

# **Implementation of the Digital Continuity 2020 Policy**

Across Entities

© Commonwealth of Australia 2019

ISSN 1036–7632 (Print)

ISSN 2203–0352 (Online)

ISBN 978-1-76033-898-5 (Print)

ISBN 978-1-76033-899-2 (Online)

Except for the content in this document supplied by third parties, the Australian National Audit Office logo, the Commonwealth Coat of Arms, and any material protected by a trade mark, this document is licensed by the Australian National Audit Office for use under the terms of a Creative Commons Attribution-NonCommercial-NoDerivatives 3.0 Australia licence. To view a copy of this licence, visit <http://creativecommons.org/licenses/by-nc-nd/3.0/au/>.

You are free to copy and communicate the document in its current form for non-commercial purposes, as long as you attribute the document to the Australian National Audit Office and abide by the other licence terms. You may not alter or adapt the work in any way.

Permission to use material for which the copyright is owned by a third party must be sought from the relevant copyright owner. As far as practicable, such material will be clearly labelled.

For terms of use of the Commonwealth Coat of Arms, visit the *It's an Honour* website at <https://www.pmc.gov.au/government/its-honour>.

Requests and inquiries concerning reproduction and rights should be addressed to:

Senior Executive Director  
Corporate Management Group  
Australian National Audit Office  
19 National Circuit  
BARTON ACT 2600

Or via email:

[communication@anao.gov.au](mailto:communication@anao.gov.au).



Canberra ACT  
31 October 2019

Dear Mr President  
Dear Mr Speaker

In accordance with the authority contained in the *Auditor-General Act 1997*, I have undertaken an independent performance audit across entities titled *Implementation of the Digital Continuity 2020 Policy*. Pursuant to Senate Standing Order 166 relating to the presentation of documents when the Senate is not sitting, I present the report of this audit to the Parliament.

Following its presentation and receipt, the report will be placed on the Australian National Audit Office's website — <http://www.anao.gov.au>.

Yours sincerely



Grant Hehir  
Auditor-General

The Honourable the President of the Senate  
The Honourable the Speaker of the House of Representatives  
Parliament House  
Canberra ACT

## AUDITING FOR AUSTRALIA

The Auditor-General is head of the Australian National Audit Office (ANAO). The ANAO assists the Auditor-General to carry out his duties under the *Auditor-General Act 1997* to undertake performance audits, financial statement audits and assurance reviews of Commonwealth public sector bodies and to provide independent reports and advice for the Parliament, the Australian Government and the community. The aim is to improve Commonwealth public sector administration and accountability.

For further information contact:  
**Australian National Audit Office**  
**GPO Box 707**  
**Canberra ACT 2601**

**Phone: (02) 6203 7300**  
**Fax: (02) 6203 7777**  
**Email: [ag1@anao.gov.au](mailto:ag1@anao.gov.au)**

Auditor-General reports and information about the ANAO are available on our website:  
<http://www.anao.gov.au>

### Audit team

Joyce Knight  
Nathan Callaway  
Jessica Kanikula  
Paul Bryant

# Contents

---

Summary and recommendations.....	7
Background .....	7
Conclusion .....	8
Supporting findings.....	9
Recommendations.....	10
Summary of entity responses .....	12
Key messages from this audit for all Australian Government entities .....	14
<b>Audit findings.....</b>	<b>15</b>
1. Background .....	16
Introduction .....	16
Rationale for undertaking the audit .....	20
Audit approach .....	21
2. Administration of the Digital Continuity 2020 policy .....	22
Have effective internal arrangements been established for the administration of the Digital Continuity 2020 policy by the National Archives of Australia? .....	22
Did the National Archives of Australia develop products, advice, and guidance material that are fit for purpose? .....	24
Does the National Archives of Australia effectively engage with stakeholders to administer the Digital Continuity 2020 policy? .....	29
Are risks to the implementation of the Digital Continuity 2020 policy being effectively identified, managed and reported? .....	32
3. Monitoring and evaluation arrangements for the Digital Continuity 2020 policy .....	34
Has the National Archives of Australia designed appropriate monitoring and evaluation arrangements? .....	34
Do the monitoring and evaluation arrangements accurately assess the extent to which entities are meeting the targets of the Digital Continuity 2020 policy? .....	40
4. Implementation of the Digital Continuity 2020 policy by the selected entities.....	46
Have the selected entities achieved the targets of the Digital Continuity 2020 policy? .....	46
Have the selected entities established effective internal arrangements to monitor and report on progress against the targets of the Digital Continuity 2020 policy? .....	61
<b>Appendices .....</b>	<b>65</b>
Appendix 1     Entity responses .....	66
Appendix 2     Digital Continuity 2020 targets and pathways .....	72
Appendix 3     The information management legislative, regulatory, and policy environment.....	75
Appendix 4     Criteria used to select entities.....	79
Appendix 5     Criteria used to assess the appropriateness of performance information .....	80
Appendix 6     The average digital maturity assessments of the selected entities for 2018 .....	81
Appendix 7     Internal monitoring and reporting guidance for information management.....	83



# Summary and recommendations

---

## Background

1. On 27 October 2015, the Secretary of the Department of Finance and the Director-General of the National Archives of Australia (the Archives) launched the Digital Continuity 2020 policy (policy). The objectives of the policy are for entities to:

- manage information as an asset, ensuring that it is created and managed for as long as required;
- 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; and
- have interoperable information, systems and processes that meet standards for short and long-term management, improve information quality, and enable information to be accessible, transferrable, and re-usable.

2. The policy was issued under the *Archives Act 1983*<sup>1</sup> and applies to all government information, data and records, in addition to systems, services, and processes. The policy is to be implemented by all Australian Government entities, including Government Business Enterprises.

## Rationale for undertaking the audit

3. Australian Government entities are legally required to manage information in a manner that properly records and explains its performance.<sup>2</sup> Effective information management supports accountability and transparency, and enables informed decision making.<sup>3</sup> The Australian Government's transition to digital service delivery creates both opportunities and risks to effective information management. The Archives has an important responsibility to ensure that an appropriate framework is designed and applied to support this transition process, and the Digital Continuity 2020 policy is central to this in providing a whole-of-government approach to digital information governance. The final targets of the policy are due for implementation by 31 December 2020, and it is therefore timely to examine the extent to which entities have implemented the policy, and how effectively the Archives is administering and overseeing its implementation.

## Audit objective and criteria

4. The objective of this audit was to examine the extent to which Australian Government entities have implemented the Digital Continuity 2020 policy, and how effectively the National

---

1 *Archives Act 1983*, Provision 2A Objects of this Act, subsections 2A(a)iii and 2A(b).

