Vlaanderen
is wetenschap

Research Security Appraisal

September 2026 – classification 1

fwo

Vlaanderen
is wetenschap

Context
Policy
Research Security Appraisal Tool
Application Form
Research Security Questions

Vlaanderen
is wetenschap

Context

NORDIC COUNTRIES

Academic spy cases: No room for simplistic conclusions

Jan Petter Myklebust 12 November 2022

Share Post Delen 10

Two recent cases of espionage involving foreign academics in Norwegian universities highlight the need for a deeper discussion about what the proper national responses should be, according to an internationalisation expert.

MIVD onthult werkwijze Chinese spionage in Nederland

Nieuwsbericht | 06-02-2024 | 15:33

De Militaire Inlichtingen- en Veiligheidsdienst (MIVD) heeft Chinese cyberspionage in Nederland blootgelegd. De dienst ontdekte geavanceerde Chinese malware die dit mogelijk maakt. Een Chinese statelijke actor is hiervoor verantwoordelijk. Dit stelt de MIVD op basis van eigen inlichtingen vast.

Bundesamt für Verfassungsschutz

Information sheets on economic security

Espionage in Science and Research

April 18, 2024

Chinese Government Poses 'Bold and Unrelenting' Threat to U.S. Critical Infrastructure, FBI Director Says

Partnerships, joint operations, and private sector vigilance can help us fight back

Twitter Facebook Email

Indicted McGill professor was caught in broad, controversial U.S. dragnet of Chinese-background scientists

Some prominent critics suggest America's trade war with China has propelled police on a witch hunt against east-Asian researchers

Tom Blackwell

Published Jul 12, 2019 • Last updated Jul 12, 2019 • 4 minute read

POLITICS

54 NIH scientists reportedly fired or resigned during espionage probe

By Mark Moore

Published June 17, 2020 | Updated June 17, 2020, 11:37 a.m. ET

'Sensitive' collaborations between Belgian universities and China peaking

Thursday, 10 October 2024

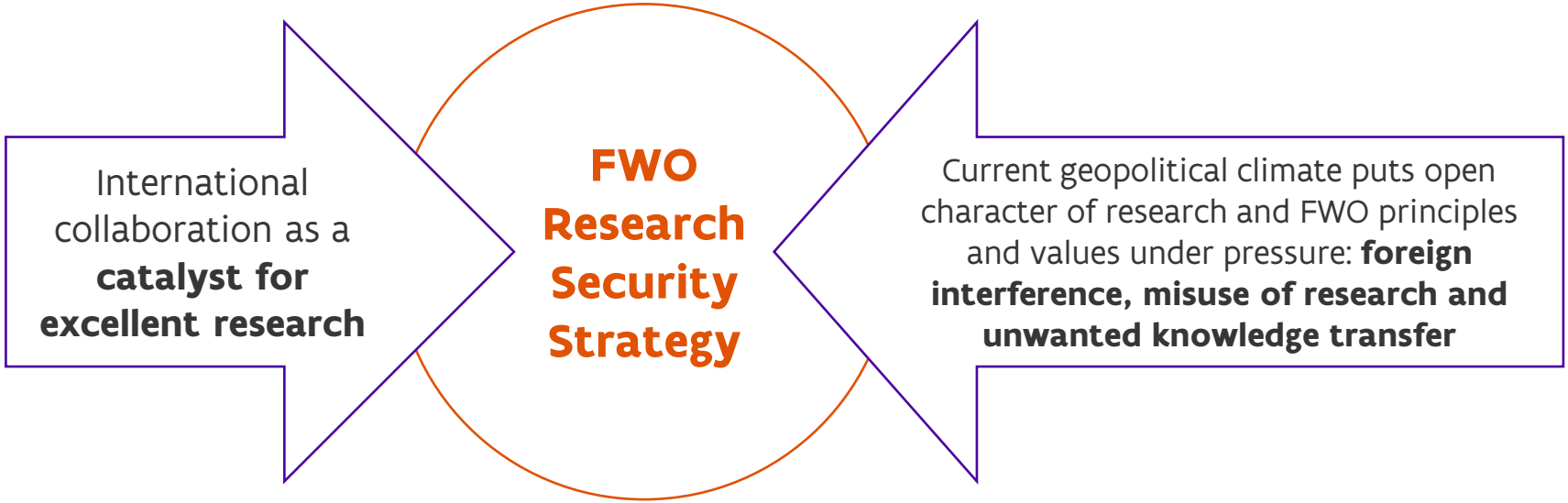
By The Brussels Times Newsroom

Institutional Restrictions

	FWO Projects	FWO Fellowships	Outgoing Mobility Grants	Incoming Mobility Grant	Mobility Projects Bilateral Research Projects	FWO Review College	Scientific Research Networks (SRNs)
Research institutions in Russia/Belarus	Not allowed as co-supervisor, no subcontracting, no Money-follows-Collaboration, … (needs to be removed)	Not allowed as foreign co-promotor (needs to be removed)	Not eligible as destination	Incoming researchers affiliated to these institutions are not eligible	Agreement with RSF was discontinued	Researchers affiliated to these institutions cannot act as internal and external expert	Not allowed to participate
Seven Sons of Defence (China)[&]	Not allowed as co-supervisor, no subcontracting, no Money-follows-Collaboration, … (needs to be removed)	Not allowed as foreign co-promotor (needs to be removed)	Not eligible as destination	Incoming researchers affiliated to these institutions are not eligible	Not eligible as foreign partner	Researchers affiliated to these institutions cannot act as internal and external expert	Not allowed to participate

& Northwestern Polytechnical University; Harbin Engineering University; Harbin Institute of Technology; Beihang University (Beijing University of Aeronautics and Astronautics); Beijing Institute of Technology; Nanjing University of Science and Technology; Nanjing University of Aeronautics and Astronautics

FWO Research Security



Responsible International Cooperation in the Current Geopolitical Climate

Funding agency well placed to take responsibility as they reach all researchers

What is Research Security

- **Undesirable transfer** of critical knowledge and technology that may affect the security of the Union and its Member States, for instance if channelled to military or intelligence purposes in third countries

- **Malign influence on research (foreign interference)** where research can be instrumentalised by or from third countries in order to inter alia create disinformation or incite self-censorship among students and researchers infringing academic freedom and research integrity in the Union

- **Ethical or integrity violations**, where knowledge and technologies are used to suppress, infringe on or undermine Union values and fundamental rights, as defined in the Treaties. (Misuse of research results)

(EU Council Recommendation on enhancing research security)

Adverse consequences research security breaches

- Loss of research data;
- Competitive disadvantage in your research domain;
- Loss of intellectual property rights, patent opportunities and potential revenues;
- Reduced confidence in your research data and results;
- Legal or administrative consequences;
- Loss of potential future partnerships;
- Reputational damage to yourself, your research group and/or your research institution;
- Economic or competitive disadvantage for Flanders, Belgium and/or Europe.

Council Recommendation on Enhancing Research Security (23/05/2024)

Engage with research funding organisations:

- '...research security is an **integral part of the application process**...'
- '... encourage beneficiaries to **consider the context in which the R&I cooperation takes place** ...'
- '... **ensuring potential risks and threats are identified up front** ...'
- '... a **risk appraisal proportionate to their risk profile**, resulting in agreeing appropriate risk management ...'
- 'Applicants ... agreeing a **partnership agreement**, ...'

