NATIONAL ARCHIVES OF AUSTRALIA

BUILDING TRUST IN THE PUBLIC RECORD

managing information and data
for government and community

DIGITAL AUTHORISATIONS FRAMEWORK

Contents

Digital Authorisations Framework **3**

Phase 1 – Business process risk assessment **7**

Phase 2 – Approval requirements **10**

Module 1: Stakeholder identification and agreement **11**

Module 2: Security and access **15**

Module 3: Business requirements **18**

Module 4: Information management **21**

Phase 3 – Approval method selection **25**

Email approval implementation task checklist **28**

Action tracking approval implementation task checklist **29**

System workflow approval implementation task checklist **30**

Optional digital signatures implementation task checklist **31**

Digital Authorisations Framework

Introduction

Digital authorisations and workflows:

- improve business efficiency
- support end-to-end digital processes
- increase the availability of more complete and meaningful information.

The *Building trust in the public record: managing information and data for government and community* policy includes the following actions for agencies:

- Action 9: Manage all digital information assets, created from 1 January 2016, digitally. Information assets created digitally from this date, that are eligible for transfer to the National Archives, will be accepted in digital format only. (Mandatory)
- Action 15: Identify remaining analogue processes and plan for transformation to digital, based on business need. (Recommended).

The Digital Authorisations Framework helps agencies to implement these policy actions and transform their analogue approval processes to 'fit for purpose' digital approvals. The framework is a risk-based assessment tool to help determine an appropriate digital approval method for an individual business process. It has three phases:

Phase 1: Business process risk assessment
This contains five questions to help identify the level of risk associated with implementing a digital approval for a business process.

Phase 2: Approval requirements
This has four modules, each with specific questions to help identify and resolve potential issues associated with implementing a digital approval process:

- Stakeholder identification and agreement
- Security and access
- Business requirements
- Information management.

Phase 3: Approval method selection
This includes questions and additional supporting guidance to help determine and implement the most appropriate digital approval method based on the results of your assessment in phases 1 and 2.

Digital approval methods

There are three digital approval methods outlined in the framework that are typically available within the Australian Government. Each approval method can be used for a range of approval processes, including lower- and higher-risk approvals, provided the requirements of Phase 2 and any applicable agency-specific requirements are met.

Note: Your agency may also have access to additional digital approval functionality, including e-forms or proprietary digital approval software. In these instances you may use the advice provided in the framework to confirm the suitability of the approval process or identify any gaps in functionality.

Email approval

A significant amount of government business is completed by email. With appropriate controls in place, email can typically be used to record both routine and more complex business decisions and approvals.

Email approval is typically suitable for:

- internal processes or those exclusively involving government entities
- non-ongoing or infrequent approval requirements.

Action tracking approval

Action tracking enables tasks associated with specific business information – for example, reviewing and approving – to be assigned to specific users. It is typically a linear process, from one user to the next.

Action tracking is typically suitable for:

- processes involving an ongoing and/or repeatable approval requirement and needing limited additional functionality
- automating capture of approval actions through system audit trails.

System workflow approval

System workflows typically automate processes within a business system to complete a specific business task. Workflows can also be manually developed in a compliant records management system to automate a specific business process or action on information within the system, for example to review and approve a document, action or request.

System workflows are typically suitable for:

- processes involving an ongoing and/or repeatable approval requirement, with the additional functionality of redirections for approvers reviewing, re-allocation of tasks, and processes involving multiple instances of information
- assigning specific approval actions to specific users
- tracking approval status, for example when something has been opened, viewed or approved
- automating capture of approval actions through system audit trails.

Additional approval controls: electronic signatures

Other approval methods can be used in conjunction with those recommended in the framework, for example, where:

- required for higher risk processes
- needed to meet legislative requirements
- alternatives are available in a particular agency.

Electronic signatures may be used in conjunction with the approval methods recommended in the framework. Common electronic signatures include:

- a typed name – for example in an e-form
- digitised or scanned hard-copy signatures
- digitally-captured signatures made on a device – for example a smartphone or tablet
- click-through agreements or radio buttons to confirm approval intent
- personal identification numbers (PIN)
- digital signatures (refer to advice below).

They are used to provide:

- additional user assurance – for example a digitised signature or digitally-captured signature may help users feel more comfortable with the digital approval process
- an additional level of security and authenticity for higher risk processes – for example adding a personal identification number (PIN) or secondary verification or a digital signature if required.

Your agency may already be using an electronic signature as part of a digital approval process, or may decide to implement an electronic signature with an approval method provided in the framework. In these instances, you should refer to your agency's existing policy and implementation procedures, or solution provider for specific implementation advice.

Digital signatures

A digital signature is a type of electronic signature that:

- may use digital keys and certificates to authenticate identity and encryption technology and to secure approvals and associated information from unauthorised access or change
- can be used in conjunction with email, action-tracking or workflow approvals, where a stronger form of authentication and non-repudiation is necessary. Generally for higher risk processes to provide an additional level of assurance when completing an approval process digitally.

Note: Digital signatures should only be used as necessary based on the risk and requirements associated with a specific business process. If a digital signature is needed, you should speak with your agency ICT security advisor and the business area/s to determine available options in your agency.

The Gatekeeper Public Key Infrastructure (PKI) Framework governs the use of digital signatures (digital keys and certificates) by the Australian Government, to assure the identity of subscribers to authentication services. The Gatekeeper PKI Framework is a whole-of-government suite of policies, standards and procedures that governs the use of PKI in government for the authentication of individuals, organisations and non-person entities (NPE)