2 A record is defined by the *Archives Act 1983* as: a document, or an object, in any form (including any electronic form) that is, or has been kept by reason of: a) any information or matter that it contains or can be obtained from it; or b) its connection with any event, person, circumstance or thing.

3 Section 37 of the *Public Governance, Performance and Accountability Act 2013* (PGPA Act) sets out the requirements for Commonwealth entities to keep records that properly document and report the entity's non-financial performance. Section 38 of the PGPA Act sets out the requirement for Commonwealth entities to measure and assess its performance in achieving its objectives, function and role. The capacity of an entity to meet this requirement is directly reliant on the entity keeping accurate and complete records.

Archives of Australia is monitoring, assisting, and encouraging entities to meet the specified targets of the policy.

5. To form a conclusion against the audit objective the ANAO adopted three audit criteria.
  - Has the National Archives of Australia established effective arrangements to administer the Digital Continuity 2020 policy?
  - Has the National Archives of Australia implemented effective monitoring and evaluation arrangements?
  - To what extent have selected Australian Government entities implemented the Digital Continuity 2020 policy?
6. The audit has examined the administration, oversight, monitoring and evaluation arrangements for the Digital Continuity 2020 policy, and the extent to which three selected Australian Government entities — the Attorney General’s Department (AGD), the Civil Aviation Safety Authority (CASA) and the Office of the Inspector-General of Intelligence and Security (IGIS) — have implemented the policy.

## Conclusion

7. The Australian Government is unlikely to achieve the objectives of the Digital Continuity policy by the end of 2020, and the National Archives of Australia (the Archives) has been largely ineffective in monitoring, assisting, and encouraging entities to meet the targets of the policy.
8. The Archives’ arrangements to administer the Digital Continuity 2020 policy are limited in effectiveness. Appropriate governance arrangements to provide strategic direction and oversight of the policy were not maintained. The products, advice, and guidance material issued by the Archives to support entities implement the policy are largely fit for purpose, with some exceptions in relation to the clarity of terminology and timeliness. The Archives does not have a stakeholder engagement and communication strategy, and does not effectively target entities requiring additional assistance to implement the targets of the policy. Risks to the implementation of the Digital Continuity 2020 policy are not being effectively identified, managed, or reported.
9. The effectiveness of the arrangements for monitoring and evaluating the implementation of the Digital Continuity 2020 policy are limited. The priorities, objectives, and targets utilised by the Archives to measure its performance in overseeing the implementation of the policy have not been designed to appropriately align with the policy’s objectives. Monitoring and reporting processes have been integrated into an annual whole-of-government survey, however the performance information is not clearly aligned with the policy itself, is not subject to sufficient quality assurance processes, and does not include clear and consistent benchmarks to measure success.
10. AGD, CASA, and IGIS have partially implemented the targets of the Digital Continuity 2020 policy due by 31 December 2018. AGD has fully implemented or made substantial progress against all of the targets. CASA has partially implemented all targets except for one. IGIS has not implemented a number of targets, particularly those associated with principle two of the policy. AGD and CASA have established specific arrangements to internally monitor and report on progress against the targets of the policy. IGIS does not have such arrangements.



## Supporting findings

### Administration of the Digital Continuity 2020 policy

11. Internal arrangements for the administration of the Digital Continuity 2020 policy by the Archives are not effective. The Archives has not developed an effective implementation strategy and has not maintained appropriate governance, oversight, and reporting arrangements.
12. The products, advice, and guidance material developed and released by the Archives to support the implementation of the Digital Continuity 2020 policy are largely fit for purpose, noting some deficiencies in the consistency of terminology within the guidance, and timeliness in relation to the delivery of supporting products.
13. The Archives' engagement activities with stakeholders to administer the Digital Continuity 2020 policy are limited in effectiveness. There is no communications or stakeholder engagement strategy in place for the implementation of the policy. In practice, communication occurs with stakeholders through a variety of channels including online, face-to-face, telephone, and annual surveys, however there has been no formal process to identify entities who are experiencing difficulties in implementing the policy and provide targeted assistance.
14. Risks to the implementation of the Digital Continuity 2020 policy are not being effectively identified, managed, and reported. A risk management plan for the implementation of the policy as a coordinated program of work was not established. Risks for a small number of individual projects associated with the implementation of the policy have been identified, however there is no evidence that these risks are being appropriately managed and reported.

### Monitoring and evaluation arrangements

15. Monitoring and evaluation arrangements were not designed appropriately. The Archives has not maintained consistent priorities and objectives in relation to the implementation of the policy since 2015–16, and the measures selected by the Archives to assess its performance in the roll-out of the policy require improvement in relation to relevance, reliability, and adequacy. The Archives has not obtained consistent and comparable data to enable an accurate analysis of entity progress to implement the policy over time, and has not taken action to define clear and consistent measures of success.
16. There are limited arrangements to accurately assess entity progress to implement the policy. Performance information is collected using an annual survey process, however the surveys have not been structured in a way that enables a direct view of entity progress to implement the policy. An analysis of a selection of questions from the 2018 survey, which could be linked to the policy, indicates a large portion of entities across government are at lower levels of maturity against the policy principles. The Archives has achieved high participation rates for the survey, however the absence of any processes in 2017 and 2018 to verify the accuracy of entity self-assessments means that there is minimal assurance regarding the accuracy of these results. The 2018 progress report to the responsible Minister is ten months overdue.

### Implementation of the Digital Continuity 2020 policy by the selected entities

17. AGD, CASA, and IGIS have partially achieved the 17 Digital Continuity 2020 targets due by 31 December 2018. All entities have implemented the majority of targets under principle one

associated with information governance. AGD and CASA have made progress in the management of information digitally under principle two. Although IGIS may be unable to digitise a selection of analogue records due to originator entity restrictions, it has not implemented any of the general targets associated with the management of information digitally. Work is required by all entities to implement the interoperability targets under principle three. However, AGD and CASA have commenced work to transfer remaining paper-based processes to digital, identify all information assets, and ensure that business systems will meet the minimum metadata and information management functional requirements.

18. Two of the three selected entities have established effective arrangements to monitor and report on progress against the targets of the Digital Continuity 2020 policy. AGD has established specific reporting arrangements within existing governance structures to internally monitor progress. CASA has consolidated previously separate reporting arrangements into a single governance committee and associated reporting structure. IGIS does not have formal arrangements in place to internally monitor or report on progress against the policy targets.

## Recommendations

19. The report makes seven recommendations to improve the administration, monitoring and evaluation arrangements, and encourage entities to prioritise the implementation of strategies to achieve the targets of the policy that have not yet been met.

### Recommendation no.1

#### Paragraph 2.8

The National Archives of Australia should establish effective internal arrangements to administer and oversee the implementation of the Digital Continuity 2020 policy, and any successor policies. The arrangements should include appropriate governance structures and a strategy to guide the administration of the Digital Continuity 2020 policy, and any successor policies, as a coordinated program of work.

