TRUSTED RESEARCH

Implementation – risk register considerations

National Protective Security Authority

National Cyber Security Centre

Contents

Risk registers for research security risk

All research security risks should be recorded in a risk register, including collaborations.

Recording research security risks allows institutions to:

- document and revisit risk strategies
- grade potential risks within the context of the institutional risk appetite
- identify mitigations to reduce or remove risk
- continually review ongoing risks
- assess the overall research security risk profile of the institution, including cumulative risk
- forecast and prepare strategies for research security risks, particularly those with a high likelihood of occurring

Research security risk register template

Below is a suggested template for a risk register, tailored to recording research security risks. This is a suggested model which you may want to use or adapt to suit your institution. It is not a mandatory template for risk registers.

The central Trusted Research function (or equivalent) at an institution should use a singular risk register to ensure consistency of risk recording across all collaborations.

If your institution has standardised template for risk registers, you should consult the risk register template owner before making any changes to the existing template or opting to use an alternative template.

Research security risk register template

							Before mitigations/controls			
Risk ID No.	**Date identified**	**Risk category**	**Risk name and description**	**Collaboration partners**	**Impact description**	**Link to strategic aim**	**Impact level**	**Probability level**	**Overall risk level**	**Mitigations and controls**
(column 1)	(column 2)	(column 3)	(column 4)	(column 5)	(column 6)	(column 7)	(column 8)	(column 9)	(column 10)	(column 11)
A number assigned to risks to facilitate easy identification.	To the highest degree of accuracy possible, the date the risk was identified.	E.g. financial, reputational, compliance, legal. A risk may fulfil more than one category.	Name of the project/ collaboration and a brief summary of the risk.	Institution/ organisation partners are associated with and country origin.	The possible outcomes if the risk is not mitigated or removed.	How does the work incurring this risk relate to the institutions' overall aims/ strategy?	Rate from 1 (lowest) to 5 (highest).	Rate from 1 (lowest) to 5 (highest).	Impact x probability (see table for corresponding rating).	What can be done to lower the impact of the risk or eliminate it, where possible?
1.	18/01/2023.	Reputational, compliance, legal.	Aerospace collaboration with X overseas university. Joint venture into aeroacoustics research with an overseas military-linked university.	University X, Country X	Reputational damage of working with military-linked overseas university. Potential for defence applications of aerospace technology to be given to overseas military.	Strategic aim to grow international partnerships.	4.	4.	16.	Define remit of research tightly to avoid defence applications. Put in place IP agreements and NDAs to prevent information sharing outside of the collaboration. Use physical and IT access restrictions.

Research security risk register template

After mitigations/controls			Evaluation							
Impact level (column 12)	**Probability level** (column 13)	**Overall risk level** (column 14)	**Adequacy of mitigations/controls** (column 15)	**Action** (column 16)	**Documentation** (column 17)	**Status** (column 18)	**Date of last review** (column 19)	**Date of next review** (column 20)	**Owner** (column 21)	**Date closed** (column 22)
Rate from 1 (lowest) to 5 (highest).	Rate from 1 (lowest) to 5 (highest).	Impact × probability (see table for corresponding rating).	Are the mitigations/ controls in place sufficient to reduce the risk? (1) Non-existent, (2) inadequate, (3) adequate, (4) robust, (5) optimal.	Is it necessary to: identify additional mitigations/ controls, monitor the risk, transfer the risk, avoid the risk?	Links or files references to relevant documents related to the risk.	Is the risk 'open' or 'closed'?	When the risk was last reviewed and the entry in the risk register updated.	When the risk is next due for review.	Who is responsible for owning the risk?	The date the risk was closed.
3.	3.	9.	Robust.	Monitor the risk.	See ‘Aerospace Collaborations’ File.	Open.	18/04/2023.	18/08/2023.	Head of Engineering – [Insert name].	N/A.

Priority calculation table

Probability					
5	5 ○	10 ◇	15 □	20 □	25 △
4	4 ○	8 ◇	12 ◇	16 □	20 □
3	3 ○	6 ◇	9 ◇	12 ◇	15 □
2	2 ○	4 ○	6 ◇	8 ◇	10 ◇
1	1 ○	2 ○	3 ○	4 ○	5 ○
	1	2	3	4	5
	Impact				

Risk threshold	Risk rating	Risk description
Red △	High	The risk is highly likely and highly damaging in impact.
Amber □	Medium	The risk is likely and damaging in impact.
Yellow ◇	Low	The risk is probable-to-likely and negative-to-damaging in impact.
Green ○	Negligible	The risk is unlikely-to-highly likely but very low in impact or, the risk is low-to-highly damaging in impact but highly unlikely.

Probability: the likelihood of the risk materialising.

Impact: the severity of the risk if it materialises.

A guide to the research security risk register template

Link to strategic aim (column 7): All activities undertaken by the institution should contribute to the overall aims and/or strategy of the institution. If work is being undertaken which does not contribute to the institutions' overall mission, particularly when that work incurs additional risk, those involved should reconsider undertaking the work.

Before mitigations/controls (columns 8 to 10) and After mitigations/controls (columns 12 to 14): It is advisable to identify the risk both before and after mitigations/controls have been put in place. Ideally the impact and/or probability level, and therefore the overall risk level, should be lower in the 'after' section of the risk register, provided that effective mitigations/controls are established.

