7.3.1 Organisation Management

Risk Identifier:	R01	
Risk Name:	Management failure	
Risk Description:	One or more aspect of organisational management is unsuccessful, resulting in a failure to deliver an anticipated or required business outcome.	
Is this Risk Relevant?:	• Is organisation subject to central management control?	
Example Risk Manifestation(s):	• Repository management fails to allocate sufficient resources to complete one or more business activities • Management's adopted preservation strategies result in information loss	
Nature of Risk:	Physical environment	
	Personnel, management and administration procedures	X
	Operations and service delivery	
	Hardware, software or communications equipment and facilities	
Owner:	Management	
Escalation Owner:	Management	
Stakeholders:	Management	
Mitigation strategy(ies):	Avoidance strategies: • Conceive comprehensive management policies and procedures and establish mechanisms for their regular review • Establish benchmarks to determine effectiveness of management policies and procedures In the event of risk's execution: • Establish continuity or recovery mechanisms to recover from effects	
Risk Relationships:	←→R02 [contagious]	
Risk Probability:	4	
Risk Potential Impact:	3	
Risk Severity:	12	

Risk Identifier:	R02	
Risk Name:	Loss of trust or reputation	
Risk Description:	One or more stakeholder communities have doubts about the repository's ability to achieve its business objectives.	
Is this Risk Relevant?:	• Does the organisation rely upon its reputation as a business asset? • Does the organisation rely upon its trustworthiness as a business asset? • Has the organisation identified a correlation between its business effectiveness and the reputation and level of trust it enjoys?	
Example Risk Manifestation(s):	• An irrecoverable loss of digital objects provokes community concerns about the repository's competence • A public statement announcing a cut in funding raises concerns that the repository will have insufficient resources to operate effectively	
Nature of Risk:	Physical environment	
	Personnel, management and administration procedures	X
	Operations and service delivery	X
	Hardware, software or communications equipment and facilities	
Owner:	Management	
Escalation Owner:	Management	
Stakeholders:	Management; financiers; staff; depositors; users; producers	
Mitigation strategy(ies):	Avoidance strategies: • Seek all available and relevant certifications to publicly demonstrate the repository's operational effectiveness • Promote organisational transparency to reveal suitability and extent of coverage of policies and procedures • Aim for excellence in pursuit of organisational objectives • Establish outreach mechanisms to reflect where possible expectations of user communities	
Risk Relationships:	←→R01 [contagious]	
Risk Probability:	4	
Risk Potential Impact:	3	
Risk Severity:	12	

Risk Identifier:	R03	
Risk Name:	Activity is overlooked or allocated insufficient resources	
Risk Description:	An integral business activity is mismanaged leading to its non-completion.	
Is this Risk Relevant?:	• Is repository responsible for budgetary development and allocation of resources?	
Example Risk Manifestation(s):	• Repository budgeting does not include a financial allocation for system security maintenance • A 0.5 FTE has sole responsibility to ingest 100 objects per day, although it takes on average 30 minutes for an individual to ingest a single object	
Nature of Risk:	Physical environment	X
	Personnel, management and administration procedures	X
	Operations and service delivery	X
	Hardware, software or communications equipment and facilities	X
Owner:	Management	
Escalation Owner:	Management	
Stakeholders:	Management; financiers; staff; depositors; users; producers	
Mitigation strategy(ies):	Avoidance strategies: • Derive activities, policies and procedures from fundamental repository objectives • Allocate resources to correspond with identified activities • Establish mechanisms to review and adjust resource allocations In the event of risk's execution: • Maintain residual fund to facilitate subsequent resourcing of originally overlooked activity	
Risk Relationships:	→R01 [contagious] →R02 [contagious] →R* [contagious]	
Risk Probability:	4	
Risk Potential Impact:	3	
Risk Severity:	12	

Risk Identifier:	R04	
Risk Name:	Business objectives not met	
Risk Description:	One or more integral business outcomes are not achieved, or are achieved inadequately.	
Is this Risk Relevant?:	• Does repository make a commitment to its stakeholder groups to achieve one or more stated objectives?	
Example Risk Manifestation(s):	• Business commits to delivering object *x* within 5 minutes of its request but on average delivery takes 15 minutes • Repository fails to adequately preserve identified significant properties of ingested materials	
Nature of Risk:	Physical environment	X
	Personnel, management and administration procedures	X
	Operations and service delivery	X
	Hardware, software or communications equipment and facilities	X
Owner:	Management	
Escalation Owner:	Management	
Stakeholders:	Management; financiers; staff; depositors; users; producers	
Mitigation strategy(ies):	Avoidance strategies: • Define activities, policies and procedures with strict reference to corresponding fundamental objectives • Secure and allocate resources based on business priorities • Establish mechanisms to regularly review and, if necessary, adjust policies and procedures in order to ensure objectives are realised In the event of risk's execution: • Undertake appropriate internal enquiries to determine the shortcomings that led to failure and update policies accordingly	
Risk Relationships:	→R01 [contagious] →R02 [contagious]	
Risk Probability:	4	
Risk Potential Impact:	3	
Risk Severity:	12	

Risk Identifier:	R05	
Risk Name:	Repository loses mandate	
Risk Description:	Basis for repository’s existence is withdrawn or substantially altered, rendering it incompatible with business activities.	
Is this Risk Relevant?:	• Is repository's mandate subject to ongoing review? • Is primary repository service contract subject to renewal or renegotiation?	
Example Risk Manifestation(s):	• Scope of repository responsibility is changed by legislative amendment • Repository obligations are altered within contract renegotiations	
Nature of Risk:	Physical environment	
	Personnel, management and administration procedures	X
	Operations and service delivery	
	Hardware, software or communications equipment and facilities	
Owner:	Management	
Escalation Owner:	Management	
Stakeholders:	Management; financiers; staff; depositors; users; producers	
Mitigation strategy(ies):	Avoidance strategies: • Seek all available and relevant certifications to publicly demonstrate the repository’s operational effectiveness • Promote organisational transparency to reveal suitability and extent of coverage of policies and procedures • Aim for excellence in pursuit of organisational objectives In the event of risk’s execution: • Establish arrangements for succession • Establish contingency plans or escrow agreements • Establish exit strategy	
Risk Relationships:	→R08 [contagious] →R01 [contagious] →R02 [contagious] →R* [contagious]	
Risk Probability:	4	
Risk Potential Impact:	3	
Risk Severity:	12	

Risk Identifier:	R06	
Risk Name:	Community requirements change substantially	
Risk Description:	Community expectations or requirements are substantially altered, and no longer correspond to business activities.	
Is this Risk Relevant?:	• Have user requirements been subject to change in the past? • Has the repository or have other external, comparable repositories experienced a change or evolution in the communities using or depositing content?	
Example Risk Manifestation(s):	• User community adopts new software systems which provide no support for legacy data formats that were previously dominant • Community becomes increasingly unfamiliar with the semantics of a previously well-known and widely employed scientific markup language	
Nature of Risk:	Physical environment	
	Personnel, management and administration procedures	
	Operations and service delivery	X
	Hardware, software or communications equipment and facilities	
Owner:	Management	
Escalation Owner:	Management	
Stakeholders:	Management; financiers; staff; depositors; users; producers	
Mitigation strategy(ies):	Avoidance strategies: • Monitor requirements, expectations and knowledge base of user community • Document and review organisational definition of understandability for each distinct user community In the event of risk's execution: • Maintain flexible approach to operational objectives to react to emerging community requirements	
Risk Relationships:	→R01 [contagious] →R02 [contagious] →R11 [contagious] →R67 [contagious] →R74 [contagious]	
Risk Probability:	4	
Risk Potential Impact:	3	
Risk Severity:	12	

Risk Identifier:	R07	
Risk Name:	Community requirements misunderstood or miscommunicated	
Risk Description:	Repository is incapable of determining the expectations of its stakeholder communities and therefore unable to tailor business activities appropriately.	
Is this Risk Relevant?:	• Does the repository have mechanisms established to monitor the community's knowledge base, requirements or expectations? • Are community members consulted about the adequacy of available service levels?	
Example Risk Manifestation(s):	• Repository fails to identify that its user communities require data to be delivered encoded as *.abc* files in order for them to be usable	
Nature of Risk:	Physical environment	
	Personnel, management and administration procedures	
	Operations and service delivery	X
	Hardware, software or communications equipment and facilities	
Owner:	Management	
Escalation Owner:	Management	
Stakeholders:	Management; financiers; staff; depositors; users; producers	
Mitigation strategy(ies):	Avoidance strategies: • Establish appropriate technical mechanisms to facilitate monitoring of requirements, expectations and knowledge base of user community In the event of risk's execution: • Maintain dialogue with community to ensure the continued correctness of understandability definition • Maintain flexibility within operational objectives to react to misunderstanding of requirements	
Risk Relationships:	→R01 [contagious] →R02 [contagious] →R11 [contagious] →R67 [contagious] →R74 [contagious]	
Risk Probability:	4	
Risk Potential Impact:	3	
Risk Severity:	12	

Risk Identifier:	R08	
Risk Name:	Enforced cessation of repository operations	
Risk Description:	Repository is forced to cease its business activities.	
Is this Risk Relevant?:	• Does the mechanism responsible for the repository's establishment include a stated and finite period for its existence before renewal measures must be undertaken? • Are mechanisms available to counterbalance periods of financial loss or constraint? • Are significant aspects of business activities susceptible to legal challenge? • Is there evidence to suggest that the scale of the repository's user community is diminishing over time?	
Example Risk Manifestation(s):	• Repository's responsibilities are withdrawn by legislative amendment • Repository fails secure renewal of its preservation contract with its primary client and/or funder • Repository goes bankrupt or is no longer financially sustainable • Repository loses its place in a competitive marketplace	
Nature of Risk:	Physical environment	
	Personnel, management and administration procedures	
	Operations and service delivery	X
	Hardware, software or communications equipment and facilities	
Owner:	Management	
Escalation Owner:	Management	
Stakeholders:	Management; financiers; staff; depositors; users; producers	
Mitigation strategy(ies):	Avoidance strategies: • Seek all available and relevant certifications to demonstrate publicly the repository's operational effectiveness • Promote organisational transparency to reveal suitability and extent of coverage of policies and procedures • Aim for excellence in pursuit of organisational objectives In the event of risk's execution: • Establish arrangements for succession • Establish contingency plans or escrow agreements • Establish exit strategy	
Risk Relationships:	→R01 [contagious] →R02 [contagious]	
Risk Probability:	4	
Risk Potential Impact:	3	
Risk Severity:	12	

Risk Identifier:	R09	
Risk Name:	Community feedback not received	
Risk Description:	Repository fails to solicit responses from the community regarding its level of service, or fails to provide mechanisms for this.	
Is this Risk Relevant?:	• Does repository have mechanisms available to solicit feedback from community members? • Is a proportion of staff time allocated to the gathering or receipt of community feedback? • Are feedback mechanisms regularly tested to ensure they are functioning correctly?	
Example Risk Manifestation(s):	• Repository fails to identify that its user communities are increasingly incapable of using data encoded within the repository's chosen formats with the software that they principally employ	
Nature of Risk:	Physical environment	
	Personnel, management and administration procedures	
	Operations and service delivery	X
	Hardware, software or communications equipment and facilities	X
Owner:	Management	
Escalation Owner:	Management	
Stakeholders:	Management; financiers; staff; depositors; users; producers	
Mitigation strategy(ies):	Avoidance strategies: • Maintain appropriate mechanisms for community to provide feedback, such as email, web-forms, telephone helpdesk and mail address • Actively solicit feedback, allocating a proportion of staff time to community engagement In the event of risk's execution: • Identify reasons for communication failure and update policies and procedures accordingly	
Risk Relationships:	→R01 [contagious] →R02 [contagious] →R10 [contagious]	
Risk Probability:	4	
Risk Potential Impact:	3	
Risk Severity:	12	

Risk Identifier:	R10	
Risk Name:	Community feedback not acted upon	
Risk Description:	Although feedback is received, it has no influence over repository's business activities.	
Is this Risk Relevant?:	• Is a proportion of staff time allocated to responding to community feedback, or reflecting it in changes to operational objectives? • Are policies and procedures in place to enable the repository to react within an appropriately timely fashion to the receipt of community feedback? • Are operational objectives adaptable to react to community feedback?	
Example Risk Manifestation(s):	• Repository fails to react to the fact that its user communities are increasingly incapable of using data encoded within the repository's chosen formats with the software that they principally employ	
Nature of Risk:	Physical environment	
	Personnel, management and administration procedures	
	Operations and service delivery	X
	Hardware, software or communications equipment and facilities	
Owner:	Management	
Escalation Owner:	Management	
Stakeholders:	Management; financiers; staff; depositors; users; producers	
Mitigation strategy(ies):	Avoidance strategies: • Establish policies to acknowledge and react to community feedback In the event of risk's execution: • Acknowledge failure to act with community and retrospectively react to received feedback	
Risk Relationships:	→R01 [contagious] →R02 [contagious] →R11 [contagious] →R67 [contagious] →R74 [contagious]	
Risk Probability:	4	
Risk Potential Impact:	3	
Risk Severity:	12	

