CHESS

Cyber-security Excellence Hub in Estonia and South Moravia

D5.1
Risk Management Plan

Project Name	Cyber-security Excellence Hub in Estonia and South Moravia
Project acronym	CHESS
Grant agreement no.	101087529
Call	HORIZON-WIDERA-2022-ACCESS-04
Type of action	HORIZON-CSA
Project starting date	1 January 2023
Project duration	48 months
Deliverable Number	D5.1
Deliverable name	Risk Management Plan
Lead Beneficiary	Masaryk University
Type	R — Document, report
Dissemination Level	PU - Public
Work Package No	WP5
Date	02 August 2024
Version	2

Funded by the European Union

Funded by the European Union under Grant Agreement No. 101087529. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or European Research Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

Editor

- Zuzana Vémolová (MUNI)

Contributors

- Pavel Čeleda (MUNI)
- Jan Hajný (BUT)
- Mubashar Iqbal (UTARTU)
- Antonín Kučera (MUNI)
- Lukáš Malina (BUT)
- Raimundas Matulevičius (UTARTU)
- Václav Matyáš (MUNI)
- Petr Švenda (MUNI)
- Jan Willemson (Cybernetica AS)

Reviewers

- Raimundas Matulevičius (UTARTU)
- Václav Matyáš (MUNI)

CHESS Consortium

Participant organization name	Short name	Country
Masaryk University	MUNI	Czechia
University of Tartu	UTARTU	Estonia
Brno University of Technology	BUT	Czechia
Tallinn University of Technology	TalTech	Estonia
Cybernetica AS	CYBER	Estonia
Red Hat	RedHat	Czechia
Guardtime	Guardtime	Estonia
Estonian Information System Authority	RIA	Estonia
CyberSecurity Hub	CSH	Czechia
National Cyber and Information Security Agency	NCISA	Czechia
South Moravian Innovation Centre	JIC	Czechia
Estonian Information Security Association	EISA	Estonia

Abbreviations

CA – Challenge Area
CHESS – Cyber-security Excellence Hub in Estonia and South Moravia
F4SLE – Framework for Security Level Evaluation
ICT – Information Communications Technology
IoST – Internet of Secure Things
R&I – Research & Innovation
WP – work package
KPIs – key performance indicators

Table of Contents

List of Tables

1. Introduction

This Risk Management Plan outlines the risk management procedures of the CHESS project. It describes the factors the CHESS consortium considers as potential risks for implementing the project activities, defines the estimated impact of the risks, and proposes risk-mitigation measures.

The document offers an overview of the project's general practices and management procedures; it describes the management structure, communication strategies, and channels to monitor the progress efficiently.

The project proposal [1] already includes some of the risks and principles described in this document. However, this Risk Management Plan offers a more detailed analysis when the consortium examines more closely management-related risks and includes a new perspective – that of Challenge Area Leaders. Therefore, a detailed description of risk management on the level of the work packages is followed by the list of risks and mitigation measures from the standpoint of the CHESS Challenge Areas.

The **CHESS project** brings together leading R&I institutions in both regions to build connected innovation ecosystems to address one of Europe's most critical issues: Cyber-Security. South Moravia is a primary ICT industry & education powerhouse of the Czech Republic, with a focused and coherent smart specialisation strategy targeting cybersecurity. Estonia is among the most advanced digital societies globally, with exceptional e-government deployment. The CHESS Hub aims to conduct a thorough needs analysis of the two regions and develop a joint cross-border R&I strategy for cybersecurity.

The CHESS project will develop a joint cross-border cyber-security research and innovation strategy focusing on six **Challenge Areas**: Internet of secure things, Security certification, Verification of trustworthy software, Security preservation in blockchain, Post-quantum cryptography, and Human-centric aspects of cyber-security. The strategy development will be aided by implementing pilot projects reinforcing cross-regional collaboration, engaging regional innovation ecosystems and building evidence for future projects. Training and knowledge transfer will remove gaps in skills and expertise in the regions. Finally, dedicated task forces will ensure the sustainability of CHESS by integration with regional, national, and EU-level strategies and funding programmes.