More info: Council Recommendation

Council of the European Union

Vlaanderen
is wetenschap

Policy

Starting Point: Core Values of FWO

- **Guarantee fair and transparent evaluation based on scientific excellence**

- **Other scientific values such as:**
  - Academic freedom
  - Research integrity
  - Ethics including e.g. dual use and misuse (human rights)
  - Equal opportunities e.g. gender
  - Reciprocity and level-playing field
  - Open science and intellectual property rights/GDPR

Built on Core Principles

- **Main goal: Raising awareness – focus on risk assessment**
- **Building a resilient research community**

- Proportionality
- Non-discriminative and country agnostic approach
- FWO wide: throughout all funding instruments
- Feasible: limited administrative impact FWO, researchers, and institutions
- Dynamic: continuous monitoring

Four pillars

FWO PARTNERSHIPS

RAISING AWARENESS

MONITORING and ANALYSIS

CYBERSECURITY ISO-27001

Vlaanderen
is wetenschap

Research Security Appraisal Tool

RAISING AWARENESS

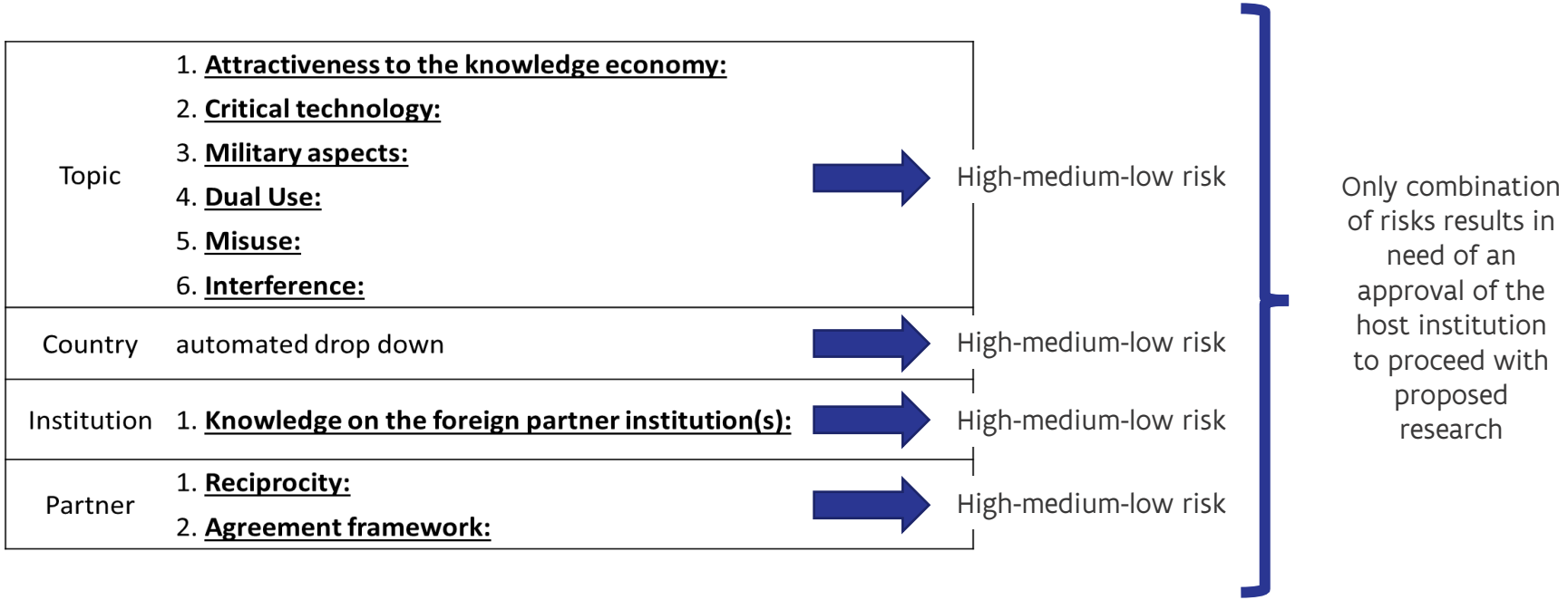
Research Security Appraisal Tool

- New tab in each FWO application form
- Self appraisal of risks by applicants
- Estimation of risks to promote risk awareness

- Process:
  - In close consultation with VLIR WG Human Rights, Dual Use, Research Security
  - Approved by FWO Board
  - Version 2026: Optimised after pilot call in 2024 and 2025 implementation phase.

Actual tool after optimisation

In total, 10 questions, three answer options; (YES) - (POSSIBLY) - (NO, NOT AT ALL)



EXAMPLE, not the actual numbers!

Threshold for approval

If sum of indicated scores ≥ 150 then research security approval of host institution is needed

	YES	POSSIBLY	NO, NOT AT ALL
Attractiveness	50	25	0
Critical technology	50	25	0
Military	100	50	0
Dual use	150	50	0
Misuse	50	25	0
Interference	100	25	0
Country	100	50	0
Institution	100	50	0
Reciprocity	50	25	0
Agreement frame	50	25	0

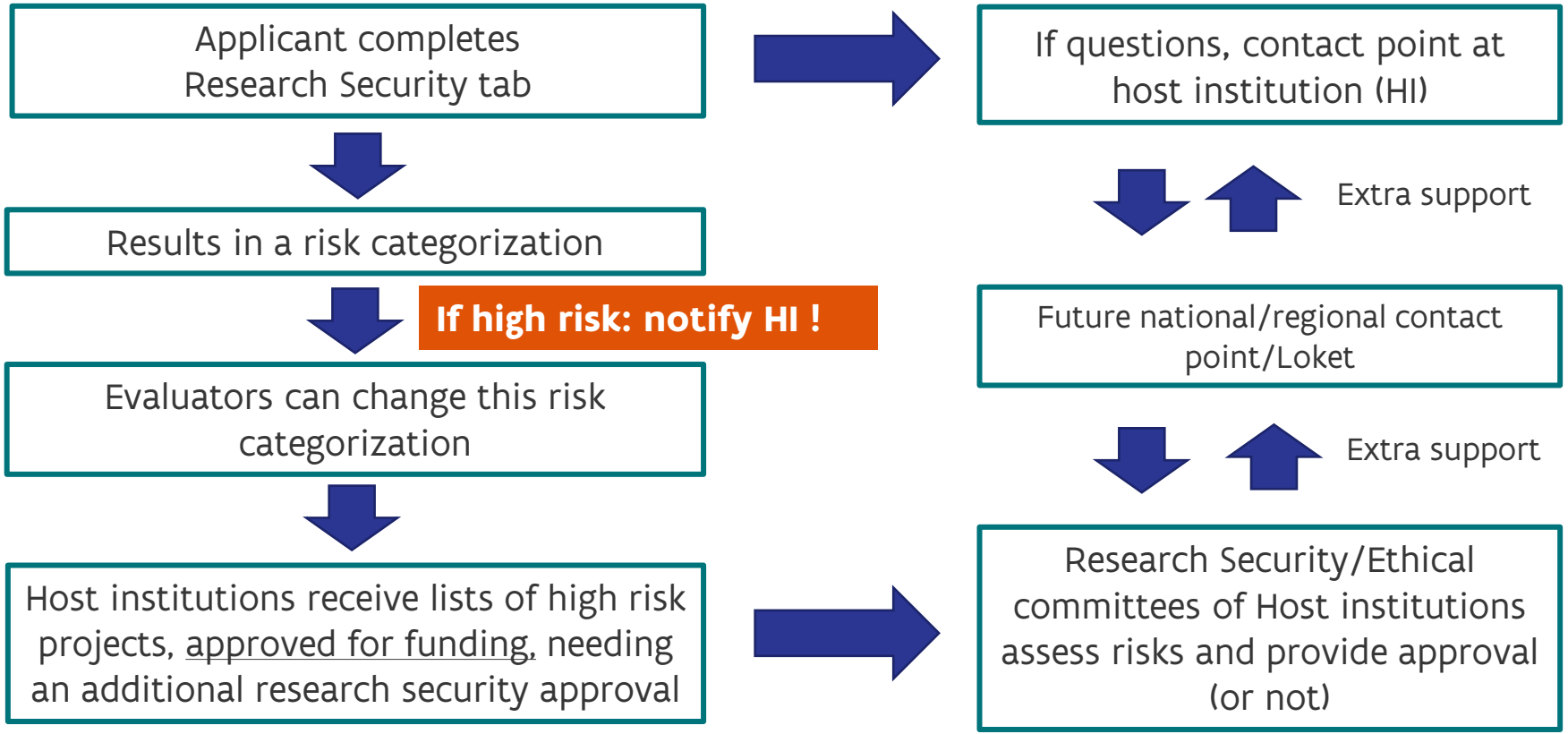
EXAMPLE, not the actual numbers!