Risk Identifier:	R11	
Risk Name:	Business fails to preserve essential characteristics of digital information	
Risk Description:	Repository's preservation activities are insufficient to maintain the properties of its digital holdings that are of greatest significance to its user communities	
Is this Risk Relevant?:	• Are significant properties defined and documented for each class of object preserved within the repository? • Are members of the community consulted throughout the process of defining significant properties? • Are preservation policies and procedures sufficient to maintain defined properties?	
Example Risk Manifestation(s):	• Repository preserves transcribed text from digitised manuscripts within *.txt* files, although user communities are interested in looking at the original illuminations in subsequent research • Repository aims to preserve images of manuscript illuminations but chosen resolution is insufficient to display the level of detail required by user community	
Nature of Risk:	Physical environment	
	Personnel, management and administration procedures	
	Operations and service delivery	X
	Hardware, software or communications equipment and facilities	
Owner:	Management	
Escalation Owner:	Management	
Stakeholders:	Management; financiers; staff; depositors; users; producers	
Mitigation strategy(ies):	Avoidance strategies: • Document significant properties of digital objects that will be maintained, based on community expectations and requirements In the event of risk's execution: • Acknowledge organisational shortcoming and revise policies and significant properties definition accordingly	
Risk Relationships:	→R01 [contagious] →R02 [contagious] →R04 [contagious] →R67 [contagious] →R74 [contagious]	
Risk Probability:	4	
Risk Potential Impact:	3	
Risk Severity:	12	

Risk Identifier:	R12	
Risk Name:	Business policies and procedures are unknown	
Risk Description:	Fundamentals of why and how repository's business activities are conducted are undocumented and unknown, or known only by specific individuals.	
Is this Risk Relevant?:	• Are policies and procedures comprehensively documented? • Is documentation widely accessible and understandable throughout the organisation? • Is the location of policy and procedure documentation recorded and well known?	
Example Risk Manifestation(s):	• Policies and procedures associated with each organisational facet are known only to the individuals responsible • Policies are documented in Microsoft Word files but stored only on an unshared partition of a workstation hard-disk	
Nature of Risk:	Physical environment	
	Personnel, management and administration procedures	
	Operations and service delivery	X
	Hardware, software or communications equipment and facilities	
Owner:	Management	
Escalation Owner:	Management	
Stakeholders:	Management; financiers; staff; depositors; users; producers	
Mitigation strategy(ies):	Avoidance strategies: • Conceive and document comprehensive policies and procedures • Circulate documentation among repository staff and create multiple copies in alternative locations • Circulate details of documentation locations	
Risk Relationships:	→R01 [contagious] →R02 [contagious] →R04 [contagious] →R19 [contagious] →R* [contagious]	
Risk Probability:	4	
Risk Potential Impact:	3	
Risk Severity:	12	

Risk Identifier:	R13	
Risk Name:	Business policies and procedures are inefficient	
Risk Description:	Rationale and/or practical approach adopted for business fail to demonstrate optimal efficiency.	
Is this Risk Relevant?:	• Do measurable aspects of performance compare favourably with those of similar organisations? • How does the repository's current operational efficiency compare with its peak level?	
Example Risk Manifestation(s):	• Repository makes objects available one hour after a dissemination request, but comparable organisations providing similar content are capable of doing so in just 30 minutes • Revised policies are demonstrably less efficient than those that preceded	
Nature of Risk:	Physical environment	
	Personnel, management and administration procedures	
	Operations and service delivery	X
	Hardware, software or communications equipment and facilities	
Owner:	Management	
Escalation Owner:	Management	
Stakeholders:	Management; financiers; staff; depositors; users; producers	
Mitigation strategy(ies):	Avoidance strategies: • Expose policies and procedures to regular review to determine their efficiency and appropriateness with respect to organisational goals • Seek external validation of policies and procedures (e.g. accredited auditors or user communities) In the event of risk's execution: • Identify those policies that are inefficient and revise them accordingly	
Risk Relationships:	→R01 [contagious] →R02 [contagious] →R* [contagious]	
Risk Probability:	4	
Risk Potential Impact:	3	
Risk Severity:	12	

Risk Identifier:	R14	
Risk Name:	Business policies and procedures are inconsistent or contradictory	
Risk Description:	Rationale and/or practical approach adopted for particular business objectives introduce obstacles to the successful completion of other business activities.	
Is this Risk Relevant?:	• Are business policies and procedures conceived with consideration of the operations of the repository as a whole? • Are mechanisms in place to resolve conflicting policies and/or procedures?	
Example Risk Manifestation(s):	• Repository requires staff to undertake quality assurance procedures for each object ingested, which takes on average 10 minutes, although an additional policy states that ingest should be completed in 10 minutes	
Nature of Risk:	Physical environment	
	Personnel, management and administration procedures	
	Operations and service delivery	X
	Hardware, software or communications equipment and facilities	
Owner:	Management	
Escalation Owner:	Management	
Stakeholders:	Management; financiers; staff; depositors; users; producers	
Mitigation strategy(ies):	Avoidance strategies: • Expose policies and procedures to regular review to determine their consistency with respect to organisational goals • Seek external validation of policies and procedures (e.g. accredited auditors or user communities) In the event of risk's execution: • Identify those policies that are inconsistent and revise them accordingly	
Risk Relationships:	→R01 [contagious] →R02 [contagious] →R* [contagious]	
Risk Probability:	4	
Risk Potential Impact:	3	
Risk Severity:	12	

Risk Identifier:	R15	
Risk Name:	Legal liability for IPR infringement	
Risk Description:	Repository is legally accountable for a breach of copyright, patent infringement or other IPR-related misdemeanour as a direct result of its business activities.	
Is this Risk Relevant?:	• Does the repository deal with content with specific associated intellectual property rights? • Does the repository consult with legal experts when determining the legality of their activities with respect to IPR restricted content? • Is there evidence of a high degree of litigiousness within the domain or jurisdiction within which the repository operates?	
Example Risk Manifestation(s):	• As part of its preservation activities, the repository reverse engineers a software application, and in doing so contravenes a condition of its end user license agreement • An institutional repository disseminates e-journal content, and in doing so is guilty of copyright breach	
Nature of Risk:	Physical environment	
	Personnel, management and administration procedures	X
	Operations and service delivery	
	Hardware, software or communications equipment and facilities	
Owner:	Legal	
Escalation Owner:	Legal	
Stakeholders:	Management; financiers; staff; depositors; users; producers	
Mitigation strategy(ies):	Avoidance strategies: • Assess preserved materials to determine those to which intellectual property restrictions may apply • Seek legal advice to determine legality of activities with respect to IPR restricted content In the event of risk's execution: • Establish policies and procedures to follow in the event of IPR challenge	
Risk Relationships:	→R01 [contagious] →R02 [contagious] →R04 [contagious] →R14 [contagious]	
Risk Probability:	4	
Risk Potential Impact:	3	
Risk Severity:	12	

Risk Identifier:	R16	
Risk Name:	Legal liability for breach of contractual responsibilities	
Risk Description:	Repository is legally accountable for either failing to fulfil responsibilities or acting beyond the scope of what is permissible, as detailed in stakeholder contracts.	
Is this Risk Relevant?:	• Does the repository engage in contractual relationships? • Does the repository consult with legal experts when determining the legality of their activities with respect to enforceable contracts that they are party to? • Is there evidence of a high degree of litigiousness within the domain or jurisdiction within which the repository operates?	
Example Risk Manifestation(s):	• Repository disseminates preserved content over the public Internet without restriction, although the corresponding deposit agreement stated that only a limited community should have access	
Nature of Risk:	Physical environment	
	Personnel, management and administration procedures	X
	Operations and service delivery	
	Hardware, software or communications equipment and facilities	
Owner:	Legal	
Escalation Owner:	Legal	
Stakeholders:	Management; financiers; staff; depositors; users; producers	
Mitigation strategy(ies):	Avoidance strategies: • Monitor contracts and ensure that implemented policies correspond to their terms • Seek legal advice to determine legality of activities with respect to IPR restricted content In the event of risk's execution: • Establish policies and procedures to follow in the event of contractual challenge	
Risk Relationships:	→R01 [contagious] →R02 [contagious] →R04 [contagious] →R14 [contagious]	
Risk Probability:	4	
Risk Potential Impact:	3	
Risk Severity:	12	

Risk Identifier:	R17	
Risk Name:	Legal liability for breach of legislative requirements	
Risk Description:	Repository is legally accountable for either failing to fulfil responsibilities or acting beyond the scope of what is permissible, as detailed in legislative instruments.	
Is this Risk Relevant?:	• Is the repository established within legislation? • Do any other legislative acts or statutory instruments establish restrictions or obligations related to repository activities? • Does the repository consult with legal experts when determining the legality of their activities with respect to relevant legislation? • Is there evidence of a high degree of litigiousness within the domain or jurisdiction within which the repository operates?	
Example Risk Manifestation(s):	• Repository fails to accept deposited materials in contravention of legal deposit laws established in local legislation	
Nature of Risk:	Physical environment	
	Personnel, management and administration procedures	X
	Operations and service delivery	
	Hardware, software or communications equipment and facilities	
Owner:	Legal	
Escalation Owner:	Legal	
Stakeholders:	Management; financiers; staff; depositors; users; producers	
Mitigation strategy(ies):	Avoidance strategies: • Monitor legislation in order to ensure that policies and procedures correspond to intrinsic requirements and prohibitions • Seek legal advice to determine legality of activities with respect to legislation In the event of risk's execution: • Establish policies and procedures to follow in the event of legislative challenge	
Risk Relationships:	→R01 [contagious] →R02 [contagious] →R04 [contagious] →R14 [contagious]	
Risk Probability:	4	
Risk Potential Impact:	3	
Risk Severity:	12	

Risk Identifier:	R18	
Risk Name:	Liability for regulatory non-compliance	
Risk Description:	Repository is liable for failure to conduct its activities in accordance with industrial, business oriented or global regulation.	
Is this Risk Relevant?:	• Do any regulations establish restrictions or obligations related to repository activities? • Does the repository consult with legal experts when determining the legality of their activities with respect to relevant regulations? • Is there evidence of a high degree of litigiousness within the domain or jurisdiction within which the repository operates?	
Example Risk Manifestation(s):	• Repository fails to conform to appropriate jurisdictional health and safety regulations for employees	
Nature of Risk:	Physical environment	
	Personnel, management and administration procedures	
	Operations and service delivery	X
	Hardware, software or communications equipment and facilities	
Owner:	Legal	
Escalation Owner:	Legal	
Stakeholders:	Management; financiers; staff; depositors; users; producers	
Mitigation strategy(ies):	Avoidance strategies: • Monitor regulatory framework and ensure policies and procedures correspond to their requirements and prohibitions • Seek legal advice to determine legality of activities with respect to regulatory framework In the event of risk's execution: • Establish policies and procedures to follow in the event of IPR challenge	
Risk Relationships:	→R01 [contagious] →R02 [contagious] →R04 [contagious] →R14 [contagious]]	
Risk Probability:	4	
Risk Potential Impact:	3	
Risk Severity:	12	

Risk Identifier:	R19	
Risk Name:	Inability to evaluate repository's successfulness	
Risk Description:	Repository is incapable of effectively determining the extent to which it has successfully achieved its business objectives.	
Is this Risk Relevant?:	• Does the repository maintain policies and procedures to verify and record the integrity, authenticity, provenance and understandability of archived information? • Does the repository maintain policies and procedures to evaluate and record the execution of repository processes and to check that their outputs are complete and correct? • Does the repository engage with user communities to determine their overall level of satisfaction? • Are mechanisms to determine the effectiveness of repository operations exploited on a regular basis?	
Example Risk Manifestation(s):	• Repository has no way of demonstrating that the integrity and authenticity of its archived materials have been maintained • Repository cannot demonstrate that submitted information has been ingested correctly and transformed into a corresponding complete and correct archival package	
Nature of Risk:	Physical environment	
	Personnel, management and administration procedures	X
	Operations and service delivery	
	Hardware, software or communications equipment and facilities	
Owner:	Management	
Escalation Owner:	Management	
Stakeholders:	Management; financiers; staff; depositors; users; producers	
Mitigation strategy(ies):	Avoidance strategies: • Establish internal means of assessment including risk management • Seek relevant external certification in order to demonstrate competence	
Risk Relationships:	→R01 [contagious] →R02 [contagious]	
Risk Probability:	4	
Risk Potential Impact:	3	
Risk Severity:	12	

