EECARO
European Export Control Association for Research Organisations

25 October 2024

Feedback on the Factsheet Research Security: Building blocks for risk appraisal

Introduction

EECARO has read with great interest the factsheet with proposed research security risk appraisal building blocks[1]. Based on its members' experiences linked to export control risk appraisal and the significant overlap in risk assessment between export control and research security, EECARO presents below firstly some general observations and recommendations. Secondly, it will provide some specific comments per building block.

General comments

The factsheet does not make a distinction between the **3 levels of research security risks** as identified by Council Recommendation on enhancing research security (9097/1/24 REV1), namely the undesirable transfer of critical knowledge and technology, the malign influence on research and the ethical or integrity violations. EECARO finds it useful to specify what part of risk appraisal is relevant for what risk. If the building blocks, in essence, only relate to the undesirable transfer of critical knowledge and technology, then this should be made clear to support scope setting by research organizations.

From an export control and sanctions perspective, the 4 building blocks and the related questions are familiar, which increases the feasibility of embedding such risk assessment in existing internal compliance measures, but it also leaves unanswered what are the additional checks needed to identify **research security risks beyond export controls and sanctions**.

The current focus of the building blocks is on **collaborations with entities**. However, research security may be compromised in actions that fall outside institutional collaboration. The building blocks do not sufficiently address the **research security challenges linked to the mobility of researchers**. On the one hand, the international mobility of researchers, with its numerous formal and informal collaborations via traveling abroad or working from abroad may pose research security risks. On the other hand, there can also be risks linked to the mobility of researchers inside research organisations, for instance when shifting from less sensitive to more sensitive research topics. EECARO sees added value in including the topic of mobility in the risk appraisal building blocks with some specific questions.

[1] https://research-and-innovation.ec.europa.eu/system/files/2024-01/ec_rtd_building-blocks-risk-appraisal.pdf

EECARO finds it imperative that the risk appraisal blocks are recognized by EU national governments as a foundational element for building a research security institutional policy. EECARO invites the European Commission to **involve national governments in gathering feedback and support** for these risk appraisal blocks, also to increase a level-playing field across the EU when research organisations approach their competent authority on this topic.

The current format of the risk appraisal block, consisting of a list of questions without further context, may **lead to diverging interpretations**. A good example is Chapter 5 of National Knowledge Security guidelines[2] from the Netherlands. In addition, there is no guidance on the **weighing of the risks** identified in the building blocks, which leaves this important step entirely to individual institutions, increasing diverging practices based on different levels of risk-appetite. While defendable from an institutional autonomy point of view, such approach does not support more EU-wide convergence on risk appraisal. Moreover, more guidance is needed on the suggested approach to reviewing the questions as a basis for the internal informed decision-making process. Is it, for instance, expected to systematically review the questions with (standardizable) underlying red-flags or risk indicators to assist such reviewing? Additional review guidance is therefore recommended.

Applying the risk appraisal requires the possibility of having a **follow-up dialogue with the national competent authority** to come to an effective internal risk management programme. EECARO believes that such dialogue on a national level is crucial to create a learning community beyond the one-dimensional perspective of purely economic, academic or security considerations. This requires the willingness of all national competent authorities to actively approach the European research ecosystem based on a level-playing field understanding of research security.

The building blocks focus on **screening for risk indicators at the beginning of a collaboration**. It could be emphasized that some screening is also relevant during the execution of a research collaboration to finetune research security safeguarding measures or trigger a review of the overall collaboration based on significant research security concerns that may arise.

Research organisations bring innovation to the (European) industry whilst the building blocks do not address industry. Lacking a shared **understanding of research security between academia and industry** will result in ineffective measures by research organisations, which often lack the authority or means to commercially and contractually restrict the application or region of technology that surpasses the technical readiness levels typical for these organisations.

[2] https://english.loketkennisveiligheid.nl/risk-analysis/documents/publications/2022/04/07/national-knowledge-security-guidelines

Comments per building block

1. The risk profile of your own organisation

- The question **about strengths and vulnerabilities** is vague. It could be reformulated to 'How embedded in existing international collaborations is your organization for the collaboration or topic under scrutiny?' Moreover, such analysis is useful at the institution's overall risk profile, but also at local level (e.g., at the department level).
- The question **about scientific leadership** could benefit from additional guidance on what relevant metrics indicators for this assessment are, as there are many possible variants.
- The question **about financial dependency** is too broad. For example, if an individual researcher attracts funding from non-EU sources, then there could be financial dependency for that particular researcher, but this does not translate automatically into a dependency for the entire organisation.
- The **research and/or business (development) typology of the organization** could be included as a relevant additional factor. For instance, does the organisation enter short-term projects or rather long-term projects? With large budget or small budget? With in-kind contributions or formal payments? How long are the internal decision-making processes prior to the start of a project? Does the profile include publicly funded research or industry-funded research for basic scientific research or applied research?

