NATIONAL ARCHIVES OF AUSTRALIA

BUILDING TRUST IN THE PUBLIC RECORD

managing information and data
for government and community

BUSINESS SYSTEM ASSESSMENT FRAMEWORK

Business system assessment framework

Contents

Background

The *Building trust in the public record: managing information and data for government and community* policy identifies key requirements for managing Australian Government information assets (records, information and data).

The Business System Assessment Framework helps agencies to implement the policy and its actions, including:

- Action 10: Ensure business systems, including whole-of-government systems, meet functional and minimum metadata requirements for information management (recommended).
- Action 15: Identify remaining analogue processes and plan for transformation to digital, based on business need (recommended).

The Business Systems Assessment Framework provides Australian Government (Commonwealth) agencies with a consistent, streamlined and risk-based approach to the assessment of information management functionality in business systems and compliance with metadata standards. It is based on Part 3 of ISO 16175 Principles and Functional Requirements for Records in Electronic Office Environments (2010), which contains an expanded list of functional requirements for business systems.

The framework will enable your agency to better manage its business information and data through:

- assessing information risks and values
- identifying the systems functionality required to manage information appropriately
- providing solutions to address gaps in a system's ability to manage information, and
- ensuring greater accountability and transparency.

The framework recognises that not all information and data is of equal value. It has been developed so that business systems managing high-risk or high-value information and data undergo a more extensive assessment than systems managing low-risk or low-value information and data.

The framework can be used to build functional specifications for new systems and applied to existing systems. It is suitable for use by information management practitioners, business owners and ICT staff.

Note: *The framework does not apply to Electronic Document and Records Management Systems (EDRMS) as they are covered by Part 2 of ISO 16175 Principles and Functional Requirements for Records in Electronic Office Environments (2011).*

Before you begin

The framework is part of a larger suite of information governance tools. To assist with assessing your business systems, you should have:

Systems register

You need to identify the systems in your agency. One way of doing this is to create a systems register listing all the business systems in use in your agency including any legacy systems. The register should list key details about the system including name, version, business owner and a summary of the type of information held. It should also indicate where systems are linked to, and relied on by other systems. The details in the systems register will help you to prioritise which systems to assess. Systems holding high-risk and/or high-value information or data should have priority.

Identifying all the systems in use will help you keep track of where you are up to with your assessments. If you do not have a systems register, a good place to start to identify systems would be your ICT area. You may also be able to draw on information from your business continuity plan, Check-up Digital assessments or information review findings.

Systems information management plan

The assessment of each system should be documented in a systems information management plan. The plan:

- will link to your systems register and other information governance documents
- should cover all relevant information about the system including software, business owners, how it will be managed over its life and details about its assessment against the framework
- may extend to systems and technology hosted in the cloud, or via social media and mobile devices.

Contact us

If you have questions or feedback about the framework please contact the National Archives Agency Service Centre.

What's in the framework?

The framework has three phases:

Phase 1: Preliminary system assessment – This phase consists of six questions that look at the risk and value of the information or data in the system and their disposal, export/import and reporting functionality:

Phase 2: Assessment of information management functionality – This phase has four modules, each with specific questions to help identify and resolve potential issues associated with managing a system. For each system, you are asked a series of questions depending on the modules suggested in the Phase 1 risk assessment. The four modules are:

- Information is trusted
- Disposal is accountable
- Export/import
- Reporting

Phase 3: Implementing solutions – This phase provides suggestions on how to manage any functionality gaps or risks identified in Phase 2 by:

- building in
- integration with other systems
- external (export)
- external (governance).

The decision to actively address an identified gap or risk will be based on your agency's risk tolerance.

Note: Throughout the framework where the word 'information' is used it covers both information and data.

Phase 1 - Preliminary system assessment

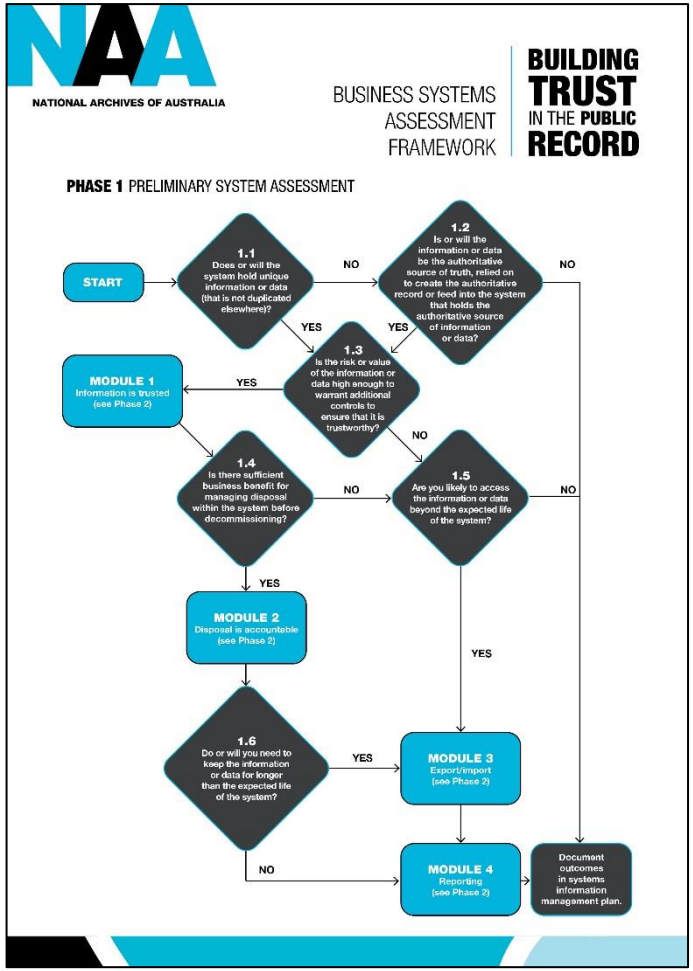
This phase will help you to prioritise which systems need to be assessed further for information management functionality. You should perform this preliminary assessment on each of your business systems to help you determine which need to progress to the next phase and which do not need to advance further.