Threshold for approval

If sum of indicated scores ≥ 150 then approval of host institution is needed

	YES	POSSIBLY	NO, NOT AT ALL
Attractiveness	50	25	0
Critical technology	50	25	0
Military	100	50	0
Dual use	150	50	0
Misuse	50	25	0
Interference	100	25	0
Country	100	50	0
Institution	100	50	0
Reciprocity	50	25	0
Agreement frame	50	25	0

Process overview



Important messages

- **Complete Research Security Appraisal first!**

- **Risk assessment NOT included in**
  → PDF send to reviewers
  And not part of external peer review if applicable

Research security risk assessment wil **NOT** impact scientific evaluation in any way

- **Projects approved for funding that need a research security approval: project cannot start until host institution grants research security approval.**

General FWO Regulations

Art. 4ter – Research security

§1. As part of their grant application, researchers must truthfully complete a self-assessment questionnaire on research security aspects of the planned research. If a file is classified as high risk, they must obtain an approval concerning research security from the competent internal authorities before starting the high-risk research activity(ies).

§2. The FWO or its authorised representative can request these approvals concerning research security ad hoc or during audits at the applicant's host institution at any time during the project period up to and including 5 years after its end.

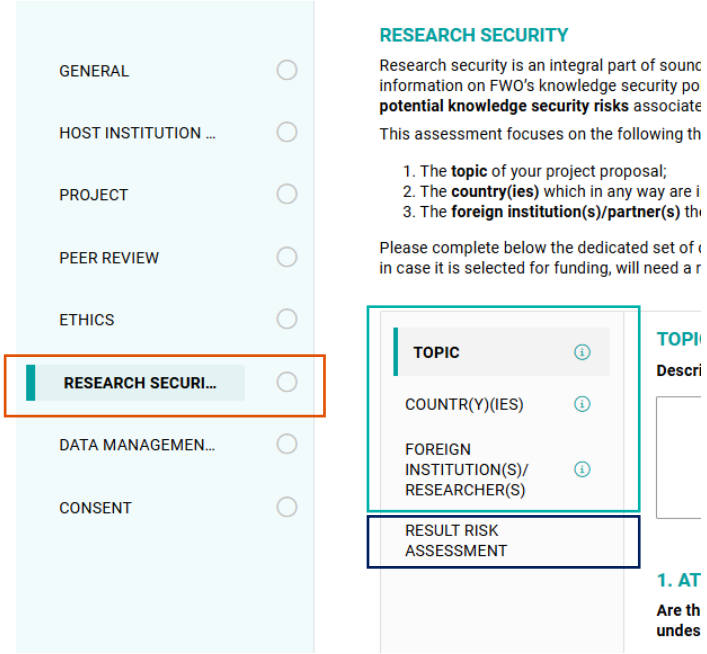
Contact persons responsible for research security

Institution	E-mail	Contact person
UAntwerpen	mihrs@uantwerpen.be	Contact point Research Security
UGent	researchsecurity@ugent.be	Vincent Eechaudt Eveline Praet
UHasselt	RRI@Uhasselt.be	Stephanie Ruysschaert
KU Leuven	knowledgesecurity@kuleuven.be	Contact point Research Security
VUB	ecdmm@vub.be	Martyna Bajorinaite Naomi Van den Broeck
VIB	Rene.Custers@vib.be jan.staelens@vib.be	René Custers Jan Staelens
IMEC	exportcontrol@imec.be	Beatrijs Thomas
Vlerick Business School	gdpr@vlerick.com camille.richelle@vlerick.com	Contact point Research Security
VITO	researchsecurity@vito.be	Contact point Research Security
ITG	research@itg.be	Contact point Research Security
Flanders Make	Marc.Engels@flandersmake.be	Contact point Research Security
VLIZ	Ethics@vliz.be	Contact point Research Security

Vlaanderen
is wetenschap

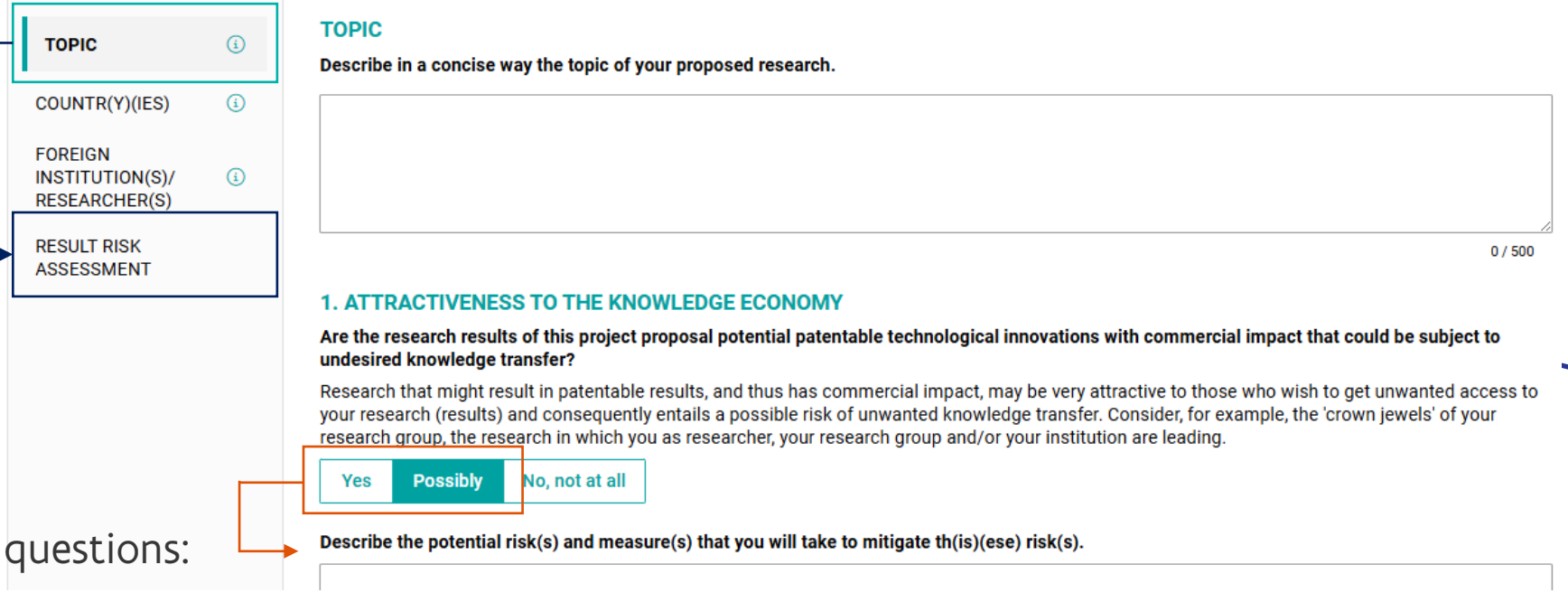
Application Form

<u>Supervisor-spokesperson</u> of application is responsible for completing Research Security Tab. Should be done in close consultation with all project partners in Flanders (if any) since research security assessment covers project as a whole.



