



DAAD KIWi

Deutscher Akademischer Austauschdienst
German Academic Exchange Service

KIWi COMPASS

KIWi Checklist Knowledge Security

A self-assessment tool for evaluating security-relevant dimensions
of international academic cooperation

daad.de/kiwi





Contents

Introduction	2
Cooperation Profile	4
Checklist	6
1. Partners and Funding	6
2. Export Control	8
3. Exploitation of Results and Intellectual Property Rights	11
4. Research Ethics	12
Notes on Background and Use of the KIWI Checklist	14
Practical Guidance and Explanations	15
About Us	20

Introduction



Against the backdrop of a shifting geopolitical landscape, international academic cooperation is increasingly situated within

a field of tension: on the one hand, the aspiration for open exchange, and on the other, the need to operate within security-sensitive frameworks. The question, how potential risks can be managed in such a way that simultaneously safeguards academic freedom while enabling the opportunities of international cooperation is gaining significance. Most recently, in the summer of 2025, the German Council of Science and Humanities presented recommendations for strengthening knowledge security within the German research system in its [position paper](#) ‘Science and Security in Times of Global Upheaval’.

To support reflection on, and assessment of, security-relevant aspects of international higher education cooperation, the Centre for International Academic Cooperation (KIWi) of the German Academic Exchange Service

(DAAD) has developed the present KIWi Checklist Knowledge Security. The KIWi Checklist systematically incorporates the security dimensions identified by the German Science and Humanities Council. It may be used both individually by researchers as well as institutionally. For example, within relevant review processes at higher education institutions (in line with the Council’s guidance, p. 46: for ‘individual reflection’, ‘collegial exchange’, and discussion within ethics committees on security-relevant research). We recommend, that the KIWi Checklist be applied jointly by those responsible for cooperation projects and the relevant administrative departments within higher education institutions. The KIWi Checklist Knowledge Security thus serves on the one hand as a tool for structured self-assessment. On the other hand, it is intentionally designed as an instrument for dialogue stimulating and supporting exchange on security-relevant aspects of international cooperation within higher education institutions. The aim is to

raise awareness among relevant stakeholders, to identify potential risks at an early stage, and develop appropriate courses of action tailored to the specific cooperation context. The KIWi Checklist offers guidance and impulses for reflection on the following aspects:

- Strategic objectives and potential of the cooperation project;
- Security-relevant dimensions of the cooperation and possible risks;
- Further assessment and review processes, both within the higher education institution or through in-depth consultation with KIWi;
- Risk mitigation measures.

The KIWi Checklist Knowledge Security comprises a total of 17 questions, clustered into four thematic structures: 1. Partners and Funding, 2. Export Control, 3. Exploitation of Results and Intellectual Property Rights and 4. Research Ethics.

Where indications of potential cooperation risks arise (i.e. a “yes” response), a more in-depth review and further internal coordination within the higher education institution are recommended. Each question includes a free-text field in which measures already implemented or planned for risk-mitigation may be recorded. The annex provides additional information on each thematic cluster. This includes not only contextual classification but also guidance on possible contact points in cases where further clarification is required, as well as selected references.

As a general principle, it is recommended that, in cases of doubt or uncertainty, the responsible units within the higher education institution, such as the International Office, the Export Control Office, or the Legal and Research Department should be consulted. KIWi itself is also available as a further point of contact and, on the basis of the checklist, offers tailored consultations on risk assessment in international cooperation.

Cooperation Profile

0.1. Title

0.2. Research field

0.3. Partner institution(s) in Germany and abroad (country, name, faculty, institute, research group)

0.4. Form of cooperation (multiple answers possible)

Student exchange

Teaching exchange

Research cooperation

Cooperation with businesses/industry
or industry-related organisations

Other

0.5. How is the cooperation funded? (multiple answers possible)

Core or third-party funding
from Germany

Third-party or grant
from abroad

Own resources of the international
cooperation partner

Other

0.6. Names and national affiliations of the funding bodies involved

0.7. What are the academic, scientific and institutional strategic objectives of the cooperation? What are the potential benefits to your higher education institution?