**National Archives of Australia response:** *Agreed.*

### Recommendation no.2

#### Paragraph 2.38

The National Archives of Australia should develop and implement a stakeholder engagement and communication strategy that:

- (a) includes measures to ensure that entities are appropriately consulted when introducing new or revised targets; and
- (b) establishes mechanisms to ensure targets are clearly identified and consistently communicated as either mandatory, suggested, or optional.

**National Archives of Australia response:** *Agreed.*

### Recommendation no.3

#### Paragraph 2.45

The National Archives of Australia should develop and implement a risk management plan for the successful implementation of the Digital Continuity 2020 policy, and any successor policies.

**National Archives of Australia response:** *Agreed.*

**Recommendation  
no.4****Paragraph 3.23**

The National Archives of Australia should establish appropriate monitoring and evaluation arrangements for the Digital Continuity 2020 policy, and any successor policies that:

- (a) include performance measures that are relevant, reliable, and adequate in order to enable an accurate assessment of performance against strategic objectives, and the effectiveness of the administration and oversight arrangements to support achievement of the policy objectives;
- (b) capture consistent performance information to enable accurate analysis of the performance of entities to implement targets over the life of the policy; and
- (c) clearly define how success will be measured and reported.

**National Archives of Australia response:** *Agreed.*

**Recommendation  
no.5****Paragraph 3.43**

The National Archives of Australia should develop and implement a regime to provide appropriate assurance on the accuracy of reported data on entity progress in the implementation of the Digital Continuity 2020 policy.

**National Archives of Australia response:** *Agreed.*

**Recommendation  
no.6****Paragraph 4.58**

The Civil Aviation Safety Authority should:

- (a) review and update the Electronic Transactions Policy to include appropriate instruction and guidance around the adoption of digital workflows and authorisation; and
- (b) complete the assessment of existing business systems and processes to ensure that information created, captured, stored, used to deliver services, or inform decision making meets minimum metadata standards and functional requirements for the management, transferral, and disposal of information.

**Civil Aviation Safety Authority response:** *Agreed.*

**Recommendation  
no.7****Paragraph 4.67**

The Office of the Inspector-General of Intelligence and Security should establish a plan for the implementation of the Digital Continuity 2020 policy, with a particular focus on those targets which were due on or before the end of 2018. The plan should also include clear processes for ongoing monitoring and reporting of progress.

**Office of the Inspector-General of Intelligence and Security:** *Agreed.*

## Summary of entity responses

### National Archives of Australia

The National Archives of Australia (the National Archives) is established by the *Archives Act 1983* as the lead agency for information policy in the Australian federal government. The National Archives sets information management requirements to support accountability and transparency, integrity of information, rights and entitlements for citizens, and trust in government.

The National Archives has a strong record for leading progress in digital information management across the Australian Government, commencing with the Digital Transition Policy in 2011 and building on this with issue of the Digital Continuity 2020 policy in 2015. This policy supports the Government's broader digital transformation agenda by embedding robust digital information governance into all digital business processes. Since the introduction of the policy in 2015, the percentage of agencies with an established digital information management capability has increased by almost 30% to over 80%.<sup>a</sup>

The National Archives is currently collaborating with other key information agencies within government to develop the next policy approach. As the lead agency, the Archives will issue this policy approach in early 2021 to further drive improvements in information management within government, improving the efficiency and effectiveness of government, and services to citizens.

The National Archives welcomes the findings of the audit of the implementation of the Digital Continuity 2020 Policy. With regard to the National Archives of Australia, the report primarily addresses issues of program governance and documentation related to the management of the policy rollout. The National Archives notes that during the course of the DC2020 implementation it has pursued opportunities to reduce internal 'red tape' and administrative overheads in order to improve its focus on delivery of services and products to the public as well as to Commonwealth entities. Consequently there has been a reduction of staff applied to the governance of the DC2020 policy rollout.

The National Archives will review the governance, project and risk management arrangements for the delivery of the policy, including communication and stakeholder engagement to meet audit recommendations, within resourcing constraints.

The National Archives will also review the monitoring and evaluation arrangements for the implementation of the Policy. Due to investment in the existing survey tool which provides consistent assessment against the core information management requirements for Australian Government, modifications to further assess progress against the Digital Continuity 2020 policy may however be limited.

Assurance of the accuracy of agency responses to the annual survey has been achieved through agency head sign-off as the accountable authority. The National Archives will consider additional validation and quality assurance of survey responses that can be undertaken within resource constraints. The National Archives will also establish arrangements to measure its own delivery of the policy, and the support provided to assist Australian Government agencies to achieve the outcomes of the Policy.

The results and recommendations of the audit will assist the National Archives in the final delivery phase of the Digital Continuity 2020 Policy, and will also inform the development and planning of future policies. The National Archives has appreciated the opportunity afforded by this audit to build its policy and program delivery capability.

### *ANAO comment on National Archives of Australia response*

- (a) The figure quoted is based on the number of agencies that have self-assessed as having a digital maturity level of 3 or above in the Check-Up Digital and Check-up Plus surveys conducted in 2016 and 2018 respectively. As stated at Paragraph 3.20, the Archives has identified that using this maturity scale to measure success is potentially inaccurate.

### **Attorney-General's Department**

Thank you for providing the department with the opportunity to comment on the ANAO's proposed report on the Implementation of the Digital Continuity 2020 policy.

I am pleased that the report recognises the significant investment the department has made in meeting the targets of the policy. The department welcomes the report's conclusions and findings and continues to be committed to the effective and efficient implementation of the policy, where practical to do so.

### **Civil Aviation Safety Authority**

CASA welcomes the recommendation related to CASA (recommendation six) and agrees with its finding without qualification.

As the audit report notes, CASA has made steady progress in delivering the Digital Continuity 2020 targets and continues to do so.

Since completion of this audit, CASA has made progress in the review and update of its information management policies and procedures including the Electronic Transactions Policy – Recommendation No.6a. CASA expects to finalise this work in the first quarter of 2019–20. CASA has also completed the assessment of current ongoing business systems against the National Archives of Australia's Business System Assessment Framework – Recommendation No.6b.

### **Office of the Inspector-General of Intelligence and Security**

The Office of the IGIS supports the findings contained in the audit report on this agency's implementation status for the Digital Continuity 2020 (DC 2020) policy and accepts Recommendation no.7.

The report acknowledges the Office of the IGIS' progress in implementing aspects of the DC 2020 policy. The report also notes some of the external security requirements that limit the Office's ability to fully satisfy certain principles of DC 2020.

