RCN Group Risk Management Policy.

<table>
<thead>
<tr>
<th>Authors:</th>
<th>Steve Cope</th>
</tr>
</thead>
<tbody>
<tr>
<td>Role:</td>
<td>Operational Planning Advisor</td>
</tr>
<tr>
<td>Version:</td>
<td>Version 10</td>
</tr>
<tr>
<td>Approved by:</td>
<td>Audit Committee</td>
</tr>
<tr>
<td>Approval date:</td>
<td>12 November 2018</td>
</tr>
<tr>
<td>Review date:</td>
<td>November 2020</td>
</tr>
</tbody>
</table>

The information contained in this document is the property of The Royal College of Nursing. The holder of this document shall keep the information within the document confidential and protect it from disclosure to third parties.
Version control.

This document will be stored on the RCN Intranet, and accessed from there. Any paper copies of the document should be considered ‘uncontrolled version’.

All updates and reissues of this document must be managed through the Operational Planning Advisor.

Table of contents.

1 Summary........................................................................................................................................3
2 RCN Policy Statement. .......................................................................................................................3
3 Summarising the risk framework........................................................................................................4
4 Areas of risk to consider, and their priority.........................................................................................6
5 Risk appetite and thresholds................................................................................................................6
6 Measuring, monitoring, and reporting. ................................................................................................7
7 Risks from partnerships and collaborations (internal and external) ...................................................8
8 Risk management responsibilities. .......................................................................................................8
9 Risk Owners.........................................................................................................................................8
10 Communication requirements. ...........................................................................................................9
11 Appendix A: layout of the group risk register and report.................................................................10
12 Appendix B: Risk triggers....................................................................................................................13
13 Appendix C: Roles having direct responsibilities for risk management. .........................................14
1 Summary.

This policy provides guidance on

- The RCN Group policy statement.
- Risk as part of our integrated management framework.
- Predominant types of risk.
- Risk appetite.
- Risk preparedness.
- Gross risk and mitigated risk.
- Risk measurement, monitoring, and reporting.
- Roles having responsibility for risk management.

Supporting information on strategic & operational processes, documentation, and tools is available on the Intranet.

2 RCN Policy Statement.

The RCN Group recognises that having a risk management framework is best practice and that, to be truly effective, risk management must be integrated into the organisation's culture and its other management processes. This ensures foreseeable risks are identified, assessed and (where appropriate) reduced or eliminated. It also ensures the knowledge of those risks forms part of our business intelligence, project planning and budgeting, as well as other decision-making activities.

The group recognises the benefits of a culture where risk is understood and effectively managed.

The group acknowledges the benefits to the organisation and its members that are gained from understanding the types of risk that influence the delivery of its services.
Consequently, the group will:

a. Ensure processes exist to identify, evaluate, prioritise, and monitor significant risks.

b. Ensure the environment in which we operate is monitored for new risks, and ensure the potential impact of existing risks is identified.

c. Ensure that information concerning risks and their potential impacts is communicated effectively - both within the organisation and amongst stakeholders.

d. Ensure our employees recognise the increased organisational effectiveness that can be achieved from managing risk.

e. Ensure our employees recognise the need to include their knowledge of risks in to other management and decision-making processes.

3 Summarising the risk framework.

The group risk management framework is the means by which potential risks are identified, categorised, and reported according to the action required: i.e.

a. Avoidance: changing the activity to eliminate a risk.

b. Transfer: shifting the impact of a risk to another party.

c. Mitigation: reducing probability and/or impact of a risk.

d. Acceptance: agreeing to accept (actively or passively) the consequences of a risk.

To achieve this, risk information flows around the organisation as shown below;
Identifying, monitoring, and communicating corporate risks throughout the RCN Group.

Start

Each Group project or department creates its own risk register(s).

Significant risks are escalated to a corresponding Directorate or Committee risk register.

Group Strategic risks are further escalated to RCN, Foundation, or RCNi risk register.

Group Secretary

RCN

Foundation

RCNi

Management

Executive Team (ET)

ET consider those appetite levels when they are assessing which hazards are Group risks.

ET maintain & review the Group risk register - and publish a summary report.

ET's risk report is presented to Council.

Council

ET’s risk report is presented to Audit Committee.

Audit Committee consider the ET risk report alongside their own judgements, and inform Council.