The assessment consists of six decision points or questions to determine which modules you need to complete. Depending on the outcomes of the preliminary assessment you may be required to complete up to four of the Phase 2 assessment modules.

- This first three decisions points (1.1, 1.2 and 1.3) determine the importance of the system and the information it contains. If the system and the information have sufficient risk or value, this assessment guides you to complete the *Information is trusted* module in Phase 2.
- The next decision point (1.4) relates to disposal and asks whether there is sufficient business benefit for managing disposal within the system. If there is sufficient need, the assessment will guide you to complete the *Disposal is accountable* module in Phase 2. In instances where you intend to dispose at the whole-of-system level, there may be no need to assess disposal capability further.
- Finally, there are two decision points (1.5 and 1.6) that relate to longer-term access (in this case, longer-term means longer than you expect to keep the system, it is not a reflection of longer-term preservation needs). These questions will help you determine whether export, import or reporting functionality is a requirement for your system. If so you will be guided to complete the Export/Import and/or Reporting modules in Phase 2.

Note: *You should speak with your agency's information manager or risk and/or security advisor regarding risk and value of information in systems, to identify any specific requirements that need to be included in the systems information management plan*

Refer to the **Phase 1 - Preliminary system assessment** diagram for an overview of Phase 1.



Phase 1: Preliminary system assessment checklist

Instructions: Provide a simple **'Yes'** or **'No'** response and follow the appropriate action.

No.	Question	Considerations	(Y/N)	For 'Yes' responses	For 'No' responses
1.1	Does or will the system hold unique information (that is not duplicated elsewhere)?	Consider if the information or data is unique and cannot be sourced elsewhere or if it is duplicated in another system. Examples where the information or data is *not* unique: • a case management system that receives documents that are then saved to an approved management system • your ICT back-up systems • any system where information or data are routinely exported and managed in another system, for example emails saved into your EDRMS.		Document what type of **unique** information or data the system holds. Continue to Question 1.3	Document what type or information or data the system holds. Continue to Question 1.2.
1.2	Is or will the information or data: • be the authoritative source of truth • relied on to create the authoritative record, or • feed into a system that holds the authoritative source of information or data?	The authoritative version is the agreed source of information or data to be shared within your agency that is deemed reliable and trustworthy. An example of a system that manages the authoritative source of truth is the whole of government Parliamentary Workflow Solution. Examples of systems where information or data are generally 'saved into' the authoritative system such as email to EDRMS or a case management system.		Document the details of the information or data held in the system, i.e. what and why it is the authoritative source of information. Continue to Question 1.3	Document where the authoritative source of information or data is held. If you have answered No for 1.1 as well, the information and data held in the system has been assessed as low value and risk and therefore does not require further assessment. Document the outcome in your systems information management plan.

No.	Question	Considerations	(Y/N)	For 'Yes' responses	For 'No' responses
1.3	Is the risk or value of the information or data high enough to warrant additional controls to ensure that it is trustworthy?	Answering this question will depend on your risk tolerance. If the value of the information or data in the business system is not sufficient, or if the risks associated with the information is within your stated risk tolerance, then the trustworthiness of the information may not need to be assessed as a priority. To determine the level of risk, think about how critical the information or data is to the performance of your agency's functions. If situations where you have to demonstrate that your information or data is authentic, reliable and has integrity are likely, you need to ensure that you can demonstrate these characteristics when asked. Examples of these may include: • FOI requests • audits • inquiries (including Royal Commissions of Inquiry) • legal proceedings. Note: A yes response should be recorded for any systems that manage information or data identified as 'Retain as National Archives' (RNA) in an agency's approved records authority, and those systems that manage information or data that do not yet have disposal coverage, to ensure these are managed appropriately.		Document the details of the risks and value of the information or data in the system and whether it is the authoritative source. Document the additional controls in place to reduce risks and ensure the information and data's trustworthiness. You will need to complete Module 1: Information is trusted in Phase 2. Continue to Question 1.4	Continue to Question 1.5
1.4	Is there sufficient business benefit for managing disposal within the system before decommissioning?	You may need to decide if the cost of implementing disposal capability within the system justifies the benefit or identify if it is a mandatory requirement to allow disposal within a specific timeframe. You may have a compelling business reason to manage disposal at the individual or aggregated level within the business system. Examples of compelling business reasons may include: • having a legal or policy requirement to destroy information or data within a certain timeframe • the system manages a high volume of information or data with short retention periods, such as a Finance system.		Document the business benefit for managing disposal within the system before decommissioning. You will need to complete Module 2: Disposal is accountable in Phase 2. Continue to Question 1.6.	Continue to question 1.5.

