



E-RIHS

EUROPEAN RESEARCH INFRASTRUCTURE
FOR HERITAGE SCIENCE

E-RIHS IP

European Research Infrastructure for Heritage Science

IMPLEMENTATION Phase

CALL: HORIZON-INFRA-2021-DEV-02 | TYPE OF ACTION: CSA | GA n. 101079148

D3.3 Risk Management Strategy

Lead Author: E. Cano

**With contributions from B. Doherty, M.T. Molina, M. Weterings
and B. Ramírez-Barat.**

We extend our special thanks to O. de Giacomo for her contributions to the deliverable, in her capacity as a member of the E-RIHS IP Research Infrastructure Advisory Board.



European Research Infrastructure for Heritage Science Implementation Phase (E-RIHS IP) has received funding from the European Union HORIZON-INFRA-2021-DEV-02 under the grant agreement No. 101079148

ABSTRACT

This deliverable is an outcome of task T3.3, E-RIHS Risk Management, which is one of the tasks of WP3, Preparing Operational Documents of E-RIHS. Both WP3 and T3.3 are led by CSIC.

This deliverable contains the updated versions of the E-RIHS ERIC Risk Management Framework and Risk Management Policy, based on the deliverables prepared under E-RIHS PP. In the revision of these documents, the current situation of the establishment of E-RIHS ERIC has been taken into account. Documents submitted for the Step 2 of the establishment of the ERIC, such as the Statutes and the Scientific and Technical Description, as well as other documents prepared (or under preparation) by E-RIHS IP, have been revised to ensure the alignment of the Risk Management Strategy with them. In the preparation of this document, examples from other RIs have also been taken into account, as well as links and connections with other tasks and deliverables of E-RIHS IP.

This deliverable sets the operational protocols for Risk Management, establishing the decision-making levels for various aspects, the assignment of responsible individuals for these tasks, and a detailed description of the decision-making process, including aspects of authority, delegation, and the practices for communicating about risk-related decisions. It also designates responsibilities for the ongoing update and maintenance of the Risk Management methodology, as well as for the promotion and dissemination of the ERIC's approach to Risk Management.

In the forthcoming months, this task will be complemented with the development of a Risk Management Database, featuring a comprehensive risk inventory and a mitigation plan. It will integrate lessons learned from the COVID-19 crisis and the IPERION CH and IPERION HS projects, among other sources. Recent changes in the international and European socio-political context, such as those caused by the war in Ukraine, will also be taken into account. In collaboration with task T2.3 Setting up the E-RIHS Central Hub, the refined strategy will be trialled in existing National Nodes to facilitate its seamless implementation as E-RIHS ERIC begins its operations.

DOCUMENT INFORMATION

Project number	101079148	Acronym	E-RIHS IP
Full title	European Research Infrastructure for Heritage Science Implementation Phase		
Project url	www.e-rihs.eu		
Document url			
EU Project Officer	Elsa PAPADOPOULOU		

Deliverable	Number	D3.3	Title	Risk Management Strategy
Work Package	Number	3	Title	Preparing Operational Documents of E-RIHS

Deliverable nature	Report			
Dissemination level	<input checked="" type="checkbox"/> Public <input type="checkbox"/> Confidential <input type="checkbox"/> Restricted			
Contractual delivery date	(31/12/2023)			
Actual delivery date	(04/04/2024)			
Status	Version 1.1		<input type="checkbox"/> Draft <input checked="" type="checkbox"/> Final	

Lead Partners(s)	CSIC		
Authors (Partner)	CSIC		
Responsible Author	Name: Emilio Cano	Email: ecano@cenim.csic.es	

Total number of pages	69
Keywords	Risk management, strategy, framework, operational documents

Version Log			
Issue Date	Rev. no.	Author	Change
30/12/2023	0.1	E. Cano	First draft
20/01/2024	0.2	E. Cano	Included comments from B. Doherty, M.T. Molina, and M. Weterings
01/02/2024	1.0	E. Cano	Version sent to partners
26/03/2024	1.1	E. Cano	Incorporation of suggestions by partners, B. Ramírez-Barat, O. de Giacomo (E-RIHS IP RIAB member) and discussion at Madrid meeting

DISCLAIMER: This document reflects only the author(s)'s view and the Agency, and the European Commission are not responsible for any use that may be made of the information it contains. It reflects the state of advancement of the project work at the time of its delivery. As such, its content may be subject to further evolution and has not been endorsed or validated by the E-RIHS interim General Assembly.

TABLE OF CONTENTS

LIST OF FIGURES AND TABLES	7
ABBREVIATIONS	8
1. INTRODUCTION	9
2. WORK CARRIED OUT	9
2.1. REFERENCE DOCUMENTS.....	11
2.2. LINKS WITH OTHER E-RIHS IP TASKS.....	14
3. E-RIHS ERIC RISK MANAGEMENT FRAMEWORK.....	15
4. E-RIHS ERIC RISK MANAGEMENT POLICY.....	15
5. E-RIHS ERIC RISK MANAGEMENT DATABASE	15
6. APPROVAL OF THE RISK MANAGEMENT POLICY	16
7. NEXT ACTIVITIES	16
ANNEX A: UPDATED E-RIHS RISK MANAGEMENT FRAMEWORK.....	17
1. INTRODUCTION AND PRINCIPLES	18
1.1. CONTEXT	18
1.2. DEFINITIONS.....	18
1.3. APPLICABILITY.....	18
1.4. OBJECTIVES.....	19
1.5. COMMITMENT TO RISK MANAGEMENT.....	19
1.6. INTERNAL FACTORS INFLUENCING RISK MANAGEMENT	19
1.7. PRACTICAL APPLICATION OF RISK MANUAL	19
1.8. DIFFERENT CLASSIFICATIONS OF RISK.....	20
1.9. FREEDOM OF INFORMATION AND GDPR CONSIDERATIONS	20
2. COMPONENTS OF THE RISK MANAGEMENT FRAMEWORK.....	21
2.1. GENERAL CONSIDERATIONS	21
2.1. INTEGRATION	21
2.2. RESOURCING OF THE RISK MANAGEMENT FUNCTION	22
2.3. IMPLEMENTATION	22
2.4. EVALUATION	22
2.5. CONTINUOUS IMPROVEMENT	23
LEVELS OF THE FRAMEWORK.....	24
2.6. OVERALL APPROACH.....	24
2.7. IDENTIFICATION OF RISK	25
2.8. ALLOCATION OF RISK OWNERSHIP	25
2.9. TRANSFERS OF RISK OWNERSHIP	26
2.10. MANAGEMENT OF RISK	26
2.11. MONITORING AND REVIEW OF RISK	27
2.12. ESCALATION OF RISK OWNERSHIP	27

2.13.	DE-ESCALATION OF RISK OWNERSHIP.....	28
2.14.	BUDGETARY AND RESOURCE CONSIDERATIONS IN CHANGES OF RISK OWNERSHIP	28
3.	SPECIAL GOVERNANCE CONSIDERATIONS FOR A MULTI-TIERED FRAMEWORK...	29
3.1.	COMMUNICATION OF AND CONSULTATION ABOUT RISK.....	29
3.2.	CONFIDENTIALITY CONSIDERATIONS	29
3.3.	GDPR AND DATA PROTECTION CONSIDERATIONS.....	30
4.	SUBSTITUTION OF LOCAL RISK MANAGEMENT PROCEDURES.....	32
4.1.	GENERAL PRINCIPLES	32
4.2.	ASSESSMENT OF COMPLIANCE VIA LOCAL PROCEDURES.....	32
4.3.	AMENDED PROCEDURES ARISING FROM COMPLIANCE	32
5.	MANAGEMENT OF RISKS RELATING TO THE ERIC OVERALL	33
5.1.	GENERAL CONSIDERATIONS.....	33
5.2.	ESCALATION OF RISKS TO THE ERIC CENTRAL HUB FROM NATIONAL NODES.....	33
5.3.	INTRODUCTION TO THE COMMON RISK MANAGEMENT PROCESSES	34
5.4.	RISK IDENTIFICATION.....	34
5.5.	RISK ANALYSIS	34
5.6.	RISK EVALUATION.....	36
5.7.	RISK TREATMENT	37
5.8.	CREATING A RISK TREATMENT PLAN.....	38
5.9.	BUDGETARY CONSIDERATIONS	39
6.	MANAGEMENT OF RISKS AT NATIONAL NODE LEVEL	40
6.1.	GENERAL CONSIDERATIONS.....	40
6.2.	ESCALATION OF RISKS TO NATIONAL NODE FROM INDIVIDUAL PARTNERS	40
6.3.	DE-ESCALATION OF RISKS FROM THE NATIONAL NODE TO AN INDIVIDUAL PARTNER	41
7.	MANAGEMENT OF RISKS AT INDIVIDUAL PARTNER LEVEL	42
7.1.	GENERAL CONSIDERATIONS.....	42
7.2.	ESCALATION OF RISKS TO NATIONAL NODE.....	42
7.3.	DE-ESCALATION OF RISKS TO INDIVIDUAL PARTNER.....	42
8.	MANAGEMENT OF RISKS RELATING TO SPECIFIC OBJECTS	43
8.1.	GENERAL CONSIDERATIONS.....	43
8.2.	OBJECT RISK MANAGEMENT PLANNING.....	43
8.3.	OBJECT RISKS DATABASE	44
9.	MANAGEMENT OF RISKS RELATING TO SPECIFIC PROCEDURES.....	45
9.1.	GENERAL CONSIDERATIONS.....	45
9.2.	PROCEDURE RISK MANAGEMENT PLANNING.....	45
9.3.	ISSUES OF PROPRIETARY KNOWLEDGE IN RISK MANAGEMENT	46
10.	MANAGEMENT OF OPPORTUNITY.....	47
10.1.	GENERAL CONSIDERATIONS.....	47
10.2.	IDENTIFICATION OF OPPORTUNITY	47

10.3.	ANALYSIS AND EVALUATION OF OPPORTUNITY	47
10.4.	RESPONSES TO OPPORTUNITY	47
10.5.	MANAGEMENT OF OPPORTUNITIES.....	48
APPENDIX 1 - SUMMARY OF TERMS AND DEFINITIONS		49
ANNEX B: UPDATED RISK MANAGEMENT POLICY		52
1.	PURPOSE	53
2.	SCOPE AND CONTEXT.....	53
3.	KEY OBJECTIVES	53
4.	REVIEW OF POLICY.....	54
5.	ACCESS TO THE POLICY.....	54
6.	RISK MANAGEMENT PROCESS AND PROCEDURES	54
7.	RISK MANAGEMENT REQUIREMENTS.....	54
8.	RISK MANAGEMENT PRINCIPLES	55
9.	RISK MANAGEMENT PROCESS.....	56
10.	RISK MANAGEMENT COMPLIANCE AND CONTROL	56
11.	ASSESSMENT OF EFFECTIVENESS.....	57
12.	REPORTING REQUIREMENTS	57
13.	RISK MANAGEMENT RESPONSIBILITIES	58
13.1.	E-RIHS GENERAL ASSEMBLY	58
13.2.	RISK MANAGEMENT COMMITTEE (RMC)	59
13.3.	E-RIHS DIRECTOR GENERAL	59
13.4.	E-RIHS RISK MANAGER (ROLE)	59
13.5.	E-RIHS CENTRAL HUB STAFF.....	60
13.6.	RISK OWNERS.....	60
14.	RISK FRAMEWORK	60
15.	APPETITE FOR RISK	61
16.	RISK MATRICES	61
17.	RISK GRADING CRITERIA – IMPACT RATINGS.....	61
18.	MULTIPLE AREAS OF IMPACT	62
19.	RISK GRADING CRITERIA – PROBABILITY RATINGS.....	63
APPENDIX 1 – RISK APPETITE / RESPONSE AT DIFFERENT PROXIMITIES.....		65
APPENDIX 2 - RISK MANAGEMENT ARRANGEMENTS: PARTNER SELF-ASSESSMENT .		
.....		68
REFERENCES		69

LIST OF FIGURES AND TABLES

ANNEX 1

FIGURE 1 - OVERALL RISK MANAGEMENT FRAMEWORK	21
FIGURE 2 – HIERARCHY OF RISK MANAGEMENT ACTIVITIES	24
FIGURE 3 - ESCALATION OF RISK OWNERSHIP SHOWS A FLOW DIAGRAM FOR THESE PROCESSES.	28
FIGURE 4 - APPLICATION OF RISK WEIGHTINGS	36

ANNEX 2

FIGURE 1 - ISO 31000:2018 RISK MANAGEMENT PROCESS	56
FIGURE 3 - CRITERIA FOR LEVELS OF IMPACT WITHIN DIFFERENT AREAS	63
FIGURE 4 - RISK GRADING CRITERIA	64
FIGURE 5 - ACTIONS TO BE TAKEN AT EACH LEVEL OF APPETITE RISK	67
FIGURE 6 - RISK MANAGEMENT SELF-ASSESSMENT CHECKLIST FOR PARTNER ORGANISATIONS ...	68

ABBREVIATIONS

Abbreviations	Expansion
(i)GA	(interim) General Assembly
ACTRIS	Aerosol, Clouds and Trace Gases Research Infrastructure
CTAO	Cherenkov Telescope Array Observatory
DoA	Description of Action
EMBRC	The European Marine Biological Resource Centre
ERIC	European Research Infrastructure Consortium
E-RIHS IP	European Research Infrastructure for Heritage Science Implementation Phase
E-RIHS PP	European Research Infrastructure for Heritage Science Preparatory Phase
ESFRI	European Strategy Forum on Research Infrastructures
HR	Human Resources
HS	Heritage Science
ICCROM	International Centre for the Study of the Preservation and Restoration of Cultural Property
KPI	Key Performance Indicators
RI	Research Infrastructure
RIAB	Research Infrastructure Advisory Board of E-RIHS IP project
RoP	Rules of Procedure

1. INTRODUCTION

Work Package 3 of E-RIHS IP is dedicated to Preparing Operational Documents of E-RIHS. According to the Description of the Action, the objective of this WP is to revise and update the necessary documents for the quality operation and management of E-RIHS (HR Policy, Risk Management Framework, Corporate Risk Management Function and E-RIHS Quality Manual and KPIs). In addition, it will create the procurement policy, strategy and procedures for the operation of the ERIC.

This deliverable is an outcome of one of the tasks of this WP, task T3.3 E-RIHS Risk Management, aimed at developing a comprehensive Risk Management Strategy (this document) alongside a detailed risk inventory and mitigation plan, including operational protocols. This task addresses the E-RIHS IP **specific objective (3) to provide E-RIHS with a thorough risk inventory and mitigation plan**.

This **Risk Management Strategy**, presented here, is based on the Risk Management Framework and Corporate Risk Management Function released in E-RIHS PP (deliverables D2.3 and D2.5 of E-RIHS PP). It highlights issues related to organisation and governance and risks connected to funding mechanisms to support user access and ensure sustainability.

The actions for the implementation of the Risk Management Strategy include:

- (i) the identification of levels at which different risk management decisions are to be taken, persons to fulfil this responsibility how such decisions are taken – levels of authority, levels of delegation, methods for upwards and downward communication of decisions about risk(s);
- (ii) the responsibility for the ongoing maintenance and amendment of the Risk Management methodology and the communication and promotion of the ERIC's approach to Risk Management.

In cooperation with E-RIHS IP task T2.3 Setting up the Central Hub, the revised Risk Management Strategy (this deliverable) will be implemented to the existing National Nodes to test it and obtain preliminary results to facilitate its application as soon as the E-RIHS ERIC starts. This activity will be carried out in the following months.

