/or critical work	Extensive national media coverage likely to result in the College being unable to maintain income from the funding councils or continue as a going concern

Risk Assessment Criteria - Likelihood

"The probability of occurrence"

The following should be used when assessing each risk, considering the likelihood of the risk materialising within a 12-month period.

Likelihood	Criteria
	Probability of occurrence within the next 12 months
1: Improbable	0 to 5%
2: Unlikely	6 to 25%
3: Likely	26 to 50%
4: Very Likely	51 to 75%
5: Probable	>75 %

Identifying and Documenting Controls

Once we have clearly described the risk & we have undertaken the inherent risk assessment, we can assess the severity of the risk by identifying the controls currently in place to manage the risk.

What is a control?

Systematic activities and/or measures such as policies, processes, systems and/or activities that are in place to manage a risk.

Remember - We want to identify **the key controls** which will have the largest effect on reducing the likelihood or impact of a risk

Considerations whilst identifying controls:

Controls	Considerations
Identify the controls	What controls do we currently have in place to manage the risk?
Focus on the controls that are specifically in place to manage the risk and have a material effect on its management	- Do controls prevent the risk from materialising? - If the risk materialises, do the controls reduce the impact of the risk? - Do the controls reduce both impact and likelihood?
Identify which component(s) of the risk the controls effect	How and by how much, e.g. fully prevent a cause leading to a risk event.
Control(s) independence	Are the controls independent or do they rely on other processes or activities to work?
Reliability of the controls	- Could the controls fail or not be available when needed? - Is so, how often could this be the case? - Are they operating effectively? - Have there been any control failures or incidents?
Control limitations	Do the controls have any limitations, e.g. will they only work up to a certain threshold of risk severity?
Redundancy	If one control fails, is there a backup?

Types of controls

Is the control preventative, detective or corrective?

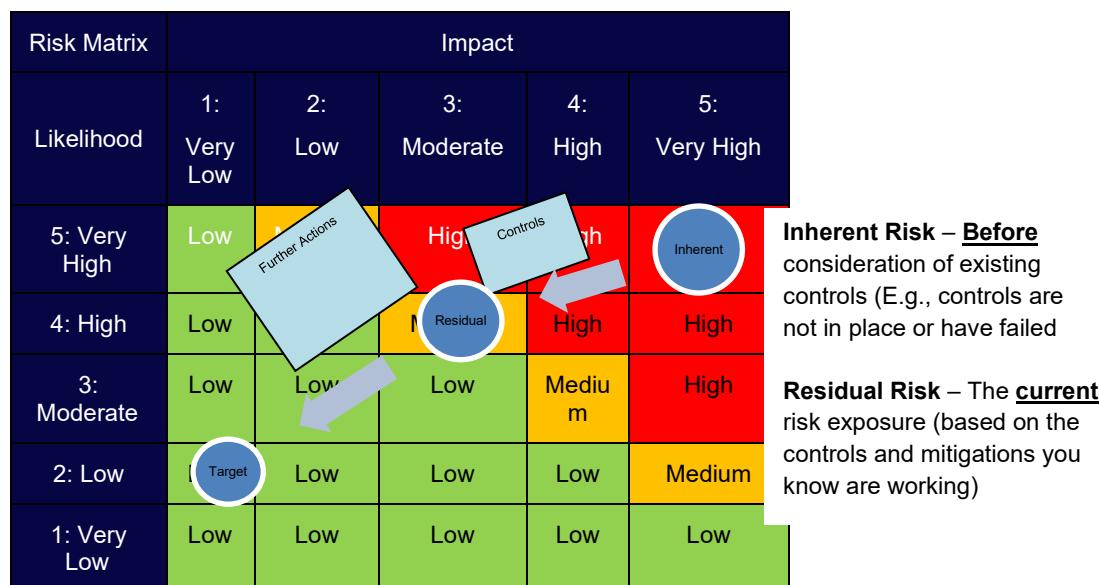
<u>Preventative</u> Controls that attempt to prevent the impact and/or likelihood of the risk occurring.	<u>Detective</u> Controls that monitor when the risk has materialised or is in the process of materialising	<u>Corrective</u> Controls that attempt to reduce the impact or likelihood of the risk, should it materialise
<u>Automated (most reliable)</u> A control activity designed to operate automatically without human intervention	<u>Semi-automated</u> Controls with both automated and manual components	<u>Manual (least reliable)</u> Controls designed to operate using human involvement and interpretation

Risk Assessment Methodology - Inherent, Residual and Target

The potential significance of the organisations exposure to a risk can be better understood by assessing the **Inherent**, **Residual** and **Target** risk positions, which considers the effect of controls as well as further actions.

