TRUSTED RESEARCH

Evaluation Framework – user guide

National Protective Security Authority

National Cyber Security Centre

Foreword

Universities' international research activities are key to making ground-breaking discoveries and finding solutions to the world's challenges.

It is important that we enable universities to undertake these activities safely and securely. The Trusted Research Evaluation Framework is a useful method for helping universities identify how they can implement risk-management processes across the breadth of their research activities.

Our sector has made a considerable effort to engage with and respond to the Trusted Research agenda – but there is always more to do. Universities will be at different stages of implementation and maturity, which requires a tailored, adaptable and proportionate approach.

This framework provides a structured method for universities to self-assess where they are on that journey, and suggests actions that can be taken to enhance their Trusted Research maturity.

We encourage universities to make use of the framework to enhance their research security processes, as we collectively seek to create a culture in which research security is seen as an indelible feature of good research practice.

Vivienne Stern
Chief Executive of Universities UK (UUK)

Introduction

NPSA and NCSC developed the Trusted Research Evaluation Framework in consultation with experts across the academic sector and within relevant parts of government to address a question consistently asked during research security interactions:[1]

"What does 'good' look like?"

To help academic institutions at various stages of their journey form a mature approach to research security, we have created a **self-assessment maturity matrix** for use by those directly involved with owning the research security agenda at their institution. This will also help those charged with implementing organisational change and ensuring legal compliance within the research environment.

While we anticipate that university professional services, or equivalents, will be involved in the implementation of the framework, endorsement and support from your institution's senior leadership will be vital to driving adoption and delivering changes.

The framework is designed to complement existing Trusted Research guidance available from the NPSA website, and should be used to shape or reinforce research security policies and procedures at your institution.

1 NPSA and NCSC consulted with experts within the Export Control Joint Unit, Cabinet Office Investment Security Unit, Foreign and Commonwealth Development Office, Intellectual Property Office, Department for Science Innovation and Technology, the Research Collaboration Advice Team and Universities UK. Further, representatives from numerous UK academic institutions were consulted prior to the publication of the Principles.

They have been published to allow self-assessment so that each institution adopting the framework can self-assess to judge its own level of Trusted Research maturity. They also help to facilitate discussions with other institutions, with government and with professional bodies, and assist institutions with ongoing ownership and management of research collaboration risks. Adopting the framework is a straightforward way of evidencing that your institution is taking research security seriously, regardless of where within the framework your current level of maturity sits.

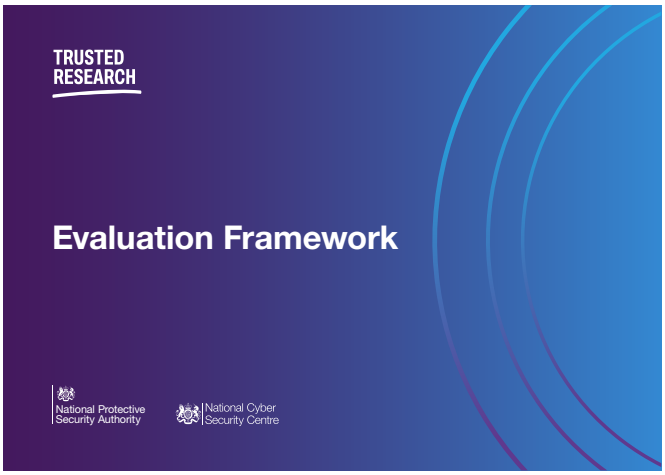
The framework represents effective research security practice which is applicable to all institutions and academics conducting research across all disciplines. However, part of taking a risk-informed approach to research security means making decisions which consider a variety of factors which may increase or decrease research security risk around particular disciplines. Therefore, many of the recommendations that exist within the framework are especially important for research-intensive institutions, and any research which might inherently be higher risk. This may include research being undertaken within any of the 17 sensitive areas of the UK economy as defined by the National Security and Investment Act (2022).

The framework

The framework is split into seven categories, broadly based on NPSA's 5E's behavioural change framework,[2] with each category including several mutually supportive sub-categories. Each of these sub-categories are split into a maximum of three levels of maturity (foundation, intermediate and developed), though some will have only one or two.

Each of the seven categories represents an aspect of organisational culture to allow institutions to approach the framework with a behavioural change mindset. Each of the sub-categories also represent practical steps that institutions can take on their overall behavioural change journey.

Each of the levels within the framework demonstrates a proportionate response based on your institutional-level risk assessment and security requirements, as well as acting as a maturity model for internal and external discussions around research security:



2 https://www.npsa.gov.uk/resources/embedding-security-behaviours-using-5es

Foundation

This is the minimum standard institutions should aim to meet to embed basic research security. They focus on having an existing basic policy or process to cover issues surrounding research security.

Intermediate

This is the level to achieve for a robust set of mitigations – you may wish to focus on achieving them for specific areas that are of concern to your institution. They generally focus on measures that are specifically recommended within the Trusted Research for Academia guidance. For example, you may have produced your own risk management framework for research.

Developed

This focusses on a comprehensive set of mitigations under Trusted Research, as well as role modelling good security practices to the wider sector – acting as a benchmark against which other institutions may judge their own level of research security maturity. At this level, you can evidence positive engagement and culture around Trusted Research via staff surveys, results, and engagement with outside institutions, including NPSA and NCSC.

