Digital Continuity 2020
the future of e-government

Your story, our history
The Digital Continuity 2020 Policy was released and published online on 27 October 2015 as a whole-of-government approach to digital information governance. It was launched by Jane Halton AO PSM, Secretary Department of Finance, who in her speech affirmed that ‘Information is a vital government asset, and while we progress more and more into the digital world, we need to ensure this asset is managed and managed well.’

The policy aims to support efficiency, innovation, interoperability, information re-use and accountability by integrating robust digital information management into all government business processes. This will allow agencies to:

- optimise the delivery of government programs and services;
- enable information reuse for economic and social benefits; and
- protect the rights and entitlements of Australians.

Its reforms will make information:
- easier to find, understand and share;
- interoperable and able to be re-used or commercialised;
- more secure; and
- accessible and preserved for as long as needed.

The policy builds on achievements of the 2011 Digital Transition Policy and enables agencies to continue progress in improving digital information governance and management.

It applies to all Australian Government agencies and relates to all government information, data and records, including systems, services and processes, and information created by a third party on behalf of Australian Government agencies.

The policy was issued under the authority of the National Archives of Australia, as established by the Archives Act, as the agency responsible for setting records and information management requirements for Australian Government agencies. The Archives’
Minister, Senator the Hon George Brandis QC, has written to his ministerial colleagues seeking their support for implementation of the policy in their departments and portfolio agencies.
The Government commits to transforming public services by

- designating digital as the default channel for interaction
- recognising the importance of public data as a national resource

The Digital Continuity 2020 Policy is very well positioned within the overall strategic environment in the Government:

During the 2013 election, the Government committed to transforming the way public services were designed and delivered including designating digital as the default channel for interaction.

Since then a number of important initiatives happened in the Government, most notably the establishment of the Digital Transformation Office in 2015. The DTO’s Digital Service Standard establishes the criteria for the digital by design approach to government services. This means that all new and redesigned services will be structured consistently and will be simple and easier to use.

We know that many agencies have already moved in this direction. For example, the Australian Taxation Office has recently finished public consultation on its plans to deliver its services digitally by default; the Department of Immigration and Border Protection has introduced a number of digital services, such as the online self-service facility for clients to digitally manage visa applications; The Federal Court of Australia’s introduction of electronic court files has created a seamless and effortless flow of electronic documents to the Court, within the Court and to those appropriate parties outside the Court. These are only few examples of a wide variety of digital transformation initiatives within the Government.

The Public Data Branch of the Department of Prime Minister and Cabinet aims to improve policies on how public sector data can be better used to achieve efficiencies for government, enable better service delivery and inform policy development, and be used by the private sector to innovate and create new products and business models. These goals were manifested in the Public Data Policy Statement issued by PM&C in December.

A robust, reliable and future-focused approach to government information is central to the Government’s digital agenda. And this is where the Digital Continuity 2020 Policy
complements all other initiatives which cannot be fully realised without the consistent approach to information governance across the Government and within individual agencies.
• DC2020 recognises the important role industry plays in making digital continuity a reality.

• Government cannot do it alone – we need to collaborate and partner with industry to implement innovative solutions and improved business interactions.

• We are briefing industry to give them the opportunity consider how their products and services for government address Digital Continuity requirements.

• Given the tight fiscal environment, products that assist you (agencies) to achieve Policy targets will be competitive in the government environment.

• The recent Department of Finance Request for Information (RFI) reaches out to industry for insight into “the most effective and efficient way to consolidate digital records management solutions, in a manner that represents value for money to Government.” (A whole-of-government approach to Electronic Document and Records Management Solutions).

• The National Archives will be working with industry to establish a mechanism of assessing their products and services against the Policy’s requirements. We expect that you will be able to access information about which products or services from industry can help you achieve your targets.
**Digital Continuity 2020 Policy Statement:**

Agencies will manage their information as an asset, ensuring that it is created and managed for as long as required, taking into account business and other needs and risks.

Agencies will transition to entirely digital work processes, meaning business processes including authorisations and approvals are completed digitally, and that information is created and managed in digital format.

Agencies will have interoperable information, systems and processes that meet standards for short and long term management, improve information quality and enable information to be found, managed, shared and reused easily and efficiently.
The policy is principles-based which means that it focuses on accountability and outcomes in the delivery of agencies’ objectives and services.