**0.8. What are the respective contributions of the partners in Germany and abroad?
Is the balance appropriate?**

Checklist

1. Partners and Funding

The following questions are intended to raise awareness of non-transparent governance structures, state or military influence, and sanctions. In particular, violations of sanctions must be excluded.

Possible contact points for further clarification:

Research Department, Technology Transfer Office (TTO), International Office, Third Party Funding Administration, Export Control Office, KIWI

1.1. Has there been previous cooperation with the institution(s) or persons involved in the project? If yes, what were the experiences? ▶ explanation

1.2. Are there any inconsistencies or unverifiable information in the CVs or publication lists of those involved, as discernible from public sources? ▶ explanation

No

At present, no indications of further need for coordination.

Yes/Unclear

Further review/ coordination recommended.

Risk Mitigation Measures

e.g. verification of information, clarification with cooperation partners

1.3. Are there indications that project participants or institutions involved in the project have connections to the military or intelligence services? ▶ explanation

No

At present, no indications of further need for coordination.

Yes/Unclear

Further review/ coordination recommended.

Risk Mitigation Measures

e.g. assessment of implications, if necessary exclusion of cooperation partners

1.4. Are any of the persons or institutions involved directly or indirectly subject to sanctions or embargoes applicable in Germany? ▶ explanation

No

At present, no indications of further need for coordination.

Yes/Unclear

Further review/ coordination recommended.

Risk Mitigation Measures

exclusion of affected persons/institutions

1.5. Are there security-related or ethical requirements imposed by the German or foreign funding body? ▶ explanation

No

At present, no indications of further need for coordination.

Yes/Unclear

Further review/ coordination recommended.

Risk Mitigation Measures

e.g. implementation of requirements in the cooperation design

2. Export Control

The following questions address cooperation dimensions that may be relevant under export control law. Where there are indications of potential risks, and in cases of doubt, consultation with the institution's Legal Department or Export Control Office, or directly with the Federal Office for Economic Affairs and Export Control (BAFA) is essential.

Possible contact points for further clarification:

Legal Department/Export Control Office, Information Security/IT Security, Research Department, Laboratory and Infrastructure Management, Data Protection Officer, BAFA, KIWI

2.1. Does the cooperation concern a field of research or technology designated as sensitive by the Federal Office for Economic Affairs and Export Control (BAFA)?

[▶ explanation](#)

No

At present, no indications of further need for coordination.

Yes/Unclear

Further review/coordination recommended.

Risk Mitigation Measures

Implementation of export control requirements

2.2. Is there a possibility that the cooperation results could be used for non-civilian purposes (dual use)?

[▶ explanation](#)

No

At present, no indications of further need for coordination.

Yes/Unclear

Further review/coordination recommended.

Risk Mitigation Measures

Implementation of export control requirements

2.3. To which Technology Readiness Level can the (research) cooperation be assigned? ▶ explanation

TRL 1 – 3
Fundamental research (principles, concepts, initial experiments)
At present, no indications of further coordination.

TRL 4 – 6
Development & validation (laboratory/ pilot-scale project)
Further review/ coordination recommended.

TRL 7 – 9
Demonstration, deployment readiness, market-oriented development
Further review/ coordination recommended.

Risk Mitigation Measures

Implementation of export control requirements

2.4. Does the cooperation involve the use or transfer of sensitive equipment, software, laboratory infrastructure or technologies that may be subject to licensing requirements? ▶ explanation

No
At present, no indications of further need for coordination.

Yes/Unclear
Further review/ coordination recommended.

Risk Mitigation Measures

Implementation of export control requirements

2.5. Do extraterritorial export control regulations of other countries need to be considered? ▶ explanation

No

At present, no indications of further need for coordination.

Yes/Unclear

Further review/ coordination recommended.