## Key messages from this audit for all Australian Government entities

20. Below is a summary of key messages, including instances of good practice, which have been identified in this audit that may be relevant for the operations of other Australian Government entities.

### **Policy implementation**

- When developing a framework to manage policy implementation, entities should ensure that administration and oversight arrangements reflect the significance of the policy.

### **Governance and risk management**

- Governance arrangements should be developed during the design phase and maintained throughout the implementation phase. The arrangements should reflect the complexity of the program or policy, facilitate a common understanding and commitment to implement, and where responsibility for implementation is spread across multiple agencies include external stakeholders.
- Effective risk management arrangements should include regular testing of the measures that have been developed and implemented to mitigate known risks, and the effectiveness of the controls.

### **Performance and impact measurement**

- Effective monitoring and evaluation arrangements should be supported by relevant and accurate data. The performance measures should be relevant, reliable, and complete, and support accurate assessment of progress and an examination of the extent to which the benefits of the policy are being realised.

### **Regulation**

- Entities responsible for administering or overseeing policy implementation should establish monitoring and reporting arrangements that are fit for purpose. In situations where systemic compliance issues are identified the effectiveness of the policy framework should be reviewed.

## **Audit findings**

# 1. Background

---

## Introduction

1.1 On 20 May 2014, the National Archives of Australia (the Archives) recommended that the Attorney-General approve the development of a new policy for information management in Australian government agencies. It was intended that the policy would assist in the delivery of broader objectives for e-government and the digital economy, and support the implementation of effective digital information management throughout the Australian Government.

### Development of the Digital Continuity 2020 policy

1.2 Development of the Digital Continuity 2020 policy commenced in August 2014.<sup>4</sup> Internal documentation indicated that the policy would be the Archives' 'flagship' policy, and that it should apply to all Australian Government entities. Development of the policy and associated implementation guidance continued throughout 2015, and the policy was formally launched on 27 October 2015 by the Director-General of the Archives and the Secretary of the Department of Finance.

### The Digital Continuity 2020 policy

1.3 The Digital Continuity 2020 policy is a successor policy to the Australian Government's Digital Transition policy, which was approved in July 2011. The objective of the Digital Transition policy was to move Australian Government entities from paper-based records to digital information and records management. The Digital Continuity 2020 policy seeks to: ensure that records and information is created, managed, and maintained digitally; and digital authorisation and approval processes are embedded into all business systems used by Australian Government entities to deliver services and undertake functions. The policy also requires entities to ensure that interoperable information, systems, and processes are developed and implemented that meet standards for short and long-term management.

1.4 The Archives issued the Digital Continuity 2020 policy under the *Archives Act 1983*, which authorises the Archives to issue standards for Commonwealth records, and to preserve and make accessible the archival resources of the Australian Government.<sup>5</sup> The policy applies to all Australian Government entities, including Government Business Enterprises.

1.5 The purposes of the policy are:

- to support the Australian Government's digital transformation initiatives;
- to enable the integration of information governance principles and practices into the work of agencies and their governance arrangements; and
- to promote a consistent approach to information governance across the Australian Government and within individual agencies.

---

4 A policy development workshop, facilitated by an external consultant, was held on 25 August 2014.

5 *Archives Act 1983*, Provision 2A Objects of this Act, subsections 2A(a)iii and 2A(b).



1.6 The policy applies to government information, data and records, as well as systems, services and processes, including those created or delivered by third parties on behalf of Australian Government entities.

### Principles

1.7 To achieve the objectives of the Digital Continuity 2020 policy there are three principles that entities are to embed by 31 December 2020, as outlined in Figure 1.1.

**Figure 1.1: Principles of the Digital Continuity 2020 policy**

Principle 1 — information is valued	• Agencies will <b>manage their information as an asset</b> , ensuring that it is created and managed for as long as required, taking into account business and other needs and risks.
Principle 2 — information is managed digitally	• Agencies will transition to <b>entirely digital work processes</b> , meaning business processes including authorisations and approvals are completed digitally, and that information is created and managed in digital format.
Principle 3 — information, systems and processes are interoperable	• Agencies will have <b>interoperable information, systems and processes</b> 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.

Source: Digital Continuity 2020 policy.

### Recommended actions

1.8 In order to embed the three principles, the policy includes 10 recommended actions with associated target dates for implementation, as outlined in Table 1.1.

**Table 1.1: Recommended actions from the Digital Continuity 2020 policy**

Recommended action	Target date
Principle 1 — Information is valued	
1. Information governance reporting	Annually until 31 December 2020
2. Agencies have established an information governance committee	30 June 2016
3. Agencies have an information governance framework	31 December 2016
4. Agencies manage their information assets for as long as they are required	31 December 2020
5. Agencies meet targets for skilled staff	31 December 2020
Principle 2 — Information is managed digitally	
6. Agencies work digitally, with business interactions, decisions and authorisations recorded digitally	31 December 2020
7. Information in analogue formats is migrated to digital format, where there is value for business	31 December 2020

Recommended action	Target date
Principle 3 — Information, systems and processes are interoperable	
8. Information is managed based on format and metadata standards for information governance and interoperability	31 December 2020
9. All business systems meet functional requirements for information management	31 December 2020
10. Cross-agency and whole-of-government processes incorporate information governance requirements and specifications	31 December 2020

Source: Digital Continuity 2020 policy.

1.9 The implementation guidance<sup>6</sup> accompanying the policy has a total of 29 targets, with due dates ranging from 30 June 2016 through to 31 December 2020. Seventeen of these targets were due by 31 December 2018. A full listing of the targets and associated due dates is provided at Appendix 2.

### Responsible Authority

1.10 As the entity responsible for setting records and information management requirements, including all information created, used, or received as part of government business in digital and non-digital formats, the Archives is responsible for overseeing the implementation of the policy. This includes establishing effective administration and monitoring and evaluation arrangements to assist and encourage Australian Government entities to achieve the targets of the policy by 31 December 2020.

1.11 In November 2015, the Archives sought endorsement of the proposed policy through the Attorney-General, and advised that:

- the policy should have minimal budget or red tape impact on entities due to its five year implementation period (2015–2020);
- its design allows for implementation within normal budget cycles and procurement processes; and
- the policy will establish recommended best practice for all agencies.

1.12 The Attorney-General subsequently dispatched letters to the Prime Minister, the Treasurer and other Ministerial colleagues seeking, and obtaining, their endorsement and support to implement the policy within their respective portfolio agencies and departments.

