E-RIHS PP

CALL: H2020-INFRADEV-2016-2

TYPE OF ACTION: CSA

GA n.739503

D2.3 Risk Management Framework

Lead Author: Clive Billenness CISA, University of Brighton, UK

With contributions from:

Professor Janet Anderson – University of Brighton, UK

Jan van 't Hof – Netherlands Cultural Heritage Agency

Marjolijn Weterings – Netherlands Ministry of Education, Culture & Science

Deliverable nature	Report (R)
Dissemination level	Public
Contractual delivery date	31/1/2019
Actual delivery date	31/1/2019
Version	1/2019
Total number of pages	42
Keywords	Risk, Corporate, Governance, Assessment, Mitigation, Opportunity

Abstract

The scope and scale of the Research Infrastructure envisaged in this proposal mean that it is necessary to establish an Enterprise-Wide Risk Management Framework (ERM) to design, implement, monitor and improve risk management consistently and efficiently across all aspects of the RI's activities using quantitative and qualitative measures in a way which is compatible with existing Risk Management arrangements within partner institutions.

This Framework has been created by reference to the Best Practice contained in:

- 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

which has been customised to reflect the specific structures and areas of activity of the Research Infrastructure.

The Framework is designed to be compatible with and capable of integration with existing Risk Management procedures and regulations already in place within partner organisations. It takes account of national Health & Safety Regulations as well as the EU General Data Protection Regulation 2016/679 and any local considerations arising from local Freedom of Information legislation.

The Framework addresses practical Risk Management from the perspectives of the different levels of the hierarchical Research Infrastructure (International, National and Individual) as well as from the perspectives of risks inherent within specific artefacts and defined preservation procedures. The overall objective is to create a consistent approach to risk management which enables all participants to share and learn from others' experience.

The Framework also considers Opportunity Management as the positive aspect of Risk Management.

The hierarchical design of the Framework has been tested with other partners via a dedicated workshop during Year 2 and is based on the author's wide experience of Risk Management Frameworks.

The Framework will now be developed into a full Corporate Risk Management Function (D2.5) as part of the creation of the overall Corporate Governance Function within WP2.

Document information

Project number	739503	**Acronym**	E-RIHS PP
Full title	European Research Infrastructure for Heritage Science – Preparatory Phase		
Project url	www.e-rihs.eu		
Document url			
EU Project Officer	Maria Theofilatou		

Deliverable	**Number**	D.2.3	**Title**	Risk Management Framework
Work Package	**Number**	2	**Title**	Governance

Date of delivery	**Contractual**	M24	**Actual**	
Status	Version 1.0		☐ Draft ☒ Final	
Nature	☐ prototype ☒ report ☐ demonstrator ☐ other			
Dissemination level	☒ Public ☐ restricted			

Authors (Partner)	UCL			
Responsible Author	**Name**	Clive Billenness	**Email**	c.billenness@brighton.ac.uk
	Partner	University of Brighton	**Phone**	+44 (0)208 123 2782

Abstract (for dissemination)	This document describes the hierarchical Corporate Risk Management Framework to be used at all levels of the Research Infrastructure
Keywords	Risk, Management, Framework, Corporate, Governance, Assessment, Mitigation, Opportunity

Version Log			
Issue Date	**Rev. no.**	**Author**	**Change**
31/01/2019	1/2019	Clive Billenness	Initial Published Version

Table of Contents

Table of Figures

Introduction and Principles

1.1. Context

This manual defines the Risk Management methods which shall be used by the 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 Hubs
- The planning of preservation activities in relation to specific items
- The development of preservation 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.

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 organization with regard to risk"
"Risk Management Framework" is defined as a "set of components that provide the foundations and organizational arrangements for designing, implementing, monitoring, reviewing and continually improving risk management throughout the organization"

1.3. Applicability

This manual defines the nature of the overall Risk Management Framework to be adopted by the ERIC and explains how it will relate to, be implemented by and impact on the activities of all Hubs and individual participating organisations, including during collaborative activities.
This manual will be complied with in full by the Central and National Hubs of the ERIC. Individual participating organisations 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 mandatory condition of membership of the ERIC.
Individual participating organisations 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 Hub, 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 preservation actions 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 preservation 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 preservation actions undertaken within the context of the ERIC.