2. WORK CARRIED OUT

The work of this is based mainly on the revision of the documents prepared during E-RIHS PP, according to the current context and situation of E-RIHS ERIC and the recommendations by the May 2020, 2020 ESFRI "Evaluation Form Scientific Case and Implementation". In this document, reviewers comment on the "Risks" section:

A risk management strategy is prepared and seems to be improving. The strategy is still very much geared towards financial risks, and these are indeed important. However, additional issues related to organisation and governance are not highlighted. The attached deliverable of the preparatory phase project "Risk Management Framework" is a step in the right direction but provides only for a very general framework on how risks will be assessed, discussed and dealt with within E-RIHS organisation. No detailed risk inventory and mitigation plan, building on the detailed and theoretical "Risk Management Framework" has been provided.

The recommendation made by ESFRI was to "Put the Risk Management Framework into reality".

To address the issues related to the organisation and governance, current situation of the establishment of E-RIHS ERIC has been considered. Since the delivery of the E-RIHS PP documents reviewed by ESFRI, official application for the ERIC has been submitted. Step 1 of the ERIC application was sent by the hosting country (Italy) to the European Commission in February 2021, that gave its feedback in October 2021. In view of this feedback, E-RIHS ERIC documents were amended, and final version approved on May 5, 2022, by the members of the iGA: 14 Member countries (BE, CY, ES, FR, GR, HU, IT, MT, NL, PL, PT, RO, SI, UK), 2 Observers (AT, SE) and the intergovernmental organisation ICCROM as Permanent Observer.

In March 2023, Step 2 was submitted. At the moment of submission of this deliverable, 10 letters of commitment have been sent by countries committed to becoming founding members of the ERIC.

The COVID-19 crisis and the experience of services implemented during the IPERION CH and IPERION HS projects have been considered in updating the Risk Management Strategy, although specific risks related to them will be identified, assessed, and evaluated in the coming months. Recent changes in the international and European socio-political context, such as those caused by the war in Ukraine, will also be taken into account.

Terminology has been adapted to the current version of Statutes and other documents of E-RIHS ERIC, including other deliverables of E-RIHS PP and E-RIHS IP projects.

This Risk Management Strategy was sent on 16 January 2024 to the E-RIHS IP partners for comments. The draft deliverable was also sent to the RIAB, and presented and discussed in the 2nd RIAB meeting held online on 24 February 2024.

It was decided to include the Risk Management as one of the topics for discussion in the E-RIHS IP meeting held in Madrid in 6-7 March 2024, allowing to review the contents of this document and the next steps in task T3.3 with all partners of the project.

2.1. Reference documents

The following documents have been consulted and used for the preparation of the updated risk management framework and policy:

- **ISO standard 31000:2018 Risk Management-Guidelines** establishes the principles, framework and process for the preparation of the risk management framework and policy of E-RIHS ERIC. The main terms (risk, risk management, stakeholder, risk source, event, consequence, likelihood and control) are also defined in this document.
- **ISO/IEC standard 31010:2009 Risk Management-Risk assessment techniques** is a supporting standard for ISO 31000, providing guidance on the selection and application of systematic techniques for risk assessment. The recommendations of this standard will be used for the selection and application of the techniques for the assessment of risks in E-RIHS, for the steps of risk identification, risk analysis and risk evaluation.
- **ISO/TR 31004:2013 Risk Management-Guidance for the implementation of ISO 31000** is a technical report intended to provide a general methodology for the implementation of ISO 31000 standard. The guidance in this TR has been used to review the documents used for the preparation of this deliverable.
- **E-RIHS PP D2.3 Risk Management Framework** was conceived as a manual which defines the Risk Management methods to be used by the ERIC. Delivered on 31/01/2019, it was necessarily general, as mentioned in the 2020 ESFRI evaluation report, due to the aim of the document (providing a general framework, as defined in ISO 31000) and the early stage of the development of the ERIC at its time. In spite of being general, it is comprehensive and addresses all the required elements included in the ISO 31000, as well as other issues related to transparency and data protection. Although most of the contents of this Framework are still valid, it has been considered that this document needs to be revised taking into account the advances in the creation of E-RIHS ERIC. With that purpose, this document has been reviewed following the guidance of ISO/TR 31004, specifically the advice provided in Annex D-Monitoring and Review.
- **E-RIHS PP D2.5 Corporate risk management function** is a document which established the E-RIHS ERIC risk management policy. The purpose of this document was:

“[...]to communicate the E-RIHS ERIC’s [hereinafter referred to as “E-RIHS”] commitment to managing enterprise-wide risks and to establish clear responsibilities for itself in order to maximize strategic and operational achievement”,

This document detailed the processes for Risk Management, and identifies bodies/positions responsible for the different elements, scales for measurement of impact, probability and proximity of risks, categories in which the risks are classified, and matrices establishing the actions to be taken depending on the risk appetite factors. Unlike the E-RIHS PP D2.5, this document is highly detailed in the operational protocols for the application of the Risk Management processes in E-RIHS ERIC. The final version was delivered on July 2020, and hence this document was not considered in the ESFRI evaluation. In fact, it already addressed some of the recommendations made in the ESFRI report. The document reflected the state of play and expectations for the creation of the ERIC at that time. Since then, some changes and clarification of different aspects of the ERIC have occurred, making necessary to review this policy to adapt it to the current status. The revision has been made according to the

recommendations of ISO/TR 31004. Thus, in section 3.1, it is recommended that “c) the implementation of the risk management process can be proportionately tailored to the size and requirements of the organisation”. A key element to be considered for this revision is the definition of Human resources policy, strategy and procedures made in E-RIHS IP D3.1, which sets the size and roles of the staff at the E-RIHS Central Hub. Section 3.1.d) mentions that “The governance [...] of the risk management policy, framework and process(s) can be integrated into existing organisational governance arrangements”. In order to do so, the revision of this document has been made in collaboration with other tasks (see Section 5.2, Links with other tasks), so the provisions of this document have been considered in the preparation of the Rules of Procedure and the Updated Business Plan.

- **E-RIHS PP D11.1 E-RIHS Business Plan** contains a section (§6.4, p. 69) dedicated to the Risk Management Framework and Plan. The information contained therein is a summary of the previous documents dedicated to Risk Management, D2.3 and D2.5. This document also contains a list of the more relevant (those with high to medium likelihood) risks and mitigation measures for the period of transition to E-RIHS ERIC, including the initial phases of implementation:

- *Insufficient support from EU Member States to become financially independent of the host country.*

Mitigation: assessment of the prospective Members’ needs and requirements and adjust the working parameters to maximize membership. If absolutely necessary, consider reducing in-cash contributions for an initial period of three years and accept the secondment of personnel as an in-kind contribution.

- *Low level of transnational funding.*

Mitigation: develop relations at the EU level and use all opportunities to demonstrate heritage science as a shared resource and shared responsibility. Organise events with high-level decision-makers and policymakers.

- *Member financial difficulties or lack of internal policy support, leading to missing fee payments.*

Mitigation: gradually build a financial reserve amounting to at least 25% of the annual cash flow; prepare an emergency budget with a 25% cut.

- *Partner financial difficulties resulting in a sudden default of a Partner.*

Mitigation: disengage E-RIHS ERIC from individual Partners and avoid situations in which E-RIHS ERIC represents a sizable source of income for a Partner. Revise commitments, e.g. reduce Partner in-kind contributions.

- *Disagreements between Partners and/or Partner and E-RIHS ERIC Head Office.*

Mitigation: establish clear and transparent decision-making rules; promote friendly relations within the E-RIHS ERIC Consortium; use the support of the National Coordinators’ Committee to resolve disagreements.

- *Low quality of delivery of services.*

Mitigation: quality criteria to be accepted as a condition for becoming a Partner, along with key performance indicators, allowing for the quality of activities under the E-RIHS ERIC Label to be monitored, including sanctions, which could lead to

discontinued partnership in extreme cases; establish a trial period for new partners (e.g. 12 months), after which the final decision of acceptance is taken.

- *Lack of collaborative culture e.g. within organisations not in the partnership.*

Mitigation: proactively establish terms of reference (based on the ethical principle of beneficence) that include all types of relationships with organisations; maintain open channels of communication.

- *Lack of impact on stakeholders.*

Mitigation: use all opportunities to advocate the E-RIHS ERIC Label; promote heritage research through all public channels, including the media; nurture relationships with policy-makers; continuously reassess the engagement strategies.

- **Risk Management Documents and experiences from other RIs.** Unlike other operational documents of other RIs, such as staff or procurement policies, examples of Risk Management frameworks and strategies are usually not publicly available. In some cases, they may be internal/confidential documents. In other cases, Risk Management even seems to be not well developed and formalized. Risk Management is an aspect with has not received much attention in the creation and development of other ERICs. For instance, in the ERIC Forum Toolkit, risk is mentioned only in relation with insurance requirements:

“Because ERICs are quite diverse in nature, so are their insurance requirements. Every ERIC should have an idea of their risk register: what kinds of possible risks there are, and how should they respond to them (i.e., risk mitigation actions)”¹

The ACTRIS IMP project² published in January 2022 the “Milestone 2.6: Refined risk management plan”. This document revised the ACTRIS risk management plan (RMP, initially developed during the preparatory phase project in 2019) at mid-term stage of the ACTRIS implementation phase. It includes a table with the ACTRIS Risk Register (status December 2021). It should be noted, though, that this document is much simpler and shorter than the Risk Management documents produced in E-RIHS PP.

EMBRC-ERIC Business Plan Update [2017] includes a section dedicated to the Risk Management Plan in which some of the main risks are highlighted. Considering the point at which the implementation of the ERIC was at that time, they are focused on those who are particularly significant at the interface between implementation and operational phase, organised in three groups: Financial Risks; Strategic and organisational factors; and Technical and Technological factors. These specific risks will be reviewed in the future preparation of the E-RIHS ERIC risk inventory. Only a brief paragraph is dedicated in this document to the description of the “relatively risk management system” with just a very simple description of some of the elements. This is far less detailed than the already existing risk management deliverables produced in E-RIHS PP.

Experiences from CTAQ (though a meeting with Federico Ferrini, Managing Director held on June 2023) and from the members of the Research Infrastructure Advisory Board (RIAB) of

¹ ERIC Forum Toolkit, <https://www.eric-forum.eu/toolkit/administration/insurance/>, Access date: 29/12/2023

² Aerosol, Clouds and Trace Gases Research Infrastructure Implementation Project (ACTRIS IMP), Horizon 2020 – Research and Innovation Framework Programme, H2020-INFRADEV-2018-2020, Grant Agreement number: 871115

E-RIHS (in the first RIAB meeting held on October 2023) have also been sought, although the feedback obtained has been limited.

2.2. Links with other E-RIHS IP tasks

The Risk Management Strategy has links with other tasks of the project, whose results depend on the results of task T3.3 or, vice versa, whose results determine the development of task T3.3. The following direct links have been identified and considered in preparation of this document:

1. Task 1.1 Project Handbook

The Project Handbook (deliverable D1.1) includes a section (§2.5) dedicated to Risk Management of the E-RIHS IP project. Some risks of the project have been identified, along with mitigation measures, and included in a Risk Management Database made available on the General channel within the Teams platform of E-RIHS IP and SharePoint. As noted in this deliverable, the Risk Management Plan of the project referred to in D1.1 is different from the Risk Management Strategy of E-RIHS ERIC.

2. Task 2.3 Setting up the Central Hub

As specified in the DoA, in collaboration with this task T2.3, the Risk Management Strategy will be implemented in the existing National Nodes to test it and obtain preliminary results to facilitate its application as soon as the E-RIHS ERIC is launched. As an operational document, this deliverable will contribute to the guidelines developed under this task for the efficient setup of the Central Hub, to be included in D2.5 Guidelines for the E-RIHS Central Hub Management Practices. The work carried out under this task, for the benchmarking of other RI staff, has been integrated in the D3.1 (see next).

3. Task 2.4: Updating the E-RIHS Rules of Procedures

The relation between the Risk Management Policy (this deliverable) and the Rules of Procedure (RoP) has been discussed with the Task leader and other participants of task T2.4 Updating the E-RIHS Rules of Procedures, in meetings and e-mail exchanges. As a result, the procedures and responsibilities for Risk Management established in this document have been incorporated into the draft of the RoP. Specifically, the roles of the GA and the Director General with regards to the risk management policy will be incorporated into the RoP. A specific article is suggested to be incorporated in the RoP. Conversely, the role of the GA in the approval of the Risk Management Policy is incorporated into this deliverable.

4. Task 3.1 Human resources policy, strategy and procedures

Amongst other activities, this task T3.1 and the deliverable produced (D3.1 E-RIHS ERIC Human Resources Strategy and Procedures) has identified the minimum staffing requirements for the operation of E-RIHS ERIC, based on the benchmarking exercise carried out in task T2.3. Amongst these, a *Head of Unit "quality and risk"*, who will ensure the quality within E-RIHS and assess the risk, has been identified as one of the roles which are to be given priority in setting up a small core team for the initial operation of the ERIC. This head of unit will hence take the role of the *E-RIHS Risk Manager* as identified in the deliverable D2.5 of E-RIHS PP.

5. Task 3.4: Implement the E-RIHS quality system

The draft E-RIHS quality manual implementation plan (D3.4) sets out the quality practices and procedures for periodic audits of all services and self-assessment of prospective and

existing partners to E-RIHS. Risk management in this respect is incorporated through hazard and countermeasure identification in service and partner monitoring, where its purpose is to assure that the quality standard of excellence established by the ERIC is appropriately set-up and adhered to so that proper actions and mitigations are taken to avoid, reduce and control associated risks.

6. Task 4.1: Updated Business Plan

As it has already been mentioned, the business plan released by E-RIHS PP (D11.1) contained a list of identified risks for the transition/implementation. Being part of this business plan, these risks were focused (as pointed out in the ESFRI report) in financial aspects. These risks will be thoroughly reviewed considering the advances in the establishment of the ERIC. Those considered to be still relevant be integrated in the Risk Management Database, in the relevant category. In turn, this section in the Business Plan is to be updated with the contents of this deliverable, and integrated in the D4.3 Revised E-RIHS Business Plan (due M24).

3. E-RIHS ERIC RISK MANAGEMENT FRAMEWORK

Annex A includes the updated E-RIHS ERIC Risk Management Framework, amended following the points previously discussed.

4. E-RIHS ERIC RISK MANAGEMENT POLICY

Annex B contains the updated E-RIHS ERIC Risk Management Policy, revised according to the points previously discussed. It includes the (i) identification of levels at which different risk management decisions are to be taken, persons to fulfil this responsibility how such decisions are taken - levels of authority, levels of delegation, methods for upwards and downward communication of decisions about risk(s) and the (ii) responsibility for the ongoing maintenance and amendment of the Risk Management methodology and the communication and promotion of the ERIC's approach to Risk Management.

5. E-RIHS ERIC RISK MANAGEMENT DATABASE

A Risk Management Database (which constitutes an enhanced version of the conventional Risk Register) will be maintained by the Head Office and will be accessible to all participants in E-RIHS ERIC.

This Risk Management Database will contain a detailed risk inventory, classified in the categories established in Section 17 of the Risk Management Strategy:

- a) Financial – impact on E-RIHS finances
- b) Operational – impact on provision of E-RIHS products, projects and services
- c) Reputational – impact on the professional and scientific reputation of E-RIHS and its membership overall and on its wider general credibility
- d) Physical/Safety – impact on the safety and well-being of people

- e) Regulatory/Legal – impact on E-RIHS of regulatory exposure
- f) People – impact on corporate knowledge / continuity / professional development and welfare of individuals.

According to Section 3.2 of the Risk Management Framework, a risk is always best expressed in the form:

“There is a Risk that [xxxxxxx] will occur, with the consequence for the ERIC/National Node/Partner/Artefact of [zzzzzzzzzz]”

Each risk will be assessed using 3 measurement scales, **Impact, Probability and Proximity**, each of which operates on a 1-5 range of scores.

6. APPROVAL OF THE RISK MANAGEMENT POLICY

Pursuant to the establishment of E-RIHS ERIC, the Director General shall implement the E-RIHS ERIC Risk Management policy, to be presented to the General Assembly for approval, as established in the RoP.