Tab Research Security:

- Three subitems
  - Topic
  - Countr(y)(ies)
  - Foreign institution(s)/researcher(s)
- Overall automated risk assessment



6 questions:

- ATTRACTIVENESS
- EU CRITICAL TECHNOLOGY
- MILITARY ASPECTS
- DUAL USE
- MISUSE
- INTERFERENCE

3 possible answers:

- Yes
- Possibly
- No, not at all

Describe risk and mitigation

AUTOMATED risk classification

Any other country than Belgium involved?

- Foreign partner and/or;
- Research on and/or in a particular country?

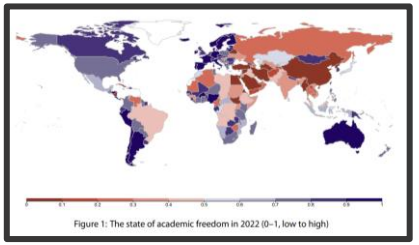
→ YES/NO

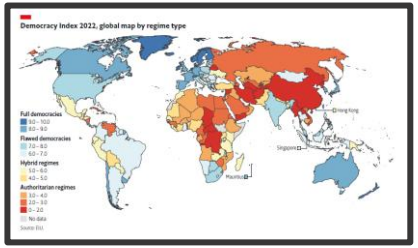
Fully automated: Drop-down country list in application

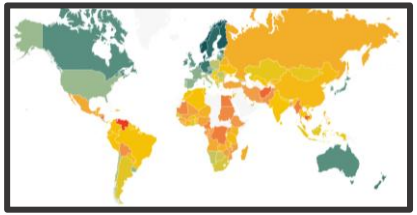
Classification on **international indices**:

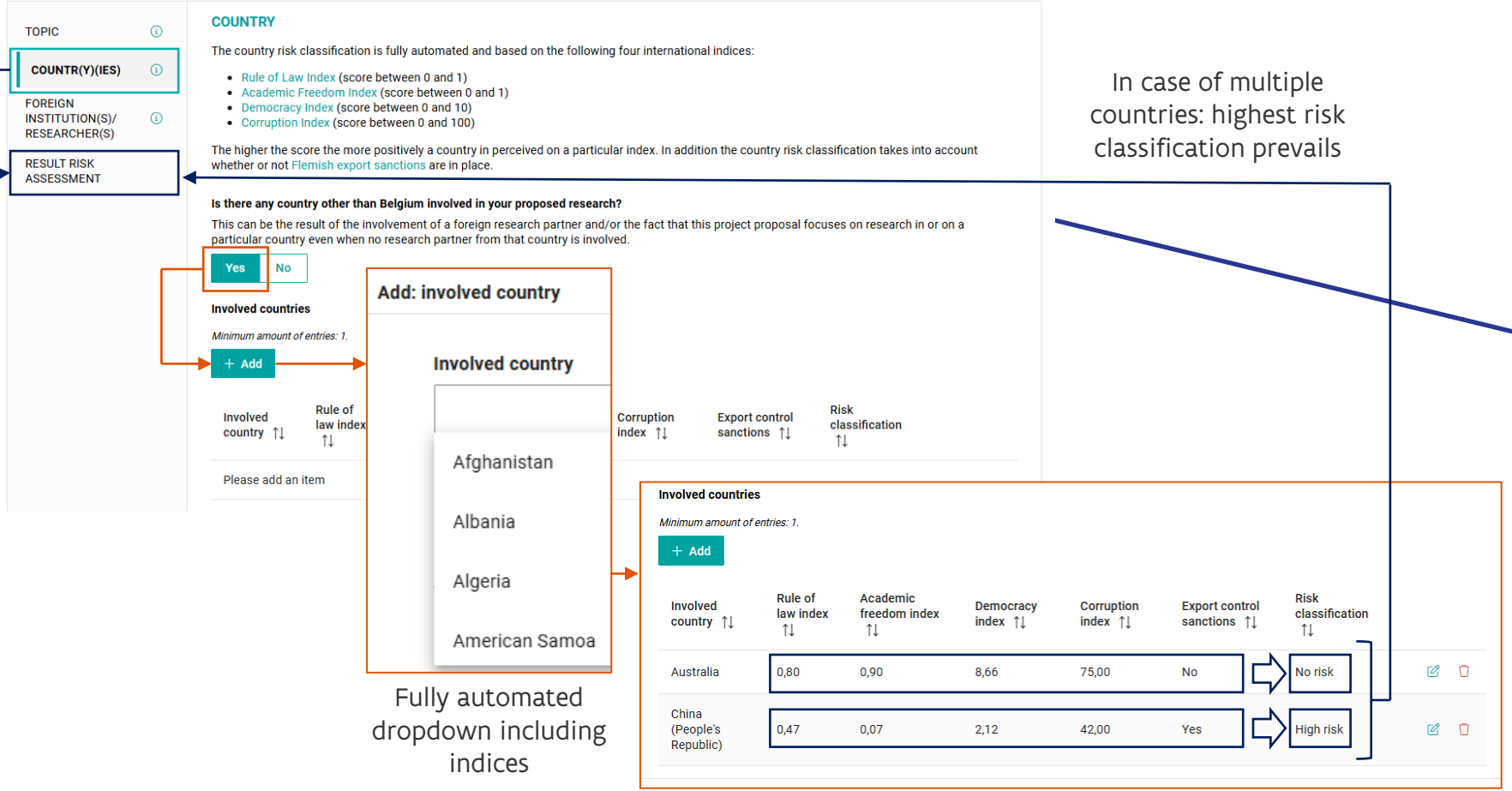
A. Academic Freedom Index
B. Country Corruption Index
C. Rule of Law Index
D. Democracy Index
E. Sanctions in place