1.5. Commitment to Risk Management

All levels of the 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. External Factors Influencing Risk Management

The ERIC will, at the Central Hub level, operate as an independent, legal entity. As such, it is likely to limit the liabilities of members. It is therefore a requirement within the "ERIC Practical Guidelines" published by the EC Directorate-General for Research and Innovation (ISBN 978-92-79-37861-4) that it will take "appropriate insurance to cover the risks relevant to its activity".
In order to obtain such insurance, it is necessary that the ERIC has in place methodologies to effectively identify, assess and mitigate such risks.
At a Corporate Governance level, there is wide international agreement that overall responsibility for effective risk management lies with the Directors of an organisation.
In the UK, the Companies Act 2006 imposes specific obligations on Directors to ensure that Companies interests are properly protected – which includes an effective Risk Management function. Failure to comply with the provisions of this Act can create a personal liability for financial losses arising from an ineffective approach to Risk Management.
Similar legislation exists in most, if not all, other EU and OECD Member Nations.

For example: Article 2381 of the Italian Civil Code vests with the chief executive officer (under the continuing supervision of the board of directors) the task of ensuring the adequacy of the organisational, administrative and accounting set-up of the corporation.
Similarly, ISO/IEC 17025 "General Requirements For The Competence Of Testing And Calibration Laboratories" – Section 8.5 - Actions to address risks and opportunities specifies that:

> "The laboratory shall consider the risks and opportunities associated with the laboratory activities in order to:
>
> a) give assurance that the management system can achieve its intended results;
>
> b) enhance opportunities to achieve laboratory's purpose objectives;
>
> c) prevent, or reduce, undesired impacts and potential failures in the laboratory activities; and
>
> d) achieve improvement."

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 Hubs will have responsibility for managing compliance with the Risk Manual both within the Hub itself and within participating organisations which operate under the supervision of the Hub.
Individual participating organisations 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:

1. Corporate Risks relating to the ERIC Overall
2. Corporate Risks relating to a National Hub
3. Corporate Risks relating to one or more individual members of the ERIC
4. Risks relating to a specific preservation technique
5. Risks relating to a specific object to be subject to preservation

Each of these is addressed separately in Sections 0 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 Manual 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.

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 the ERIC's principle 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 member organisations.
The ISO describes the Framework as a Management Cycle with the following steps

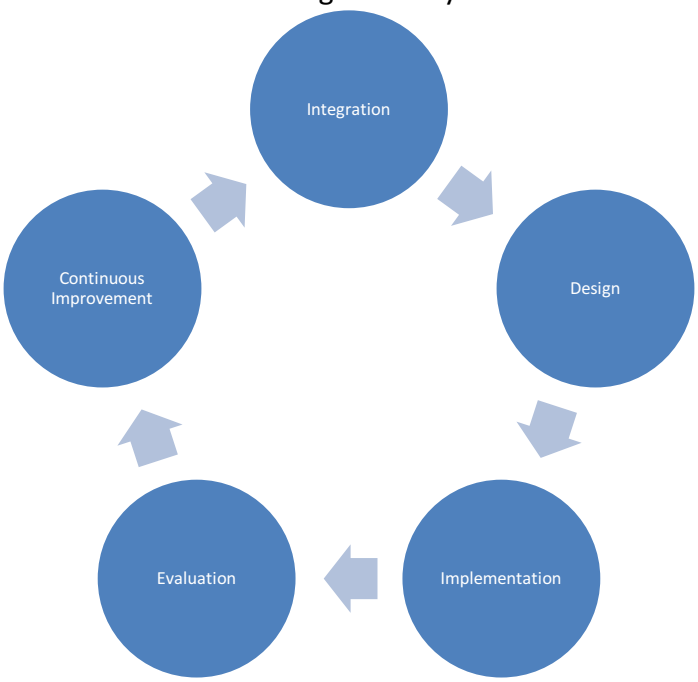

Figure 1 - Overall Risk Management Framework

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 members and also the hierarchical relationships between members, national hubs and the Central Hub. It also permits different contractual and operational relationships between individual organisations and also between individual organisations and hubs to be reflected in the processes.