Controls are defined as systematic preventative activities and/or measures such as policies, processes or systems that are in place to manage a risk.

Each risk should be assessed 3 times on an **Inherent**, **Residual** and **Target** basis.



Risk Response – Evaluating the need for a risk response

Once the target risk position has been established, it should be compared against the residual risk position to understand whether an additional risk response or mitigation is required.

Where the two are not aligned, decisions need to be made to adopt appropriate actions and allocate resources accordingly.

When prioritising the risks to respond to, consider the following:



Risk Response – Identifying and selecting risk response options

A risk response is required by assessing the appropriateness of the residual risk rating and comparing to the target rating. This decision can be made considering the following strategies:

Risk Response Type	Explanation
Treat	Take action to reduce the risk impact and/ or likelihood through enhancing existing controls or implementing additional controls
Transfer	Reduce risk likelihood or impact by transferring or otherwise sharing a portion of the risk. I.e., outsourcing activities or purchase insurance for the activities that give rise to the risk
Terminate	Exit the activities that give rise to a risk, as the risk is unacceptable: - Avoiding or eliminating the risk by deciding not to start or continue with the activity that gives rise to the risk, or by doing something differently, e.g., substitution of an alternative step or activity - This can reduce the risk to zero but may introduce other risks as a result that must be evaluated
Tolerate	No action is taken to affect the risk impact or likelihood. This means that the current risk exposure is accepted. Where no action is taken, this must be captured in the risk acceptance process. (Risk Acceptance Form)

The risk owner is responsible for selecting the appropriate response and developing an action plan.

Risk Response – Action Plan

Actions required to manage a risk must be assigned to an owner. The action owner is responsible for ensuring that individual or multiple actions are implemented, and any delays or challenges are escalated to the risk owner.

The action owner has delegated authority from the risk owner, who maintains the overall accountability for the risk.

Details of all risk action plans, timelines, status and actions owners should be documented in the risk register.

Risk Response	Further Actions Required	Action Owner	Actions Required To Be Completed By (Date)	Actions Implementation Status
Treat Transfer Terminate Tolerate				

Risk Acceptance

Where management elects not to implement all relevant controls or take appropriate mitigating actions for a material risk, the associated risk or control gap must be clearly communicated, documented and accepted by appropriate level of senior management in writing.

A Risk Acceptance form must be completed by the risk owner.

- For low risks, approval must be sought from the appropriate management level in order to accept the risk.
- For high and medium risks, these must be assessed and approved by the Risk Management Committee or The Board to ensure risk acceptance is within our risk appetite and provide transparency.

Risk Acceptance Form

Risk ID	Date	Completed By
Department / Project Impacted		
Risk Rating	☐ Red ☐ Orange ☐ Green	
Risk Description		
Risk Owner		
Inherent Rating (as per the risk scoring matrix)		
Mitigation Response		
Residual Rating (as per the risk scoring matrix)	Impact: (x) ☐ Operational Failure ☐ Financial Loss ☐ Loss of Reputation ☐ Non-compliance (With Regulation or Legislation) Likelihood: (x) ☐ Improbable ☐ Unlikely ☐ Likely ☐ Very Likely ☐ Probable Overall Risk Severity: (x) (Out of a possible 25) Rationale for Acceptance:	
Authorised By	Authorisation Date	
Date Added to Risk Register	Next Review Date	
Further Commentary		

Risk Monitoring and Escalation - Overview

Monitoring and upward escalation of risk information is required in order to review and respond to changes in risk profile in a timely manner. Capturing, monitoring and upward notification of risk information is required in order to review and respond to changes in risk profile in a timely manner.