2. Management Structure and Communication Channels

The management structure of the CHESS project and complex communication channels ensure efficient project monitoring and information flow. The project partners use internal mailing lists for communication between all participants. MUNI, responsible for *WP5 Project Management*, has established an electronic project monitoring workspace to keep all documents common to the project available to all partners. The consortium uses an all-inclusive and consensus-based management style. We have simple, straightforward management structures with clearly defined roles and responsibilities throughout the project.

Project monitoring will take place at several levels of project management. The consortium has already established crucial management structures. The Management Team of Masaryk university includes a Project Coordinator, Project Manager, Financial Manager with extensive expertise in financial management, and an administrative team that supports them. UTARTU has designated its management team that coordinates activities in Estonia and is led by UTARTU Project Leader.

In close cooperation with the Project Manager, the Project Coordinator monitors the project to identify situations/points when identified risks can occur to take preventative/corrective measures. The PC supported by his team also tracks performance indicators defined in this proposal as objectives, tasks, deliverables, milestones, person-months, budget consumptions and risks.

MUNI and UTARTU hold monthly meetings to discuss general management issues. Each month, Project Coordinator, in cooperation with the Project Manager, prepare a meeting agenda. If necessary/beneficial, other partners or WP Leaders are invited to join the meeting.

CHESS Thematic Working Groups are networks of researchers and innovators responsible for development within the six Challenge Areas. Each Challenge Area group includes several project partners from South Moravia and Estonia. The groups meet regularly, and these meetings are open not only to official members but to anyone from or outside the consortium interested in the topic. Each group has a Leader and Co-leader who coordinate the group's activities. They cooperate closely with WP Leaders and communicate regularly with the Project Coordinator and Project Manager. Project Manager also participates in the Challenge Areas Groups meetings to monitor progress, provide essential information and support the teams.

The **CHESS Strategy Board** consists of the Project Coordinator, UTARTU Project Leader, WP Leaders, one representative from each region for each Challenge Area (Leaders and Co-Leaders) and representatives of government agencies RIA and NCISA. The Board meets at least five times a year, and the Project Manager also participates in every meeting. Challenge Area Leaders provide a short update about the activities within their CAG during each Strategy Board meeting. This way, CHESS partners can identify any potential problems or delays in work in time and take necessary actions.

The **Steering Committee** is the main decision-making body, consisting of 1 representative from each partner. The Project Coordinator and UTARTU Project Leader co-chair the meetings. The Steering Committee will meet online every six months and in person every 12 months, co-scheduled with other activities.

By the end of 2023, the Steering Committee will establish other necessary management bodies: The CHESS Sustainability Task Forces and CHESS Project Development Groups will bring in additional resources to extend project activities further. CHESS Exploitation Board will advise researchers with a vision to commercialise and/or deploy their results. CHESS Advisory Group will facilitate coordination with EU and national-level strategies.

Risk monitoring at all levels is based on **high-quality communication** between the different actors and **timely reporting of any problems**. Each partner is responsible for reporting any risky situation to the Project Coordinator. WP Leaders monitor the progress within their respective work package, and Challenge Area Leaders are responsible for the risk monitoring within their CA. Project Coordinator, Project Manager, WP Leaders and CA Leaders meet regularly during the Strategy Board meetings. They inform each other regularly about the progress within their agendas and any delays or drawbacks that might affect the project objectives or their successful completion.

3. Risk Management on Work Package Level

Table 1 describes the possible risks related to the project work plan and the remedial actions on the level of work packages. We also classify their probability and negative impact (likelihood: low, medium, high; impact: low, medium, high).