		If the information needs to be disposed of before the system is expected to be decommissioned, it must be either exported from the system or accountably destroyed within the system. ***Note:*** *A yes response should be recorded for any systems that manage information identified as 'Retain as National Archives' (RNA) in an agency's approved records authority, and those systems that manage information that do not yet have disposal coverage, as these may need to be migrated or transferred from the system to manage them over time.*			
No.	**Question**	**Considerations**	**(Y/N)**	**For 'Yes' responses**	**For 'No' responses**
1.5	Are you likely to access the information or data beyond the expected life of the system?	Consider: • how long you expect the system to be in use • minimum retention periods for the information in the system • whether the information is in regular use, and • whether access to the information or data is likely to decline over time. For this decision, you need to weigh-up the likelihood of needing to access the information against the cost of migrating it to, and managing it in, another format. If you do not need to keep the information for longer than the expected life of the system, you may be able to dispose of the information when you decommission the system. This may mean you would not need to address disposal functionality within the system. ***Note:*** *A yes response should be recorded for any systems that manage information identified as 'Retain as National Archives' (RNA) in an agency's approved record authority, and those systems that manage records that do not yet have disposal coverage*.		Document the details of the information or data in the system including: • how long you expect the system to be in use • minimum retention periods for the information in the system • whether the information is in regular use, and • whether access to the information is likely to decline over time. You will need to complete Module 3: Export/import and Module 4: Reporting.	If No, and no other modules have been identified for completion in Phase 1, document the outcome of your risk assessment in your systems information management plan.
1.6	Do or will you need to keep the information or data for longer than the expected life of the system?	Consider: • minimum retention periods for the information or data in the system • the expected life of the system		Document the details of the information or data in the system including: • how long you expect the system to be in use	You will need to complete Module 4: Reporting and any other modules identified earlier.

		• likely costs for maintaining the system after its active business use ends (for access purposes). You may be required to maintain a system even after you have stopped actively using it so that you can continue to access legacy information or data. For example, for a system managing short-term records that you must keep for at least 2 years, you may choose to maintain the system for 2 years after you stop using it so that the information can continue to be accessed until it can be destroyed. If you need to keep the records for longer than the time you expect to maintain the system, and you need to destroy records within a specific timeframe, you will need to export the records to manage the destruction accountably. Note: A yes response should be recorded for any systems that manage information or data identified as 'Retain as National Archives' (RNA) in an agency's approved record authority, and those systems that manage information or data that do not yet have disposal coverage.		• minimum retention periods for the information in the system • whether the information or data are in regular use, and • whether access to the information or data is likely to decline over time. You will need to complete Module 3: Export/import and Module 4: Reporting and any other modules identified earlier.	

Phase 2 - Assessment of information management functionality

Based on your answers in Phase 1, you may have been instructed to undertake additional assessment against one (or more) of the following four modules:

Module 1: Information is trusted - This module helps determine if you can trust the information in the system. It is based on the records characteristics described in ISO 15489: Australian and International Standard for Records Management.

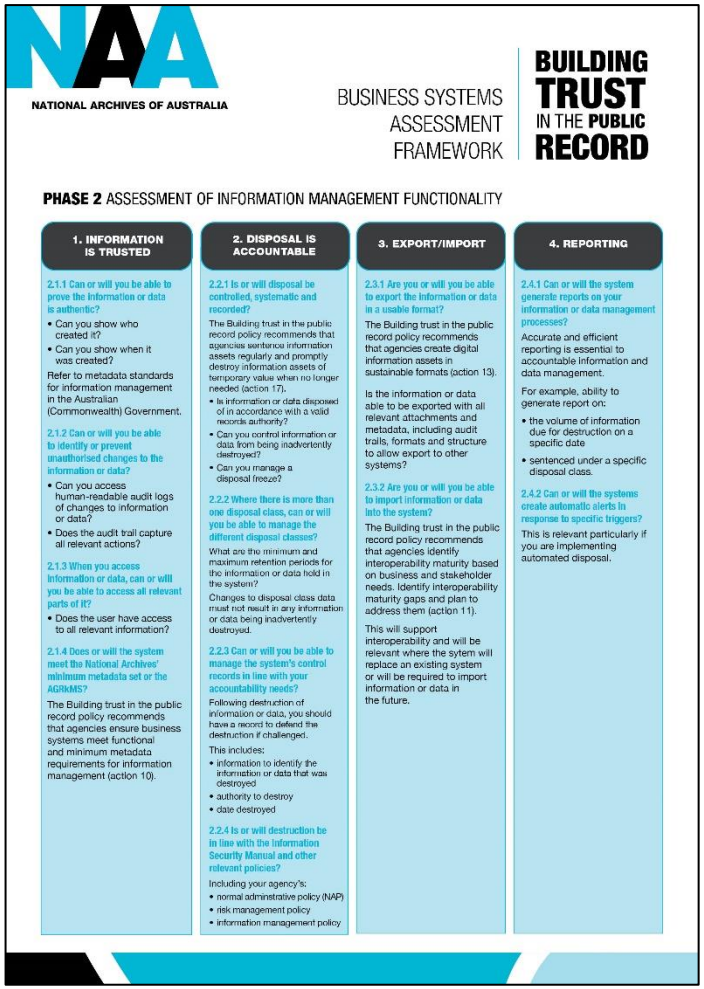
Module 2: Disposal is accountable - This module is for those systems with a business need to manage disposal within the business system. The key functions are to:

- manage disposal at the appropriate item or aggregated level
- destroy information in the way you need to, and
- manage multiple disposal classes if needed.

Module 3: Export/import - Export/import functionality may be a business or information management requirement depending on what you need to do with the data over time. There may also be a requirement to import long-term temporary or permanent information into a new system when the existing system is no longer supported or the cost of maintaining the system over time is significant. Export/import functionality is vital for information management through machinery of government change, or restructure or reorganisation within agencies.

Module 4: Reporting - This module asks if the system is capable of reporting on information management processes such as the number of records due for destruction on a particular date. Accurate and efficient reporting is essential for accountable information management. Most systems are capable of generating reports. Often it is a case of configuring the systems to produce the types of reports required for a particular business need.

Note: Only assess against the modules that were identified in your Phase 1 assessment.


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 administrative 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.

Refer to the **Phase 2 - Assessment of information management functionality** diagram for an overview of Phase 2.

Phase 2: Assessment of information management functionality checklist

Instructions: Respond to all questions in the appropriate module by providing a 'Yes' or 'No' response.

A **'Yes'** response means functionality exists. No further action is required. Add a review date and document the assessment outcomes and other relevant information in the system information management plan.

A **'No'** response to each question will mean that this specific functionality is not met.

Module 1 – Information is trusted - This module helps determine if you can trust the information in the system. It is based on the records characteristics described in ISO 15489: Australian and International Standard for Records Management.

No	Question	Considerations	(Y/N)	For 'Yes' responses	For 'No' responses
2.1.1	Can or will you be able to prove the information or data is authentic?	Consider the risks if you cannot show: • who created it • when it was created • what metadata you will need to show its authenticity. Archives endorses two metadata standards for information management in the Australian Government. These are: • the Australian Government Recordkeeping Metadata Standard (AGRkMS) • the Australian Government Locator Service (AGLS) metadata standard.		Document how you will prove the information or data is authentic. Continue to Question 2.1.2	Document how you plan to address this lack of functionality to prove the authenticity of information or data. Continue to Question 2.1.2

No	Question	Considerations	(Y/N)	For 'Yes' responses	For 'No' responses
2.1.2	Can or will you be able to identify or prevent unauthorised changes to the information or data?	Consider what security controls are needed for your system to avoid, detect, counteract or minimize security risks to information or systems. Consider the risks if you cannot: • access human-readable audit logs showing changes to content • capture all relevant actions in an audit trail.		Document how you will identify and prevent unauthorised changes to information or data. Continue to Question 2.1.3	Document how you plan to identify and prevent unauthorised changes to information or data. Continue to Question 2.1.3
2.1.3	When you access information or data, can or will you be able to access all relevant parts of it?	Consider the risks if: • a user accesses part of the information or data without realising there is other relevant information, or • decisions are made based on incomplete information or data when additional information is available.		Document how you ensure users have all relevant information or data before making a decision. Continue to Question 2.1.4	Document how you will make all relevant information or data available to all users. Continue to Question 2.1.4
2.1.4	Does or will the system meet the Archives' metadata requirements?	The Building trust in the public record policy requires that: • Ensure business systems, including whole-of-government systems, meet functional and minimum metadata requirements for information management (action 10 – recommended).		Document how your business systems are meeting the minimum metadata requirements. Continue to the next module identified in Phase 1 or Phase 3	Document how your agency is going to meet the minimum metadata requirements. Continue to the next Phase 2 module identified in Phase 1 or Phase 3

Module 2: Disposal is accountable - This module is for those situations where business needs to manage disposal within the business system.
The key functions are to:

- manage disposal at the appropriate item or aggregated level
- destroy information in the way you need to
- manage multiple disposal classes if needed.

