



The Open College of the Arts



The Open
University

Information Security Risk Management Policy

Table of Contents

1.	3
2.	3
3.	4
4.	4
5.	6
6.	6
7.	6
7.1	6
7.2	6
7.3	7
7.4	7
7.5	9
8. Risk Assessment.....	9
8.1 Generalities.....	9
8.2	9
8.3	10
8.4	10
9.	10
9.1 Generalities.....	10
9.2 Identifying Controls for Risk Treatment.....	11
9.3 Risk Treatment Plan.....	11
10.	12
11.	12
12.	13
13.	13
14.	13
Appendix A – Impact Rating Criteria.....	15
Appendix B – Likelihood Rating Criteria	17
Document Control	18
Document Revision History	18

1. Purpose

- 1.1 The purpose of this policy is to specify and communicate guidance and requirements for the effective management of information security risk across The Open College of the Arts (OCA).
- 1.2 An information security risk can be defined as the effect of uncertainty on information security objectives.
- 1.3 The information security objectives of the OCA are the preservation of the confidentiality, integrity and availability of its information. To achieve these objectives, it is vital that all potential information security risks are identified, assessed, prioritised and managed. Where the current risk levels are not acceptable against the OCA's risk acceptance criteria, risk treatment actions need to be identified and implemented.
- 1.4 Information security risk management is applicable to all areas of the OCA for both business-as-usual operations and any change-related initiatives or activities.
- 1.5 The management of information security risks in the OCA is aligned to its corporate risk management framework, which provides a structured and consistent approach to identifying, assessing, evaluating, treating, tracking and communicating risks. This policy outlines the requirements for achieving this in reference to information security risks
- 1.6 See the following policies for related information:
 - [Information Security Policy](#);
 - [Information Security Management System Policy](#);
 - [Information Security Audit and Compliance Policy](#).

2. Scope

- 2.1 This policy applies to the management of all information security risks that could affect the OCA¹.
- 2.2 This policy contains requirements and guidance for the following subject areas with regard to information security risk²:
 - Risk management roles and responsibilities;
 - Risk ownership;
 - Context establishment;
 - Risk criteria;
 - Risk assessment, consisting of:
 - Risk identification;
 - Risk analysis;

¹ Including risks related with the supply chain and cloud security.

² This policy is aligned to ISO/IEC 27005:2022 ("Information security, cybersecurity and privacy protection – Guidance on managing information security risks").

- Risk evaluation;
- Risk treatment;
- Risk register;
- Metrics and reporting;
- Monitoring and review;
- Process improvement.

3. Policy Statement

3.1 The policy of the OCA regarding the management of information security risk is that the OCA shall have an established and efficient information security risk management process in place to identify, assess, treat, track, communicate and report all relevant information security risks. To achieve this, the following requirements shall be met:

- Organisational considerations and the requirements of interested parties shall be taken into consideration for the establishment of the context of information security risk management.
- Risk criteria shall be established and maintained.
- Risk assessment shall be conducted, following established criteria, and consisting of:
 - Risk identification;
 - Risk analysis;
 - Risk evaluation.
- Risk treatment options shall be selected, prioritised and implemented.
- Information about the results of risk assessment and risk treatment shall be documented within an information security risk register.
- Information security risks shall be monitored, reviewed, and re-assessed if and when required.
- Information security risk management metrics shall be defined, regularly obtained and reported.
- Opportunities for improvement of the information security risk management process shall be identified and pursued.

4. Roles and Responsibilities

- **The OCA Board (The Board)** is responsible for:
 - Overseeing and approving the risk management policy and strategy;
 - Approving the process by which the College will determine its risk appetite and keep this under review;

- Agreeing a set of Key Risk Indicators (KRIs) with the Principal / Leadership Team by which those risks identified as significant to OCA can be closely monitored and reviewed.
- **The Principal** is responsible for:
 - Implementing the risk management framework and ensuring compliance with the policy;
 - Providing adequate information in a timely manner to The Board on the status of risks and controls; balance risk against reward; ensure that the College's management of information systems cater for the monitoring of risks through relevant KRIs and early warning mechanisms;
 - Bringing to the immediate attention of The Board any significant risk occurrence or any indication that an occurrence may materialise;
 - Ensuring that the process of day-to-day risk management is adequately documented, including disaster recovery and business continuity plans;
 - Undertaking an annual review of the College's approach to risk management and its effectiveness during the review period; comment on any recommendations for change, areas of weakness identified, and the management rectification actions taken; provide an annual written report to The Board on the findings of the review; and provide assurances and evidence that effective and ongoing systems of internal control are in place.
- **The Finance Employment Audit and Risk Committee (FEAR)** is responsible for overseeing and reviewing the risk management process and reporting to The Board.
- **Heads of Teams, Programme Leaders and Senior Leadership** are responsible for maintaining risks that relate to their domains of responsibility, in line with the college's [Risk Management Procedure](#).