### Broader legislative and policy framework

1.13 The Digital Continuity policy sits within a broader framework of supporting standards, whole-of-government policies and strategies that Australian Government entities are to

---

6 National Archives of Australia, 'Agency implementation targets and pathways,' *Digital Continuity 2020 — the future of e-government*, available from [http://www.naa.gov.au/Images/DigCon2020-brochure-update-Feb2019\\_tcm16-96316.pdf](http://www.naa.gov.au/Images/DigCon2020-brochure-update-Feb2019_tcm16-96316.pdf) [accessed 2 August 2019].

implement to meet legislative and regulatory requirements associated with information management. An overview of this framework is provided at Table 1.2.<sup>7</sup>

**Table 1.2: Supporting standards and whole-of-government policies that apply to information management**

Standard/ policy <sup>a</sup>	Legislative Authority	Lead agency	Date	Description
Digital Service Standard	<i>Public Governance, Performance and Accountability Rule 2014</i>	Digital Transformation Agency	2016	The Digital Service Standard is a set of best-practice principles for designing and delivering government services. The Digital Service Standard applies to Australian Government Services that are public facing, owned by non-corporate Commonwealth entities, and distribute information and/or provide transactional services. Where the result of a transaction is used to inform decision making it is to be included as part of the relevant record, and maintained in accordance with the <i>Archives Act 1983</i> .
Information Management Standard	<i>Archives Act 1983</i>	National Archives of Australia	2017	The Information Management Standard identifies eight principles that Australian Government entities are to implement. The standard does not prescribe how entities should meet the principles, identifying that the principles should be implemented using a risk and value based approach. The purpose of the standard is to assist entities create and manage information, regardless of format. The standard is also intended to support entities implement the targets of the Digital Continuity 2020 policy.

<sup>7</sup> The list of legislation, policies, strategies and advice available on the Archives' website that is related to information management is not exhaustive and does not include sources relevant to entities responsible for unique regulatory or business functions: <http://www.naa.gov.au/information-management/information-governance/legislation-standards/index.aspx> [accessed 10 May 2019].

Standard/ policy <sup>a</sup>	Legislative Authority	Lead agency	Date	Description
Protective Security policy Framework	<i>Directive on the Security of Government business issued by the Attorney-General</i>	Attorney-General's Department	2018	The Protective Security Policy Framework applies to people, information and assets. All Australian Government entities are required to apply the policy as it relates to their risk environment. Core requirements identified in the policy framework that relate to information security apply to sensitive and classified information, access to information, safeguarding information from cyber threats and robust ICT systems. The policy framework identifies the National Archives of Australia as a key lead protective security entity responsible for Commonwealth records and information standards and advice.

Note a: The Archives has categorised whole-of-government strategies and policies, including the Digital Continuity 2020 policy, as required practice. Required practices are practices that entities must be aware of, and implement to the level required as defined in the relevant strategy or policy.

Source: Analysis of the, 'Legislation, policies, standards and advice,' available the National Archives of Australia website: <http://www.naa.gov.au/information-management/information-governance/legislation-standards/index.aspx> [accessed 10 April 2019].

1.14 Detail on the Australian Government's information management legislative, regulatory, and policy environment is provided at Appendix 3.

## Rationale for undertaking the audit

1.15 Australian Government entities are legally required to manage information in a manner which properly records and explains their performance.<sup>8</sup> Effective information management supports accountability and transparency, and enables informed decision making.<sup>9</sup> The Australian Government's transition to digital service delivery creates both opportunities and risks to effective information management. The Archives has an important responsibility to ensure that an appropriate framework is designed and applied to support this transition process, and the Digital Continuity 2020 policy is central to this in providing a whole-of-government approach to digital information governance. The final targets of the policy are due for implementation by 31 December 2020, and it is therefore timely to examine the extent to which entities have implemented the policy, and how effectively the Archives is administering and overseeing its implementation.

---

8 A record is defined by the *Archives Act 1983* as: a document, or an object, in any form (including any electronic form) that is, or has been kept by reason of: a) any information or matter that it contains or can be obtained from it; or b) its connection with any event, person, circumstance or thing.

9 Section 37 of the *Public Governance, Performance and Accountability Act 2013* (PGPA Act) sets out the requirements for Commonwealth entities to keep records that properly document and report the entity's non-financial performance. Section 38 of the PGPA Act sets out the requirement for Commonwealth entities to measure and assess its performance in achieving its objectives, function and role. The capacity of an entity to meet this requirement is directly reliant on the entity keeping accurate and complete records.

## Audit approach

### Audit objective, criteria and scope

1.16 The objective of this audit was to examine the extent to which selected Australian Government entities have implemented the Digital Continuity 2020 policy, and how effectively the National Archives of Australia is monitoring, assisting, and encouraging entities to meet the specified targets.

1.17 To form a conclusion against the audit objective the ANAO adopted three audit criteria:

- Has the National Archives of Australia established effective arrangements to administer the Digital Continuity 2020 policy?
- Has the National Archives of Australia implemented effective monitoring and evaluation arrangements?
- To what extent have selected Australian Government entities implemented the Digital Continuity 2020 policy?

1.18 The audit examined the administration, oversight, monitoring and reporting arrangements for the Digital Continuity 2020 policy, and the extent to which three selected Australian Government entities have implemented the policy.

#### *Entities selected*

1.19 The Attorney-General's Department, the Civil Aviation Safety Authority and the Office of the Inspector-General of Intelligence and Security were selected by the ANAO to assess the extent to which the Digital Continuity 2020 policy has been implemented. The criteria used to select the entities is detailed at Appendix 4.

### Audit methodology

1.20 Audit procedures included:

- examining documentation held by the Archives including briefing material, reports and advice, as well as administrative, quality assurance, monitoring and evaluation documentation;
- examining documentation held by the selected entities, particularly documentation detailing the information governance arrangements in place; and
- interviewing personnel from the Archives and the selected entities.

1.21 The audit was conducted in accordance with the ANAO Auditing Standards at a cost to the ANAO of approximately \$367,500. The team members for this audit were Joyce Knight, Nathan Callaway, Jessica Kanikula and Paul Bryant.

## 2. Administration of the Digital Continuity 2020 policy

---

### Areas examined

This chapter examines the National Archives of Australia's (the Archives') administration of the Digital Continuity 2020 policy and includes an assessment of the effectiveness of the support and assistance provided to entities to encourage them to meet the targets of the Digital Continuity 2020 policy.

### Conclusion

The Archives' arrangements to administer the Digital Continuity 2020 policy are limited in effectiveness. Appropriate governance arrangements to provide strategic direction and oversight of the policy were not maintained. The products, advice, and guidance material issued by the Archives to support entities implement the policy are largely fit for purpose, with some exceptions in relation to the clarity of terminology and timeliness. The Archives does not have a stakeholder engagement and communication strategy, and does not effectively target entities requiring additional assistance to implement the targets of the policy. Risks to the implementation of the Digital Continuity 2020 policy are not being effectively identified, managed, or reported.

### Recommendations

This chapter includes three recommendations aimed at improving the effectiveness of the arrangements in place to administer the Digital Continuity 2020 policy.