2. The research domain in which the international cooperation is to take place

- **About the reference to 'project'** in the first question under this building block: it implies a narrow screening scope. Research collaborations can be diverse, including Intellectual Property transfers or in-kind contributions. Hence, 'project' could be reformulated into 'collaboration'.
- **About the reference to 'dual-use technologies'** in the second question: this scope is too small as it seems to narrow down research security risk appraisal to dual-use export control risk appraisal. Consider adding sensitive, critical or emerging technologies in the reference to technologies. Moreover, as brought forward by EECARO in its Feedback on the Call for Evidence on enhancing research security in Europe[3], EECARO cautions to make cross-references between research security risk appraisals and dual-use export control risk appraisals without further guidance. EECARO is concerned about the growing proliferation of requirements and concepts connected to the notion of security

[3] https://eecaro.eu/eecaro-publications/eecaros-feedback-on-the-enhancing-research-security-in-europe-call-for-evidence/

and dual-use. As an example: Consider that a research collaboration involves listed dual-use technology, and that the project gets a good-to-go due to an available export licence. Does this mean that due to research security considerations, the collaboration could/should be stopped, nonetheless? This implies a delicate balancing between regulatory export controls requirements and beyond-regulatory research security commitments.

- **About the reference to key-enabling technologies:** a cross-reference to the EU common list of key-enabling technologies is useful, but this could also be the case for the critical technologies under the Economic Security Strategy. EECARO notes that some Member States, like the Netherlands, have drawn up their own derivative list of sensitive knowledge areas for a new screening policy for persons. Having a multitude of technology lists complicates collaborations within the EU, leaves even more room for scope interpretation and actually discourages research organisations to proactively work with one or some of the lists.

3. The risk profile of the third country where the international partner is based

- When using different **risk indicators based on multiple international indices**, their combination will result in a diffuse country list. EECARO sees added value in a list of high-risk third countries for research security considerations.
- Research organisations should be able to **consult reliable and up-to-date information sources** that are accessible on national basis, or even EU basis. Duplication of work (everybody finding information on these topics on their own) is not a smart use of resources and will lead to conflicting findings. If currently available information sources are not considered adequate, then steps should be taken to create new ones. Although the Council Recommendation adopts a country-agnostic approach as baseline, EECARO prefers in the guidance to prioritize and focus first on those non-EU countries that may pose more risks on research security than some other non-EU countries.
- EECARO also notes that while in many cases not triggering export controls, **EU-based entities owned or controlled by entities or governments from non-EU high-risk countries** of concern could trigger research security concerns and guidance on how to deal with such risks triggered when evaluating a research collaboration should be made available.

4. The risk profile of the international partner organisation

- **Being able to retrieve reliable information** is crucial under this building block. Ultimate Beneficial Ownership information or funding origin information is often not open-source data or is even unavailable due to GDPR restrictions. Moreover, even if research organisations can make use of commercial screening tools, these tools focus on screening of entities with a corporate structure and business-

oriented operations. This is not the typical collaboration partner of research organisations. Hence, there is a gap in the screening capabilities for public, government-related or not-for-profit entities. EECARO urges the European Commission and EU Member States to provide guidance on the expected due diligence level for retrieving such info and provide a data supporting role, where possible.

- **About the question related to the background or affiliation of researchers:** when an institutional agreement is signed, the names of the researchers/staff involved are (often) not yet known. A check on the background/staff should be included later on (e.g. whether they are on the sanctions list).
- **About the question related to the interests from the research partners:** EECARO notes that a balanced mutual interest is not necessarily a lower risk than an unbalanced interest. Important is whether it is clear to both partners what their interest is and their mutual expectations, and whether the own research organisation can identify a worthwhile benefit in the proposed collaboration.

Conclusions

EECARO appreciates the ongoing work of the European Commission and the EU Member States on the risk appraisal building blocks for research security.

EECARO underscores the need to offer guidance on the expected due diligence levels for retrieving critical information about international partners critical technologies and risk flags for problematic cooperation from a research security viewpoint.

EECARO expresses its willingness to actively engage as a stakeholder in the dialogue on research security, leveraging its lessons learned from export control risk assessment in a research context.

About EECARO

The European Export Control Association for Research Organisations (EECARO) is a network that unites European research institutes, universities, and their export control compliance officers with a view to addressing the specific character of export controls in a research context. This includes the intersection of export controls and other relevant areas such as knowledge/research security and R&D funding for technologies with civil/military synergy potential. For more information, please visit: http://www.eecaro.eu | Contact: info@eecaro.eu