All the OCA employees, contractors and agents shall understand and comply with this policy, including:

- Raising any information security risks identified through the performance of their usual duties and documenting them where appropriate;
- Accepting ownership of information security risks assigned to them, and being responsible for their management;
- Prioritising and carrying out any actions they have been assigned in relation to the treatment of information security risks.

5. Risk Ownership

- 5.1 All information security risks shall be assigned a risk owner. The risk owner shall typically be the individual who owns the service/area that would be most impacted in the event that a stated risk materialises.
- 5.2 Where risk ownership is unclear, it shall be assigned by the RMC, with escalation to The Board if required.
- 5.3 Risk owners shall have appropriate accountability and authority for managing the risks owned by them.

6. Context Establishment

- 6.1 Aspects including but not limited to the OCA's size, organisational structure, position in its sector, legal and regulatory obligations, information security posture and supply chain shall be taken into consideration in the establishment of the context for information security risk management and the definition of risk criteria.
- 6.2 The overall risk appetite of the OCA shall be established and regularly reviewed by The Board, taking into consideration the aspects listed above, and shall feed into the risk acceptance criteria. Currently the risk appetite is established as **Medium**.
- 6.3 Compliance with the requirements of interested parties (both internal and external) shall be taken into consideration and feed into the information security risk assessment and risk treatment processes. (See the [Information Security Management System Policy](#) for related information.)

7. Risk Criteria

7.1 Generalities

- 7.1.1 In alignment to the OCA's risk management framework, the criteria for information security risk assessment shall be based on the concepts of impact and likelihood. Both of these concepts shall be measured using 5-point scales, with qualitative designations and associated numerical values (from 1 to 5).
- 7.1.2 Risk values shall be calculated by multiplying the numerical values of impact and likelihood, as follows:

$$\text{risk} = \text{impact} \times \text{likelihood}$$

- 7.1.3 Qualitative risk ratings shall be applied using a 3-point scale (Low / Medium / High) corresponding to defined bands of risk values.
- 7.1.4 The subsections that follow describe the impact, likelihood and risk scales and criteria in more detail.

7.2 Impact

- 7.2.1 **Impact** (resulting from loss of confidentiality, integrity or availability of information) shall be rated using the following 5-point scale:
 - 1: Insignificant;
 - 2: Low;

- 3: Medium;
- 4: High;
- 5: Catastrophic.

7.2.2 Impact rating using the scale above shall take into consideration the following different types of impact, and consider the highest value among them:

- Financial impact;
- Legal and regulatory (Non-compliance) impact;
- Operational impact;
- Reputational impact;

7.2.3 See Appendix A – Impact Rating Criteria for the details of the rating criteria for each of these types of impact.

7.3 Likelihood

7.3.1 **Likelihood** shall be rated using the following 5-point scale:

- 1: Improbable;
- 2: Unlikely;
- 3: Likely;
- 4: Very Likely;
- 5: Probable.

7.3.2 See Appendix B – Likelihood Rating Criteria for the details of the likelihood rating criteria.

7.4 Risk

7.4.1 The value of the **risk** shall be calculated by applying the formula **risk = impact × likelihood**. This formula implies that a risk value will always be a number between 1 (minimum) and 25 (maximum). Qualitative risk ratings are defined on a 3-point scale based on bands of risk values, as follows:

- Low: 1 to 9;
- Medium: 10 to 12;
- High: 13 to 25;

7.4.2 The following **risk matrix** depicts the relationship between impact, likelihood and risk:

Risk Matrix	Impact
-------------	--------



The Open College of the Arts



The Open
University

Likelihood	1: Very Low	2: Low	3: Moderate	4: High	5: Very High
5: Very High	Low	Medium	High	High	High
4: High	Low	Low	Medium	High	High
3: Moderate	Low	Low	Low	Medium	High
2: Low	Low	Low	Low	Low	Medium
1: Very Low	Low	Low	Low	Low	Low

7.5 Risk Acceptance Criteria

7.5.1 The following criteria shall be applied for risk acceptance:

- Risks with a rating of Low shall be accepted pending approval.
- Risks with a rating of Medium shall be evaluated case by case to decide whether they can be accepted or whether a different risk treatment option must be selected.
- Risks with a rating of High shall not be accepted.