Each of the three parts of the policy statements mentioned on the previous slide is supported by a principle:

- Principle 1 – information is valued (ie managed as an asset)
- Principle 2 – information is managed digitally (to document digital work processes)
- Principle 3 – information, systems and processes are interoperable

The Policy requires improvements in five key domains of digital information management by the end of 2020:

- Agencies will develop and implement a comprehensive information governance framework. This includes a strategic, multi-disciplinary approach to managing information at an organisational level to ensure regulatory, business and accountability requirements are met. It means that information management will be embedded in all areas of corporate governance in agencies including risk management, security, compliance and accountability.
- Annual agency survey will report on agencies’ information management practices.
- Government information will be interoperable to facilitate information sharing and re-use, to promote efficiency and to enable open data initiatives. Interoperability will be based on standards for functionality in systems, formats and metadata.
- Business processes will be digital from end to end. Business decisions will be made and recorded digitally, using digital authorisations and workflows.
- Agencies will meet standard information management professionalism and capability levels set by the Archives.

It is expected that improvements will be made by agencies during normal business review and technology maintenance and investment cycles.
The policy identifies what success looks like for each principle and the targets that agencies should be able to reach by 2020. To help you meet the policy targets, we also identified a few interim implementation pathways. They break the targets into smaller goals with staggered implementation dates. When you meet these interim goals you will know that your agency is on track to meet the targets.

The Archives will continuously release supporting products, tools, strategies, standards and advice to assist you in the implementation of the policy. We have already published a number of new products:

• Guidance on building an information governance framework and establishing an information governance committee
• Business systems assessment framework
• Minimum metadata standard

These will be discussed in detail later in the session.

The Archives will report annually to the Government on the policy implementation progress and the status of digital information management in agencies. It will make recommendations for further improvements.

We will now discuss what agencies need to do to successfully implement the Digital Continuity Policy and to achieve its targets.
Let us now go through the policy again, its targets and pathways that will lead to achieving digital continuity for Australian Government information.
Digital Continuity is an approach to creating and managing information that can be trusted and used for as long as needed despite technological change.

Continuity is a natural step from digital transition to allow the government to capitalise on achievements made until now and to move towards the culture of fully digital information management. As noted by our Director-General at a conference in 2014:

‘we know... that business processes come and go, we know that whole Departments of State come and go, we know that software and technology become obsolete. But we also know with equal certainty that in 10, 20 or a 100 years from now we will still be deriving value from the information created by these temporary systems...It is time to rethink the balance between designing systems and creating information assets – by that I mean digital assets for a digital economy. It’s time for Digital Continuity’.

The National Archives’ Digital Continuity 2020 Policy is aimed to enable agencies to maintain digital continuity for government information.
DC2020 Principle 1: Information is valued
Focus on governance and people

Agencies will manage their information as an asset, ensuring that it is created and managed for as long as required, taking into account business and other needs and risks.

Principle 1: ‘Information is valued’ focuses on governance and people.

As we all agree that government information is an asset, so we need to make sure that it is managed as such. The policy makes clear that information is as important to agencies as their finances, property or equipment. And as any important asset, information should be managed by skilled and professional workers.

Digital information managed as a strategic asset makes the Government’s digital transformation initiatives possible and ensures that other agency governance requirements are met, including those for security, privacy, quality and accessibility.

What will success look like? We hope that in 2020:

• agency heads are accountable for information governance in their agency
• Information is created, stored, used and managed effectively and accountably destroyed if it is no longer needed
• Information governance is embedded into the overall agency corporate governance structure: they have appropriate policies, processes, standards, controls and metrics to ensure that business, information management and legislative requirements are met and risk is managed
• Information management workforce planning and capability development enable agencies to have access to appropriately skilled information management staff, and all employees and third parties acting on behalf of the Government meet their information responsibilities
By the end of 2015 your agencies were expected to reach a number of related digital transition targets:

- Agency senior management drives change
- Annual reports to the Archives are authorised by agency heads.

These were the requirements of the Digital Transition Policy and we know that many agencies have had good progress in this respect. We also communicate with agency heads quite regularly to inform them about Check-up Digital results or about other updates on our activities and initiatives to allow them to have the knowledge and to take interest in information management within their organisations.

Under the Digital Continuity approach further targets were set to be achieved by 2020:

- Annual reporting on the state of information management in each agency (through Check Up Digital or a similar tool). The Archives will also report annually to its Minister.
- Agencies will manage their information assets for as long as they are required. This is about ensuring that information governance arrangements are in place, they are implemented and reviewed on a continuous basis.
- Agencies meet targets for professionally qualified or accredited information managers. The intended result is to build up the level of information management professionalism and capability in Australian Government agencies.
Annual survey reporting targets in 2016: our information and records management practices survey is out and due for completion by 18 March 2016. Although not a distinct target of the DC2020 Policy, information gathered from agencies will contribute to our understanding of government practices and feed into planning of our own activities and products for you.

Check-up Digital submissions will be open as usual on 1 July and expected for completion at the usual time by 30 September.

We are also currently working on the new generation version of the survey tool that will be released in 2017. Any feedback on the current Check-up Digital content or process will be much appreciated and contribute to the development of the new product.