Risk Identifier:	R20	
Risk Name:	False perception of the extent of repository's success	
Risk Description:	Repository’s assessments of success are flawed and indicate a level of performance inconsistent with reality.	
Is this Risk Relevant?:	• Do the repository's various efforts to determine effectiveness result in inconsistent results? • Do repository's evaluation mechanisms offer comprehensive and reliable coverage?	
Example Risk Manifestation(s):	• Based on flawed end-user survey evidence solicited from just a small subsection of its user community, the repository is satisfied that its efforts are successful, although mechanisms in place are actually insufficient to maintain the understandability, integrity and authenticity of archived information	
Nature of Risk:	Physical environment	
	Personnel, management and administration procedures	X
	Operations and service delivery	
	Hardware, software or communications equipment and facilities	
Owner:	Management	
Escalation Owner:	Management	
Stakeholders:	Management; financiers; staff; depositors; users; producers	
Mitigation strategy(ies):	Avoidance strategies: • Establish internal means of assessment including risk management • Seek relevant external certification in order to demonstrate competence	
Risk Relationships:	→R01 [contagious] →R02 [contagious] →R19 [contagious]	
Risk Probability:	4	
Risk Potential Impact:	3	
Risk Severity:	12	

7.3.2 Staffing

Risk Identifier:	R21	
Risk Name:	Loss of key member(s) of staff	
Risk Description:	Individuals with roles, responsibilities or aptitudes vital to the achievement of business objectives part company with the repository, rendering the achievement of those objectives less straightforward.	
Is this Risk Relevant?:	• Has the repository experienced significant staff turnover? • Is the status, expertise or knowledge of any individual staff member such that their loss would be of considerable detriment to the organisation's business objectives?	
Example Risk Manifestation(s):	• Repository's head systems' administrator, the sole individual with knowledge of the system's root password, leaves the organisation to work within an alternative industry	
Nature of Risk:	Physical environment	
	Personnel, management and administration procedures	X
	Operations and service delivery	
	Hardware, software or communications equipment and facilities	
Owner:	Personnel	
Escalation Owner:	Personnel	
Stakeholders:	Management; financiers; staff; depositors; users; producers	
Mitigation strategy(ies):	Avoidance strategies: • Offer favourable terms and conditions for staff In the event of risk's execution: • Promote sharing of organisational responsibilities and duplication of skills in order to limit the impact of losing individual members of staff • Ensure policies and procedures are widely circulated and not known only to selected individuals	
Risk Relationships:	→R01 [contagious] →R02 [contagious] →R12 [contagious] →R* [contagious]	
Risk Probability:	4	
Risk Potential Impact:	3	
Risk Severity:	12	

Risk Identifier:	R22	
Risk Name:	Staff suffer deterioration of skills	
Risk Description:	Staff members demonstrate a diminishing level of skills over time.	
Is this Risk Relevant?:	• Are staff members required to possess skills that are practically employed only on an infrequent basis? • Are skills refreshment opportunities available to staff?	
Example Risk Manifestation(s):	• Repository technical staff are rarely required to recover content from backups, and consequently suffer a deterioration of the appropriate skills to use backup retrieval mechanism	
Nature of Risk:	Physical environment	
	Personnel, management and administration procedures	X
	Operations and service delivery	
	Hardware, software or communications equipment and facilities	
Owner:	Personnel	
Escalation Owner:	Personnel	
Stakeholders:	Management; financiers; staff; depositors; users; producers	
Mitigation strategy(ies):	Avoidance strategies: • Establish means for staff skills refreshment, and for staff to employ skills of limited frequent value in test environment • Implement staff performance reviews to regularly determine skill levels and training requirements In the event of risk's execution: • Provide training facilities to reverse skills haemorrhage	
Risk Relationships:	→R01 [contagious] →R02 [contagious] →R* [contagious]	
Risk Probability:	4	
Risk Potential Impact:	3	
Risk Severity:	12	

Risk Identifier:	R23	
Risk Name:	Staff skills become obsolete	
Risk Description:	Staff members' skills stagnate and are no longer current.	
Is this Risk Relevant?:	• Does the repository's natural development presuppose that staff will develop new skills and abilities over time? • Are training and professional development opportunities made available to staff? • Are staff members required to identify and pursue appropriate training activities?	
Example Risk Manifestation(s):	• Staff are only capable of employing dated preservation strategies and are not trained in or exposed to emerging techniques or technologies	
Nature of Risk:	Physical environment	
	Personnel, management and administration procedures	X
	Operations and service delivery	
	Hardware, software or communications equipment and facilities	
Owner:	Personnel	
Escalation Owner:	Personnel	
Stakeholders:	Management; financiers; staff; depositors; users; producers	
Mitigation strategy(ies):	Avoidance strategies: • Establish means for staff training, and for staff to employ skills of limited frequent value in test environment • Implement staff performance reviews to regularly determine skill levels and training requirements In the event of risk's execution: • Provide training facilities to reverse obsolescence of skills	
Risk Relationships:	→R01 [contagious] →R02 [contagious] →R* [contagious]	
Risk Probability:	4	
Risk Potential Impact:	3	
Risk Severity:	12	

Risk Identifier:	R24	
Risk Name:	Inability to evaluate staff effectiveness or suitability	
Risk Description:	Repository is incapable of effectively determining the extent to which staff are capable of achieving business objectives.	
Is this Risk Relevant?:	• Does the repository maintain policies and procedures to review staff performance?	
Example Risk Manifestation(s):	• Repository has no record of performance levels of individuals within its staff or means to effectively identify training requirements	
Nature of Risk:	Physical environment	
	Personnel, management and administration procedures	X
	Operations and service delivery	
	Hardware, software or communications equipment and facilities	
Owner:	Management	
Escalation Owner:	Management	
Stakeholders:	Management; financiers; staff; depositors; users; producers	
Mitigation strategy(ies):	Avoidance strategies: • Establish internal means of assessment including risk management • Seek relevant external certification in order to demonstrate staff competence • Undertake regular staff development reviews	
Risk Relationships:	→R01 [contagious] →R02 [contagious] →R19 [contagious]	
Risk Probability:	4	
Risk Potential Impact:	3	
Risk Severity:	12	

7.3.3 Financial Management

Risk Identifier:	R25	
Risk Name:	Finances insufficient to meet repository commitments	
Risk Description:	Finances are insufficient to adequately resource each of the business's integral activities.	
Is this Risk Relevant?:	• Does the repository undertake budgetary management? • Is financial investment necessary to achieve repository objectives? • Within its current business model, is the repository capable of self-sustainable income generation?	
Example Risk Manifestation(s):	• Repository operating on an annual loss • Insufficient resource to facilitate every intrinsic activity	
Nature of Risk:	Physical environment	
	Personnel, management and administration procedures	X
	Operations and service delivery	
	Hardware, software or communications equipment and facilities	
Owner:	Budgeting	
Escalation Owner:	Budgeting	
Stakeholders:	Management; financiers; staff; depositors; users; producers	
Mitigation strategy(ies):	Avoidance strategies: • Develop self-sustainability with charged-for services • Seek assurances of level of budget In the event of risk's execution: • Solicit additional funding to enable achievement of organisational objectives • Revise objectives if funding stream is insufficiently flexible • Maintain contingency fund where possible to meet shortfalls	
Risk Relationships:	→R01 [contagious] →R02 [contagious] →R* [contagious]	
Risk Probability:	4	
Risk Potential Impact:	3	
Risk Severity:	12	

Risk Identifier:	R26	
Risk Name:	Misallocation of finances	
Risk Description:	Repository allocates resources ill-advisedly, representing a poor investment, with benefits not proportional to expenditure.	
Is this Risk Relevant?:	• Is budgetary management and expenditure within the responsibilities of the repository?	
Example Risk Manifestation(s):	• Management invest heavily in software that offers functionality far in excess of operational requirements, when cheaper alternatives with limited, but adequate features are available	
Nature of Risk:	Physical environment	
	Personnel, management and administration procedures	X
	Operations and service delivery	
	Hardware, software or communications equipment and facilities	
Owner:	Budgeting	
Escalation Owner:	Budgeting	
Stakeholders:	Management; financiers; staff; depositors; users; producers	
Mitigation strategy(ies):	Avoidance strategies: • Establish policies and budgetary authorisation infrastructure to ensure appropriate use of repository funding In the event of risk's execution: • Revise policies to limit likelihood of subsequent misallocation	
Risk Relationships:	→R01 [contagious] →R02 [contagious] →R25 [contagious]	
Risk Probability:	4	
Risk Potential Impact:	3	
Risk Severity:	12	

Risk Identifier:	R27	
Risk Name:	Liability for non-adherence to financial law or regulations	
Risk Description:	Repository is liable for failing to fulfil its responsibilities with respect to jurisdictional financial responsibilities.	
Is this Risk Relevant?:	• Is the repository subject to regulation that compels it to manage financial records in a particular fashion? • Does the repository solicit the advice of appropriate experts in order to fulfil its financial and accounting responsibilities?	
Example Risk Manifestation(s):	• Failure to address taxation requirements • Failure to conduct compulsory financial auditing	
Nature of Risk:	Physical environment	
	Personnel, management and administration procedures	X
	Operations and service delivery	
	Hardware, software or communications equipment and facilities	
Owner:	Budgeting	
Escalation Owner:	Budgeting	
Stakeholders:	Management; financiers; staff; depositors; users; producers	
Mitigation strategy(ies):	Avoidance strategies: • Monitor financial legislation and regulations in order to ensure that policies and procedures correspond to intrinsic requirements and prohibitions • Seek legal and professional financial advice to ensure adequate fulfilment of responsibilities In the event of risk's execution: • Establish policies and procedures to follow in the event of legislative challenge	
Risk Relationships:	→R01 [contagious] →R02 [contagious] →R04 [contagious] →R14 [contagious]	
Risk Probability:	4	
Risk Potential Impact:	3	
Risk Severity:	12	

Risk Identifier:	R28	
Risk Name:	Financial shortfalls or income restrictions	
Risk Description:	Atypical operational circumstances result in budgetary shortfall or gap.	
Is this Risk Relevant?:	• To what extent is the repository's annual budgetary allocation assured? • Is the repository required to make any capital investments on a less than annual basis? • Is there a possibility of expenditure commitments arising without warning and with a requirement for immediate investment?	
Example Risk Manifestation(s):	• Unanticipated enforced expenditure, such as replacement of non-functioning technological assets • Expenditure on new server systems every four years, rendering investment during those budgeting periods far in excess of the other three-quarters of the time	
Nature of Risk:	Physical environment	
	Personnel, management and administration procedures	X
	Operations and service delivery	
	Hardware, software or communications equipment and facilities	
Owner:	Budgeting	
Escalation Owner:	Budgeting	
Stakeholders:	Management; financiers; staff; depositors; users; producers	
Mitigation strategy(ies):	Avoidance strategies: • Manage budgetary allocations, bearing in mind commitments that are less than annual • Calculate replacement timescale for repository resources and aim to pre-empt hardware failure by reinvesting regularly In the event of risk's execution: • Maintain residual emergency fund	
Risk Relationships:	→R01 [contagious] →R02 [contagious] →R25 [contagious]	
Risk Probability:	4	
Risk Potential Impact:	3	
Risk Severity:	12	

Risk Identifier:	R29	
Risk Name:	Budgetary reduction	
Risk Description:	Repository's operational budget is reduced.	
Is this Risk Relevant?:	• To what extent are the repository's funding streams assured? • What proportion of budget is controlled and allocated externally as opposed to self-generated?	
Example Risk Manifestation(s):	• Local recession provokes budgetary reduction of government financed repository	
Nature of Risk:	Physical environment	
	Personnel, management and administration procedures	X
	Operations and service delivery	
	Hardware, software or communications equipment and facilities	
Owner:	Budgeting	
Escalation Owner:	Budgeting	
Stakeholders:	Management; financiers; staff; depositors; users; producers	
Mitigation strategy(ies):	Avoidance strategies: • Develop self-sustainability with charged-for services • Seek assurances of level of budget In the event of risk's execution: • Solicit additional funding to enable achievement of organisational objectives • Revise objectives if funding stream is insufficiently flexible • Maintain residual fund where possible to meet shortfalls	
Risk Relationships:	→R02 [contagious] →R25 [contagious]	
Risk Probability:	4	
Risk Potential Impact:	3	
Risk Severity:	12	