7. NEXT ACTIVITIES

The next activities of Task 3.3 will be focused on two specific aspects: the creation of the Risk Management Database, and the identification of risks and mitigation strategies; and the procedure for testing the Strategy by implementation in the National Nodes, in collaboration with task T2.3, to obtain preliminary results to facilitate its application as soon as the E-RIHS ERIC is launched.

As agreed in the meeting in Madrid on 7th March 2024, a dedicated workshop will be organised with a representative of each National Node to carry out an initial risk assessment exercise, according to the procedures and techniques in ISO 31010. This workshop will be organised online during May-June 2024.

Annex A: Updated E-RIHS Risk Management Framework

1. INTRODUCTION AND PRINCIPLES

1.1. Context

This manual defines the Risk Management methods which shall be used by E-RIHS ERIC to identify, assess, mitigate and modify risk in the areas of:

- The day-to-day and strategic management of the overall ERIC
- The day-to-day and strategic management of National Nodes
- The planning of research activities in relation to specific items
- The development of research methods to be applied to generic classes of item.

The Risk Management methods contained in this manual have been based on the International Standard ISO 31000:2018(E) – “Risk Management Guidelines” published 2018. This is referred to as “the ISO” hereafter.

This Manual will be reviewed and updated each time that the ISO is updated, changes have occurred in the internal or external context, or any other reason deeming adaptation or improvement of the framework (See section 5.7 of the ISO).

1.2. Definitions

“**Risk**” is defined in the ISO as “the effect of uncertainty on objectives”.

“**Risk Management**” is defined as “coordinated activities to direct and control an organisation with regard to risk”.

“**Risk Management Framework**” is defined as a “set of components that provide the foundations and organisational arrangements for designing, implementing, monitoring, reviewing and continually improving risk management throughout the organisation”.

1.3. Applicability

This manual defines the nature of the overall Risk Management Framework to be adopted by E-RIHS ERIC and explains how it will relate to, be implemented by and impact on the activities of all National Nodes and individual partners, including during collaborative activities. In the context of this document, “partners” are the facilities offering access or other services to the ERIC, formerly referred to as “access providers” in the previous Integrating Activities.

This manual will be complied with in full by the Central Hub and National Nodes of the ERIC. Individual partner facilities may choose to substitute local risk management methodologies where these are mandated by their own governance rules.

Where such local substitutions are not made, however, compliance in full with the provisions of this manual will be a recommended condition of partnership of the ERIC. Individual participating facilities are, however, required to periodically demonstrate and certify the adequacy of the local risk management protocols adopted in comparison with those described in this manual. The management of the National Nodes, in consultation with the Central Hub, will determine the frequency with which such demonstrations and certifications will be required.

1.4. Objectives

The objective of this manual is to ensure that a transparent and consistent approach to risk management, based on internationally-recognised Best Practice, is adopted throughout the ERIC. This will serve to reassure the bodies and groups to which the participating organisations are accountable that proper consideration is given to all aspects of risk which confront them in their activities on behalf of the ERIC.

It will also serve to demonstrate to the wider stakeholder community that research activities relating to objects of potentially high heritage and cultural value have all been defined, planned and executed with proper regard to all risks identified as relating to those objects, and to the health and safety of personnel engaged in such research actions.

It is anticipated that the insurers of participating organisations will wish to place reliance on compliance with this manual when assessing premia, restrictions and liability relating to research activities undertaken within the context of the ERIC.

1.5. Commitment to Risk Management

All levels of E-RIHS ERIC are committed to rigorous, but proportionate, management of Risk. The purpose of this manual is to ensure that:

1. Accountabilities within the ERIC for Risk Management are aligned with its overall corporate structure.
2. Risk Management is aligned with the overall culture and ethos of an organisation dedicated to the preservation of cultural heritage.
3. Risk Management contributes to overall legal and regulatory compliance across a range of national jurisdictions.
4. Risk Management remains appropriate as the ERIC grows.

1.6. Internal Factors Influencing Risk Management

E-RIHS ERIC will, at the Central Hub level, operate as an independent, legal entity (Article 1 of E-RIHS ERIC Statutes) As such, it limits the liabilities of members. Article 5 of Statutes establishes:

“1. E-RIHS ERIC shall be liable for its debts.

2. Members are not jointly liable for the debts of E-RIHS ERIC. The financial liability of the members for the debts of E-RIHS ERIC shall be limited to their respective annual contribution, as specified in Annex II.

3. E-RIHS ERIC shall take appropriate insurance to cover the risks specific to its operation.”

In order to obtain such insurance, it is necessary that the ERIC has in place methodologies to effectively identify, assess and mitigate such risks. This framework will facilitate the activities required to create and operate an “appropriate Risk Management function”.

1.7. Practical Application of Risk Manual

The Central Hub will have overall responsibility for the ongoing definition and compliance with the risk manual throughout the ERIC.

The National Nodes will have responsibility for managing compliance with the risk manual both within the Node itself and within participating partners which operate under the supervision of the Node.

Individual participating partners will have responsibility for ensuring compliance with the Risk Manual in relation to all activities arising from participation in the ERIC.

All the above organisations shall ensure that their compliance activities are visible to the bodies which are above and below them in the organisational hierarchy.

1.8. Different Classifications of Risk

This manual recognises and considers separately 5 types of Risk, each of which required a different treatment:

- Corporate Risks relating to the ERIC Overall
- Corporate Risks relating to a National Node
- Corporate Risks relating to one or more individual partners of the ERIC
- Risks relating to a specific service
- Risks relating to a specific object to be subject to a research activity

Each of these is addressed separately in Sections 6 to 10 below.

The Management of Opportunities is then considered separately in Section 11.

1.9. Freedom of Information and GDPR Considerations

Because of the requirements of Freedom of Information legislation and also the requirement to protect personal data from error and/or unauthorised disclosure, participating organisations should have due regard to ensuring full compliance with this legislation in the preparation and maintenance of all risk management documentation. They should also ensure that the members of their organisation with responsibility for overseeing compliance with this (and other relevant) legislation are consulted and updated about risk management documentation (physical or electronic) which is created under the auspices of this Manual.

Although this document gives some general guidance about issues relating to compliance, it does **not** over-ride any local arrangements or directions given by specialists in this area.

2. COMPONENTS OF THE RISK MANAGEMENT FRAMEWORK

2.1. General Considerations

The overall objective of this Framework is to enable Risk Management to be seamlessly integrated into E-RIHS ERIC's principal activities and operations. It is therefore intended that it shall be embedded throughout the governance of the ERIC from its overall management down to individual preservation activities by national partners.

The ISO describes the Framework as a Management Cycle with the following steps

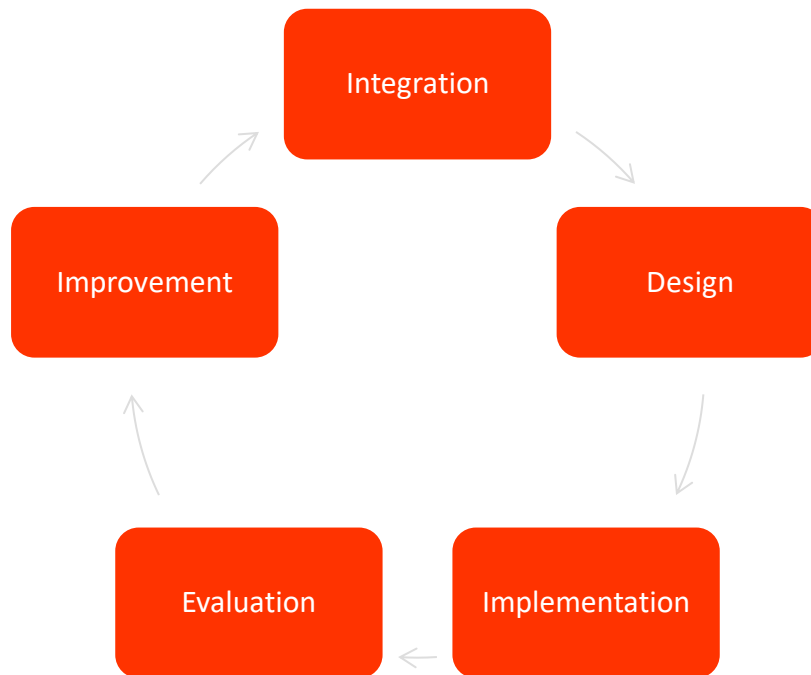


Figure 1 - Overall Risk Management Framework

The Risk Management Framework is designed to be compatible with the international, federated nature of the ERIC, and to permit, where appropriate, local governance (legal, financial, political) factors to be taken into account without reducing its overall effectiveness.

It recognises the potentially complex relationships between individual partners and also the hierarchical relationships between partners, National Nodes and the Central Hub. It also permits different contractual and operational relationships between individual partners and also between individual partners and nodes to be reflected in the processes.

2.1. Integration

Risk Management is a *function* of organisational governance at all levels. It is therefore essential that at each level, appropriate levels of accountability are established to ensure that the function lies with one or more individuals with appropriate authority to manage risk, as well as ensuring that the Framework continues to be assessed, maintained and evolved in accordance with changes in the overall environment within which the E-RIHS ERIC is operating as well as with legislative and procedural changes at any level within the ERIC.

Function holder(s) are responsible for ensuring that Risk Management is properly implemented at their level within the organisational hierarchy. They also have an oversight role to ensure that Risk Management at lower levels beneath them in the hierarchy has been properly implemented.

“Implementation” should in this context be taken to mean “fully embedded within the organisation’s practices and processes”.

For the ERIC, Risk Management is also a relevant consideration within its strategic and financial planning at Central and National levels.

2.2. Resourcing of the Risk Management Function

This Manual does not specify how Risk Management shall be resourced within the ERIC.

It is the responsibility of the Central Hub and National Nodes to identify and quantify the appropriate levels of competent resources required. These will vary, depending on the final governance model for the ERIC and the levels of activity being undertaken by different parts of the ERIC.

Risk Management responsibilities are detailed in Section 13 of the Risk Management Strategy.

2.3. Implementation

Risk Management must be in place before the first day of the operation of the ERIC. To enable this, the following is defined in the Risk Management Policy:

- Identification of levels at which different risk management decisions are to be taken;
- Identification of persons to fulfil this responsibility;
- Identification of how such decisions are taken – levels of authority, levels of delegation, methods for upwards and downward communication of decisions about risk(s);
- Responsibility for the ongoing maintenance and amendment of the Risk Management methodology;
- Responsibility for the communication and promotion of the ERIC’s approach to Risk Management.

2.4. Evaluation

At each hierarchical level, the management of the ERIC shall, periodically, assess the effectiveness of their Risk Management.

Risk Management can be a specific agenda item at meetings of the governing bodies at Central and National level of the ERIC.

Performance Indicators for measuring the effectiveness of Risk Management will be considered.

Subject to the direction of the Governing Bodies, this Risk Manual will be subject to review after 12 months’ operational activity by the ERIC, and thereafter every 24 months, except in the event of a substantial revision of the ISO standard on which this Manual is based or in the event of major incident where it appears that a defect or omission in the Manual requires a revision to be made. Where any organisation providing insurance to the ERIC at any level requires modifications to the Risk Management approach as a condition of providing or maintaining insurance cover for ERIC-

related activities, those modifications shall be reviewed as a matter of urgency and adopted where the ERIC considers them to be to the overall benefit of the stakeholders of the ERIC.

Where any risk 'crystallises' or an unforeseen event occurs, action should be taken to identify whether a modification to the Risk Manual or to the procedures adopted locally to comply with it is required to prevent or further mitigate a recurrence.

It is assumed that all partners seeking to join the ERIC will be required to perform a self- evaluation of the expected effectiveness of their internal Risk Management procedures by reference to performance experienced in other, previous spheres of activity.

Where a partnership application is to be submitted by a prospective partner, the person signing the application will be required to certify that they are satisfied with the adequacy of the partner's Risk Management arrangements in achieving the objectives of the ERIC. Applicants will be invited to cite any external validations or certifications already held in this area. In assessing an application, the ERIC shall reserve the right to make further enquiries into an applicant's Risk Management arrangements should they wish to do so.

Subsequent to an organisation becoming a partner of the ERIC, in the event of an incident or a failure of local Risk Management, the ERIC shall reserve the right to suspend the organisation's partnership and/or issue a notice requiring specific improvements within a given time. In such circumstances, the ERIC shall also reserve the right to conduct, at the partner's expense, any enquiries it deems fit to ensure that specified improvements have been implemented.

2.5. Continuous Improvement

As an organisation committed to quality and effectiveness, in addition to the review cycle referred to above, all participants of the ERIC, whether specifically responsible for the Risk Management Function or not, are encouraged to consider whether ways exist to improve the way in which Risk Management is implemented at any level of E-RIHS.

LEVELS OF THE FRAMEWORK

2.6. Overall Approach

It is essential that the Framework operates appropriately at different levels of the ERIC to ensure that Risk Management is undertaken at the level where ownership and management of each risk can be managed most effectively.

It is also important to recognise that the different Risk Management activities of:

- identification
- ownership
- monitoring.

within the ERIC may be appropriate to be undertaken at different levels within the overall management hierarchy.

Monitoring of individual risks may be required at multiple levels which are hierarchically higher than the levels at which the risks have been identified and would have an initial direct impact.

A particular consideration for Risk Management within an ERIC is the potential for an indirect impact from a risk in the form of reputational damage, either to the ERIC overall at an international level, or to the National Node of the ERIC, arising from an incident occurring which might lower public, political or scientific confidence in the overall capability of the ERIC. It is therefore in the interests of all parties to ensure that effective Risk Management is in place throughout the entire partnership of E-RIHS.

Figure 2 below shows how Risk Management activities are to be performed at different hierarchical levels of E-RIHS.


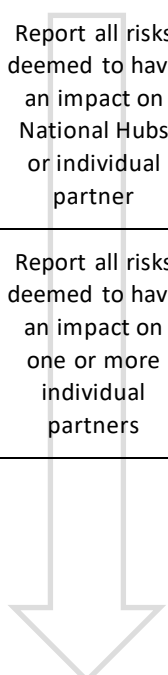
	Identify	Own/Manage	Monitor	Escalation	Communication and Consultation
CentralHub	Any participating organisation may identify any risk at any time. Ownership will be allocated according to the procedures adopted by the National Node and/or the Central Hub	Risks relating to the ERIC overall including reputational risks	All risks owned / managed by the organisation also all risks at any level which are deemed to have an impact on that organisation		Report all risks deemed to have an impact on National Hubs or individual partner
NationalNode		Risks relating to the National Implementation of the ERIC including reputational risks		Notify all risks deemed to have a potential impact at Multi-National Level	Report all risks deemed to have an impact on one or more individual partners
Individual Partners		Risks relating to the Partner organisation and to research activities undertaken by the Partner		Notify all risks deemed to have a potential impact at National level	

Figure 2 – Hierarchy of Risk Management Activities

2.7. Identification of Risk

It is the responsibility of all participants in E-RIHS from individual employee of individual partners up to staff of the Central Hub to report any risks which they identify as having a potential impact on the operations of the ERIC.

A risk is always best expressed in the form:

“There is a Risk that [xxxxxxx] will occur, with the consequence for the ERIC/National Node/Partner/Artefact of [zzzzzzzzzz]”

This facilitates assessment of probability and impact, and also the identification of the most appropriate Risk Owner.

Once identified, all risks will be analysed and initially evaluated by the person(s) responsible for Risk Management at the level where the risk was initially identified and a decision taken about escalation and/or treatment. Details of the analysis and evaluation procedures are given in Section 6.5 and 6.6 below. During all phases of Risk Identification, consideration should be given to involving persons with appropriate skills and knowledge to ensure the most accurate outcome.