Dynamic: yearly updated



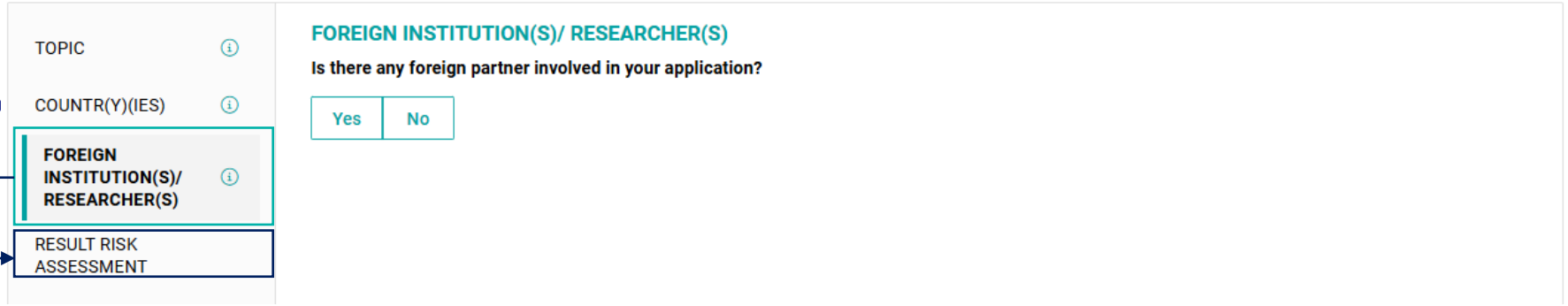


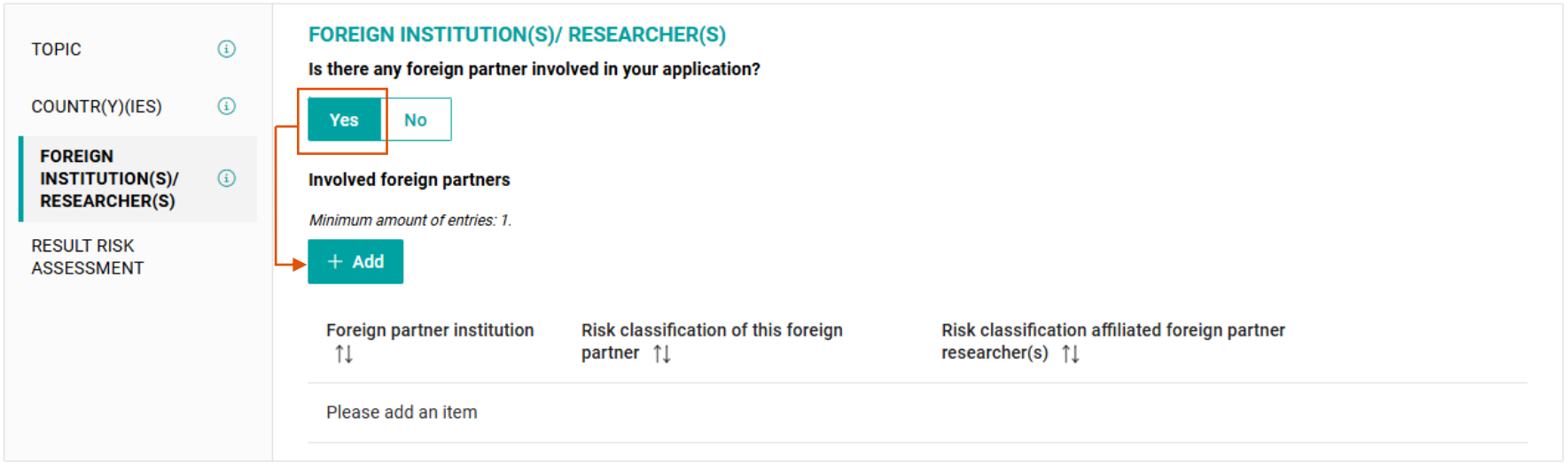




In case of multiple countries: highest risk classification prevails

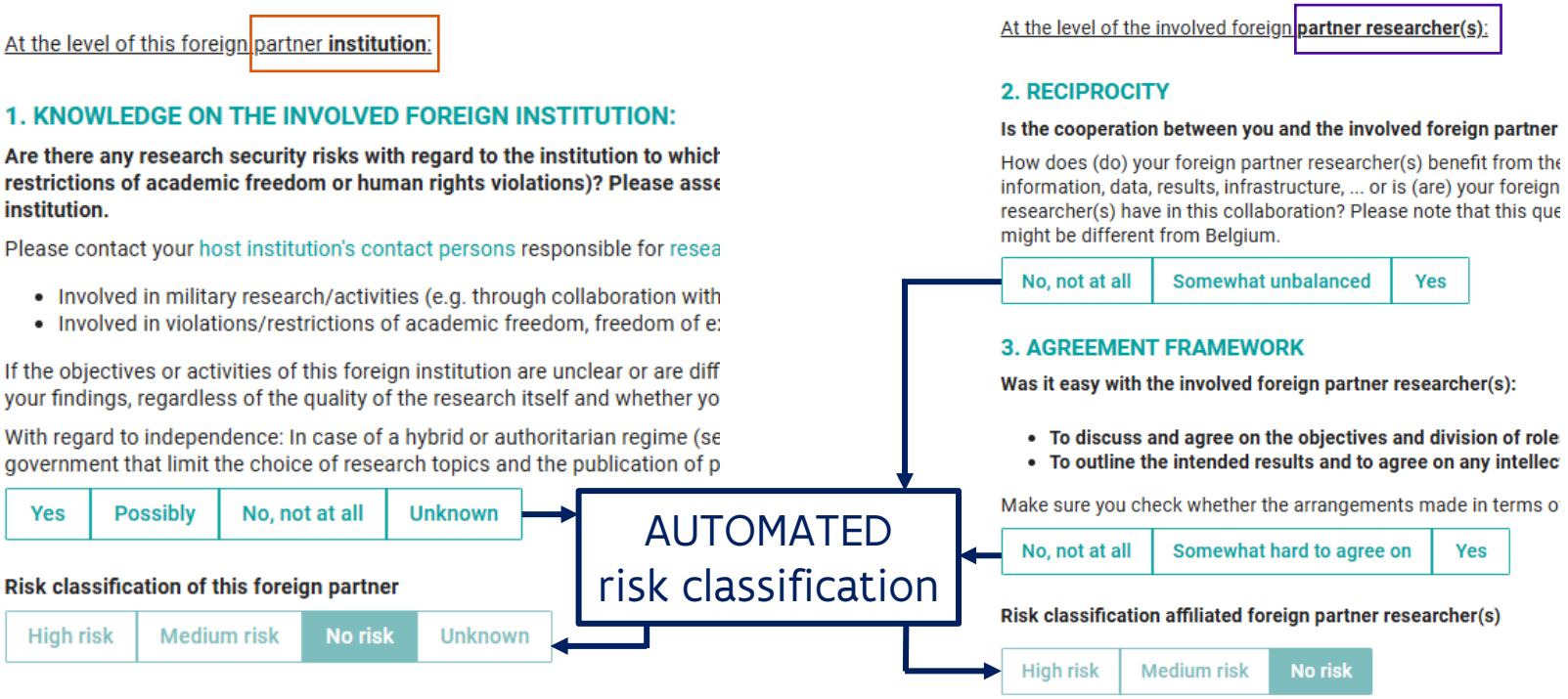
Fully automated dropdown including indices