7.3.4 Technical Infrastructure and Security

Risk Identifier:	R30	
Risk Name:	Hardware failure or incompatibility	
Risk Description:	System hardware is rendered incapable of facilitating current business objectives.	
Is this Risk Relevant?:	• Are policies and procedures in place to monitor the adequacy of hardware technologies amid changing community requirements and external influences? • What service level guarantees are offered from third-party hardware service providers? • Is a proportion of staff time allocated to determining the ongoing suitability and operational functionality of hardware?	
Example Risk Manifestation(s):	• Server's power supply burns out, rendering hardware unusable	
Nature of Risk:	Physical environment	
	Personnel, management and administration procedures	
	Operations and service delivery	
	Hardware, software or communications equipment and facilities	X
Owner:	Technical	
Escalation Owner:	Technical	
Stakeholders:	Management; financiers; staff; depositors; users; producers	
Mitigation strategy(ies):	Avoidance strategies: • Allocate a proportion of staff time to monitoring the ongoing suitability of repository hardware and assessing the potential value of emerging technologies • Evaluate effects of system changes prior to their implementation • Pre-empt hardware failure with anticipatory investment In the event of risk's execution: • Seek formal assurances or SLAs from hardware suppliers or providers of third-party hardware services	
Risk Relationships:	→R01 [contagious] →R02 [contagious] →R32 [contagious] →R35 [contagious] →R52 – 79 [contagious]	
Risk Probability:	4	
Risk Potential Impact:	3	
Risk Severity:	12	

Risk Identifier:	R31	
Risk Name:	Software failure or incompatibility	
Risk Description:	System software is rendered incapable of facilitating current business objectives.	
Is this Risk Relevant?:	• Are policies and procedures in place to monitor the adequacy of software technologies amid changing community requirements and external influences? • What service level guarantees are offered from third-party software service providers? • Is a proportion of staff time allocated to determining the ongoing suitability and operational functionality of software?	
Example Risk Manifestation(s):	• Software update breaks dependencies of other core software services	
Nature of Risk:	Physical environment	
	Personnel, management and administration procedures	
	Operations and service delivery	
	Hardware, software or communications equipment and facilities	X
Owner:	Technical	
Escalation Owner:	Technical	
Stakeholders:	Management; financiers; staff; depositors; users; producers	
Mitigation strategy(ies):	Avoidance strategies: • Allocate a proportion of staff time to monitoring the ongoing suitability of repository software and assessing the potential value of emerging technologies • Evaluate effects of system changes prior to their implementation • Pre-empt software obsolescence with anticipatory investment In the event of risk's execution: • Seek formal assurances or SLAs from software suppliers or providers of third-party software services	
Risk Relationships:	→R01 [contagious] →R02 [contagious] →R32 [contagious] →R35 [contagious] →R52 – 79 [contagious]	
Risk Probability:	4	
Risk Potential Impact:	3	
Risk Severity:	12	

Risk Identifier:	R32	
Risk Name:	Hardware or software incapable of supporting emerging repository aims	
Risk Description:	Technical infrastructure, while adequate for meeting current aims, is incapable of meeting new requirements resulting from organisation's natural evolution.	
Is this Risk Relevant?:	• Are additional technical facilities required to facilitate the repository's anticipated development? • To what extent is the repository's current service level likely to increase over time?	
Example Risk Manifestation(s):	• Technical infrastructure is insufficiently scalable to handle an anticipated escalation in number of objects or requests • Hardware is incompatible with emerging operation systems	
Nature of Risk:	Physical environment	
	Personnel, management and administration procedures	
	Operations and service delivery	
	Hardware, software or communications equipment and facilities	X
Owner:	Technical	
Escalation Owner:	Technical	
Stakeholders:	Management; financiers; staff; depositors; users; producers	
Mitigation strategy(ies):	Avoidance strategies: • Allocate a proportion of staff time to monitoring the scalability and compatibility of repository technologies with respect to emerging organisational aims	
Risk Relationships:	→R01 [contagious] →R02 [contagious] →R52 – 79 [contagious]	
Risk Probability:	4	
Risk Potential Impact:	3	
Risk Severity:	12	

Risk Identifier:	R33	
Risk Name:	Obsolescence of hardware or software	
Risk Description:	Core technology is no longer current or is incongruent with that of most comparable organisations.	
Is this Risk Relevant?:	• Do vendors of currently employed hardware and software technologies offer a guaranteed period of support? • Are hardware and software technologies employed widely within contemporary and comparable organisations? • What is the mean-time-between-failure associated with the repository's chosen technologies?	
Example Risk Manifestation(s):	• Operating systems no longer supported by vendor, and therefore security updates are no longer being made available.	
Nature of Risk:	Physical environment	
	Personnel, management and administration procedures	
	Operations and service delivery	
	Hardware, software or communications equipment and facilities	X
Owner:	Technical	
Escalation Owner:	Technical	
Stakeholders:	Management; financiers; staff; depositors; users; producers	
Mitigation strategy(ies):	Avoidance strategies: • Allocate a proportion of staff time to monitoring the ongoing suitability of repository technologies and assessing the potential value of emerging technologies • Pre-empt technological obsolescence with anticipatory investment	
Risk Relationships:	→R01 [contagious] →R02 [contagious] →R52 – 79 [contagious]	
Risk Probability:	4	
Risk Potential Impact:	3	
Risk Severity:	12	

Risk Identifier:	R34	
Risk Name:	Media degradation or obsolescence	
Risk Description:	Storage media deteriorates, limiting the extent to which it can be written to and read from.	
Is this Risk Relevant?:	• Does the repository preserve digital content on removable media such as tapes, optical disks and flash devices? • Are employed storage media formats used widely within contemporary and comparable organisations? • Is the mean lifetime of relied upon media technologies understood and documented?	
Example Risk Manifestation(s):	• Tape-stored content is inaccessible or corrupted due to physical deterioration of magnetic tape • Contemporary tape drives are incapable of reading dated storage media which is prolific throughout archive	
Nature of Risk:	Physical environment	
	Personnel, management and administration procedures	
	Operations and service delivery	
	Hardware, software or communications equipment and facilities	X
Owner:	Technical	
Escalation Owner:	Technical	
Stakeholders:	Management; financiers; staff; depositors; users; producers	
Mitigation strategy(ies):	Avoidance strategies: • Allocate a proportion of staff time to monitoring the expected lifetime of storage media and assessing the potential value of emerging technologies • Pre-empt media obsolescence with anticipatory investment In the event of risk's execution: • Maintain redundant copies of information objects • Establish policies and procedures to extract archived materials from degraded media	
Risk Relationships:	→R02 [contagious] →R52 – 79 [contagious]	
Risk Probability:	4	
Risk Potential Impact:	3	
Risk Severity:	12	

Risk Identifier:	R35	
Risk Name:	Exploitation of security vulnerability	
Risk Description:	Shortcoming in repository's security provisions is identified and used to gain unauthorised access.	
Is this Risk Relevant?:	• Are vulnerabilities conceivably evident within repository's physical and system security? • Is it possible that individuals internal or external to the repository might be motivated to compromise system security to acquire or vandalise materials? • Are archived materials stored on network accessible computers?	
Example Risk Manifestation(s):	• Unpatched software security loophole hack • Intruder gains physical access to repository through a security door that is wedged open	
Nature of Risk:	Physical environment	X
	Personnel, management and administration procedures	
	Operations and service delivery	
	Hardware, software or communications equipment and facilities	X
Owner:	Technical	
Escalation Owner:	Technical	
Stakeholders:	Management; financiers; staff; depositors; users; producers	
Mitigation strategy(ies):	Avoidance strategies: • Establish and regularly evaluate policies and procedures for physical and software security in accordance with relevant standards • Limit execution of non-essential services • Update software with latest security patches • Allocate staff time to analyse attempted security compromises and monitor security sources for details of known vulnerabilities • Compel users to change passwords frequently In the event of risk's execution: • Rebuild system to ensure there are no residual effects of system compromise	
Risk Relationships:	→R01 [contagious] →R02 [contagious] →R36 [contagious] →R37 [contagious] →R38 [contagious] →R42 [contagious] →R46 [contagious →R52 – 79 [contagious]	
Risk Probability:	4	
Risk Potential Impact:	3	
Risk Severity:	12	

Risk Identifier:	R36	
Risk Name:	Unidentified security compromise, vulnerability or information degradation	
Risk Description:	Security exploitation or vulnerability occurs and is not monitored or identified by repository staff.	
Is this Risk Relevant?:	• Are mechanisms in place to identify all system access attempts? • Are mechanisms in place to determine when and how changes to stored content have taken place? • Are system logs regularly analysed to seek evidence of security breaches or attempted breaches?	
Example Risk Manifestation(s):	• System is hacked and key logger installed without knowledge of systems staff	
Nature of Risk:	Physical environment	X
	Personnel, management and administration procedures	
	Operations and service delivery	
	Hardware, software or communications equipment and facilities	X
Owner:	Technical	
Escalation Owner:	Technical	
Stakeholders:	Management; financiers; staff; depositors; users; producers	
Mitigation strategy(ies):	Avoidance strategies: • Undertake appropriate measures to limit likelihood of system compromises, and implement monitoring to detect where attempts have taken place in accordance with relevant standards In the event of risk's execution: • Allocate staff time to analyse system logs for details of security compromises • Rebuild system to ensure there are no residual effects	
Risk Relationships:	→R01 [contagious] →R02 [contagious] →R42 [contagious] →R46 [contagious →R52 – 79 [contagious]	
Risk Probability:	4	
Risk Potential Impact:	3	
Risk Severity:	12	

Risk Identifier:	R37	
Risk Name:	Physical intrusion of hardware storage space	
Risk Description:	Intruder gains access to area within which repository technical hardware is physically located.	
Is this Risk Relevant?:	• Are vulnerabilities conceivably evident within repository's physical security? • Is it possible that individuals internal or external to the repository might be motivated to compromise system security to acquire or vandalise materials?	
Example Risk Manifestation(s):	• Intruder breaks into repository, bypassing security measures	
Nature of Risk:	Physical environment	X
	Personnel, management and administration procedures	
	Operations and service delivery	
	Hardware, software or communications equipment and facilities	
Owner:	Technical	
Escalation Owner:	Technical	
Stakeholders:	Management; financiers; staff; depositors; users; producers	
Mitigation strategy(ies):	Avoidance strategies: • Establish, test and regularly evaluate policies and procedures for physical security in accordance with relevant standards	
Risk Relationships:	→R01 [contagious] →R02 [contagious] →R42 [contagious] →R46 [contagious →R52 – 79 [contagious]	
Risk Probability:	4	
Risk Potential Impact:	3	
Risk Severity:	12	

Risk Identifier:	R38	
Risk Name:	Remote or local software intrusion	
Risk Description:	Repository suffers software intrusion conducted either from onsite or from a remote location, by bypassing network security provisions.	
Is this Risk Relevant?:	• Are vulnerabilities conceivably evident within repository's system security? • Is it possible that individuals internal or external to the repository might be motivated to compromise system security to acquire or vandalise materials? • Are archived materials stored on network accessible computers?	
Example Risk Manifestation(s):	• Hacker remotely exploits server software security via secure shell tunnelling, executing malicious code on the server	
Nature of Risk:	Physical environment	
	Personnel, management and administration procedures	
	Operations and service delivery	
	Hardware, software or communications equipment and facilities	X
Owner:	Technical	
Escalation Owner:	Technical	
Stakeholders:	Management; financiers; staff; depositors; users; producers	
Mitigation strategy(ies):	• Establish and regularly evaluate policies and procedures for software security in accordance with relevant standards • Limit execution of non-essential services • Update software with latest security patches • Allocate staff time to analyse attempted security compromises and monitor security sources for details of known vulnerabilities • Compel users to change passwords frequently In the event of risk's execution: • Rebuild system to ensure there are no residual effects of system compromise	
Risk Relationships:	→R01 [contagious] →R02 [contagious] →R42 [contagious] →R46 [contagious →R52 – 79 [contagious]	
Risk Probability:	4	
Risk Potential Impact:	3	
Risk Severity:	12	