The ISO states:

“Risk identification should include examination of the knock-on effects of particular consequences, including cascade and cumulative effects. It should also consider a wide range of consequences even if the risk source or cause may not be evident. As well as identifying what might happen, it is necessary to consider possible causes and scenarios that show what consequences can occur. All significant causes and consequences should be considered.” [5.4.2]

All risks will be held in a Risk Management Database which can be researched to determine whether a similar risk has already been identified and, if so, the status of the risk, who is/was the owner and what treatment(s) have already been applied in mitigation.

A Risk Management Database will be maintained by the Central Hub and will be accessible to all participants in E-RIHS ERIC.

This Risk Management Database will contain a detailed risk inventory, classified in the categories established in Section 17 of the Risk Management Policy:

- a) Financial – impact on E-RIHS finances
- b) Operational – impact on provision of E-RIHS products, projects and services
- c) Reputational – impact on the professional and scientific reputation of E-RIHS and its partnership overall and on its wider general credibility
- d) Physical/Safety – impact on the safety and well-being of people
- e) Regulatory/Legal – impact on E-RIHS of regulatory exposure
- f) People – impact on corporate knowledge / continuity / professional development and welfare of individuals.

2.8. Allocation of Risk Ownership

Upon initial identification, the person with overall responsibility for Risk Management at the level whence the risk has been identified will have initial responsibility for assessing the risk and determining the most likely ownership. Where necessary, the risk will be escalated to Risk Management at National Node or Central Hub Level to agree the most appropriate ownership.

Risks should, except in exceptional cases, always be allocated to a role and not to a named individual. In this way, in the course of normal personnel turnover within an organisation as large as an entire ERIC, the implicit risk that a risk will be overlooked or be lost is mitigated.

2.9. Transfers of Risk Ownership

There may be occasions when it is necessary to transfer the ownership of a risk:

- The scope of a risk may change, necessitating an escalation or reduction in level of the ownership.
- The nature of a risk may change, leading to a re-assessment of the treatment(s) to be applied. This may cause a change in the skills and/or authority required of the Risk Owner.

There is a duty therefore on a person fulfilling a role which includes the ownership of one or more Risks to ensure that in the event of a change in their role or their departure from the organisation, that the new role-holder is fully informed about any Risks for which they are recorded as the Owner.

Anyone taking on a role within the ERIC is recommended to verify that the role does not include responsibility for or ownership of any risks. Partners are recommended to include reference to this risk methodology within any induction procedures for persons joining the ERIC, and also to verify during any exit procedures for persons leaving the ERIC the nature of any Risk Management activities for which the outgoing role holder was responsible.

2.10. Management of Risk

It is the Risk Owner, working in consultation and collaboration with other persons/organisations where appropriate, who will take overall responsibility for the management, treatment and monitoring of a specific risk. Even where multiple persons/organisations are responsible for performing activities relating to a specific risk, ultimate responsibility and authority will always vest in the Risk Owner. It is the Risk Owner who must report on the status of a risk to the overseeing body and must oversee any treatments being applied to mitigate it.

The Risk Owner (in consultation with the appropriate Risk Manager(s)) will be responsible for:

- A detailed analysis of Impact, Probability and Proximity;
- Evaluation of the risk against organisational criteria for Risk Management and appetites for Risk defined in the organisation's and/or the ERIC's Risk Management Policies;
- Identification of option(s) for Risk Treatment, including identification of any risks created by the selection of any particular option;
- Recommending to governing bodie(s) the treatment(s) to be adopted;
- Creation of a Treatment Plan for the treatment(s) adopted;
- Implementation of the Treatment Plan – delegating as necessary;
- Monitoring, Recording and Reporting on the Risk and the Treatment Plan;
- Execution of any Treatment activities in the event that a Risk occurs.

It should be noted that Risk Treatments may be performed by one or more other people or organisations which may or may not be under the direct control of the Risk Owner. It is the responsibility of the Risk Owner to continue to liaise with others involved in the Treatment Plan.

2.11. Monitoring and Review of Risk

Monitoring and review of risk are both regular activities and may also be performed on an ad hoc basis in the event of a change of circumstances relating to the risk.

The purposes of this activity are:

- To verify that the risk has not changed in its nature, affecting impact, likelihood or proximity;
- To ensure that controls relating to risks are still effective;
- To ensure that there have been no changes in external or internal contexts which might have an effect on risk;
- To consider whether lessons learned relating to other risks may have an impact on this risk;
- To identify any emerging risks arising from the existing ones.

Monitoring of risk may occur at levels within the ERIC where there is no ownership or even responsibility for treatment, but where the consequences of the risk may have an impact at that level.

2.12. Escalation Of Risk Ownership

Notwithstanding the Ownership of Risk [see 3.3 above], changes in the scope, nature, context, impact or probability of a Risk may require that it be escalated to a higher tier within the organisation and the ownership re-allocated accordingly.

Examples of circumstances which may lead to an escalation are:

- Elevated risk of adverse reputational impact on the ERIC at national or international level arising from a risk occurring;
- Multiple partners in one or more countries experiencing the same, or closely associated, risks;
- Capacity to treat a risk rising beyond the ability or capacity of the current Risk Owner;
- Changes in a national or international **Political, Economic, Social, Technical, Legal or Environmental** factor (PESTLE).

Upon identification of one of the above circumstances, escalation may be proposed by a current Risk Owner or may be requested by any stakeholder at any level.

Such a request must specify the level to which it is proposed to escalate the Risk Ownership with an explanation of why the proposal is submitted.

The proposal for Escalation of Risk Ownership will initially be considered by the person/body responsible for overall Risk Management within the entity which currently holds Risk Ownership. If they support the proposal, they will forward it to the person/body responsible for overall Risk Management at the level to which it is proposed to escalate the Ownership.

In the event that, following consideration by the responsible person/body, it is decided not to propose to escalate Ownership, the decision will be recorded with reasons for the decision. These will be communicated to the current Risk Owner and also to the Higher Level of Risk Ownership to which it was proposed to escalate it.

At any time, any higher level of Risk Ownership within the ERIC may claim Ownership of a Risk and assume full responsibility for it.

2.13. De-Escalation of Risk Ownership

Similarly, to 3.7 above a change in circumstances may occur leading to Risk Ownership being passed to a lower hierarchical level within the ERIC.

Where a Risk Owner proposes to lower the level of Risk Ownership, this must be with the consent of the proposed new Risk Owner.

2.14. Budgetary and Resource Considerations in Changes of Risk Ownership

Where Ownership of a risk is transferred between levels within the ERIC, it is necessary to recognise the potential impact on resources and budgets of individual partners. The new Risk Owner may reserve the right not to assume ownership where this will cause budgetary or resource pressures or conflicts.

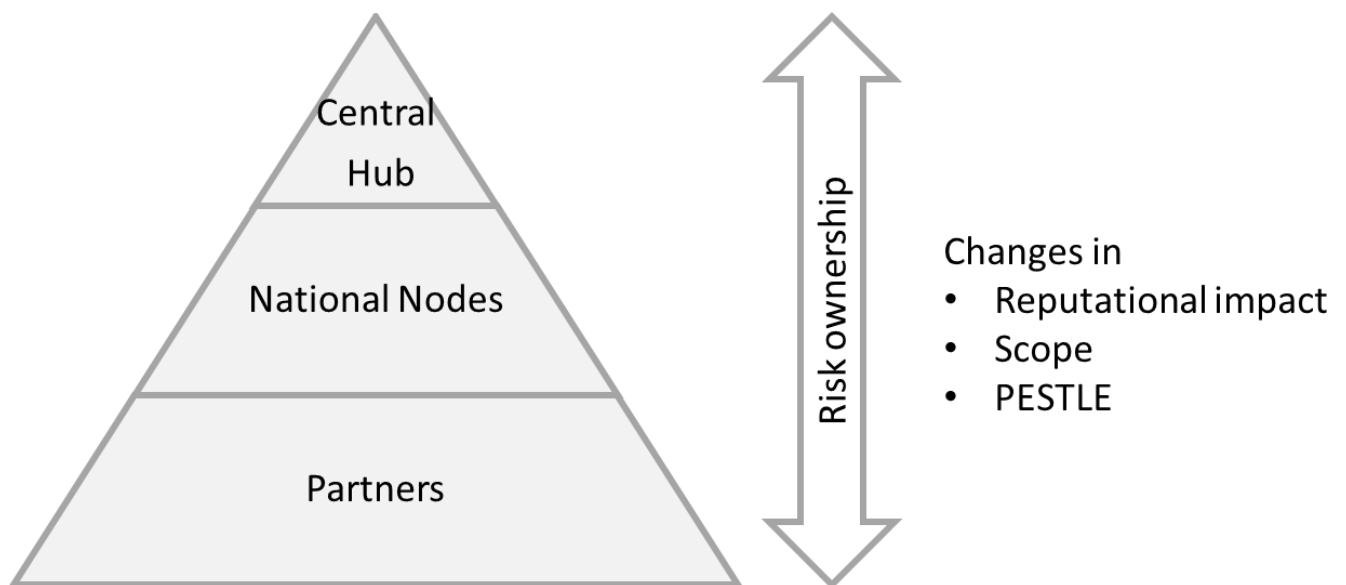


Figure 3 - Escalation of Risk Ownership shows a flow diagram for these processes.

3. SPECIAL GOVERNANCE CONSIDERATIONS FOR A MULTI-TIERED FRAMEWORK

3.1. Communication of and Consultation About Risk

Risks may be of interest to more stakeholders than those directly affected by it. It is necessary to recognise that both internal and external stakeholders may have a continuing interest in specific risks and how they are being treated.

Similarly, within stakeholders, the Risk Owner may be able to identify individual skills or areas of interest which would justify consulting them when initially evaluating a risk and/or assessing different potential treatments.

Consideration should always therefore be given to what consultation activities might be required during the Risk Management process.

The ISO states [5.2] that:

“A consultative team approach may:

- help establish the context appropriately;*
- ensure that the interests of stakeholders are understood and considered;*
- help ensure that risks are adequately identified;*
- bring different areas of expertise together for analysing risks;*
- ensure that different views are appropriately considered when defining risk criteria and in evaluating risks;*
- secure endorsement and support for a treatment plan;*
- enhance appropriate change management during the risk management process;*
- develop an appropriate external and internal communication and consultation plan.*

Communication and consultation with stakeholders are important as they make judgements about risk based on their perceptions of risk. These perceptions can vary due to differences in values, needs, assumptions, concepts and concerns of stakeholders. As their views can have a significant impact on the decisions made, the stakeholders' perceptions should be identified, recorded, and taken into account in the decision-making process.

Communication and consultation should facilitate truthful, relevant, accurate and understandable exchanges of information, taking into account confidential and personal integrity aspects.”

The Risk Management Policy contains over-riding considerations and responsibilities in relation to communication and consultation about risk.

3.2. Confidentiality Considerations

When undertaking communication and consultation activities, it is important to take into account considerations of commercial confidentiality and also personal privacy.

Contracts with third party providers of services to the ERIC, as well as terms and conditions of ERIC partnership may include clauses relating to the maintenance of confidentiality about aspects of the operation of the ERIC. While no contractual clauses can override legal obligations relating to the reporting of risk, it is important that any confidentiality agreements be taken into account.

Risk Managers should make themselves aware of any Non-Disclosure Agreements or confidentiality clauses which might impact on the communication and consultation of risk, and should seek advice from their organisation's legal officers in any case where they are concerned about a possible conflict with such clauses.

Similarly, national Freedom of Information legislation may compel the disclosure of Risk Database entries. While there are normally exceptions to an obligation to disclose documents, these are not intended to frustrate public accountability and transparency.

Risk Database entries should therefore always be phrased to be factual and fully traceable. Where a Freedom of Information request is received by an organisation for disclosure of the contents of the Risk Database, in part or in full, special considerations arise where such disclosure might reveal sensitive or contractual information about a Third Party or other ERIC partner. In all such cases, Risk Managers should immediately consult the person with responsibility for the co-ordination of Freedom of Information requests within their own organisation, and should also inform the Risk Manager(s) of any other organisation whose information might be disclosed.

Similarly, due consideration should be given to any disclosure which may include Personal Data. [See 4.3 below]

3.3. GDPR and Data Protection Considerations

Regulation (EU) 2016/679 (General Data Protection Regulation), known as 'GDPR' came into force across the European Union on 25 May 2018. It is applicable to all countries within the EC as well as any organisation located outside the EC which processes data on behalf of an organisation within the EC.

The Regulation applies to all Personal Data processed by an organisation.

'Personal Data' means any information relating to an identified or identifiable natural person ('data subject') who is alive.

"An identifiable natural person" is one "who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person."

Any personal data included on an entry in a Risk Database would be subject to disclosure in the event of a Data Subject Access Request (DSAR), and the organisation(s) holding or managing the copy of the Risk Database would have the same obligation to ensure that any personal data contained in the Database was held securely and accurately, and only for as long as necessary.

When preparing a Risk Database Entry, it is therefore essential to take account of these legal obligations if Personal Data is to be placed on the Entry.

Wherever possible, references to identifiable persons should be avoided.

No subjective judgements or opinions about an individual should ever be placed on the Database, nor any data about an individual which might be regarded as 'sensitive' – e.g., physical, physiological, genetic, mental, economic, cultural or social data.

It must be borne in mind that referring to an individual by the title of their role or position within an organisation does not exempt the author of a Risk Database entry from their duty of care and accuracy, since if the person is identifiable from the description of their role or position then the data is deemed 'personal' again.

Where a Risk Manager or Risk Owner finds personal data in a Risk Database Entry, they should consider whether the inclusion of that data is justified, and in any case of uncertainty, should consult the person with responsibility for Data Protection within their organisation.

Similarly, if a Data Subject Access Request is received which will require disclosure of a Risk Database Entry, due consideration must be given to avoiding the disclosure of personal data about other individual(s) both within the partner and elsewhere.

4. SUBSTITUTION OF LOCAL RISK MANAGEMENT PROCEDURES

4.1. General Principles

While this manual forms the basis of Risk Management Procedures for the ERIC Central Hub and National Nodes, it is recognised that most, if not all, individual partners with the ERIC may already have put in place Risk Management procedures to address the risks that they already manage.

The ERIC does not intend to increase the administrative overhead of any partner where existing processes are already sufficient to properly identify, assess, treat and monitor risks associated with partnership of the ERIC.

4.2. Assessment of Compliance via Local Procedures

Appendix 2 of the Risk Management Policy provides a checklist to enable partners to compare their internal Risk Management Procedures with those required within the ERIC.

In the first instance, each partner is responsible for assessing its own level of compliance and reporting this to the ERIC.

All facilities seeking to become partner of the ERIC are required to include a statement of compliance, before any artefact from another partner or a Third Party may be processed by them under the auspices of the ERIC.

All such self-certifications must be renewed every 3 years as part of the partnership renewal process on the third anniversary of a partner joining the ERIC.

The ERIC shall reserve the right to require an independent certification of a facility self- certification if there are reasonable grounds for concern that the local procedures are not compliant.

4.3. Amended Procedures Arising from Compliance

Where full compliance has already been achieved or exceeded, partners may choose to comply with their local Risk Management procedures in preference to adopting those specified in this manual.

In such circumstances, entries in the ERIC's Risk Database can be cross-referenced to entries in the partner's Risk Database, and treatment, monitoring and reporting undertaken via that Database. Where only Partial Compliance has been achieved, partners may choose to comply with this Manual only where a non-Compliance exists, or, if preferred, to incorporate the procedures contained in this manual into their own local procedures.

In such cases, entries in the Risk Database may refer to the local Risk Database where compliant procedures exist.

The use of a local Database to maintain records of risks does not remove the obligation of a Risk Owner to keep stakeholders elsewhere in the ERIC consulted and informed where required.

If a risk is escalated to either a National Node or the Central Hub of the ERIC, the risk must be transferred fully into the ERIC's own Risk Register, even if the Owner does not change.

