

## **Risk Management Policy**

Risk management encompasses the identification, analysis and response to risk factors that form part of Inspire Education Group's (IEG) operating environment. Effective risk management means attempting to control, as much as possible, future outcomes by acting proactively, rather than reactively. Good risk management offers the potential to reduce both the possibility of the risk occurring and the potential impact, should it occur. The purpose of this policy is to provide a framework for the Group on which to manage the risks inherent in delivering operations. This provides a consistency of approach in identifying, evaluating and monitoring risk, removing as far as is possible individual bias and risk appetite.

By implementing the risk management policy, the Group aims to:

- Provide continuous, high-quality services to all IEG students
- Use appropriate identification and analysis techniques to identify risks to the Group and determine the long-term and short-term impact
- Prioritise and implement control measures to reduce or remove risks
- Protect and promote the reputation of the Group
- Through the use of education, training and communication, develop and maintain a structured risk management culture, where risk is considered in the decision-making process
- Reduce the long-term cost of risk to the Group
- Report on and review the risk management policy in accordance with best practice guidelines

### **Scope**

The Policy applies to all activities undertaken by the Group, including those activities undertaken through subsidiary companies and subcontractors.

### **The Policy Statement**

IEG has a moral and statutory duty to take all reasonable actions to safeguard its employees, assets and the public and ensure that it is not financially or operationally disrupted. It will meet this duty by ensuring that risk management plays an integral part in the governance of the Group at a strategic and operational level.

The Executive Team has the responsibility to plan and systematically approach the identification, analysis and control of risk.

### **Responsibilities**

#### **Governors**

- Approve the Risk Management Policy
- Monitor the effectiveness of risk management throughout the Group
- Challenge the view of risk presented by the Risk Management Group and the Executive, if appropriate

**Policy Name:** RISK001 – Risk Management Policy

**Responsibility:** Chief Financial Officer

**Issue:** March 2025

**Approved by:** IEG Board

**Review Date:** March 2027

**Site:** Inspire Insight, IEG Website

- Review the movements in primary risks each term (through the Audit Committee), and the Board at least annually
- Monitor the effectiveness of risk management arrangements through internal audit work and other reports to the Audit Committee
- Consider the Annual Report to the Board by the Audit Committee

### **Group Executive**

- Ensure that the college manages risk systematically, economically and effectively to deliver both Group strategic aims and compliance with legislation
- Review primary risks monthly
- Develop a risk management culture and communicate it across all disciplines
- Promote and oversee the implementation of the policy across the Group

### **Risk Management Group (RMG)**

The RMG meets half-termly to review the risks for the Group. Consisting of the Executive Team, the Vice Principals, the Assistant Principal, and, where relevant, Group Directors. Generally, these are the risk owners. The role of the group is to:

- Support the Group to develop, implement and review the risk management policy
- Share the experience of managing risk
- Promote, support and oversee its implementation across the Group
- Identify any resources required to support the implementation of this policy
- Identify and communicate risk issues to the different service areas
- Consider new and emerging risks
- Review 'near misses' and risks that have crystallised, and reconsider associated procedures
- Monitor, review and report the effectiveness of the risk management policy
- Share good practice on all elements of risk management

### **Managers**

- Create and implement a control environment to manage risks in each particular service area
- To recommend the necessary training on risk management for the employees in the section. To share relevant information with other service sections
- To identify any risk management issues in their service area
- To provide feedback to the Risk Management Group on their experience of implementing the policy and their perceptions of the effectiveness of the policy

### **Related Documentation**

- Appendix 1 – Risk Management Procedures
- Appendix 2 – Likelihood and Impact Definitions for IEG and UCP
- HS001 - Health & Safety Policy
- Governance Documentation

## **Risk Management Procedure**

### **Risk Management Approach**

Failure to pay proper attention to the likelihood and consequences of risk could cause great damage to the Group. Some examples of damage include service disruption, threat to public health, financial costs, compensation claims and bad publicity. Risk management is consequently a key part of the Group's approach to the delivery of sound governance.

Increasing risk awareness is a very important part of implementing risk management, as it helps to develop a risk management culture.

