COMPARISON CHART
(ISO/TRAC/iRODS)

ISO MOIMS-rac	TRAC	TRAC Assessment - iRODS Rules	ISO MOIMS-rac
AUDIT & CERTIFICATION CRITERIA > A. Organizational Infrastructure			
AUDIT & CERTIFICATION CRITERIA > A. Organizational Infrastructure > A1. Governance & organizational viability			
A1.1 Repository has a mission statement that reflects a commitment to the long-term retention of, management of, and access to digital information.	*A1.1*	*17 – Print report - mission statement* *85 – Verify existence of mission statement*	
A1.2 Repository has an appropriate, formal succession plan, contingency plans, and/or escrow arrangements in place in case the repository ceases to operate or the governing or funding institution substantially changes its scope.	*A1.2*	*17 – Print report - succession plan, contingency plan, escrow arrangement* *86 – Verify existence of succession plan, contingency plan and escrow arrangements*	
AUDIT & CERTIFICATION CRITERIA > A. Organizational Infrastructure > A2. Organizational structure & staffing			
A2.1 Repository has identified and		*2 – List rules specific to a collection*	*2 – List rules specific to a*

ISO MOIMS-rac	TRAC	TRAC Assessment - iRODS Rules	ISO MOIMS-rac
established the duties that it needs to perform and has appointed staff with adequate skills and experience to fulfill these duties.		*4 – List micro-services referenced by a rule* *6 – List persistent state information generated by a micro-service Preservation rules include control of transformative migrations, replication, generation of audit trails, verification of assessment criteria, generation of reports, and federation with other archives. The federation rules include specifying which rules and micro-services will be applied to the replicated copy of the AIP. This rule list is the core.irb file.* *17 – Print report - List staffing plan containing number of staff and required training courses* *40 – List staff who have archivist execution permission on collection* *17 – Print report - staff experience report*	*collection(defines duties)* *4 – List micro-services referenced by a rule* *6 – List persistent state information generated by a micro-service. Preservation rules include control of transformative migrations, replication, generation of audit trails, verification of assessment criteria, generation of reports, and federation with other archives. The federation rules include specifying which rules and micro-services will be applied to the replicated copy of the AIP. This rule list is the core.irb file.* *17 – Print report - List staffing plan containing number of staff and required training courses. Correlate staffing plan to preservation rules.* *40 – List staff who have archivist execution permission on collection for each procedure* *17 – Print report periodically - staff experience report*
A2.2 Repository has the appropriate number of staff to support all functions and services.	*A2.2*	*96 – Compare staffing level required by a collection to current staffing*	
A2.3 Repository has an active professional development program in place that provides staff with	*A2.3*	*97 - Compare staffing expertise with collection staffing expertise requirements*	*110 – Assign a development schedule for each staff member* *111 – track progress of each staff member*

ISO MOIMS-rac	TRAC	TRAC Assessment - iRODS Rules	ISO MOIMS-rac
skills and expertise development opportunities.			*on development schedule*
AUDIT & CERTIFICATION CRITERIA > A. Organizational Infrastructure > A3. Procedural accountability & policy framework			
A3.1 Repository has defined its designated community(ies) and associated knowledge base(s) and has publicly accessible definitions and Preservation Policies in place to dictate how its preservation service requirements will be met.	*A3.1*	*56 – Generate report listing all preservation attributes* *2 – List rules specific to a collection* *4 – List micro-services referenced by a rule* *6 – List persistent state information generated by a micro-service*	*56 – Generate report listing all preservation attributes* *2 – List rules specific to a collection* *4 – List micro-services referenced by a rule* *6 – List persistent state information generated by a micro-service* *112 – for each collection, define the knowledge community and designated community* *113 – for each collection, list the service level agreement that defines the required policies*
A3.2 Repository has procedures and Preservation Policies in place, and mechanisms for their review, update, and development as the repository grows and as technology and community practice evolve.	*A3.2*	*23 – Add-modify rule, micro-service, persistent state information* *10 – Generate audit trail for all changes to rules, micro-services, and persistent state information* *17 –Print report - review of plans for updating procedures and policies*	*23 – Add-modify rule, micro-service, persistent state information* *10 – Generate audit trail for all changes to rules, micro-services, and persistent state information* *17 –Print report - review of plans for updating procedures and policies* *114 – periodically print report of current policies for controlling transfer, submission, quality control, storage*