Risk Mitigation Measures

Implementation of export control requirements

2.6. Is there a risk that sensitive data, technologies or systems might be processed, used or made accessible without adequate protection in the context of the cooperation? ▶ explanation

No

At present, no indications of further need for coordination.

Yes/Unclear

Further review/ coordination recommended.

Risk Mitigation Measures

e.g. access regulations

3. Exploitation of Results and Intellectual Property Rights

The following questions address the use and exploitation of cooperation results. It is strongly recommended that aspects of utilisation and exploitation be defined in advance of cooperation through a written agreement with all partners.

Possible contact points for further clarification:

Research/Transfer Department, Legal Department, where appropriate external legal counsel on international contractual arrangements is provided, KIWi

3.1. Are there indications of unintended or non-transparent use, exploitation or publication of cooperation results? ▶ explanation

No

At present, no indications of further need for coordination.

Yes/Unclear

Further review/coordination recommended.

Risk Mitigation Measures

e.g. written utilisation agreement

3.2. Are one's own scientific interests and those of the home institution adequately safeguarded in relation to the reciprocal use, exploitation and publication of project results? ▶ explanation

No

At present, no indications of further need for coordination.

Yes/Unclear

Further review/coordination recommended.

Risk Mitigation Measures

e.g. internal consultation, written cooperation agreement

4. Research Ethics

The following questions address aspects of research integrity and ethics in context of cooperation. They are relevant not only from an academic and ethical perspective but also in terms of potential reputational risks for the partners involved and for the home institution.

Possible contact points for further clarification:

Committee for Ethics of Security-Relevant Research/Ethics Committee, International Office, Legal Department, KIWi

4.1. Are there concerns that the principles of good scientific practice and integrity may not be upheld within the cooperation? ▶ explanation

No

At present, no indications of further need for coordination.

Yes/Unclear

Further review/ coordination recommended.

Risk Mitigation Measures

e.g. discussion with partners involved in the project, written agreement

4.2. Is academic freedom at risk due to governmental or institutional constraints in the cooperation context? ▶ explanation

No

At present, no indications of further need for coordination.

Yes/Unclear

Further review/ coordination recommended.

Risk Mitigation Measures

e.g. discussion with partners involved in the project, inclusion of exit strategies

4.3. Could the project or its outcome be misused for unwanted influence or political propaganda? ▶ explanation

No

At present, no indications of further need for coordination.

Yes/Unclear

Further review/ coordination recommended.

Risk Mitigation Measures

e.g. discussion with partners involved in the project, consideration within the project design

4.4. Might the cooperation entail risks of endangerment or persecution for German or international partners? ▶ explanation

No

At present, no indications of further need for coordination.

Yes/Unclear

Further review/ coordination recommended.

Risk Mitigation Measures

e.g. discussion with those involved in the project, elimination of risks in project design

COMPLETED BY:

Name & Position

Date

Institution, Department

Notes on Background and Use of the KIWi Checklist

The KIWi Checklist Knowledge Security was developed by the DAAD's Centre for International Academic Cooperation (KIWi) and is based on five years of expertise in advising on security-relevant issues in international academic cooperation. KIWi employs the checklist in its own advisory practice as a framework for assessing cooperation-related risks. The checklist is not primarily intended as a formal review or approval mechanism; rather, it serves as a criterion-based tool for self-assessment. It may be applied both in the planning and in the implementation of cooperation projects. Responses should be guided by the principle of due diligence. This involves the careful collection, analysis, and evaluation of cooperation-related information. A due diligence review generally involves the identification, analysis and evaluation of publicly available or otherwise

accessible information relevant to those responsible for the cooperation. This provides the basis for identifying security-relevant risks, which may in turn trigger further coordination, review processes, or risk mitigation measures.

The preparation of the KIWi Checklist Knowledge Security drew on the perspectives and experience of numerous experts from academia, research management and higher education administration (including International Offices, Export Control and Legal Departments, and Information Security Offices). We gratefully acknowledge their support.