	Question	Considerations	(Y/N)	For 'Yes' responses,	For 'No' responses
2.2.1	Is or will disposal be controlled, systematic and recorded?	Consider the risks if: • you cannot prevent information or data being inadvertently destroyed • you cannot manage a disposal freeze, or • information or data are not disposed of in accordance with a valid records authority Consider if you export information to another system, how is disposal going to be managed in the new and the legacy system?		Document the steps involved in disposing of information or data, how it is recorded and controlled, and what disposal authority is being used. Continue to Question 2.2.2	Document how you intend on controlling the disposal of information or data so it is recorded and carried out in a systematic way. Continue to Question 2.2.2
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? Your approach to disposal management may mean you need to import or export your information or data into another system or consider the cost of maintaining a system until all information or data are due for disposal. Changes to disposal class data must not result in any information or data being inadvertently destroyed.		Document the retention periods for the information and data held in the system and how you manage more than one disposal class at a time. Continue to Question 2.2.3	If you have more than one disposal class, document the retention periods for the information and data held in the system and how you plan to manage each class. Continue to Question 2.2.3
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 keep a record of what has been destroyed in case you need to defend its destruction if challenged. Consider the risks if you: • do not know what has been destroyed • cannot prove whether or not specific information or data existed at a particular date		Document how your agency knows what information or data has been destroyed, when they were destroyed and under what disposal authority was used.	Document how you plan on managing the systems control records in line with accountability needs, for example:

		• cannot show what disposal authority you used or who approved the destruction of information.		Continue to Question 2.2.4	• recording what is destroyed • when it was destroyed, and • which disposal authority was used. Continue to Question 2.2.4
2.2.4	Is or will destruction be in line with the Information Security Manual and other relevant policies?	Consider Information Security Manual requirements for destroying digital media. Other policies the you might need to align with include your organisation's: • normal administrative policy (NAP) • risk management policy, and • information and data management policy.		Document how you are meeting the Information Security Manual destruction requirements and other relevant policies. Continue to the next module identified in Phase 1. If no other modules are relevant continue to Phase 3.	Document how you will align destruction with the Information Security Manual requirements and other relevant policies. Continue to the next module identified in Phase 1. If no other modules are relevant continue to Phase 3.

Module 3: Export/import - Export/import functionality may be a business, information or data management requirement depending on what you need to do with it over time. There may be a requirement to import long-term temporary or permanent information or data into a new system when the existing system is no longer supported or the cost of maintaining the system over time is significant.					
	Question	**Considerations**	**Y/N**	**For 'Yes' responses**	**For 'No' responses**
2.3.1	Are you or will you be able to export the information or data in a usable format?	Export functionality may be a business or information management requirement, depending on what you need to do with information over time. This functionality is vital for managing information in situations such as: • software as a service (SAAS) arrangements • through machinery of government changes • restructures or reorganisations within your organisation, or • transferring RNA material to Archives. Could the information be exported with all the relevant attachments and metadata, including audit trails and structure? Consider the risks if: • your export does not include all the metadata you need • you are unable to access or use the exported information, or • your exported information does not support sharing with other agencies.		Document what format the system can export information or data and how all relevant information or data will be exported. Continue to Question 2.3.2	Document how you will be able to achieve the functionality to export of the system. Continue to Question 2.3.2
2.3.2	Are you or will you be able to import information or data into the system?	Import functionality supports interoperability and may be relevant to conduct business, where the system will replace an existing system or will be required to import information in the future. There may be a requirement to import long-term temporary or permanent information or data into a new system when the existing system is no longer supported, machinery of government changes occur or the cost of maintaining a legacy system over time is significant.		Document how you import information or data into the system. Continue to the next module identified in Phase 1. If no other modules are relevant continue to Phase 3.	Document how you will achieve the functionality to import into the system. Continue to the next module identified in Phase 1. If no other modules are relevant continue to Phase 3.