2.2. 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 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.

2.3. 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 and National Hubs 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.
It is expected that this section will be expanded in the next Project Deliverable as the rest of the organisational structure is defined in more detail and the overall size of the ERIC is quantified.
It should be borne in mind, however, that ongoing training and awareness raising concerning Risk Management within the ERIC will form part of the ERIC's activities.

2.4. Implementation

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

- Identification of levels at which different risk management decisions are to be taken
- Identification of persons to fulfil this responsibility (depending on the management structure(s) adopted for the ERIC).
- 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.

These activities will be undertaken during Year 3 of the Project

2.5. Evaluation

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

Risk Management shall be an automatic agenda item at all meetings of the Governing bodies at Central and National level of the ERIC.

Performance Indicators for measuring the effectiveness of Risk Management will be agreed during Year 3 of the Project.

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 organisations 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 membership application is to be submitted by a prospective member organisation, the person signing the application will be required to certify that they are satisfied with the adequacy of the organisation'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 member 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 membership 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 member's expense, any enquiries it deems fit to ensure that specified improvements have been implemented.

2.6. Continuous Improvement

As an organisation committed to quality and effectiveness, in addition to the review cycle referred to above, all members 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 the organisation.

Levels Of The Framework

3.1. 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 and
- 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 instance 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 membership of the ERIC.

Figure 2 below shows how Risk Management activities are to be performed at different hierarchical levels within the ERIC.

<table>
<tr><th></th><th>Identify</th><th>Own/Manage</th><th>Monitor</th><th>Escalation</th><th>Communication and Consultation</th></tr>
<tr><td>Central Hub</td><td rowspan="3">Any participating organisation may identify any risk at any time. Ownership will be allocated according to the procedures adopted by the National Hub and/or the Central</td><td>Risks relating to the ERIC overall including reputational risks</td><td rowspan="3">All risks owned / managed by the organisation also all risks at any level which are deemed to have an impact on that organisation</td><td rowspan="3"></td><td>Report all risks deemed to have an impact on National Hubs or individual member</td></tr>
<tr><td>National Hub</td><td>Risks relating to the National Implementation of the ERIC including reputational risks</td><td>Notify all risks deemed to have a potential impact at Multi-National Level</td><td>Report all risks deemed to have an impact on one or more individual members</td></tr>
<tr><td>Individual Members</td><td>Risks relating to the Member organisation and to Preservation Actions undertaken by the Member</td><td>Notify all risks deemed to have a potential impact at National level</td><td></td></tr>
</table>

Figure 2 – Hierarchy of Risk Management Activities

3.2. Identification of Risk

It is the responsibility of all participants in the ERIC from individual employee of individual member organisation up to Board Member 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/Hub/Member/Artefact of [zzzzzzzzzzz]"

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 within the organisation 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 XX 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 Register / Knowledgebase 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.

The nature/location(s) of the Risk Register will be agreed during Year 3 of the Project.

3.3. Allocation of Risk Ownership

Upon initial identification, the person with overall responsibility for Risk Management within the organisation 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 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.

3.4. Transfers of Risk Ownership

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

1. The scope of a Risk may change, necessitating an escalation or reduction in level of the ownership.
2. 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. Member Organisations 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.

3.5. Management of Risk

It is the Risk Owner, working in consultation and collaboration with other 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.

3.6. 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.

3.7. 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:

1. Elevated risk of adverse reputational impact on the ERIC at national or international level arising from a risk occurring.
2. Multiple member organisations in one or more countries experiencing the same, or closely associated, risks.
3. Capacity to treat a Risk rising beyond the ability or capacity of the current Risk Owner.
4. Changes in a national or international **P**olitical, **E**conomic, **S**ocial, **T**echnical, **L**egal or **E**nvironmental 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 organisation 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.

3.8. 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.

3.9. 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 member organisations. The new Risk Owner may reserve the right not to assume ownership where this will cause budgetary or resource pressures or conflicts.
FFFigure 3 - Escalation of Risk Ownership below shows a flow diagram for these processes.