Please note: This publication is provided for information purposes only and does not constitute legal advice. Any liability is excluded.

Practical Guidance and Explanations

The following explanations provide additional background and supplementary information on the four thematic sections of the checklist. Selected sources for further references are also included.

COOPERATION PROFILE

The profile at the beginning of the checklist covers the core elements of the cooperation (thematic focus, institutions involved, form of cooperation, source of funding) as well as the potentials and strategic objectives of the cooperation (e.g. scientific objectives, transfer/exploitation of results, and development of strategic networks).

The disciplinary focus and the participating countries are particularly relevant for assessing potential risks. A considerable number of the checklist's questions are of particular significance for application-oriented, technical, and natural science disciplines, as well as for cooperation with partner countries that are subject to export control restrictions or international sanctions. The type of cooperation is likewise relevant for the assessment of risks. For example, student or teaching exchanges generally entail lower risks in terms of export control and exploitation. Nonetheless, attention also has to be paid to the risks of unauthorised dissemination of knowledge, to issues of research ethics, and, where relevant, to considerations of personal safety. For research collaborations, all questions in the checklist are relevant, regardless of the focus of the research and the countries involved in the cooperation. Partnerships with industry or industry-related institutions may require additional scrutiny regarding export controls as well as patent and intellectual property rights.

1. PARTNERS AND FUNDING

Information on partners and funding provides transparency and forms the basis for/of a trustworthy cooperation relationship. In particular, potential breaches of sanctions or embargoes must be excluded.

QUESTION 1.1

[▲ back](#)

Where cooperation partners are already known from earlier collaborations, previous experiences – particularly sensitive ones – should be reflected upon and incorporated into the design of the current project.

QUESTION 1.2

[▲ back](#)

For new partners (e.g. international requests for cooperation), verification of academic biographies and publication records is essential to establish a reliable foundation for collaboration. Inconsistencies or gaps in publicly available information do not automatically imply misconduct, but they may signal the need for closer review. Such verification processes promote transparency, protect academic integrity, and contribute to risk assessment.

QUESTION 1.3

[▲ back](#)

Links between partners or institutions and military, or military-affiliated entities, may be of direct security relevance (to dual-use risks). They ought to be carefully considered both with regard to their implications and from an ethical perspective. The political context of the partner country is a critical factor here. Early clarification enables compliance with legal obligations, such as non-proliferation and export control regulations, the identification of unintended consequences, and the avoidance of reputational risks.

Selected sources of information on 1.2 and 1.3 – due diligence

- [KIWi Compass – No red lines Academic cooperation under complex Framework Conditions.](#)
- [Safeguarding-Science.eu](#)
- [Safeguarding Research in Canada. A Guide for University Policies and Practices](#)

QUESTION 1.4

[▲ back](#)

The involvement of institutions or individuals subject to embargoes or sanctions may entail legal implications. Relevant provisions of the EU, UN or individual state regulations may restrict, prohibit, or render subject to authorisation cooperation in

specific disciplines or technology fields. It is therefore essential to verify whether individuals or organisations are subject to sanction regimes. Publicly accessible websites can be used to check individuals and organisations directly against sanction lists. Please note that apparent matches be verified against additional information, as name similarities may occur.

Indirect or secondary references to sanctions must also be taken into account: Even if none of the cooperating individual or institution appears on the list, a connection may exist, for example, where indications arise that organisations are controlled by sanctioned individuals/companies, or where listed actors control essential resources, financial flows or infrastructure. In such cases, a more detailed examination should be undertaken, for example by requesting a declaration from the organisation concerned, including disclosure of ownership and control structures.