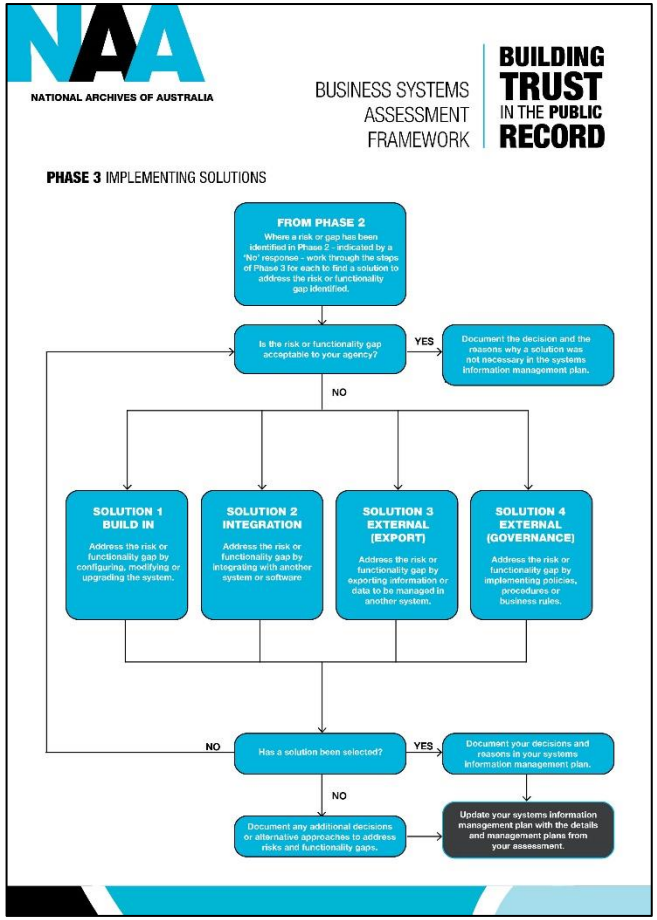
Module 4: Reporting - This module asks if the system is capable of reporting on information management processes such as the number of records due for destruction on a particular date. Accurate and efficient reporting is essential for accountable information management. Most systems are capable of generating reports. Often it is a case of configuring the systems to produce the types of reports required for a particular business need.					
	Question	**Considerations**	**Y/N**	**For 'Yes' responses**	**For 'No' responses**
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. Consider if you need reports such as the number of records: • due for destruction on a specific date • sentenced on a specific date, or • under a specific disposal class.		Document how the system generates reports that detail information or data management processes i.e. when they are due for destruction. Continue to Question 2.4.2	Document how you will meet reporting requirements. Continue to Question 2.4.2
2.4.2	Can or will the system create automatic alerts in response to specific triggers?	Alerts when specific information or data is due for review, transfer or destruction would be helpful. For example, if you are implementing automated disposal.		Continue to Phase 3	Continue to Phase 3

Phase 3 - Implementing solutions

Phase 3 provides suggestions on how to manage any shortfalls, gaps or risks identified in Phase 2. The decision to actively address an identified gap or risk will be based on your agency's risk tolerance. Where you have identified a risk or gap in Phase 2 (where you have answered 'No' to any of the assessment questions), you will need to consider if it is acceptable to your agency. Alternatively, you could use one or a combination of the following solutions to mitigate risks or address gaps by:

- building in functionality
- integration with other systems
- external (export)
- external (governance).

Refer to the **Phase 3 - Implementing solutions** diagram for an overview of Phase 3.



Phase 3: Implementing solutions

Instructions:

A **'Yes'** response to questions in Phase 2 means risk and functionality gaps have been addressed and information management functionality exists.

A **'No'** response to questions in Phase 2 indicates that a risk or functionality gap has not been addressed.

1. Make a list of each of the risks or functionality gaps not addressed, as identified in Phase 2 by 'No' responses.
2. Review each risk or gap and consider if it is acceptable to your agency (Question 3.1) – Yes or No.
3. Yes - If the risk or gap identified is acceptable, document the decision and reasons for this in your system information management plan and add a review date.
4. No - If the risk or gap is not acceptable, review each risk or gap against the available solutions (Questions 3.2 – 3.5) to see if you can find a suitable approach to address it. Note – in some circumstances a combination of solutions may be required to address a particular risk or gap.
5. Document your approach in a system information management plan.

No.	Question	Considerations	(Y/N)	For 'Yes' responses	For 'No' responses
3.1	Where you have identified a risk or gap in Phase 2 by answering 'No' to any of the assessment questions, is the risk or gap acceptable to your agency?	Refer to your agency's information manager, risk or security advisor for more information on risk tolerances.		Document the decision and the reasons why a solution was not necessary in your system information management plan. **End of assessment**	Continue to **Solution 1 – Build in**

Solution 1 – Build in - configuring, modifying or upgrading the business system to manage the risk or gap. For example, if you have identified that you cannot prove the information is authentic, you might build in this functionality by configuring metadata fields to capture additional information to support authenticity.					
	Question	**Considerations**	**(Y/N)**	**For 'Yes' response**	**For 'No' response**
3.2	Where you have identified a risk or gap in Phase 2 by answering 'No' to an assessment question, is the **Build in** solution appropriate to reduce the risks or address any functionality gaps?	Consider the cost of configuring, modifying or upgrading the system and if it is possible to reconfigure, modify or upgrade the system to build in missing information or data management functionality. For example, if you have identified that you cannot prove the information or data is authentic, you might build in this functionality by configuring metadata fields to capture additional information or data to support authenticity. What are the advantages and disadvantages to managing risks or gaps in this way? When and how the missing functionality could be built into the system eg is there an existing agreement with the vendor that outlines how changes to configuration or upgrades are managed? Consider whether a combination of solutions is necessary to address the risk or gap entirely.		Document how you intend to: • configure, modify or upgrade the system • when it is likely to happen, and • any risks associated with the upgrade/ reconfiguration. Document your plan to address risks or gaps in your system information management plan. Continue to work through your list of identified risks and gaps that still need addressing.	Continue to **Solution 2 - Integration**
	Examples of building in functionality include: • Configure metadata fields to capture additional information to support authenticity. This may be populated automatically or manually. • Upgrade or modify the system to make audit logs available to appropriate end users. • Configure audit logs to capture all relevant actions. • Configure additional metadata fields to capture file structure and record/document relationships. • Configure/write reports in the system that will call up the relevant data. • Configure additional metadata fields to capture relevant information or data. • Configure system to ensure that metadata is retained after 'record content' is destroyed.				