Evaluation (columns 15 and 16): The evaluation column allows an assessment of the effectiveness of the mitigations/controls put in place.
The institution may wish to use a numerical scale to quantify the effectiveness of the mitigations/controls in addition to written comments.

Date of last review (column 19): Updated entries to the risk register should be dated to facilitate the identification of changes in the mitigations, the risk level and/or the nature of the risk etc. If the risk changes significantly, it may be pertinent to make a new entry in the risk register. Related entries should be cross-referenced in the 'Risk name & description' column using the 'Risk ID No.' or institutions may wish to make an additional column for cross-reference numbers.

Date of next review (column 20): Institutions may have policies and/or processes which determine the regularity of risk reviews, in which case institutions should adhere to the appropriate policy. It is advisable however, that the regularity of reviews is based on the overall risk level. For example, using the thresholds outlined in the priority calculation table, institutions may wish to review risks at the suggested intervals. Note that institutions will need to consider the length and intensity of the activity presenting the risk when determining the regularity of reviews.

If any changes are made during the course of a collaboration, for example a new partner and/or funder is introduced, the risk should be immediately reviewed.

To ensure confidence in the risk register system, institutions may want to conduct internal audits between agreed review dates to ensure individual collaborations are progressing as expected. The combination of reviews and audits should allow institutions to identify previously unknown non-negligible risks emerging from ongoing collaborations which need to be mitigated against.

Risk threshold	Regularity of risk review
Red △	Monthly
Amber □	Bi-monthly
Yellow ◇	Quarterly
Green ○	Yearly

Date closed (column 22): The risk should only be 'closed' when the activity which presented the risk has ended completely. Risks should not be closed if the risk is entirely resolved by mitigations. Instead, they should remain 'open' to allow for continual review and to acknowledge that there is an ongoing mitigated/resolved risk.

Identifying cumulative risk

As an institution, you may wish to use the ‘overall risk level’ columns to aggregate the total risk your institution is carrying both before and after mitigations are put in place.

To contextualise these numbers, you will also need to consider the following elements of the risk landscape:

- the size of the institution and the number of collaborations being undertaken
- the financial aspect of the collaborations
- the diversity (or lack thereof) of collaboration partners, including funders, and any dependencies created
- the amassing of collaborations in a specific research area
- the amassing of collaboration partners, including funders, from a single overseas geographic location

Considering these elements of the risk landscape will enable you to identify any existing or emerging dependencies. Where these exist, you may want to consider diversifying your risk landscape in the event that one of your single sources of risk becomes unmanageable to protect your institution and research.

It will be necessary for your institution to determine its overall risk appetite to identify whether the aggregated risk is acceptable to your institution.

This function will enable your institution to determine whether you have the tolerance to take on additional higher risk research collaborations, or whether you have reached your maximum risk tolerance.

Cumulative risk threshold	Risk rating	Risk description
Red △	High	Your institution is carrying a **high** amount of risk within its research portfolio. Disruption of **a small number** of these projects **would have a significant effect** on the ability of your institution to fulfil its core functions.
Amber □	Medium	Your institution is carrying a **medium** amount of risk within its research portfolio. Disruption of **a number** of these projects **would have a significant effect** on the ability of your institution to fulfil its core functions.
Yellow ◇	Low	Your institution is carrying a **low** amount of risk within its research portfolio. Disruption of **a significant number** of these projects **may have a significant effect** on the ability of your institution to fulfil its core functions.
Green ○	Negligible	Your institution is carrying a **negligible** amount of risk within its research portfolio. Disruption of **a significant number** of these projects **would not have a significant effect** on the ability of your institution to fulfil its core functions.

Disclaimer

This resource has been prepared by NPSA and NCSC and is intended to aid academic institutions to help them understand and mitigate security risks arising from research, in combination with additional resources and the application of institutions' own judgement. This document is provided on an information basis only, and while NPSA and NCSC have used all reasonable care in producing it, NPSA and NCSC provides no warranty as to its accuracy or completeness.

It is important to emphasise that no security measures are proof against all threats. You remain entirely responsible for the security of your own sites and/or business, and compliance with any applicable law and regulations. You must use your own judgement as to whether and how to implement our recommendations, seeking your own legal/professional advice as required.

To the fullest extent permitted by law, NPSA and NCSC accept no liability whatsoever for any expense, liability, loss, damage, claim or proceedings incurred or arising as a result of any error or omission in the document or arising from any person acting or refraining from acting, relying upon or otherwise using the guidance.

This exclusion applies to all losses and damages whether arising in contract, tort, by statute or otherwise including where it is a result of negligence. NPSA and NCSC separately and expressly exclude any liability for any special, indirect and/or consequential losses, including any loss of or damage to business, market share, reputation, profits or goodwill and/or costs of dealing with regulators and fines from regulators.

Institutions and individuals have a responsibility to ensure that they comply with all relevant legal obligations, as well as any other obligations to which they are beholden. This guidance included in this document should not be considered exhaustive. This guidance raises issues for consideration but does not dictate or purport to dictate what conclusions institutions should reach.