International Organization for Standardization
Organisation internationale de normalisation
Международная организация по стандартизации

ISO Research Grant 2024

Call for research proposals

Table of Contents

1. About the ISO Research Grant

The ISO Research Grant is awarded annually to a postgraduate student or a team (Masters, PhD or post-doc) to conduct a research study related to a theme proposed by ISO. The grant amount is 25,000 CHF. A different theme is proposed each year, but the broad focus is on evaluating the impacts of international standards.

Applicants submit a research proposal related to the year's theme. This proposal can be for a research project related to the researcher's academic work. However, it shall be for an original piece of work and must not have been previously published. ISO recognizes the right of the researcher to later produce a publication on the basis of the scientific results of the research submitted to ISO, provided that this does not interfere with the right of ISO to use the final output of the research for its own purposes, including for marketing and promotional activities (in any media).

In particular, ISO will be granted a worldwide, royalty-free, perpetual, non-exclusive right and license to use, copy, publish, modify, create derivative works therefrom, distribute or make available the final output or translations of it, for any of its own purposes, provided that appropriate credits to the author are given. For example, the final output of the research would be used by the ISO/CS Strategy and Research unit to create materials for dissemination for the attention of ISO members (the format of these materials will depend on the nature of the study). The researcher will also provide ISO with all data used in the project. Access provisions will be negotiated depending on data sources and applicable law, but ISO must have access to all data included in the final report, including data collected by the researcher directly.

The awarding of the grant does not create any employer-employee relationship with ISO. The researcher or their employing institution will be responsible for paying all the taxes applicable to the fees they will receive. Further details may be defined in a separate contractual arrangement, which will govern the relationship with the selected researcher.

2. Theme 2024

The ISO Research Grant, awarded annually, provides an opportunity for postgraduate students or teams of students to conduct a research study related to a theme proposed by ISO. The 2024 theme for the ISO Research Grant is “Standards for cybersecurity”. This theme is a reflection of the growing importance of cybersecurity in our increasingly digital world.

ISO already has an established presence in the area of cybersecurity, with ISO/IEC 27001 and ISO/IEC 27035, for example, identified as key standards for building a resilient cybersecurity strategy. ISO/IEC 27001 lays the groundwork for a robust cybersecurity strategy by instilling a systematic approach to information security management, while ISO/IEC 27035 focuses on incident management and response. These standards collectively strengthen cybersecurity strategies, ensuring that they are not only effective but also efficient, maximizing the impact of resources in an era where agility is paramount.

As we step into 2024, the field of cybersecurity brings forth new challenges and opportunities for organizations worldwide. Cyber threats are evolving at an unprecedented rate, necessitating a strategic and comprehensive approach to safeguard sensitive information and maintain operational integrity. The ISO Research Grant 2024 aims to further investigate the role standards can and have played in technology governance and supporting a safer cyberspace.

This year’s research grant theme underscores the critical role of standards in enhancing cybersecurity and invites innovative research proposals that evaluate the impacts of international standards in this domain. It is an exciting opportunity for researchers to contribute to this vital field and help shape the future of cybersecurity standards.

Annex 1 offers a list of examples of topics relevant to the theme. Applicants may choose to develop one of them or to propose a different topic of their own. This list is by no means exhaustive and is simply provided for inspiration. What is critical, however, is that the topic of this year’s Research Grant shows originality and adds to the existing body of available research. Annex 2 includes a series of relevant materials and webpages that can be of benefit to connect the theme with pre-existing work.

3. Eligibility criteria

To be eligible for the research grant, the applicant(s)* must be:

- Currently enrolled in postgraduate studies or a post-doc at an institution of higher education or a public research organization;
- Able to demonstrate the relevance of standardization to their field of study;

- Proficient in English (the study must be written in English).

*a joint proposal can be made by more than one person, provided that all applicants fit the above criteria. In the case of joint proposals, only one grant will be awarded.

4. Timeline

Milestone/steps	Date
Call for research proposals launched	22 April 2024
Deadline to submit research proposals	**1st July 2024 23:59 (CEST)**
Expected evaluation of proposals (including references)	July-September 2024
Announcement of winning proposal	October 2024
Contract negotiations	October-December 2024
Research kick-off meeting	January 2025
Deadline for submission of the final research to ISO	November 2025

5. Proposal elements and structure

Proposals for the ISO Research Grant must contain three elements:

1. Letter of motivation – Include, for example, your reasons for applying, your inspiration for the proposed study, why you are qualified to carry out this study and how you expect to benefit from it.
2. CV with 2 referees (e.g. supervisors)
3. Research proposal – Following the structure outlined in the table below. Please note: the proposal must not exceed 2,500 words, excluding references and annexes.