Agencies will establish an information governance committee (or equivalent) by 30 June 2016. This is the first real target for completion under the DC2020 Policy and that is why our guidance on information governance was released at the time of the Policy launch. Our guidance also includes advice and templates for the next target: Agencies will establish an IG framework by 31 December 2016. We will discuss what we expect you to do in this space later in the session.

In the area of information management skills and professionalism development, we as a government need to make continuous progress towards the 2020 goal of setting and meeting targets for professionally qualified or accredited information managers. The intended result is to build the level of information management professionalism and capability in Australian Government agencies and to give information managers an established career path and the same recognition as ICT, finance or other professional roles have.

We want the government to have information management specialist positions within agencies with standardised role descriptions, career progression and professional development requirements.
We already have our Digital information management capability matrix available for you to use while recruiting new staff or when planning professional development. We are also currently working on model role descriptions for professional information managers in government agencies. The first one will be the role of an agency senior information specialist who will coordinate the work of the Information Governance Committee.
DC2020 Principle 1: Questions and answers

What further advice can the Archives provide about the capability and professionalism targets for information management? How does the Archives expect these targets to be met?

How does the Archives see agencies establishing an Information Governance Committee?

What further advice can the Archives provide about the capability and professionalism targets for information management? How does the Archives expect these targets to be met?

The first step is to define the role of the senior information management officer position. We expect to have completed this work by June this year. We are also engaging with the tertiary sector, industry and our Government colleagues to identify skills and capabilities needed in the information management sector into the future.

Targets and pathways for achieving the capability and professionalism targets are yet to be determined however further advice will be available soon. The final recommendations will consider the varying size and structure of Government agencies.

The digital information management capability matrix (http://naa.gov.au/records-management/development/qualifications/capability-matrix/index.aspx) currently available on our website identifies skills and knowledge that government agencies and their employees need to create and manage information effectively to meet their business and accountability needs.

How does the Archives see agencies establishing an Information Governance Committee?

An information governance committee can be established as a board, a working group, or its responsibilities can be absorbed into an existing governance committee within your agency. The structure you decide to implement will depend on your agency’s specific circumstances.

There’s more advice about establishing an Information Governance Committee, including a sample terms of reference (http://www.naa.gov.au/records-management/information-governance/governance-committee/index.aspx) on our website. If you represent a micro-agency and are unsure how to meet this requirement we encourage you to contact our Agency Service Centre (http://www.naa.gov.au/records-management/help/) to discuss your specific circumstances.
What is the Archives reporting process for the Digital Continuity 2020 Policy targets?

Annual agency survey reporting in 2016 will continue through Check-up Digital. Agencies will be able to report on their progress towards the Digital Continuity 2020 targets through their assessments. In 2017-2020 a new version of the survey tool will be used. The Archives will continue to report to its Minister annually about the progress made across the government on digital information governance.

What are the consequences for not meeting these targets?

Firstly, it’s important to acknowledge there are many benefits for meeting the Policy targets. Information will be:

- Easier to find, understand and share;
- Interoperable and able to be re-used or commercialised;
- More secure; and
- Accessible and preserved for as long as needed.

The Digital Continuity 2020 Policy is issued under the Archives Act 1983. All entities, corporate and non-corporate, and wholly-owned Commonwealth companies, are required to comply with the Archives Act. If agencies do not manage records digitally, they will be unable to transfer RNA records to us – they will either need to continue to store physical records at their own cost, or convert them to digital to transfer to us. It also relates to accountability under the Public Service Act 1999— if records aren’t being created and maintained to meet long term preservation needs – which means in digital formats - there is no accountability. The Archives will also report annually to the Minister on achievements towards digital continuity, which may include identifying individual agencies which are not meeting the targets.

The interim targets are provided as a pathway to assist agencies to meet the 10 recommended actions.
Principle 2: Information is managed digitally focuses on digital assets and processes.

What will success look like?

- Agencies will have entirely digital work processes and keep information in accessible digital form, for as long as it is required.
- They will work digitally by default and transition analogue or immature digital processes to efficient and mature digital processes that maximise information value.
- Where there are benefits for agency business, information in analogue formats will be migrated to digital format.

Developing end-to-end digital work processes provides opportunity for agencies to establish more mature and efficient procedures and services that engage the public directly and effectively with additional benefit of opportunities for continuous improvement and innovation. This very much in line with the Government’s digital transformation agenda and initiatives.

Information created by digital processes will be completely digital and will be managed digitally. Properly automated workflows should record decisions and authorisations digitally. Records resulting from such processes should be to an evidentiary standard and be able to be used and reused for as long as they are needed. And some of them will need to be available in perpetuity as the archival resources of the Commonwealth.
DC2020 Principle 2: Targets and pathways

By 2016 (Digital Transition)
- Reduced reliance on paper and duplication of information in digital and physical formats
- Paper-based business processes are identified
- All records created in digital formats from 1 January 2016 to be managed digitally.