Risk registers describe the hazard and its effect on the Annual Plan deliverables. They quantify the risk impact and likelihood, risk direction, and (mis)alignment with risk appetite ... Plus mitigating actions we have taken and any work yet to be done ... and indicate how well prepared we are to mitigate each risk.

Risk registers are used to expose Corporate risks.
4 Areas of risk to consider, and their priority.

The most prevalent and significant types of risk the Group faces are;

- Financial / Economic (including commercial activities)
- Reputation
- Governance and Management
- Legal
- Membership
- Compliance
- Technology
- Infrastructure
- Employee

At any one time, the priority of each of these should be recognised amongst the group Executives, Audit Committee, and Council – who should then communicate to staff which types of risk have the greatest bearing on achieving the organisation's operational and strategic deliverables.

5 Risk appetite and thresholds.

Employees must recognise that some activities and circumstances carry such significant levels of risk that they lead to the group being put in harm's way. The aim is not to completely avoid such activities or circumstances - in fact, there may be instances where it is a 'risk worth taking'. However, employees need to recognise such risks, understand the implications for the organisation, and seek approval before proceeding further.

The group executives assist staff in making these decisions by defining the appetite for a number of risk types, and by setting high and low thresholds beyond which a risk will become problematic.
At the time of publishing the risk appetites are:

![Our Appetite for Risk](image)

<table>
<thead>
<tr>
<th></th>
<th>Unacceptable to take risk</th>
<th>Willingness to take risk</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reputation &amp; Brand</td>
<td>&lt;</td>
<td>&gt;</td>
</tr>
<tr>
<td>Compliance</td>
<td>&lt;</td>
<td>&gt;</td>
</tr>
<tr>
<td>Financial</td>
<td>&lt;</td>
<td>&gt;</td>
</tr>
<tr>
<td>Change</td>
<td>&lt;</td>
<td>&gt;</td>
</tr>
<tr>
<td>Our People and Culture</td>
<td>&lt;</td>
<td>&gt;</td>
</tr>
<tr>
<td>Membership</td>
<td>&lt;</td>
<td>&gt;</td>
</tr>
<tr>
<td>Partnerships and Collaboration</td>
<td>&lt;</td>
<td>&gt;</td>
</tr>
<tr>
<td>Commercial</td>
<td>&lt;</td>
<td>&gt;</td>
</tr>
<tr>
<td>Member/Customer Experience</td>
<td>&lt;</td>
<td>&gt;</td>
</tr>
</tbody>
</table>

6 Measuring, monitoring, and reporting.

The group recognises the benefits of a collective, objective approach to risk; this ensures that the views of any dominant individuals are balanced by a broader organisational perspective, and allowing previous experience to be represented during risk reviews.

A risk register template (Appendix A) is used to capture information from the risk reviews undertaken by staff, executives, committees, and council. The template is one way in which risk information is then communicated amongst the group.
7 Risks from partnerships and collaborations (internal and external).

The group register should not be restricted solely to internal activities, but should also reflect any corporate risk arising from partnerships and collaborations.

Partners have a 'duty to inform' each another of any notable changes to their risk status, or any changes to the tools or processes they use to assess risk.

To facilitate this, once a year the internal audits of RCN Foundation & RCN Publishing will be presented to the Audit Committee, highlighting any risk issues. RCN Publishing and RCN Foundation management will attend that Audit Committee meeting.

8 Risk management responsibilities.

To be truly effective, risk management requires active ownership and involvement. There is a requirement for risks to be understood, identified, monitored and communicated by all staff and members, recognising that their activities - and the activities of others - should not put the group "in harm's way".

Appendix C outlines the roles deemed to have direct responsibilities for risk management; including Council & Committees, Group Executives, other staff, and external partners.

9 Risk Owners

a. The corporate risk register and all local risk registers will not only identify risks and their impact, but will assign a named owner to each risk.
b. The named owner has responsibility for communicating the status of that risk to the organisation and any auditors.
c. The risk owner will ensure the corporate risk register accurately describes the implications of the risk, provides assurance that appropriate controls and actions are in place, and provides planned dates for completion of those actions.