5. MANAGEMENT OF RISKS RELATING TO THE ERIC OVERALL

5.1. General Considerations

The Management of Risks relating to the ERIC overall is the responsibility of the Central Hub. All risks relating to the ERIC overall must be escalated to this level.

The Risks which will arise in this category are both Physical (risks to assets, premises, information systems, staff safety etc) and Managerial (economic, political, reputational, social etc).

The Physical risks which might arise will be similar to those identified in any large, premises-based organisation, but with consequences with the capacity to have an impact across the entire partnership of the ERIC.

For example: the loss of a central file server containing a knowledgebase of techniques and research outcomes owing to a virus infection or a network outage would have the potential to impact every ERIC partner and to hinder or prevent their activities. Similarly, the loss of a central financial database containing details of contracts, payments, grant agreements, etc. could cause a great deal of inconvenience.

While the options for the treatment of a risk relating to a file server will be identical whatever the size of an organisation, differences in impact across the ERIC may justify on cost-effectiveness grounds more dramatic treatments than a treatment for a server used by only one ERIC partner. Scope and Scale of the impact of any Risk will therefore be a material consideration in all Risk Assessments and will affect decisions on Risk Ownership as well as on Risk Treatments.

5.2. Escalation of Risks to the ERIC Central Hub from National Nodes

There will be a number of circumstances when a Risk identified at National Level may be escalated to Central Hub level:

- The Impact of the Risk is considered to affect more than one Nation. (For example, changes in European legislation affecting all Members);
- A National Node recognises that a Risk that they have identified has also been identified by one or more other National Nodes, and a common treatment or a shared treatment is seen as the optimum approach which seems that this is best co-ordinated by the Central Hub;
- The Central Hub notes from its records that a similar or identical risk has been identified by 2 or more National Nodes.

The Central Hub shall always have the right to determine if a risk shall be escalated to be monitored at Central Hub Level, even if the risk treatments are performed and managed at a lower level. In such cases, the Risk Manager at the Central Hub will liaise with the Risk Managers at National Nodes to provide an overview of the status of the risk and its treatments in order to ensure that all National Nodes are equally well-informed about the risk.

Once a risk has been escalated to the Central Hub, it will not normally be de-escalated until it has been closed.

5.3. Introduction to the Common Risk Management Processes

The following risk management processes are based on the ISO as well as the best practice identified in the UK Office of Government Commerce's methodology "Management of Risk" (M_o_R).

The processes are applicable at all levels of the ERIC. The following sections should therefore be read by all persons involved in Risk Management within the ERIC.

5.4. Risk Identification

The ISO states:

"The organisation should identify sources of risk, areas of impacts, events (including changes in circumstances) and their causes and their potential consequences.

Identification should include risks whether or not their source is under the control of the organisation, even though the risk source or cause may not be evident. Risk identification should include examination of the knock-on effects of particular consequences, including cascade and cumulative effects. It should also consider a wide range of consequences even if the risk source or cause may not be evident. As well as identifying what might happen, it is necessary to consider possible causes and scenarios that show what consequences can occur. All significant causes and consequences should be considered."

Risks may be identified in a number of ways:

- A facilitated risk workshop addressing specific topic areas;
- A facilitated 'Pre-Mortem' to consider a specific scenario in advance and seek to identify all the reasons why a failure might occur;
- Performance indicators which show symptoms of potential failures;
- Intelligence obtained from individuals based either on their professional and/or technical knowledge or on incidents observed by them to be occurring elsewhere;
- An alert from another organisation;
- Management consideration of a change in the context or the circumstances of an organisation triggered by an announcement from outside the organisation;

As stated in 3.2 above, Risks are best expressed in the form:

"There is a Risk that [xxxxxxx] will occur, with the consequence for the ERIC/National Node/Partner/Artefact of [zzzzzzzzzz]"

Once identified, it should be verified that no identical or similar risk already exists within the Risk Database. If an identical or similar risk does already exist, then, in the event that the context or scope is different, the existing Risk Database entry should proceed to the next stage of the process along with any freshly identified risks.

5.5. Risk Analysis

The ISO states that:

"Risk analysis involves developing an understanding of the risk. Risk analysis provides an input to risk evaluation and to decisions on whether risks need to be treated, and on the

most appropriate risk treatment strategies and methods. Risk analysis can also provide an input into making decisions where choices must be made and the options involve different types and levels of risk.

“Risk analysis involves consideration of the causes and sources of risk, their positive and negative consequences, and the likelihood that those consequences can occur. Factors that affect consequences and likelihood should be identified. Risk is analysed by determining consequences and their likelihood, and other attributes of the risk. An event can have multiple consequences and can affect multiple objectives. Existing controls and their effectiveness and efficiency should also be taken into account.

Risk is often measured in terms of Impact and Probability in order to permit quantitative methods to be applied. In order to compare different Risks and identify those which are the greatest threat to the organisation, it is common to multiply numeric values assigned to different levels of Impact and Probability and then evaluate product of that multiplication in order to create a measurement scale for **Risk Weighting**.

A 3-point scale to measure Impact and Probability – High, Medium, Low – is commonly adopted, but is potentially lacking in sensitivity, since any product will have a Risk Weighting numeric value of only 1 – 9. In a complex organisation, this lacks granularity for prioritisation.

A 5-point scale can be created by adding Very High, and Very Low, thereby producing a Risk Weighting value range of 25.

It is proposed to adopt a 5-level scale but to include in the Risk Policy specific factors which will define the level of Impact and Probability for different contexts – e.g. Human Health and Safety, Integrity and Risk of Harm to an artefact, Financial or Reputational Impact, Measurements of Probability linked to absolute events.

One additional factor which should be considered is Risk Proximity – the time before a risk might occur and the likely duration of the period during which the risk would be capable of occurring. This measurement can assist in deciding when to apply different treatments and for how long these might be required.

A third 5-level scale is therefore defined to assist in the identification of Proximity.

An example of where Risk Proximity might be of great importance would be in determining capital expenditure profiles where there was uncertainty about costs. If the risk of cost over-runs might only occur in the next financial year, and uncertainty would be removed by the end of the financial year, then any treatment in which additional provision was to be made in capital budgets would only require to be included for one financial year. Since there is a cost associated with reserving capital, either through loss of investment opportunity elsewhere or through the need to extend credit arrangements, proper measurement of Proximity could reduce these costs.

The application of this third, 5-level scale, will be applied to assist in prioritisation of Risk Management, since it now enables the creation of a 1 – 125 scale of measurement for Risk Weightings.

The process of Risk Analysis may be quantitative, qualitative or a combination of both.

The Risk Analysis may require consultation with a wide range of stakeholders to fully determine the nature of the risk. Among possible consultees are:

- Acknowledged experts on the subject under consideration;

- Persons who have experienced similar risks;
- Auditors who have already identified and assessed existing controls to determine their effectiveness in managing the risk under consideration;
- Manufacturers or service providers who can provide data on failure rates.

It may be necessary to commission an experimental study or conduct simulation or modelling exercises.

The ERIC might establish an Expert Panel, comprising both persons who are already participants in the ERIC with acknowledged expertise in the areas of risk being analysed and also independent persons with similar expertise.

Depending on the nature of the risk being considered, the Risk Manager may seek direction from the Management Board of their organisation as to what level of Risk Analysis to undertake. Similarly, where there is a divergence of opinion between persons consulted about a risk, the Risk Manager may seek a Direction from the Management Board as to how to balance divergent opinions.

The practical application of these scales of measurement to calculate a Weighting is shown below. A measurement scale is defined in the following terms:

A measurement scale is defined in the following terms:			
IMPACT	PROBABILITY	PROXIMITY	WEIGHTING
Very High	Very High	Now	5
High	High	Very Soon	4
Medium	Medium	In 1 Year	3
Low	Low	In 2 Years	2
Very Low	Very Low	In > 2 Years	1

A Risk is identified with a **High** Impact, **Medium** Probability and likely to occur in **2** Years. The weightings are thus $4 \times 3 \times 2 = \underline{24}$

Another Risk is identified with a **Medium** Impact but a **Very High** Probability which is likely to occur **Very Soon**. The weightings are therefore $3 \times 5 \times 4 = \underline{60}$

Provided agreed, consistent definitions are applied to each weighting, this system can be used to compare and prioritise Risks for Treatment.

Figure 4 - Application of Risk Weightings.

5.6. Risk Evaluation

All organisations must understand their Appetite For Risk – the quantity of risk that they are willing to accept or attempt to treat. This Appetite for Risk of E-RIHS ERIC is detailed in Section 20 of the Risk Management Policy.

It will also be necessary, however, to consider the Appetite for Risk of individual partners, National Nodes and associated third parties.

There may also be legal and regulatory considerations. For the Central Hub, it will be necessary to take into account any such considerations arising for only one partner arising from a local change in the legal or regulatory environment.

Based on the above considerations, as well as the outcomes of the Risk Analysis, a decision will be taken whether to:

- Seek further information about the risk
- Tolerate the risk, and take no further action beyond maintaining existing controls.
- Apply new treatments to the risk

Although it is the responsibility of the Risk Manager to prepare the Risk Evaluation, subject to any delegation of authority contained within the ERIC's Risk Policy, the ultimate decision on how to respond to the Evaluation will lie with the overall executive body of the ERIC.

5.7. Risk Treatment

A Treatment for a Risk is intended to reduce either the Impact or Probability of a Risk in order to bring it within the ERIC's Risk Appetite.

Treatments normally fall into one of the following 5 categories:

- **Risk Avoidance.** Discontinue or do not perform an activity which will give rise to a Risk.
- **Risk Reduction.** Reduce the Impact or Probability of a Risk occurring by adopting different procedures or increasing controls.
- **Risk Contingency** (also referred to as Fallback). Take no action to reduce the probability of a Risk occurring but create a detailed plan about how to respond if and when it does.
- **Transfer Risk.** This is commonly used to describe the use of an insurance policy to mitigate a financial risk. A Transfer of Risk can also be accomplished by contracting with a Third Party to provide a service where a Risk of non-delivery owing to absence of resources or lack of capability exists. It must be borne in mind, however, that it is not possible to transfer risks of reputational harm to the organisation, nor to transfer legal or regulatory obligation.
- **Share Risk.** Similar to Risk Transfer, the consequences of a Risk can be shared with a Third Party where there are counter-balancing benefits where the Risk does not occur and both parties agree to share those benefits. An example of this might be agreeing to share income in return for a shared approach to development costs. The caveat regarding Reputational Risk at 4 above also applies in this case.
- **Accept Risk.** Take no action to mitigate the Impact or Probability. Rely on existing controls, where applicable.

Generally, Treatments are used to reduce either Impact or Probability but not both. It may therefore be appropriate to apply multiple treatments to a single risk. A Treatment may also be capable of lowering Proximity (e.g., delay an activity for a period of time).

It must also be recognised that the adoption of a specific treatment for risk may generate risks itself. These must be taken into account in the overall options appraisal of what Risk Treatment(s)

to adopt. These new risks should, however, be clearly linked to the Risk being treated, since they are not a risk in the absence of the Risk Treatment being planned.

In selecting Risk Treatment(s), it is also important to consider the values and perceptions of stakeholders. A particular potential Risk Treatment may be unacceptable to stakeholders on political, ethical or cultural grounds (In the context of the ERIC, an example of an unacceptable Risk Treatment might be the relocation of a heritage object to a different country for processing)

Once a possible Treatment has been identified, using the same calculations shown in Figure 4 - Application of Risk Weightings above, it is possible to compare the pre- and post-Treatment weightings of any particular risk and thus measure the effectiveness of a Treatment. In this way, the effectiveness of potential different Treatments can be compared.

The selection of a particular Risk Treatment might require a financial analysis of the cost of the treatment against the possible financial (or other) losses incurred should a risk materialise.

The best method of conducting such an analysis is to compare the potential financial impact of the risk with the cost of the proposed Treatment, taking into account any residual impact which the Treatment will not address.

The following is an example of how to perform such an analysis.

A risk has been identified which has a 20% probability of occurring. If it were to occur, the financial cost to the organisation would be €100,000.

By the expenditure of €5,000 the probability of the Risk occurring can be reduced from 20% to 5%.

The following analysis is performed:

$$\frac{\text{Potential Financial Impact of Risk}}{\% \text{ Probability of Occurrence}} > (\text{Cost of Treatment} + \text{Residual Impact Costs})$$

$$\frac{€100,000 \text{ (PFIR)}}{20\% = 5 \times \frac{100}{20}} = €20,000$$

$$\text{Cost of Treatment} = €5,000.$$

$$\text{Residual Impact Costs} = \text{Probability reduced to 5\%} = \frac{€100,000}{5\% = 20 \times \frac{100}{5}} = €5,000$$

Therefore, in this example, the Potential Financial Impact of the Risk (PFIR) is €20,000. The total costs of Treatment = €5,000 + €5,000 = €10,000.

This does not dictate that the organisation will automatically authorise the expenditure of €5,000 to reduce the risk. This decision will be influenced by the organisation's Risk Policy. However, it enables an informed decision to be made about Treatment of Risk.

5.8. Creating a Risk Treatment Plan

Once the Risk Treatment(s) have been selected, a Plan is created to show how those Treatment(s) will be implemented. The Plan will show:

1. The reasons for the Treatment(s) selected including expected benefit(s) –e.g., estimated reduction in impact / probability;
2. Identities of those approving the plan and those responsible for implementing the plan;
3. Details of action(s) required;
4. Resource requirements (including any contingencies included);
5. Performance measures;

6. Any constraints identified in the Plan;
7. Monitoring and reporting requirements;
8. Timing and scheduling details;
9. Details of stakeholders to receive communications about the plan.

The Plan is then associated with the entry in the Risk Database, and forms the basis of ongoing reviews of that Risk.

Such reviews should include a regular review of the pre- and post-Treatment Weightings of the Risk to determine whether the Treatment remains effective and whether the status of the Risk itself is rising or falling, and thus whether further, or amended, Treatments are required.

5.9. Budgetary Considerations

Depending on the final governance model adopted for the ERIC, and for the funding of the Central Hub, there may need to be discussions about funding of Risk Treatments where there are budgetary considerations for partners.

All Risk Treatments which involve expenditure shall be reviewed as part of annual financial planning activities and shall be explicitly shown in the ERIC Central Hub's Financial Plan.

In the event that it is necessary to discontinue or re-scale a Risk Treatment as a result of budgetary constraints, the revised impact of the Risk shall be clearly stated in a report to the governing body of the ERIC overall. The ERIC's Risk Manager is responsible for the preparation of all such reports.

6. MANAGEMENT OF RISKS AT NATIONAL NODE LEVEL

6.1. General Considerations

While many of the techniques and procedures described in Section 6.3 et seq. above continue to apply at National Node Level, there are some additional considerations to take into account.

While the National Node has oversight of all activities by partners within their geographical scope, it must also always consider whether the risks which it is managing have implications beyond its own territorial boundaries, and could impact on other regions or possibly on the ERIC overall.

When identifying and reviewing risks, it is therefore essential for the National Node to consider whether the impact of a risk extends beyond its own boundaries and also whether another part of the ERIC is already addressing a similar risk. If another part of the ERIC is addressing a similar risk, consideration must be given to whether the treatment(s) being put in place might also be capable of treating this new risk.

For example, if one National Node has already entered into a contract for a standby cloud-based server service in the event of a local systems failure, would it be possible to join the same contract to treat a similar risk identified by another National Node.

This example also raises the question of whether, where multiple National Node are treating an identical risk, whether this should be escalated to the Central Hub for the creation of a single, common treatment.

For this reason, when a new risk is identified or escalated to the National Node, the Risk Manager must review the ERIC Risk Database to determine whether an identical or similar risk already exists and then decide, in consultation with their Node coordination and with the Owner identified on the database, the extent to which the existing, or a similar treatment might be applied to the risk.