7.5.2 The risk acceptance criteria stated above are aligned to the current risk appetite which has been established by the OCA as **low** and shall be revised if the risk appetite changes.

8. Risk Assessment

8.1 Generalities

8.1.1 Risk assessment consists of:

- Risk identification;
- Risk analysis;
- Risk evaluation.

8.1.2 Risk assessment is a key pillar of the establishment of the OCA's Information Security Management System (ISMS), to enable the achievement of its information security objectives – see the [Information Security Management System Policy](#) for more information.

8.1.3 Risk assessment shall be applied to assess all relevant information security risks, enabling risk owners to prioritise risks aligned with the treatment perspective, based primarily on their impact and likelihood.

8.1.4 Risk assessment can also be performed in a different, more specific context, such as project management, or even on an *ad hoc* basis for a given specific topic. In any case, a consistent approach to performing risk assessments shall be adopted, so that repeated information security risk assessments produce consistent, valid and comparable results.

8.2 Risk Identification

8.2.1 Information security risks can be identified in relation to business-as-usual operations and during the delivery of any change initiatives or activities (e.g. project management, supplier management, security testing, internal or external audit activities) or via information security risk identification workshops run by the IT Manager.

8.2.2 It is the responsibility of all personnel to identify and raise information security risks where they are seen to exist within their respective business area.

8.2.3 The IT Manager shall do the initial review and triage of any new potential information security risks to be considered. The Board shall be responsible for their validation as relevant information security risks that need to be managed.

8.2.4 All validated information security risks shall be:

- Designated using consistent naming criteria;
- Classified using a consistent risk taxonomy and appropriate granularity that enables grouping and comparing risks of similar types;
- Recorded in the information security risk register, which shall be used to capture all the relevant information about each risk (see section 10).

8.3 Risk Analysis

8.3.1 The following requirements for risk analysis shall be met:

- The information assets that need to be assessed, and the corresponding information asset owners, shall be identified.
- Relevant threats and vulnerabilities shall be identified.
- The impacts resulting from losses of confidentiality, integrity and availability shall be evaluated (using the scale and criteria described in subsection 7.2).
- The likelihood of threats exploiting vulnerabilities shall be evaluated (using the scale and criteria described in subsection 7.3).
- The resulting risk ratings shall be determined (using the formula and bands described in subsection 7.4).

8.4 Risk Evaluation

- 8.4.1 For each information security risk being assessed, the risk rating determined by the risk analysis (as described in subsection 8.3) shall be compared with the risk acceptance criteria (described in subsection 7.5) to determine whether the risk can be Tolerated (accepted), or whether a different risk treatment option needs to be selected.
- 8.4.2 Information security risks that cannot be accepted shall be prioritised for risk treatment, in direct relation to the corresponding risk ratings and risk values.

9. Risk Treatment

9.1. Generalities

- 9.1.1. Risk treatment is the process of selecting and implementing measures – risk treatment options – to manage the risk.
- 9.1.2. Effective information security risk treatment options shall be evaluated and selected for risks that require treatment, based on the information from risk assessment.
- 9.1.3. Risk treatment options – other than risk acceptance, which is an informed choice to retain the risk – include:
- Treat - Risk mitigation, consisting of implementing measures to decrease the impact and/or the likelihood of the risk;

- Terminate - Risk avoidance, consisting of discontinuing or not starting the activity that gives rise to the risk;
- Transfer - Risk sharing, consisting of by splitting responsibilities with other parties (e.g. sharing the impact via insurance).

9.2. Identifying Controls for Risk Treatment

9.2.1. The information security controls that are necessary to implement the selected risk treatment options shall be identified. This can include:

- Controls that are not yet in place;
- Controls that are partially in place / not sufficiently effective and need to be improved.

9.2.2. Decisions to implement additional controls shall depend on a comparison of the expected material effect of the controls against the cost of their implementation.