By 31 December 2020 (Digital Continuity)
- Agencies have entirely digital work processes and keep information in an accessible digital form.
- Where there are benefits for agency business, information in analogue formats is migrated to digital format.

Again here we are starting from a sound basis of the Digital Transition Policy achievements:


And we know that many agencies have done these things and are in the position to manage their information digitally. Most of agencies comply with the January 2016 target and we are working with those that haven’t to assist them with making sure that information is managed properly. We published advice on the website on what agencies can do to succeed.

There are 2 Digital Continuity 2020 targets that focus on digital processes and digital formats for information. Whatever digital transformation is taking place in your agencies, we do not expect anything to be done for the sake of doing it: any transformation should bring you business benefits of more effective and efficient outcomes.

To help you to achieve the 2020 targets we have identified pathways to those targets.
DC2020 Principle 2: Targets and pathways

To do now

• Identify high-value and long-term information assets, evaluate risk and management requirements, and implement strategies by 31 December 2016
• Identify strategies for all information assets by 31 December 2018 and implement them by 31 December 2019
• Transform most paper-based processes to digital and routinely make and record decisions using digital authorisations and workflows by 31 December 2017

These pathways are closely connected to the targets under Principle 1: the emphasis here is on implementing your information governance arrangements to make sure that your information assets are managed properly. It is not enough to just identify your information assets, evaluate risk and management requirements and to have strategies. You need to implement them to ensure that information is safe, accessible, useable and that it is destroyed when you can or transferred to the Archives. That is why we want you by the end of this year to identify at least your high-value and long-term information assets and to implement strategies for managing them in compliance with your legislation, external and internal requirements and other necessary considerations. By the end of 2019 all information assets should be managed properly and digitally.

To help to get to this point, you could transform most of paper-based processes to digital and also routinely make and record decisions using digital authorisations and workflows. This could be achieved by the end of the next year.

We already have a number of information governance templates that will help you with planning and putting the necessary framework in place. We have had advice on how to conduct an information review on our website for a while now. It is currently been updated to give you more tools and examples. Our new product on business systems assessment to be discussed later in the session has a template for a system information management plan, which can be used here. The business systems assessment framework itself can help you to identify the value of your information and the management requirements.

The work is about to be started on guidance on digital authorisations which will hopefully be published by the end of the financial year.

The last points here:
• ongoing disposal of information is part of management process and records authorities are the enablers for you to do this.
• Migration of information, decommissioning of legacy systems and digital preservation activities are all part of what needs to be done under Principle 2: Information is managed digitally. The emphasis is on ‘managed’.
How does the Archives intend to help agencies with managing technical obsolescence?

Digital continuity is about ensuring your agency’s digital information is managed well so that it can be accessed and used over time. The Digital Continuity 2020 policy encourages agencies to use best practice in the management and preservation of digital records and information to achieve this.

As each agency’s business systems, information and data sets are unique to its core business, how an agency should manage technical obsolescence is dependent upon several factors, including: As

- the technology that is currently being used by the business, and what they are likely to acquire in the near future
- the most financially feasible option, based upon a risk analysis that takes into account the agency's accountability obligations, the type of information and data held; and
- the long term implications for the integrity of the agency’s records of any preservation processes adopted.

Application of appropriate information governance and identification of the businesses information assets through information reviews and risk assessments will allow agencies to identify potential risks for file format and digital obsolescence. Agencies need to develop and implement a proactive program to identify records at risk and take necessary action to ensure their ongoing viability.

The Archives has information and resources available for agencies to assist them with addressing this challenge. This includes:

assist agencies in assessing information risks and values and identifying system functionality required to manage information appropriately.

- Advice around information governance committees (http://naa.gov.au/records-management/information-governance/governance-committee/index.aspx) to enable agencies to develop a consistent, systematic and whole-of agency approach to managing information.

**What advice does the Archives have about using digital approvals?**

The third principle is about interoperability of information, systems and processes. It focuses on metadata and standards.

The Government’s digital transformation initiatives (https://www dto.gov.au/) will make government services simpler, faster and easier to use. These initiatives will be enabled by interoperable information, systems and processes which make it less costly and easier to share information, improve information quality, reduce unnecessary duplication and the impact of structural changes in government.

As we know, interoperability is an issue every time there is a machinery of government change, every time there is a restructure or reorganization across agencies.