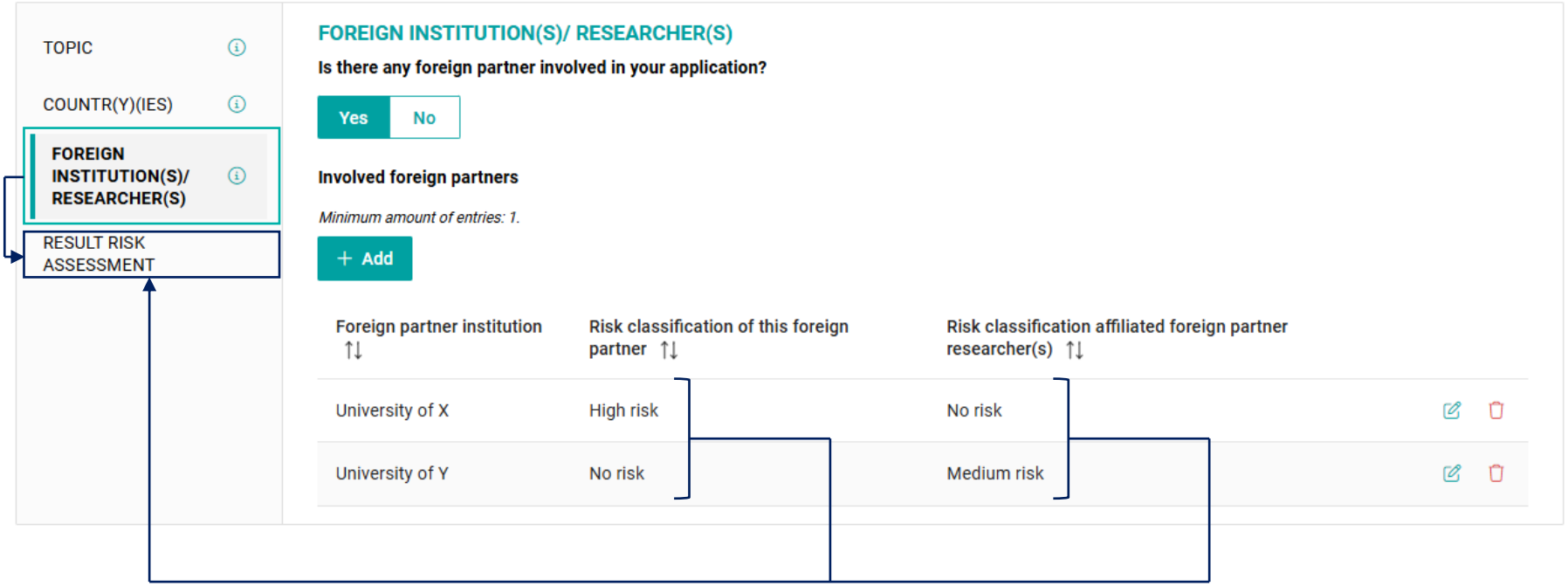

TOPIC
COUNTR(Y)(IES)
FOREIGN INSTITUTION(S)/ RESEARCHER(S)
RESULT RISK ASSESSMENT
FOREIGN INSTITUTION(S)/ RESEARCHER(S)
Is there any foreign partner involved in your application?
Yes
No


TOPIC
COUNTR(Y)(IES)
FOREIGN INSTITUTION(S)/ RESEARCHER(S)
RESULT RISK ASSESSMENT
FOREIGN INSTITUTION(S)/ RESEARCHER(S)
Is there any foreign partner involved in your application?
Yes
No
Involved foreign partners
Minimum amount of entries: 1.
+ Add
Foreign partner institution
Risk classification of this foreign partner
Risk classification affiliated foreign partner researcher(s)
Please add an item

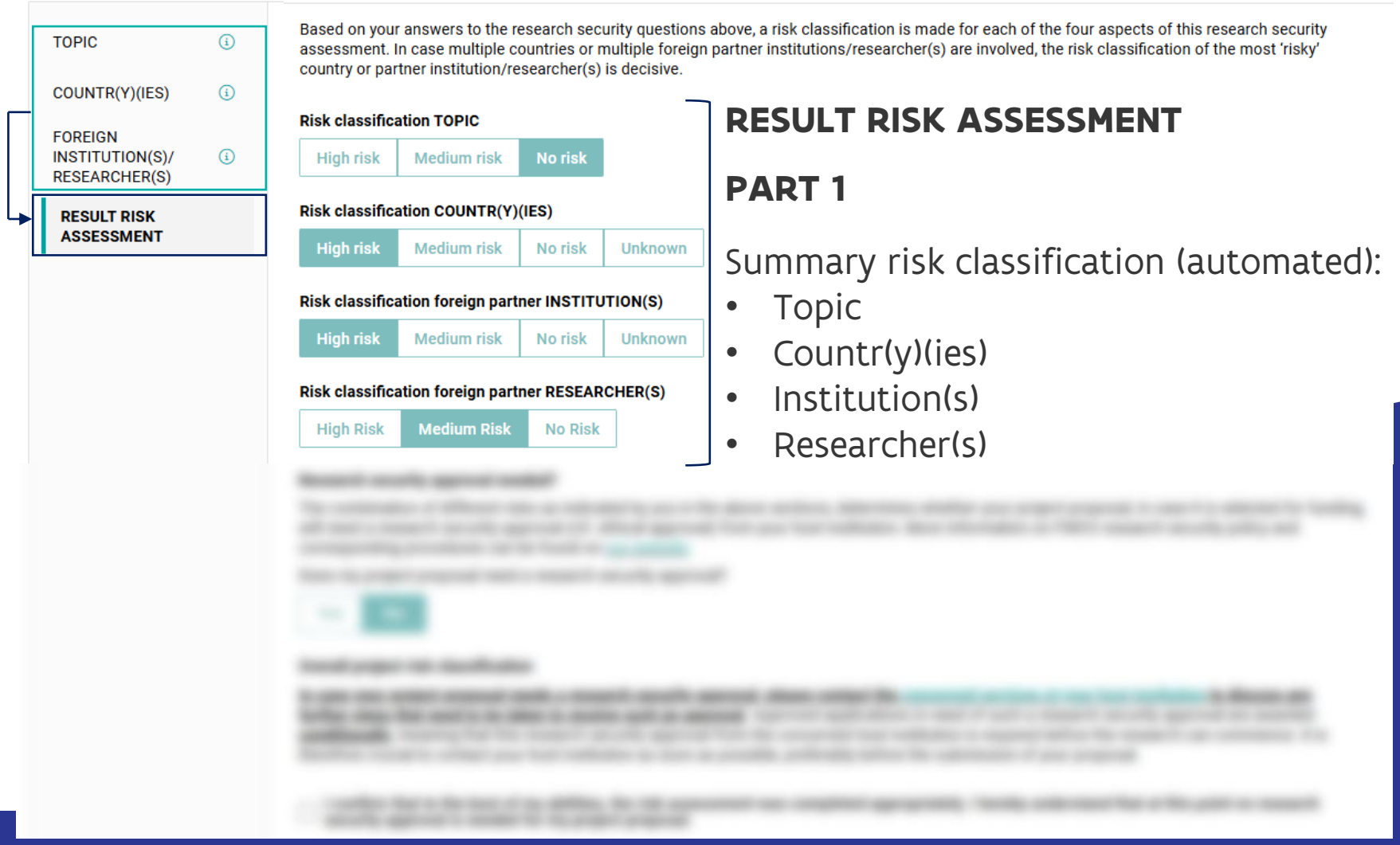
Answer for each foreign partner institution 3 questions:

- 1 on partner INSTITUTION
- 2 on partner RESEARCHER(s)





In case of multiple foreign partners: highest risk classification institution and researcher(s) prevails

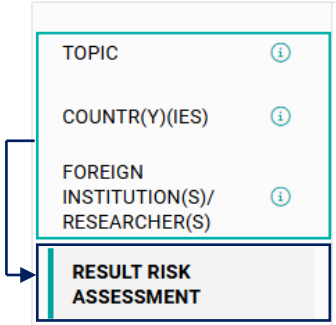


RESULT RISK ASSESSMENT

PART 1

Summary risk classification (automated):

- Topic
- Countr(y)(ies)
- Institution(s)
- Researcher(s)



RESULT RISK ASSESSMENT

PART 2

Research security approval needed?

NO

Research security approval needed?

The combination of different risks as indicated by you in the above sections, determines whether your project proposal, in case it is selected for funding, will need a research security approval (cfr. ethical approval) from your host institution. More information on FWO's research security policy and corresponding procedures can be found on our website.

Does my project proposal need a research security approval?