### Have effective internal arrangements been established for the administration of the Digital Continuity 2020 policy by the National Archives of Australia?

Internal arrangements for the administration of the Digital Continuity 2020 policy by the Archives are not effective. The Archives has not developed an effective implementation strategy and has not maintained appropriate governance, oversight, and reporting arrangements.

2.1 In August 2015, the Archives identified a range of initiatives, including the development and release of tools, advice, training, and web content, that would be required to support entities across the Australian Government implement the Digital Continuity 2020 policy (detail on the products, advice and guidance material developed by the Archives is provided at paragraphs 2.11 to 2.24). Responsibility for these initiatives was added into the 2015–16 annual work plans for the responsible areas to be managed as business-as-usual activities.<sup>10</sup>

---

10 Responsibility for delivering projects associated with the Digital Continuity 2020 policy were spread across multiple sections within the Archives. Since the policy was launched in 2015, responsibility for overseeing the implementation of the policy has transferred from the Government Information Assurance and Policy (GIAP) Branch. In 2016, the Government Information Assurance and Policy Branch was renamed the Information and Systems Branch and in 2017 responsibility was transferred to the Collections Management Branch.

2.2 Between July 2015 and September 2016, information on the progress of these initiatives was included in branch reports. These reports were discussed at a monthly senior managers meeting involving the Director-General, Assistant Directors-General (Branch heads), and State and Territory Directors. The Executive Board, comprising the Director-General and Assistant Directors-General, were provided with formal updates on the progress of each branch against relevant corporate plan targets, however the progress of initiatives associated with the Digital Continuity 2020 policy were not consistently identified in the reporting provided.

2.3 In July 2016, the Archives recognised that the projects established to support implementation of the policy were not being managed as a coordinated program of work. In November 2016, a Digital Continuity 2020 Project Implementation Register (PIR) was established which identified 20 individual projects (and associated sub-projects) and linked each to the relevant 'recommended action'<sup>11</sup> and 'target'<sup>12</sup> of the Digital Continuity 2020 policy. The PIR also recorded a complexity rating<sup>13</sup> and the current status of each project.<sup>14</sup> A draft document titled 'DC2020 Project Management Framework' outlined that each project should have a project proposal or brief developed, however project documentation was only prepared for eight of the 20 projects, and the PIR has not been maintained since July 2017.

2.4 In March 2018, the Archives commenced an internal review to evaluate progress against the projects listed in the PIR and to identify any gaps and opportunities for further development. A final report from this review was not provided to management.

2.5 In August 2018, the projects established to support the implementation of the policy were incorporated into a high-level register provided to the Archives' Project Management Committee, which is responsible for overseeing the administration and delivery of major projects across the Archives. However, the projects associated with the policy were not required to provide regular reports to this committee.

2.6 Since the launch of the Digital Continuity 2020 policy, the Archives has made several attempts to establish effective internal arrangements to coordinate the administration of the projects established to support and encourage entities implement the policy. However, appropriate program governance, oversight, and reporting arrangements were not maintained.

2.7 In January 2019, an internal audit commissioned by the Archives found that a project management approach had not been utilised to administer the implementation of the Digital Continuity 2020 policy. The internal audit subsequently recommended that the Archives should develop and implement a program of work to achieve the objectives of the policy, and any successor whole-of-government policies in the future, and Archives has agreed to implement the recommendation.

---

11 Actions are those defined in the Digital Continuity 2020 policy as recommended actions.

12 National Archives of Australia, 'Agency implementation targets and pathways,' Digital Continuity 2020 — the future of e-government, available from [http://www.naa.gov.au/Images/DigCon2020-brochure-update-Feb2019\\_tcm16-96316.pdf](http://www.naa.gov.au/Images/DigCon2020-brochure-update-Feb2019_tcm16-96316.pdf) [accessed 2 August 2019].

13 There are three complexity ratings level 1 projects – light, level 2 – standard and level 3 – complex.

14 The status rating allocated uses a Red, Amber or Green colour code. Green denotes that the project is on track, Amber denotes that the project needs attention and Red denotes that the project is overdue.



## Recommendation no.1

2.8 The National Archives of Australia should establish effective internal arrangements to administer and oversee the implementation of the Digital Continuity 2020 policy, and any successor policies. The arrangements should include appropriate governance structures and a strategy to guide the administration of the Digital Continuity 2020 policy, and any successor policies, as a coordinated program of work.

**National Archives of Australia response:** *Agreed.*

2.9 *The National Archives will review current governance and administrative arrangements for the Digital Continuity 2020 policy and revise them to achieve maximum effectiveness of resources and outcomes in line with this recommendation and the broader findings of the audit.*

2.10 *Effective governance and administrative arrangements will also be established for the development and implementation of any successor policies.*

## Did the National Archives of Australia develop products, advice, and guidance material that are fit for purpose?

The products, advice, and guidance material developed and released by the Archives to support the implementation of the Digital Continuity 2020 policy are largely fit for purpose, noting some deficiencies in the consistency of terminology within the guidance, and timeliness in relation to the delivery of supporting products.

### Products, advice, and guidance material

2.11 The Digital Continuity 2020 policy states that the Archives will ‘develop advice, products and tools to support information governance, digital information management and interoperable information, systems and processes.’

2.12 The Archives’ Project Information Register (PIR) established a listing of projects, and associated products, that would be developed in this regard. While the PIR was not maintained after July 2017 (see paragraph 2.3), those projects from the PIR that have been completed and delivered<sup>15</sup> have generated the following products to support the implementation of the policy:

- implementation guidance, and associated implementation material;
- an information management and data capabilities matrix<sup>16</sup>;

---

15 From the total listing of 20 projects in the PIR, 12 have been marked as ‘closed’. The remaining projects are identified as either ‘in progress’, ‘not started’, or ‘open’. The 20 projects identified in the PIR include individual entries for the annual surveys from 2016 through to 2021. The annual surveys are examined in more detail at paragraphs 3.12 to 3.17.

16 The information management and data capabilities matrix details the skills, knowledge, and information management experience required by all staff, information management professionals and senior executives.



- a minimum metadata set<sup>17</sup>;
- a digital authorisation framework;
- a business systems assessment framework; and<sup>18</sup>
- an interoperability toolkit.<sup>19</sup>

### *Implementation guidance and associated implementation material*

2.13 The development of implementation guidance and associated material commenced in January 2015, was released alongside the policy in October 2015, and is comprised of the following products.

- Implementation guidance — In October 2015, the Archives released the *Digital Continuity 2020 – Agency Implementation and Pathways*. This document breaks down the 10 recommended actions under the policy into smaller targets, with staggered implementation dates across the five year implementation period of the policy.
- Associated implementation material — the Archives has published advice to guide entities in establishing an information governance committee, and an information governance framework. The guidance material includes sample terms of reference and identifies what information should be included in key supporting documentation such as an information management strategy and associated policy.