What will success look like? By 2020:

- Agency information, systems and processes are interoperable and meet standards for short and long-term management
- Australian Government processes incorporate information governance requirements and specifications to ensure that information remains findable, sharable and reusable

We need to have and use standards for metadata, information quality, and file and data formats.
DC2020 Principle 3: Targets and pathways

By 31 December 2020 (Digital Continuity)
• Information is managed based on format and metadata standards for information governance and interoperability.
• Business systems meet functional requirements for information management.
• Cross-agency and whole-of-government processes incorporate information governance requirements and specifications.

DC2020 targets include:

• Information is managed based on format and metadata standards for information governance and interoperability.
• Business systems meet functional requirements for information management.
• Cross-agency and whole-of-government processes incorporate information governance requirements and specifications.

Achieving interoperable information, systems and processes takes time and requires interoperability to be planned, designed and integrated from the initial stages. A more efficient way to do this would be at the whole-of-government and cross-agency levels. And some work has been already done, but much more needs to be accomplished in this space.
The 2020 targets set the bar quite high. Here is what could you do to achieve success by following the pathways we identified.

- Business systems procured after 31 December 2016 should meet the minimum metadata standards and be evaluated against the Archives’ business systems assessment framework to meet functional requirements for information management
- Existing systems with high-value and long-term information meet minimum metadata standards by 31 December 2017
- All systems are evaluated against the Archives’ business systems assessment framework by the end of 2018 and functional requirements are implemented where necessary.

We have recently issued the key products to enable you to implement these pathways on the way to 2020 targets: the minimum metadata set and the business systems assessment framework. They will be presented to your later in the session.
In relation to the Minimum Metadata Set, can you provide guidance on using the <title> property?

The title should be human-readable text which provides a description of the content of the record and assists with discovery. In a business system which doesn’t require a title, it can be compiled from other relevant fields, for example the name of the applicant and date of application. For further advice refer to the metadata set reference tables (http://www.naa.gov.au/records-management/agency/minimum-metadata/minimum-metadata-set-reference.aspx)

In relation to the Minimum Metadata Set, why isn’t a date of destruction included as a mandatory property?

The minimum metadata set applies to all records. It thus only includes metadata properties which are relevant to all records and information. Date of destruction only applies to records which have been destroyed – it does not apply to current records, or records which will never be destroyed, hence does not form part of the minimum metadata set.

In addition to the minimum metadata, your agency should capture any additional metadata needed to meet your business and information management needs. This includes metadata needed to support information management processes such as disposal date or end date (date of destruction). Under the AFDA, metadata for destroyed records, including the date of destruction, is RNA and must be retained for accountability purposes.

Will the Minimum Metadata Set result in less metadata being applied to some information?

No. As noted above, in addition to the minimum metadata, agencies should capture any additional metadata needed to meet business and information management needs. The minimum metadata set has been identified to support interoperability, in particular the
transfer of information between systems within an agency, between agencies, or to the Archives. You should ensure that systems in your agency capture the minimum metadata properties as a minimum, while still capturing all other metadata needed for your business and information management needs.

The Archives can and will accept all other metadata captured by agencies when RNA records are transferred to the Archives.

**How does the Archives see the Business Systems Assessment framework influencing ICT procurement processes and what is the role of the Information Governance committee for this?**

The Business System Assessment Framework will be a useful tool to build into your agency’s internal ICT procurement processes to ensure that new systems have appropriate information management functionality. Your information governance committee will be a mechanism to achieve this. Part of the role of the information governance committee would be to:

- approve business cases for the procurement or development of business systems and ensure these systems meet appropriate standards and needs

- oversight of assessments against the Framework to ensure existing systems have the necessary functionality to manage business information needs and risks.
The Digital Continuity 2020 Policy is a 5-year policy with the key targets to be achieved by 2020. We will continuously release supporting products, tools, strategies, standards and advice to assist you in the implementation of the policy.

We will also collaborate with agencies and key partners to develop whole-of-government products, strategies and standards.

We have already released new products and you’ll hear more about them in a moment.
Information Governance
Information governance

Information governance is an approach to managing information assets across an entire organisation to support its business outcomes.

It involves having frameworks, policies, processes, standards, roles and controls in place to meet regulatory, legal, risk and operational requirements.

Information governance is an essential element of corporate governance that must be aligned with business outcomes and risks.

The National Archives’ updated definition of information governance to complement the Policy. The definition emphasises the strong link to business outcomes and information as an asset.
The IG related targets are the foundation and facilitate all DC 2020 targets - digital continuity will fail if left to chance.

Good information governance at agency level will give the Government greater leverage to pursue whole-of-Government information and data initiatives.

**Often the focus of governance is compliance. Information governance is more than compliance.**

You need control of your information in order to comply with legislation and regulations, but information governance is also about treating the information as an asset.

As we head towards 2020, we will have the capacity to looking at what broader opportunities information and data can bring - in addition to ensuring it is created, stored and managed for as long as it is required.

