NATIONAL ARCHIVES OF AUSTRALIA

BUSINESS SYSTEMS ASSESSMENT FRAMEWORK

BUILDING TRUST IN THE PUBLIC RECORD

PHASE 2 ASSESSMENT OF INFORMATION MANAGEMENT FUNCTIONALITY

1. INFORMATION IS TRUSTED

2.1.1 Can or will you be able to prove the information or data is authentic?

- Can you show who created it?
- Can you show when it was created?

Refer to metadata standards for information management in the Australian (Commonwealth) Government.

2.1.2 Can or will you be able to identify or prevent unauthorised changes to the information or data?

- Can you access human-readable audit logs of changes to information or data?
- Does the audit trail capture all relevant actions?

2.1.3 When you access information or data, can or will you be able to access all relevant parts of it?

- Does the user have access to all relevant information?

2.1.4 Does or will the system meet the National Archives' minimum metadata set or the AGRkMS?

The Building trust in the public record policy recommends that agencies ensure business systems meet functional and minimum metadata requirements for information management (action 10).

2. DISPOSAL IS ACCOUNTABLE

2.2.1 Is or will disposal be controlled, systematic and recorded?

The Building trust in the public record policy recommends that agencies sentence information assets regularly and promptly destroy information assets of temporary value when no longer needed (action 17).

- Is information or data disposed of in accordance with a valid records authority?
- Can you control information or data from being inadvertently destroyed?
- Can you manage a disposal freeze?

2.2.2 Where there is more than one disposal class, can or will you be able to manage the different disposal classes?

What are the minimum and maximum retention periods for the information or data held in the system?

Changes to disposal class data must not result in any information or data being inadvertently destroyed.

2.2.3 Can or will you be able to manage the system's control records in line with your accountability needs?

Following destruction of information or data, you should have a record to defend the destruction if challenged.

This includes:

- information to identify the information or data that was destroyed
- authority to destroy
- date destroyed

2.2.4 Is or will destruction be in line with the Information Security Manual and other relevant policies?

Including your agency's:

- normal adminstrative policy (NAP)
- risk management policy
- information management policy

3. EXPORT/IMPORT

2.3.1 Are you or will you be able to export the information or data in a usable format?

The Building trust in the public record policy recommends that agencies create digital information assets in sustainable formats (action 13).

Is the information or data able to be exported with all relevant attachments and metadata, including audit trails, formats and structure to allow export to other systems?

2.3.2 Are you or will you be able to import information or data into the system?

The Building trust in the public record policy recommends that agencies identify interoperability maturity based on business and stakeholder needs. Identify interoperability maturity gaps and plan to address them (action 11).

This will support interoperability and will be relevant where the sytem will replace an existing system or will be required to import information or data in the future.

4. REPORTING

2.4.1 Can or will the system generate reports on your information or data management processes?

Accurate and efficient reporting is essential to accountable information and data management.

For example, ability to generate report on:

- the volume of information due for destruction on a specific date
- sentenced under a specific disposal class.

2.4.2 Can or will the systems create automatic alerts in response to specific triggers?

This is relevant particularly if you are implementing automated disposal.