Yes | **No**

Overall project risk classification

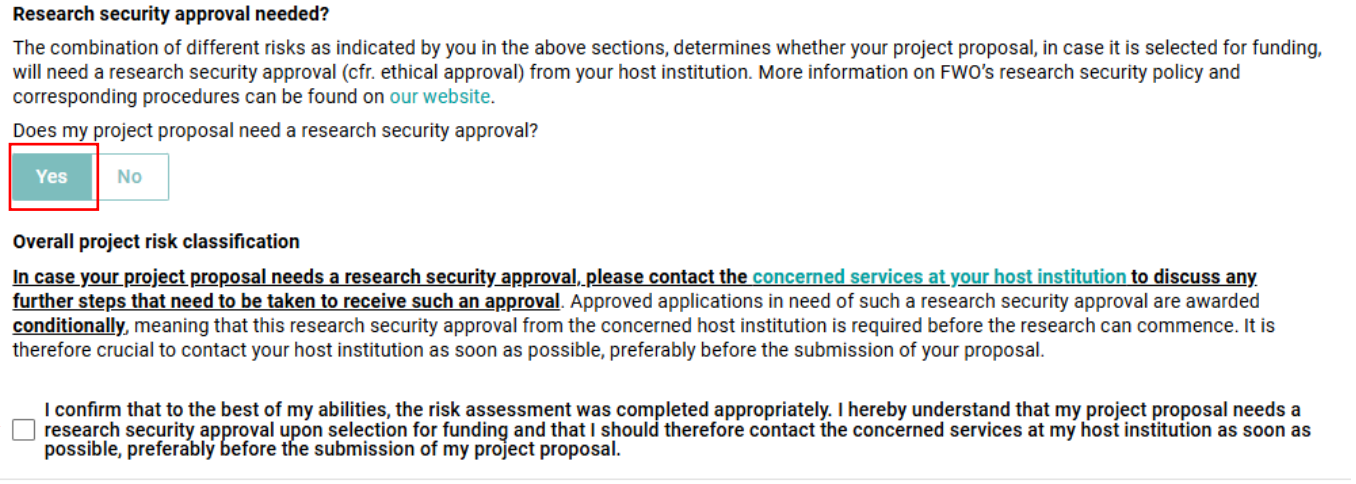
In case your project proposal needs a research security approval, please contact the concerned services at your host institution to discuss any further steps that need to be taken to receive such an approval. Approved applications in need of such a research security approval are awarded **conditionally**, meaning that this research security approval from the concerned host institution is required before the research can commence. It is therefore crucial to contact your host institution as soon as possible, preferably before the submission of your proposal.

☐ **I confirm that to the best of my abilities, the risk assessment was completed appropriately. I hereby understand that at this point no research security approval is needed for my project proposal.**

RESULT RISK ASSESSMENT

PART 2

Research security approval needed?



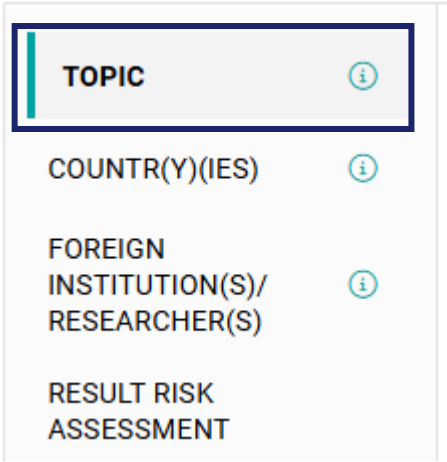
YES

- **Complete Research Security Tab asap when drafting application** to verify if approval is needed.
- **If approval is needed, pro-actively contact host institution (even before final submission of application)**: the sooner possible research security risks are put on the radar of the institution, the sooner internal procedure can start.

  Approved applications in need of such a research security approval are awarded **conditionally**, meaning that this research security approval from the concerned host institution is required before the research can commence.

Vlaanderen
is wetenschap

Research Security Questions



TOPIC

1. Attractiveness
2. EU Critical Technology
3. Military Aspects
4. Dual Use
5. Misuse
6. Interference

1. Attractiveness to the knowledge economy:

Are the research results of this project proposal potential patentable technological innovations with commercial impact that could be subject to undesired knowledge transfer?

Research that might result in patentable results, and thus has commercial impact, may be very attractive to those who wish to get unwanted access to your research (results) and consequently entails a possible risk of unwanted knowledge transfer. Consider, for example, the 'crown jewels' of your research group, the research in which you as researcher, your research group and/or your institution are leading.

2. EU critical technology:

Does this project proposal involve:

1. **research on or**
2. **the development of any of the following EU critical technologies?**

Please be aware that this question refers to the critical technology being the object of your research in itself and not only serving as a methodological tool for your research (i.e. merely the utilisation of the technology).

More info: Commission Recommendation on critical technology areas for the EU's economic security for further risk assessment with Member States

GENERAL

HOST INSTITUTION ...

PROJECT

PEER REVIEW

ETHICS

RESEARCH SECURI...

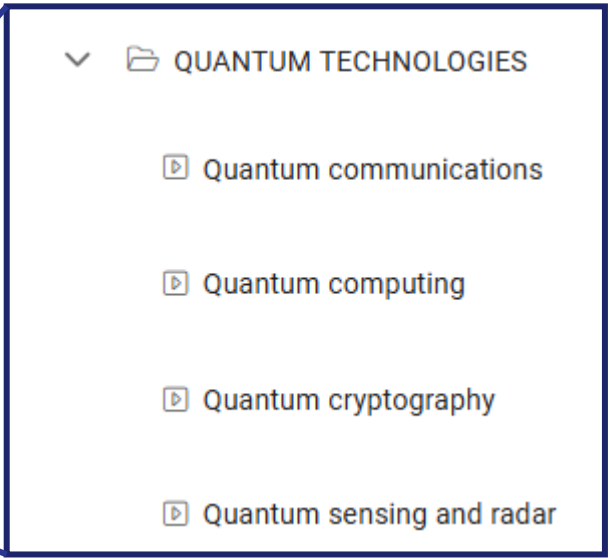
DATA MANAGEMEN...

CONSENT

Add: technologies

Technology

- ADVANCED CONNECTIVITY NAVIGATION AND DIGITAL TECHNOLOGIES
- ADVANCED MATERIALS MANUFACTURING AND RECYCLING TECHNOLOGIES
- ADVANCED SEMICONDUCTORS TECHNOLOGIES
- ADVANCED SENSING TECHNOLOGIES
- ARTIFICAL INTELLIGENCE TECHNOLOGIES
- BIOTECHNOLOGIES
- ENERGY TECHNOLOGIES
- QUANTUM TECHNOLOGIES
- ROBOTICS AND AUTONOMOUS SYSTEMS
- SPACE & PROPULSION TECHNOLOGIES



3. Military aspects:

Does this project proposal include research on military aspects?

E.g. literature studies on war practices. **This question does not probe research for military purposes/applications**.

4. Dual-use:

Could the research results of this project proposal be used for military applications? Does this research involve dual-use items within the meaning of Regulation (EU) 2021/821, or other items requiring an export licence? Please make sure to carefully consult the VLIR Guidelines for researchers on dual use and misuse of research.

Dual-use items are materials, substances, techniques, etc. that can be used for both civilian and military purposes. Think of items that have applications in academia, medicine or industry, but which also can be used for military purposes. For example, items that can be used for the design, development, production or use of (biological, chemical or nuclear) weapons and/or the transport of such weapons.