Information governance is also misunderstood as IT governance. Managing the hardware and software that manages the information is only part of the broader IG agenda.
Information governance is holistic; it considers all data and information regardless of format, wherever it is held.

The Policy recognises that poor digital information governance can result in the information becoming unreliable, out of date or unavailable, being misused, difficult to find or interpret, or having uncertain status or authority.

Poor digital information governance can be a cause of major inefficiency and can introduce major risks to the agency, to the government and to citizens, other customers and suppliers.

It is a false economy to underinvest in digital information governance. The cost and consequences of poor information governance may not be immediate, but will always need to be faced eventually.

As for all resources or assets that need to be managed, the key is to ensure that the governance investment is appropriate to the business risks and value of the asset.

The planning and monitoring to achieve and maintain continuity of digital information requires good governance to make sure that it occurs.
Information governance framework

31 December 2016 target: Agencies will develop and implement a comprehensive information governance framework.

An information governance framework is the legal, regulatory and business context within which information assets are created, used and managed. Documenting this for your agency sets out an approach and commitment to implementing an effective information governance framework and the controls that are required to maintain it.

Documenting the framework:
- outlines the broad environment within which information is created and managed;
- describes the factors and business drivers which determine or influence the creation, management and use of information, including legislation, regulations, compliance, risk, and business needs;
- documents the principles which guide the creation, management and use of information;
- provides an overarching description of how information is governed with particular emphasis on whole-of-agency coordination, planning and leadership; and
- documents your organisation’s commitment to information governance and provides senior management endorsement.

The framework also provides the overarching context within which other information governance documents, such as your information, records and data management strategies, policies and related procedures, can be understood.

The information governance framework template (http://www.naa.gov.au/records-management/strategic-information/information-governance/key-documents/framework.aspx) on our website provides a useful guide to the key aspects and components to include in an agency framework.

Accountability is at the core of digital information governance framework
In order to have clear accountability, it is necessary to identify who has overall responsibility for how digital information is managed and used, and who is responsible for each significant digital information asset. The nature and purpose of the digital information assets needs to be understood.

Conducting an information review (http://www.naa.gov.au/records-management/agency/digital/digital-continuity/plan/conducting-an-information-review.aspx) is recommended to understand the value of your information assets.

Additional information on our website about building a robust information governance.
Establishing an IG Committee

- Oversees all information-related matters
- Reviews the effectiveness of your information governance framework, strategies, policies and architecture.
- Allows representation from all relevant information stakeholders
- Not necessarily a separate committee
- Appropriate to the size of your agency
- Further advice on the National Archives’ website, including the role, the structure and sample terms of reference

The information governance committee will be responsible for all information matters ranging from compliance, strategy and infrastructure to metadata standards and privacy. It requires key senior management buy-in and support from all relevant information specialist stakeholders such as those responsible for ICT, business, information management, security. The first target - due to be in place by 30 June 2016.

Establishes and reviews the effectiveness of your information governance framework, strategies, policies and architecture.

It’s purpose is to:

- Oversee all information matters ranging from compliance, strategy and infrastructure to metadata standards and privacy
- Allow senior management buy-in and support from all relevant information specialist stakeholders such as those responsible for ICT, legal, business, information management, security, privacy, and freedom of information. These specialisations join to minimise information risks and maximise the value of information assets.

An information governance committee can be established as a board, a working group, or its responsibilities can be absorbed into an existing governance committee. Your agency is in the best position to set up a workable committee and determine where it sits in your organisational structure.

Membership of the committee should be appropriate to the size and complexity of your agency. Senior representation is required from all information, data and records stakeholders.

Part of it’s role is to define, assign and coordinate information-related roles and responsibilities. By mapping out roles and responsibilities your agency will be in a better position to manage risks associated with information.
The information governance committee, particularly for smaller agencies, can be absorbed into an existing governance committee.

Advice about the role of the committee, how it might be structured for your agency and sample terms of reference for an information governance committee are on the National Archives' website.
Business Systems Assessment Framework
Minimum Metadata Set
### Business System Assessment Framework

<table>
<thead>
<tr>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>31 December 2016</td>
<td>Business systems procured after this date will be evaluated against the Archives' business systems assessment framework to meet functional requirements for information management.</td>
</tr>
<tr>
<td>31 December 2018</td>
<td>All existing business systems are evaluated against the Archives' business systems assessment framework to meet functional requirements for information management.</td>
</tr>
<tr>
<td>31 December 2020</td>
<td>All business systems meet functional requirements for information management.</td>
</tr>
</tbody>
</table>

The business systems assessment framework is a key product supporting Principle 3 of the Digital Continuity 2020 Policy.