Section	Guidance on content
Title	Provide a short, concise title that conveys what your research is about.
Abstract	Describe the topic and aims of the study. Provide a summary of who will be involved in the research, the methods, the timeframe and a statement explaining the relevance of the research.
Introduction	Explain why you chose this topic, how your proposed research is relevant to the theme and how it contributes to the body of knowledge on impact of standards (significance to the research field).
Research question(s)	What is the question you are trying to answer? The purpose of this research; why it needs to be done.
Literature review /state of knowledge	Give a brief summary of relevant existing research related to the topic (including potential gaps or limitations) and an indication of potential sources. Demonstrate your understanding of the topic and its wider context.
Methodology	What is the systematic approach you will use to solve your research problem?

Research design and methods	Provide in depth description and justification of the methodology including sources of data, potential participants, methods of data collection, methods for data analysis and synthesis, limitations of the study.
Ethics	Are there any ethical concerns associated with your research proposal?
Data protection strategy	Are there any data protection risks associated with the research? Provide details of and elaborate on your data protection strategy in the context of the Research Grant project.
Communication of results	How will your research findings be shared? What is / are the foreseen research products?
Timeline	Estimate how long each task will take and show how you will complete your study in the given timeframe.
Detailed Budget	Indicate how the funds from the research grant will be allocated.
References	List of references used when writing the proposal.

6. How to apply

To apply for the ISO Research Grant, send your letter of motivation, CV and research proposal by email to research@iso.org before the **deadline of 23:59 (CEST) on Monday 1 July 2024**.

7. Selection criteria

The following selection criteria will be taken into account in selecting the grant winner.

Threshold criteria – proposals not meeting these criteria will not be given further consideration:

Domain	Criteria
Topic and project planning	Project topic is clearly relevant to the theme – topic identifies a link between International Standards and cybersecurity.
	Project budget is clear and calculations are correct.
Applicant background and support	Applicant's academic/professional background is relevant to the topic and proposed methodology.
	Applicant has the support of supervisors/appropriate referees.

Evaluation criteria – proposals meeting the threshold criteria will be assessed as follows:

Domain	Criteria	Weight
Quality of the project proposal	Soundness of the proposed methodology (including sufficient planning for access to data, outline of intended analytic approach, etc.).	30%
	Originality/novelty of the topic and importance of the results to the existing body of research.	15%
	Utility of intended project outputs (e.g. Full report, summaries, briefing points, etc.).	5%

	Written communication skills: clarity of message, structure and logical flow of proposal.	15%
	Budget outline: proposed budget represents effective planning and expenditure. Budget should be transparent, detailed and demonstrate value for money.	10%
	Data protection strategy: The proposal includes a sound data protection strategy, which is compliant with applicable data protection regulations and Section 10 of the Call for Proposals.	5%
Experience and expertise	Breadth and depth of experience and expertise in the proposed subject area: quality and relevance of previous publications and academic background.	12%
Motivation	Motivation expressed by the applicant: stated reasons for applying, inspiration for the proposed study, expected benefits for the student.	8%

ISO will not, except at its own discretion, provide information about the evaluation process, or feedback on individual submissions.

8. ISO Central Secretariat (ISO/CS) involvement

The ISO/CS Strategy and Research unit is responsible for all aspects related to management and administration of the award. The successful applicant(s) will be expected to keep the ISO/CS Research and Innovation unit informed about the progress of the study (for example, by providing regular progress updates. A schedule of updates will be agreed on with the successful applicant(s) as appropriate for the project plan).

The ISO/CS Research and Innovation unit will provide guidance and support to the successful applicant(s) in the completion of the study as far as possible (for example, by commenting on outlines/drafts, and providing contacts within ISO members or ISO-related data).

9. Legal Disclaimer

By responding to this ISO research grant proposal, applicants agree that ISO reserves the right to withdraw it for any reason and, shall not in any way be responsible for any costs incurred in the preparation and presentation of the application.

10. Data Protection

Shall processing of any personal data be necessary in the context of the Research Grant and the performance of the Services/Deliverables under the future Research Grant Agreement (hereafter referred to as the “Personal Data”), it is expected that the Applicants will comply with the applicable laws on the protection of personal data, in particular but not limited to, the Swiss Federal Data Protection Act (FADP) or any local regulations applicable to the protection of personal data, where applicable (hereafter referred to as the “Applicable Laws”), as well as in accordance with the purposes for which the Personal Data would be transmitted and/or processed.

It is also expected that the Applicants will undertake to inform the data subjects of the processing of Personal Data and obtain their consent, when and where this is required by Applicable Laws.