More info: VLIR Guidelines for researchers on dual use and misuse of research

5. Misuse:

Can the research results arising from this project proposal (when shared) be misused for:

- **Human rights violations, such as (internal) repression, mass surveillance, discrimination and stigmatisation and/or;**
- **Criminal/terrorist purposes and/or;**
- **Justifying of, for example, a certain policy/ideology?**

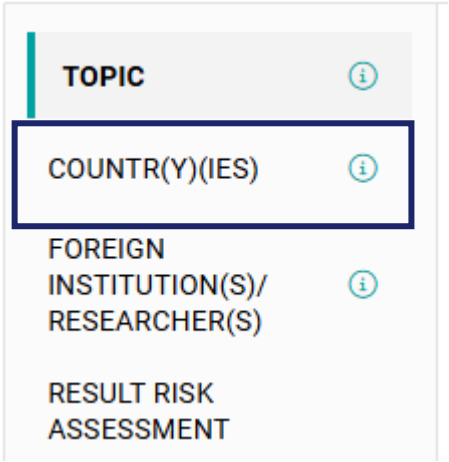
'Misuse' refers to using the research or research results for unethical purposes. Examples include artificial intelligence technology that may (unintentionally) lead to discrimination or the curtailment of civil rights, vaccination research where knowledge can be misused to spread viruses, or interrogation techniques that might be used for repression within a country. **In the wrong hands, research results can cause serious harm to people, animals and the environment, even when research is conducted with the best of intentions.** This risk presents itself in particular with technology or knowledge (1) that may contribute to **human rights violations**, or (2) that **terrorists or criminals** can exploit, or (3) that may **endanger individuals, groups or countries**. It is therefore important not only to look at the research topic but also to check whether the funding agency or research partners could misuse the results for these purposes.

More info: **VLIR Guidelines for researchers on dual use and misuse of research**

6. Interference:

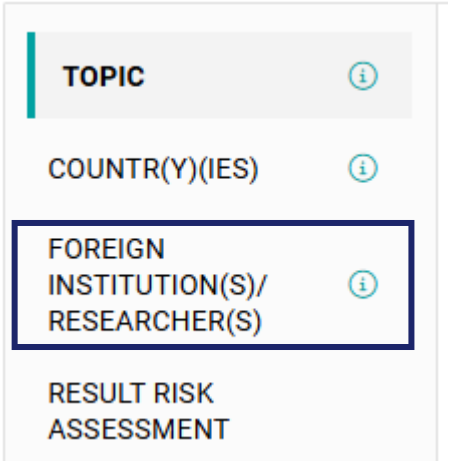
Is the research outlined in this project proposal related to topics that are (e.g. politically) sensitive or prohibited in the country that is researched or where the research is carried out? If so, is there a risk of interference/censorship?

Certain research topics, which are not sensitive in Flanders, may be perceived differently abroad. As a result you – as a researcher – may be pressured by third parties that do not want you to conduct and publish research on a certain topic. This **may jeopardise** principles such as **the right to freedom of expression and academic freedom**, but also values and standards with regard to **scientific integrity**.



COUNTR(Y)(IES)

› Fully automated



FOREIGN INSTITUTION(S)/ RESEARCHER(S)

› On an institutional level

1. Knowledge on the involved foreign institution:

Are there any research security risks with regard to the institution to which your foreign partner researcher(s) is (are) affiliated (for instance, involvement in military research, involvement in restrictions of academic freedom or human rights violations)?

Please assess to the best of your ability, taking into account the international reputation, independence, … of this foreign institution.

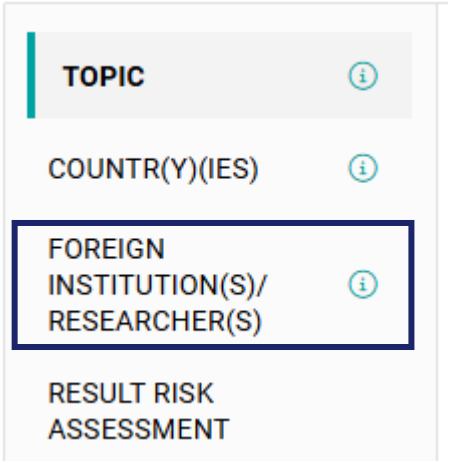
Please contact your host institution's contact persons responsible for research security in case of any doubt or lack of knowledge.

With regard to **international reputation**, is this foreign institution:

- **Involved in military research/activities** (e.g. through collaboration with the military or defence companies or the development of defence technology) and/or;
- **Involved in violations/restrictions of academic freedom, freedom of expression, and/or other human rights** (e.g. by developing technology used for this purpose).

If the objectives or activities of this foreign institution are unclear or are difficult to ascertain, the collaboration might be undesirable. Consider whether critics can use the collaboration to discredit your findings, regardless of the quality of the research itself and whether you and/or your host institution could suffer reputational damage by collaborating with this institution.

With regard to independence: In case of a hybrid or authoritarian regime (see 'Country'), is the foreign institution subject to certain **restrictions and/or forms of censorship imposed by the government that limit the choice of research topics and the publication of particular research findings**?



FOREIGN INSTITUTION(S)/ RESEARCHER(S)

› On the level of individual partner researcher(s)

1. Reciprocity:

Is the cooperation between you and the involved foreign partner researcher(s) balanced and sustainable (equal intellectual investments - equal benefits)?

How does (do) your foreign partner researcher(s) benefit from the proposed collaboration? Is there a **balanced equilibrium (reciprocity**) both in terms of intellectual investment as well as access to information, data, results, infrastructure, ... or is (are) your foreign partner researcher(s) pulling the research and results towards themselves? **What interests does (do) your foreign partner researcher(s) have in this collaboration?** Please note that this question does not refer to financial investments such as the requested budget, as the labor/consumable costs in the foreign country might be different from Belgium.

2. Agreement Framework: Was it easy with the involved foreign partner researcher(s):

- **To discuss and agree on the objectives and division of roles within the project when drafting the project?**
- **To outline the intended results and to agree on any intellectual property associated with them in advance?**

Make sure you check whether the arrangements made in terms of GDPR, IPR, data storage, etc. are in line with standard practices and regulations within your institution.

Things to keep in mind as supervisor-spokesperson:

- **Responsible for completing Research Security Tab**. Should be done in close consultation with all project partners in Flanders (if any) since research security assessment covers project as a whole.
- **Complete Research Security Tab asap when drafting application** to verify if approval is needed.
- **If approval is needed, pro-actively contact host institution (even before final submission of application)**: the sooner possible research security risks are put on the radar of the institution, the sooner internal procedure can start.
- If research security approval is needed: this should be provided by the host institution to which the supervisor-spokesperson is affiliated (in consultation with other involved host institutions in Flanders, if any, especially if research security sensitive activities take place in these institutions)

Things to keep in mind as supervisor-spokesperson:

- **Responsible for completing Research Security Tab**. Should be done in close consultation with all project partners in Flanders (if any) since research security assessment covers project as a whole.
- **Complete Research Security Tab asap when drafting application** to verify if approval is needed.
- **If approval is needed, pro-actively contact host institution (even before final submission of application)**: the sooner possible research security risks are put on the radar of the institution, the sooner internal procedure can start.
- If research security approval is needed: this should be provided by the host institution to which the supervisor-spokesperson is affiliated (in consultation with other involved host institutions in Flanders, if any, especially if research security sensitive activities take place in these institutions)

FWO website on Research Security

FWO contacts:
Isabelle.Verbaeys@fwo.be
Gregory.Absillis@fwo.be
Tinne.Jacobs@fwo.be

September 2026 – classification 1