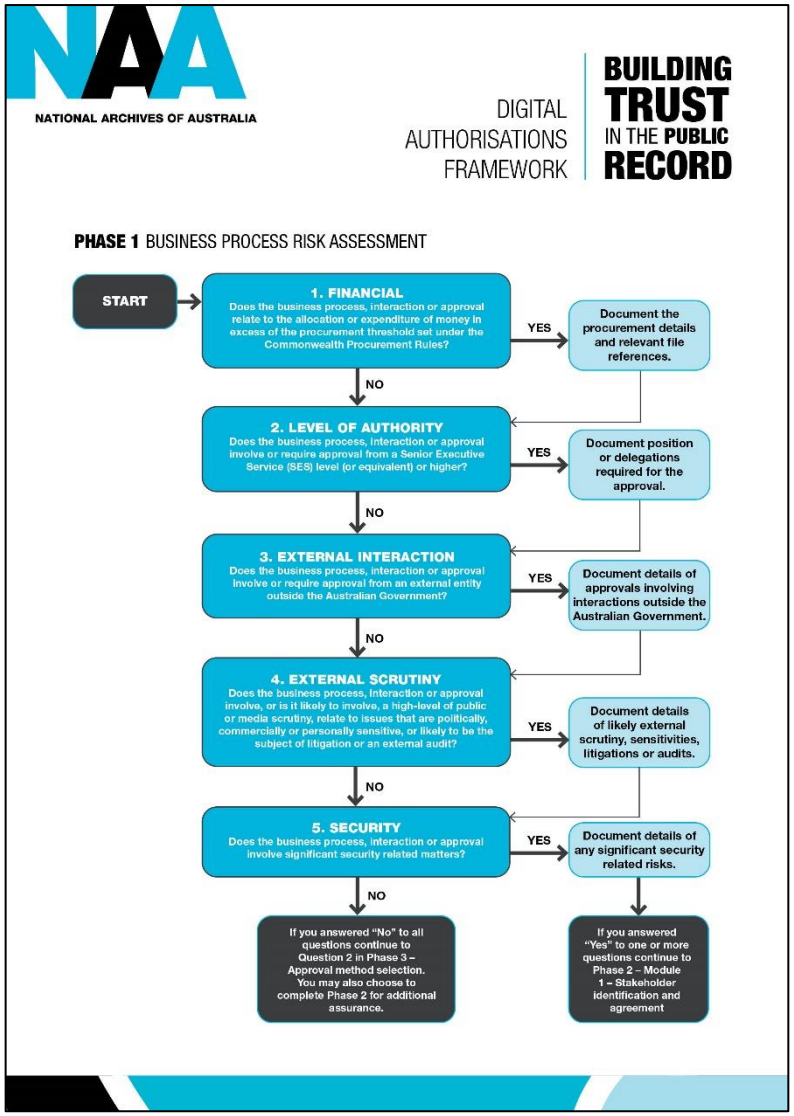
If you have questions about the framework, or would like to apply it outside the Australian Government please contact the National Archives through the Agency Service Centre.

Phase 1 - Business process risk assessment diagram

The purpose of Phase 1 is to identify the level of risk associated with implementing digital approval for a business process. Your answers in Phase 1 will determine which level of risk applies to your business process and Phase 2 will inform the controls needed to ensure the digital approval meets business and accountability needs.

Note: If you have already assessed the business process as low risk through your own risk methodology, or have determined a similar process as being low risk, you may choose to proceed directly to *Phase 3: Approval method selection*, although completing phases 1 and 2 is recommended.

Phase 1 - Business process risk assessment diagram: Refer to the **Phase 1 - Business process risk assessment workflow diagram (pdf 235)** for an overview of the assessment process.



Phase 1 - Business process risk assessment

Risk levels

There are two categories of risk used in this assessment - low risk and medium to high risk. A low risk rating is determined by answering 'No' to all Phase 1 questions. A medium to high risk rating is determined by answering 'Yes' to one or more Phase 1 questions.

Lower risk approvals:	Medium to High risk approvals:
• typically involve low risk and often high volume business processes with an approval requirement • typically relate to routine and/or internal approval processes • have a generally low level of scrutiny or public interest in the business process and/or approval.	• are more likely to involve interaction with multiple parties, internally and/or externally, with some known level of external scrutiny • typically involve high risk and/or less frequently occurring business processes • more often involve sensitive and/or high value information.

The risk rating will determine the level of assessment required throughout the framework. If available, use your agency's own risk rating guidance to confirm the level of risk associated with the specific business process.
Note: You should speak with your agency's risk and/or security advisor regarding medium to high risk processes to identify any specific requirements that need to be included in a digital approval process.

Instructions

Address each question and follow the recommended action based on your response.

- A lower risk rating is determined by answering 'No' to **all** Phase 1 questions.
- A higher risk rating is determined by answering 'Yes' to **any** Phase 1 questions.

	Question	Considerations	Y/N	For 'Yes' responses	For 'No' responses
1	**Financial** Does the business process, interaction or approval relate to the allocation or expenditure of money in excess of the procurement threshold set under the Commonwealth Procurement Rules?	Approvals for amounts which exceed the procurement threshold set under the Commonwealth Procurement Rules indicate a higher level of risk.		• A higher risk rating applies. • Document procurement details with relevant file references. • Continue to question 2	• 'No' indicates a lower level of risk. • Continue to Question 2

	Question	Considerations	Y/N	For 'Yes' responses	For 'No' responses
2	**Level of authority** Does the business process, interaction or approval involve or require approval from a Senior Executive Service (SES) level (or equivalent) or higher?	Approval required by a Senior Executive Service (SES) level (or equivalent) or higher may indicate a higher level of risk or delegation required.		• A higher risk rating applies. • Document positions or delegations for the approval. • Continue to question 3	• 'No' indicates a lower level of risk. • Continue to Questions 3
3	**External interaction** Does the business process, interaction or approval involve or require approval from an external provider or entity outside the Australian Government?	Approval required by an external provider or an entity outside the Australian Government may indicate a higher level of risk and require additional controls to be used.		• A higher risk rating applies. • Document the details of approvals involving interactions outside the Australian Government. • Continue to Question 4	• 'No' indicates a lower level of risk. • Continue to Question 4
4	**External scrutiny** Does the business process, interaction or approval involve, or is it likely to involve a high level of public or media scrutiny, relate to issues that are politically, commercially or personally sensitive, or likely to be the subject of litigation or an external audit?	• Approvals matching these criteria indicate a higher level of risk and require additional controls to be used. • If the level of external scrutiny is unknown, or is considered high enough to warrant additional controls, a 'Yes' response should be recorded.		• A higher risk rating applies. • Document the details of likely external scrutiny, sensitivities, litigations or audits. • Continue to Question 5	• 'No' indicates a lower level of risk. • Continue to Question 5
5	**Security** Does the business process, interaction or approval involve significant security related matters?	• Approvals or supporting business processes involving significant security issues, such as those relating to national security, indicate a higher level of risk and require additional controls to be used. • If the extent of the security-related issues is unknown, or considered high enough to warrant additional controls, a 'Yes' response should be recorded.		• A higher risk rating applies. • Document all details of any significant security related risks. • Continue to Phase 2: Approval requirements	• If you have answered 'No' to **all** Phase 1 questions, continue to Q2 Phase 3: Approval implementation. You may choose to complete Phase 2 for additional assurance. • If you have answered 'Yes' to **any** Phase 1 questions, continue to Phase 2.