Selected sources of information on 1.4 – sanctions and embargoes

- [BAFA Information Country Embargoes](#)
The overview provided by the BAFA on country-specific and individual embargoes serve primarily as an information source. It is particularly useful for evaluating cooperation countries and research locations, as well as for assessing the export of materials and equipment.
- [United Nations Security Council Consolidated List](#)
Central list of all sanctions imposed by the United Nations Security Council.
- [EU Sanctions Map](#)
An interactive map with detailed information on all sanctions imposed by the EU (both autonomous and implementing UN measures).
- [Financial Sanctions List \(FiSaLis 2025\)](#)
The official database of the Bundesbank for checking whether individuals or organisations are subject to EU financial sanctions. It includes links to legal acts and is also used as a reference by the judiciary and public administration. In case of a match, relevant EU regulations are linked, enabling the legal basis and precise content of the sanction to be verified.

- [Sanctions List Search](#)

A US verification tool for all sanctions lists administered by the Office of Foreign Assets Control (as part of US export control law). Although not directly binding, it may be relevant due to extra-territorial legal effects, for example in cases involving a US nexus.

QUESTION 1.5

[▲ back](#)

The financial basis of cooperation should be scrutinised to identify any potential implications. Unilateral financial dependencies on international partners should be avoided. Third-party funding may entail political requirements.

Selected sources of information on 1.5 – third-party funding and political funding requirements

- [German Foreign Trade and Payments Act \(Außenwirtschaftsgesetz – AWG\)](#)
- [Foreign Trade and Payments Ordinance \(Außenwirtschaftsverordnung – AWW\)](#)
- [Federal Office for Economic Affairs and Export Control \(BAFA\) Handbook: Export Control and Academia \(2nd edition\)](#)
- National funding guidelines (in Germany and, where applicable, in the partner country)

2. EXPORT CONTROL

Export controls regulate and restrict the export of material goods and the transfer of knowledge or information, known as intangible goods. Proliferation risks may arise, for example, in the export of laboratory equipment, materials, software or process technologies. In the context of academic cooperation, consideration should also be given to the transfer of intangible knowledge and technologies within joint research projects. As violation of export control regulations can have legal consequences, it is strongly recommended to consult the competent institutional offices within the higher education institution and, where appropriate, with the Federal Office for Economic Affairs and Export Control (BAFA).

QUESTION 2.1[▲ back](#)

In assessing regulatory aspects, it is particularly important to clarify whether the existing or planned cooperation falls within a technological or research field that according to the BAFA, is classified as sensitive and thereby entails a licence requirement related to specific goods or their intended usage.

These include, among others:

- Biology, including Biotechnology and Medicine,
- Chemistry and Biochemistry,
- Physics,
- Nuclear technology,
- Energy and Environmental technology,
- Information and Communication technology,
- Aerospace,
- Mechanical engineering,
- Materials science and Engineering,
- Process engineering,
- Electrical engineering.

QUESTION 2.2[▲ back](#)

Of particular relevance in terms of export control are research collaborations with dual-use potential, i.e. the possible application of technologies or goods for both civilian and military purposes. Potentially, almost all technologies can also be used for military purposes. For this reason, research is increasingly characterised as having a multiple-use dimension. The central concern is therefore a careful weighing of risk potentials.

QUESTION 2.3[▲ back](#)

In view of a potential (military) application, the evaluation of the Technology Readiness Level (TRL) is also of critical importance. The TRL scale measures the development of a given technology, ranging from basic research (TRL 1–3) to the application-oriented development (TRL 4–9). At levels 4–9, a more detailed export-control assessment is strongly recommended. For research projects in the social sciences, the Societal Readiness Level (SRL) may also provide a valuable reference point.

QUESTION 2.4[▲ back](#)

It must also be noted that certain devices, software or technologies may be subject to licensing requirements under the EU dual-use regulation, EU and national control lists, or embargo provisions.

Determining whether such requirements apply cannot usually be undertaken by project leadership alone. Dedicated Export Control Offices or Legal Departments within higher education institutions, as well as BAFA, can assist in consulting the relevant lists and regulations, making the classification, and, where necessary, preparing licence applications.

