DCC

CARDIO

collaborative assessment of research data infrastructure and objectives

Collaborative Assessment of Research Data Infrastructure and Objectives (CARDIO)

Workflow Planning and Documentation

Table of Contents

Foreword – Using this Document

This document is designed to introduce the **Collaborative Assessment of Research Data Infrastructure and Objectives (CARDIO)** workflow, and can also be used as an instrument for collecting responses throughout the process.

CARDIO is a tool and associated workflow for performing data management **benchmarking** across a data context that may range in size from a small project to a complete institution. It supports, and requires, a **collaborative** approach to contextual benchmarking, ensuring that everyone has their say and that perceptions are given a significance as great as organisational realities. CARDIO enables benchmarking against a **consolidated collection of real world data**, via the DCC CARDIO Knowledgebase, itself intended to evolve on the basis of further community engagement.

Like the CARDIO workflow, the main part of this document is divided into three principal sections, as follows:

- **Organisation:** Issues surrounding administration, policy and legal accountability;
- **Technology:** Issues surrounding technological infrastructure and information security;
- **Resources**: Issues surrounding adequacy of staffing and financial sustainability.

Within each, participants are encouraged to consider the level of capacity evident within their own data context across a range of issues. Each assessment contributes to an overall evaluation of data management maturity. To support this evaluation, a range of statements, intended to be indicative of a range of maturity levels is provided for each issue. Participants can determine which appears closest to their own circumstances in selecting a particular rating:

1		2		3	✓	4		5	
Data ownership is unclear		Ownership of data is assigned ad hoc		A basic policy and guidance on data ownership is in place		Data ownership is routinely documented		Systems to define ownership and license data function well	
Nobody accepts responsibility for data management		Responsibility for data management is implied but not explicit		Some individuals accept responsibility for data management but gaps exist - some data management activities lacking		Roles and responsibilities for data management are well defined Individuals accept their responsibilities and take them seriously		There is a co-ordinated approach to data management across roles	

Table 1: Example Maturity Table

Additional fields are available to record further **justifications** for particular ratings and to note the names of individuals with appropriate insight to act as **nominated experts** in any given area. More detailed examples of associated **risks** and **objectives**, and of things that an organization may **do** or **put in place**, **policies they may establish** and **rights and responsibilities** that they should perhaps be aware of are available in the corresponding section of this document's appendices. These and their page number(s) are referenced on each form.

Section 1 – Organisation

Organisational infrastructure covers the policies, procedures, systems, and skills needed for research data management. The key underlying question is:

- **Are the policies and systems in place sufficiently well known, understood and implemented to ensure research data are effectively managed and shared?**

Contents

Appendices

Data Ownership and Management

Critical questions:

- Who owns data and associated documentation?
- Who has responsibility for data management?
- To what extent are roles and responsibilities defined and accepted?

Maturity rating:

1		2		3		4		5	
Data ownership is unclear		Ownership of data is assigned ad hoc		A basic policy and guidance on data ownership is in place		Data ownership is routinely documented		Systems to define ownership and license data function well	
Nobody accepts responsibility for data management		Responsibility for data management is implied but not explicit		Some individuals accept responsibility for data management but gaps exist - some data management activities lacking		Roles and responsibilities for data management are well defined Individuals accept their responsibilities and take them seriously		There is a co-ordinated approach to data management across roles	

Justification for maturity rating

Nominated experts

More help

More relevant considerations (including associated objectives, risks and suggested best practice requirements) are available on page 40 of this document.

Data Policies and Procedures

Critical questions:

- Does the organisation have written policies for data management and sharing?
- Are policies implemented?

Maturity rating:

1	2	3	4	5
Data management and sharing are not considered	Local guidelines or unwritten rules for data management may be in place	Data policies are formalised	Policies are supported by tools, guidance and infrastructure	Data policies are ratified, well communicated and adopted Data management and sharing is effective

Justification for maturity rating

Nominated experts

More help

More relevant considerations (including associated objectives, risks and best practice requirements) are available on page 42 of this document.

Data Policy Review

Critical questions:

- Are policies reviewed and updated?
- Is the policy in line with wider context?
- Are updates reflected in new procedure?

Maturity rating:

1		2		3		4		5	
Data policies aren't revisited (if they exist at all)		Data policies are periodically reviewed		The data management landscape is monitored to inform policy changes		Updates to data policy are well communicated and support is given for implementation		Amendments to the data policy are reflected in new procedures The data policy continues to be referenced as a model of good practice	

Justification for maturity rating

Nominated experts

More help

More relevant considerations (including associated objectives, risks and best practice requirements) are available on page 43 of this document.

Sharing of Research Data / Access to Research Data

Critical questions:

- Are there systems in place to control access to data?
- Do you know of requirements to share data?
- Are there systems in place to share data?
- Are data accessed and shared in conformance with requirements?

Maturity rating:

1	2	3	4	5
Individuals store data and manage access requests	Guidance and services are provided for data access but are poorly used	A mix of systems is in place to meet different access needs (e.g. shared storage, laptops, portable storage, commercial services) Security is often questionable due to the varied working practices	Access is systematically controlled in all cases through user rights and strong passwords	Data can be accessed when needed and security is maintained Systems meet all user needs (e.g. remote access, sharing with external collaborators etc)
Low awareness of data sharing requirements	Ad hoc data sharing occurs (e.g. data provided on request)	Data sharing is supported - training is provided and the necessary infrastructure is in place	Data are shared as appropriate (i.e. where legally and ethically possible) Support and infrastructure for data sharing functions well and is broadly adopted	There is a culture of openness Data sharing systems are recognised and copied by others

Justification for maturity rating

Nominated experts

More help

More relevant considerations (including associated objectives, risks and best practice requirements) are available on page 44 of this document.

Preservation and Continuity of Research

Critical questions:

- Does the institution understand and plan for preservation?
- Do you know of requirements to preserve data?
- Is there a process to select data for long term preservation?
- Is there an infrastructure for long term data management and preservation?

Maturity rating:

1	2	3	4	5
Low awareness of requirements to preserve data	Data may remain available but mostly due to chance than as a consequence of active preservation practice	Preservation is understood and well planned	High levels of awareness and engagement e.g. data are selected for preservation; active management of data over time; repositories / data centres exist	Data are efficiently and effectively preserved The infrastructure in place is understood, functions well and is widely used

Justification for maturity rating

Nominated experts

More help

More relevant considerations (including associated objectives, risks and best practice requirements) are available on page 46 of this document.

Internal Audit of Research Activities

Critical questions:

- Are the research activities and resulting data well documented?
- Do you know what data you hold and where it is?
- Do you know how data are used?

Maturity rating:

1		2		3		4		5	
Poor awareness of research activities and data outputs		Individuals have pockets of knowledge about certain research projects and datasets but little/no overview		A central record is kept / good documentation is provided on research activities and data		You know (or can easily find out) - What research has been undertaken - What data are held - Where data are held - How data are used		High levels of knowledge exist about research activities and data, and this is routinely put to good use Exemplary systems for research information management	

Justification for maturity rating

Nominated experts

More help

More relevant considerations (including associated objectives, risks and best practice requirements) are available on page 48 of this document.

Monitoring and Feedback of Publication

Critical questions:

- Do you know how your data is used externally?
- Are there data publication policies and procedures?
- Are there data citation guidelines?