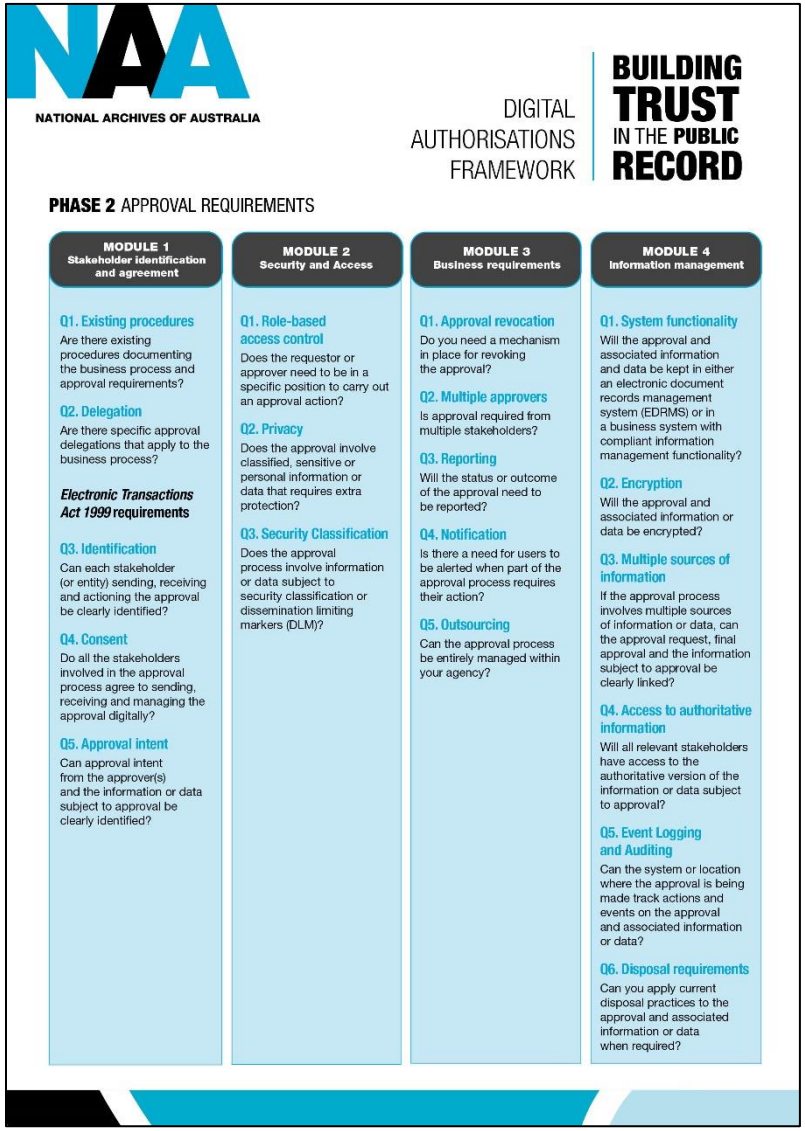
Phase 2 - Approval requirements

Phase 2 includes questions and guidance to help determine an appropriate digital approval method. If completing Phase 2 is recommended, you will answer questions divided into four modules to identify and resolve potential issues associated with implementing a digital approval method.

The modules are:

- Stakeholder identification and agreement
- Security and access
- Business requirements
- Information management

Phase 2 - Approval requirements diagrams: Refer to **Phase 2 - Approval requirements checklist (pdf 692)** for an overview of the modules.

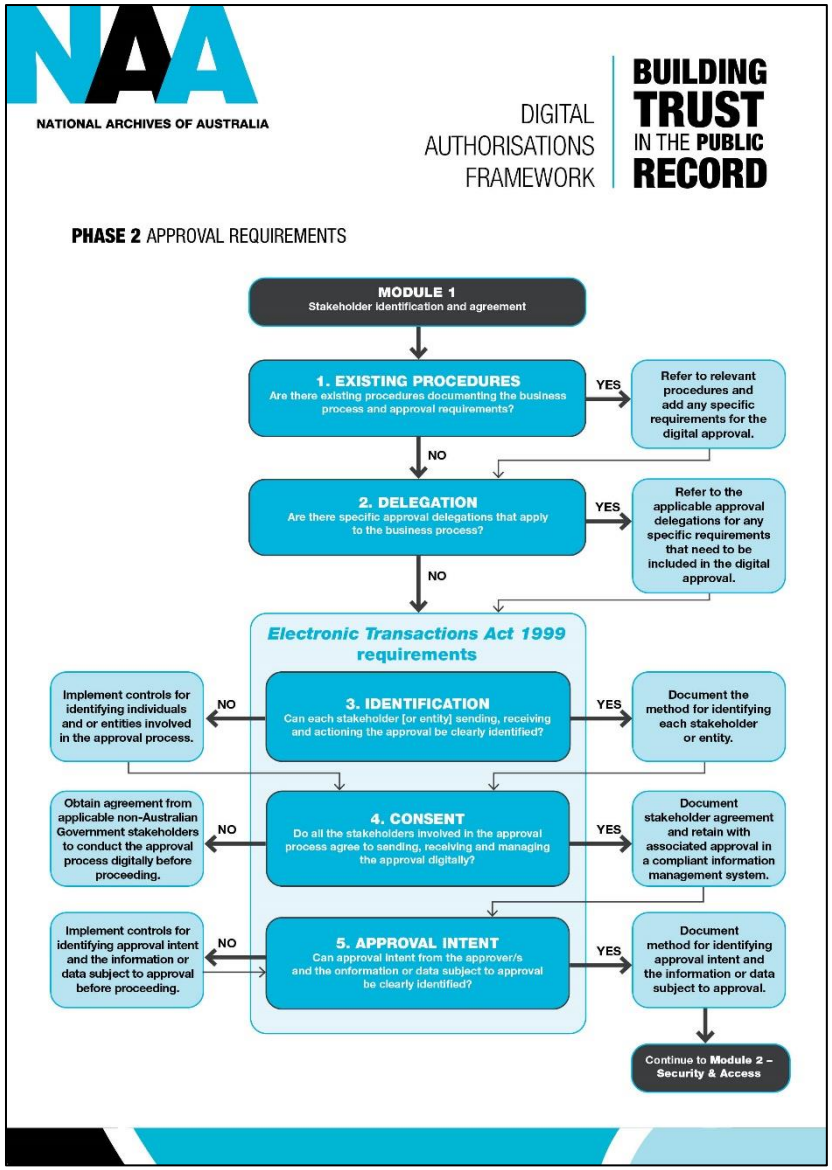


Module 1: Stakeholder identification and agreement

This module helps identify stakeholders involved in the approval process and ensures that all parties agree to complete the approval digitally.

Note: The questions represented in this module are consistent with the requirements of the *Electronic Transactions Act 1999.* However, you should also consider your agency's specific operating circumstances and requirements before implementing a digital approval process.