### *Information management and data capabilities matrix*

2.14 Initially, the Archives intended to develop a whole of government information management strategic workforce plan which would include professionalism and capability targets for entities. In June 2016, an agency professionalism working group was established which included representatives from across the Australian Government. As a result of engagement with the Australian Public Service Commission (APSC), Digital Transformation Agency (DTA) and external agencies through the working group, this approach was revised in June 2016.

2.15 The revised approach introduced two new targets to support entities meet the recommended action for skilled staff. The first target was added in November 2016, requiring all entities to establish a 'Chief Information Governance Officer' role by 31 December 2017. The second new target was introduced in September 2017 for all entities 'to establish and implement a program

---

17 The minimum metadata set has been established using the Australian Government Recordkeeping Metadata Standard 2.2.

18 The business system assessment framework is based on Part 3 of *ISO 16175 Principles and Functional Requirements for Records in Electronic Office Environments*. It does not apply to Electronic Document and Records Management Systems, as they are covered by Part 2 of *ISO 16175 Principles and Functional Requirements for Records in Electronic Office Environments*.

19 The interoperability toolkit was announced in a GAIN e-bulletin released in early 2019, available from [https://email.synergymail.com.au/t/ViewEmail/r/3E9C5B8F95D5F5252540EF23F30FEDED/7850160C786CFA646D5E5F9A8728A5A6#toc\\_item\\_1](https://email.synergymail.com.au/t/ViewEmail/r/3E9C5B8F95D5F5252540EF23F30FEDED/7850160C786CFA646D5E5F9A8728A5A6#toc_item_1) [accessed 27 September 2019]. The interoperability toolkit was launched to assist entities achieve the interoperability targets under Principle 3 of the Digital Continuity 2020 policy. The due date for these targets is 31 December 2020. Targets due after 31 December 2018 were considered to be outside the scope of the audit and as such the product has not been assessed.

of continuing professional development of information management staff to achieve professional recognition' by 31 December 2018.

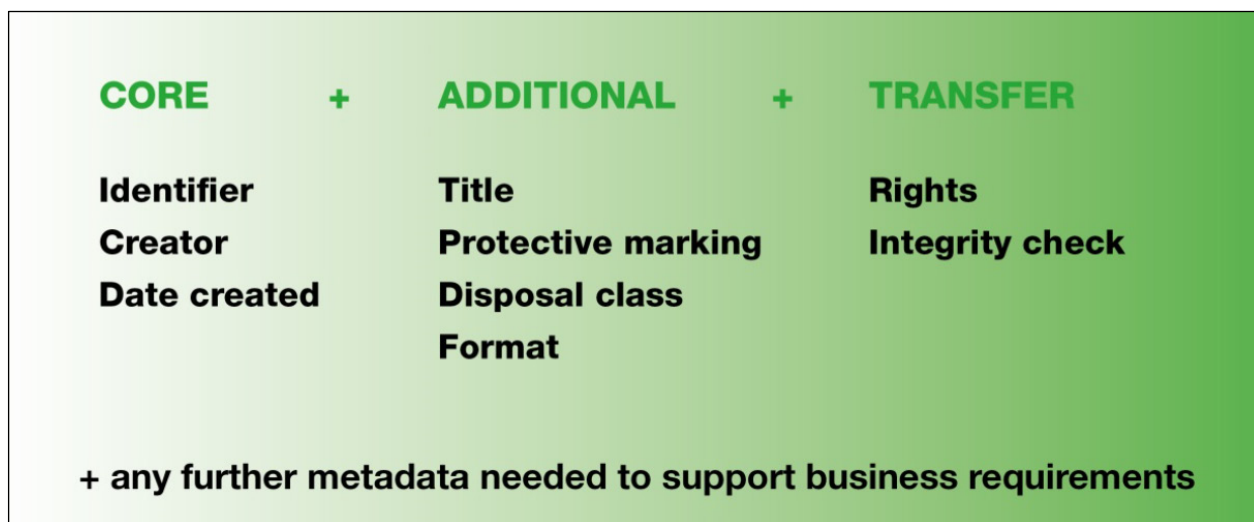
2.16 To support entities in undertaking work associated with the continuing professional development target, the Archives redesigned an existing tool, the digital information capability matrix<sup>20</sup>, to identify the skills and knowledge that are needed to create and manage information and data effectively in order to meet business and accountability requirements.<sup>21</sup> The resulting product is similar to the Australian Public Service (APS) work level standards, identifying the information management capabilities that 'all staff' and 'information management staff' should have, and mapping the capabilities to one of four proficiency levels. The revised information management and data capabilities matrix was released in May 2018, seven months prior to the due date for this target.

#### *Minimum metadata set*

2.17 The minimum metadata set identifies metadata properties essential for the management of business information created and used by Australian Government entities to inform decision making and deliver government services. The minimum metadata set was developed by the Archives based on the Australian Government Recordkeeping Metadata standard<sup>22</sup>, and provides guidance on the transfer of information to the Archives, or other entities, to support interoperability, accessibility and re-use (including auditability).

2.18 The minimum metadata set identifies nine properties required for the effective management of business information, and is made up of three components (see Figure 2.1).

**Figure 2.1: Minimum metadata set**



Source: National Archives of Australia, available from <http://www.naa.gov.au/information-management/digital-transition-and-digital-continuity/information-is-interoperable/metadata/index.aspx> [accessed 22 May 2019].

20 Development of the digital information capability matrix commenced in April 2015.

21 During the development process Archives engaged with the APSC to align the information management and data capabilities matrix with the APSC Job Family Review and to support the development of the learning design standard for data being developed by the DTO (now the DTA).

22 The Australian Government Recordkeeping Metadata Standard (AGRkMS) describes information about records and the context in which they are captured and used in Australian Government agencies.

2.19 Development of the set commenced in March 2015, with the product released in February 2016.

2.20 Under the policy, entities are responsible for ensuring the requirements of the minimum metadata set are met by all new and existing business systems. The Archives engaged with the Digital Transformation Agency (DTA) in 2017 to explore incorporating the minimum metadata standards into whole-of-government Information and Communications Technology (ICT) procurement templates that were being developed.<sup>23</sup> In 2018, it was agreed that a generic reference to compliance with all relevant laws applying to the procurement process was sufficient to address the policy's requirements, and that individual entities are responsible for determining how the minimum metadata set should be met when procuring new business systems.

### *Digital authorisations framework*

2.21 The digital authorisations framework is a risk-based assessment tool designed to assist entities determine its digital approval requirements and select an appropriate digital approval method. Acceptable methods include email, action tracking, system workflows, and digital signatures. The Archives is also piloting an online digital authorisations tool.