Risk Identifier:	R39	
Risk Name:	Local destructive or disruptive environmental phenomenon	
Risk Description:	Repository business activities are affected by circumstances that originate externally to the repository, with localised consequences.	
Is this Risk Relevant?:	• Is the repository likely to be exposed to adverse or extreme weather conditions? • Is the repository under threat from geological or man-made dangers (such as earthquakes, volcanoes, mining-related subsidence or coastal erosion)?	
Example Risk Manifestation(s):	• Hurricane, tornado or typhoon in nearby vicinity • Earthquake	
Nature of Risk:	Physical environment	X
	Personnel, management and administration procedures	
	Operations and service delivery	
	Hardware, software or communications equipment and facilities	
Owner:	Technical	
Escalation Owner:	Technical	
Stakeholders:	Management; financiers; staff; depositors; users; producers	
Mitigation strategy(ies):	Avoidance strategies: • Monitor for likelihood of applicable environmental concerns • Take physical precautions against the most locally profound threats, such as installing hurricane-proof windows In the event of risk's execution: • Establish redundant storage facilities at remote location	
Risk Relationships:	→R01 [contagious] →R02 [contagious] →R42 [contagious] →R46 [contagious] →R52 – 79 [contagious]	
Risk Probability:	4	
Risk Potential Impact:	3	
Risk Severity:	12	

Risk Identifier:	R40	
Risk Name:	Accidental system disruption	
Risk Description:	Business activities are adversely affected by non-deliberate intervention, or intervention that was not intended to result in these outcomes.	
Is this Risk Relevant?:	• Do repository systems permit members of staff to perform interactions that are contrary to agreed policies or procedures? • Are interactions reversible?	
Example Risk Manifestation(s):	• Staff member accidentally stops integral repository software services • Content is inadvertently deleted during its ingest	
Nature of Risk:	Physical environment	
	Personnel, management and administration procedures	
	Operations and service delivery	X
	Hardware, software or communications equipment and facilities	X
Owner:	Technical	
Escalation Owner:	Technical	
Stakeholders:	Management; financiers; staff; depositors; users; producers	
Mitigation strategy(ies):	Avoidance strategies: • Develop systems to limit extent to which non-valid interactions, or those that contradict policy can physically occur • Ensure staff are well trained in use of systems and informed of the importance of checking their interactions prior to execution In the event of risk's execution: • Identify reason for accidental action and introduce measures to disallow or dissuade users from repeating the error	
Risk Relationships:	→R01 [contagious] →R02 [contagious] →R52 – 79 [contagious]	
Risk Probability:	4	
Risk Potential Impact:	3	
Risk Severity:	12	

Risk Identifier:	R41	
Risk Name:	Deliberate system sabotage	
Risk Description:	Business activities are adversely affected by measures intended to have these effects.	
Is this Risk Relevant?:	• Is it conceivable that individuals may seek to maliciously damage repository content or systems? • To what extent are system interactions, or those undertaken by circumventing the system, reversible? • Are members of staff that leave the organisation accompanied off-site and stripped of system access and authorisations?	
Example Risk Manifestation(s):	• e-Terrorism or physical (conventional) terrorism • Disaffected staff members maliciously vandalise systems	
Nature of Risk:	Physical environment	X
	Personnel, management and administration procedures	X
	Operations and service delivery	X
	Hardware, software or communications equipment and facilities	X
Owner:	Technical	
Escalation Owner:	Technical	
Stakeholders:	Management; financiers; staff; depositors; users; producers	
Mitigation strategy(ies):	Avoidance strategies: • Maintain, test and revise physical and software security in accordance with relevant standards • Monitor for suspicious network activity or physical activity that appears unusual • Remove staff members or ex-staff members that are likely to be disaffected and immediately revoke system privileges In the event of risk's execution: • Ensure as far as possible that all system interactions are reversible • Ensure availability of redundant copies of system state and archived information at remote geographical location	
Risk Relationships:	→R01 [contagious] →R02 [contagious] →R42 [contagious] →R46 [contagious] →R52 – 79 [contagious]	
Risk Probability:	4	
Risk Potential Impact:	3	
Risk Severity:	12	

Risk Identifier:	R42	
Risk Name:	Destruction or non-availability of repository site	
Risk Description:	Repository's physical premises are destroyed or rendered permanently or temporarily unusable.	
Is this Risk Relevant?:	• Are the repository's operational activities undertaken within a single physical building or group of buildings within a small geographical area? • Are redundant system and storage facilities established?	
Example Risk Manifestation(s):	• Fire damage • Asbestos found within building	
Nature of Risk:	Physical environment	X
	Personnel, management and administration procedures	
	Operations and service delivery	
	Hardware, software or communications equipment and facilities	
Owner:	Technical	
Escalation Owner:	Technical	
Stakeholders:	Management; financiers; staff; depositors; users; producers	
Mitigation strategy(ies):	Avoidance strategies: • Maintain, test and revise physical and software system security policies in accordance with relevant standards In the event of risk's execution: • Establish redundant storage facilities capable of becoming operational base	
Risk Relationships:	→R01 [contagious] →R02 [contagious] →R52 – 79 [contagious] →R52 – 79 [explosive]	
Risk Probability:	4	
Risk Potential Impact:	3	
Risk Severity:	12	

Risk Identifier:	R43	
Risk Name:	Non-availability of core utilities	
Risk Description:	Key third-party, externally originating services suffer from temporary disruption, and are not available.	
Is this Risk Relevant?:	• Does repository rely upon availability of externally provided utilities such as gas, electricity, network services or water?	
Example Risk Manifestation(s):	• Temporary disruption to repository's electrical supplies	
Nature of Risk:	Physical environment	X
	Personnel, management and administration procedures	
	Operations and service delivery	
	Hardware, software or communications equipment and facilities	
Owner:	Management	
Escalation Owner:	Management	
Stakeholders:	Management; financiers; staff; depositors; users; producers	
Mitigation strategy(ies):	Avoidance strategies: • Establish service level agreements or service commitments with utility provider In the event of risk's execution: • Establish internal means to nullify disruption wherever possible, such as installing a petrol electricity generator and UPS systems	
Risk Relationships:	→R01 [contagious] →R02 [contagious] →R42 [contagious] →R52 – 79 [contagious]	
Risk Probability:	4	
Risk Potential Impact:	3	
Risk Severity:	12	

Risk Identifier:	R44	
Risk Name:	Loss of other third-party services	
Risk Description:	Other third-party services that the repository relies upon suffer disruption.	
Is this Risk Relevant?:	• Does the repository sub-contract any of its repository activities? • Does the repository rely upon any other third-party services such as cleaning or catering?	
Example Risk Manifestation(s):	• The web hosting company serving the repository's information dissemination systems goes out of business • Repository's catering company takes industrial action and staff are unable to receive meals	
Nature of Risk:	Physical environment	X
	Personnel, management and administration procedures	
	Operations and service delivery	X
	Hardware, software or communications equipment and facilities	X
Owner:	Management	
Escalation Owner:	Management	
Stakeholders:	Management; financiers; staff; depositors; users; producers	
Mitigation strategy(ies):	Avoidance strategies: • Establish service level agreements or service commitments with third-party provider In the event of risk's execution: • Establish internal means to nullify disruption wherever possible	
Risk Relationships:	→R01 [contagious] →R02 [contagious] →R42 [contagious] →R52 – 79 [contagious]	
Risk Probability:	4	
Risk Potential Impact:	3	
Risk Severity:	12	

Risk Identifier:	R45	
Risk Name:	Change of terms within third-party service contracts	
Risk Description:	Conditions with which third-party services are delivered change substantially.	
Is this Risk Relevant?:	• Are third-party service or utilities contracts subject to renewal or due to be renegotiated?	
Example Risk Manifestation(s):	• Electricity prices escalate • Web hosting service provider withdraws a relied-upon technology from its servers	
Nature of Risk:	Physical environment	X
	Personnel, management and administration procedures	X
	Operations and service delivery	X
	Hardware, software or communications equipment and facilities	X
Owner:	Management	
Escalation Owner:	Management	
Stakeholders:	Management; financiers; staff; depositors; users; producers	
Mitigation strategy(ies):	Avoidance strategies: • Establish lasting service level agreements with third-party provider with minimal scope for their subsequent renegotiation In the event of risk's execution: • Implement policy to seek alternative service providers capable of offering more favourable terms	
Risk Relationships:	→R01 [contagious] →R02 [contagious] →R42 [contagious] →R52 – 79 [contagious]	
Risk Probability:	4	
Risk Potential Impact:	3	
Risk Severity:	12	

Risk Identifier:	R46	
Risk Name:	Destruction of primary documentation	
Risk Description:	Repository documentation is partially or completed destroyed.	
Is this Risk Relevant?:	• Is repository documentation maintained and stored within the principal repository site? • Are multiple copies of documentation maintained and stored?	
Example Risk Manifestation(s):	• Fire damage within repository's administrative offices destroys contracts and policy documentation	
Nature of Risk:	Physical environment	
	Personnel, management and administration procedures	X
	Operations and service delivery	X
	Hardware, software or communications equipment and facilities	X
Owner:	Management	
Escalation Owner:	Management	
Stakeholders:	Management; financiers; staff; depositors; users; producers	
Mitigation strategy(ies):	Avoidance strategies: • Maintain multiple electronic and hard copies of documentation stored in multiple locations	
Risk Relationships:	→R01 [contagious] →R02 [contagious] →R12 [contagious] →R52 – 79 [contagious]	
Risk Probability:	4	
Risk Potential Impact:	3	
Risk Severity:	12	

Risk Identifier:	R47	
Risk Name:	Inability to evaluate effectiveness of technical infrastructure and security	
Risk Description:	Repository is incapable of effectively determining the extent to which its technical infrastructure and security provisions are capable of facilitating business objectives.	
Is this Risk Relevant?:	• Does the repository maintain policies and procedures to verify and record attempted security compromises? • Does the repository maintain policies and procedures to identify non-authorised or inappropriate system interactions? • Does the repository maintain policies and procedures to ensure the ongoing suitability and functionality of hardware and software technologies and storage media? • Are mechanisms to determine the effectiveness of technical and security provisions exploited on a regular basis?	
Example Risk Manifestation(s):	• Repository has no mechanisms to test security provisions or to evaluate the effectiveness of technological infrastructure	
Nature of Risk:	Physical environment	
	Personnel, management and administration procedures	X
	Operations and service delivery	
	Hardware, software or communications equipment and facilities	X
Owner:	Management	
Escalation Owner:	Management	
Stakeholders:	Management; financiers; staff; depositors; users; producers	
Mitigation strategy(ies):	Avoidance strategies: • Establish internal means of assessment including risk management • Seek relevant external certification in order to demonstrate competence	
Risk Relationships:	→R01 [contagious] →R02 [contagious] →R19 [contagious]	
Risk Probability:	4	
Risk Potential Impact:	3	
Risk Severity:	12	

7.3.5 Acquisition and Ingest

Risk Identifier:	R48	
Risk Name:	Structural non-validity or malformedness of received packages	
Risk Description:	Received packages fail to correspond to what repository expects or is capable of preserving.	
Is this Risk Relevant?:	• Does repository define the structure that should be conformed to by submitted content? • Does repository stipulate acceptable formats?	
Example Risk Manifestation(s):	• Deposited content is encoded in a format that is unsupported by the repository • Deposited XML-encoded content does not validate against the schema provided by the repository	
Nature of Risk:	Physical environment	
	Personnel, management and administration procedures	
	Operations and service delivery	X
	Hardware, software or communications equipment and facilities	
Owner:	Ingest	
Escalation Owner:	Ingest	
Stakeholders:	Management; financiers; staff; depositors; users; producers	
Mitigation strategy(ies):	Avoidance strategies: • Develop definition for submission package structure • Establish list of acceptable formats for submission • Communicate definition to depositors and producers In the event of risk's execution: • Maintain policy and procedure to determine whether package is disposed of, returned or ingested	
Risk Relationships:	→R01 [contagious] →R02 [contagious] →R49 [contagious]	
Risk Probability:	4	
Risk Potential Impact:	3	
Risk Severity:	12	

Risk Identifier:	R49	
Risk Name:	Incompleteness of submitted packages	
Risk Description:	Received packages do not contain information that is necessary to facilitate their preservation.	
Is this Risk Relevant?:	• Does repository define the structure that should be conformed to by submitted content? • Does repository stipulate metadata requirements for submitted content?	
Example Risk Manifestation(s):	• Submitted package lacks metadata information that, in accordance with contracts, must accompany all deposited content	
Nature of Risk:	Physical environment	
	Personnel, management and administration procedures	
	Operations and service delivery	X
	Hardware, software or communications equipment and facilities	X
Owner:	Ingest	
Escalation Owner:	Ingest	
Stakeholders:	Management; financiers; staff; depositors; users; producers	
Mitigation strategy(ies):	Avoidance strategies: • Develop definition for submission package structure • Establish list of acceptable formats for submission • Communicate definition to depositors and producers In the event of risk's execution: • Maintain policy and procedure to determine whether package is disposed of, returned or ingested	
Risk Relationships:	→R01 [contagious] →R02 [contagious]	
Risk Probability:	4	
Risk Potential Impact:	3	
Risk Severity:	12	