6.2. Escalation of Risks to National Node from Individual Partners

There are a number of situations where a risk may be escalated to a National Node from an individual partner:

1. The Impact of the risk is considered to affect more than one partner (For example, changes in legislation affecting conditions of service of employees);
2. The partner recognises that a risk that they have identified has also been identified by one or more other partner, and a common treatment or a shared treatment is seen as the optimum approach which seems that this is best co-ordinated by the National Node (even if it leads to multiple independent treatment plans);
3. The National Node notes from its records that a similar or identical risk has been identified by 2 or more partners.

The National Node shall always have the right to determine if a risk shall be escalated to be monitored at national level, even if the risk treatments are performed and managed at a local level. In such cases, the Risk Manager at the National Node will liaise with the Risk Managers at individual partners to provide an overview of the status of the risk and its treatments in order to ensure that all partners are equally well-informed about the risk.

6.3. De-Escalation of Risks from the National Node to an Individual Partner

There may be occasions when a risk ceases to impact more than one partner.

An example of this might be where there is a widespread initiative to upgrade a particular item of software, and security implications, requiring a Risk Treatment, exist until the upgrade is performed. It is likely that at some point, only one partner will remain where the required upgrade has not yet been performed. In such a case, provided the Risk no longer has any impact at national level (or above), the National Node may wish to cease to co-ordinate or monitor the Risk Treatment. In such a case, the National Node may wish to discontinue any central Risk Treatment and return Ownership to the one remaining partner.

Any wish to de-escalate a risk must be indicated to the partner to which it will be de-escalated with reasonable advance written notice. Except where otherwise agreed, 'Reasonable' shall be deemed to be not less than 3 calendar months.

Where a Risk Treatment requires the provision of external services, the National Node will provide all reasonable support to the partner to enable it to assume ownership.

Where a partner considers that it lacks the expertise or resources to assume ownership of a risk, it may request the National Node to continue to maintain ownership, subject to mutually satisfactory financial arrangements being agreed for the continued provision of any funded services (e.g., external servers, additional maintenance contracts) which are now solely for the benefit of the partner.

7. MANAGEMENT OF RISKS AT INDIVIDUAL PARTNER LEVEL

7.1. General Considerations

While many of the techniques and procedures described in Section 6.3 et seq. above continue to apply at individual partner level, there are, again, some additional considerations to take into account.

Firstly, as explained at Section 5 above, partners are permitted to substitute equivalent local techniques and procedures for Risk Management to the ones defined in this manual. This does not remove an obligation to include all risks on the ERIC Risk Database, but permits risks to be managed in accordance with local arrangements.

Partner must continue to update the ERIC Risk Database as the Treatment of a risk evolves.

Secondly, similar to the higher tiers of Risk Management, where a partner identifies a new risk, it must also always consider whether the risk might have implications beyond its own facility, and could impact on other partners or possibly on the ERIC overall.

7.2. Escalation of Risks to National Node

See Section 7.2 for details of the circumstances where a risk may be escalated to the National Node level.

It should be borne in mind that any cost or other resource implications relating to the risk must always be mutually agreed between the individual partner and the National Node.

7.3. De-Escalation of Risks to Individual Partner

See Section 7.3 above for details of the circumstances where a risk may be de-escalated from the National Node back to an individual partner and the procedures to be followed.

8. MANAGEMENT OF RISKS RELATING TO SPECIFIC OBJECTS

8.1. General Considerations

There will be occasions where the research activities of a specific object give rise to risks which are unique to that object.

For example, where an object is fragile or has deteriorated badly, risks may arise relating to protecting it from any, or further, harm during each stage of research activities. This will include the entire life-cycle of an object's study, from initial transportation, through storage, handling and return. See Section 10 below for the Management of risks relating to specific procedures.

A Risk Management planning exercise should always be performed for any object accepted for study by the ERIC. It may be that a generic Risk Plan can be applied to the object if the partner is well-experienced in dealing with objects of this type, or that an existing generic plan can be customised to address specific attributes of the object.

Although ultimately an individual partner will be responsible and accountable for the safe custody of an object which is entrusted to the ERIC for study, it will be one of the strengths of the ERIC that the combined specialist knowledge and experience of the entire partnership can be drawn upon in order to safeguard an object entrusted to our care.

A Risk Management planning exercise may also identify additional costs relating to the study of the object (for example – additional security requirements) which must then be agreed with all stakeholders including any apportionment of costs between different parties.

It should be noted that this approach is likely to be mandated by the insurers of all organisations involved in the study of an object, and will also serve to give confidence to the wider public that the ERIC places a high level of value and respect for objects placed in its care.

8.2. Object Risk Management Planning

When an object/artefact is identified as a candidate for study by the ERIC, a high-level risk planning exercise should be undertaken as early as possible in order to determine whether it should be accepted for treatment. This exercise should also identify whether there are any special conditions or exclusions which should be applied to any agreement to undertake research within the ERIC.

At the initial stage, one consideration will be the risk to the reputation of the ERIC and its partners in the event of any damage occurring to the object. Where a partner has concerns about this risk, they should consult the National Hub, who will decide whether escalation to the Central Hub is also required. This exercise will identify an overall Risk Owner for the object.

At this stage, the risk planning exercise is likely to be conducted entirely within the ERIC partnership.

Subject to any exclusions or limitations identified in this initial exercise, the Risk Owner will then conduct a detailed risk planning exercise, consulting with other stakeholders – including the object owner, any identified specialists, any third-party organisations involved in transportation or storage and the person(s) responsible for the management of each treatment.

This will first identify all the stages in the lifecycle of the object while in the care of the ERIC and then identify any risks which relate to that stage. For each risk so identified, the procedures described in Section 6.3 et seq. above can be followed.

The output of this will be an object Risk Management Plan, which will describe the treatments for each risk identified, and the identity of the owner for each risk.

It should be noted that in many cases, the capability and expertise of the partner owing each Risk will be sufficient that the only treatment required is to rely on existing controls – e.g., building security, environmental control in storage, handling procedures etc.

The person acting as overall Risk Owner may change during the course of the object's lifecycle within the ERIC, but that person will be responsible for all monitoring and co-ordination of individual Risks and Risk Owners until the object leaves the responsibility of the ERIC.

It may be appropriate at the completion of an object's treatment to conduct a short lesson learned exercise to identify where Risk Treatments proved to be effective or where they were found to be insufficient and had to be supplemented, or excessive and un-necessary.

8.3. Object Risks Database

Object Risk Management Plans will be gathered and stored in the ERIC's Risk Database to be accessible in the event of a similar object being submitted for analysis in the future.

9. MANAGEMENT OF RISKS RELATING TO SPECIFIC PROCEDURES

9.1. General Considerations

Certain analysis procedures carry implicit risks within them. These risks can relate both to the integrity of an object/artefact being treated, and also to the health and safety of persons carrying out these techniques.

For example, the use of a particular chemical on an object might require special handling techniques to protect the object from harm as well as special protective clothing or a protective environment to safeguard the health and safety of the person(s) undertaking the procedure.

In many cases, a partner's controls to ensure compliance with existing legislation and regulation will already protect the health and safety of the person(s) undertaking the procedure.

It is, however, desirable to note the risks associated with elements of a procedure since they may have a bearing on the capability of a partner to accept an object for submission to a particular procedure and also on the costs of performing a particular procedure.

For example, if a certification of competence is required for a member of staff undertaking a procedure, it may place restrictions on the pool of staff capable of performing that procedure, thus impacting on overall resource demands and also on the timescales within which a procedure can be completed.

Conversely, it may also identify the need to undertake further certification and training of staff where a procedure is much in demand – or to identify alternative sources of staff holding the required certification where this is only needed on an infrequent basis.

9.2. Procedure Risk Management Planning

The process to be followed in undertaking a planning exercise for a procedure is similar to that described in Section 9.2 above.

The Risk Management planning exercise is likely to take place in 2 stages, and may well be conducted in parallel with an object Risk Management planning activity.

The initial exercise will be to determine whether the partner possesses the competence to perform the procedure and adequately manage the associated risks.

The detailed exercise will be to examine each component of the procedure and identify risks associated with it. It should be noted that during the detailed exercise, it is essential to consult the person with overall responsibility for the Health and Safety of Persons both within the partner and also the equivalent person in any other partner which will be involved in the procedure should the detailed exercise identify any risks relating to personal Health and Safety – e.g., the use of hazardous chemicals, radiological materials or cryogenic techniques.

The output of this detailed exercise will be the procedure Risk Management plan which will identify an overall Risk Owner. While this person may be the same person who acts as Overall Risk Owner for an Object Risk Management plan for the object to which the procedure will be applied, they must have sufficient authority to ensure that risk treatments relating to Health and Safety are fully complied with, actions properly documented and issues of non-compliance within the organisation are addressed without delay.

The overall Risk Owner will oversee and co-ordinate the activities of individual Risk Owners throughout the duration of the procedure. While the immediate responsibility of the overall Risk Owner will finish once the procedure is certified as complete, there is the potential for subsequent enquiry in the event of subsequent issues about long-term damage to an object or to the physical well-being of a person involved in the procedure.

Documentation must therefore be stored in accordance with the partner's own local procedures for compliance with Health and Safety regulations. It should be noted that it might be required by law to store such documentation for many decades.

Supplementary to this, procedure Risk Management plans should also be stored in the ERIC's Risk Database in order to assist any other partner planning to use a similar procedure.

9.3. Issues of Proprietary Knowledge in Risk Management

It is acknowledged that in some cases, partners may be undertaking procedures which are rendered possible only by the use of proprietary knowledge which will not be shared under the terms of partnership of the ERIC.

It is the highest priority of this Risk Management Framework, however, that risks to the Health and Safety of all persons dealing with the ERIC shall be eliminated or at least minimised.

Where a partner, in registering a Procedure Risk Management Plan, is concerned to protect proprietary knowledge, or is constrained by other confidentiality agreements, the Risk Management Plan should still be uploaded to the Risk Database but with proprietary knowledge redacted. In this instance, a note should be attached to the Risk Management Plan noting the redaction and giving details of a contact at the Partner Organisation in the event of an enquiry concerning the redacted information.

10. MANAGEMENT OF OPPORTUNITY

10.1. General Considerations

Where a risk offers positive consequences (as opposed to negative), it is often referred to as an **Opportunity**.

While this framework primarily addresses the management of negative consequences, it is appropriate to consider the management of opportunities since many of the same processes referred to above continue to apply.

10.2. Identification of Opportunity

An opportunity to achieve a positive consequence may be identified from anywhere within the ERIC. Opportunities may arise from new or more efficient procedures, new knowledge, new clients/partners/associates or new sources of funding or support.

The level at which an opportunity will be managed is determined in the same way as for a risk.

10.3. Analysis and Evaluation of Opportunity

An opportunity must be subjected to the same scrutiny as a risk in order to determine the best response. This will require the identification of not only the benefits which the opportunity will offer, but also any new risks which will arise from pursuing it.

In some cases, the benefits and risks may be directly opposed to one another. For example, an increase in reputation and potential new funding in the event that the opportunity is fully and successfully exploited may be counterbalanced by loss of reputation and existing funding in the event that the attempt to exploit the opportunity is unsuccessful.

In order to achieve these benefits, new financial investment might be required in equipment or staff resources, and it is important to assess these against the estimated benefits to be accrued.

10.4. Responses to Opportunity

The M_o_R methodology proposes 4 responses **to an opportunity**:

1. **Reject.** The ERIC/National Node/partner may decide, after assessment and evaluation, that the risks which accompany the opportunity, were it to be pursued, outweigh the potential benefits.
2. **Exploit.** Pursue the opportunity if possible. The ability to do this may be determined by a number of events occurring.
3. **Enhance.** Since an opportunity is, by its definition, not certain but only a possibility, it may be possible to take actions to increase the probability of it occurring or the impact if it does occur. This is an interim response since it will be necessary to decide to **Exploit** the opportunity if it does occur.
4. **Share.** By engaging with one or more other parties/partners, it might be possible to reduce the risks associated with an opportunity by sharing the benefits should it occur.

In the case of responses 2 – 4, it will be necessary to prepare an **Opportunity Management Plan** and identify an Opportunity Owner.

10.5. Management of Opportunities

The opportunity will then be managed in the same way as a risk.

It should be noted that financial or other investment to exploit or enhance opportunities may not be made by the same organisation as the one(s) to whom the benefit(s) will accrue.

It may therefore be necessary to agree budgetary arrangements for all those involved so that risks and benefits are equitably shared.

APPENDIX 1 - SUMMARY OF TERMS AND DEFINITIONS

TERMS AND DEFINITIONS (as defined in ISO-31000)

Risk

effect of uncertainty on objectives.

Risk management

coordinated activities to direct and control an organisation with regard to risk management framework.

set of components that provide the foundations and organisational arrangements for designing, implementing, monitoring, reviewing and continually improving risk management throughout the organisation.

Risk management policy

statement of the overall intentions and direction of an organisation related to risk management.

Risk attitude

organisation's approach to assess and eventually pursue, retain, take or turn away from risk.

Risk management plan

scheme within the risk management framework specifying the approach, the management components and resources to be applied to the management of risk.

Risk owner

person or entity with the accountability and authority to manage a risk.

Risk management process

systematic application of management policies, procedures and practices to the activities of communicating, consulting, establishing the context, and identifying, analysing, evaluating, treating, monitoring and reviewing risk.

Establishing the context

defining the external and internal parameters to be taken into account when managing risk, and setting the scope and risk criteria for the risk management policy.

External context

external environment in which the organisation seeks to achieve its objectives.

Internal context

internal environment in which the organisation seeks to achieve its objectives.

Communication and consultation

continual and iterative processes that an organisation conducts to provide, share or obtain information and to engage in dialogue with stakeholders regarding the management of risk.

Stakeholder

person or organisation that can affect, be affected by, or perceive themselves to be affected by a decision or activity.

Risk assessment

overall process of risk identification, risk analysis and risk evaluation.

Risk identification

process of finding, recognizing and describing risks. Includes the identification of risk sources, events, their causes and their potential consequences.

Risk source

element which alone or in combination has the intrinsic potential to give rise to risk.

Event

one or more occurrences (or non-occurrences) or change of a particular set of circumstances.

Consequence

outcome of an event affecting objectives.

Likelihood

chance of something happening.

Risk profile

description of any set of risks.

Risk analysis

process to comprehend the nature of risk and to determine the level of risk.

Risk criteria

terms of reference against which the significance of a risk is evaluated

Level of risk

magnitude of a risk or combination of risks, expressed in terms of the combination of consequences and their likelihood.

Risk evaluation

process of comparing the results of risk analysis with risk criteria to determine whether the risk and/or its magnitude is acceptable or tolerable.

Risk treatment

process to modify risk.

Control

measure that is modifying risk

Residual (or retained) risk

risk remaining after risk treatment.

Monitoring

continual checking, supervising, critically observing or determining the status in order to identify change from the performance level required or expected.

Review

activity undertaken to determine the suitability, adequacy and effectiveness of the subject matter to achieve established objectives

References

ISO31000:2009 as updated in ISO31000:2018 (Risk Management – Principles and Guidelines)

ISO IEC 31010:2009 - Risk management - Risk assessment techniques

ISO/TR31004:2013 - Risk management — Guidance for the implementation of ISO 31000

The Management of Risk (M_o_R) – produced by Axelos as part of the Prince2 suite of methodologies ISBN 9780113312740

A Risk Practitioners Guide to ISO 31000: 2018 - Institute of Risk Management

EU General Risk Assessment Methodology - Action 5 of Multi-Annual Action Plan for the surveillance of products in the EU (COM(2013)76)

ERIC Practical Guidelines published by the EC Directorate-General for Research and Innovation (ISBN 978-92-79-37861-4)

Annex B: Updated Risk Management Policy

1. PURPOSE

The purpose of this Risk Management policy is to communicate the E-RIHS ERIC's [hereinafter referred to as "E-RIHS"] commitment to managing enterprise-wide risks and to establish clear responsibilities for itself in order to maximize strategic and operational achievement.