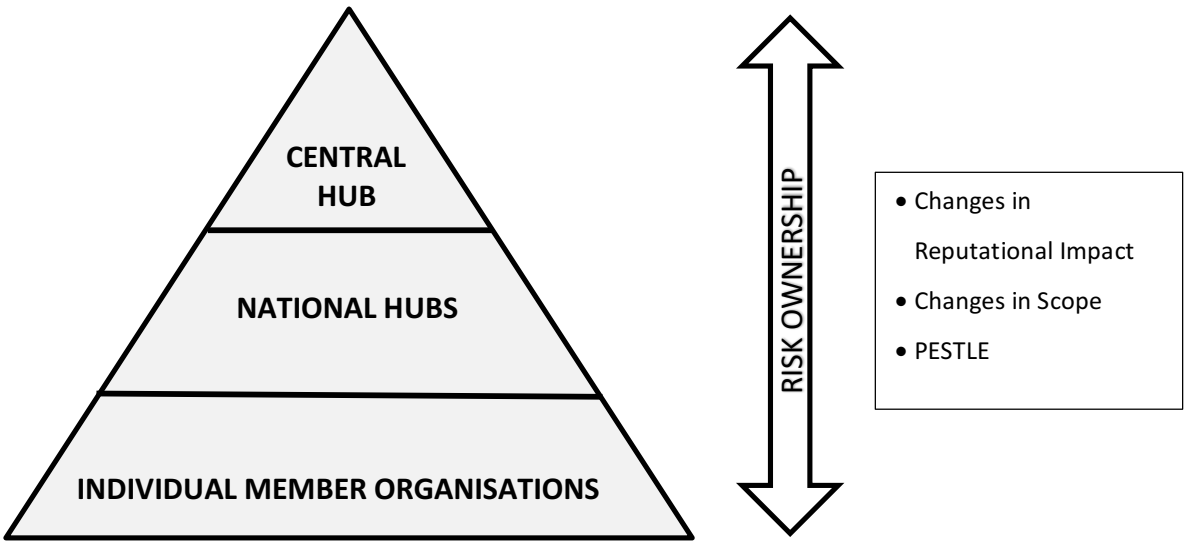

Figure 3 - Escalation of Risk Ownership

Special Governance Considerations for a Multi-Tiered Framework

4.1. 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; and*
> *– develop an appropriate external and internal communication and consultation plan.*
> *Communication and consultation with stakeholders is 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."*

During Year 3 of the Project, the ERIC will define its Risk Management Policy which will include over-riding considerations in relation to Communication and Consultation About Risk.

4.2. 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 3rd Party providers of services to the ERIC, as well as Terms and Conditions of ERIC Membership 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 Register entries. While there are normally exceptions to an obligation to disclose documents, these are not intended to frustrate public accountability and transparency.

Risk Register 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 Register, in part or in full, special considerations arise where such disclosure might reveal sensitive or contractual information about a Third Party or other ERIC member. 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]

4.3. 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 Register 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 Register would have the same obligation to ensure that any personal data contained in the Register was held securely and accurately, and only for as long as necessary.

When preparing a Risk Register 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 Register, 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 Register 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 Register 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 Register Entry, due consideration must be given to avoiding the disclosure of personal data about other individual(s) both within the Member Organisation and elsewhere.

During Year 3 of the Project, as the ERIC develops its policies on Personal Data Protection, this guidance will be expanded on within those documents.

Substitution of Local Risk Management Procedures

5.1. General Principles

While this manual forms the basis of Risk Management Procedures for the ERIC Central and National Hubs, it is recognised that most, if not all, individual member organisations 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 member organisation where existing processes are already sufficient to properly identify, assess, treat and monitor risks associated with membership of the ERIC.

5.2. Assessment of Compliance via Local Procedures

A Checklist will be provided during Year 3 to enable member organisations to compare their internal Risk Management Procedures with those required within the ERIC.

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

All organisations seeking to become members of the ERIC are required to include a statement of compliance, duly certified by the person within the organisation with overall responsibility for Risk Management, before any artefact from another member 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 membership renewal process on the third anniversary of a member joining the ERIC.