Risk Identifier:	R50	
Risk Name:	Externally motivated changes or maintenance to information during ingest	
Risk Description:	Between the points of receipt and the creation of an archivable object the received package is subjected to changes that are not sanctioned or implemented by the repository.	
Is this Risk Relevant?:	• Does repository obtain full physical and intellectual control of submitted content?	
Example Risk Manifestation(s):	• An intrinsic part of a submitted object is not included within the deposited package and instead is remotely referenced. During the process of ingest this remote object is subject to alteration by external actors	
Nature of Risk:	Physical environment	
	Personnel, management and administration procedures	
	Operations and service delivery	X
	Hardware, software or communications equipment and facilities	
Owner:	Ingest	
Escalation Owner:	Ingest	
Stakeholders:	Management; financiers; staff; depositors; users; producers	
Mitigation strategy(ies):	Avoidance strategies: • Ensure that sole, complete physical and intellectual control is obtained over received object In the event of risk's execution: • Maintain policy and procedure to determine whether package is disposed of, returned or ingested	
Risk Relationships:	→R01 [contagious] →R02 [contagious] →R52 – 79 [contagious]	
Risk Probability:	4	
Risk Potential Impact:	3	
Risk Severity:	12	

Risk Identifier:	R51	
Risk Name:	Archival information cannot be traced to a received package	
Risk Description:	An archival object cannot be traced to a corresponding received package or selection of packages.	
Is this Risk Relevant?:	• Are policies and procedures in place to validate that archived content corresponds with what was originally submitted? • Is ingested content subject to transformation to an archival package?	
Example Risk Manifestation(s):	• Repository cannot identify the origins of an archived package in order to ensure that its integrity has been adequately preserved	
Nature of Risk:	Physical environment	
	Personnel, management and administration procedures	
	Operations and service delivery	X
	Hardware, software or communications equipment and facilities	
Owner:	Ingest	
Escalation Owner:	Ingest	
Stakeholders:	Management; financiers; staff; depositors; users; producers	
Mitigation strategy(ies):	Avoidance strategies: • Record appropriate provenance information, detailing interactions undertaken during receipt and ingest process In the event of risk's execution: • Maintain policy and procedure to determine whether package is disposed of, returned or retained	
Risk Relationships:	→R01 [contagious] →R02 [contagious] →R55 [contagious] →R60 [contagious]	
Risk Probability:	4	
Risk Potential Impact:	3	
Risk Severity:	12	

7.3.6 Preservation and Storage

Risk Identifier:	R52	
Risk Name:	Loss of confidentiality of information	
Risk Description:	Information protected by confidentiality agreements is made available to communities, in contravention of those agreements.	
Is this Risk Relevant?:	• Is repository bound by requirements to maintain information confidentiality?	
Example Risk Manifestation(s):	• Repository authorisation subsystems fail and commercially sensitive information is exposed to a community that is considerably wider than that to whom, according to the relevant deposit agreement, access may be legitimately afforded	
Nature of Risk:	Physical environment	
	Personnel, management and administration procedures	
	Operations and service delivery	X
	Hardware, software or communications equipment and facilities	
Owner:	Preservation	
Escalation Owner:	Preservation	
Stakeholders:	Management; financiers; staff; depositors; users; producers	
Mitigation strategy(ies):	Avoidance strategies: • Ensure policies and procedures are conceived with due consideration of any confidentiality requirements that the repository is subject to • Ensure software and hardware systems and preservation strategies are capable of meeting requirements of policies In the event of risk's execution: • Implement policy to withdraw availability of confidential materials and invoke treatment strategies to alleviate loss of reputation	
Risk Relationships:	→R01 [contagious] →R02 [contagious]	
Risk Probability:	4	
Risk Potential Impact:	3	
Risk Severity:	12	

Risk Identifier:	R53	
Risk Name:	Loss of availability of information and/or service	
Risk Description:	Repository is unable to provide a comprehensive range of services or access to all of its information holdings for which access ought to be available.	
Is this Risk Relevant?:	• Does repository commit to defined service levels? • Does repository provide assurances of information availability?	
Example Risk Manifestation(s):	• Repository's servers fail, rendering a proportion of its collections inaccessible, although contracts stipulate that access should be afforded	
Nature of Risk:	Physical environment	
	Personnel, management and administration procedures	
	Operations and service delivery	X
	Hardware, software or communications equipment and facilities	
Owner:	Preservation	
Escalation Owner:	Preservation	
Stakeholders:	Management; financiers; staff; depositors; users; producers	
Mitigation strategy(ies):	Avoidance strategies: • Ensure policies and procedures are conceived with due consideration of any service levels that the repository has committed to • Ensure software and hardware systems and preservation strategies are capable of meeting service levels In the event of risk's execution: • Invoke treatment strategies to alleviate loss of reputation or trust	
Risk Relationships:	→R01 [contagious] →R02 [contagious]	
Risk Probability:	4	
Risk Potential Impact:	3	
Risk Severity:	12	

Risk Identifier:	R54	
Risk Name:	Loss of authenticity of information	
Risk Description:	Repository is incapable of demonstrating that information objects are what they purport to be.	
Is this Risk Relevant?:	• Does repository commit to the preservation of information authenticity?	
Example Risk Manifestation(s):	• Repository is unable to demonstrate the authenticity of preserved records that purport to describe government departmental expenditure	
Nature of Risk:	Physical environment	
	Personnel, management and administration procedures	
	Operations and service delivery	X
	Hardware, software or communications equipment and facilities	
Owner:	Preservation	
Escalation Owner:	Preservation	
Stakeholders:	Management; financiers; staff; depositors; users; producers	
Mitigation strategy(ies):	Avoidance strategies: • Ensure policies and procedures are conceived with due consideration of authenticity requirements • Maintain and review policies and procedures to ensure adequate recording of provenance information to demonstrate that archived material represents authentic representation of what was initially deposited or received • Ensure software and hardware systems and preservation strategies are capable of preserving authenticity In the event of risk's execution: • Invoke treatment strategies to alleviate loss of reputation or trust	
Risk Relationships:	→R01 [contagious] →R02 [contagious]	
Risk Probability:	4	
Risk Potential Impact:	3	
Risk Severity:	12	

Risk Identifier:	R55	
Risk Name:	Loss of integrity of information	
Risk Description:	Repository is incapable of demonstrating that the integrity of information has been maintained since its receipt, and that what is stored corresponds exactly with what was originally received.	
Is this Risk Relevant?:	• Does repository commit to preservation of information integrity?	
Example Risk Manifestation(s):	• Records documenting government expenditure have been subjected to unauthorised or unanticipated changes, rendering them no longer representative of originally deposited content	
Nature of Risk:	Physical environment	
	Personnel, management and administration procedures	
	Operations and service delivery	X
	Hardware, software or communications equipment and facilities	
Owner:	Preservation	
Escalation Owner:	Preservation	
Stakeholders:	Management; financiers; staff; depositors; users; producers	
Mitigation strategy(ies):	Avoidance strategies: • Ensure policies and procedures are conceived with due consideration of integrity requirements • Maintain and review policies and procedures to ensure adequate recording and comparison of checksums to demonstrate that archived information has suffered no loss of integrity since its deposit or receipt • Ensure software and hardware systems and preservation strategies are capable of preserving information integrity In the event of risk's execution: • Invoke treatment strategies to alleviate loss of reputation or trust	
Risk Relationships:	→R01 [contagious] →R02 [contagious]	
Risk Probability:	4	
Risk Potential Impact:	3	
Risk Severity:	12	

Risk Identifier:	R56	
Risk Name:	Unidentified information change	
Risk Description:	Repository is incapable of tracking or monitoring where one or more changes to archived information has taken place.	
Is this Risk Relevant?:	• Are repository mechanisms available to identify where preserved information has been subject to interactions or change?	
Example Risk Manifestation(s):	• Repository has failed to record or maintain adequate checksum information to detect where changes have been made to archived information	
Nature of Risk:	Physical environment	
	Personnel, management and administration procedures	X
	Operations and service delivery	X
	Hardware, software or communications equipment and facilities	X
Owner:	Preservation	
Escalation Owner:	Preservation	
Stakeholders:	Management; financiers; staff; depositors; users; producers	
Mitigation strategy(ies):	Avoidance strategies: • Implement policies and procedures to record, calculate and compare checksum values for archived information on a regular basis In the event of risk's execution: • Implement policies and procedures to record, calculate and compare checksum values for archived information on a regular basis • Invoke treatment strategies to alleviate loss of reputation or trust	
Risk Relationships:	→R01 [contagious] →R02 [contagious]	
Risk Probability:	4	
Risk Potential Impact:	3	
Risk Severity:	12	

Risk Identifier:	R57	
Risk Name:	Loss of non-repudiation of commitments	
Risk Description:	Repository is incapable of ensuring that commitments cannot later be denied by either of the parties involved.	
Is this Risk Relevant?:	• Does repository engage in agreements where obligations are assumed by contracting parties?	
Example Risk Manifestation(s):	• Repository fails to record details of transactions with contractor who later denies that they have agreed to the information exchanged, and its implied obligations	
Nature of Risk:	Physical environment	
	Personnel, management and administration procedures	X
	Operations and service delivery	X
	Hardware, software or communications equipment and facilities	
Owner:	Preservation	
Escalation Owner:	Preservation	
Stakeholders:	Management; financiers; staff; depositors; users; producers	
Mitigation strategy(ies):	Avoidance strategies: • Maintain and review policies and procedures to ensure contractual commitments are communicated, understood, recorded and agreed upon by both parties. In the event of risk's execution: • Implement policy to define appropriate procedural response, such as seeking legal advice to pursue enforcement of contract	
Risk Relationships:	→R01 [contagious] →R02 [contagious] →R16 [contagious]	
Risk Probability:	4	
Risk Potential Impact:	3	
Risk Severity:	12	

Risk Identifier:	R58	
Risk Name:	Loss of information reliability	
Risk Description:	Repository is incapable of demonstrating the reliability of its information holdings.	
Is this Risk Relevant?:	• Does repository commit to preserve reliability of information?	
Example Risk Manifestation(s):	• Archived information within a meteorological data centre is regarded as being insufficiently reliable to form the basis for scientific research • A court of law refuses to admit archived information as evidence on the grounds that it is unreliable	
Nature of Risk:	Physical environment	
	Personnel, management and administration procedures	
	Operations and service delivery	X
	Hardware, software or communications equipment and facilities	
Owner:	Preservation	
Escalation Owner:	Preservation	
Stakeholders:	Management; financiers; staff; depositors; users; producers	
Mitigation strategy(ies):	Avoidance strategies: • Ensure policies and procedures are conceived with due consideration of reliability requirements • Maintain and review policies and procedures to ensure adequate recording and comparison of checksums to demonstrate that archived information has suffered no loss of integrity since its deposit or receipt • Maintain and review policies and procedures to ensure adequate recording of provenance information to demonstrate that archived material represents authentic representation of what was initially deposited or received • Ensure software and hardware systems and preservation strategies are capable of preserving information reliability In the event of risk's execution: • Invoke treatment strategies to alleviate loss of reputation or trust	
Risk Relationships:	→R01 [contagious] →R02 [contagious]	
Risk Probability:	4	
Risk Potential Impact:	3	
Risk Severity:	12	

Risk Identifier:	R59	
Risk Name:	Loss of information provenance	
Risk Description:	Repository is incapable of demonstrating the provenance of its information holdings, and their traceability from receipt and through each interaction that they have been subject to.	
Is this Risk Relevant?:	• Are mechanisms in place to record the origins and lifecycle of an archived package and any transactions or interactions that it has been subject to?	
Example Risk Manifestation(s):	• Repository fails to document the preservation processes undertaken to convert a received Microsoft Word file into a plain text preservation master	
Nature of Risk:	Physical environment	
	Personnel, management and administration procedures	
	Operations and service delivery	X
	Hardware, software or communications equipment and facilities	
Owner:	Preservation	
Escalation Owner:	Preservation	
Stakeholders:	Management; financiers; staff; depositors; users; producers	
Mitigation strategy(ies):	Avoidance strategies: • Ensure policies and procedures are conceived with due consideration of provenance requirements • Maintain and review policies and procedures to record the origins and lifecycle of archived packages and any transactions or interactions that they have been subject to • Ensure software and hardware systems and preservation strategies are capable of maintaining and recording provenance information In the event of risk's execution: • Invoke treatment strategies to alleviate loss of reputation or trust	
Risk Relationships:	→R01 [contagious] →R02 [contagious] →R51 [contagious] →R69 [contagious]	
Risk Probability:	4	
Risk Potential Impact:	3	
Risk Severity:	12	