Selected sources of information on 2.1 – 2.4 – sensitive technology areas and dual-use

- [Federal Office for Economic Affairs and Export Control \(BAFA\) Handbook: Export Control and Academia \(2nd edition\)](#)
- [Federal Office for Economic Affairs and Export Control \(BAFA\) Control Lists](#)
- [General Introduction to Export Control](#)
- [EU dual-use regulation \(EU 2021/821\)](#)
- [Foreign Trade and Payments Act \(Außenwirtschaftsgesetz – AWG\)](#)
- [Foreign Trade and Payments Ordinance \(Außenwirtschaftsverordnung – AWW\)](#)
- [Leopoldina and DFG Recommendations of the Joint Committee on the Handling Security-Relevant Research](#)
- [Principles of Good Scientific practice of the German Research Foundation](#)
- [Position Paper of the German Council of Science and Humanities ‘Science and Security in Times of Global Political Upheaval’](#)
- [Technology Readiness Levels](#)
- [Societal Readiness Levels](#)

QUESTION 2.5[▲ back](#)

Export control law may, for example in the case of the USA, also have extraterritorial applicability. Once US-origin goods, software, technologies or components are utilised, US regulations may apply to non-US individuals or institutions abroad, even where the usage takes place exclusively within Germany.

Selected sources of information on 2.5 – extraterritoriality

- [Federal Office for Economic Affairs and Export Control \(BAFA\) Handbook: Export Control and Academia \(2nd edition\)](#)
- [Sanctions List Search](#)

QUESTION 2.6

[▲ back](#)

Critical physical and digital infrastructures relevant in the cooperation context should be identified at an early stage. This enables the integration of necessary protective measures into the project design from the outset as well as the implementation of suitable registration and access control systems.

Selected sources of information on 2.6 – sensitive data and infrastructures

- [General Data Protection Regulation \(GDPR\)](#)
- [Leopoldina and DFG Recommendations of the Joint Committee on Handling Security-Relevant Research](#)
- [EU dual-use regulation \(EU 2021/821\)](#)
- [German Council of Science and Humanities Position Paper: ‘Science and security in times of global political upheaval’](#)

3. EXPLOITATION OF RESULTS AND INTELLECTUAL PROPERTY RIGHTS

In research cooperations, questions related to the use and exploitation of results are of particular relevance. As a general principle, these should be discussed and set out in a written agreement by all cooperation partners prior to the commencement of the collaboration. Institutional strategic interests should be clearly defined and coordinated internally beforehand.

QUESTION 3.1

[▲ back](#)

Prior to the commencement of any cooperation, issues relating to the use and exploitation of results should be discussed with project partners and formally documented in a written agreement. These should include address IP ownership and licensing, confidentiality and publication rights, patent filing and open-access strategies. Legal and regulatory

requirements, such as national and international provisions on intellectual property, data protection and patent law, may also be relevant. Additionally, internal institutional regulations governing the exploitation of research results should be taken into account where appropriate.

Selected sources of information on 3.1 – transparency and usage rights

- [General Data Protection Regulation \(GDPR\)](#)
- [German Patent and Trade Mark Office](#)
- [Intellectual Property Management \(Horizon Europe\)](#)
- [European Patent Office](#)

QUESTION 3.2

[▲ back](#)

With regard to the use and exploitation of cooperation content and results, it is strongly recommended that institutions and researchers consciously reflect upon, and safeguard, their own strategic objectives and interests within the framework of cooperation. A written cooperation agreement can serve to establish transparency and binding commitments and is therefore generally advisable.

Selected sources of information on 3.2 – strategic interests

- [WIPO – IP Policies for Universities and Research Institutions](#)
- [Fraunhofer IP guidelines](#)

4. RESEARCH ETHICS

Questions of research integrity and ethics should be considered before beginning any cooperation with partners in countries whose principles and values of democracy and the rule of law differ from those in Germany. Such considerations are equally of great importance with regard to potential reputational risks.