	• Ensure that metadata can be exported to be retained as a control record for the system after the system is decommissioned.
	• Configure the system to suspend all disposal action while disposal data is being updated.
	• Configure system to maintain disposal data including:
	  ○ Disposal class number
	  ○ Minimum retention period
	  ○ Disposal trigger
	  ○ Disposal action
	• Embed restrictions into user-initiated disposal actions.
	• Configure or upgrade the system to ensure that all necessary information is exported in the export/migration process.
	• Configure or upgrade system to provide automatic alerts as required.

Solution 2 Integration - integrating the business system with another system to manage the risk or gap. For example, if disposal is not controlled, systematic and recorded in a particular system, you could manage the gap by integrating with another business system or software application that is capable of providing adequate functionality to manage the disposal process.					
	Question	**Considerations**	**(Y/N)**	**For 'Yes' response**	**For 'No' response**
3.3	Where you have identified a risk or gap in Phase 2 by answering 'No' to an assessment question, is the **Integration** solution appropriate to reduce the risks or address any functionality gaps?	Consider whether the risks or gaps in the business system functionality could be addressed by integrating with another system. For example if disposal is not controlled, systematic and recorded in a particular system, you could manage the gap by integrating the business system with your organisation's content management system and manage the disposal process there? What are the advantages and disadvantages to managing risks or gaps in this way? When could the missing functionality be built into the system? Consider whether a combination of solutions is necessary to address the risk or gap entirely. Consider data exchange or integration as an alternative solution.		Document which systems you intend on integrating, and how integrating these would provide the functionality needed. Document your plan to address risks or gaps in your system information management plan. Continue to work through your list of identified risks and gaps that still need addressing.	Continue to **Solution 3 – External (export)**

	Examples of integration include:
	• Integrate the system with another compliant information management system (eg EDRMS) to:
	  ○ capture audit data
	  ○ manage disposal processes
	  ○ use reporting functionality
	  ○ use alert and digital workflow functionality
	• Integrate the system with specialised or customised software applications capable of performing particular specific information management processes, such as disposal, classification, security or storage.
	• Use Extract Transform Load (ETL) software that can convert data into the desired format to integrate with other systems.
	• Use an Application Programming interface (API) to enable data integration between applications and devices to provide functionality.
	• Use agreed data exchange formats and structures to allow data exchange with other systems.				

Solution 3 External (Export) - managing the risk or gap by exporting the relevant data so it can be managed in a separate system. For example, if the system cannot provide adequate internal controls to protect the integrity and authenticity of the information it creates and maintains, it may be possible to export the information to an external system (such as an EDRMS) capable of providing the necessary information management functionality.					
	Question	**Considerations**	**(Y/N)**	**For 'Yes' response**	**For 'No' response**
3.4	Where you have identified a risk or gap in Phase 2 by answering 'No' to an assessment question, is the **External (Export)** solution appropriate to reduce the risks or address any functionality gaps?	Can information or data be exported and managed in another system (e.g. EDRMS) to mitigate identified gaps in Information management functionality? Consider managing the risk or gap by exporting the relevant information or data so it can be managed in a separate system. For example, if the system cannot generate reports of its information management processes, consider exporting the data periodically into a format that allows you to interrogate the data (for example spreadsheets). What are the advantages and disadvantages of this approach? Consider whether a combination of solutions is necessary to address the risk or gap entirely.		Document how you will manage the risk or gap by exporting the relevant information or data, so that it can be managed in a separate system. Document your plan to address risks or gaps in your system information management plan. Continue to work through your list of identified risks and gaps that still need addressing.	Document why this approach is not recommended Continue to **Solution 4 – External (Governance)**
	Examples and other considerations for export activities include: • Export and maintain the required metadata in an external system (ie spreadsheet, compliant information management system). • Export and maintain additional metadata in an external system (ie catalogues, registers, spreadsheets), that captures information and data structures and relationships. • Use agreed data exchange formats and structures to allow export to other systems. • Use Extract Transform Load (ETL) software that can convert data into the necessary formats to facilitate export to external systems. • Use 'machine learning' software for automated mapping of data structures to facilitate exporting data to external systems. • Export the data periodically or as required into a format that allows you to interrogate the data (ie a business intelligence tool, spreadsheet). • Maintain relevant data in an external system (e.g. a spreadsheet) and make scheduled checks against the data to determine if information management actions need to be taken. • Prior to destruction, export a full manifest of system holdings so that data indexing and searching technologies can be used to scan the system.				