As a maturity matrix, at the time of publication we anticipate that most institutions in the UK will be at foundation level or below, but hope that the framework will help them to increase their maturity levels as time goes on.

How to use the framework

At the beginning of the process of self-assessment, institutions can consider themselves to have 'adopted' the framework, regardless of their overall maturity level. This represents a commitment by the institution to use the framework to measure and monitor their own research security maturity level.

The framework should be used by whoever at an institution is responsible for the ownership and/or implementation of research security-relevant policies and procedures. This will vary from institution to institution. They should form the basis of an honest assessment of Trusted Research maturity, highlighting where you are achieving sufficient reassurance for your own risk profile, and where more could be done. Institutions may also wish to use them in their interactions with relevant government stakeholders (such as the Research Collaboration Advice Team) when research security is being discussed.

NPSA does not necessarily expect an institution to consistently demonstrate Developed behaviours across all sub-categories. Each institution should use the framework in concert with their own risk appetite and aim to achieve the corresponding level accordingly.

Each sub-category's levels builds upon the one beneath it. Therefore, an institution cannot achieve intermediate level in a sub-category without having first achieved foundation level. As such, when first using the framework, institutions should look to identify where they are achieving foundation level before seeking to identify any levels above that. Future re-evaluation of an institution's maturity level using the framework will likely be required on a semi-regular basis, and NPSA may issue additional versions of the framework in future which develop existing categories or introduce new ones in reference to new or emerging risks.

Existing and future material published by NPSA on the Trusted Research website will align with this framework. For example, to meet requirements for intermediate level within the 'Internal communications strategy' sub-category, an institution must:

"… have an internal communications programme which promotes awareness of the Trusted Research campaign and your institutions' policies in relation to managing research security risks."

To aid with this, NPSA provides a range of media including a Trusted Research promotional video, blog, training materials and example policy considerations. These are available for institutions to use in any internal comms programmes or staff education initiatives.

There are some instances where interaction with other bodies may contribute to your assessment, for example, where the developed level under the 'Wider Trusted Research links' sub-category requires an institution to:

"…demonstrate active engagement in sector-wide workshops on sharing Trusted Research practice."

While there are events run by NPSA which would contribute towards satisfying this criteria, there will be those run by other bodies within HM Government and the sector more widely, or by more specialised organisations such as the Higher Education Export Control Association.

Initial considerations

The following considerations may be helpful in directing future actions to address any gaps identified after reviewing the principles:

Endorse: senior endorsement and governance

- Who is best placed at your institution to act as the senior risk owner? What level of support would they need to affect meaningful change?
- How do you currently assess risk more widely at your institution? Does research risk, and all of the component parts of it (e.g. reputational risk, financial risk, legal risk) factor into it? If not, could it exist within those established processes?
- Who is responsible for compliance on a day-to-day basis and do they have relationships with all of the relevant bodies within government to fulfil their role?

Encourage: communications

- How do you embed culture change at your institution? What culture change programmes have you run recently which might inform how to embed research security culture?
- How do you communicate with staff? How effective are those channels and how do you measure their reach across your institution? Are you satisfied that top-level communications are received and digested by their intended audience?

Educate: training

- How are training programmes run throughout your institution and what do they cover? Would Trusted Research fit within your existing offering, or would it require a new programme to be created?
- Does your institution provide support for those who need or wish to undertake external learning which supports their core function?

- Do the staff who need to understand the legislative requirements that exist within academia, such as export control, have access to the knowledge that they need to provide advice to staff, or know where they can seek that advice themselves?

Environment: institutional risk and collaboration

- Do you have appropriate policies and procedures in place at your institution governing research risk?
- Are those policies widely understood by those to whom they apply?
- How is risk centrally recorded? Does your institution have the ability to survey the cumulative risk of all research being conducted at any one time?

Enable: people, processes and guidance

- Do you support staff travelling overseas and is this applied consistently across your institution?
- How do you address non-compliance?
- Who is responsible for due diligence at your institution and are they sufficiently trained on how to make risk-based assessments?

Environment: data and devices

- Do you have regular and rigorous cyber security testing procedures for your research infrastructure?
- Are you confident that academics at your institution are using institutional networks, rather than their own, particularly to house their most sensitive research?

Evaluate: impact measurement

- Do you regularly survey your staff on any number of issues, and could you feasibly include research security focus and awareness as part of this?
- If asked, would you be able to evidence engagement with the wider research security agenda among your academic and non-academic staff, whether by providing attendance at training sessions, a log of high-risk collaborations, a record of export control license applications or similar?

Further guidance

For further guidance and materials, please see the NPSA website,[3] or contact a member of the NPSA Trusted Research team.

Disclaimer

This guide has been prepared by NPSA and NCSC and is intended only to guide readers in their use of the Trusted Research Evaluation Framework. This document is provided on an information basis only, and whilst NPSA and NCSC have used all reasonable care in producing it, NPSA and NCSC provide 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 and 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 report or arising from any person acting, refraining from acting, relying upon or otherwise using this user guide, or the Trusted Research Evaluation Framework. 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 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 and the mitigations 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.

3 https://www.npsa.gov.uk/specialised-guidance/trusted-research