In the event it is envisaged that the personal data processing would be made on behalf of ISO and according to ISO’s instruction in the context of the Research Grant, Applicants undertake to sign a data processing agreement in parallel with the Research Grant Agreement, the provisions of which shall in principle prevail over those of the Research Grant Agreement. Unless a data processing agreement is signed, the recipient of the Research Grant will be considered to be processing personal data as an independent data controller.

Applicants will have to take in any case all appropriate technical and organizational measures to ensure the security of the Personal Data in the context of the Research Grant, in particular to prevent the Personal Data from being accessible to unauthorized persons, to ensure the availability of the Personal Data, to prevent the modification of the Personal Data without right or inadvertently and to enable the traceability of the processing.

In the event of a breach or an incident related to the security of Personal Data in the context of the Research Grant, Applicants will be expected to immediately inform ISO and take immediate steps to identify and understand the reasons and circumstances of the breach or incident. It is also expected that they will take the necessary measures to put an end to the breach and mitigate its consequences for the persons concerned.

If the Applicants are located in a country that does not have an adequate level of protection under the Applicable Laws (i.e., outside the EEA, Switzerland, UK, Canada, New Zealand, Uruguay, Argentina or Israel), it is expected that Applicants will have the ability to take appropriate measures to ensure an adequate level of protection for transfers of Personal Data. The Applicants will have to agree in such event to enter into the standard contractual clauses approved by the European Commission Implementing Decision (EU) 2021/914 of 4 June 2021[1] and any modifications required by the Applicable Laws (the “Standard Contractual Clauses” or “SCC”) and which will be implemented into the Research Grant Agreement.

Where applicable, and if necessary, it is expected that Applicants shall have the ability to provide all necessary assistance to ISO in the context of ISO’s performance of its obligations under the Applicable Laws, for example: establishing and updating the register of processing activities, carrying out data protection impact assessments and responding to requests from authorities or data subjects.

11. Contact

Please contact research@iso.org if you have any questions or require further information about the ISO Research Grant.

[1] As currently set out at https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj

12. Appendix 1: Research Examples

The following table contains possible generic topics for applicants to explore or take inspiration from. The list is by no means exhaustive and any original contributions that address the theme (standards and cybersecurity) and respect the established criteria will be considered equally.

CATEGORIES	FOCUS	EXAMPLES
IMPACT STUDIES	- Specific standard/group of standards - Theme: sector, geographic focus…	Evaluate: • the impacts of ISO XXXXX on Y • the contribution of standard(s) XXXXX on Y • how much/whether standards help promote good cybersecurity governance in (X sector; X geographic region…) Note: impact studies could be quantitative, qualitative, or both
USE OF STANDARDS	- Specific standard/group of standards - Theme: sector, geographic focus…	• Choose one or more ISO standards and investigate who is using them, how and why (or why not) • Explore the standards landscape in a sector, or a geographic region to see where ISO standards fit in - what other standards/guidelines are being used and where the gaps are
MARKET NEEDS	- Are current standards addressing market needs? - What new standardization opportunities exist?	Select one or multiple challenges/risks that society could face as a result of breaches in cybersecurity: • What is the potential role of standards to address these challenges? • Do standards already exist to tackle those risks? • What may be missing (standardization agenda)? • What could be the limitations?
STANDARDS RELATIONSHIP DYNAMICS	Standards and regulations	Explore: • the connection between ISO standards and regulations in a chosen sector or geographic region. Are ISO standards referenced? What other standards/ guidelines are being used and where are the gaps? • the role of ISO standards in helping drive cyber-resilience. What standards are being used and at which level (for example terminology, evaluation, reporting...)? • the relationship between regulatory compliance and international standards

	Involvement of civil society and vulnerable people	• Assess the involvement of civil society and vulnerable people in the standardization process • Evaluate the contribution of standards to a more equitable access to cyber-resilience / privacy-protection • Investigate the awareness about/ access to/ use of standards in vulnerable countries, to protect vulnerable groups or small businesses. Are relevant standards used by those who need them most (how and why, or why not)?

13. Appendix 2: Resources

Web pages and relevant ISO committees

ISO Online Browsing Platform - The OBP lets users partially access standards, providing key information such as introductions, scope, normative references, and bibliographies. Applicants may find this useful if choosing to focus their proposal on a specific standard.

ISO Research Library – The library offers a collection of research publications on standards and standardization.

ISO/IEC JTC 1/SC 27 – Information security, cybersecurity and privacy protection

Iso.org – ISO/IEC 27000 family – Information security management

Brochures and news articles

ISO – Keeping cyberspace safe for 30 years

ISO – Protecting our privacy in smart cities

ISO – Keeping cybersafe