Solution 4 External (Governance) - managing any risk or gaps by implementing procedures and business rules. For example, if the system cannot prevent unauthorised changes, consider controlling access to the system by using business rules and manual security protocols.					
	Question	**Considerations**	**(Y/N)**	**For 'Yes' response**	**For 'No' response**
3.5	Where you have identified a risk or gap in Phase 2 by answering 'No' to an assessment question, is an **External (Governance)** solution appropriate to reduce the risks or address any functionality gaps?	Can the identified gaps be mitigated through implementing governance processes (e.g. procedures and business rules)? Managing any risk or gap by implementing procedures and business rules. For example if the system cannot prevent unauthorised changes, consider controlling access to the system by using business rules and security protocols. What are the advantages and disadvantages of this approach? Consider whether a combination of solutions is necessary to address the risk or gap entirely.		Document which business rules/ procedures need to be changed/implemented to manage risks and address gaps in the system. Document your plan to address risks or gaps in your system information management plan. Continue to work through your list of identified risks and gaps that still need addressing. **End of assessment**, if no further risks or gaps remain.	Document why this approach is not recommended or give details of the procedures and business rules that are already in place for the system. Document any additional decisions or alternative approaches to address risks and functionality gaps. Continue to work through your list of identified risks and gaps that still need addressing. **End of assessment**, if no further risks or gaps remain.
	Examples of managing risks or gaps through governance include: • Develop and implement business rules and information security policies to identify how information is accessed and assign appropriate user access categories. • Control access to the system using business rules and manual security protocols (eg restrict physical access to systems). • Where it is not possible to develop appropriate functionality within the system, apply information management controls at the whole-of-system level, (eg records authority disposal classes may be applied to the system as a whole, based on the longest retention period applicable to the system content). • Support business system policies with user training and education programs (eg information access restrictions are reinforced by training users to only access information directly relevant to their duties, where systems cannot enforce user access categories). • Ensure that responsibility for managing and maintaining business systems is clearly assigned and that operational practices are reflected in your information management policy and information governance framework. • Create and define roles and responsibilities for business system administrators and other authorised users via business rules and policies, rather than software mechanisms.				

System information management plan

The assessment of each system should be documented in a system information management plan. This plan:

- will link to your systems register and other information governance documents
- should cover all relevant information about the system including software, business owners, how it will be managed over its life and details about its assessment against the framework, and;
- may extend to systems and technology hosted in the cloud, or via social media and mobile devices.

Question	System details	Plan / Actions
Full system details		
○ System name / full product name		
○ System common name/abbreviation		
○ Business owner (Division/Branch/Section)		
○ Business processes supported by system		
○ External or internal use only?		
○ Security classification		
○ Access controls Can user roles be defined?		
Technical details		
○ System version		
○ System type eg database		
○ Software/OS requirements		
○ Age of system/date acquired		
○ Upgrade due date		
○ Server location (physical)		
○ Current size of data holdings		
System administration and support		
○ System administrator		
○ Number of administrators		
○ Is there a maintenance agreement with vendor?		
○ Where is the source code kept?		
○ Where is system information kept? eg TRIM location		
○ Where is the configuration/customisation		

documentation kept? eg TRIM location		
○ Cost of system (initial procurement)		
○ Ongoing costs (eg licensing and support)		
○ Is there any related legacy system?		
○ Is the legacy data managed?		
○ Identify systems that use data from this system		
○ Identify systems that this system uses data from		
Business System Assessment Framework		
PHASE 1 - Risk assessment	**Yes – Document details**	**No – Document details**
1.1 Does or will the system hold unique information or data (that is not duplicated elsewhere)?		
1.2 Is or will the information or data: • be the authoritative source of truth, • relied on to create the authoritative record, or • feed into a system that holds the authoritative source of information or data?		
1.3 Is the risk or value of the information high enough to warrant additional controls to ensure that it is trustworthy?		
1.4 Is there sufficient business benefit for managing disposal within the system before decommissioning?		
1.5 Are you likely to access the information or data beyond the expected life of the system?		
1.6 Do or will you need to keep the information or data for longer than the expected life of the system?		
PHASE 2 - Assessment of information management functionality	Yes – Document details	No - Where a risk or gap was identified in Phase 2 - indicated by a 'No' response – document the solution to address the risk or functionality gap identified.
Modules 1: Information is trusted		
2.1.1 Can or will you be able to prove the information or data is authentic?		

2.1.2 Can or will you be able to identify or prevent unauthorised changes to the information or data?		
2.1.3 When you access information or data, can or will you be able to access all relevant parts of it?		
2.1.4 Does or will the system meet the Archives' minimum metadata requirements?		
Module 2: Disposal is accountable		
2.2.1 Is or will disposal be controlled, systematic and recorded?		
2.2.2 Where there is more than one disposal class, can or will you be able to manage the different disposal classes?		
2.2.3 Can or will you be able to manage the system's control records in line with your accountability needs?		
2.2.4 Is or will destruction be in line with the Information Security Manual and other relevant policies?		
Module 3: Export/import		
2.3.1 Are you or will you be able to export the information or data in a usable format?		
2.3.2 Are you or will you be able to import information or data into the system?		
Module 4: Reporting		
2.4.1 Can or will the system generate reports on your information or data management processes?		
2.4.2 Can or will the system create automatic alerts in response to specific triggers?		
Assessment information		
○ Assessor name		
○ Business area contact name		
○ Date assessed		
○ Review date		