ISO MOIMS-rac	TRAC	TRAC Assessment - iRODS Rules	ISO MOIMS-rac
			management, access, rights management, staffing, security.
A3.3 Repository maintains written Preservation Policies that specify the nature of any legal permissions required to preserve digital content over time, and repository can demonstrate that these permissions have been acquired when needed.	*A3.3*	*17 – Print report – listing of required legal permissions and the associated rules for enforcement* *17 – Print report – listing of the legal permissions that have been obtained*	*115 – for each submission, create a signed list of permissible preservation operations that may be applied (replication, transformative migration, migration, metadata parsing, access, disposition, retention)* *116 – for each collection, compare preservation operations with list of permissible operations, and identify collections at risk*
A3.4 Repository is committed to formal, periodic review and assessment to ensure responsiveness to technological developments and evolving requirements.	*A3.4*	*17 – Print report - periodic assessment by review committee*	*117 – Define sources of information about technology advances, and document periodic technology briefings* *118 – Print report comparing current technology with new technologies*
A3.5 Repository has Preservation Implementation Plans and procedures to ensure that feedback from producers and users is sought and addressed over time.	*A3.5*	*17 – Print report - summarize solicited feedback and modifications to policies and procedures*	*119 – maintain Chat and bugzilla systems to manage requests and track responses*
A3.6 Repository has a documented history of the changes to its operations, procedures, software, and hardware	*A3.6*	*18 – Print audit trail of changes to hardware* *17 – Print report - summarize audit trail of changes to rules, micro-services, and state information* *39 – Verify consistency of assessment*	*120 – print audit trail of changes to policies and procedures, software and hardware* *121 – within each procedure (micro-service) document software used (Doxygen)*

ISO MOIMS-rac	TRAC	TRAC Assessment - iRODS Rules	ISO MOIMS-rac
		criteria across changes and generate a report	
A3.7 Repository commits to transparency and accountability in all actions supporting the operation and management of the repository, especially those that affect the preservation of digital content over time.	*A3.7*	*20 – Set public access controls on reports*	*122 – periodically publish report to chat list that includes all producers, and put reports online*
A3.8 Repository commits to defining, collecting, tracking, and providing, on demand, its information integrity measurements.	*A3.8*	*2 – List rules specific to a collection* *4 – List micro-services referenced by a rule* *6 – List persistent state information generated by a micro-service* *18 – Print audit trail of changes to hardware* *17 – Print report - summarize audit trail of changes to rules, micro-services, and state information* *39 – Verify consistency of assessment criteria across changes and generate a report*	*123 – publish report on integrity assessment that contains results from validation of information integrity*
A3.9 Repository commits to a regular schedule of self-assessment and certification and, if certified, commits to notifying certifying bodies of operational changes that will change or nullify its certification status.	*A3.9*	*102 – Generate periodic evaluation of assessment criteria* *63 – Send report on evaluation of assessment criteria to certifying body*	

ISO MOIMS-rac	**TRAC**	**TRAC Assessment - iRODS Rules**	**ISO MOIMS-rac**
AUDIT & CERTIFICATION CRITERIA > A. Organizational Infrastructure > A4. Financial sustainability			
A4.1 Repository has short- and long-term business planning processes in place to sustain the repository over time.	*A4.1*	*50 – Generate planning approval report for changes to policies and procedures* *51 - Generate report that quantifies cost per Terabyte and compares to funding for collection*	*124 – list financial reports documenting income sources versus expenses, amortization of capital upgrades, reserve assets*
A4.2 Repository has in place processes to review and adjust business plans at least annually.	*A4.2*	*17 – Print report - business plan update report*	
A4.3 Repository's financial practices and procedures are transparent, compliant with relevant accounting standards and practices, and audited by third parties in accordance with territorial legal requirements.	*A4.3*	*17 – Print report - financial audit report*	
A4.4 Repository has ongoing commitment to analyze and report on risk, benefit, investment, and expenditure (including assets, licenses, and liabilities).	*A4.4*	*17 – Print report - financial audit report* *52 - Generate monthly report on risk (list all incidents, date, type of incident, number of files lost, recovery procedure)*	*125 – list risk assessment for perceived threats and planned responses; capital investment planning (amortization); cost benefit analyses; required licenses, contracts, and asset management*
A4.5 Repository commits to monitoring for and bridging gaps in funding.	*A4.5*	*17 – Print report - funding analysis report*	*126 – list federations for ensuring collections have additional supporting repositories*
AUDIT & CERTIFICATION CRITERIA > A. Organizational			

ISO MOIMS-rac	TRAC	TRAC Assessment - iRODS Rules	ISO MOIMS-rac
Infrastructure > A5. Contracts, licenses, & liabilities			
A5.1 If repository manages, preserves, and/or provides access to digital materials on behalf of another organization, it has and maintains appropriate contracts or deposit agreements.	*A5.1*	*87 – Verify existence of Service Level Agreement for each collection* *99 – Compare Service Level Agreement to a Service Level Agreement template* *100 – Compare rules required by a Service Level Agreement for a collection with the rule set actually applied to the collection*	
A5.2 Repository contracts or deposit agreements must specify and transfer all necessary preservation rights, and those rights transferred must be documented.	*A5.2*	*99 – Compare Service Level Agreement to a Service Level Agreement template. Preservation properties include, number of copies, retention period, disposition, replica distribution, frequency of integrity checks, access controls, allowed transformations, required provenance, chain of custody, and a list of the associated rules, micro-services, and state information.* *17 – Print report - Submission document or Service Level Agreement*	
A5.3 Repository has specified all appropriate aspects of acquisition, maintenance, access, and withdrawal in written agreements with depositors and other relevant parties.	*A5.3*	*58– Parse Service Level Agreement or Disposition agreement to extract required risk mitigation policies, retention period, disposition action, and transfer agreement* *88 – Verify collection has set the required risk mitigation policy (number and distribution of copies), retention period, disposition action, and transfer agreement*	

ISO MOIMS-rac	TRAC	TRAC Assessment - iRODS Rules	ISO MOIMS-rac
		flag.	
A5.4 Repository tracks and manages intellectual property rights and restrictions on use of repository content as required by deposit agreement, contract, or license.	*A5.4*	*8 – List all persons with access permissions on collection* *103 – Analyze audit trails to verify identity of all persons accessing the data, and compare their roles with desired access controls* *13 – Generate report listing all persons who accessed or applied archival functions on file*	*127 – store intellectual property right statements and legal requirements for each collection/object* *128 – define access restrictions for each record*
A5.5 If repository ingests digital content with unclear ownership/rights, policies are in place to address liability and challenges to those rights.	*A5.5*	*89 – Verify ownership is set, if not, set restricted access and dispute flag* *68 – Override access restrictions if dispute flag is set and access is by data grid administrator*	*129 – track legal opinions on disputed records*
AUDIT & CERTIFICATION CRITERIA > B. Digital Object Management			
AUDIT & CERTIFICATION CRITERIA > B. Digital Object Management > B1. Ingest: acquisition of content			
B1.1 Repository identifies properties or information content it will preserve for digital objects.	*B1.1*	*2 – List rules specific to a collection* *4 – List micro-services referenced by a rule* *6 – List persistent state information generated by a micro-service* *17 – Print report - preservation metadata template*	*130 – Store submission agreements for each collection or record series* *131 – Store mapping of submission agreement to policies and procedures that will be used to manage the collection*

ISO MOIMS-rac	TRAC	TRAC Assessment - iRODS Rules	ISO MOIMS-rac
B1.2 Repository clearly specifies the information that needs to be associated with digital material at the time of its deposit (i.e., SIP).	*B1.2*	*70 – Store template that defines the structure of a SIP* *59 – Parse SIP and extract descriptive metadata and source*	*132 – store producer-archive submission agreement* *133 – map from submission agreement to required preservation information*
B1.3 Repository has mechanisms to validate the source of all materials.	*B1.3*	*90 – Verify descriptive metadata and source against SIP and set SIP compliance flag*	*134 – track source of each record* *135 – compare source of record with required source specified in submission agreement*
B1.4 Repository's ingest process verifies each submitted object (i.e., SIP) for completeness and correctness as specified in B1.2.	*B1.4*	*90 – Verify descriptive metadata and source against SIP and set SIP compliance flag* *53 – Generate SIP compliance report (check status of SIP compliance flags)*	
B1.5 Repository obtains sufficient physical control over the digital objects to preserve them.	*B1.5*	*67 – Check whether file is master copy and turn off deletion, turn off user access, turn on versioning*	*136 – The submission agreement specifies the physical record components that will be preserved. For each physical record component, a physical copy is made in the archive.*
B1.6 Repository provides producer/depositor with appropriate responses at agreed points during the ingest processes.	*B1.6*	*64 – Send SIP ingestion audit report. Notify producer of all inconsistencies and errors detected in the ingestion process. This requires creating state information for each observed problem, and listing the state information.*	
B1.7 Repository has written policies that indicate when it accepts preservation responsibility	*B1.7*	*66 – Set formal acceptance flag and acceptance date stamp* *44 – List formally accepted files*	*137 – create report of formally accepted records*

ISO MOIMS-rac	TRAC	TRAC Assessment - iRODS Rules	ISO MOIMS-rac
for the contents each set of submitted data objects (i.e., SIPs).			
B1.8 Repository has contemporaneous records of actions and administration processes that are relevant to preservation (Ingest: content acquisition).	*B1.8*	*11 – Generate audit trail for each micro-service that is applied to file and list the controlling rule and the resulting state information.*	
AUDIT & CERTIFICATION CRITERIA > B. Digital Object Management > B2. Ingest: creation of the archivable package			
B2.1 Repository has an associated, written definition for each AIP or class of AIP preserved by the repository that is adequate to fit long-term preservation needs.	*B2.1*	*71 – Store template for parsing an AIP* *60 – Parse descriptive metadata from an AIP* *80 – Create an AIP based on the AIP template*	*101 – Compare AIP content with AIP template, and list all non-compliant files* *65 – Replace an AIP template*
B2.3 Repository has a description of how AIPs are constructed from SIPs.	*B2.3*	*82 – Create an AIP template from a SIP template*	*138 – define preservation procedures that are applied to convert a SIP to an AIP*
B2.4 Repository can demonstrate that all submitted objects (i.e., SIPs) are either accepted as whole or part of an eventual archival object (i.e., AIP), or otherwise disposed of in a recorded fashion.	*B2.4*	*54 – Generate Submission report listing all SIPs that were not successfully ingested*	*139 – Maintain record of the SIP from which each AIP is generated*
B2.5 Repository has and uses a naming convention that generates visible, persistent, unique identifiers for all archived objects (i.e., AIPs).	*B2.5*	*22 – Generate a GUID or handle as well as a logical name*	

ISO MOIMS-rac	TRAC	TRAC Assessment - iRODS Rules	ISO MOIMS-rac
B2.7 Repository demonstrates that it has access to necessary tools and resources to establish authoritative Representation Information of the digital objects it contains.	*B2.7*	*73 – Store link to format registry for a collection*	*140 – define the tools that will be used to display and interpret the record, maintaining either a link to the source or a copy of the tool.* *141 – maintain Representation Information as preservation metadata for each record*
B2.9 Repository has documented processes for acquiring preservation metadata (i.e., PDI) for its associated Content Information and acquires preservation metadata in accordance with the documented processes. The repository must maintain viewable documentation on how the repository acquires and manages Preservation Description Information (PDI).	*B2.9*	*79 – Set preservation metadata for an AIP including: size, checksum, logical name, and extract descriptive metadata* *57 – Generate audit trail of all changes to the AIP with date and archivist name.*	*142 – maintain auditable trail to support claims of authenticity, and track unauthorized changes to the digital holdings* *143 – Maintain links between Preservation description information and the record.*
B2.10 Repository has a documented process for testing understandability of the AIP at ingest for their Designated Communities; the repository must bring the AIP up to the agreed level of understandability.	*B2.10*	*91 – Verify descriptive metadata against semantic term list* *74 – Store definitions for each of the semantic terms in the semantic term list for a collection*	*144 – build ontology for the terms used by the Designated Community for validation of vocabulary within the descriptive metadata.* *145 – Validate ability to parse and display records at time of ingestion*
B2.11 Repository verifies each AIP for completeness and correctness at the point it is generated.	*B2.11*	*101 – Compare AIP content with AIP template, and list all non-compliant files*	
B2.12 Repository provides an	*B2.12*	*34 – Validate checksums*	*146 – verify that all records transmitted*

ISO MOIMS-rac	**TRAC**	**TRAC Assessment - iRODS Rules**	**ISO MOIMS-rac**
independent mechanism for inventorying the integrity of the repository collection/content.		*35 – Verify the required number of replicas exist* *31 – Synchronize replicas and generate error report*	*through submission agreements are present in the archive (compare records in vault with PDI metadata).*
B2.13 Repository has contemporaneous records of actions and administration processes that are relevant to preservation (AIP creation).	*B2.13*	*10 – Generate audit trail for all changes to rules, micro-services, and persistent state information* *11 – Generate audit trail for each micro-service that is applied to file along with the controlling rule and the resulting state information.*	
AUDIT & CERTIFICATION CRITERIA > B. Digital Object Management > B3. Preservation planning			
B3.1 Repository has documented preservation strategies relevant to its holdings.	*B3.1*	*2 – List rules specific to a collection* *4 – List micro-services referenced by a rule* *6 – List persistent state information generated by a micro-service. Preservation rules include control of transformative migrations, replication, generation of audit trails, verification of assessment criteria, generation of reports, and federation with other archives. The federation rules include specifying which rules and micro-services will be applied to the replicated copy of the AIP. This rule list is the core.irb file.*	*147 – periodic rules are evaluated to check for degradation of storage media, obsolescence of media drives, obsolescence of Representation Information including formats.* *148 – periodic rules are evaluated to verify mechanisms for mitigating risk of data loss*

ISO MOIMS-rac	**TRAC**	**TRAC Assessment - iRODS Rules**	**ISO MOIMS-rac**
B3.2 Repository has mechanisms in place for monitoring and notification when Representation Information is inadequate for the Designated Community(ies) to understand the data holdings, and mechanisms for creating or identifying or gathering any extra Representation Information required.	*B3.2*	*45 – List records that do not have an allowed data format type* *69 – Assign viability lifetime to each format type in the collection* *46 – List records that have a data format with an expired lifetime*	*149 – update knowledge community ontology to remove obsolete terms and incorporate new terms* *150 – compare Representation Information against revised ontology* *151 – validate ability of new parsing routines to manipulate the records*
B3.3 Repository has mechanisms to change its preservation plans as a result of its monitoring activities.	*B3.3*	*28 – Transform files from non-viable format to a viable format* *27 – Transform file for display* *30 - Migrate collection from an old rule set to a new rule set*	*152 – detect failing storage systems and migrate contents*
B3.4 Repository can provide evidence of the effectiveness of its preservation planning.	*B3.4*	*102 – Generate periodic evaluation of assessment criteria*	*153 – audit all records within archive for compliance with preservation policies*
AUDIT & CERTIFICATION CRITERIA > B. Digital Object Management > B4. Archival storage & preservation/maintenance of AIPs			
B4.1 Repository employs documented preservation strategies.	*B4.1*	*2 – List rules specific to a collection* *4 – List micro-services referenced by a rule* *6 – List persistent state information generated by a micro-service*	*153 – audit all records within archive for compliance with preservation policies*
B4.2 Repository	*B4.2*	*30 - Migrate collection from an old rule set*	

ISO MOIMS-rac	TRAC	TRAC Assessment - iRODS Rules	ISO MOIMS-rac
implements/responds to strategies for AIP bit-level storage and employs the appropriate strategies for maintaining Information content in a format acceptable/usable by the designated community.		*to a new rule set*	
B4.3 Repository preserves the Content Information of AIPs.	*B4.3*	*80 – Create an AIP based on the AIP template*	*154 – verify compliance of AIPs with AIP template (format, semantic terms, parsing application)*
B4.4 Repository actively monitors integrity of archival objects AIPs.	*B4.4*	*34 – Validate checksums* *35 – Verify the required number of replicas exist* *31 – Synchronize replicas and generate error report* *36 - Verify authenticity (all files have metadata, all metadata records point to a file)* *101 - Compare AIP content with AIP template, and list all non-compliant files*	*155 – maintain audit trail on all integrity validation operations performed upon an AIP*
B4.5 Repository has contemporaneous records of actions and administration processes that are relevant to preservation (Archival Storage).	*B4.5*	*10 – Generate audit trail for all changes to rules, micro-services, and persistent state information* *11 – Generate audit trail for each micro-service that is applied to file along with the controlling rule and the resulting state information.* *14 – Generate report summarizing audit trail information for all events applied to a file*	

ISO MOIMS-rac	TRAC	TRAC Assessment - iRODS Rules	ISO MOIMS-rac
AUDIT & CERTIFICATION CRITERIA > B. Digital Object Management > B5. Information management			
B5.1 Repository specifies minimum Description Information requirements to enable the designated community(ies) to discover and identify material of interest.	*B5.1*	*90 - Verify descriptive metadata and source against SIP template and set SIP compliance flag*	*156 – support queries on descriptive metadata*
B5.2 Repository captures or creates minimum Descriptive Information and ensures that it is associated with the AIP.	*B5.2*	*59 – Parse SIP and extract descriptive metadata and source* *79 - Store preservation metadata for an AIP including: size, checksum, logical name, and extract descriptive metadata*	
B5.3 Repository can demonstrate that all AIPs are associated with their descriptive information and there is descriptive information for each AIP.	*B5.3*	*36 - Verify authenticity (all files have metadata, all metadata records point to a file)* *60 - Parse descriptive metadata from an AIP*	
B5.4 Repository can demonstrate that it maintains the associations between its AIPs and their descriptive information.			157 – use logical name spaces to maintain link between descriptive metadata and the AIPs. 158 – use versions to enforce link between original AIP and descriptive metadata
AUDIT & CERTIFICATION CRITERIA > B. Digital Object Management > B6. Access management			

ISO MOIMS-rac	**TRAC**	**TRAC Assessment - iRODS Rules**	**ISO MOIMS-rac**
B6.1 Repository documents what access and delivery options are available.	*B6.1*	*47 – List access mechanisms available for data types present within a collection.* *72 – Store template for mapping AIPs to DIPs* *81 – Create DIP from AIP* *48 – List available transport mechanisms for collection*	2 – List access rules specific to a collection
B6.2 Repository has a documented policy for recording access actions (includes requests, orders etc.) that meet the requirements of the repository and information producers/depositors.	*B6.2*	*11 - Generate audit trail for each micro-service that is applied to a file and list the controlling rule and the resulting state information*	*2 – list audit trail rules specific to a collection*
B6.3 Repository ensures that agreements applicable to access conditions are adhered to.	*B6.3*	*8 – List all persons with access permissions on collection* *103 – Analyze audit trails to verify identity of all persons accessing the data, and compare their roles with desired access controls*	
B6.4 Repository has documented and implemented access policies (authorization rules, authentication requirements) consistent with deposit agreements for stored objects.	*B6.4*	*40– List staff who have archivist execution permission on collection* *8 – List all persons with access permissions on collection* *103 – Analyze audit trails to verify identity of all persons accessing the data, and compare their roles with desired access controls* *13 – Generate report listing all persons who accessed or applied archival functions*	

ISO MOIMS-rac	TRAC	TRAC Assessment - iRODS Rules	ISO MOIMS-rac
		on the collection	
B6.5 Repository access management system fully implements access policy.	*B6.5*	*Generic property – access controls implemented in server-side workflows*	
B6.6 Repository logs all access management failures, and staff review inappropriate "access denial" incidents.	*B6.6*	*61 - Parse access failures from audit trail on data and generate report* *75 – Store review dates of denied access reports*	
B6.7 Repository can demonstrate that the process that generates the requested digital object(s) (i.e., DIP) is completed in relation to the request.	*B6.7*	*62 – Parse audit trail for completion status of all DIP requests*	*159 – status information is returned to user on all access requests, including reasons for partial response*
B6.8 Repository can demonstrate that the process that generates the requested digital object(s) (i.e., DIP) is correct in relation to the request.	*B6.8*	*11 - Generate audit trail for each micro-service that is applied to a file and list the controlling rule and the resulting state information* *72 – Store template for mapping AIPs to DIPs* *81 – Create DIP from AIP*	
B6.9 Repository demonstrates that all access requests result in a response of acceptance or rejection.	*B6.9*	*61 - Parse access failures from audit trail on data and generate report* *62 - Parse audit trail for completion status of all DIP requests*	
B6.10 Repository enables the dissemination of authentic copies of the original or objects traceable to originals.	*B6.10*	*49 - Generate authenticate copy from master (validate checksum before copy and after copy)*	
AUDIT & CERTIFICATION			

ISO MOIMS-rac	TRAC	TRAC Assessment - iRODS Rules	ISO MOIMS-rac
CRITERIA > C. Technologies, Technical Infrastructure, & Security > C1. System infrastructure			
C1.1 Repository functions on well-supported operating systems and other core infrastructural software.	*C1.1*	*55 - Generate list of all storage resources used to store collection and databases used to store the metadata*	
C1.2 Repository ensures that it has adequate hardware and software support for backup functionality sufficient for the repository's services and for the data held, e.g., metadata associated with access controls, repository main content.	*C1.2*	*92 – Verify status of metadata catalog backup (create a snapshot of metadata catalog)* *104 - Rebuild the database from the metadata present within the AIPs.* *105 – Rebuild the database from metadata in a federated archive*	
C1.3 Repository manages the number and location of copies of all digital objects.	*C1.3*	*35 – Verify the required number of replicas exist* *98 - Compare actual storage locations against list of allowed storage locations and report non-compliance* *Generic property – Replica location information registered in metadata catalog*	
C1.4 Repository has mechanisms in place to ensure any/multiple copies of digital objects are synchronized.	*C1.4*	*31 – Synchronize replicas and generate error report*	
C1.5 Repository has effective mechanisms to detect bit corruption or loss.	*C1.5*	*34 – Validate checksums*	
C1.6 Repository reports to its administration all incidents of data corruption or loss, and steps taken	*C1.6*	*52 - Generate monthly report on risk (list all incidents, date, type of incident, number of files lost, recovery procedure)*	

ISO MOIMS-rac	TRAC	TRAC Assessment - iRODS Rules	ISO MOIMS-rac
to repair/replace corrupt or lost data.		*15 – Generate report documenting all errors, date, impact in terms of file loss, recovery procedure*	
C1.7 Repository has defined processes for storage media and/or hardware change (e.g., refreshing, migration).	*C1.7*	*29 – Migrate data to new storage resource*	
C1.8 Repository has a documented change management process that identifies changes to critical processes that potentially affect the repository's ability to comply with its mandatory responsibilities.	*C1.8*	*10 - Generate audit trail for all changes to rules, micro-services, and persistent state information* *39 – Verify consistency of assessment criteria across changes and generate a report* *38 - Verify consistency of rules, micro-services, and persistent state information after changes to policies and procedures*	
C1.9 Repository has a process for testing the effect of critical changes to the system.	*C1.9*	*38 - Verify consistency of rules, micro-services, and persistent state information after changes to policies and procedures. This may require examining all possible combinations of rules for consistency of changes to state information. This can be done by applying rules on a test collection and verifying the results.*	
C1.10 Repository has a process to react to the availability of new software security updates based on a risk-benefit assessment.	*C1.10*	*30 - Migrate a collection from an old rule set to a new rule set* *29 – Migrate data to new storage resource*	*160 – use federation to evaluate impact of new technology while preserving replicas on the old technology*
AUDIT & CERTIFICATION			

ISO MOIMS-rac	**TRAC**	**TRAC Assessment - iRODS Rules**	**ISO MOIMS-rac**
CRITERIA > C. Technologies, Technical Infrastructure, & Security > C2. Appropriate technologies			
C2.1 Repository has hardware technologies appropriate to the services it provides to its designated community(ies) and has procedures in place to receive and monitor notifications, and evaluate when hardware technology changes are needed.	*C2.1*	*16 - Generate audit trail of notifications from user community on problems* *33 – Parse notifications to determine types of problems*	
C2.2 Repository has software technologies appropriate to the services it provides to its designated community(ies) and has procedures in place to receive and monitor notifications, and evaluate when software technology changes are needed.	*C2.2*	*16 - Generate audit trail of notifications from user community on problems* *33 – Parse notifications to determine types of problems* *30 - Migrate a collection from an old rule set to a new rule set* *29 – Migrate data to new storage resource*	
AUDIT & CERTIFICATION CRITERIA > C. Technologies, Technical Infrastructure, & Security > C3. Security			
C3.1 Repository maintains a systematic analysis of such factors as data, systems, personnel, physical plant, and security needs.	*C3.1*	*18 – Print audit trail of changes to hardware* *17 – Print report - summarize audit trail of changes to rules, micro-services, and state information* *39 – Verify consistency of assessment*	*161 – generate a report listing all first class objects* *162 – generate a report that analyzes technology advances and user requests to identify changes needed on first class objects*

ISO MOIMS-rac	TRAC	TRAC Assessment - iRODS Rules	ISO MOIMS-rac
		criteria across changes and generate a report *96 - Compare staffing level required by a collection to current staffing*	
C3.2 Repository has implemented controls to adequately address each of the defined security needs.	*C3.2*	*8 – List all persons with access permissions on collection*	*162 – list all security events and responses*
C3.3 Repository staff have delineated roles, responsibilities, and authorizations related to implementing changes within the system.		*17 – Print report - List staffing plan containing number of staff and required training courses* *17 – Print report - staff experience report* *96 - Compare staffing level required by a collection to current staffing* *103 – Analyze audit trails to verify identity of all persons accessing the data, and compare their roles with desired access controls*	
C3.4 Repository has suitable written disaster preparedness and recovery plan(s), including at least one off-site backup of all preserved information together with an off-site copy of the recovery plan(s).	*C3.4*	*24 – Set federation rules for specifying how rules and micro-services will be applied in remote federation* *32 - Synchronize with a federated archive (replicate user identity, preservation metadata, and records)* *105 - Rebuild the database from metadata in a federated archive*	*160 – use federation to provide risk mitigation against loss of data from all sources*