Essentially, this framework and its associated targets is really all about assessing what information management functionality is needed in business systems in order to ensure that the information and records they contain are appropriately managed. Key targets that relate to the framework include:

- **31 December 2016**
  - Business systems procured after this date will be evaluated against the Archives’ business systems assessment framework to meet functional requirements for information management.

- **31 December 2018**
  - All existing business systems are evaluated against the Archives’ business systems assessment framework to meet functional requirements for information management.

- **31 December 2020**
  - All business systems meet functional requirements for information management.

It is important to note here that whilst the target mention the need to assess against the Archives assessment framework, it is by no means mandatory to use this. We know that a number of you have you own approach to this, and our framework has been informed by this, so the approach you have adopted to fit your purposes is equally valid. The main thing here is that you’re assessing business systems for information management functionality.

The assessment framework also supports targets in:
- Principle 1 by providing a key tool for building sound information governance in your agency;
- and
- Principle 2 by helping to identify weaknesses in business processes such as paper-reliant work flows and approvals.

ISO 16175 sets out a number of requirements for assessing information management functionality, however given the complexity of the standard, we have developed this framework to provide a more practical approach.

The framework provides a consistent approach for Australian Government agencies in assessing business systems for information management functionality. The framework will enable your agency to better manage its business information 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
- ensuring greater accountability, transparency and enhanced service delivery.

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

The framework can be applied to both new and existing systems and can be used by information and records management practitioners, ICT staff and business owners. The framework does not apply to Electronic Document and Records Management Systems (EDRMS).

The framework has three phases:
**Phase 1** is a risk assessment. You use this phase to assess each system to determine the extent of the functionality assessment in phase 2. It is likely that low risk, low value systems get ticked off here without any further work required.

**Phase 2** is the section of the framework which is actually aligned with Part 3 of ISO16175. This is divided into **four modules**. This way, systems are only assessed against the modules that are relevant to them based on their phase 1 assessment.

**Phase 3** provides guidance on how to address any gaps identified in Phase 2.

The framework is now available on our website. It consists of an overview page, 3 diagrams covering each phase of the framework as well as a checklist and supporting guidelines for phase 1 and 2.

I’ll now talk about how each phase works in a bit more detail.
Phase 1: Risk assessment

How important is this system?

Note: image in this slide is hyperlinked (http://www.naa.gov.au/Images/Phase-1-Risk-Assessment_tcm16-89010.pdf)

Phase 1 is a risk assessment. Essentially, at this phase one needs to determine how important the system is, as the extent of the assessment will determine on the value and importance of the system.

The risk assessment consists of six decision points or questions that test your risk tolerance:

Three decision points determine the importance of the system and information. If the system and the information have sufficient risk or value, the risk assessment guides you to the Information is trusted module in Phase 2. One decision point relates to disposal and asks whether there is sufficient business benefit for managing disposal within the system.

Finally, there are two decision points 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 or import functionality is a requirement for your system.

Depending on the outcomes of the risk assessment, you may then be required to complete up to four of the Phase 2 assessment modules.
Phase 2: Functionality Assessment

How well does the system manage records?

**Note:** image in this slide is hyperlinked (http://www.naa.gov.au/Images/Phase-2-Functionality-Assessment_tcm16-89011.pdf)

Phase 2 is the actual functionality assessment of the system. It is at this phase where we are trying to determine how well the system manages records.

The functionality assessment consists of 4 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 AS ISO 15489: *Australian and International Standard for Records Management: authenticity, integrity and reliability*. The mechanisms for meeting the requirements in this module rely wholly on the system’s metadata.

**Module 2: Disposal is accountable**
This module is for those cases 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
- manage multiple disposal classes if you need to.

**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 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.
Phase 3: Implement Solution

How do I fix it?

Note: image in this slide is hyperlinked (http://www.naa.gov.au/Images/Phase-3-Implementing-Solutions_tcm16-89012.pdf)

Phase 3 provides suggestions on how to manage any shortfalls, gaps or risks identified in Phase 2. Essentially, this phase provide options for fixing any gaps. 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. If the risk is acceptable, make a record of the decisions and reasons.

If the risk is not acceptable, consider your options for implementing a solution. The four broad solutions options include:

- **build in**
- **integration**
- **external (export)**
- **external (governance).**

**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.

**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 the business system with your agency's EDRMS and manage the disposal process there.

**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 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).

**Solution 4: External (governance)** – 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.
The minimum metadata set is the other tool that has been developed to support Principle 3 (interoperable information, systems and processes). The targets for minimum metadata are very similar to those for the business system assessment framework. They are progressive with targets first applying to new systems procured after 31 January 2017, the second applying from the end of 2017 to systems which contain high value and long term information assets and the final target applying to all systems, including those which hold low value information from the end of 2020.