10 Communication requirements.

The group will ensure processes and tools are in place to allow effective communication of risk management policy, priorities, and findings … across organisational hierarchies, departments, and functions.
11 Appendix A: layout of the group risk register and report.
<table>
<thead>
<tr>
<th>Summary Title</th>
<th>Description</th>
<th>Annual Plan/Year</th>
<th>Risk appetite Category</th>
<th>Appraoch</th>
<th>Owner</th>
<th>Mitigating actions</th>
<th>Gross Impact</th>
<th>Gross Likelihood</th>
<th>Gross risk indicator</th>
<th>Preparedness indicator</th>
<th>Risk treatment strategy</th>
<th>Mitigated impact</th>
<th>Mitigated Likelihood</th>
<th>Mitigated risk indicator</th>
<th>Mitigated velocity of impact</th>
</tr>
</thead>
</table>
| Gross Finances | Risk: Group Finance  
Increase in 50% subscription and 50% foundation donations in FY1 member funded debt now leads to decline in personal subscription revenue and donations.  
50% is unable to manage transition of international and business from 60% to 80%.  
Decline in 54% classified revenue continues throughout FY1 resulting in classified being 800% under budget by year end.  
The foundation continues to rely heavily on returns from its investment income to support its activities.  
The delay in CTI and the impact of risks delaying progress on a number of fundraising activities. | 2016 | Financial | Low | Davis | PEN campaign to demonstrate value of package of journal, learning & portfolio to the focus throughout 2017.  
additional contribution for grants to be agreed with ICMS for 2017 to refresh investments made due to these being classified on non-disclosure.  
Capital with strategic group to be made - based on 201/2020.  
Foundation is able to determine future direction of publication.  
Foundation is able to plan in place and longer-term fundraising planning being developed.  
Research and prioritizing the need to diversify sources of income in time.  
A fundraising plan in place and a fundraising plan is needed with a focus on increasing income. | Serious | High | Medium | 10 | Agreed contribution of £350,000 from ICMS in 2021.  
Package and product review needed, sales product strategy and sales team implementation.  
Agreed to implement.  
Agreed to implement.  
AGM with Executive Team and Council. | Serious | Very High | Medium |
| Compliance | Risk: Information management, Data protection and more  
A significant failure in IT infrastructure or a key IT system will result in loss of information, inability to operate effectively and/or financial or other loss or potential.  
Without a clear, Group-wide information strategy linking information management, business intelligence, IT, digital, records management and information governance, we will not be able to manage our information and the risks associated with it.  
We are not able to address the risks presented by the implementation of the General Data Protection Regulation (GDPR). | 2016 | Compliance | High | Doburn | Technology assessment performed regularly to identify areas of need and opportunities for improvement.  
Improvements in place across major projects approved configuration changes, application updates and the development and delivery of new systems.  
Clear policies and procedures in place to resolve Key Systems with a raised incident and incident activity.  
Consideration into appointment of a Chief Information Officer role or equivalent.  
Information is held planned to inform development of information strategy and implementation plan.  
As part of this work GDA key performance indicators commissioned and Action Plan to be developed. | Serious | High | Fact | 0 | Ongoing investment programme in core infrastructure, office and mobile solutions to support the store environment.  
ongoing annual review and testing of our corporate and local GDA and disaster recovery plans.  
Independent information Audit to form the basis of an action plan to address high/medium risks identified. | Very Serious | High | Fact |
The template contents should ensure information;

- is restricted to a manageable and focused set of key risks
- is clear and concise
- shows changes to the document made since the previous version
- shows risks of particular interest to Executive Team, Committees, or Council.

Each risk on the register must outline its root cause(s) and identify the subsequent effects that may be felt – both before and after any mitigation.

The register assesses the scope and scale of each risk, measuring the likelihood of occurrence, the risk’s overall impact, and the speed at which that impact would make itself felt. Importantly, the register also identifies the organisation's degree of preparedness for each risk.

Active (Gross) risks have a direct, often immediate impact on the organisation. In its early stages the full implications of an active risk might not be understood - and even when fully understood the risk requires close monitoring and an action plan. The gross impact, likelihood, velocity and preparedness scores we assign to a risk indicate the levels posed before we take any steps to manage it.

By contrast, residual risk is the degree of risk remaining once an active risk has been mitigated i.e. after action plans are in place and the immediate threat is removed. The degree of mitigation is shown in the risk register - which outlines the controls in place, and the assurance those controls provide.
Appendix B: Risk triggers.