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

5.3. Amended Procedures Arising From Compliance

Where Full Compliance has already been achieved or exceeded, Member Organisations 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 Register can be cross-referenced to entries in the Member's Risk Register, and treatment, monitoring and reporting undertaken via that Register.
Where only Partial Compliance has been achieved, Member Organisations 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 Register may refer to the local Risk Register where compliant procedures exist.

The use of a local Register 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 Hub 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.

Management of Risks Relating to the ERIC overall

6.1. 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 membership of the ERIC.
For example: the loss of a central file server containing a knowledgebase of techniques and preservation outcomes owing to a virus infection or a network outage would have the potential to impact every ERIC member 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 member.
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.

6.2. Escalation of Risks to the ERIC Central Hub from National Hubs

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

1. The Impact of the Risk is considered to affect more than one Nation. (For example, changes in European legislation affecting all Members)
2. A National Hub recognises that a Risk that they have identified has also been identified by one or more other National Hubs, 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.
3. The Central Hub notes from its records that a similar or identical Risk has been identified by 2 or more National Hubs.

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 Hubs to provide an overview of the status of the Risk and its Treatments in order to ensure that all Member Organisations 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.

6.3. 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 as well as in the Management of Risk for individual preservation techniques and in relation to the management of preservation for different types of artefact. The following sections should therefore be read by all persons involved in Risk Management within the ERIC.

6.4. Risk Identification

The ISO states:

> "The organization 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 organization, 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:

1. A Facilitated Risk Workshop addressing specific topic areas
2. A Facilitated 'Pre-Mortem' to consider a specific scenario in advance and seek to identify all the reasons why a failure might occur
3. Performance Indicators which show symptoms of potential failures
4. Intelligence obtained from individuals based either on their professional and/or technical knowledge or on incidents observed by them to be occurring elsewhere
5. An alert from another organisation
6. 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/Hub/Member/Artefact of [zzzzzzzzzzz]"

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

6.5. 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 will therefore be 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:

1. Acknowledged experts on the subject under consideration
2. Persons who have experienced similar Risks.
3. Auditors who have already identified and assessed existing controls to determine their effectiveness in managing the Risk under consideration.
4. 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 will 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:

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 x 3 x 2 = 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 x 5 x 4 = 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

6.6. 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 will be contained in the ERIC's Risk Policy and will be deemed a guiding authority in deciding how to respond to any particular Risk.

This Risk Policy will be created during Year 3 of the Project once the governance arrangements are finalised.

It will also be necessary, however, to consider the Appetite for Risk of individual member organisations, National Hubs 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 Member 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:

1. Seek further information about the Risk
2. Tolerate the Risk, and take no further action beyond maintaining existing Controls.
3. 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 governing body of the ERIC.

6.7. 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:

1. Risk **Avoidance.** Either discontinue or do not perform an activity which will give rise to a Risk.
2. Risk **Reduction.** Reduce the Impact or Probability of a Risk occurring by adopting different procedures or increasing controls.
3. 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.
4. **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.
5. **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.
6. **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 WeightingsFigure 4 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:

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

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

Cost of Treatment = €5,000.

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

6.8. 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 Register, 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.

6.9. 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 Member Organisations.

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.

Management of Risks at National Hub Level

7.1. General Considerations

While many of the techniques and procedures described in Section 6.3 et seq above continue to apply at National Hub Level, there are some additional considerations to take into account.
While the National Hub has oversight of all activities by Member Organisations 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 Hub 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 Hub 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 Hub.

This example also raises the question of whether, where multiple National Hubs 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 Hub, the Risk Manager must review the ERIC Risk Log to determine whether an identical or similar Risk already exists and then decide, in consultation with their Hub Management and with the Owner identified for the Risk on the Register, the extent to which the existing, or a similar treatment might be applied to the Risk.