10. Risk Treatment Plan

10.1. The following requirements shall be met:

- An information security risk treatment plan³ shall be developed and include:
 - Each risk to be treated;
 - Selected risk treatment option and corresponding justification;
 - Associated risk treatment actions required, with defined owners and agreed delivery dates.
- The target risk rating expected to result from treatment of each risk (i.e. the remaining risk expected after the risk treatment has been fully implemented) shall be determined.
- Risk owners' approval of the information security risk treatment plan and acceptance of the target risk ratings shall be obtained.
- Approval of the risk treatment plan and target risk ratings by The Board shall be obtained.
- Where new controls are identified and implemented:
 - Policies, procedures and/or standards shall be developed or updated, where relevant, to describe how these controls shall work in practice;
 - Staff shall be made aware of their responsibilities and trained where appropriate.
- In the event that necessary risk treatment controls cannot be implemented within budget or within the appropriate timeframe, the IT Manager shall work with the risk owner and other relevant stakeholders to identify appropriate

³ The risk treatment plan can be contained in the information security risk register (see section 10). However, it can also be documented separately and/or supplemented by additional documentation, as deemed appropriate.

temporary mitigation and set appropriate timescales for necessary risk treatment, with decisions recorded.

11. Risk Register

- 11.1. An information security risk register shall be created and maintained, capturing all the relevant information about information security risks, including information about their assessment and treatment. The information security risk register shall be considered as a subset of the corporate risk register but shall be maintained separately.
- 11.2. The IT Manager shall be responsible for keeping the information security risk register up to date, with support from the risk owners and the owners of risk treatment actions.
- 11.3. As a minimum, the following information shall be recorded and kept up to date, for each information security risk:
 - A unique risk identifier;
 - Risk designation / description;
 - Risk category, aligned to a consistent taxonomy;
 - Risk owner;
 - The initial impact rating, likelihood rating, risk value and risk rating (corresponding to the outcomes of the risk assessment – see section 8);
 - Selected risk treatment option and corresponding justification;
 - Associated risk treatment actions and the following related information:
 - Action owners;
 - Delivery dates;
 - Status per action.
 - The residual risk rating, based on actions already implemented and their evaluated effect in terms of impact and likelihood;
 - The target risk rating, as established in the risk treatment plan.

12. Monitoring and Review

- 12.1. The information security risk register shall be regularly reviewed by The Board. The review by The Board shall be done with a greater emphasis on the risks rated as high, but risks with lower ratings shall not be overlooked and follow the same cadence of review by risk owners as appropriate. The table below establishes the maximum time between reviews of risks based on the risk rating.

Risk Rating	Maximum Time between Risk Reviews
High	3 months

Medium	6 months
Low	12 months

12.2. The review of information security risks shall take into consideration, for each risk:

- The status of implementation of risk treatment actions against the established due dates;
- The residual risk, compared to the agreed target risk;
- The effectiveness of implemented controls in the risk mitigation;
- Whether there is any indication that the risk should be re-assessed, especially where there may be new vulnerabilities / threats to consider.

13. Metrics and Reporting

13.1. Relevant metrics for the information security risk management process shall be defined, regularly obtained and reported to The Board, along with relevant supporting information for review, as applicable.

14. Process Improvement

14.1. Opportunities for improvement of the information security risk management process can mainly arise from:

- Risk management activities, including but not limited to:
 - Risk identification, analysis and evaluation workshops;
 - Risk assessment and treatment reviews;
- Information security audits – see the [Information Security Audit and Compliance Policy](#);
- Analysis of metrics of the information security risk management process.

14.2. The IT Manager shall be responsible for identifying opportunities for process improvement (arising from the above activities, or any others) and proposing the implementation of the corresponding changes to The Board, which shall be responsible for their review and approval.

15. Policy Review Date

15.1. This policy shall be reviewed and appropriately updated on an annual basis. It shall also be reviewed and appropriately updated when there are any changes to relevant regulations on information security and/or data protection.

Appendix A – Impact Rating Criteria

The following table reproduces the detailed criteria for impact rating for the different types of impact.

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 regulatory intervention	Minor local operational issues over a 1-week period affecting 10% or more of students and/or staff having some effect on ability to complete study activities and/or routine work Or Several key College objectives or core College activities not	National media activity (press, TV, social media) lasting more than 2 weeks resulting in negative comment by up to 600 current and potential students and/or enquiries from influencers, MPs, funding bodies etc.

			achieved by a due date	
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

Appendix B – Likelihood Rating Criteria

The following table reproduces the detailed criteria for likelihood rating.

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 %

Document Control

Document Control	
Title:	Information Security Risk Management Policy
Reference:	
Version:	1.0
Date:	
Status:	Draft
Owner:	IT Manager
Classification:	Internal

Document Revision History

Version	Date	Author	Summary of changes
0.1			Initial draft
1.0	06/11/2025	Dean Humphreys	Final revisions approved and version updated to 1.0 for release