Risk triggers are symptoms or warning signs that indicate an event has occurred (or is about to occur) having potentially significant implications for the organisation. Identifying and discussing triggers at the earliest opportunity allows our risk reports to give the rest of the group advanced warning. Consequently, it is important that risk reviews are not only restricted to analysis of existing risks, but also devote time to understanding how triggers may affect the group’s future.

Examples of triggers include:

a. The influence of the global economy, having negative effects on the staff pension scheme and our investment portfolio.

b. The effects on our reputation from involvement in campaigning - particularly where the cause may be perceived not to align with member sentiments.

c. Employee activities that could lead to staff claims against the RCN (claims of unfair dismissal, perceived harassment & bullying).

d. Legal activities that - without careful monitoring - could lead to corporate fraud.

e. Restructuring member categories, removal of member benefits.

f. Failure to submit details to recognition/award bodies e.g. failure to return the required 'annual Trade Union return' document.

g. Implementing IT infrastructure or software projects.

h. Office rebuilds or relocations.

i. Failure to seek, and gain council approval before undertaking significant member-affecting activities.
13 Appendix C: Roles having direct responsibilities for risk management.

13.1 Council.

a. Council is the owner of risk management, and ultimately responsible to members for ensuring all reasonable measures are in place to manage identifiable risks.
b. Council will actively seek assurances that a robust risk management framework is in place which meets the requirements of Auditors and which complies with accepted best practice.
c. Council holds the CEO/General Secretary and the group executives accountable for implementing appropriate risk management measures within the organisation.
d. Council will review a risk report at each meeting, in conjunction with risk reports from Audit Committee. Council will also bring its own judgement to bear, feeding its opinions on risk into the framework (appendix A).
e. Council will inform the Audit Committee of their comments or decisions regarding corporate risk. In addition, Council meeting minutes will record any risk-related actions arising from the council meeting.

13.2 Audit Committee.

The Audit Committee will:

a. Review the risk report at each meeting.
b. Seek assurance that the group is adhering to its risk policy statement.
c. Report their findings to council, and react to any risk-related actions/decisions arising from council meetings.
13.3 **CEO/General Secretary (and delegated authority).**

a. The CEO/General Secretary has overall responsibility for fulfilling the group risk policy and for sustaining a culture where risks are openly identified, analysed, and managed. This is a delegated authority to the Chief Executive & General Secretary from council.

b. Day-to-day control and implementation of risk management is delegated to the Director, Finance and Business Enablement.

13.4 **Group executives.**

Group executives will:

a. Ensure an efficient risk management framework is maintained and monitored by each directorate.

b. Regularly review the group risk register. No fewer than eight reviews should be held per annum (although one review per month is the target).

c. Ensure risk based internal audits are scheduled and undertaken throughout the group’s directorates.

d. Ensure that risks are assessed for potential impact on the delivery of the Annual Plan, council and executive Priorities, and the Strategic Plan.

e. Provide a risk report to Audit Committee meetings. This report will identify significant changes in risk impact, likelihood or preparedness since the previous report.

f. Ensure that each year the group reviews the contribution that risk management has made to good business decision making. Risk management processes will be updated to reflect any findings.

g. Ensure this policy is reviewed at three yearly intervals, and that amendments are communicated to employees.
13.5 Executive Directors.

In addition to their group responsibilities, individual executives will:

a. Regularly communicate with their teams to ensure risk responsibilities are understood and are being embedded into the organisational culture.
b. Ensure their Directorates dedicate appropriate staff resources to the identification, management, and monitoring of local risks.
c. Ensure that the risk registers held in their Directorates, functional areas (e.g. Health & Safety), or by group-wide projects meet the requirements of this policy. Those risk registers must be written in a way that enables effective communication of significant local risks up in to the group risk register. Where significant local risks are incorporated into the group risk register, they should not be removed from the local register: instead, the risk should co-exist on both documents - with the local register indicating that ownership of the risk has passed to the group executives.

13.6 Operational Planning Advisor.

a. Will support Council, Committees, group executives, and the Group Secretary in their risk management roles, and maintain the corporate risk register.

13.7 Internal Audit providers.

a. Will review information gathered from audits and provide feedback to group executives and the Audit Committee in areas relevant to risk management.
b. Will review their audit plans and identify any themes that result from, or potentially lead to, organisational risk.