Refer to the **Phase 2 – Approval requirements diagrams (pdf)** for an overview of this module.



	Module 1 - Stakeholder identification and agreement				
	Instructions				
	Beginning with Module 1, address each question and follow the recommended action based on your response.				
	Question	**Considerations**	**Y/N**	**For 'Yes' responses**	**For 'No' responses**
1	**Existing procedures** Are there existing procedures documenting the business process and approval requirements?	Existing business procedures can help inform your responses throughout the assessment process.		• Refer to business procedures when completing the assessment. • After determining an appropriate digital approval method, document any specific requirements in the applicable business procedures. • Continue to Q2	• Continue to Q2
2	**Delegations** Are there specific approval delegations that apply to the business process?	Consider any agency-specific or internal delegation requirements that may apply. Approval delegations include: • legal delegations • financial delegations, such as Accountable Authority Instructions and Chief Financial Officer's Directions • agency-specific delegations.		• Refer to and document the applicable approval delegation for any specific requirements to be incorporated into the digital approval. • Continue to Q3	• Continue to Q3

	The following three questions are based on the requirements of the *Electronic Transactions Act 1999.* Meeting these requirements is a prerequisite for accountably completing an approval process digitally. You should also consider your agency's specific operating circumstances and requirements before implementing a digital approval process. This includes seeking further advice on the application of the *Electronic Transactions Act 1999* and any specific requirements imposed by the legislation governing the specific approval process, including whether it is excluded from operation of the rules under the Act.				
	Question	**Considerations**	**Y/N**	**For 'Yes' responses**	**For 'No' responses**
3	**Identification** Can each stakeholder (or entity) sending, receiving and actioning the approval be clearly identified?	You must be able to clearly identify each individual involved in the approval process, including requestors and approvers, particularly stakeholders outside the Australian Government including: • state government representatives • non-government representatives within Australia • international government or non-government representatives. Further identification advice is available in the Trusted Digital Identity Framework (TDIF).		• Document the method for identifying individuals and/ or entities in a compliant records management system. • Continue to Q4	• Continue to Q4
4	**Consent** Do all the stakeholders involved in the approval process agree to sending, receiving and managing the approval digitally?	All stakeholders outside the Australian Government must agree to send, receive and have the approval managed digitally.		• Document stakeholder agreement and retain with the associated approval in a compliant records management system. • Continue to Q5	• Continue to Q5

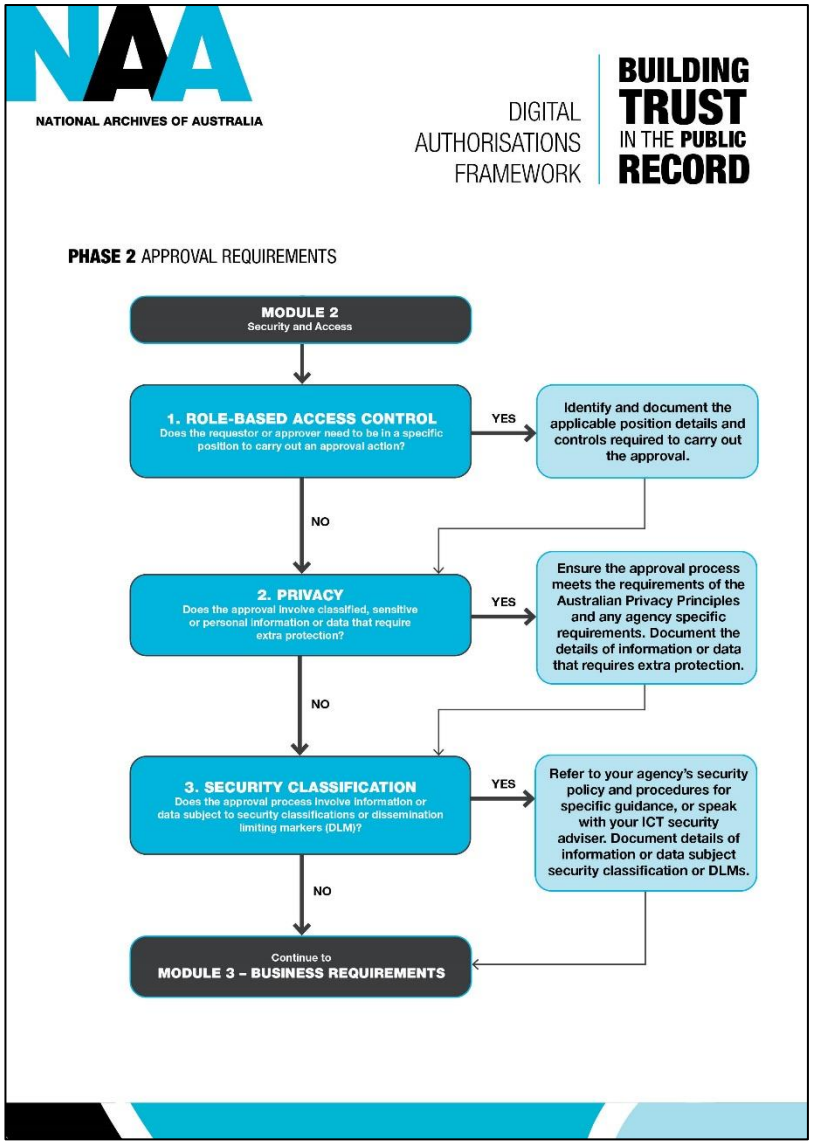
	Question	Considerations	Y/N	For 'Yes' responses	For 'No' responses
5	**Approval intent** Can approval intent from the approver/s and the information or data subject to approval be clearly identified?	• A digital process that replaces a wet signature must be functionally equivalent, be able to identify each individual involved and clearly indicate their approval intent. • Functional equivalence means the digital process has the same degree of authenticity, integrity, reliability and usability as the original wet signature process. • Approval intent may be provided in an email body or subject line, or in a system workflow acknowledgment. • Information or data subject to approval may be identified through a unique file reference, or as an attachment embedded in an accompanying email.		• Document the method for identifying approval intent where the information or data subject to approval is held and include any relevant file references. • Continue to Module 2: Security and access.	• Continue to Module 2: Security and access.

Module 2: Security and access

This module considers the level of security and access needed for the digital approval process based on the security classification of the information or data, its value and the risks associated with it.

Note: Your agency's own internal policies and procedures, consistent with the Australian Government's Information Security Manual and Protective Security Policy Framework should also be used in conjunction with the following questions to determine appropriate controls for the approval process.