Table 1 Risks and Remedial Actions

Risks	WP	Proposed risk-mitigation measures
Weak policy support for cybersecurity R&I (likelihood: medium; impact: medium)	1	Work with policy-making stakeholders (RIA, CSH, NCISA, eGA, Ministries) to understand their concerns and include them in strategy design. CHESS partners will seek their contributions actively in T1.1-T1.4, and in T1.5, we will reach out to the policy sector to ensure the representation of cybersecurity in relevant strategies. Also, the consortium will work closely with the CHESS Advisory Group to facilitate coordination with EU and national level strategies.
Lack of standardisation and harmonisation hindering market opportunities (likelihood: medium; impact: high)	1-4	We actively shape the regulatory landscape in cybersecurity by focusing on Security Certification of software, devices, and organisations according to selected national (F4SLE) and international (Common Criteria, NIST 140, EUCC) standards of focus. The CHESS R&I framework connects certification with synergic areas, such as software verification and IoST, and involves human-centric aspects in cybersecurity certification. We will prevent this risk by the pre-emptive design of solutions to contribute to both certification (by existing standards) and standardisation with harmonisation of cybersecurity practices and actively create market opportunities via such practices.
Lack of stakeholder involvement in strategy building (likelihood: medium; impact: high)	1	We have designed a stepwise process for strategy development in WP1. It involves mapping the ecosystems, connection to regional stakeholders from all sectors through brokerages (scheduled to mid-project period to be able to showcase first piloting results), and their engagement through the flexible architecture of working groups and task forces. We created liaisons that can be utilized in case of this risk emerging.
Lack of interest in training events from external target groups (likelihood: low; impact: medium)	2	We have a reserved budget to support the participation of external audiences (internationally and cross-sectorally) through travel grants. Upon registration, participants will have the opportunity to ask for a contribution to their travel costs. We will promote the events using expert communities that we are part of, such as through the Cybersecurity Competence Pilot consortia.
Communication and implementation problems (likelihood: low; impact: medium)	1-5	Consortium members experienced in international projects will communicate regularly via email, MS Teams, and in person. Project Manager, CA leaders and WP leaders are prepared to redesign and reattribute activities within the

		consortium and seek expertise in the Advisory Group in case circumstances should change and this risk increase.
Expenses exceeding budget (likelihood: low; impact: medium)	5	Experienced Financial Manager will regularly review expenditures and work with partners to ensure timely and accurate cost certification. Identified expense issues will be resolved through standard institutional procedures and knowledge/experience of dedicated senior administrative staff.
Circumstances prevent in-person meetings/ events (likelihood: medium, impact: low)	1-5	Whenever possible, we will organise smaller or online meetings. We will schedule events during the period when the likelihood of travel complications is the lowest. In case of adverse events and circumstances that may cause travel problems we will be ready to hold also wider meetings online.
Lack of funding beyond CHESS project to implement the cross-regional strategy (likelihood: medium; impact: high)	1	Within WP1, we will use dedicated Sustainability Task Forces to seek a good representation of CHESS priorities in regional, national, and European strategies to determine the future allocation of public resources.
Peripheral location of Estonia and South Moravia, which makes them less attractive to the best talents (likelihood: low; impact: medium)	1-3	With the increased reputation of regional institutions, Estonia and South Moravia will become much more attractive destinations for talented researchers. We will promote professional opportunities (e.g. close cooperation between academia and industry) and other benefits of coming here when advertising to potential PhDs, researchers and ICT professionals (e.g. safety, good school education for families with children etc.). Inviting the international audience to a significant fraction of our training events will showcase the excellent conditions and expertise available in the regions.
Low preparedness of public sector for deployment of cybersecurity innovation (likelihood: medium; impact: medium)	1-3	We actively integrate public sector representatives into our strategy-building activities, especially RIA (but also CSH), which frequently serves as the implementing body NCISA, having vital roles in leading the tasks of WP1. Local administrations support the CHESS initiative and will be invited to participate in discussions on strategies and actions to ensure proper representation of their needs and in piloting activities, typically as end-users.
Important team members leaving the team (likelihood: medium; impact: low)	1-5	The consortium is built on previous cooperation; many members have known each other for a long time and have strong partnerships. If a vital team member leaves, project partners will select an alternative team member capable of implementing the tasks. The Steering Committee will select an alternative research direction in case of significant drop-out within a Challenge Area.

