**ICP Process structure**

Below are some thoughts on the need for “Risk management” and “planning activities” to run parallel with other ICP process stages. I think you can get away with a “step by step” process structure up until a project hands over to an archive. However if the ICP is to be compliant with TRAC a lot of iterative processes are implied

**Dynamic Elements based on TRAC requirements**

3.1.2.2 The repository shall monitor its organizational environment to determine when to execute its succession plan, contingency plans, and/or escrow arrangements.

3.1.3 The repository shall have a Collection Policy or other document that specifies the type of information it will preserve, retain, manage and provide access to.

3.2.1 The repository shall have identified and established the duties that it needs to perform and shall have appointed staff with adequate skills and experience to fulfil these duties.

3.2.1.1 The repository shall have identified and established the duties that it needs to perform.

3.2.1.2 The repository shall have the appropriate number of staff to support all functions and services.

3.3.1The repository shall have defined its Designated Community and associated knowledge base(s) and shall have these definitions appropriately accessible.

3.3.2 The repository shall have Preservation Policies in place to ensure its Preservation Strategic Plan will be met.

3.3.2.1 The repository shall have mechanisms for review, update, and ongoing development of its Preservation Policies as the repository grows and as technology and community practice evolve

3.3.4 The repository shall commit to transparency and accountability in all actions supporting the operation and management of the repository that affect the preservation of digital content over time.

3.3.5 The repository shall define, collect, track, and appropriately provide its information integrity measurements.

3.4.3 The repository shall have an ongoing commitment to analyze and report on financial risk, benefit, investment, and expenditure (including assets, licenses, and liabilities).

4.1.8 The repository shall have contemporaneous records of actions and administration processes that are relevant to content acquisition.

4.2.5.2The repository shall have tools or methods to determine what Representation Information is necessary to make each Data Object understandable to the Designated Community.

4.2.5.4The repository shall have tools or methods to ensure that the requisite Representation Information is persistently associated with the relevant Data Objects.

4.3.2 The repository shall have mechanisms in place for monitoring its preservation environment.

4.3.2.1 The repository shall have mechanisms in place for monitoring and notification when Representation Information is inadequate for the Designated Community to understand the data holdings.

4.3.3 The repository shall have mechanisms to change its preservation plans as a result of its monitoring activities.

4.3.3.1 The repository shall have mechanisms for creating, identifying or gathering any extra Representation Information required.

4.4.2 The repository shall have contemporaneous records of actions and administration processes that are relevant to storage and preservation of the AIPs.

4.4.2.1 The repository shall have procedures for all actions taken on AIPs.

4.4.2.2 The repository shall be able to demonstrate that any actions taken on AIPs were compliant with the specification of those actions.

4.6.2.1 The repository shall record and act upon problem reports about errors in data or responses from users.

5.1.1.1 The repository shall employ technology watches or other technology monitoring notification systems.

5.1.1.1.2 The repository shall have procedures in place to monitor and receive notifications when hardware technology changes are needed.

5.1.1.1.3 The repository shall have procedures in place to evaluate when changes are needed to current hardware.

5.1.1.1.6 The repository shall have procedures in place to monitor and receive notifications when software changes are needed

5.1.1.1.7 The repository shall have procedures in place to evaluate when changes are needed to current software.

5.1.1.3 The repository shall have effective mechanisms to detect bit corruption or loss.

5.1.1.4 The repository shall have a process to record and react to the availability of new security updates based on a risk benefit assessment.

5.1.1.5 The repository shall have defined processes for storage media and/or hardware change (e.g., refreshing, migration).

5.1.1.6.1 The repository shall have a documented change management process that identifies changes to critical processes that potentially affect the repository’s ability to comply with its mandatory responsibilities.

The implied processes’ at a high level are monitoring (preservation environment, designated community, technologies, semantics, strategic remit of the archive, fixity , media ), risk assessment, planning , preservation action and acquisitions. Which is why I suggest a risk management and planning process which runs in parallel with the other ICP stages.

The conceptual model below was designed to capture the key information which should allow you to manage the preservation state of an archive and supply necessary evidence for audit and certification



The information collected in the entities above is all necessary evidence in terms of TRAC.

**Need for a supporting Risk Standard and Drambora .**

DRAMBORA <http://www.repositoryaudit.eu/> . DRAMBORA having been closely aligned with RAC from the start refer to these areas at a very high level and offers a very generic risk management technique. I believe we require a more in depth standard, which characterise format, hardware software and sematic risk in particular. The risk of “format obsolescence” is too generic ad formats become obsolete/unusable for different reasons. Word document will become obsolete when the majority of the community say 90% no longer use it. However the met office PP format that is highly specialised will become obsolete if we lose the format specification and key expertise from the archive. Resulting monitoring/preservation will therefore be different. The problem is equality complex for software and semantics. Ideally we would want a library of standardised risk characterisations and appropriate preservation strategies.