Maturity rating:

1		2		3		4		5	
Data are not typically published or made available		Each researcher defines their own publication workflow Little co-ordination or guidelines		Guidelines for publishing and citing data are provided Some support is available		Agreed procedures and mechanisms are in place to publish, link to and cite data		Systems function well to ensure data are published and can be cited Published data are monitored and statistics are logged (e.g. views, citations, feedback)	

Justification for maturity rating

Nominated experts

More help

More relevant considerations (including associated objectives, risks and best practice requirements) are available on page 50 of this document.

Metadata Management

Critical questions:

- Do you understand the need to document data?
- Are research data labelled, annotated and organised?
- Are community norms and standards used where possible?

Maturity rating:

1	2	3	4	5
Metadata is an unfamiliar concept Low engagement with the need to document data	Practice varies by individual – some label, organise and document data well, whereas others don't consider this at all	Metadata is well understood and support/guidance is provided to make sure data are documented Metadata standards are typically used	Data are well labelled, annotated and systematically organised The metadata ensures it is easy for researchers to understand each other's data	Metadata are routinely created and well managed The exemplary practice advances community standards

Justification for maturity rating

Nominated experts

More help

More relevant considerations (including associated objectives, risks and best practice requirements) are available on page 51 of this document.

Legal Compliance

Critical questions:

- Is there an awareness of legislation that affects research data management? e.g. DPA, FoI, EIR, IPR
- Are data managed and shared in line with relevant legislation?
- Are there systems and policies to respond to relevant liabilities?

Maturity rating:

1		2		3		4		5	
Low awareness of relevant legislation		Data may be managed according to legislation at times, but compliance is uncertain and risks high		Guidance and support is available to adhere to relevant legislation Researchers understand how legislation affects data management practice		Policies and associated systems are in place to manage data in line with legislation		Systems are shown to work effectively Staff are aware of legislation and accept various tasks / responsibilities to conform	

Justification for maturity rating

Nominated experts

More help

More relevant considerations (including associated objectives, risks and best practice requirements) are available on page 53 of this document.

Intellectual Property Rights and Rights Management

Critical questions:

- Is it clear who owns data?
- Are data properly licensed for distribution and reuse?
- Are Intellectual Property Rights (IPR) managed appropriately so challenges can be addressed?

Maturity rating:

1	2	3	4	5
Data ownership is unclear	Intellectual Property Rights are assigned ad hoc	Guidance and policies are in place for IPR / data ownership	Data ownership is routinely documented Data are properly licensed for distribution and reuse	Functioning systems are in place so: - ownership is clear - IPR is managed - disputes can be resolved

Justification for maturity rating

Nominated experts

More help

More relevant considerations (including associated objectives, risks and best practice requirements) are available on page 54 of this document.

Disaster Planning and Continuity of Research

Critical questions:

- Are procedures in place to avoid data loss from technological failure?
- Have fallback options been considered for potential risks so research can continue?
- Are sustainability plans in place to safeguard data and ensure continued access?

Maturity rating:

1		2		3		4		5	
Data management activities focus on the day-to-day No thought for long-term or disaster planning		Some awareness of potential data management risks but few take preventative action or have alternatives in place		Policies and plans are in place for disaster recovery and long-term sustainability		Disaster recovery plans are accompanied by procedures for implementation Data loss, a break in the research process, or loss of access to data is unlikely		Disaster recovery plans are routinely tested and shown to be effective Succession plans (e.g. an alternative data centre) are in place to safeguard data	

Justification for maturity rating

Nominated experts

More help

More relevant considerations (including associated objectives, risks and best practice requirements) are available on page 55 of this document.

Section 2 – Technology

Technology covers the requisite equipment, software, hardware, a secure environment, and skills to enable research data management. The key underlying question is:

- **Does the organisation have the necessary technology to satisfy research data management requirements?**

Contents

Appendices

Technological Infrastructure

Critical questions

- Does the technological infrastructure (e.g. network bandwidth, power, storage) meet research data management needs?
- Is there sufficient technological capacity to support the volume of research data?

Maturity rating

1		2		3		4		5	
Technological infrastructure is insufficient to meet data management needs		Technological infrastructure is usually sufficient but has issues e.g. reliability		Satisfactory technological infrastructure in place Capacity is sufficient		Technological infrastructure functions seamlessly and invisibly – it just works		Excellent technological infrastructure that is also flexible and scalable to meet evolving needs	

Justification for maturity rating

Nominated experts

More help

More relevant considerations (including associated objectives, risks and best practice requirements) are available on page 56 of this document.

Appropriate Technologies

Critical questions

- Is the necessary equipment available for research data management?
- Is the necessary software available for research data management?
- Are open standards understood and employed?
- Is data lifespan a consideration when choosing technology?

Maturity rating

1	2	3	4	5
Necessary equipment and/or software for research data management is not available	Some equipment/software for research data management is available There may be insufficient access to the equipment or software, or functionality may be limited	Necessary equipment and/or software is in place	Necessary equipment and/or software is in place and staff are supported in its use	There is a strategy to ensure equipment/software continues to be in place and well supported
Low awareness of appropriate technologies for data management	Individuals may adopt open standards and sustainable technological approaches but there is no coordinated approach	There is an organisational strategy that promotes appropriate technological approaches	Strategy promoting appropriate technologies is understood and implemented across the organisation	There is widespread participation in the development and promotion of appropriate technologies and standards within the institution and beyond

Justification for maturity rating

Nominated experts

More help

More relevant considerations (including associated objectives, risks and best practice requirements) are available on page 57 of this document.

Ensuring Availability

Critical questions

- Are there policies and procedures in place for robust data backup and redundancy?
- Are there policies and procedures in place to synchronise multiple copies of data?
- How is the use of removable or local storage regulated?

Maturity rating

1	2	3	4	5
There is low awareness of the need for data backup and redundancy there is little backing up carried out and there is a high risk of data loss	Backing up is carried out on an ad hoc basis by individuals	A central backup service is provided There are guidelines in place for backing up data	Backup provision meets appropriate standards and is demonstrably robust there is an appreciation of the importance of backup among researchers	Backup is systematically coordinated and managed throughout Backup consists of a rich array of services which are frequently tested and validated

Justification for maturity rating

Nominated experts

More help

More relevant considerations (including associated objectives, risks and best practice requirements) are available on page 59 of this document.

Managing Data Integrity

Critical questions

- Is data integrity monitored and managed?
- How is data integrity validated and restored?
- How is storage media integrity validated?

Maturity rating

1		2		3		4		5	
Data integrity is poorly understood and rarely considered		Integrity of data and storage media may be manually checked now and again Integrity loss is typically irrecoverable		There are policies and associated processes in place to manage data integrity and address identified errors		Policies are enacted through automated systems that monitor and validate data integrity at regular intervals Integrity loss is effectively mitigated e.g. via backup systems		Systems to monitor and restore data integrity are secure and scalable to cope with increasing demand	

Justification for maturity rating

Nominated experts

More help

More relevant considerations (including associated objectives, risks and best practice requirements) are available on page 60 of this document.

Obsolescence

Critical questions

- Is potential obsolescence a consideration when selecting technologies for data and data management (e.g., formats, systems, hardware and storage media)?
- Are open formats and standards prioritised where applicable?
- How are risks of technological obsolescence identified and resolved?

Maturity rating

1		2		3		4		5	
Poor understanding of the risks of obsolescence		There is some awareness of how to manage obsolescence e.g. by choosing open standards		There is an organisational strategy to ensure data remains accessible and usable		There is a proactive approach to managing obsolescence throughout the organisation		Approaches to obsolescence are widely acclaimed There are significant contributions to wider community understanding	

Justification for maturity rating

Nominated experts

More help

More relevant considerations (including associated objectives, risks and best practice requirements) are available on page 61 of this document.

Managing Technological Change

Critical questions

- How are technology changes planned and implemented?
- How are processes and changes to those processes documented?

Maturity rating

1		2		3		4		5	
Changes occurs in an ad hoc, unplanned manner without reference to the broader context		Technological change and the documentation of new processes is managed at a local level		Technological advances are monitored and changes are implemented in a co-ordinated manner		There is a strategic and forward-thinking approach to anticipate and roll-out the necessary technological changes		Changes are effectively planned, well communicated and implemented with little disruption to working practice	

Justification for maturity rating

Nominated experts

More help

More relevant considerations (including associated objectives, risks and best practice requirements) are available on page 62 of this document.

Security Provisions

Critical questions

- Are there adequate information security policies and procedures in place?
- Are technological risks managed?
- Is access controlled?
- Are security provisions tested?

Maturity rating

1		2		3		4		5	
Security is poorly considered and there is little awareness of exposure to risk		Individual practice threatens security e.g. using memory sticks, laptops, personal email to move/store data		There is a good awareness of security issues and relevant policies and procedures are in place		Good implementation of security policies and access is systematically controlled in all cases		There are excellent security policies, supported by a robust technological infrastructure, both of which are regularly reviewed	

Justification for maturity rating

Nominated experts

More help

More relevant considerations (including associated objectives, risks and best practice requirements) are available on page 63 of this document.

Security Processes

Critical questions

- Are security threats monitored and resolved?
- Is security infrastructure operated and maintained appropriately?

Maturity rating

1		2		3		4		5	
The systems in place to manage security are inadequate. Breaches are frequent and disruptive.		Systems are in place but rely on ongoing good practice by individuals		There are a suite of systems in place to manage security. Threats are dealt with but may still impact on working practice.		Systems are well adopted and function effectively		Security is robustly managed. Threats are monitored, anticipated and handled efficiently without disruption.	

Justification for maturity rating

Nominated experts

More help

More relevant considerations (including associated objectives, risks and best practice requirements) are available on page 64 of this document.

Metadata Tools

Critical questions

- Are appropriate technologies available to create metadata in line with standards?
- Is the process of metadata creation automated where possible?
- Are tools to make use of metadata available?

Maturity rating

1		2		3		4		5	
No tools are available to aid metadata creation and use		Tools are available but metadata creation is a manual and time-consuming process		There is a significant amount of automation, guidance and support to aid metadata creation and management		Metadata tools are well suited to researchers' needs, function well and are adopted widely		A strategy is implemented to maintain good practice and ensure appropriate metadata tools continue to be in place	

Justification for maturity rating

Nominated experts

More help

More relevant considerations (including associated objectives, risks and best practice requirements) are available on page 65 of this document.

Institutional Repository

Critical questions

- Do you have an Institutional Repository that accepts data, not just publications?
- To what extent is the repository embedded in research culture/process?

Maturity rating

1		2		3		4		5	
There is no Institutional Repository for data or appreciation of the benefits it would provide		An Institutional Repository for research data is planned or in development		An Institutional Repository is in place, which accepts data. Researchers are aware of the need to manage data and how the repository supports this.		The Institutional Repository is widely known and well used to manage research data		The Institutional Repository is well embedded within research processes. The repository is recognised within the community and used as an example of good practice.	

Justification for maturity rating

Nominated experts

More help

More relevant considerations (including associated objectives, risks and best practice requirements) are available on page 66 of this document.

Section 3 – Resources

The maintenance and development of a range of resources is required for effective research data management. Elements covered in the Resources section include human resources, financial sustainability, business planning and risk management. The critical underlying questions are:

- **Are sufficient resources in place to ensure research data are effectively managed and shared?**
- **Are the resources suitably developed and sustainable?**

Contents

Appendices

Data Management Costs and Sustainability

Critical questions

- Are the costs associated with data management understood and accounted for?
- Are plans in place to ensure resourcing for data management is sustained?
- Is research data management embedded as a core function and financed appropriately?

Maturity rating

1		2		3		4		5	
Data management costs are not considered		Some aspects of data management costs are understood. Funding is sought to cover these costs.		Data management costs are understood by individuals and reflected in research funding applications		Costs are well understood and budgets incorporate explicit data management allocations.		Controls are in place to ensure the availability of explicit data management funding now and for the foreseeable future.	

Justification for maturity rating

Nominated experts

More help

More relevant considerations (including associated objectives, risks and best practice requirements) are available on page 68 of this document.

Business Planning

Critical questions

- Is data management a consideration when developing business plans?
- Is research data management embedded as a core function of the organisation?

Maturity rating

1		2		3		4		5	
Data management is not a consideration in wider business planning		There is some awareness of the impact of data management but this is not reflected in strategic plans		Proposals exist to exploit opportunities associated with data management		Business planning activities explicitly and systematically consider data management implications		Data management is an intrinsic part of the organisation's business and central to its plans	

Justification for maturity rating

Nominated experts

More help

More relevant considerations (including associated objectives, risks and best practice requirements) are available on page 69 of this document.

Technological Resources Allocation

Critical questions

- Are resources sufficient to ensure sustainability and scalability of technology provision?
- Is technology investment appropriate to data management demands?
- Are staff equipped to fully exploit technological resources?

Maturity rating

1		2		3		4		5	
Technological resources are insufficient to satisfy current data management challenges		Technological resources seem to meet researchers' data management needs but the planning and costing is uncoordinated		Technological resources support researchers' current data management needs and are regularly reviewed. Staff have the skills needed to exploit the technology.		Technological resources are well allocated to support data management needs and consideration is given to how to sustain this.		Data management requirements are assessed and explicitly factored into future technological resource allocation to ensure scalability. Skills are well distributed across the team to ensure technology is fully exploited	

Justification for maturity rating

Nominated experts

More help

More relevant considerations (including associated objectives, risks and best practice requirements) are available on page 70 of this document.

Risk Management

Critical questions

- Does the organisation understand and proactively manage risks associated with data management?
- Is there capacity to mitigate risks when identified?

Maturity rating

1		2		3		4		5	
Risk exposure is not formally evaluated. There is not capacity to identify and mitigate risks.		Risks may be considered locally or in a limited capacity Potential issues such as data loss are poorly understood.		Good understanding of risks associated with poor data management. Organisational policy requires maintenance of a risk register		Systematic risk assessments are undertaken and mitigation strategies are revised accordingly.		Risks are effectively managed and resources are available to respond to risks as identified.	

Justification for maturity rating

Nominated experts

More help

More relevant considerations (including associated objectives, risks and best practice requirements) are available on page 71 of this document.

Transparency of Resource Allocation

Critical questions

- Is it clear how resources are allocated to support research data management?
- Is the income associated with research data management clearly identified and traceable for audit purposes?

Maturity rating

1		2		3		4		5	
Data management funds and resources are not specifically covered in income or expenditure reporting		Some data management costs may be identifiable in budgets but practice is ad hoc		Policies determine how funding should be allocated and available to support data management activity and this is clearly identified		Allocation of data management resources is coordinated and recorded at an organisational level		Allocation of data management resources is completely transparent and evident in policy and documentation	

Justification for maturity rating

Nominated experts

More help

More relevant considerations (including associated objectives, risks and best practice requirements) are available on page 72 of this document.

Sustainability of Funding for Data Management and Preservation

Critical questions

- Are there sustainable financial resources for research data management?
- Are efforts made to seek additional funding sources?
- Are central resources allocated appropriately to support research data management activity?

Maturity rating

1		2		3		4		5	
Resources to support data management are often from short term competitive funding and as such cannot be reliably sustained.		Central resources subsidise research income for research data management		Staff are centrally funded to support data management activities. Plans are in place for sustainable data management support services		Plans for sustainable services are formally supported by the organisation and in the process of being implemented		Enough income is generated to resource data management activity sustainably.	

Justification for maturity rating

Nominated experts

More help

More relevant considerations (including associated objectives, risks and best practice requirements) are available on page 74 of this document.

Data Management Skills

Critical questions

- Do research staff have the skills they need to undertake research data management?
- Is there a sufficient support provision and appropriate alignment of skills with roles?
- Are skills shared within the institution (e.g. to mitigate loss of knowledge due to staff turnover)?

Maturity rating

1		2		3		4		5	
Most staff lack specific data management skills and are poorly equipped to undertake such work		A small number of individuals have data management skills, but their departure would leave a skills gap that would be difficult to fill.		Data management skills are widespread throughout the organisation. Good training and resource allocation ensures data management skills are maintained and sufficient support is provided.		Data management skills are well aligned with roles and formalised in job descriptions A policy of skills sharing encourages the transfer of skills throughout the staffing resource		Dedicated data management support staff are in place and these individuals are widely known across the organisation. Data management training is exemplary and continuously revised to reflect changing demands Skills are habitually and systematically shared through staff talks, workshops and collaborative activity	

Justification for maturity rating

Nominated experts

More help

More relevant considerations (including associated objectives, risks and best practice requirements) are available on page 75 of this document.

Number of Staff for Data Management

Critical questions

- Are there enough members of staff to undertake and/or support research data management?
- Are adequate funds available to maintain necessary staff levels?
- Do you understand the staffing requirements to ensure data management success?

Maturity rating

1		2		3		4		5	
The number of staff required has not been considered due to a lack of resources		Some areas are well supported, but generally there are too few people assigned to data management roles to ensure work is carried out adequately		Staffing is currently adequate to undertake basic data management but may need to be increased as requirements change.		Staff numbers are good and there is some forward planning to ensure these levels are maintained.		Staff levels are well managed and contingency funding is available to ensure additional staff resource can be procured as required	

Justification for maturity rating

Nominated experts

More help

More relevant considerations (including associated objectives, risks and best practice requirements) are available on page 76 of this document.

Staff Development Opportunities

Critical questions

- Do staff have access to data management training and other development opportunities?
- Is the training appropriate and up to date?
- Are staff development needs identified, monitored and responded to?

Maturity rating

1		2		3		4		5	
No resource is available to support staff development		Needs are only identified when individuals request training Relevant opportunities exist in some cases but skills are often lacking		A satisfactory staff development budget is available and an appropriate range of development opportunities are provided.		Specific data management training is available and widely promoted. Staff development needs are regularly evaluated and responded to through improved development opportunities		Staff development is evident as a result of systematic review and excellent training provision Dedicated funds are allocated to staff development, ensuring skills levels are sustained	

Justification for maturity rating

Nominated experts

More help

More relevant considerations (including associated objectives, risks and best practice requirements) are available on page 77 of this document.

Section 4 - Appendices

The appendices of these document present tables of example information intended to better understand the meaning of "maturity" in each of CARDIO's individual areas, in more practical terms.

These have been compiled by reference to a range of institutional assessments and evaluations undertaken within a range of digital curation and digital preservation projects (including the Digital Curation Centre[1], Digital Preservation Europe[2] and DELOS[3]). Because they are principally derived from work in the area of digital repository audit they tend to anticipate a more traditional repository model of data ingest, management and dissemination, which may not be applicable to every data management context. Nevertheless, the content is not intended to be prescriptive (and nor is it exhaustive), and is instead intended to offer context and inspiration.

Each table corresponds to a single CARDIO area and contains the following information:

1. **Corresponding Objectives:** intended to provide further context, this is a subset of data management objectives considered relevant to this area;
2. **Corresponding Risks:** intended to illustrate some relevant threats that may become more likely or more severe if performance in this area is substandard;
3. **Relevant things to have in place:** these are examples of resources or assets that if acquired or in place may contribute towards improved maturity within this area;
4. **Relevant policy considerations:** these are examples of issues that may be worth formalizing as part of a policy, pertaining to this area;
5. **Relevant rights or responsibilities:** these are examples of rights and responsibilities (which may derive from legislation, contracts or from more local regulations or mandates) that may be indicative of maturity within this area;
6. **Relevant things to do:** these are examples of actions that if undertaken may contribute towards improved maturity within this area.

[1] http://www.dcc.ac.uk
[2] http://www.digitalpreservationeurope.eu
[3] http://www.delos.info

Appendix A – Best practice considerations for *organisation*

Data Ownership and Management

Corresponding Objectives:	Ensure appropriate contractual management	
	Establish and maintain terms of deposit	
	Establish data ownership	
	Establish terms of use	
	Initiate stakeholder dialogue	
	Maintain depositor dialogue	
	Make explicit (and optionally transfer) preservation responsibility	
	Establish ratification of preservation mission from parent or governing entity	
	Physically acquire content	
Corresponding Risks:	Business policies and procedures are unknown	
	Extent of what is within the archival object is unclear	
	Legal liability for breach of contractual responsibilities	
	Legal liability for breach of legislative requirements	
	Legal liability for IPR infringement	
	Loss of confidentiality of information	
	Loss of non-repudiation of commitments	
	Loss of trust or reputation	
	Repository loses mandate	
Relevant Things to Have in Place:	Communication channels	
	Stakeholder relationships	
	Deposit agreement	
	Custodial history records	
	Relationship with partner associations	
	Mandate definition	
Relevant Policy Considerations:	Rights and ownership definitions	
	Policy for negotiation of preservation responsibility	
	Compliance responsibility	
	Policy governing withdrawal of data management responsibility	
	Exemptions to preservation responsibility	

Relevant Rights or Responsibilities:	Data management responsibility	
	Data management rights	
	Selection or acquisition mandate	
	Data management objectives consistent with parent's overall objectives	
Relevant Things to Do:	Log Accessions	
	Engage in dialogue with stakeholder	
	Exchange transfer documentation	
	Accept data management responsibility	
	Negotiate data management mandate	

Data Policies and Procedures

Corresponding Objectives:	Maintain business planning autonomy	
	Define policies and procedures for undertaking backups	
	Define disaster recovery policy	
	Establish and exercise ingest policy	
	Establish and exercise selection policy	
	Establish hardware upgrade policy	
	Establish information security policy	
	Establish media refreshment policy	
	Establish policy transparency	
	Establish software upgrade policy	
Corresponding Risks:	Business objectives not met	
	Business policies and procedures are inefficient	
	Business policies and procedures are unknown	
	Loss of performance or service level	
	Management Failure	
Relevant Things to Have in Place:	Policy documentation	
	Policy makers	
Relevant Policy Considerations:	Business prioritisation areas	
	Policy responsibility	
	Policy for wider data management integration	
	Policy flexibility	
	Policy transparency	
	Policy steering	
Relevant Rights or Responsibilities:	Mandate for policy and procedure discretion	
Relevant Things to Do:	Evaluate and reform policy	
	Evaluate and reform procedures	

Data Policy Review

Corresponding Objectives:	Establish policy review policy	
Corresponding Risks:	Activity is overlooked or allocated insufficient resources	
	Business policies and procedures are inconsistent or contradictory	
	Business policies and procedures are inefficient	
	False perception of the extent of repository's success	
Relevant Things to Have in Place:	Policy review manager	
	Policy stakeholders	
	Historical policy records	
	External policy influences	
Relevant Policy Considerations:	Policy review	
	Policy flexibility	
	Policy development traceability	
	Policy development triggers	
	Policy review due process	
Relevant Rights or Responsibilities:	Mandate for policy and procedure discretion	
Relevant Things to Do:	Manage policy revision	
	Define policy and procedure review triggers	
	Engage internally on policy review	

Sharing of / Access to Research Data

Corresponding Objectives:	Establish conditions for access	
	Establish designated community	
	Establish physical and logical provisions for access	
	Establish relationship between access and archival packages	
	Implement access controls	
	Implement categories of access	
	Monitor access behaviours	
	Monitor unauthorised access	
Corresponding Risks:	Community requirements change substantially	
	Community requirements misunderstood or miscommunicated	
	Non-availability of information delivery services	
	Non-discoverability of information objects	
	Shortcomings in semantic or technical understandability of information	
Relevant Things to Have in Place:	Communication channels	
	Redistribution rights	
	Catalogue	
	Closed data policy	
	Access platform	
	Access validation system	
	Access personalisation system	
	Terms of access/use	
	Access control system	
	Access processing system	
	User database	
	Discovery metadata	
Relevant Policy Considerations:	Understandability	
	Terms of access	
	Policy on access control	
	Service level	
	Designated community definition	
	Content closure	
	Cost model for access provision	
Relevant Rights or	Has mandated data sharing triggers	

Responsibilities:	Has mandated data sharing responsibilities	
	Has mandated data closure responsibilities	
Relevant Things to Do:	Document public release of dataset	
	Anonymise data	
	Communicate service disruption	
	Regulate dataset closure	
	Disseminate content and metadata	
	Monitor user requirements	
	Monitor access	
	Regulate access to data	

Preservation and Continuity of Research Data

Corresponding Objectives:	Adopt appropriate preservation formats	
	Limit data loss incidence	
	Establish and exercise ingest policy	
	Establish and exercise selection policy	
	Establish conditions for access	
	Establish criteria for data identification	
	Establish criteria for data review	
	Establish criteria for disposal	
	Establish levels of preservation	
	Exercise preservation plans	
	Plan for preservation	
	Select and appraise ingested content	
	Select preservation strategies	
	Establish means to track data object through preservation workflow/lifecycle	
Corresponding Risks:	Ambiguity of understandability definition	
	Archival information cannot be traced to a received package	
	Business fails to preserve essential characteristics of digital information	
	Loss of authenticity of information	
	Loss of information reliability	
	Loss of trust or reputation	
	Preservation plans cannot be implemented	
	Preservation strategies result in information loss	
	Shortcomings in semantic or technical understandability of information	
Relevant Things to Have in Place:	Representation information registry	
	Preservation capacity	
	Preservation plan	
	Preservation policy	
	Preservation management system	
	Preservation validation system	
	Package relationship documentation	
	Understandability definition	
	Glossary of preservation terminology	
Relevant Policy	Policy on relationship between ingest, archival and dissemination packages	

Considerations:	Policy describing designated community	
	Preservation prioritisation	
	Review of designated community	
	Preservation package structure	
	Preservation level assignment	
	Preservation level implications	
	Preservation strategy	
	Preservation validation	
	Data representation	
	Discontinuing preservation	
Relevant Rights or Responsibilities:	Has preservation rights	
	Has preservation discretion	
	Has preservation responsibility	
Relevant Things to Do:	Link preserved content with original	
	Verify characteristics of data	
	Reference external sources during data management planning	
	Identify data properties	
	Establish preservation plan	
	Execute preservation plan	
	Evaluate preservation plan	
	Log object lifecycle	
	Establish referential integrity	
	Monitor designated community evolution	

Internal Audit of Research Activities

Corresponding Objectives:	Authenticate source of ingested packages	
	Monitor access behaviours	
	Monitor unauthorised access	
	Establish means to track data object through preservation workflow/lifecycle	
Corresponding Risks:	Archival information cannot be traced to a received package	
	Documented change history incomplete or incorrect	
	Extent of what is within the archival object is unclear	
	Inability to validate effectiveness of dissemination mechanism	
	Inability to validate effectiveness of ingest process	
	Inability to validate effectiveness of preservation	
	Incompleteness of submitted packages	
	Non-traceability of received, archived or disseminated package	
	Structural non-validity or malformedness of received packages	
	Unidentified information change	
	Unidentified security compromise, vulnerability or information degradation	
Relevant Things to Have in Place:	Acquisition tracking system	
	Communication records	
	Data transformation plans	
	Processing record	
	Custodial history record	
	Peer evaluator	
Relevant Policy Considerations:	Content removal/deletion	
	Content change	
	Policy on relationship between ingest, archival and dissemination packages	
	Process/infrastructure review	
	Data review	
	Documentation review	
Relevant Rights or Responsibilities:	Sufficiency and suitability of audit practice	
Relevant Things to Do:	Assign a processing record to data	
	Document interactions surrounding dataset	
	Document package content	
	Document package structure	

	Record system changes	
	Record media movement	
	Audit collections and procedures	

Monitoring and Feedback of Publication

Corresponding Objectives:	Maintain end user dialogue	
	Monitor access behaviours	
	Monitor and respond to designated community evolution	
	Monitor unauthorised access	
Corresponding Risks:	Community feedback not acted upon	
	Community feedback not received	
	Inability to evaluate repository's successfulness	
	Inability to validate effectiveness of dissemination mechanism	
	Inability to validate effectiveness of preservation	
Relevant Things to Have in Place:	End user focus group	
	Feedback mechanism	
	Terms of use	
	Access/use logger	
Relevant Policy Considerations:	Policy on relationship between ingest, archival and dissemination packages	
	Policy describing designated community	
	Use/preservation level relationship	
Relevant Rights or Responsibilities:	Has stakeholder management responsibility	
Relevant Things to Do:	Monitor dataset usage	
	Monitor user satisfaction	
	Monitor user requirements	
	Monitor data citations and reuse	

Metadata Management

Corresponding Objectives:	Define ingest package specification	
	Document archival data	
	Backup documentation	
	Establish archival packages configuration(s)	
	Establish means for data identification	
	Maintain archival package referential integrity	
	Maintain link between data and metadata	
	Manage formation of dissemination package	
	Record and maintain descriptive metadata	
	Record and maintain representation information	
	Record appropriate metadata	
Corresponding Risks:	Archival information cannot be traced to a received package	
	Business fails to preserve essential characteristics of digital information	
	Destruction of primary documentation	
	Documented change history incomplete or incorrect	
	Extent of what is within the archival object is unclear	
	Identifier to information referential integrity is compromised	
	Incompleteness of submitted packages	
	Loss of authenticity of information	
	Loss of information provenance	
	Metadata to information referential integrity is compromised	
	Non-discoverability of information objects	
	Non-traceability of received, archived or disseminated package	
	Preservation plans cannot be implemented	
	Shortcomings in semantic or technical understandability of information	
	Structural non-validity or malformedness of received packages	
Relevant Things to Have in Place:	Metadata management system	
	Package specification documentation	
	Metadata records	
	Metadata standards	
Relevant Policy Considerations:	Policy on relationship between ingest, archival and dissemination packages	
	Metadata format	
	Package specifications	

	Minimal required metadata	
	Documentation review	
	Metadata storage	
	Content versioning	
Relevant Rights or Responsibilities:	Has prescribed minimal metadata requirements	
Relevant Things to Do:	Perform metadata format conversion	
	Link metadata to corresponding data	
	Automate metadata extraction	
	Define package specifications	
	Publish package specifications	
	Review metadata	

Legal Compliance

Corresponding Objectives:	Ensure appropriate contractual management	
	Monitor and fulfil freedom of information responsibilities	
	Monitor and fulfil other legislative and legal responsibilities	
Corresponding Risks:	Legal liability for breach of contractual responsibilities	
	Legal liability for breach of legislative requirements	
	Liability for non-adherence to financial law or regulations	
	Liability for regulatory non-compliance	
Relevant Things to Have in Place:	Formal contracts/terms	
	Legislation	
	Legal advice	
	Data security enforcement	
Relevant Policy Considerations:	Content selection/acceptance	
	Legal requirements/due process	
	Legal responsibilities	
	Content modification	
	Policy on content availability	
Relevant Rights or Responsibilities:	Has limitation of liabilities	
	Has legal responsibility to manage data	
	Has responsibility to limit access	
	Has legal responsibility to share data/provide access	
Relevant Things to Do:	Dispose of content/media/metadata	
	Regulate access to data	
	Expose data to access	
	Renegotiate legal basis (mandate)	
	Review legal responsibilities/rights	

Intellectual Property Rights and Rights Management

Corresponding Objectives:	Establish data ownership	
	Make explicit (and optionally transfer) preservation rights	
	Monitor and fulfil IPR responsibilities	
Corresponding Risks:	Legal liability for IPR infringement	
	Loss of confidentiality of information	
Relevant Things to Have in Place:	Copyright trigger	
	Rights database	
	Legal expertise	
	Copyrighting mechanism	
Relevant Policy Considerations:	Data rights transfer	
	Copyright/access restrictions	
	Policy covering distribution of copyright material	
	Copyright challenge response	
	Copyright in collection	
Relevant Rights or Responsibilities:	Has mandate to manage/distribute copyright materials	
	Has restrictions on data management/distribution based on copyright status	
Relevant Things to Do:	Monitor copyright status	
	Evaluate data copyright status	
	Respond to IPR challenge	

Disaster Planning and Continuity of Research

Corresponding Objectives:	Establish suitability of backup infrastructure through testing	
	Establish appropriate business planning	
	Establish appropriate contingency funding	
	Establish assurances of recoverability of any lost data	
	Define disaster recovery policy	
	Establish relationships with succession partners	
	Establish appropriate strategies for facilitating succession of organisation or content	
Corresponding Risks:	Accidental system disruption	
	Destruction or non-availability of repository site	
	Enforced cessation of repository operations	
	Local destructive or disruptive environmental phenomenon	
	Repository loses mandate	
Relevant Things to Have in Place:	Contingency fund	
	Succession partner agreement	
	Redundant data/system site(s)	
	Membership of partners' network	
	Disaster plan	
Relevant Policy Considerations:	Content/system redundancy	
	Contract/mandate cessation	
	Succession responsibilities	
	Succession arrangement	
	Preservation commitment	
	Disaster planning	
Relevant Rights or Responsibilities:	Has restrictions on termination of data management responsibilities	
	Has rights to defer data management responsibility	
	Succession partnership agreement	
Relevant Things to Do:	Establish succession arrangements	
	Perform test system recoveries	
	Maintain redundant systems/data	

Appendix B – Best practice considerations for *technology*

Technological Infrastructure

Corresponding Objectives:	Establish hardware upgrade policy	
	Establish software upgrade policy	
	Establish appropriate hardware infrastructure	
	Establish appropriate software infrastructure	
	Establish assurances of sufficiency of staff skills and capacity	
Corresponding Risks:	Authentication subsystem fails	
	Authorisation subsystem fails	
	Hardware failure or incompatibility	
	Non-availability of core utilities	
	Non-availability of information delivery services	
	Software failure or incompatibility	
	Ingest subsystem fails	
Relevant Things to Have in Place:	Technical community and literature	
	Changelog	
	System maintenance/support agreement	
	Update/upgrade prompts	
Relevant Policy Considerations:	Media refreshment	
	Technology licensing	
	Supported systems/applications	
	Systems development management	
	Technology skills development	
Relevant Things to Do:	Report technical status	
	Review technical provision	
	Liaise with technology provider	
	Plan and execute system upgrades	
	Refresh media/hardware	
	Record system changes	
	Develop technical training/induction	

Appropriate Technologies

Corresponding Objectives:	Establish logical storage provisions	
	Establish means for data disposal	
	Establish physical and logical provisions for access	
	Establish appropriate hardware infrastructure	
	Implement access controls	
	Physically acquire content	
	Process ingested content	
	Select preservation strategies	
	Establish appropriate software infrastructure	
	Establish assurances of availability of appropriate technical skills	
Corresponding Risks:	Business objectives not met	
	Enforced cessation of repository operations	
	Hardware or software incapable of supporting emerging repository aims	
	Non-availability of information delivery services	
	Preservation plans cannot be implemented	
Relevant Things to Have in Place:	Backup platform	
	Security platform	
	Ingest platform	
	Access platform	
	Preservation platform	
	Storage platform	
	Administration platform	
	Network	
	General hardware	
	Media support	
	Format support	
	General software	
Relevant Policy Considerations:	Supported ingest formats	
	Supported preservation formats	
	User competency requirements	
	Logical storage	
	Physical storage	
	Policy on supported access types	

	Ingest mechanism	
	Content representation	
	Metadata representation	
	Supported dissemination formats	
	Preservation mechanism	
Relevant Things to Do:	Maintain ingest platform	
	Maintain network protocol support	
	Maintain authentication platform	
	Maintain storage platform	
	Maintain backup platform	
	Maintain authorisation platform	
	Maintain access platform	
	Maintain preservation platform	
	Maintain administration platform	
	Maintain generic/shared technology	

Ensuring Availability

Corresponding Objectives:	Establish appropriate provisions for backup	
	Establish appropriate backup redundancy provisions	
	Establish appropriate backup remoteness provisions	
	Establish suitability of backup infrastructure through testing	
	Ensure synchronisation of data separated by time or space	
	Establish appropriate database backup infrastructure	
	Define policy and procedures for undertaking backups	
	Backup documentation	
Corresponding Risks:	Inconsistency between redundant copies	
	Loss of availability of information and/or service	
	Loss of trust or reputation	
	Loss or non-suitability of backups	
Relevant Things to Have in Place:	Redundant utilities	
	Secure storage location	
	Backup media	
	Identifier resolver	
	Redundant storage	
	Backup/recovery management system	
Relevant Policy Considerations:	Identification/naming	
	Policy on backup location	
	Policy on backup frequency	
	Backup strategy	
	Policy on contents of backup package	
	Required redundancy	
	Recovery drills	
Relevant Things to Do:	Validate content	
	Duplicate content	
	Duplicate systems	
	Duplicate metadata	
	Synchronise redundant data	
	Undertake test recovery	
	Manage unique identification	

Managing Data Integrity

Corresponding Objectives:	Validate integrity of backups	
	Continuously validate data integrity	
	Maintain archival package referential integrity	
	Maintain data integrity	
	Validate data integrity	
	Verify ingest package conformity with specification	
Corresponding Risks:	Identifier to information referential integrity is compromised	
	Loss of authenticity of information	
	Loss of integrity of information	
	Metadata to information referential integrity is compromised	
Relevant Things to Have in Place:	Package relationship documentation	
	Package specification documentation	
	Generated fixity values	
	Depositor fixity values	
	Validation system	
Relevant Policy Considerations:	Ingest specification	
	Validation checks/requirements	
	Specification for archival packages	
	Dissemination specification	
	Specification relationships	
Relevant Things to Do:	Scan for viruses	
	Generate fixity information	
	Validate content	
	Validate media/storage	
	Manage package specifications	

Obsolescence

Corresponding Objectives:	Adopt appropriate preservation formats	
	Classify archival data	
	Establish list of supported formats	
	Establish means for data review	
	Establish media refreshment policy	
	Exercise preservation plans	
	Monitor file format obsolescence	
	Plan for preservation	
	Select preservation strategies	
Corresponding Risks:	Loss of availability of information and/or service	
	Media degradation or obsolescence	
	Obsolescence of hardware or software	
	Preservation strategies result in information loss	
	Shortcomings in semantic or technical understandability of information	
Relevant Things to Have in Place:	Format documentation	
	Obsolescence metric	
	Means for format/media representation	
	Media degradation diagnosis tools	
Relevant Policy Considerations:	Preservation level implications	
	Supported ingest formats	
	Supported preservation formats	
	Format migration	
	Media refreshment	
	Risk assessment validation	
	Obsolescence risk tolerance	
	Supported dissemination formats	
Relevant Things to Do:	Verify data formats	
	Migrate format/media	
	Evaluate format/media risks	
	Manage format/media support	

Managing Technological Change

Corresponding Objectives:	Establish hardware upgrade policy	
	Establish software upgrade policy	
	Establish appropriate technical documentation base	
Corresponding Risks:	Business policies and procedures are inconsistent or contradictory	
	Documented change history incomplete or incorrect	
	Loss of information provenance	
	Unidentified information change	
	Unidentified security compromise, vulnerability or information degradation	
Relevant Things to Have in Place:	Change management system	
	Stakeholder liaison forum	
	Changelog	
Relevant Policy Considerations:	Policy on circumstances that provoke change	
	Procedure for change management	
	Policy for documenting change	
Relevant Things to Do:	Record changes	
	Test effects of changes	
	Plan and execute system upgrades	

Security Provisions

Corresponding Objectives:	Establish information security policy	
	Establish appropriate physical security provisions	
	Establish assurances of site stability	
Corresponding Risks:	Deliberate system sabotage	
	Exploitation of security vulnerability	
	Loss of performance or service level	
	Physical intrusion of hardware storage space	
Relevant Things to Have in Place:	Alarm system	
	Room access system	
	Physical security monitoring	
	Secure safe	
	Weather protection system	
	Fire detection/suppression	
	Ambient environment sensors	
	Moisture detection/mitigation	
Relevant Policy Considerations:	Physical security responsibility	
	Content access levels	
	Physical security measures	
	Security failure defaults	
	Physical access authorisation	
Relevant Things to Do:	Securely store data/media	
	Liaise with security provider	
	Monitor security status	
	Evaluate physical security threats	
	Log actions and interactions	
	Log unauthorized access attempts	

Security Processes

Corresponding Objectives:	Authenticate source of ingested packages	
	Establish information security policy	
	Implement access controls	
	Implement categories of access	
	Establish appropriate logical security provisions	
Corresponding Risks:	Authentication subsystem fails	
	Authorisation subsystem fails	
	Deliberate system sabotage	
	Exploitation of security vulnerability	
	Externally motivated changes or maintenance to information during ingest	
	Loss of authenticity of information	
	Loss of information reliability	
	Loss of integrity of information	
	Loss of trust or reputation	
	Remote or local software intrusion	
Relevant Things to Have in Place:	Logical security monitoring system	
	Secure network infrastructure	
	Authorisation subsystem	
	Authentication subsystem	
Relevant Policy Considerations:	Content access levels	
	Security failure defaults	
	Logical security responsibility	
	Logical security measures	
	Logical authorisation	
Relevant Things to Do:	Liaise with security provider	
	Monitor security status	
	Enforce secure logical environment	
	Log actions and interactions	
	Log unauthorized access attempts	
	Evaluate logical security threats	

Metadata Tools

Corresponding Objectives:	Define ingest package specification	
	Document archival data	
	Document software dependencies	
	Backup documentation	
	Establish archival packages configuration(s)	
	Establish means for data identification	
	Establish naming convention	
	Maintain archival package referential integrity	
	Maintain link between data and metadata	
	Manage formation of dissemination package	
	Record and maintain descriptive metadata	
	Record and maintain representation information	
	Record appropriate metadata	
Corresponding Risks:	Archival information cannot be traced to a received package	
	Destruction of primary documentation	
	Documented change history incomplete or incorrect	
	Identifier to information referential integrity is compromised	
	Loss of information provenance	
	Metadata to information referential integrity is compromised	
	Shortcomings in semantic or technical understandability of information	
Relevant Things to Have in Place:	Metadata schema	
	Metadata creation guidelines	
	Metadata extraction	
Relevant Policy Considerations:	Minimal required metadata	
	Metadata creation workflow	
	Metadata creation responsibility	
Relevant Rights or Responsibilities:	Has prescribed minimal metadata requirements	
Relevant Things to Do:	Document package content	
	Document package structure	
	Create package descriptor	
	Create object metadata	
	Define package specifications	

Institutional Repository

Corresponding Objectives:	Establish appropriate business planning	
	Establish and exercise ingest policy	
	Establish and exercise selection policy	
	Establish and maintain terms of deposit	
	Establish conditions for access	
	Establish levels of preservation	
	Establish transformation procedure from ingest to archival packages	
	Establish appropriate hardware infrastructure	
	Implement access controls	
	Implement categories of access	
	Manage formation of dissemination package	
	Record and maintain descriptive metadata	
	Establish appropriate software infrastructure	
Corresponding Risks:	Authentication subsystem fails	
	Authorisation subsystem fails	
	Business objectives not met	
	Business policies and procedures are inconsistent or contradictory	
	Business policies and procedures are inefficient	
	Business policies and procedures are unknown	
	Enforced cessation of repository operations	
	Hardware failure or incompatibility	
	Hardware or software incapable of supporting emerging repository aims	
	Incompleteness of submitted packages	
	Loss of availability of information and/or service	
	Loss of other third-party contracts/services	
	Management Failure	
	Non-availability of information delivery services	
	Ingest subsystem fails	
Relevant Things to Have in Place:	Acquisition tracking system	
	Content retriever	
	Content processing system	
	Content processing forms	
Relevant Policy	Supported acquisition methods	

Considerations:	Repository integration	
	Selection	
Relevant Rights or Responsibilities:	Has mandate to aggregate published data	
Relevant Things to Do:	Notify data originator of data receipt	
	Request data deposit	
	Retrieve content	
	Aggregate data that's referenced by or contextual to dataset	
	Digitise analogue content	
	Dispose of non-ingested content	
	Refuse content ingest	

Appendix C – Best practice considerations for *resources*

Data Management Costs and Sustainability

Corresponding Objectives:	Establish appropriate financial accounting infrastructure	
	Maintain budget carry-over facility	
	Establish budgetary protection assurances	
	Establish appropriate contingency funding	
	Maintain comprehensive costings breakdown	
	Establish assurances that all costs are and will continue to be covered	
Corresponding Risks:	Business objectives not met	
	Business policies and procedures are inconsistent or contradictory	
	Finances insufficient to meet repository commitments	
	Financial shortfalls or income restrictions	
	Management Failure	
Relevant Things to Have in Place:	Budgetary assurances	
	Income streams	
	Dedicated budget	
	Contingency/reserve fund	
	Expenditure projections	
	Income generation skills	
Relevant Policy Considerations:	Service business model	
	Policy on budgetary management	
	Budgetary separation/autonomy	
	Funding sources	
	Policy on budgetary planning	
Relevant Rights or Responsibilities:	Has assurance of financial sustainability	
Relevant Things to Do:	Seek budgetary assurances	
	Plan expenditure	
	Establish income streams	

Business Planning

Corresponding Objectives:	Establish appropriate business planning	
	Establish appropriate coordination and steering platform	
Corresponding Risks:	Business objectives not met	
	Business policies and procedures are inconsistent or contradictory	
	Business policies and procedures are inefficient	
	Business policies and procedures are unknown	
	Change of terms within third-party service contracts	
	Finances insufficient to meet repository commitments	
Relevant Things to Have in Place:	Contingency fund	
	Management board	
	Business plan	
	Risk register	
Relevant Policy Considerations:	Service breadth/prioritisation	
	Coordination and steering	
	Policy on accountability	
	Policy on business planning	
	Terms of reference	
Relevant Rights or Responsibilities:	Has business steering	
Relevant Things to Do:	Review partnerships and alignments	
	Review business priorities	
	Review business performance	

Technological Resources Allocation

Corresponding Objectives:	Establish appropriate hardware infrastructure	
	Establish appropriate software infrastructure	
	Establish assurances of availability of appropriate technical skills	
Corresponding Risks:	Activity is overlooked or allocated insufficient resources	
	Business objectives not met	
	Hardware failure or incompatibility	
	Hardware or software incapable of supporting emerging repository aims	
	Software failure or incompatibility	
Relevant Things to Have in Place:	Training budget	
	Forum for technical exchange	
	Technical capacity	
	Technical community and literature	
Relevant Policy Considerations:	Technical review	
	Scalability requirements	
	Technology to workflow mapping	
	Service level parameters	
	Technological contingency	
Relevant Things to Do:	Report technical status	
	Review technical provision	
	Technological training/induction	

Risk Management

Corresponding Objectives:	Maintain risk awareness	
Corresponding Risks:	Business objectives not met	
	Finances insufficient to meet repository commitments	
	Loss of availability of information and/or service	
	Loss of performance or service level	
	Loss of trust or reputation	
	Management Failure	
Relevant Things to Have in Place:	Contingency fund	
	Risk register	
	Redundant resources	
	Contingency (non-monetary) resources	
	Risk intelligence data	
Relevant Policy Considerations:	Preservation risks	
	Risk tolerance	
	Risk management	
Relevant Things to Do:	Evaluate risk exposure	
	Maintain risk register	
	Plan for risk mitigation/avoidance	

Transparency of Resource Allocation

Corresponding Objectives:	Establish appropriate financial accounting infrastructure	
	Policy transparency	
	Evaluate and certify activities	
Corresponding Risks:	Business policies and procedures are unknown	
	False perception of the extent of repository's success	
	Inability to evaluate effectiveness of technical infrastructure and security	
	Inability to evaluate repository's successfulness	
	Inability to evaluate staff effectiveness or suitability	
	Inability to validate effectiveness of dissemination mechanism	
	Inability to validate effectiveness of ingest process	
	Inability to validate effectiveness of preservation	
	Loss of information reliability	
	Loss of trust or reputation	
	Negative perception of curation capacity	
Relevant Things to Have in Place:	Stakeholder relationships	
	External evaluators	
	Awarded certifications	
	Documentation discovery system	
	System documentation	
	Data documentation	
	Transaction documentation	
	Policy documentation	
	Business/organisation documentation	
	Quality assurance infrastructure	
Relevant Policy Considerations:	Policy transparency	
	Documentation availability	
	Documentation requirements	
	Evaluation metrics and participants	
	Quality assurance responsibility	
Relevant Rights or Responsibilities:	Has mandated transparency requirement	
Relevant Things to Do:	Undertake independent audit	
	Maintain appropriate documentation	

	Self-evaluate activities	

Sustainability of Funding for Data Management and Preservation

Corresponding Objectives:	Establish budgetary protection assurances	
	Establish appropriate contingency funding	
	Establish assurances that all costs are and will continue to be covered	
Corresponding Risks:	Activity is overlooked or allocated insufficient resources	
	Budgetary reduction	
	Finances insufficient to meet repository commitments	
	Financial shortfalls or income restrictions	
	Loss of other third-party contracts/services	
	Misallocation of finances	
	Loss of budgetary autonomy	
Relevant Things to Have in Place:	Contingency fund	
	Budgetary assurances	
	Income streams	
	Justification of resources	
Relevant Policy Considerations:	Budgetary separation/autonomy	
	Internal budgetary allocation	
	Income/expenditure	
Relevant Rights or Responsibilities:	Has assurance of financial sustainability	
Relevant Things to Do:	Pursue dedicated research funding	
	Develop dedicated budget	
	Develop income streams	
	Justify resources	

Data Management Skills

Corresponding Objectives:	Maintain best practice awareness	
	Establish assurances of sufficiency of staff skills and capacity	
	Establish assurances of availability of appropriate technical skills	
Corresponding Risks:	Business policies and procedures are inefficient	
	Loss of key member(s) of staff	
	Staff suffer deterioration of skills	
Relevant Things to Have in Place:	Dedicated budget	
	Content skills	
	Data management skills	
	Technical skills	
	Management skills	
	Delineated roles and responsibilities	
	Skills monitoring system	
	External skills pools	
Relevant Policy Considerations:	Alignment of roles, skills and function	
	External skills procurement	
	Technology skills development	
Relevant Things to Do:	Procure external expertise	
	Monitor skills gaps	
	Transfer skills	

Number of Staff for Data Management

Corresponding Objectives:	Establish appropriate categories of staff (roles and responsibilities)	
Corresponding Risks:	Business policies and procedures are inefficient	
	Loss of availability of information and/or service	
	Loss of key member(s) of staff	
	Loss of performance or service level	
Relevant Things to Have in Place:	Dedicated budget	
	Employment incentives	
	Employment flexibility	
	Dedicated human resources service	
	Recruitment network	
Relevant Policy Considerations:	Staff turnover	
	Staff resource scalability requirements	
	Recruitment and retention	
	Contract types	
Relevant Things to Do:	Recruit skilled staff	
	Incentivise/retain staff	

Staff Development Opportunities

Corresponding Objectives:	Establish budget dedicated to training provision	
	Establish portfolio of internal or external staff training provisions	
Corresponding Risks:	Inability to evaluate staff effectiveness or suitability	
	Staff skills become obsolete	
Relevant Things to Have in Place:	Training materials and infrastructure	
	Training budget	
	Societies/professional organisations membership	
Relevant Policy Considerations:	Training	
	Professional membership	
Relevant Rights or Responsibilities:	Has mandated staff development requirements	
Relevant Things to Do:	Develop active training plans	
	Monitor training requirements	
	Monitor training opportunities	