QUESTION 4.1[▲ back](#)

Where concerns arise regarding the research integrity of activities undertaken within the framework of cooperation, a more thorough review should be conducted and, if necessary, discussed with the cooperation partners. Written agreements defining cooperation rules and standards in advance can foster transparency and strengthen the binding nature of the cooperative framework.

Selected sources of information on 4.1 – research integrity

- [The Principles of Good Research Practice of the German Research Foundation](#)
- [The European Code of Conduct for Research Integrity](#)

QUESTION 4.2[▲ back](#)

Academic freedom is enshrined in Article 5 (3) of the German Basic Law. Particular care must be taken when cooperating with partners in countries where academic freedom is not guaranteed to the same extent as in Germany. The objectives, content and conditions of cooperation should be communicated openly and regulated in a binding manner. It is also advisable to design an exit strategy for use in case of failure to comply with agreed terms of the cooperation.

QUESTION 4.3[▲ back](#)

There remains, in principle, a risk that cooperative activities or outcomes may be misused for unwanted influence or political propaganda (e.g. manipulation, censorship or misuse of research results). If such indications arise, they should be addressed in the design and implementation of the project, with a corresponding exit strategy retained as an option.

QUESTION 4.4[▲ back](#)

International collaborations can give rise to risks concerning the individual security of project participants. This pertains, on the one hand, to issues of personal (including travel-related) security for both German and international participants in the cooperation. On the other hand, there remains the fundamental possibility that involvement in a cooperative project, or the publication of its results,

could expose participants to risks of endangerment or persecution. A careful risk assessment prior to the commencement of cooperation is therefore strongly recommended.

Selected sources of information on 4.2 – 4.4 – academic and freedom, influence and endangerment

- [Academic Freedom Index \(AFI\)](#)
- [Leopoldina and DFG, Recommendations of the Joint Committee on Handling Security-Relevant Research](#)

About Us

CENTRE FOR INTERNATIONAL ACADEMIC COOPERATION (KIWI)

The Centre for International Academic Cooperation (KIWi) of the DAAD supports German higher education institutions, scholars, and scientists in initiating and shaping their international cooperations. It provides individualised advice, brings together expertise from across the DAAD global network, and promotes peer-to-peer exchange through networking formats. KIWi not only provides guidance on the strategic design of higher education cooperations on an institutional level but also assists individual scientists and academics with questions related to their cooperation projects.

A key focus lies on case-specific advisory services aimed at the systematic assessment

and balancing of opportunities and risks in international academic cooperation projects. The present KIWi Checklist Knowledge Security serves as the principal foundation for this advisory work. In addition to individual project-based consultation, KIWi also supports German higher education institutions through full-day in-house seminars, accompanying them in the (further) development and institutional implementation of integrated security management systems. With these services, KIWi seeks to support and strengthen German higher education institutions, individual academics and scientists and researchers in pursuing interest-oriented, risk-reflective and competence-based approaches to international academic cooperation.



**Further information
is available
on our website.**

IMPRINT

Publisher

Deutscher Akademischer Austauschdienst e.V.
(DAAD)
Kennedyallee 50
D – 53175 Bonn

Phone: +49 228 882-0
Fax: +49 228 882-444

Email: kiwi@daad.de
Internet: www.daad.de

Authorised Representative of the Executive Committee:

Prof. Dr Joybrato Mukherjee
District Court of Bonn
Register of associations, number VR 2107
Sales tax number: DE122276332

Person responsible according to § 18 Abs. (2) MStV :
Dr Kai Sicks, Kennedyallee 50, 53175 Bonn, Germany

The DAAD is an association of German universities and their student bodies. It is institutionally funded by the German Federal Foreign Office.

Editorial Team

Centre for International Academic Cooperation
(KIWi)
Kennedyallee 50
D – 53175 Bonn

Realisation

Fazit Communication GmbH
Frankfurt am Main
Design and Layout: Anabell Krebs, Kerim Demir

Published as a digital publication on the internet
1st version September 2025
© DAAD

Photo credit

bagotajr/iStock (Title)



With funding from the:

