MINISTRY FOR CULTURE AND HERITAGE

TVNZ ARCHIVE COLLECTION RECORDS MANAGEMENT ASSESSMENT

RELEASED UNDER THE OFFICIAL INFORMATION ACT

5 August 2014

DOCUMENT CONTROL

Revision History

Date	Version	Author	Description
28/07/14	0.1	Michael Upton	First draft for circulation to MCH
31/07/14	0.2	Michael Upton	Second draft following feedback from MCH
04/08/14	0.3	Michael Upton	Third draft reflecting name change of Ngā Taonga
05/08/14	1.0	Michael Upton	Approved final version

Distribution

Name	Title	Document Version	Date
Paul Stone	CIO, MCH	1.0	5/08/14
Katrina Ellwood	Senior Information Management Advisor, MCH	1.0	5/08/14

Document Approval

Name	Title	Document Version	Signature	Date
Paul Stone	CIO, MCH	1.0		5/08/14

RELEASED UNDER THE OFFICIAL INFORMATION ACT

TABLE OF CONTENTS

RELEASED UNDER THE OFFICIAL INFORMATION ACT

1 BACKGROUND AND APPROACH

On the first of August 2014, the TVNZ archive collection is being transferred to the control of The Ministry for Culture and Heritage (MCH). MCH has established an agreement with Ngā Taonga Sound and Vision (the Archive), formerly known as the New Zealand Film Archive, to manage these records. The agreement includes a clause that the Archive will manage the transferred records in accordance with the Public Records Act 2005 (PRA) and relevant standards.

MCH approached Davanti Consulting to provide an independent assessment of the Archive's current capability to manage the TVNZ archive collection in a manner that meets the requirements of the PRA and the associated mandatory standard issued under the Act, the Records Management Standard for the Public Sector (the Standard).

Specifically, in relation to the TVNZ archive collection, Davanti was asked to:

1. Assess the Archive's Collection Management System (the database) against the metadata requirements in the Standard. The database is used to capture information about AV records and supports their ongoing management.
2. Assess the Archive's operations against other operational requirements relevant to the PRA and the Standard.

The scope of the assessment was limited to the Archive's capabilities, so did not include analysis of the current state of the records being transferred to the Archive. MCH also put examination of the physical storage facilities out of scope.

Davanti's approach was based on a principle of assessing as much as possible within a short timeframe, given the reasonably narrow scope, on the understanding that MCH will carry out further analysis and investigation as required. Davanti developed a questionnaire around the content of the Standard and met with Virginia Callanan and Sarah Davy from the Archive to interview them on current practices and to see the database.

The Archive provided the following documents to Davanti, which inform this report:

- Records Management Policy,
- Records Server User Guide,
- Records Security Principles, and
- Privacy Policy.

Additionally, Davanti reviewed the Memorandum between MCH and the Archive regarding the transfer of the TVNZ archive collection, and the Disposal Authority that covers the records in scope.

RELEASED UNDER THE OFFICIAL INFORMATION ACT

2 OVERALL STATEMENT OF FIT TO REQUIREMENTS

Davanti's high level assessment is that the Archive's database and current supporting processes meet the records management requirements of the mandatory Standard for the most part and that none of the compliance gaps identified suggest a significant or immediate business risk beyond non-compliance. There was also no in-scope requirement that the Archive completely or even mostly failed to meet.

The current structure of the database, being purpose developed for the Archive and well managed, will largely support very effective management of the records that comprise the TVNZ archive collection. Its design is informed by archival practices and collection items are described in a practical separation of the intellectual entity (the "Title" record) and any related instantiations of that work ("Materials"), whether they are on physical media or made up of digital files. This allows the Archive to hold information around matters such as rights clearances and production details once for each Title, distinct from more specific details about, for instance, the location or condition of a particular recording.

The database also contains Deposit records and many People records, which could be used to identify the TVNZ archive collection distinct from other collection items managed by the Archive and, if necessary, carry out any actions on them as a set.

The corporate records of the Archive are maintained on the records server, which is a traditional shared file server. This poses the expected challenges of any such an environment, most obviously a lack of records management metadata and audit trails that can be used to defend the authenticity of the records. However, the practice at the Archive seems to be to largely manage any records that relate to collection objects in the database, so any shortcomings of the records server may be largely irrelevant to the records being transferred from TVNZ and any subsequent records created about them.

3 KEY GAPS

This section summarises the key areas where the Archive may require further work to comply with the Standard. These gaps and other more minor points are explored in a subsequent section.

3.1 Metadata management in the database

While point of capture metadata is created and maintained in the database, Requirement 3.1 in the standard also states that subsequent actions related to records need to be recorded, including who carried out the action, what the action was, and when the action occurred. While the database certainly keeps information on who last updated any given record, it would be prudent for MCH to look into what kind of audit trails are captured and whether the information contained is fit for purpose. A full history of actions against each record may exist, but if so this was not observed.

Another gap to examine is regarding the management of records that the Archive will create post-transfer related to the transferred TVNZ archive collection. These will likely be correspondence records related to the collection, clearances and communications with the commissioned creators of the works. Staff can attach PDFs of such records in the database, but from the initial meeting it was unclear what metadata is recorded about these attached

OFFICIAL INFORMATION RELEASED UNDER THE ACT

files, and the extent to which these are managed. For example, it is important to confirm whether they can be modified, overwritten or deleted by staff (see requirements 1.5 and 5.3), whether point of capture metadata or subsequent actions are captured (requirement 3.1), and how easily they can be located and understood (requirement 4.2). Similarly, while meeting records are captured within the database, it seems their integrity is not guaranteed (again, requirements 1.5 and 5.3).

3.2 Other operational

The principal gap that MCH needs to explore in this area also relates to the database. There is an operational risk that comes with keeping core records in a custom-developed application that is supported by one person, and built in the uncommon format of FileMaker Pro. So the gap is not about current state, as such, but rather about this "key person risk".

While the substantial effort that the Archive has put into the custom database likely gives the solution a lot of its strength, it also introduces the potential that if the administrator were to leave (or was otherwise unavailable) that they could not be easily replaced. This could have a large impact on business continuity and may result in missed opportunities if development resources are not available when changes to the database need to be made.

The Standard specifies that "records must be accessible when required" (requirement 4.2) and that "risks to the accessibility of records must be identified and mitigated" (requirement 4.4). If the database fails and the right person is not available to restore access this may have a high impact on accessibility. The Archive may have very limited means to locate and manage access to the records described in the database.

While in the short term such a scenario is unlikely, the risk may increase over time as there is no indication that FileMaker Pro is gaining market traction and so the market for professional support shows no signs of increasing.

This same key person risk could also mean that future changes are made more complicated and/or costly than necessary, due to limited availability of development resources, and that this ultimately impacts on the ability of the Archive to provide or extend access to the TVNZ archive collection.

A second significant gap was identified in the Appraisal Report (DA63) that covers the TVNZ archive collection, as published on Archives New Zealand's Archway website. This gap relates to the storage of supplementary or collection management records that are required to facilitate access to the audiovisual records. The Appraisal Report notes that the "Paper Vault" where these records are kept requires "further assessment" to confirm it is suitable for long-term storage of physical records.

While Davanti did not carry out this further assessment, we note this as a potential failure to comply with requirement 6.8 of the Standard. Requirement 6.8 states that "dedicated storage areas for inactive physical records or for inactive digital records held on removable media must ensure the survival of those records in a usable form."

This may also be a failure to comply with requirement 4.4, which says that "risks to the accessibility of records must be identified and mitigated". Records containing production information are essential for providing access to records, as they allow the Archive to identify any need for clearances and similar. If the Paper Fault is found to not be appropriate for long-term storage, then the Archive needs to identify and mitigate any risk posed by potentially losing these supplementary records.

RELEASED UNDER THE OFFICIAL INFORMATION ACT

4 HIGH-LEVEL ASSESSMENT

This section expands on the key gaps in the previous section to give a high-level assessment of how the Archive's systems and processes meet each of the requirements of the mandatory Standard, with regard to managing the TVNZ archive collection. The section is divided up by the principles of good records management from the Standard.

The icons below have been used to give a quick indication of strengths, risks and issues identified.

Legend

● No practical risk	◑ Compliance gap to address, but low risk or low business impact beyond PRA compliance	○ Compliance gap to address and high risk or high impact beyond PRA compliance

4.1 Principle 1: Create and maintain records

Requirement		Commentary
1.1 Internal requirements and external obligations to create and maintain records of business activity must be identified and documented	●	The Archive's obligations have been identified and are outlined in their records management policy, and in the records server user guide.
1.2 Records must be created and maintained to meet internal requirements and external obligations	●	Records of any Archive activities that could impact on the transferred TVNZ archive collection records look to be captured. Staff will capture access requests, including internal requests that would result in preservation actions, in the Requests file in the database. The results of preservation actions will likely involve the creation of a new Materials record, which describes the creation of a new instantiation of the work, with appropriate metadata. The database contains a Meetings file that Archive staff will use to document internal decisions that result in changes to ways in which records are managed. Contracts or agreements that are not specific to a work will be captured on the records server, but those relevant to the TVNZ archive collection are likely to be copies. MCH would be prudent to manage these records themselves, in the same way they would manage records of their relationships with any supplier operating on their behalf.

RELEASED UNDER THE OFFICIAL INFORMATION ACT

Requirement		Commentary
1.3 The content and structure of records must fit their purpose and audience	●	The database is set up to capture appropriate levels of detail to meet the Archive's business needs and external obligations. The core AV records are captured as Title records, which contain information about the intellectual work, such as titles, creators, creation information, broadcast information, and so on. Each Title has associated Materials records, which describe the physical instantiations of the Title such as a film reel, a digital file on a tape, a digital file on a server, etc. The metadata includes the format, location, and a link to the relevant deposit through which the Archive received that copy. Many other types of entities exist in the database, such as people, requests, deposits and supplementary records, and it appears that they are appropriately linked so that relationships between these entities can be traced and understood. The Archive's database includes the functionality to capture and relate supplementary documentation to AV records, such as production notes and financial records or correspondence with rights holders. This enables the Archive to ascertain rights and determine whether clearances are necessary for access and usage of any work. The naming scheme proposed in the Records Server User Guide includes using ID numbers from the database to relate documents on the server to records in the database. For instance, a document that relates to a particular title might have both the relevant party's ID number and the relevant title in the file name. Although this work has to be done manually by Archives staff, it is a practical way to relate records on the records server to those in the database.
1.4 Records must be created in a timely manner	●	Access requests and correspondence records are captured as part of the core business of the Archive, and there are operational incentives to do this. Given the nature of the Archive's work this looks to be low risk.
1.5 The content of records must be fixed	◑	The content of the AV records themselves is not changed. If it is necessary to create a modified record for access, re-use, or preservation reasons, then this is done as an additional derivative, rather than replacing the previous version. These derivatives are documented as new Materials records in the database. The main database records are fixed once they are created and cannot be modified. Meeting records are not fixed and can be edited. Therefore, there is a risk that records of decisions that affect the management of the TVNZ records will be overwritten or deleted.

RELEASED UNDER THE OFFICIAL INFORMATION ACT

4.2 Principle 2: Classify and organise records

Requirement		Commentary
2.1 Business activities must be documented in a business classification scheme	●	The Archive developed a classification scheme in 2011 and maintains this scheme. The Director, Systems Development is responsible for considering and managing changes that would affect the top two levels. Documentation of the classification scheme exists and is kept up to date by the Director, Systems Development. The scheme is a fairly typical three-level functional scheme (function, activity, and sub-activity) with some series of case files where it serves a practical purpose. This is good practice, as it reduces any need to rearrange records if the organisation's structure changes.
2.2 Records must be classified and organised according to a business classification scheme	◑	The database records are not incorporated into a broader classification scheme and are not grouped around functions or activities, but rather by types of entities, e.g. Titles, People, Meetings, etc. It is easy to argue that the database records are arranged well enough that the context and purpose of the records can be understood, but if this requirement is followed to the letter then there is no data element that shows how the records in the database fit within the classification scheme. The records server's folder structure adheres to the controlled classification scheme described above, and policy and procedure define how significant changes are made. The server's security roles minimise the risk that Archives staff will bypass the defined the procedure and make ad hoc changes to the higher levels of the folders.

RELEASED UNDER THE FREEDOM OF INFORMATION ACT

4.3 Principle 3: Assign records management metadata to records and aggregations

Requirement		Commentary
3.1 The following minimum records management metadata must be assigned to records and aggregations of records (see also requirement 5.6): • a unique identifier • a name • the date of creation • the business activity documented by the record • the creator (person or system) of digital records • the name and version of the software application used to create digital records • the subsequent actions, if any, carried out on the record, such as accessing, modifying or disposing • the identification of the persons or systems carrying out those actions, and • the dates those actions were carried out.	◑	The database is easily capable of storing the point of capture metadata. The records server, however, does not allow for some point of capture metadata to be created automatically. Audit trails need to be explored further. The elements in the database relates to this requirement as follows: • **Unique ID** - An ID exists for each kind of record. • **Name** - Each Title record has the option for multiple names. • **Date of creation** - Every record has a date reflecting when it was first registered in the database. • **Business activity** - This can be inferred from the record being in the Collections Management System database, combined with the kind of database record, production metadata, and related entities. • **Creator** - Each record in the database captures the employee who has created that entry, including for additional materials where e.g. a migration has been completed for preservation purposes. A variety of People records can also be linked to a Title or a Deposit. • **Application name and version** - Digital AV records have this information in a Materials record. • **Subsequent actions** - Access requests are captured as their own records. This includes documenting actions where new copies or derivatives have been created. Each includes the people, actions and dates relevant to the action. PDFs can also be attached, for example to document communications around rights clearances. The last update metadata is captured. Davanti did not observe whether audit trails are kept. The metadata captured in files on the records server relates to this requirement as follows: • **Unique ID** - The requirement is met as per the note in the Standard that "Organisations will be compliant with this requirement if they assign to records a unique combination of other metadata elements such as name, date and file-path." This is not persistent or tamper-proof, but meets the minimum requirement. • **Name** - Each file has a name. • **Date of creation** - The date that a file is created on the server is captured and the naming scheme encourages staff to add a date to each file name. • **Business activity** - The file-path reflects this, since it follows the functional business classification. • **Creator** - The employee's name is captured against any internally-created file, but any externally created file will come with its own author details internal to it. The staff member who saved the file is not identified. • **Application name and version** - Only what the operating system and applications capture. • **Subsequent actions** - as is typical of operating systems, there is close to no audit trail of changes to records. The Archive has appropriate mitigations in place, such as managing the folder structure, using appropriate security groups, and issuing guidance that embeds sensible records management practices.

RELEASED UNDER THE OFFICIAL INFORMATION ACT

Requirement		Commentary
3.2 Metadata management tools must be developed and maintained, and changes made to them must be tracked and documented	◑	There is no documentation or tool that represents the metadata the Archive captures for all types of records. A schema is maintained for the system that is used to manage the Archive's core records (the database), and not for other systems that hold corporate records (the records server). This is typical of many organisations, but does not meet the requirement to the letter. The database implements a metadata schema that is standards-based and controlled. The schema is based on Dublin Core, supplemented with PBCore, a set of metadata elements that extend Dublin Core for public broadcasters. Any change requests are considered by a Database Management Group. Decisions are documented through the Meetings file in the database, and common practice is discussed with other institutions that collect AV materials. The only metadata that exists for files on the records server is the information automatically captured and/or updated by the operating system and applications. Unsurprisingly, the only documentation or control of this metadata is limited to naming conventions in the user guide.
3.3 Records management metadata must be persistently linked to records and aggregations of records	●	Most users cannot delete the key database records that contain the metadata. Business processes exist around deletion of these database records to minimise the chances that the information will be lost. Deletions and changes such as mergers of suspected duplicates are considered by a committee and implemented only if approved. With digital records on the records server, the only metadata that exists is persistently linked to the records by the nature of the operating system. MCH will need to satisfy itself that the Archive has appropriate means to persistently and uniquely link the records in the database to the physical records within the TVNZ archive collection, through labels and/or barcodes. It is reasonable to assume that this will be in place, but it is so fundamental to proper management that it may be worth confirming.
3.4 The disposal of records management metadata must be managed systematically	●	Point of capture metadata in the database cannot be overwritten, and comprehensive process metadata is captured in the form of request records. This degree of management is built into the design of the database. Both point of capture and process metadata for files on the records server is likely to be as unreliable as with any shared drive, for instance it may be changed accidentally through administration actions such as moving content to a new disk or any kind of format migration activities. These risks can be mitigated through careful planning and testing of activities that would involve moving, restructuring, or "tidying up" the content of the server. The small amount of process metadata that exists on the records server will be overwritten each time a file is updated, as the operating system only captures when a file was last modified and by whom. There is a broader risk that files on the records server are destroyed without authority, and if this occurred the metadata would also be lost. This is considered further under requirement 5.3, since it is not exclusively about metadata.

RELEASED UNDER THE OFFICIAL INFORMATION ACT

4.4 Principle 4: Provide access to records

Requirement		Commentary
4.1 Access to records must be managed appropriately		The database's Requests records are part of an agreed and understood process of managing access to physical records, augmented through supplementary records and dossier entries that inform rights clearances and other access decisions. A document entitled Records Security Principles defines access to the information on the records server, which includes the security groups needed from a business perspective and how they are to be implemented on the server. Access is open by default. The Records Security Principles also states that a log is being maintained of unauthorised access to folders or files.
4.2 Records must be accessible when required		It is a core part of the Archive's business to facilitate access to AV records such as those in the TVNZ archive collection. The Archive has established practices and systems to achieve this, including the online medianet facilities to provide access to digitised video. Regarding internal access to records, Archive documents lay out an expectation that staff will save records centrally to make them accessible to other staff. The database has export functionality that would allow for sets of records to be extracted. The Archive staff expressed confidence that all of the records in the TVNZ archive collection could be identified and exported if necessary. This supports ongoing access to the records in the case where the information about them needs to be moved for whatever reason. Search functionality was not explored beyond name searches in the scope of developing this report. Once TVNZ's metadata is understood, MCH and the Archive may identify ways to make records easily discoverable beyond simple name searches.
4.3 The use of records must be promoted		Again, the use of records is fundamental to the business of the Archive. One benefit of the managed design of the database is that it ensures clear and usable metadata exists for any work in the collection, and progressive improvements can be made in a careful and considered fashion to support searching and other finding methods.

RELEASED UNDER THE OFFICIAL INFORMATION ACT

Requirement		Commentary
4.4 Risks to the accessibility of records must be identified and mitigated	◑	The Archive's core records are managed through a bespoke database that was developed in a relatively uncommon database format (FileMaker Pro). If the one Archive staff member who maintains the database were to leave, it may be difficult for the Archive to find appropriate professional support, and this may in turn compromise access to records. This appears to be an unmitigated risk, although it needs to be discussed with the Archive to confirm. This kind of "key person" risk typically has a low likelihood of eventuating, as a solid database should continue working without active maintenance for quite some time. However, the impact of the database failing and support being unavailable could be severe. A lack of support would also make the Archive's technology environment increasingly inflexible over time, as changes such as desktop or server upgrades may undermine the stability of the database. The Archive has established practices around identifying challenges to accessing audiovisual records and means for addressing those risks. When access or preservation copies are created, they are always in addition to the previous version rather than replacing it. All such actions are documented in a controlled manner in the database through Requests and Materials records. The Archive staff noted that typically obtaining appropriate rights clearances is what requires most effort in order to provide access to records, rather than technical barriers.

RELEASED UNDER THE OFFICIAL INFORMATION ACT

4.5 Principle 5: Appraise records and dispose of them appropriately

Requirement		Commentary
5.1 The value of records must be appraised	●	This requirement has already been met. A disposal authority exists that covers both the transfer of custody of the TVNZ archive collection to MCH, and subsequent disposal actions.
5.2 Retention periods and disposal actions for records must be defined and documented	●	This requirement has already been met. A disposal authority has been signed off by the Chief Archivist and the documentation is available to all relevant parties.
5.3 The correct statutory process for disposing of records must be followed	◑	The records in scope have been appraised and while a proportion of them are due for disposal, MCH is following the correct statutory process by seeking an agreement from the Chief Archivist to defer transfer. The Memorandum of Understanding between MCH and The Archive states that "the Crown will obtain the agreement in writing of the Chief Archivist under the Public Records Act 2005 to defer under section 22 of that Act [...] the transfer of the Archive Collection that has been in existence for 25 years or more." The TVNZ archive collection records transferred to the Archive will be managed by systems and processes in order to prevent their unauthorised destruction. However, any supplementary or additional records that are created by the Archive that are saved on the records server are at risk of being destroyed by staff members and the Archive would have no practical means to identify when and where this has occurred. It also may be worth reviewing what controls exist around documents attached to database records, to ensure that they cannot be destroyed either through deletion or by being overwritten.
5.4 A systematic internal process for disposing of records must be set up and followed	N/A	Davanti has assumed that requirements 5.4, 5.5, and 5.6 do not need to be met, with regard to the TVNZ archive collection, so long as the Chief Archivist agrees to defer transfer. This will mean that for the foreseeable future disposal does not need to occur.
5.5 Records must be disposed of regularly	N/A	Davanti has assumed that requirements 5.4, 5.5, and 5.6 do not need to be met, with regard to the TVNZ records, so long as the Chief Archivist agrees to defer transfer. This will mean that for the foreseeable future disposal does not need to occur.

RELEASED UNDER THE OFFICIAL INFORMATION ACT

Requirement		Commentary
5.6 The following minimum metadata must be generated or captured during the disposal process, and retained for as long as required to account for the disposal of records (see also requirements 3.1 and 3.4): • a unique identifier • a name • the date of creation • the business activity documented by the record • the creator (person or system) of digital records • the date of disposal • the authority governing the disposal of the records, and • the person/role carrying out the disposal.	N/A	Davanti has assumed that requirements 5.4, 5.5, and 5.6 do not need to be met, with regard to the TVNZ archive collection, so long as the Chief Archivist agrees to defer transfer. This will mean that for the foreseeable future disposal does not need to occur.

4.6 Principle 6: Maintain the integrity of records

Requirement		Commentary
6.1 Records must be secure	N/A	Out of scope, as it relates to the Archive's storage facilities.
6.2 Records must be protected from natural and man-made hazards	N/A	Out of scope, as it relates to the Archive's storage facilities.
6.3 Records must be stored on appropriate media or hardware, and in suitable containers and locations	N/A	Out of scope, as it relates to the records being transferred and to the Archive's storage facilities.

RELEASED UNDER THE OFFICIAL INFORMATION ACT

Requirement		Commentary
6.4 At-risk records must be identified and managed appropriately	N/A	Out of scope, as it relates to the Archive's storage facilities.
6.5 Business continuity and disaster management planning must address the protection and salvage of records	◑	The Archive staff noted that there has been some ambiguity as to who is responsible for disaster management relating to IT systems and that they are looking to address this in the position description of a new IT support role. Business continuity plans do exist, full off-site backups could be restored to an external party if required. Disaster management planning for the physical records themselves was not assessed.
6.6 Physical records and digital records held on removable media must be stored in conditions that ensure their safe care and custody. These records must be: • stored in buildings with fire protection systems and equipment compliant with the New Zealand Building Code • stored above floor-level using shelving or equipment appropriate to the format of the records or the size of the storage media • stored away from sunlight and artificial light • stored away from magnetic interference, if they are digital records held on removable media • arranged in an orderly manner, and • retrieved, handled and reshelved in accordance with set procedures.	N/A	Largely out of scope, as it relates to the Archive's storage facilities. However, set procedures for retrieval and access do exist and these activities are documented in the database.
6.7 Inactive physical records and inactive digital records held on removable media must be identified and stored in a dedicated storage area	N/A	Out of scope, as it relates to the Archive's storage facilities.

RELEASED UNDER THE OFFICIAL INFORMATION ACT

Requirement		Commentary
6.8 Dedicated storage areas for inactive physical records or for inactive digital records held on removable media must ensure the survival of those records in a usable form. These storage areas must: • be located in buildings which comply with the provisions of the New Zealand Building Code in force at time of construction and with any associated codes and standards • have adequate floor loading capacity • have drainage systems adequate to prevent flooding or must be located in buildings with drainage systems adequate to prevent flooding • be insulated from the outside climate • be protected from internal hazards • be maintained over time in accordance with a documented maintenance programme • be intruder resistant and have an alarm system or be located within buildings that are intruder resistant and have an alarm system, and • be kept clean and free of pests such as rodents and insects.		While visiting the Archive's storage facilities was out of scope, the Appraisal Report (DA603) does note that the supplementary records kept in the "Paper Vault" are "not housed or stored in keeping with archival standards and may be vulnerable to deterioration over time if they remain in current conditions long term." The Archive's staff noted that such records were essential for facilitating access to audiovisual records, as they contained essential production information that identified records' provenance and, therefore, requirements around rights clearances.

RELEASED UNDER THE OFFICIAL INFORMATION ACT

4.7 Principle 7: Manage records systematically

Requirement		Commentary
7.1 Records management responsibilities must be assigned	●	The Records Management Policy exists and has been distributed. It documents these responsibilities, from the CE through to all staff.
7.2 Staff must be trained to create and maintain records	●	The Archive staff that will work with the TVNZ archive collection are employed on the basis of appropriate background in collections, archival or heritage management. They are provided with training in the specific systems and practices of the Archive.
7.3 Trained staff must be assigned to carry out records management functions and activities		
7.4 Policy for records management must be set and documented	●	The Records Management Policy exists and has been distributed.
7.5 Records management objectives must be defined and documented	◑	The Records Management Policy outlines some organisational strategic values that the policy aligns to, and gives practical statements of objectives, such as "Only important, high value records will be retained for the long term". However, the policy does not explicitly cover collection items, such as the TVNZ archive collection, so this requirement may not be met to the letter. This probably has no practical impact, as the objectives of managing the collection records are likely clear to the Archive's staff, since it is the organisation's business.
7.6 Records management policies and processes must be implemented, monitored and regularly reviewed	◑	System design and staff processes for usage of systems support records management. The Records Management Policy identifies IT as responsible for providing infrastructure that supports good records management. This could be bolstered to make it more explicit what IT activities this relates to, such as procurement, design, security reviews, migration, and so on. The Records Management policy does not include a stated review period, nor is a monitoring mechanism identified.
7.7 Records management activities must be documented	●	The Archive has documented its business classification, and keeps records of decisions that affect changes to records, as well as access requests, as noted under previous requirements such as 3.2 and 3.3. Davanti observed that the Archive captures most information about its core collection management activities, which seems in-keeping with the statement in the Standard that the level of documentation should be matched to the importance of the activity. This could be an area that MCH could explore further with the Archive, as the guidance is relatively open to interpretation.

RELEASED UNDER THE OFFICIAL INFORMATION ACT

Requirement		Commentary
7.8 Records management must be resourced	●	Given the Archive's overall staffing, it seems adequately resourced to carry out its records management obligations, and the nature of its work means many staff will have higher than usual knowledge of records management or sympathetic disciplines. A specific role exists to administer records and implement policies. A specific role exists to manage the database that manages the core records. Committees have been established that consider particular records management activities such as metadata changes, disposal (destruction), access, and preservation actions. A further role is being resourced in IT that will have responsibility for assessing the Archive's business continuity planning and disaster recovery capabilities.

RELEASED UNDER THE OFFICIAL INFORMATION ACT

5 PROPOSED NEXT STEPS

Davanti recommends the following next steps:

5.1 Assess the information about the records coming from TVNZ

MCH needs to satisfy itself that the Archive will receive the necessary metadata about the TVNZ archive collection, both in terms of quality and completeness, to meet the requirements under Principle 3 of the Standard. Beyond completeness and quality, it will be important to understand whether the metadata requires substantial manipulation to be ingested into the Archive's systems, what export functionality the TVNZ database has, and so on.

This will confirm that there is no compliance gap in this area, which in turn indicates that the TVNZ archive collection is properly described and records can be found and understood. Assessing any gaps here will also allow MCH to act on any risks or issues identified.

5.2 Explore the key person risk around the database

MCH should investigate the extent of this risk, outlined in the Key gaps section, and determine what mitigations are appropriate. Mitigations could include ensuring extensive system documentation is available, exploring shared administrative responsibilities (spreading knowledge of the database), or determining whether another database platform is acceptable. Any such investigation of the last point needs to weigh up the benefits of such a purpose-designed core system against the risks, as well as consider the costs.

The Archive may be using FileMaker Pro as a front-end to a more mainstream database technology such as SQL, which would reduce the key person risk to some extent.

This will address the potential compliance gaps around Principle 4 of the Standard, which asserts the need for accessibility to be guaranteed.

5.3 Address the storage of existing supplementary records

The potential inadequacy of the storage facility for paper production records and finding aids described in the Appraisal Report must be addressed, in order to comply with Principles 4 and 6 of the Standard.

Ultimately, this will support discovery and access to the TVNZ archive collection.

5.4 Investigate supplementary database records, audit trails and process metadata

As described in the Key gaps section, MCH would be prudent to look at how supplementary records will be captured by the Archive after 1st August 2014 and to what extent changes to these records are captured in audit trails or similar mechanisms. Audit trails and other process metadata could also be explored more generally.

This will provide more detail into the ongoing management of the TVNZ archive collection, and will clarify any technical requirements related to the database that need to be addressed to support Principles 1 and 3 of the Standard. These requirements affirm that records have integrity and can be trusted.

RELEASED UNDER THE OFFICIAL INFORMATION ACT