7.2. Escalation of Risks to National Hub from Individual Members

There are a number of situations where a Risk may be escalated to a National Hub from an individual member:

1. The Impact of the Risk is considered to affect more than one Member Organisation. (For example, changes in legislation affecting conditions of service of employees)
2. The Member Organisation recognises that a Risk that they have identified has also been identified by one or more other Member Organisations, 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 Hub (even if it leads to multiple independent Treatment Plans)
3. The National Hub notes from its records that a similar or identical Risk has been identified by 2 or more Member Organisations.

The National Hub shall always have the right to determine if a Risk shall 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 Hub will liaise with the Risk Managers at individual

Member Organisations to provide an overview of the status of the Risk and its Treatments in order to ensure that all Member Organisations are equally well-informed about the Risk.

7.3. De-Escalation of Risks from the National Hub to an Individual Member

There may be occasions when a Risk ceases to impact more than one Member Organisation.
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 Member Organisation 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 Hub may wish to cease to co-ordinate or monitor the Risk Treatment. In such a case, the National Hub may wish to discontinue any central Risk Treatment and return Ownership to the one remaining Member Organisation.

Any wish to De-Escalate a Risk must be indicated to the Member Organisation 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 Hub will provide all reasonable support to the Member Organisation to enable it to assume Ownership.

Where a Member Organisation considers that it lacks the expertise or resources to assume Ownership of a Risk, it may request the National Hub 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 Member Organisation.

Management of Risks at Individual Member Organisation Level

8.1. General Considerations

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

Firstly, as explained at Section 0 above, Member Organisations 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 Register, but permits Risks to be managed in accordance with local arrangements.

Member Organisations must continue to update the ERIC Risk Register as the Treatment of a Risk evolves.

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

8.2. Escalation of Risks to National Hub

See Section 7.2 for details of the circumstances where a Risk may be escalated to the National Hub 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 Member and the Hub.

8.3. De-Escalation of Risks to Individual Member

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

Management of Risks Relating to Specific Objects

9.1. General Considerations

There will be occasions where the treatment of a specific object gives 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 treatment. This will include the entire life-cycle of an object's treatment, from initial transportation, through storage, handling and return. See Section 0 below for the Management of Risks relating to specific treatments.

A Risk Management Planning exercise should always be performed for any object accepted for treatment by the ERIC. It may be that a generic Risk Plan can be applied to the object if the organisation 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 Member Organisation will be responsible and accountable for the safe custody of an object which is entrusted to the ERIC for treatment, it will be one of the strengths of the ERIC that the combined specialist knowledge and experience of the entire membership 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 treatment 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 treatment 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.

9.2. Object Risk Management Planning

When an object/artefact is identified as a candidate for treatment 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 preservation work within the ERIC.

At the initial stage, one consideration will be the risk to the reputation of the ERIC and its members in the event of any damage occurring to the object. Where a Member Organisation 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 membership.

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 lifecyle 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 Organisation 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 Lessons 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.

9.3. Object Risks Knowledgebase

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

Management of Risks Relating to Specific Procedures

10.1. General Considerations

Certain preservation 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, an organisation'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 an organisation 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.

10.2. 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 Organisation 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 Member Organisation and also the equivalent person in any other Organisation 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 organisation'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 Knowledgebase in order to assist any other Member organisation planning to use a similar procedure

10.3. Issues of Proprietary Knowledge in Risk Management

It is acknowledged that in some cases, Member Organisations may be undertaking Procedures which are rendered possible only by the use of proprietary knowledge which will not be shared under the terms of membership 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 Member Organisation, 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 Knowledgebase 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 Member Organisation in the event of an enquiry concerning the redacted information.

Management of Opportunity

11.1. 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.

11.2. 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.

11.3. 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.

11.4. Responses to Opportunity

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

1. **Reject.** The ERIC/Hub/Member 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 a **Opportunity Management Plan** and identify an Opportunity Owner.

11.5. 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 organization with regard to **risk**

risk management framework
set of components that provide the foundations and organizational arrangements for designing, implementing, **monitoring**, reviewing and continually improving **risk management** throughout the organization

risk management policy
statement of the overall intentions and direction of an organization related to **risk management**

risk attitude
organization'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, analyzing, 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 organization seeks to achieve its objectives

internal context
internal environment in which the organization seeks to achieve its objectives

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

stakeholder
person or organization 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)