Refer to the **Phase 2 - Approval requirements diagrams (pdf 250)**



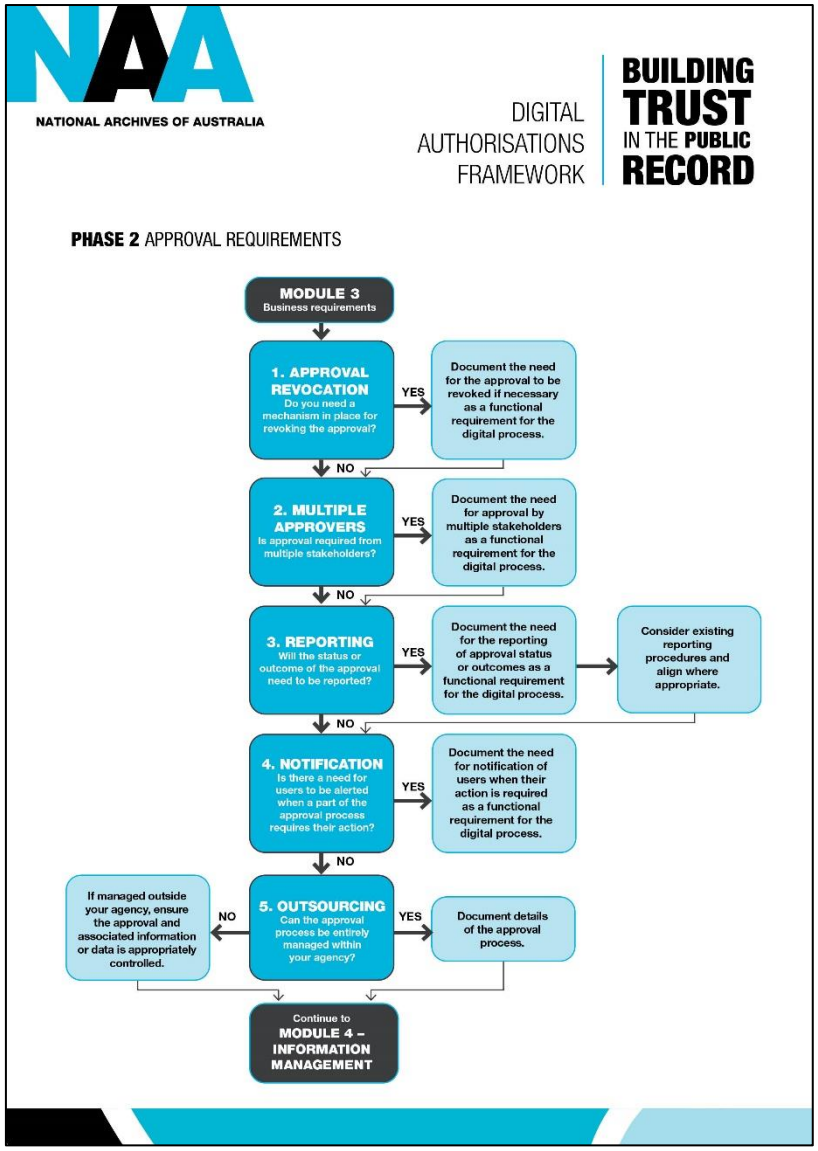
	Module 2: Security and access				
	Question	**Considerations**	**Y/N**	**For 'Yes' responses**	**For 'No' responses**
1	**Role-based access control** Does the requestor or approver need to be in a specific position to carry out an approval action?	• Consider the applicable access or approval authorities for the position responsible for undertaking the approval. • Does it require a certain position in a workflow, as it has the financial delegation to approve.		• Identify and document position details and controls required to carry out approvals. • Continue to Q2	• Continue to Q2
2	**Privacy** Does the approval involve classified, sensitive or personal information or data that requires extra protection?	• Consider any potential issues for inappropriate disclosure of security-classified or sensitive information. • The Australian Privacy Principles outline how to handle, use and manage personal information.		• You must be able to ensure the approval process meets the requirements of the *Australian Privacy Principles* and any agency-specific requirements (including compliance with Australian Government policy). • Document the details of information or data that requires extra protection. • Continue to Q3	• Continue to Q3
3	**Security classification** Does the approval process involve information or data subject to security classification or dissemination limiting markers (DLM)?	• Ensure the use of security classifications and DLMs meet the requirements of the Protective Security Policy Framework (PSPF) and Information Security Manual. • The Australian Government security classifications are: ○ Unofficial		• Refer to your agency's security policy and procedures for specific guidance, or speak with your ICT security advisor. • Document details of information or data subject security classification or DLMs.	• Continue to Module 3: Business requirements.

		○ Official ○ Official: Sensitive ○ Protected ○ Secret ○ Top Secret. From 1 October 2018 classifications changed to those listed above however, entities have an extended period to implement the new classifications until October 2020. See the PSPF website for more information.		• Continue to Module 3: Business requirements.	

Module 3: Business requirements

This module helps ensure the digital approval process is fit for purpose and meets the requirements of the business area/s involved, including the applicable stakeholders.

Refer to the **Phase 2 - Approval requirements diagrams (pdf 250)**



	Module 3: Business requirements This module helps ensure the digital approval process is fit for purpose and meets the requirements of the business area/s involved, including the applicable stakeholders.				
	Question	**Considerations**	**Y/N**	**For 'Yes' responses**	**For 'No' responses**
1	**Approval revocation** Do you need a mechanism in place for revoking the approval?	You may need to be able to revoke an ongoing or repeatable approval process, or an approval provided for a set period of time, for example revoking a legal delegation if required.		• Document the need for the approval to be revoked if necessary as a functional requirement for the digital process. • Continue to Q2	• Continue to Q2
2	**Multiple approvers** Is approval required from multiple stakeholders?	• Some approval processes require multiple levels of approvals or review before a final approval can be made. • A parallel approval process which allows multiple sequential approvers may be required for higher-risk processes needing a greater level of assurance.		• Please enter details of how approval by multiple stakeholders will be managed. • Continue to Q3	• Continue to Q3
3	**Reporting** Will the status or outcome of the approval need to be reported?	• Approval status or outcome, or the information or data subject to approval, may need to be available for internal or external reporting purposes. • Reporting of classified, sensitive or personal information should be managed in accordance with Australian Government policy and the Australian Privacy Principles.		• Document the need for the reporting of approval status or outcomes as a functional requirement for the digital process. • Continue to Q4	• Continue to Q4