Just to explain a few terms used in the targets – namely minimum metadata standards, and business systems.

By business systems, we mean any system which holds information. This of course includes EDRMSs, as well as any other line of business systems which hold information. It excludes transactional systems which do not hold information.

The reference to minimum metadata standards refers to the minimum metadata set, which we are about to look at more closely. Basically, in order to meet minimum metadata standards, we expect systems which hold information to be able to capture as a minimum, the metadata properties in the minimum metadata set.
Minimum Metadata Set

- Identifies metadata properties essential for agency management of information as well as those needed for records which will be transferred to the Archives
- Supports Digital Continuity 2020 Principle 3 for interoperable systems and processes
- Practical application of the Australian Government Recordkeeping Metadata Standard 2.0 (AGRkMS)

The minimum metadata set identifies metadata properties essential for agency management of information as well as those needed for records which will be transferred to the Archives. It supports the Digital Continuity 2020 principles of interoperable systems and processes (Digital Continuity 2020 principles of interoperable systems and processes) and is a practical application of the Australian Government Recordkeeping Metadata Standard 2.0 (AGRkMS) (http://www.naa.gov.au/records-management/publications/agrkms/index.aspx) to support metadata implementation and information use in agencies.

The set was developed in consultation with a focus group and is consistent with minimum metadata requirements in other Australian and overseas jurisdictions. The aim in developing the set was to identify the minimum properties necessary for agencies to manage their information, as well as those needed to support Archives business processes for those records that will be transferred to the Archives. We were concerned in development of the set to restrict it as far as possible to those properties which were already being captured by agencies for their business purposes. This means that agencies using an Electronic Document and Records Management System (EDRMS) to manage their information should already meet the minimum metadata standard as EDRMS’ can capture the required metadata.
The minimum metadata set consists of a total of 9 properties. The set is cumulative, with the Core properties applying to all systems, the Additional properties added for systems which hold high value and long-term information assets, and the Transfer properties added to complete the set for systems holding records of archival value that may be transferred to the Archives.

The first three properties are required to be captured for all systems. They are Identifier, Creator and Date created.

The Additional Properties are Title, Protective Marking (or security classification), Disposal Class and Format.

The final set applies to records of archival value which may be transferred to the Archives – although they should also be captured if you are retaining these higher value records in your agency to assist with access and preservation over time. These are Rights and Integrity Check. Rights refers to whether the public access status of the information and should capture information about whether or not the record has already been made publicly available for example through publication on the Agency website or under FoI, or whether it contains any sensitivities which may impact on its ability to be made publicly available once it reaches the open access period. The integrity check also assists with ensuring that records maintain their integrity and authenticity over time. Records in the Transfer group have a long retention period – ie permanently which means that without a doubt they will need to be migrated from one system to another and probably more than once to ensure their ongoing preservation and accessibility. Undertaking an integrity check at the point of transfer and capturing this metadata ensures you can validate the authenticity of that information.

You’re probably looking at this set and thinking that there’s a lot of other metadata that you capture and use as part of ongoing management of records and information in your agency. That’s fine, you should continue to do that! Any metadata that you need to manage your
records and information should be captured and maintained. When it comes to transfer to the Archives, we can and will accept all other metadata that has been captured.
In terms of meeting the Digital Continuity targets, you only need to ensure that your systems capture the metadata appropriate to the value of the information held by the system.

For example, business systems which only manage low-value information and records need only capture the Core minimum metadata. Systems which hold a mix of low value and high value information and records, excluding records of archival value, should capture both Core and Additional properties. Systems which include records of archival value should capture the full minimum metadata set (Core, Additional and Transfers).

All EDRMS should be capable of capturing the metadata identified in the minimum metadata set. Business systems should be designed or adapted to capture the level of minimum metadata appropriate to the information they hold and manage.

As mentioned, the minimum metadata set is based on the Australian Government Recordkeeping Metadata Standard AGRkMS 2.0. The properties in the minimum set have all been mapped to AGRkMS in reference tables which are available on our website. The reference tables also indicate where additional sub-properties must be used. These reference tables should be referred to when implementing the minimum metadata set in your agency.

The Business Systems Assessment Framework which we discussed earlier also includes a component to assess whether your systems meet minimum metadata standards to support reliability and integrity of information.

That’s just been a brief overview of the business systems assessment framework and the minimum metadata set. There’s more information on our website, and we’ll be happy to take any questions at the end of this session.
Next steps

• NAA committed to providing additional implementation advice and products
• Welcome suggestions for implementation advice and products

Today we discussed what supporting products, tools, strategies, standards and advice are currently available (to assist you in the implementation of the policy).
• There is more to be done in terms of implementation advice and products.
• We welcome feedback about any gaps in our advice and products
• We also value any feedback on existing advice and products.