Operational Risk Policy and Procedures

Document Control

Document Owner: Nina Cranfield

Approval Date: 11/08/2025
Effective Date: 11/08/2025

Review Date: September 2026

Note: This policy must be reviewed annually or when significant changes occur to ensure its continued relevance and effectiveness.

Date	Version	Author	Reason for amendment
11/08/2025	1.0	Claire Robinson	Create formalised document.

1. Introduction

Operational Risk Management (ORM) refers to the process of identifying, assessing, mitigating, and monitoring risks arising from inadequate or failed processes, systems, people, or external events that could impact One-Eighty's operations, service users, or reputation. This policy outlines the approach to managing operational risks across all functions of the business to ensure continuity, quality, and integrity of service delivery.

2. Scope

This Policy applies to all employees, subcontractors, volunteers and students on placement working with One-Eighty, including those employed on a permanent, temporary, part-time, or casual basis. It also applies to all applicants for employment, volunteers, and interns. Operational risk management is relevant to all business activities, processes, systems, and personnel.

3. Policy Statement

One-Eighty is committed to maintaining a proactive approach to operational risk management, promoting an organisational culture where risks are regularly assessed and mitigated. This policy is designed to ensure that risks are identified in advance, managed effectively, and that appropriate corrective measures are in place to avoid any adverse impact on One-Eighty's service users or reputation.

4. Procedures

One-Eighty recognises that managing operational risks is essential to ensuring business continuity and protecting the reputation of the organisation. This policy sets out the procedures to identify, assess, mitigate, and monitor operational risks in all business activities.

4.1. Identifying Operational Risks

Operational risks can arise from various sources, including:

- **Processes:** Failures or inefficiencies in processes that may lead to delays, errors, or interruptions in service delivery.
- **Systems:** Issues related to technology systems such as failures, cyber-attacks, or data breaches.
- **People:** Human error, non-compliance, or malicious actions.
- **External events:** Natural disasters, regulatory changes, or supply chain disruptions.

Staff at all levels are encouraged to report any potential risks they identify through internal channels. A structured risk identification process should be carried out during regular business reviews and any significant changes in processes or systems.

4.2. Assessing Operational Risks

Once a potential risk is identified, it must be assessed in terms of:

- Likelihood: The probability of the risk occurring.
- Impact: The severity of the impact on business operations, clients, customers, and reputation if the risk materialises.

Each risk should be assigned a risk rating (high, medium, low) based on these factors. The assessment should consider both direct and indirect effects on the organisation and its stakeholders.

4.3. Mitigating Operational Risks

Mitigation strategies must be developed to address any identified risks. These may include:

- Preventative measures: Implementing safeguards or controls to reduce the likelihood of the risk occurring (e.g., additional training, system updates, policy changes).
- Contingency planning: Preparing responses to reduce the impact should the risk occur (e.g., backup systems, alternate suppliers, disaster recovery plans).

Risk mitigation strategies should be documented and monitored to ensure they are implemented and remain effective over time.

4.4. Monitoring and Reporting

Operational risks must be continuously monitored to identify any changes or new emerging risks. Regular reporting on operational risks should be provided to management and relevant stakeholders.

Each locality is responsible for maintaining an operational risk register, which is reviewed at regular intervals. Any significant risks or changes should be escalated to senior management for review and action.

4.5. Can Risks be Raised Anonymously?

While anonymous reporting of risks is discouraged, staff may raise concerns anonymously if they believe it is necessary. However, anonymity may hinder the ability to investigate or mitigate the risk effectively. Where anonymity is chosen, the reporting person's identity will be kept confidential unless disclosure is required by law.

4.6. How to Report Operational Risks

Risks should be reported to the COO as soon as they are identified. Reports can be made verbally or in writing and should include detailed information such as the nature of the risk, any supporting evidence, and potential consequences.

An appointed risk officer or the risk management team will review the report, and where necessary, further investigations will be carried out to determine the best course of action.

4.7. Response to Operational Risk Reports

Once a risk is reported, it will be reviewed and evaluated by the risk management team. This includes:

- Assessing the risk level.
- Determining the appropriate response or mitigation actions.
- Communicating any necessary steps to relevant stakeholders.

Follow-up actions and any outcomes will be documented, and the reporting party will be kept informed where possible. If the risk cannot be addressed satisfactorily, escalation procedures will be followed.

5. Status of this Policy

This policy does not confer contractual rights to any staff member and may be updated or amended as necessary. Changes will be communicated to all affected individuals.

6. Legislation and Guidance

This policy is guided by relevant industry standards and best practices, including ISO 31000:2018– Risk Management Guidelines. It is aligned with regulatory requirements to ensure the safety and resilience of the business and its operations.

7. Review, Maintenance and Continuous Improvement

The COO will maintain a register of all identified operational risks. This will be reviewed on a quarterly basis to ensure that risks are managed appropriately, and any necessary adjustments are made to the risk management strategy. This policy shall be reviewed annually or following significant changes to systems, networks, or threat landscapes. Lessons learned will be incorporated into the policy to improve the overall process. Regular reviews will ensure the policy remains relevant and effective.

8. Exceptions

Any exceptions to this policy must be formally documented and approved by the relevant management team. Exceptions will only be granted where there is a legitimate business need, and appropriate compensating controls must be implemented.

9. Enforcement

Non-compliance with this policy may result in disciplinary actions, in line with One-Eighty disciplinary procedures, ranging from corrective actions to termination of employment or contracts, as appropriate.

10. Authorisation & Document Control

Document Title	Operational Risk Policy and Procedures			Status	Live
Classification	Internal and external on request	Last Review	September 2025	Next Review	September 2026

Authorisation	Responsible Person or Body
Document Owner	Nina Cranfield
Authorised By	Nina Cranfield

Version History

Version	Author	Issued	Summary of Changes
1.0	Claire Robinson	11/08/2025	Creation of formalised policy