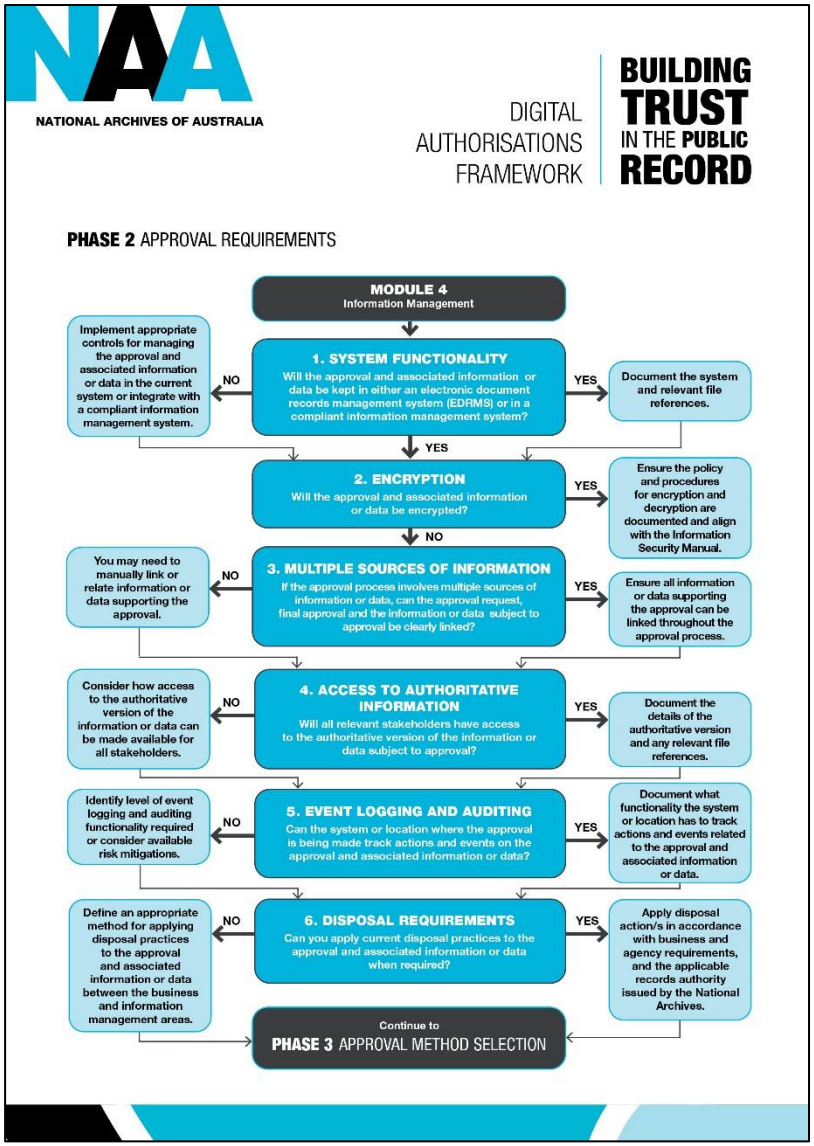
	Question	Considerations	Y/N	For 'Yes' responses	For 'No' responses
4	**Notification** Is there a need for users to be alerted when part of the approval process requires their action?	The level of significance, risk or urgency associated with an approval may require users to be notified when an action is needed. For example, they might need to review or approve something within a particular timeframe.		• Document the need for the notification of users when their action is required as a functional requirement for the digital process. • Continue to Q5	• Continue to Q5
5	**Outsourcing** Can the approval process be entirely managed within your agency?	• Additional controls will likely be needed if the approval process involves external or outsourced systems or systems managed by an external provider. • For example, ensure your agency maintains access to and ownership of all relevant information when entering into outsourced arrangements.		• Document the details of the approval process. • Continue to Module 4: Information management.	• If managed outside your agency, ensure the approval and associated information or data is appropriately controlled. • Continue to Module 4: Information management.

Module 4: Information management

This module helps ensure the approval and associated information and data can be accountably managed and accessed for as long as required and incorporated into your agency's existing information and data governance practices.

Note: You should liaise with your agency's information management area to complete this module.

Refer to the **Phase 2 - Approval requirements diagrams (pdf)**



	Module 4: Information management				
	Question	**Considerations**	**Y/N**	**For 'Yes' responses**	**For 'No' responses**
1	**System functionality** Will the approval and associated information and be kept in either an electronic document records management system (EDRMS) or in a business system with compliant information management functionality?	• Consider specific requirements for higher risk approvals or where it's known the approval and associated information or data must be kept for a longer period of time. • Export functionality is required for approvals and associated information or data that needs to be kept for longer than the expected life of the system. • Systems assessed against the Business Systems Assessment Framework should be able to manage the approval and associated information or data for as long as required.		• Document the details of the system and approval related file references. • Continue to Q2	• Implement appropriate controls for managing the approval and associated information or data in the current system for as long as required. This may include assessing the system's functionality against the Archives' Business Systems Assessment Framework. • Alternatively, capture the approval and associated information or data in a compliant information management system. This may include establishing a process where the approval and associated information or data is either manually or automatically captured in a compliant information management system. • Continue to Q2