2. SCOPE AND CONTEXT

This policy applies to directors, management and staff of the Central Hub of E-RIHS. The principles contained within the Policy will also apply to any National Node or individual partners which have formally adopted the policy in preference to a local policy.

E-RIHS is committed to the formal, systematic and structured proactive management of risks across the entire ERIC.

Risk is inherent in all aspects of E-RIHS's activities and whilst many of these risks cannot be eliminated, they can, however, be identified, quantified and controlled. Risks that impact on the objectives of E-RIHS can offer both opportunity and threat. This policy is designed to provide E-RIHS personnel with a systematic framework in order to minimise threats and maximise opportunities to E-RIHS.

The document should be read in conjunction with the E-RIHS Risk Management Framework.

3. KEY OBJECTIVES

The key objectives of this policy are as follows:

1. This policy adopts the International Standard "Risk Management – Guidelines" ISO 31000 Second Edition 2018-02 definition of risk management as **"coordinated activities to direct and control an organisation with regard to risk"**.
2. This policy confirms that E-RIHS is committed to implementing a strategic, consistent and structured enterprise-wide approach to risk management in order to effectively manage opportunities for gain and minimise the impact of threats causing losses.
3. This policy is aligned to reflect ISO 31000:2018 [hereafter referred to as "the ISO"] which provides the framework used to develop the E-RIHS enterprise-wide risk management framework. Policy is defined by the ISO as being a control to measure and/or modify risk (Section 3.8).
4. Risk will manifest itself in many forms and has the potential to impact the health and safety, environment, community, reputation, regulatory, operational, and financial performance of E-RIHS and, thereby, the achievement of the organisation's objectives as well as causing reputational harm.
5. By understanding and managing risk, E-RIHS will provide greater certainty and confidence for our stakeholders, E-RIHS directors and employees, participants, and for the communities in which we operate.

6. E-RIHS will use our risk management capabilities to maximise the value from our assets, projects, programs and other business opportunities and to assist us in fostering participation and/or performance in our organisation.
7. Risk management will be embedded into our business activities, functions and processes. Risk understanding and our tolerance for risk will be key considerations in our decision making.
8. Risk issues will be identified, analysed and ranked in a consistent manner. Common systems and methodologies will be used.
9. Risk controls will be designed and implemented to reasonably assure the achievement of organisational objectives. The effectiveness of these controls will be systematically reviewed and, where necessary, improved.
10. Risk management performance will be monitored, reviewed and reported. Oversight of the effectiveness of our risk management processes will provide assurance to executive management, the General Assembly and relevant stakeholders.
11. The effective management of risk is vital to the growth and success of E-RIHS.

4. REVIEW OF POLICY

This policy is subject to formal review initially after 2 years or any time that a new edition of the ISO is released.

5. ACCESS TO THE POLICY

This policy will be available for viewing to any employee of E-RIHS and also to any person in a partner organisation engaged on work commissioned via the E-RIHS. In addition, this policy may be made available to any third party at the discretion of E-RIHS' Director General.

6. RISK MANAGEMENT PROCESS AND PROCEDURES

The directors and management of E-RIHS view risk management as integral to its strategic intentions as defined in Article 2 of Statutes and Section 1 (E-RIHS Principles) of the Scientific and Technical Description.

E-RIHS' risk management policy provides a system to manage the risks associated with its core activities in order to achieve these intentions.

7. RISK MANAGEMENT REQUIREMENTS

The following are the central requirements of E-RIHS' approach to Risk Management:

1. Risk management will be incorporated into the strategic and operational planning processes of E-RIHS;
2. All partners will, as a condition of partnership of E-RIHS, operate a Risk Management Approach for all E-RIHS related activities which is compatible with the principles of the E-RIHS Risk Management Policy and Framework;
3. Risk and the management of risk will be identified and monitored according to E-RIHS' enterprise-wide risk management policy;
4. Risk assessments will be conducted on all new ventures and projects prior to commencement to ensure alignment with E-RIHS' risk appetite and organisational objectives;
5. Risks will be identified, reviewed and monitored on an ongoing basis as outlined in Sections 6 to 10 of the Risk Management Framework;
6. Relevant risks that are identified will be recorded within E-RIHS' Risk Management Database;
7. All risks will be assigned an owner whose responsibilities are specified under section 13 of this policy.

8. RISK MANAGEMENT PRINCIPLES

E-RIHS has adopted the principles detailed in Section 4 of the ISO, to ensure risk management is effective within the organisation. These principles are summarised below:

1. Risk management is the creation and protection of value. It improves performance, encourages innovation and supports the achievement of objectives;
2. Risk management is an integral part of all organisational activities;
3. A structured and comprehensive approach to risk management contributes to consistent and comparable results;
4. The risk management framework and process are customized and proportionate to the organisation's external and internal context related to its objectives;
5. Appropriate and timely involvement of stakeholders enables their knowledge, views and perceptions to be considered. This results in improved awareness and informed risk management;
6. Risks can emerge, change or disappear as an organisation's external and internal context changes;
7. Risk management anticipates, detects, acknowledges and responds to those changes and events in an appropriate and timely manner;
8. The inputs to risk management are based on historical and current information, as well as on future expectations. Risk management explicitly takes into account any limitations and uncertainties associated with such information and expectations. Information should be timely, clear and available to relevant stakeholders;
9. Human behaviour and culture significantly influence all aspects of risk management at each level and stage;

10. Risk management is continually improved through learning and experience.

9. RISK MANAGEMENT PROCESS

E-RIHS' risk management process is based upon the ISO 31000:2018 Risk Management Process as shown in Figure 1 (below). Risks identified will be managed according to this process.

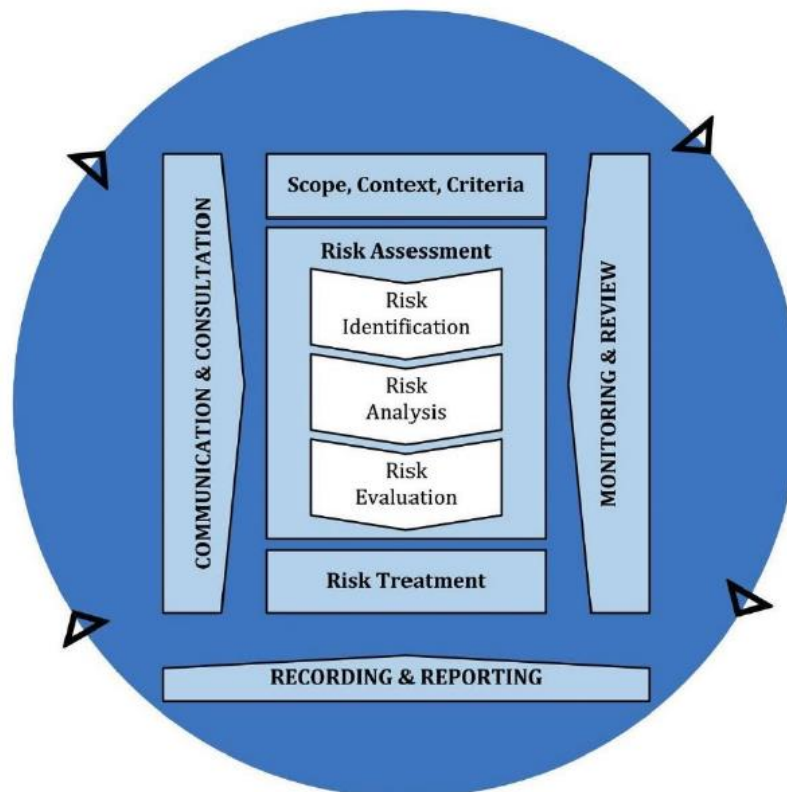


Figure 1 - ISO 31000:2018 Risk Management Process.

10. RISK MANAGEMENT COMPLIANCE AND CONTROL

In developing a culture of risk management, E-RIHS' senior management is responsible for appropriate responses to manage risk, aided by the risk action plans and the creation of a risk register.

To enable this E-RIHS:

1. Has implemented a systematic process to assist in the identification, assessment, treatment and monitoring of risks;
2. Provides the necessary tools and resources to senior management and employees to support the effective management of risks;
3. Reviews and communicates risk management best practice on a regular basis.

11. ASSESSMENT OF EFFECTIVENESS

E-RIHS assesses the effectiveness of its risk management plan through structured continuous improvement processes to ensure risks and controls are continuously monitored and reviewed. This includes an ongoing feedback loop via regular senior management meetings and appraisal of risk owners' actions taken to manage risks via employee performance management.

Where partners have substituted (or wish to substitute) their own Risk Management processes, they are required to perform a self-assessment of those management processes and confirm the outcomes of the self-assessment in writing to the Risk Manager in their National Node. Such a self-assessment must be renewed every three years.

Partner organisations may alternatively place reliance on assessments performed on their behalf as part of any independent or audit review of their governance arrangements provided these are based on a comparison with either Best Practice as contained in ISO 31000:2018 or the E-RIHS

The Risk Management Self-Assessment Questionnaire is provided at Appendix 2 to this document.

12. REPORTING REQUIREMENTS

E-RIHS' senior management via its Director General ensures that the General Assembly is adequately informed of significant risk management issues and the actions undertaken to manage risks on a regular basis. The following reporting process is in place:

1. The Risk Manager will assume overall responsibility for the maintenance and updating of the Risk Management Database, co-ordinating with National Node coordinators and Risk Owners as necessary;
2. Management will regularly review the Risk Management Database with their teams and, where they are the Risk Owner update the mitigation strategies and perceived levels of risk as appropriate;
3. Where they are not the Risk Owner, they will provide any relevant updating information to the Risk Manager and Risk Owner as appropriate;
4. New risks will be added to the database through a formal notification process from staff, management and directors to E-RIHS' Risk Manager, who will brief the Director General as necessary;
5. A "top ten" list of major risks (as agreed by the General Assembly) to be discussed at periodic management meetings (fixed agenda item), together with any new or emerging risks (including escalated risks);
6. The General Assembly will be updated at each meeting through the Director General board report;
7. The General Assembly to be briefed on all major risks by the Director General at each board meeting;
8. Under the facilitation of the Risk Manager, the General Assembly to workshop all risks (with reference to the Risk Database) as well as a general brainstorm/workshop on emerging risks at least once each year, normally as soon as possible after any changes have occurred to General Assembly membership.

13. RISK MANAGEMENT RESPONSIBILITIES

13.1. E-RIHS General Assembly

The General Assembly of E-RIHS is responsible for overseeing the establishment (and implementation via management) of risk management systems and reviewing the effectiveness of these systems.

The General Assembly's role in relation to risk includes:

1. Overseeing the creation, implementation and maintenance of the risk management systems across the entire E-RIHS ERIC and the internal control framework of the Central Hub, including information systems;
2. Establishing a risk profile for the entire E-RIHS ERIC setting out both financial and non-financial material and/or strategic risks facing the E-RIHS ERIC overall;
3. Reviewing the effectiveness of E-RIHS' implementation of its risk management systems and internal controls on an on-going basis and reviewing the outcome of any non-financial audits;
4. Seeking to reach a common understanding with management, partner and sponsoring organisations, auditors and other interested parties about the risk management process, key financial and regulatory risks and related controls including focusing on the "key" risks which are considered to be currently, or may in the future be, more significant or more likely to occur;
5. Analysing the effectiveness of the entire E-RIHS ERIC 's risk management and internal compliance systems and the effectiveness of their implementation;
6. Developing an understanding of the overall business environment, relevant laws and codes of importance to E-RIHS and the programs/projects that E-RIHS has in place to provide reasonable assurance of compliance;
7. Reviewing the E-RIHS' Central Hub's health and safety at work policy and ensuring regular reporting to the General Assembly on issues related to workplace health and safety;
8. Ensuring that the Director General states in writing to the General Assembly annually that the statement given to the General Assembly that E-RIHS Central Hub's financial reports present a true and fair view, in all material respects, of E-RIHS 's financial condition and operational results and are in accordance with the relevant accounting standards, are founded on a sound system of risk management and internal compliance and control which implements the policies adopted by the General Assembly; internal compliance and control which implements the policies adopted by the General Assembly; internal compliance and control which implements the policies adopted by the General Assembly;³

³ 2 Cf International Standard on Auditing – ISA 700 - International Auditing and Assurance Standards Board

9. Ensuring that the Director General states in writing to the General Assembly annually that E-RIHS ERIC's overall risk management and internal compliance and control system is operating efficiently and effectively in all material respects, and/or highlighting any issues which exist within any sub-organisation with the E-RIHS ERIC;
10. Reviewing insurance coverage and claims trends;

13.2. Risk Management Committee (RMC)

The ERIC RMC is comprised of:

1. The E-RIHS General Assembly Chairman (or delegated member);
2. Director General;
3. Risk Manager (note: this may be a role not a full-time post);
4. Head of unit "Administration";
5. Additional legal, technical and insurance expertise is co-opted as required.

It is responsible for:

1. Implementation of the principles, actions and requirements of the risk management plan and monitoring its implementation within the E-RIHS ERIC overall;
2. Provision of the necessary tools and resources to identify and manage risks;
3. Review of risks on a quarterly basis, including identification of new risks, changes to existing risks (including escalations, de-escalations and closures of previously identified risks);
4. The manner in which ownership of risks is taken by senior management or others in accordance with function or expertise;
5. Regular reporting of the status or risk items to the General Assembly;
6. Appraisal of risk owners' actions taken to manage risk and correction of inappropriate performance;
7. Internal compliance and control systems for the implementation of the risk management plan;
8. Consideration of non-financial audits;
9. Compliance with regulatory requirements and best practices;
10. Liaison with RMC's in National Nodes.

13.3. E-RIHS Director General

The Director General is responsible for monitoring the implementation of the E-RIHS Risk Management Framework across the entire organisation.

13.4. E-RIHS Risk Manager (role)

In the current structure of E-RIHS ERIC, this role will be taken by the Head of Unit "Quality and Risk"

1. Identifying legislation, policy and guidelines affecting risk management practices at E-RIHS;

2. Maintaining E-RIHS 's Risk Database and monitoring recorded Risks
3. Promotion of Risk Management throughout the E-RIHS ERIC
4. Defining, developing, disseminating and maintaining Risk Appraisal Techniques
5. Assist the Central Hub Finance Manager with establishing insurance arrangements and managing claims.
6. Providing assistance and support throughout the E-RIHS ERIC for risk management;
7. Providing assistance over decisions to escalate or de-escalate risks;
8. Liaison with Risk Managers in other part of the E-RIHS ERIC;
9. Organising appropriate risk management education and training for E-RIHS staff and staff of partner organisations;
10. Act as external support and assurance to partner organisations undertaking self-assessment of local Risk Management arrangements.

13.5. E-RIHS Central Hub staff

Senior management will be responsible for:

1. Championing the roll out of the E-RIHS Risk Management Framework into the E-RIHS ERIC's operations at the Central Hub;
2. Ensuring staff understand their responsibilities with respect to operational risk management;
3. Developing a risk aware culture within their area of responsibility;
4. Advising the Risk Manager of needs for any training, development and facilitation;
5. Maintenance of entries in the Risk Database relating to their areas.

13.6. Risk Owners

All Risks are allocated a named Risk Owner. Risk Owners throughout the E-RIHS ERIC are responsible for:

1. Identifying existing controls to help manage the risk;
2. Developing treatment plans to reduce the likelihood and/or impact of the risk;
3. Monitoring the implementation of the treatment plans and reporting on their effectiveness and outcomes;
4. In co-operation with Risk Managers, monitoring and alerting senior management of significant changes in risk status.

14. RISK FRAMEWORK

The E-RIHS Risk Framework contains a detailed methodology for the management of risk across E-RIHS. It described how to assess and compare risks using 3 measurement scales (Impact, Probability and Proximity), each of which operates on a 1-5 range of scores in accordance with the methodology detailed in Section 6.5 of the E-RIHS Risk Management Framework.