Delayed implementation according to the project schedule (likelihood: medium; impact: medium)	1-5	Project Coordinator will monitor the progress. The regular project monitoring will cover financial aspects and achievements/milestones in individual work packages and on the level of 6 Challenge Areas. Project Coordinator/Manager will track achievements/progress through KPIs.
Personnel fluctuation in Coordinator's administrative team (likelihood: medium; impact: low)	1	Masaryk University has substantial experience in the management of EU funding. There is a strong pool of managerial (3 senior potential leads already identified) and administrative workers (2 fallback candidates identified) capable of alternating with each other.
Delay in one partner's work will negatively influence the workflow of the whole group (likelihood: medium; impact: high)	3	Close monitoring of the progress, regular meetings of the CA groups, good communication and close cooperation of all members of the CA groups. We will try to minimise the risk of potential bottlenecks that could hinder the work of the partners involved. Most importantly, we will identify and communicate benefits for parties involved in our R&I efforts, i.e., offer them knowledge, experience or at least benchmarking with similar institutions in both the Czech Republic and Estonia, and thus help identify internal opportunities for improvement.
Problem in the recruitment of new research staff (likelihood: low; impact: medium)	3	The PI in the participating partners should continuously look for new, talented staff members and hire them for the project. Active recruitment of students attending courses on related topics, creating appropriate motivation factors.

4. Risk Management on the Level of Challenge Areas

CHESS Challenge Areas (CAs) are the cornerstone of the CHESS project activities. Challenge Area Leaders will work closely with WP Leaders, Project Coordinator and Project Manager. Most of the work done will be on the level of individual Challenge Areas. Therefore, considering potential risks from their perspective is crucial. Tables 2-7 describe possible risks and mitigation measures viewed by and discussed with the CA Leaders.

Table 2: Risk Management in CA1: Internet of Secure Things:

Risks	CA	Proposed risk-mitigation measures
Lack of interest of external partners/ companies in contributing to empirical research on the use of ITS/IoST (likelihood: medium; impact: medium)	CA1	Collecting partners' feedback and their needs in ITS and IoST cybersecurity. Focusing on research topics related to companies and institutions in South Moravia and Estonia. Offering and explaining benefits for external partners and companies from their participation in the research activities. Interviewing selected partners about the use of IoST in their premises.
Privacy-enhancing technologies will be too complex and not maturated for ITS/IoST services (likelihood: medium; impact: low)	CA1	Performing analysis of usable PETs for ITS. Finding well-established techniques, using best practices and designing suitable solutions for ITS/IoST services/applications. Readiness to assist in PET integration in IoST solutions with assistance of additional research staff and students if necessary.

Table 3: Risk Management in CA2: Security Certification:

Risks	CA	Proposed risk-mitigation measures
Lack of interest of external partners/companies in the tool we are developing (sec-certs) (likelihood: low; impact: medium)	CA2	Continuous two-way communication with diverse and independent target groups. We aim to collect feedback from the application sphere and government organisations from Estonia and South Moravia. Thanks to the diversification of the target groups (various sectors and regions), we will better accommodate the tool to end users' needs, ensuring we collect ideas for further development from diverse/independent user institutions. At the same time, we will continuously explain the benefits of the tool to interested parties. Harmonization with EUCC efforts planned for the 2nd period also reduces this risk.
Implementation problems related to the software we have been developing (likelihood: low; impact: high)	CA2	Our software will be open source, which (among others) means that more actors (developers) can participate in the software development process. These steps will remove a potential bottleneck in development if our internal software development team gets strained. Monitoring the development and assignment of more developers/students or those with different required skills if needed.