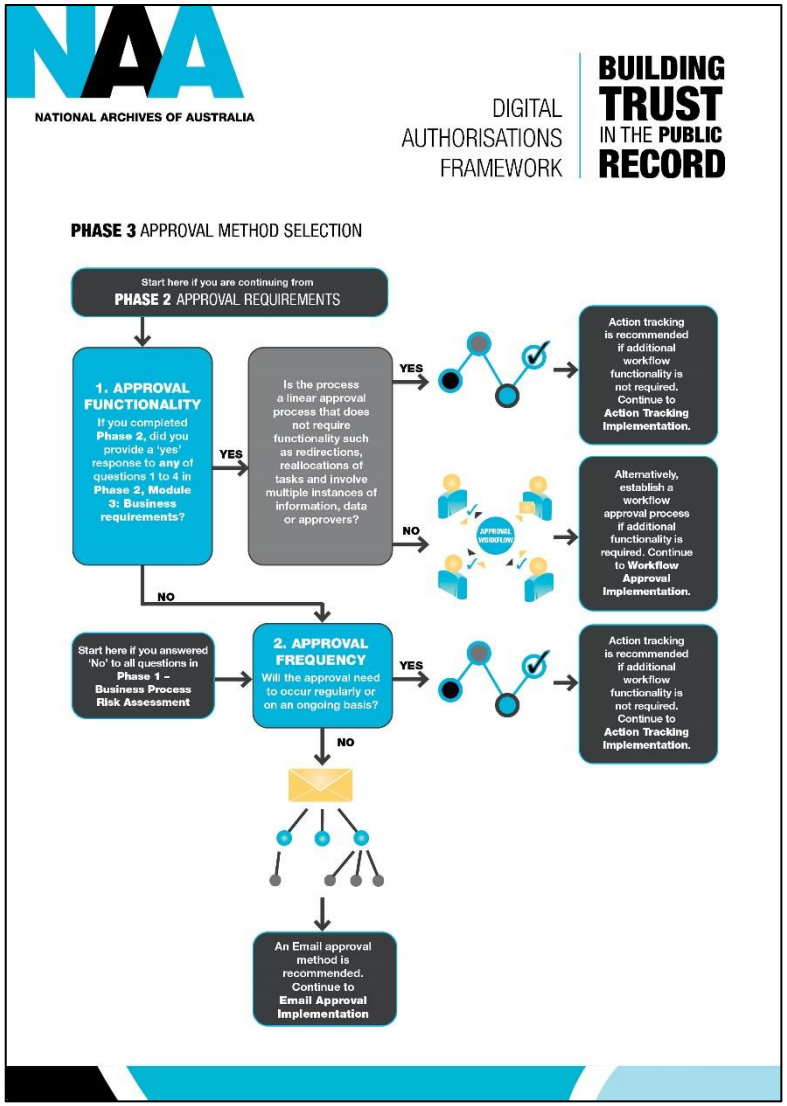
	Question	Considerations	Y/N	For 'Yes' responses	For 'No' responses
2	**Encryption** Will the approval and associated information or data be encrypted?	• Encryption should only be used on a limited basis where required, for example with sensitive or high-risk processes, or as required by legislation. • Encryption will typically take place at a system level. You should speak with your ICT security advisor or system administrator if you are unsure if the approval and supporting information or data is or will be encrypted in the system. • If encryption is used, you must be able to maintain access to the information or data for as long as needed, including being able to decrypt at a later point. • Metadata can verify the encryption and decryption process.		• Ensure the policy and procedures for decryption are documented and accessible. • Ensure encrypted information or data is accessible to those who require it by implementing appropriate procedures and controls for data recovery in line with the Information Security Manual information on cryptography. • Continue to Q3	• Continue to Q3
3	**Multiple sources of information** If the approval process involves multiple sources of information or data, can the approval request, final approval and the information or data subject to approval, be clearly linked?	For accountability purposes, information from multiple sources, systems or locations supporting the approval should be linked or able to be related together.		• Ensure all information supporting the approval can be linked throughout the approval process and document any relevant file references. • Continue to Q4	• You may need to manually link or relate information or data supporting the approval, for example by documenting all related file references with the approval request. • Continue to Q4

	Question	Considerations	Y/N	For 'Yes' responses	For 'No' responses
4	**Access to authoritative information** Will all relevant stakeholders have access to the authoritative version of the information or data subject to approval?	The authoritative version of the information subject to the approval must be available and readily identifiable to support accountable and effective decision making.		• Document the details of the authoritative version and any relevant file references. • Continue to Q5	• Confirm and document how access to the authoritative version of the information can be made available to applicable stakeholders. • Continue to Q5
5	**Event logging and auditing** Can the system or location where the approval is being made track actions and events on the approval and associated information or data?	All actions and changes to an approval and associated information should be recorded by the system's audit logs and be available to support accountability and authenticity.		• Document what functionality the system or location has to track actions and events related to the approval and associated information or data. • Continue to Q6	• Identify the level of event logging and auditing functionality required. • For a lower risk process managed outside of a system with information management functionality, consider available mitigations. • Continue to Q6
6	**Disposal requirements** Can you apply current disposal practices to the approval and associated information or data when required?	• Disposal functionality should be applied based on business requirements, system functionality and the applicable records authority issued by the National Archives. • See the National Archives' advice on compliant destruction of Australian Government records for further information.		• Apply disposal action/s in accordance with business and agency requirements, and the applicable records authority issued by the National Archives. • Document disposal practices and the relevant disposal authority. • Continue to Phase 3: Approval implementation.	• Define an appropriate method for applying disposal practices to the approval and associated information between the business and information management areas. • Continue to Phase 3: Approval implementation.

Phase 3 - Approval method selection

Phase 3 will help you determine and implement the most appropriate digital approval method.

Refer to the **Phase 3 - Approval implementation workflow diagram (pdf)** for an overview of this module.



	Phase 3 - Approval method selection				
	Instructions				
	Approval method selection Address the question/s below to confirm the most appropriate digital approval method.				
	Question	**Considerations**	**Y/N**	**For 'Yes' responses**	**For 'No' responses**
1	**Approval functionality** If you completed Phase 2, did you provide a 'yes' response to **any** of questions 1 to 4 in Phase 2, Module 3: Business requirements? Is the process a linear approval process that does not require functionality such as redirections, reallocations of tasks and involve multiple instances of information, data and approvers?	The applicable questions in Phase 2, Module 3: Business requirements addressed: • approval revocation • multiple approvers • reporting functionality • notification functionality		• Action tracking is recommended if additional workflow functionality is not required. See Approval method overview below for further information. • Alternatively, establish a workflow approval process if additional functionality is required. See Approval method overview below for further information. • Continue to action-tracking or workflow approval implementation advice below as appropriate.	Continue to Q2
	Approval frequency Will the approval need to occur regularly or on an ongoing basis?	• Action tracking and workflow can provide a consistent and repeatable approach for recurring business processes and approvals. • Email approval is typically suited to infrequent or one-off approvals, where it's less efficient to establish action-tracking or workflow approval processes, or where this functionality is unavailable.		• Action tracking is recommended if additional workflow functionality is not required. See Approval method overview below for further information. • Alternatively, establish a workflow approval process if additional functionality is required. See Approval method overview below for further information. • Continue to action-tracking or workflow approval implementation advice below as appropriate.	

Approval method implementation

Practical guidance is included below for each of the three digital approval methods recommended in the framework. This advice should be used in consultation with the relevant stakeholders involved in the approval process, including the business, information management and ICT areas, to successfully implement the recommended digital approval method.

Note: Before implementing the recommended approval method you should consider your agency's specific operating circumstances and any specific requirements associated with the business process. If you are unsure which approval method to use or require further advice, you should consult with your agency's legal, business and information management representatives.