15. APPETITE FOR RISK

The Risk Management Committee of the E-RIHS ERIC have defined different responses to different levels of Residual Risk after Risk Treatments have been put in place. These reflect the levels of Residual Risk, measured in terms of Probability and Impact but moderated in relation to the Proximity of the Risk.

Three Sets of Responses have been identified and these reflect the E-RIHS ERIC's Risk Appetite.

The actions to be taken in respect of each level of Risk Appetite are shown in Figure 2.

RISK APPETITE FACTOR	ACTION TO BE TAKEN
High	Frequent monitoring by Risk Manager with Risk Owner. Review mitigations to see if these can be strengthened Ensure that Risk is raised with organisation's Management General Assembly at least 1x/month. Consider discontinuation of the activity giving rise to the Risk if additional mitigations cannot be applied. <i>If applicable:</i> Consider escalating Risk up to next tier in organisation hierarchy
Medium	Regular monitoring by Risk Manager with Risk Owner Ensure that Risk is reported to organisation's Management General Assembly regularly
Low	Regular review by Risk Manager with Risk Owner Include details in reports to organisation's Management General Assembly If risk was originally escalated, consider de-escalation

Figure 2 - Actions to be taken at each level of Appetite Risk.

16. RISK MATRICES

The Tables at Appendix 1 show the Risk Appetite Factors to be applied at each level of post-mitigation Probability, Impact and Proximity. The E-RIHS ERIC's Risk Manager will be responsible for liaison with Risk Managers in National Nodes and individual partners of the ERIC.

17. RISK GRADING CRITERIA – IMPACT RATINGS

The General Assembly of E-RIHS has resolved that risk be assessed over the following categories in relation to impact (consequence):

- Financial – impact on E-RIHS finances;
- Operational – impact on provision of E-RIHS products, projects and services;
- Reputational – impact on the professional and scientific reputation of E-RIHS and its partnership overall and on its wider general credibility;

- d) Physical/Safety – impact on the safety and well-being of people;
- e) Regulatory/Legal – impact on E-RIHS of regulatory exposure;
- f) People – impact on corporate knowledge / continuity / professional development and welfare of individuals.

18. MULTIPLE AREAS OF IMPACT

Where multiple impacts are identified, the impact with the highest rating should be used when assessing what Risk Appetite Factor to apply.

For example, where a Financial Impact of ‘Medium’ is identified for a specific Risk, but a Physical Impact of ‘High’ has also been identified, then the rating of ‘High’ should be used when assessing the Risk Appetite consequences.

Impact levels and criteria are shown in the following table:

				Financial	Operational	Brand/ Reputational	Physical/ Safety	Regulatory/ Legal	People/ Participation
IMPACT	5	Very High	A risk that can prove catastrophic or terminal for the part of the organisation where it has arisen or for the wider E-RIHS organisation.	More than 25% of the organisation's annual turnover	Unable to deliver services across E-RIHS. Widespread migration of users to other organisations. Unable to participate in wider scientific community All projects relying on a specific service are delayed or cancelled.	Collapse of entire organisation. Major inquiry into systemic misconduct. Wholesale resignation of General Assembly Members or Senior Management. Total withdrawal of support by EC.	Death or total permanent disability of 1 or more persons due to compromised or badly-defined safety standards. Criminal prosecution by Health and Safety authorities of either a partner organisation or an individual member of staff.	Criminal prosecution of any partner organisation and/or individual General Assembly members due to failure to comply with the law. Sanctions applied by EC / OLAF	Active participating membership overall declines by more than 25% in terms of annual financial value. More than 25% of Central E-RIHS General Assembly Members resign during a 3-month period (except during normal rotation).
	4	High	Risks which can significantly jeopardise some aspects of the organisation, but which will not result in a total organisational failure.	More than 15% but less than 25% of the organisation's annual turnover	Widespread failure or loss of service standards. (Across more than one regional hub coverage area) Increasing migration of partners to other organisations. Reduced participation in wider scientific community. Delays occur in executing more than one project.	Closure of one regional hub Investigation of allegations of serious corporate or individual misconduct. Loss of significant skills from General Assembly or Senior Management. Sustained public or professional criticism of the organisation across more than one region.	Serious injury of 1 or more persons due to compromised or badly-defined safety standards. Criminal investigation by Health and Safety authorities of either a partner organisation or an individual member of staff.	Civil action against any partner organisation and/or individual General Assembly member due to negligence related to E-RIHS. New regulations that impede operations at overall or regional level.	Active participating membership overall declines at least 15%, but less than 25% in terms of annual financial value. More than 25% of one of more Regional Hub General Assembly Members resign during a 3-month period (except during normal rotation).
	3	Medium	Risks which will cause some problems, but which will be confined to one region.	More than 5% but less than 15% of the organisation's annual turnover	Moderate loss of service standards. (Confined to only one regional bug coverage area) Loss of partners within one	Threats of withdrawal from E-RIHS by partners within 1 regional hub. Failure of high-profile or high-	Injury requiring hospital treatment of 1 or more persons due to compromised or badly-defined	Regulatory/ EC / police investigation with adverse findings against any partner organisation	Active participating membership overall declines at least 5%, but less than 15% in terms of annual

				regional hub coverage area). Expressions of discontent by partners/participants in more than one regional hub coverage area. Delays occur in executing a single project.	value project. Failure of a service provider. Allegations of individual or group misconduct. Sustained public or professional criticism of the E-RIHS organisation within one region.	safety standards. Increased frequency of 'reportable' near misses. Published criticism by Health and Safety authorities of either a partner organisation or an individual member of staff.	and/or R-RIHS General Assembly.	financial value. Core Hub HR Dept expresses concern about staff turnover rates and/or recruitment difficulties. Regional Hub HR expresses similar concerns.
2	Low	Any risks which will have just a mild impact, but should be addressed.	More than 1% but less than 5% of the organisation's annual turnover	Minor impact on service delivery. Service users begin to seek alternatives to using E-RIHS. Constrained capacity to meet the demands of existing or new partners/participants. More than 1 proposed project is declined.	Localised negative media coverage. Public or professional criticism of a single participating organisation	Minor injury not requiring hospital treatment but requiring sickness absence from work of 1 of more persons due to compromised or badly-defined safety standards.	Regulatory/police / EC investigation of any partner organisation and/or General Assembly without adverse findings.	Net active participation declines by more than 0%, but less than 5%. Any partner organisation expresses concerns about staff turnover rates and/or recruitment difficulties.
1	Very Low	Risks which do not pose any significant threat and for which specific mitigations beyond normal operational procedures may not be necessary.	Less than less than 1% of the organisation's annual turnover	Very minor, temporary service disruption. 1 proposed project is declined.	Media interest in local issue.	Insignificant injuries of players /participants and/or public.	Persistent complaints against any partner organisation and/or General Assembly.	A temporary staff turnover or recruitment issue is reported at any level within the organisation.

Figure 3 - Criteria for levels of impact within different areas.

19. RISK GRADING CRITERIA – PROBABILITY RATINGS

The General Assembly of E-RIHS has resolved that the following probability thresholds and ratings in relation to assessing risks be used. In order to ensure consistency in the estimation of Probability, measurements are based either on empirical evidence or the results of the operation of simulation exercises.

This policy does not specify what form of simulation might be used. Reliance is placed on the skills and experience of those conducting simulation exercises. The results of such exercises must be accompanied by full documentation of the approach used, assumptions made and any Quality Assurance activities undertaken to validate the simulation.

PROBABILITY	Level	Description	Empirical Evidence	Outcome of Simulations
	5	Very High	Is already occurring somewhere else within E-RIHS despite mitigations in place. Knowledge exists that this risk will occur somewhere else within E-RIHS.	Identified as having a probability of $\geq 80\%$
	4	High	Is already occurring somewhere else within a non-E-RIHS organisation. Knowledge exists that this risk will occur somewhere else within a non-E-RIHS organisation.	Identified as having a probability of $\geq 66\%$ but $< 80\%$
	3	Medium	Has occurred in the past within E-RIHS despite mitigations in place (but is now marked CLOSED)	Identified as having a probability of $\geq 33\%$ but $< 66\%$
	2	Low	Has been identified as a possible risk in a non-E-RIHS organisation	Identified as having a probability of $\geq 10\%$ but $< 33\%$
	1	Very Low	Has been identified as potential Risk during an E-RIHS workshop but is considered purely theoretical	Identified as having a probability of $< 10\%$

Figure 4 - Risk Grading Criteria.

APPENDIX 1 – RISK APPETITE / RESPONSE AT DIFFERENT PROXIMITIES

		PROXIMITY = VERY LOW				
IMPACT	VERY HIGH	MEDIUM	MEDIUM	MEDIUM	HIGH	HIGH
	HIGH	LOW	LOW	MEDIUM	HIGH	HIGH
	MEDIUM	LOW	LOW	LOW	MEDIUM	MEDIUM
	LOW	LOW	LOW	LOW	LOW	MEDIUM
	VERY LOW	LOW	LOW	LOW	LOW	MEDIUM
		VERY LOW	LOW	MEDIUM	HIGH	VERY HIGH
PROBABILITY						

		PROXIMITY = LOW				
IMPACT	VERY HIGH	MEDIUM	MEDIUM	HIGH	HIGH	HIGH
	HIGH	LOW	MEDIUM	MEDIUM	HIGH	HIGH
	MEDIUM	LOW	LOW	MEDIUM	MEDIUM	HIGH
	LOW	LOW	LOW	LOW	MEDIUM	MEDIUM
	VERY LOW	LOW	LOW	LOW	LOW	MEDIUM
		VERY LOW	LOW	MEDIUM	HIGH	VERY HIGH
PROBABILITY						

		PROXIMITY = MEDIUM				
IMPACT	VERY HIGH	MEDIUM	MEDIUM	HIGH	HIGH	HIGH
	HIGH	LOW	MEDIUM	HIGH	HIGH	HIGH
	MEDIUM	LOW	LOW	MEDIUM	HIGH	HIGH
	LOW	LOW	LOW	LOW	MEDIUM	MEDIUM
	VERY LOW	LOW	LOW	LOW	LOW	MEDIUM
		VERY LOW	LOW	MEDIUM	HIGH	VERY HIGH
PROBABILITY						

		PROXIMITY = HIGH				
IMPACT	VERY HIGH	MEDIUM	HIGH	HIGH	HIGH	HIGH
	HIGH	MEDIUM	MEDIUM	HIGH	HIGH	HIGH
	MEDIUM	LOW	MEDIUM	MEDIUM	HIGH	HIGH
	LOW	LOW	LOW	MEDIUM	MEDIUM	HIGH
	VERY LOW	LOW	LOW	LOW	MEDIUM	MEDIUM
		VERY LOW	LOW	MEDIUM	HIGH	VERY HIGH
PROBABILITY						

		PROXIMITY = VERY HIGH				
IMPACT	VERY HIGH	MEDIUM	HIGH	HIGH	HIGH	HIGH
	HIGH	MEDIUM	HIGH	HIGH	HIGH	HIGH
	MEDIUM	MEDIUM	MEDIUM	MEDIUM	HIGH	HIGH
	LOW	LOW	LOW	MEDIUM	MEDIUM	HIGH
	VERY LOW	LOW	LOW	MEDIUM	MEDIUM	MEDIUM
		VERY LOW	LOW	MEDIUM	HIGH	VERY HIGH
PROBABILITY						

Figure 5 - Actions to be taken at each level of appetite risk.

APPENDIX 2 - RISK MANAGEMENT ARRANGEMENTS: PARTNER SELF-ASSESSMENT

The Self-Assessment checklist published overleaf has been imported from a Microsoft Excel Spreadsheet as a graphic copy for information purposes.

Original copies of the Excel Spreadsheet will be available on demand from the E-RIHS Central Hub Risk Manager and will also be downloadable from:

https://URL_to_be_completed_when_E-RISH_ERIC_is_functioning.


 E-RIHS <small>EUROPEAN RESEARCH INFRASTRUCTURE FOR HERITAGE SCIENCE</small>		E-RIHS ORGANISATIONAL RISK MANAGEMENT SELF-ASSESSMENT QUESTIONNAIRE		
Organisation Name		Date of Completion		
Question Reference	Cross - Reference	Question	Answer Yes / No / Partial	Comments
0	N/A	Has your organisation received an independent accreditation for its Risk Management Arrangements during the past 24 months ?		
<p>If the answer to this question is 'Yes', you may discontinue this questionnaire and submit details of the accreditation to the Regional Hub</p> <p>If the answer is 'Partial', you may discontinue this questionnaire. Please provide details of any Action Plan arising from the recommendations of the accreditation to the Regional Hub, together with any progress reports written since.</p>				
1.1	5.2	Does your organisation have formal Risk Management Arrangements which cover the areas of activity in which E-RIHS will be involved.		
1.2	5.2	Are your organisation's Risk Management Arrangements managed and supervised by Senior Management.		
1.3	5.2	Do your Risk Management Arrangements take account of legal and regulatory compliance requirements.		
1.4	5.3	Are your Risk Management Arrangements integrated into other aspects of management (e.g. strategy / planning / finance)		
1.5	5.4.1	Do your Risk Management Arrangements take account of the context of the organisation as part of larger structures		
1.6	5.4.2	Do you consider that Risk Management forms part of the overall culture of the organisation		
1.7	5.4.3	Are named individuals are responsible for Risk Management within the organisations		
1.8	5.4.4	Does your organisation have documented Risk Management procedures		
1.9	5.4.5	Are these Risk Management procedures communicated throughout your organisation		
1.10	5.5	Is there a clear understanding of who makes what decisions regarding the management of Risks within the part of the organisation which will undertake work related to E-RIHS.		
2.1	6.1	Does your organisations's risk management process involve the systematic application of policies, procedures and practices to the activities of communicating and consulting, establishing the context and assessing, treating, monitoring, reviewing, recording and reporting risk.		
2.2	6.2	Does your organisation understand how to communicate information about risks to internal and external stakeholders		
2.3	6.3.4	Does your organisation understand what its Appetite for Risk is in relation to activities which it will perform on work related to E-RIHS		
2.4	6.4.2	Does your organisation know how to identify and document Risks that it encounters		
2.5	6.4.3	Does your organisation have a process to analyse the Probability and Impact of Risks it identifies		
2.6	6.4.3	Does your organisation have a process to identify the Proximity of Risks it identifies		
2.7	6.4.4	Does your organisation have a process to consider how the Risk will relate to its Risk Appetite		
2.8	6.5	Does your organisation have a process to decide how it will Treat the Risks it identifies		
2.9	6.6	Does your organisation have arrangements to regularly monitor and review identified Risks		
2.10	6.7	Does your organisation have an integrated Risk Logging and Reporting system		
Completed by (Name and Position)		Date of Completion		

Figure 6 - Risk Management Self-Assessment Checklist for Partner Organisations.

REFERENCES

ISO31000:2018 (Risk Management – Principles and Guidelines)

<https://www.iso.org/standard/65694.html>

ISO IEC 31010:2009 - Risk management - Risk assessment techniques

<https://www.iso.org/standard/51073.html>

ISO/TR31004:2013 - Risk management — Guidance for the implementation of ISO 31000

<https://www.iso.org/standard/56610.html>

The Management of Risk (M_o_R) – produced by Axelos as part of the Prince2 suite of methodologies ISBN 9780113312740

A Risk Practitioners Guide to ISO 31000: 2018 - Institute of Risk Management

<https://www.theirm.org/media/6907/irm-report-iso-31000-2018-v2.pdf>

EU General Risk Assessment Methodology - Action 5 of Multi-Annual Action Plan for the surveillance of products in the EU (COM(2013)76)

<http://ec.europa.eu/DocsRoom/documents/17107/attachments/1/translations/>

ERIC Practical Guidelines published by the EC Directorate-General for Research and Innovation (ISBN 978-92-79-37861-4)