- **Risk Owners** in the departmental functions are accountable for the management and ongoing monitoring of their risks, including effectiveness of controls to mitigate these. They are also responsible for the identification of control gaps and trends to facilitate key decision making by senior management to ensure we operate within our risk appetite and to prevent risk from materialising.
- **Head of Teams, Programme Leaders and Senior Leadership** are responsible for the ongoing monitoring and review of key controls and the risk profile of the organisation through regular reviews of their risk registers and any control assessment reviews. They are also responsible for the monitoring and reporting risk profile, control quality, and emerging risks which are reported to The Board of Trustees and Risk Management Committee.

Risk Monitoring

Capturing, monitoring and upward notification of risk information is required in order to review and respond to changes in risk profile in a timely manner. It also supports oversight, challenge and decisions on business activities by management.

The **Risk Owner** should establish the frequency of review and monitoring for their risks inline with the risk rating:

Risk Rating	Maximum Time between Risk Reviews
High	3 months
Medium	6 months
Low	12 months

Regular risk monitoring enables the risk owner to:

- Confirm that enhanced or additional controls have been correctly defined and fully implemented
- Confirm that the controls implemented to manage the risk are operating effectively
- Adjust controls as required
- Ensure risk action plans are delivered against committed dates and outcomes
- Identify changes to the risk that can affect risk impact and likelihood, and escalate as necessary
- Ensure any significant changes to the risk are reported or escalated to the appropriate levels

Risk Escalation

Escalation is the required upward notification to a specified person or group of a specific risk, a change in its status or an action to manage it. Risk Escalation does not transfer risk ownership, rather it is to be brought to the attention of the reviewer.

Risks that meet one of the following criteria should be reported **outside** of the formal reporting cycle:

- Risks that have materialised with an impact of severe or High or Catastrophic, or where there is the possibility of contagion between departments or projects
- Risks material to the organisation's reputation, financial situation and overall risk profile
- Material breaches of risk appetite statements and Key Risk Indicators (KRIs)

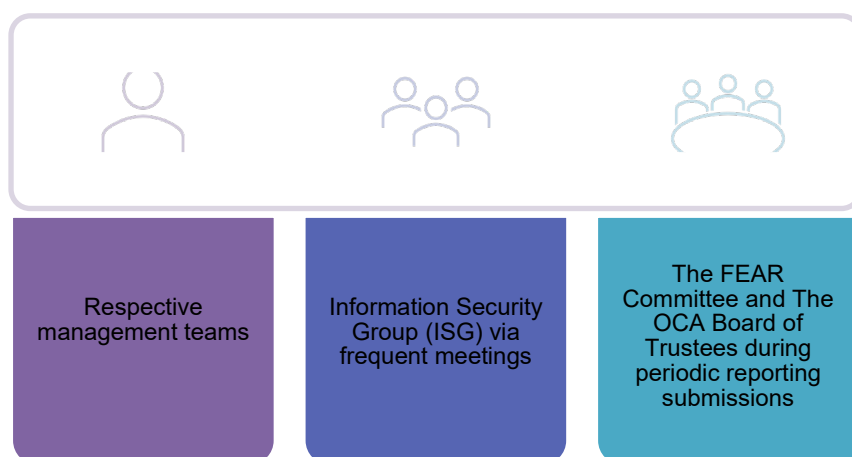
- Externally material reportable events (e.g., major health and safety event, data protection incident, report to regulator)

Risk Escalation and Formal Reporting Cycle

Why do we report on risks?

- To present consistent risk information in a timely manner
- To provide management with insight into the risk environment

Department leaders and functions responsible for managing risk within their area should escalate and report all top risks with details of action plans to:



The following outlines risk reporting that takes place:

Reporting Audience	Frequency	Key Reporting Items
Management Teams	Monthly	Departmental top risks and current action status
Information Security Group (ISG)	Every 1 to 4 weeks.	Cross departmental risks and current action status
FEAR Committee and Board of Trustees	Annually	- Organisational risk profile - Risk appetite reporting - Key risk events - Risk acceptance - Emerging risks