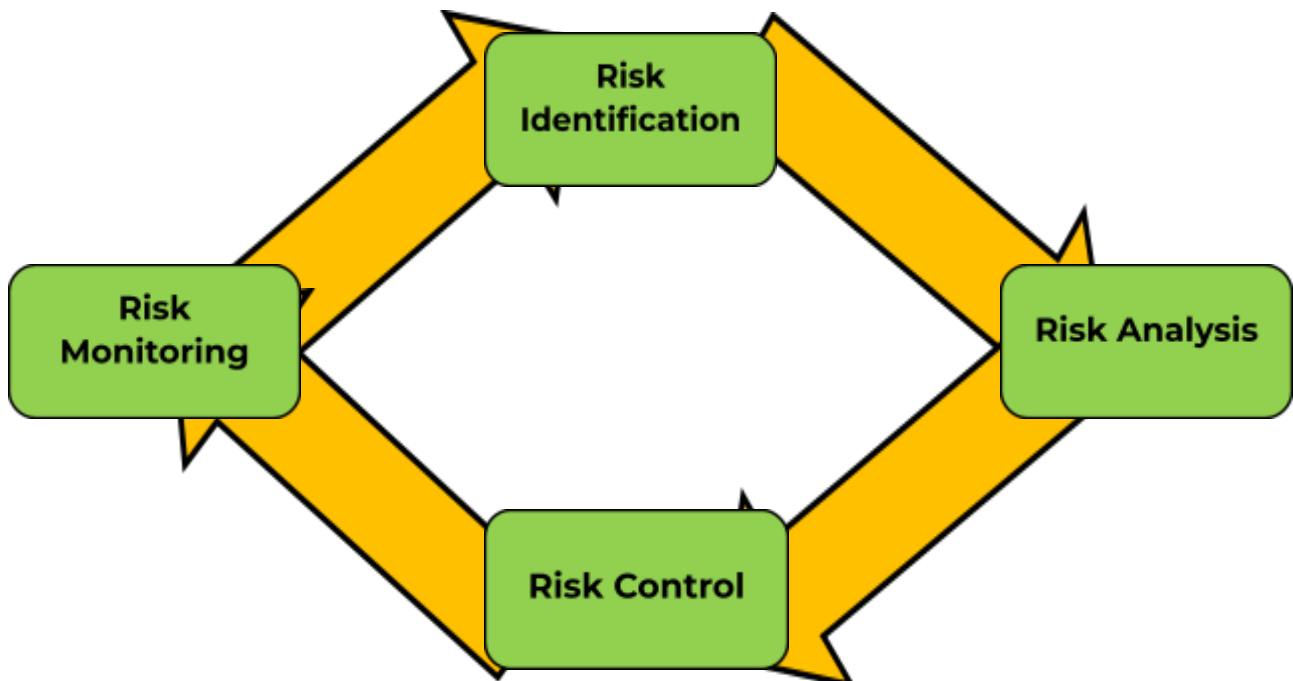
Risk management should not be seen as a "bolt on", it should be integral to policy planning and operational management within the Group. Applying the risk management cycle will help key officers make informed decisions about the appropriateness of adopting policy or service delivery options.

The benefits of managing risk include:

- Improved Strategic Management
- Better informed decision making in the selection of strategic objectives and related targets as a result of the risk identification, analysis, control and monitoring process
- Enhanced ability to deliver against more realistic and attainable objectives and targets
- Improved Operational Management
- Decline in the number of interruptions to service delivery

### **The Risk Management Cycle**

The risk management cycle will generate information that will help to ensure that risks can be avoided or minimised in the future. It will also inform judgements on the balance to be reached between self-insurance and external protection.