Risk Identifier:	R60	
Risk Name:	Loss or non-suitability of backups	
Risk Description:	Repository is unable to retrieve content or system state information from backup mechanism.	
Is this Risk Relevant?:	• Does repository rely upon backups of its system or content to react to the loss or non-availability of primary digital resources? • Are backup systems built upon well-established and widely used technologies? • In the event of destruction or damage to the primary repository site, is the safety of backed-up materials also threatened?	
Example Risk Manifestation(s):	• Faced with the loss of primary archival information, the repository discovers that it is unable to restore content because backup tapes are irreparably corrupted	
Nature of Risk:	Physical environment	
	Personnel, management and administration procedures	
	Operations and service delivery	X
	Hardware, software or communications equipment and facilities	X
Owner:	Technical	
Escalation Owner:	Technical	
Stakeholders:	Management; financiers; staff; depositors; users; producers	
Mitigation strategy(ies):	Avoidance strategies: • Maintain multiple copies of backups • Store backed-up content in remote locations • Undertake regular ‘fire-drill’ tests to determine whether systems and data can be restored from backup In the event of risk’s execution: • Recover as much content as possible, exploiting techniques such as digital archaeology and digital forensics • Invoke treatment strategies to alleviate loss of reputation	
Risk Relationships:	→R01 [contagious] →R02 [contagious] →R52-69 [explosive]	
Risk Probability:	4	
Risk Potential Impact:	3	
Risk Severity:	12	

Risk Identifier:	R61	
Risk Name:	Inconsistency between redundant copies	
Risk Description:	Where repository maintains multiple copies of archived information, one or more differs from peers.	
Is this Risk Relevant?:	• Does repository maintain multiple redundant copies of archived content? • Does repository employ mechanisms to check for inconsistencies between multiple copies? • Are policies and procedures in place to react to the discovery of such inconsistencies?	
Example Risk Manifestation(s):	• Repository maintains three redundant copies of archived information, but random checksum comparisons reveal that one is different from its peers	
Nature of Risk:	Physical environment	
	Personnel, management and administration procedures	
	Operations and service delivery	X
	Hardware, software or communications equipment and facilities	X
Owner:	Preservation	
Escalation Owner:	Preservation	
Stakeholders:	Management; financiers; staff; depositors; users; producers	
Mitigation strategy(ies):	Avoidance strategies: • Record and compare checksum information corresponding to redundant packages on a regular basis • Maintain system technologies and security to limit likelihood of data corruption or malfeasance In the event of risk's execution: • Conceive policies and procedures to react to the discovery of such inconsistencies – for instance, use an election system where the checksum values in the majority are assumed to be correct and the minority is/are disposed of and replaced	
Risk Relationships:	→R01 [contagious] →R02 [contagious] →R12 [explosive]	
Risk Probability:	4	
Risk Potential Impact:	3	
Risk Severity:	12	

Risk Identifier:	R62	
Risk Name:	Extent of what is within the archival object is unclear	
Risk Description:	Repository is incapable of determining the parts of the archival object that will be subject to ongoing preservation.	
Is this Risk Relevant?:	• Does repository define the scope and extent of its archival package format(s)? • Do policies and procedures exist to validate archival packages for completeness and correctness?	
Example Risk Manifestation(s):	• Repository fails to adequately define its archival package format	
Nature of Risk:	Physical environment	
	Personnel, management and administration procedures	
	Operations and service delivery	X
	Hardware, software or communications equipment and facilities	
Owner:	Preservation	
Escalation Owner:	Preservation	
Stakeholders:	Management; financiers; staff; depositors; users; producers	
Mitigation strategy(ies):	Avoidance strategies: • Conceive definition for archival package In the event of risk's execution: • Conceive policy to react to ambiguity surrounding archival object	
Risk Relationships:	→R01 [contagious] →R02 [contagious] →R12 [explosive]	
Risk Probability:	4	
Risk Potential Impact:	3	
Risk Severity:	12	

Risk Identifier:	R63	
Risk Name:	Inability to validate effectiveness of ingest process	
Risk Description:	Repository is incapable of asserting that integrity and authenticity were maintained during the process of ingesting digital information.	
Is this Risk Relevant?:	• Does the repository maintain policies and procedures to record and compare checksum values? • Does the repository maintain policies and procedures to evaluate and record the execution of repository processes and to check that their outputs are complete and correct? • Are mechanisms to determine the effectiveness of ingest procedures exploited on a regular basis?	
Example Risk Manifestation(s):	• Repository is unable to demonstrate that ingest procedures have resulted successfully in complete and correct archival packages	
Nature of Risk:	Physical environment	
	Personnel, management and administration procedures	X
	Operations and service delivery	X
	Hardware, software or communications equipment and facilities	
Owner:	Preservation	
Escalation Owner:	Preservation	
Stakeholders:	Management; financiers; staff; depositors; users; producers	
Mitigation strategy(ies):	Avoidance strategies: • Establish internal means of assessment including risk management • Seek relevant external certification in order to demonstrate effectiveness of ingest process	
Risk Relationships:	→R01 [contagious] →R02 [contagious] →R19 [contagious]	
Risk Probability:	4	
Risk Potential Impact:	3	
Risk Severity:	12	

Risk Identifier:	R64	
Risk Name:	Identifier to information referential integrity is compromised	
Risk Description:	Where identifiers are applied to information, the repository is incapable of locating the archival package that corresponds to a given ID.	
Is this Risk Relevant?:	• Does repository apply or maintain existing persistent identifiers for information packages? • Is identifier potentially distinguishable from related information?	
Example Risk Manifestation(s):	• Repository maintains the use of the file path from the digital object's original environment as the identifier for the archived object, resulting in two distinct objects that originated from different locations sharing the duplicate identifer "C:\Documents and Settings\John Smith\Document.pdf" • Identifiers generated at ingest consist of the timestamp at the point of ingest, but two ingest systems operate simultaneously and duplicate identifiers are consequently applied	
Nature of Risk:	Physical environment	
	Personnel, management and administration procedures	
	Operations and service delivery	X
	Hardware, software or communications equipment and facilities	
Owner:	Preservation	
Escalation Owner:	Preservation	
Stakeholders:	Management; financiers; staff; depositors; users; producers	
Mitigation strategy(ies):	Avoidance strategies: • Define, document and review policies and procedures describing the means by which identifiers are associated with corresponding information packages and communicate this information widely within the organisation • Define and review policies and procedures describing the creation of identifiers to ensure their uniqueness, or mandating the adoption of third-party identifier technologies such as Handles, DOIs or PURLs In the event of risk's execution: • Define policy to respond to fracturing of relationship between identifiers and information • Invoke treatment strategies to alleviate loss of reputation	
Risk Relationships:	→R01 [contagious] →R02 [contagious] →R12 [contagious]	
Risk Probability:	4	
Risk Potential Impact:	3	
Risk Severity:	12	

Risk Identifier:	R65	
Risk Name:	Preservation plans cannot be implemented	
Risk Description:	Repository is incapable of executing in practice the preservation planning it has undertaken.	
Is this Risk Relevant?:	• Is preservation planning undertaken within the repository with the anticipation that it will subsequently be implemented? • Does preservation planning reflect the extent of technological, financial and human resources available within the repository as well as its organisational objectives?	
Example Risk Manifestation(s):	• Repository's planned emulation strategy requires technological expertise to implement that is unavailable within the staff, and insufficient resource exists to contract with third-party developers to undertake the work	
Nature of Risk:	Physical environment	
	Personnel, management and administration procedures	
	Operations and service delivery	X
	Hardware, software or communications equipment and facilities	
Owner:	Preservation	
Escalation Owner:	Preservation	
Stakeholders:	Management; financiers; staff; depositors; users; producers	
Mitigation strategy(ies):	Avoidance strategies: • Aim to reflect the extent of technological, financial and human resources available within the repository as well as its organisational objectives when conceiving preservation plans • Seek additional resources to facilitate original plans In the event of risk's execution: • Implement policy to refine preservation plans to correspond more closely to that which is feasible within the organisation	
Risk Relationships:	→R01 [contagious] →R02 [contagious] →R67 [contagious]	
Risk Probability:	4	
Risk Potential Impact:	3	
Risk Severity:	12	

Risk Identifier:	R66	
Risk Name:	Preservation strategies result in information loss	
Risk Description:	Exposure of an archived object to preservation plans results in loss or damage to one or more of its significant characteristics.	
Is this Risk Relevant?:	• Does repository offer a definition of acceptable loss that may result from preservation activities?	
Example Risk Manifestation(s):	• Repository's proposed migration strategy results in loss of 'look and feel' of archived documents, regarded as essential properties by user community	
Nature of Risk:	Physical environment	
	Personnel, management and administration procedures	
	Operations and service delivery	X
	Hardware, software or communications equipment and facilities	
Owner:	Preservation	
Escalation Owner:	Preservation	
Stakeholders:	Management; financiers; staff; depositors; users; producers	
Mitigation strategy(ies):	Avoidance strategies: • Evaluate preservation strategies in testbed environment prior to execution • Ensure procedures are reversible in the event of unexpected or inappropriate results In the event of risk's execution: • Define policies to describe the acceptable levels of loss tolerated by the repository	
Risk Relationships:	→R01 [contagious] →R02 [contagious] →R52-R69 [contagious] →R61 [explosive]	
Risk Probability:	4	
Risk Potential Impact:	3	
Risk Severity:	12	

Risk Identifier:	R67	
Risk Name:	Inability to validate effectiveness of preservation	
Risk Description:	Repository is incapable of effectively determining the extent to which its preservation activities are successful in terms of its business objectives.	
Is this Risk Relevant?:	• Does repository maintain policies and procedures to verify the preservation of information understandability, authenticity and integrity?	
Example Risk Manifestation(s):	• Repository lacks means to demonstrate continued preservation, including understandability to the appropriate user communities, of its holdings over a number of years, given the age of the repository and its holdings	
Nature of Risk:	Physical environment	
	Personnel, management and administration procedures	
	Operations and service delivery	X
	Hardware, software or communications equipment and facilities	
Owner:	Preservation	
Escalation Owner:	Preservation	
Stakeholders:	Management; financiers; staff; depositors; users; producers	
Mitigation strategy(ies):	Avoidance strategies: • Establish internal means of assessment including risk management • Seek relevant external certification in order to demonstrate competence	
Risk Relationships:	→R01 [contagious] →R02 [contagious] →R19 [contagious]	
Risk Probability:	4	
Risk Potential Impact:	3	
Risk Severity:	12	

Risk Identifier:	R68	
Risk Name:	Non-traceability of received, archived or disseminated package	
Risk Description:	Packages cannot be traced to corresponding packages or groups of packages from an earlier point within the repository's information lifecycle.	
Is this Risk Relevant?:	• Are mechanisms in place to record the origins and lifecycle of information packages and any transactions or interactions that they have been subject to?	
Example Risk Manifestation(s):	• Repository fails to maintain appropriate documentation describing the origins and lifecycle of an archived package and any transactions or interactions to which it has been subject	
Nature of Risk:	Physical environment	
	Personnel, management and administration procedures	X
	Operations and service delivery	X
	Hardware, software or communications equipment and facilities	
Owner:	Management	
Escalation Owner:	Management	
Stakeholders:	Management; financiers; staff; depositors; users; producers	
Mitigation strategy(ies):	Avoidance strategies: • Record appropriate provenance information, detailing interactions undertaken during receipt, ingest, preservation and dissemination processes In the event of risk's execution: • Define policy and procedures to determine whether package should be disposed of, returned or retained	
Risk Relationships:	→R01 [contagious] →R02 [contagious]	
Risk Probability:	4	
Risk Potential Impact:	3	
Risk Severity:	12	

7.3.7 Metadata Management

Risk Identifier:	R69	
Risk Name:	Metadata to information referential integrity is compromised	
Risk Description:	Associations between information packages and corresponding metadata are broken, and can no longer be traversed.	
Is this Risk Relevant?:	• Does repository maintain metadata records associated with archived information? • Is it conceivable that metadata records might become divorced from corresponding archived information? • How are associations defined and described?	
Example Risk Manifestation(s):	• Documentation describing the repository's directory structure, which represents relationships between metadata and corresponding objects, is irretrievably lost	
Nature of Risk:	Physical environment	
	Personnel, management and administration procedures	X
	Operations and service delivery	X
	Hardware, software or communications equipment and facilities	
Owner:	Documentation	
Escalation Owner:	Documentation	
Stakeholders:	Management; financiers; staff; depositors; users; producers	
Mitigation strategy(ies):	Avoidance strategies: • Define, document and review policies and procedures describing the means by which metadata are associated with corresponding information packages and communicate this information widely within the organisation • Define and review policies and procedures describing the metadata schema that will be used within the repository's activities In the event of risk's execution: • Define policy to respond to fracturing of relationship between metadata and information • Invoke treatment strategies to alleviate loss of reputation	
Risk Relationships:	→R01 [contagious] →R02 [contagious] →R52 - 69[contagious]	
Risk Probability:	4	
Risk Potential Impact:	3	
Risk Severity:	12	