Failure to adapt the Estonian F4SLE standard for evaluating organisations' information security level in South Moravia (likelihood: medium; impact: low)	CA2	We need to test the applicability (and cross-compare between Estonian and South Moravian organisations) of the Estonian F4SLE standard for evaluating organisations' information security level – whether it will be valid and equally or comparably applicable in Estonia and the Czech Republic. We will test the applicability of the standard in either English or Czech (so far, the testing in Estonia went in the Estonian language only). In case of a negative (valid) outcome, the final recommendation would be that a different approach should be used to evaluate organisations' information security levels for Czech institutions.

Table 4: Risk Management in CA3: Verification of Trustworthy Software:

Risks	CA	Proposed risk-mitigation measures
Scalability problems preventing successful analysis of real-world software by industrial partners (likelihood: medium; impact: medium)	CA3	The software will be gradually applied to larger and larger instances after identifying and resolving crucial bottlenecks during the process. When encountering problems unsolvable by standard approaches, new priorities for fundamental research will be formulated and investigated.

Table 5: Risk Management in CA4: Security Preservation in Blockchain:

Risks	CA	Proposed risk-mitigation measures
Failure to establish shared methods and protocols for cooperation between the participant bodies and groups (likelihood: low; impact: medium)	CA4	We will organise periodic meetings to discuss small-scale projects, search for joint interests, and define the shared methods and protocols. The participating bodies are encouraged to propose their small-scale projects to create broader opportunities for collaborative participation.
The problem of the small-scale project does not get precise enough to develop demonstration or proof of concept (likelihood: medium; impact: medium)	CA4	The partners need to agree on the explicit vision of the solution to the small-scale project. The small-scale team should continuously monitor the progress through discussions and joint consensus. The Coordinator will be ready to step in the specification process if necessary.

Weak governance and decision-making (likelihood: low; impact: medium)	CA4	Decisions regarding the design and implementation of a blockchain solution, security measures, and protocols may involve multiple stakeholders, including developers, users, and regulators. The challenge area participants will continuously monitor the progress, report, and discuss ongoing issues to find the best decisions.

Table 6: Risk Management in CA5: Post-Quantum Cryptography:

Risks	CA	Proposed risk-mitigation measures
Security weaknesses in some post-quantum algorithms (likelihood: low; impact: high)	CA5	Intensive monitoring of the ongoing NIST standardisation process and publications concerning PQC security. Identification of backup algorithms and use of a modular architecture. Identification of fallback/backup algorithms based on different underlying hard problems and implementation of multiple algorithms wherever feasible.
Implementation problems (likelihood: medium; impact: medium)	CA5	Careful selection of libraries to be used (with identification of possible alternatives), intensive testing and open-source licensing of products. Involvement of larger community. Evaluation of PQC primitives on multiple platforms, from constrained to standard ones.
Performance and integration problems (likelihood: medium; impact: medium)	CA5	Further research on the primitives, enhancing collaborative testing infrastructure and keeping up-to-date with the developments of libraries and other infrastructure components.

Table 7: Risk Management in CA6: Human-Centric Aspects of Cybersecurity:

Risks	CA	Proposed risk-mitigation measures
Lack of interest in training events from external target groups (likelihood: medium; impact: medium)	CA6	We will organise training events in physical and online modes to lower the participation barrier (e.g., travel costs, travel overhead). We will promote the events using expert communities we are part of, such as through the Cybersecurity Competence Pilot consortia, national authorities and policy-making stakeholders, and local communities.
Failure to offer training on topics interesting for the target groups (likelihood: low; impact: high)	CA6	We will communicate the type of target training audience and prerequisites for the training. We aim to fill the gap in current training offerings by providing training featuring recent threats, vulnerabilities, tactics, techniques, and procedures. We will liaise with identified target groups closer if we identify emerging risk here.

5. Conclusion

The CHESS Risk Management Plan identifies the risks from the work packages and Challenge Areas perspective and proposes mitigation measures. We have not identified any risks with a high likelihood of occurrence and, at the same time high probability of negative impact. However, several risks listed above require special attention (likelihood: medium, impact: high), and the Coordinator will closely cooperate with WP Leaders and CA Leaders to minimise these risks.

6. References

[1] CHESS Project Proposal, 2022