**Policy Name:** RISK001 – Risk Management Policy - Risk Procedure - Appendix 1

**Responsibility:** Chief Financial Officer

**Issue:** March 2025

**Approved by:** IEG Board

**Review Date:** March 2027

**Site:** Inspire Insights, IEG Website

## Risk Appetite

IEG is committed to providing a safe and supportive learning environment for all students. Our risk appetite is defined as follows:

- **Student and Staff Safety:** We have a zero tolerance for risks that could jeopardise student or staff safety, including physical harm and safeguarding concerns.
- **Academic Achievement:** We have a low tolerance for risks that could negatively impact student academic achievement, such as inadequate teaching resources or ineffective curriculum delivery. We accept a moderate level of risk associated with innovative teaching methodologies, provided they are supported by research and evaluation.
- **Financial Stability:** We have a low tolerance for financial risks that could threaten the district's long-term financial stability. We accept a moderate level of risk associated with seeking grants and other funding opportunities.
- **Reputational Risk:** We have a low tolerance for risks that could damage the Group's reputation, such as negative media coverage or student satisfaction.
- **Operational Efficiency:** We have a moderate tolerance when new corporate systems and processes in a controlled manner
- **IT Systems:** We have a low tolerance for risks that could significantly disrupt critical technology systems, such as the student information system or the learning management platform. We accept a moderate level of risk for short, planned outages for maintenance and upgrades.
- **Technology Adoption:** We have a moderate tolerance for risks associated with adopting new technologies, provided that appropriate training and support are provided to users. We encourage exploration and innovation in technology use, but with careful planning and evaluation.
- **Cybersecurity:** We have a low tolerance for cybersecurity risks, including phishing attacks, malware, and data breaches. We invest in robust security measures and provide regular training to staff and students on cybersecurity best practices.

## Risk Identification

Identifying and understanding the risks that the Group faces is essential for informed decisions to be made about policies or service delivery methods. The risk associated with these decisions can then be effectively managed.

Risks can be identified through:

- Team Meetings (including Executive)
- Health and Safety Audits
- Review of accident and near-miss reports
- Review of strategic objectives
- Risk Management Group
- Governor feedback
- Internal Audit
- Sector-wide training and networking

**Policy Name:** RISK001 – Risk Management Policy - Risk Procedure - Appendix 1

**Responsibility:** Chief Financial Officer

**Issue:** March 2025

**Approved by:** IEG Board

**Review Date:** March 2027

**Site:** Inspire Insights, IEG Website

## Risk Analysis

Once the risks have been identified, they need to be systematically analysed using proven analysis techniques and all available data on the potential frequency/likelihood and impact/consequences of events. If a risk is seen to be unacceptable, steps need to be taken to control or respond to it.

## Response to Risks

After identifying a risk, it is good practice to start by considering the response to the risk. As most risks cannot be eliminated altogether, judgements have to be made as to what level of risks is acceptable. There are four categories of response: transfer, treat, terminate and tolerate. Details of each response can be found in the following table:

Response	Description
Transfer	Risks are transferred to an insurer, e.g. legal liability. However, it must be remembered that this is not possible for all risks. Some service delivery risks can also be transferred to a partner or contractor by way of a formal contract or written agreement. Some risks, however, cannot be transferred, for example, reputational risks.
Treat	Risks need additional treatments (controls) to reduce the likelihood and impact levels. This response is most likely where the risk has been identified as a high risk due to the likelihood and impact levels.
Terminate	A risk is identified as being so serious that there is no other option than to terminate the activity generating the risk.
Tolerate	The controls in place reduce the likelihood and impact levels to a tolerable level. It is therefore decided to <i>tolerate</i> the risk.

## **Risk Control**

For those risks that cannot be terminated or transferred, risk control is the process of taking actions to reduce the chance of a risk occurring and/or the impact of the risk should it occur. These factors should be reduced to the lowest point where the action taken is still economical. Risk control often requires projects to be implemented or operating procedures to be revised.

## **Risk Monitoring**

The main tools used to monitor risk are the Strategic Risk Board Assurance Framework and Contingency Risk Registers. These are reviewed by the Board, and to a greater level of detail by the Audit Committee.

Internally, the Strategic risks are reviewed by the Executive monthly, and the risk management group meets every term.

## **Strategic Risks**

The Group uses 1<sup>st</sup>, 2<sup>nd</sup>, and 3<sup>rd</sup> lines of defence to manage strategic risks.

- 1<sup>st</sup> line of defence – Management Controls/Policies and Procedures/Staff Training
- 2<sup>nd</sup> line of defence – Financial Controls/Security/Risk Management/Quality/Inspection
- 3<sup>rd</sup> line of defence – Internal Audit

For each risk, an action plan is given to show how the risk is being actively managed.