Email approval implementation task checklist	Y/N
Do all stakeholders associated with the business process, interaction or approval agree to sending, receiving and recording approval/s using email? **Note:** Agreement from internal stakeholders may often not be explicitly required depending on your agency's policy and procedures. For example, approval between business areas to use email approval may be sufficient. Alternatively, email approval might already be endorsed as an approval method under particular circumstances or for specific business processes.	
Each party can be identified through system and/or email audit trail metadata.	
Each party has their signature block embedded into the body of the email (including name, position and organisation). If used, a digital signature will also provide additional identity assurance.	
Where email is incorporated into the action-tracking process, approval intent is distinguishable as a defined task in the process.	
Approval intent is included in the subject line and body of the email.	
Where applicable, dissemination limiting markers (DLMs) are appropriately applied?	
Define and document the steps for implementing email approval for the associated business process, by ensuring business, accountability, agency and broader legislative requirements are met. Ensure policy and procedures are in place to ensure the information associated with the email approval are supported through:	
• up-to-date position details which are embedded into systems that enable the approval process	
• alerts to users when they need to perform an action in the approval process	
• maintenance of an authoritative version of the approved information, finalised and managed in an accessible form (not subject to further changes) consistent with agency filing procedures and security classification requirements	
• clear association of the information and the approval, maintained over time through metadata (see metadata requirements below)	
• retention of the approval and associated information as required under the relevant records authority or longer, based on business or stakeholder needs.	
Appropriate metadata should be captured to support the approval process and management of the associated information. This should be based on business need and any other legal or agency-specific requirements. The Archives minimum metadata set identifies nine properties required for the efficient and effective management of business information and can be extended to include any metadata needed by your agency to meet your business and information management needs.	

Action tracking approval implementation task checklist	Y/N
Do all stakeholders associated with the business process, interaction or approval, agree to sending, receiving and recording approval/s using action tracking? **Note:** Agreement from internal stakeholders will often not be explicitly required depending on your agency's policy and procedures. For example, approval between business areas to use action-tracking approval may be sufficient. Alternatively action-tracking approval might already be endorsed as an approval method under particular circumstances or for specific business processes.	
Each party can be identified through system and/or email audit trail metadata and their signature block is embedded in the email body (including name, position and organisation). If used, a digital signature will also provide additional identity assurance.	
Approval intent is distinguishable as a defined task in the action-tracking process. Where email is incorporated into the action-tracking process, approval intent is included in the subject line and/or body of the email.	
Define and document the steps for implementing action-tracking approval for the associated business process, ensuring business, accountability, agency and broader legislative requirements are met. Implement policy and procedures to ensure the information associated with the action-tracking process is supported through:	
• up-to-date position details, including access and approval delegations which are embedded into systems to enable the approval process	
• alerts to users when they need to perform an action in the approval process	
• maintenance of an authoritative version of the approved information, finalised and managed in an accessible form (not subject to further changes) consistent with agency filing procedures and security classification requirements	
• clear association of the information and the approval, maintained over time through metadata (see metadata requirements below)	
• retention of the approval and associated information as required under the relevant records authority or longer, based on business or stakeholder needs.	
Appropriate metadata should be captured to support the approval process and management of the associated information. This should be based on business need and any other legal or agency-specific requirements. The Archives minimum metadata set identifies nine properties required for the efficient and effective management of business information and can be extended to include any metadata needed by your agency to meet your business and information management needs. **Note:** You may need to liaise with your information management and ICT areas to determine the best approach for exporting metadata associated with the action-tracking approval.	

System workflow approval implementation task checklist	Y/N
All stakeholders associated with the business process, interaction or approval agree, to sending, receiving and recording approval/s using a workflow. **Note:** Agreement from internal stakeholders will often not be explicitly required depending on your agency's policy and procedures. For example, approval between business areas to use workflow approval may be sufficient. Alternatively workflow approval might already be endorsed as an approval method under particular circumstances or for specific business processes.	
Each party should be able to be identified through system and/or email audit trail metadata and their signature block embedded in the email body (including name, position and organisation). If used, a digital signature will also provide additional identity assurance.	
Approval intent is distinguishable as a defined task in the workflow process. Where email is incorporated into the workflow, approval intent is included in the subject line and or body of email.	
Define and document the steps for implementing workflow approval for the associated business process, ensuring business, accountability, agency and broader legislative requirements are met. Ensure policy and procedures are in place to ensure the information associated with the action-tracking process is supported through:	
• up-to-date position details which are embedded into systems to enable the approval process	
• alerts to users when they need to perform an action in the approval process	
• maintenance of an authoritative version of the approved information, finalised and managed in an accessible form (not subject to further changes) consistent with agency filing procedures and security classification requirements	
• clear association of the information and the approval, maintained over time through metadata (see metadata requirements below)	
• retention of the approval and associated information as required under the relevant records authority or longer, based on business or stakeholder needs.	
Appropriate metadata should be captured to support the approval process and management of the associated information. This should be based on business need and any other legal or agency-specific requirements. The Archives minimum metadata set identifies nine properties required for the efficient and effective management of business information and can be extended to include any metadata needed by your agency to meet your business and information management needs. **Note:** You may need to liaise with your information management and ICT areas to determine the best approach for exporting metadata associated with the workflow approval.	

Optional digital signatures implementation task checklist	Y/N
Note: Digital signatures should only be used as necessary based on the risk and requirements associated with a specific business process. If a digital signature is needed, you should speak with your agency ICT security advisor and the business area/s, to determine available options in your agency.	
All stakeholders associated with the business process, interaction or approval must agree to sending, receiving and recording approval/s digitally, using Digital Signature Public Key Infrastructure (PKI) authentication.	
Each party should be able to be identified through system and/or email audit trail metadata and their signature block embedded in the email body (including name, position and organisation) or digital signature.	
Approval intent (explicit or implicit) is distinguishable in the system used, such as software for distribution (email), financial transactions, contract management. Explicit approval is 'Yes' or equivalent. Implicit approval can be reasonably established based on the context of the software.	
Define and document the steps for implementing digital signatures for the associated business process, ensuring business, accountability, agency and broader legislative requirements are met. Ensure policy and procedures are in place to ensure the information associated with digital signatures is supported through:	
• encryption/decryption – ensure encrypted information is accessible by implementing appropriate procedures and controls for data recovery in line with the Information Security Manuals information on cryptography. Document the policy and procedure for decryption.	
• maintenance of an authoritative version of the approved information finalised and managed in an accessible form (not subject to further changes) consistent with agency filing procedures and security classification requirements	
• clear association of the information and the approval, maintained over time through metadata (see metadata requirements below)	
• retention of the approval and associated information as required under the relevant records authority or longer, based on business or stakeholder needs.	
Appropriate metadata should be captured to support the approval process and management of the associated information. This should be based on business need and any other legal or agency-specific requirements. The Archives minimum metadata set identifies nine properties required for the efficient and effective management of business information and can be extended to include any metadata needed by your agency to meet your business and information management needs. **Note:** You may need to liaise with your information management and ICT areas to determine the best approach for exporting metadata associated with the workflow approval.	