Risk Identifier:	R70	
Risk Name:	Documented change history incomplete or incorrect	
Risk Description:	Metadata recording interactions, implemented preservation strategies or procedures undertaken with respect to information packages are undocumented, or only partially documented.	
Is this Risk Relevant?:	• Are mechanisms in place to record the origins and lifecycle of an information package and any transactions or interactions that it has been subject to?	
Example Risk Manifestation(s):	• Repository fails to maintain appropriate documentation describing the origins and lifecycle of an archived package and any transactions or interactions that it has been subject to	
Nature of Risk:	Physical environment	
	Personnel, management and administration procedures	X
	Operations and service delivery	X
	Hardware, software or communications equipment and facilities	
Owner:	Documentation	
Escalation Owner:	Documentation	
Stakeholders:	Management; financiers; staff; depositors; users; producers	
Mitigation strategy(ies):	Avoidance strategies: • Ensure policies and procedures are conceived with due consideration of provenance requirements • Maintain and review policies and procedures to record the origins and lifecycle of archived packages and any transactions or interactions that it has been subject to • Ensure software and hardware systems and preservation strategies are capable of maintaining and recording provenance information In the event of risk's execution: • Invoke treatment strategies to alleviate loss of reputation or trust	
Risk Relationships:	→R01 [contagious] →R02 [contagious] →R60 [contagious]	
Risk Probability:	4	
Risk Potential Impact:	3	
Risk Severity:	12	

Risk Identifier:	R71	
Risk Name:	Non-discoverability of information objects	
Risk Description:	Metadata supporting information package discovery are insufficient.	
Is this Risk Relevant?:	• Does repository make discovery metadata available to a user community, however small that community may be? • What degree of flexibility is offered to the user with respect to discovering archived content? • What systems are integral to the discovery of information objects?	
Example Risk Manifestation(s):	• A geophysical data centre records discovery metadata to facilitate searching only by name of data set, but researchers within the community wish to search based on the physical location where the data was acquired and the name of the instrument used	
Nature of Risk:	Physical environment	
	Personnel, management and administration procedures	
	Operations and service delivery	X
	Hardware, software or communications equipment and facilities	X
Owner:	Documentation	
Escalation Owner:	Documentation	
Stakeholders:	Management; financiers; staff; depositors; users; producers	
Mitigation strategy(ies):	Avoidance strategies: • Determine extent of discovery mechanisms and searchable fields in consultation with designated community • Communicate full range of available information discovery mechanisms to community In the event of risk's execution: • Introduce alternative means for information discovery based on perceived shortcomings	
Risk Relationships:	→R01 [contagious] →R02 [contagious] →R75 [contagious]	
Risk Probability:	4	
Risk Potential Impact:	3	
Risk Severity:	12	

Risk Identifier:	R72	
Risk Name:	Ambiguity of understandability definition	
Risk Description:	Repository is unable to describe what understandability means with reference to their stakeholder communities' expectations or requirements.	
Is this Risk Relevant?:	• Does the repository define understandability with respect to its user communities' expectations and requirements?	
Example Risk Manifestation(s):	• Repository preserves information and associated metadata based on a perception of what is required by user communities that is not necessarily representative	
Nature of Risk:	Physical environment	
	Personnel, management and administration procedures	X
	Operations and service delivery	X
	Hardware, software or communications equipment and facilities	
Owner:	Documentation	
Escalation Owner:	Documentation	
Stakeholders:	Management; financiers; staff; depositors; users; producers	
Mitigation strategy(ies):	Avoidance strategies: • Define and regularly review the concept of understandability with respect to community's expectations, requirements and knowledge base • Make understandability definition available to community and solicit their feedback In the event of risk's execution: • Retrospectively introduce policy detailing understandability definition	
Risk Relationships:	→R01 [contagious] →R02 [contagious]	
Risk Probability:	4	
Risk Potential Impact:	3	
Risk Severity:	12	

Risk Identifier:	R73	
Risk Name:	Shortcomings in semantic or technical understandability of information	
Risk Description:	Repository fails to maintain appropriately complete representation information to facilitate information understandability.	
Is this Risk Relevant?:	• Does repository record or refer to adequate representation information such as file format information? • Are understandability requirements referenced when determining minimal essential semantic or technical metadata?	
Example Risk Manifestation(s):	• Repository preserving social science data documents information about the *SPSS* format within which much of its content is encoded but fails to record the meaning of the acronyms used as field headings throughout these files	
Nature of Risk:	Physical environment	
	Personnel, management and administration procedures	
	Operations and service delivery	X
	Hardware, software or communications equipment and facilities	
Owner:	Documentation	
Escalation Owner:	Documentation	
Stakeholders:	Management; financiers; staff; depositors; users; producers	
Mitigation strategy(ies):	Avoidance strategies: • Record or refer to appropriate representation information such as file format information, taking into account community understandability requirements • Solicit community feedback as to the extent to which preserved information remains understandable	
Risk Relationships:	→R01 [contagious] →R02 [contagious]	
Risk Probability:	4	
Risk Potential Impact:	3	
Risk Severity:	12	

7.3.8 Access and Dissemination

Risk Identifier:	R74	
Risk Name:	Non-availability of information delivery services	
Risk Description:	Repository is unable to provide access to information packages.	
Is this Risk Relevant?:	• What systems are required to provide dissemination services? • Does the repository offer a variety of alternative delivery services? • Do policies and procedures exist to describe the means by which information is disseminated?	
Example Risk Manifestation(s):	• Web server relied upon for dissemination of materials is off-line due to network services failure	
Nature of Risk:	Physical environment	
	Personnel, management and administration procedures	
	Operations and service delivery	X
	Hardware, software or communications equipment and facilities	X
Owner:	Dissemination	
Escalation Owner:	Dissemination	
Stakeholders:	Management; financiers; staff; depositors; users; producers	
Mitigation strategy(ies):	Avoidance strategies: • Define policies describing available information delivery services and communicate these to the user community • Implement appropriate systems to meet delivery policy requirements • Establish sufficiently robust technical infrastructure to satisfy demands of proposed delivery services	
Risk Relationships:	→R01 [contagious] →R02 [contagious] →R79 [contagious]	
Risk Probability:	4	
Risk Potential Impact:	3	
Risk Severity:	12	

Risk Identifier:	R75	
Risk Name:	Authentication subsystem fails	
Risk Description:	Systems for limiting accessibility of information are insufficient, resulting in inappropriate accesses or failures to access.	
Is this Risk Relevant?:	• Is repository compelled by contracts or mandate to establish and maintain a means of limiting end-user access to archived information? • What systems are necessary to maintain the operation of the repository's authentication controls?	
Example Risk Manifestation(s):	• Individuals who are not entitled to have access to the content can access it. Repository system relies upon IP-based authentication, but since all users within University *x* access the web via a web proxy the application perceives any access from that campus as coming from a single IP, and every resident user gains access.	
Nature of Risk:	Physical environment	
	Personnel, management and administration procedures	
	Operations and service delivery	X
	Hardware, software or communications equipment and facilities	X
Owner:	Dissemination	
Escalation Owner:	Dissemination	
Stakeholders:	Management; financiers; staff; depositors; users; producers	
Mitigation strategy(ies):	Avoidance strategies: • Define policies describing authentication requirements to correspond with conditions expressed in deposit agreements and other regulatory, legislative or contextual provisions • Implement appropriate systems to meet authentication policy requirements • Establish sufficiently robust technical infrastructure to satisfy demands of proposed authentication services In the event of risk's execution: • Determine the shortcoming that led to authentication failure and subsequently remedy it • If system is self-aware of its failure, implement a policy to describe the appropriate reaction; for instance, upon failure refuse all access attempts	
Risk Relationships:	→R01 [contagious] →R02 [contagious] →R79 [contagious]	
Risk Probability:	4	
Risk Potential Impact:	3	
Risk Severity:	12	

Risk Identifier:	R76	
Risk Name:	Authorisation subsystem fails	
Risk Description:	Systems to ensure appropriate allocation of system privileges are insufficient, resulting in incorrect rights allocations to users.	
Is this Risk Relevant?:	• Is the repository compelled by contracts or mandate to define and control multiple levels of end-user access? • What systems are necessary to maintain the operation of the repository's authorisation controls?	
Example Risk Manifestation(s):	• Authorisation system which allocates privileges based on database username look-ups fails because two distinct users are permitted to share the same username string	
Nature of Risk:	Physical environment	
	Personnel, management and administration procedures	
	Operations and service delivery	X
	Hardware, software or communications equipment and facilities	X
Owner:	Dissemination	
Escalation Owner:	Dissemination	
Stakeholders:	Management; financiers; staff; depositors; users; producers	
Mitigation strategy(ies):	Avoidance strategies: • Define policies describing authorisation requirements to correspond with conditions expressed in deposit agreements and other regulatory, legislative or contextual provisions • Implement appropriate systems to meet authorisation policy requirements • Establish sufficiently robust technical infrastructure to satisfy demands of proposed authorisation services In the event of risk's execution: • Determine the shortcoming that led to authorisation failure and subsequently remedy it • If system is self-aware of its failure, implement a policy to describe the appropriate reaction; e.g., upon failure restrict all user privileges	
Risk Relationships:	→R01 [contagious] →R02 [contagious] →R79 [contagious]	
Risk Probability:	4	
Risk Potential Impact:	3	
Risk Severity:	12	

Risk Identifier:	R77	
Risk Name:	Inability to validate effectiveness of dissemination mechanism	
Risk Description:	Repository is incapable of effectively determining the extent to which its dissemination mechanisms are successful in terms of its overall business objectives.	
Is this Risk Relevant?:	• Does the repository maintain policies and procedures to verify and record the integrity, authenticity, provenance and understandability of disseminated information? • Does the repository maintain policies and procedures to determine usage rights and limit inappropriate access? • Are mechanisms to determine the effectiveness of delivery operations exploited on a regular basis?	
Example Risk Manifestation(s):	• Repository end-user feedback questionnaires provide a non-exhaustive set of multi-choice responses that restrict the extent to which responses reflect the success of the dissemination	
Nature of Risk:	Physical environment	
	Personnel, management and administration procedures	X
	Operations and service delivery	X
	Hardware, software or communications equipment and facilities	X
Owner:	Dissemination	
Escalation Owner:	Dissemination	
Stakeholders:	Management; financiers; staff; depositors; users; producers	
Mitigation strategy(ies):	Avoidance strategies: • Establish internal means of assessment including risk management • Seek relevant external certification in order to demonstrate effectiveness of dissemination	
Risk Relationships:	→R01 [contagious] →R02 [contagious] →R19 [contagious]	
Risk Probability:	4	
Risk Potential Impact:	3	
Risk Severity:	12	

Risk Identifier:	R78	
Risk Name:	Loss of performance or service level	
Risk Description:	Repository is incapable of meeting service level goals in accordance with its business objectives.	
Is this Risk Relevant?:	• Does repository make a commitment to its stakeholder groups to offer a minimal level of service or performance?	
Example Risk Manifestation(s):	• Repository aims to deliver each object in less than 5 minutes after the request but it consistently takes 10 minutes per object	
Nature of Risk:	Physical environment	
	Personnel, management and administration procedures	X
	Operations and service delivery	X
	Hardware, software or communications equipment and facilities	
Owner:	Dissemination	
Escalation Owner:	Dissemination	
Stakeholders:	Management; financiers; staff; depositors; users; producers	
Mitigation strategy(ies):	Avoidance strategies: • Define realistic service levels and implement policies and procedures for their review and adjustment • Secure and allocate resources based on business priorities • Establish mechanisms to regularly review and if necessary adjust policies and procedures in order to ensure objectives are realised In the event of risk's execution: • Undertake appropriate internal enquiries to determine the shortcomings that led to failure and update policies accordingly	
Risk Relationships:	→R01 [contagious] →R02 [contagious] →R04 [contagious]	
Risk Probability:	4	
Risk Potential Impact:	3	
Risk Severity:	12	