## **Contingency Risks**

IEG uses a risk register, to identify the risk and describe the controls and mitigations for each risk. This risk register is reviewed by the Risk Management Group termly.

To complete the risk management process, where relevant, risk control measures lead to revisions in operating procedures.

### Risk Scoring Matrix

Once it has been established that a risk cannot be transferred or terminated a risk is scored at its inherent level (with no control or management), and residual level (after control measures have been applied).

The scoring is undertaken on the basis of both likelihood and impact, using the matrix below. Appendix 2 details the levels of severity that apply to each score for both impact and likelihood.

Impact	6 Very High Impact	6	12	18	24	30	36
	5 High Impact	5	10	15	20	25	30
	4 Medium Impact	4	8	12	16	20	24
	3 Low Impact	3	6	9	12	15	18
	2 Very Low Impact	2	4	6	8	10	12
	1 Negligible Impact	1	2	3	4	5	6
		1 Almost Impossible	2 Very Low	3 Low	4 Medium	5 High	6 Very High
Likelihood							

Where the residual score is 18 or above, it is likely that this will be classed as a strategic risk.

Red	Significant focus to be monitored monthly
Amber	Monitor at least termly
Green	Monitor at least annually

## IEG Likelihood and Impact Definitions

<b>IMPACT</b>	<b>FINANCIAL:</b>	<b>SERVICE QUALITY:</b>	<b>H&amp;S:</b>	<b>REPUTATION:</b>
<b>1 Negligible Impact</b>	Less than £5k	Negligible Effects on service	No injury	No Effects on reputation
<b>2 Very Low Impact</b>	£5k to £20k	Marginally impaired, a slight adjustment to service delivery is required.	Very minor injury	Minimal effect
<b>3 Low Impact</b>	£20k to £50k	Service quality is impaired in isolated areas, leading to changes in service delivery required to maintain quality.	Minor injury	Slight reputation damage arising
<b>4 Medium Impact</b>	£50k to £250k	Significant reduction in service quality expected.	Significant injury	Reputation damage is uncomfortable for the Group
<b>5 High Impact</b>	£250k to £500k	Service quality cannot be maintained, such that there is a need to reassess resource allocation	Serious injury	Reputation damage occurs with Key Stakeholders
<b>6 Very High Impact</b>	£500K+	Complete failure of services	Fatality	Reputation damage is irrecoverable

<b>LIKELIHOOD</b>	
1 Almost Impossible	Very unlikely to occur
2 Very Low	Unlikely to occur
3 Low	May occur very infrequently
4 Medium	Likely to occur infrequently
5 High	Likely to occur within the next three years
6 Very High	Very likely to occur in the next 12 months





## Likelihood and Impact Definitions – UCP

To be used for subsidiary Boards only, not reporting of subsidiary risks to the IEG Board

<b>IMPACT</b>	<b>Financial: UCP</b>	<b>Service Quality:</b>	<b>H&amp;S:</b>	<b>Reputation:</b>
<b>1 Negligible Impact</b>	Less than £10k	Negligible Effects on service	No injury	No Effects on reputation
<b>2 Very Low Impact</b>	£10k to £50k	Marginally impaired, A slight adjustment to service delivery is required.	Very minor injury	Minimal effect
<b>3 Low Impact</b>	£50k to £100k	Service quality is impaired in isolated areas, leading to changes in service delivery required to maintain quality.	Minor injury	Slight reputation damage arising
<b>4 Medium Impact</b>	£100k to £150k	Significant reduction in service quality expected.	Significant injury	Reputation damage is uncomfortable for the College
<b>5 High Impact</b>	£150k to £250k	Service quality cannot be maintained, such that there is a need to reassess resource allocation	Serious injury	Reputation damage occurs with Key Stakeholders
<b>6 Very High Impact</b>	£250k+	Complete failure of services	Fatality	Reputation damage is irrecoverable

<b>LIKELIHOOD</b>	
1 Almost Impossible	Very unlikely to occur
2 Very Low	Unlikely to occur
3 Low	May occur very infrequently
4 Medium	Likely to occur infrequently
5 High	Likely to occur within the next three years
6 Very High	Very likely to occur in the next 12 months