2.22 Development of the digital authorisations framework commenced in June 2015, with entities invited to participate in a digital workflows working group in July 2016. The working group continued until mid-2017 and the digital authorisations framework was released in October 2017, two months prior to the due date of 31 December 2017 for the associated Digital Continuity 2020 policy target.<sup>24</sup>

### *Business systems assessment framework*

2.23 The Archives developed a business systems assessment framework that entities can use to assess information management functionality.<sup>25</sup> The framework provides entities with a structured approach to the assessment of information management functionality in business systems, based on the value of information and the associated level of risk.

2.24 The first policy target that refers to the use of the business system assessment framework requires entities to ensure that information management functional requirements are incorporated into any new business systems purchased after 31 December 2016.<sup>26</sup> Development of the business systems assessment framework commenced in April 2015, and the Archives released the framework in February 2016. In 2018, the Archives commenced work to refine the Business System Assessment Framework, and is currently piloting an online tool to simplify and streamline the business systems assessment process.

---

23 The ICT procurement templates were managed by the Department of Finance before responsibility to develop and manage the templates was transferred to the Digital Transformation Agency.

24 The target states that entities are to transform most paper-based business processes to digital, and routinely make and record decisions using digital authorisations and workflows by 31 December 2017.

25 The Business Assessment Framework is based on Part 3 of the *ISO 16175 Principles and Functional Requirements for Records in Electronic Office Environments*.

26 The first target in the implementation guidance that refers to the business systems assessment framework states that all business systems procured after 31 December 2016 will be evaluated against the Archives' business systems assessment framework to meet functional requirements for information management.

## Entity views on Digital Continuity 2020 guidance

2.25 The selected entities advised that the products, advice and guidance material issued by the Archives to support the policy are comprehensive and valued, however expressed confusion in relation to the consistency of terminology within the guidance, and indicated that some material has not been consistently delivered in a timely fashion, with sufficient lead time for entity implementation.

### *Consistency of terminology*

2.26 The Digital Continuity 2020 targets are interchangeably referred to as ‘recommended actions’, ‘targets’, and ‘interim targets’ within the Digital Continuity 2020 policy document, the Agency Implementation and Pathways document (implementation guidance), and the advice and guidance material published on the Archives website. There is also a mix of recommended actions listed in the policy and the targets detailed in the guidance provided within previous annual survey instruments, particularly the 2017 Digital Continuity Statements and the 2018 Check-Up Plus annual survey. As a result, entities have expressed confusion regarding the status of the actions of the policy, the targets in the implementation guidance, and whether the targets are mandatory, recommended or optional. Ensuring that clear and consistent language is used to communicate the mandatory requirements of legislation, regulation or policy was one of the key themes identified in the Belcher Review.<sup>27</sup>

### *Introduction of new targets*

2.27 When the policy was launched in October 2015, the accompanying implementation guidance had a total of 25 ‘targets’ with links to the products and guidance material that had been developed and released by Archives to support entities achieve the targets and complete the recommended actions of the policy. In October 2017, and again in February 2019, the Archives revised the implementation guidance<sup>28</sup> adding a total of four new targets. The new targets state:

- entities are to establish a Chief Information Governance Officer (31 December 2017);
- entities are to establish and implement a program of continuing professional development of information management staff for professional recognition (31 December 2018);
- entities identify remaining analogue approval processes and evaluate against the Archives’ digital authorisations framework to implement fully digital authorisations and workflows (30 June 2019); and

---

27 The Belcher Review made seven recommendations associated with unclear and inaccessible regulations and guidance. Recommendation 1.5 requires regulators to ensure that guidance documents assist entities to meet mandatory requirements contained in legislation, subordinate legislation, or policy issued by ministers, and do not set out additional requirements as if they were mandatory. Recommendation 1.7 relates to ensuring that consistent language is used in regulatory and guidance documents, whereby mandatory requirements are suggested through the use of language such as ‘must, shall, require/required to and should’. The Archives has identified the Digital Continuity 2020 policy as required practice, indicating that implementation of the policy is mandatory, and the use of the term targets and pathways in the implementation guidance supports this interpretation. However, the actions of the policy are identified as ‘recommended’.

28 The guidance material referred to is revised versions of the ‘Agency implementation targets and pathways,’ *Digital Continuity 2020 — the future of e-government* brochure, available from [http://www.naa.gov.au/Images/DigCon2020-brochure-update-Feb2019\\_tcm16-96316.pdf](http://www.naa.gov.au/Images/DigCon2020-brochure-update-Feb2019_tcm16-96316.pdf) [accessed 2 August 2019].

- chief information governance officers or senior officers responsible for information governance individually join a professional association to support their continuing development (31 December 2019).

2.28 Three of the four targets added to the implementation guidance are mapped to principle one of the Digital Continuity 2020 policy, and are intended to support entities in meeting targets for skilled staff. When introducing the new professionalism related targets the Archives consulted with entities across the Australian government, including the Australian Public Service Commission (APSC) and the DTA prior to introducing the new targets requiring entities to establish a CIGO and a program of continuing professional development for information staff in 2016 through to 2017.

2.29 In January 2019, records managers across the Australian government sector were advised that the target to support the professionalisation of CIGO's and senior officers responsible for information governance was being introduced. The new target requires 'CIGO's or senior officers responsible for information governance individually join a professional association to support their continuing development.' This target is highly prescriptive and does not align with a principles based policy. During the course of the audit the selected entities advised that they were unsure why the target was introduced.

2.30 As part of the development of a wider stakeholder engagement and communication strategy, Recommendation no.2 (see paragraph 2.38) addresses the need for the Archives to ensure that stakeholders are appropriately consulted when introducing new or revised targets, and that mechanisms are established to ensure targets are clearly identified and consistently communicated as either mandatory, suggested, or optional.

### Does the National Archives of Australia effectively engage with stakeholders to administer the Digital Continuity 2020 policy?

The Archives' engagement activities with stakeholders to administer the Digital Continuity 2020 policy are limited in effectiveness. There is no communications or stakeholder engagement strategy in place for the implementation of the policy. In practice, communication occurs with stakeholders through a variety of channels including online, face-to-face, telephone, and annual surveys, however there has been no formal process to identify entities who are experiencing difficulties in implementing the policy and provide targeted assistance.

### Stakeholder engagement and communication — strategy and planning

2.31 In July 2015, the Archives commenced the development of a communications plan for the Digital Continuity 2020 policy. In November 2016 the draft plan articulated: key communications objectives; target audiences; roles and responsibilities; risk and budget information; and key performance indicators, however the communications plan was not formally approved, and there is no evidence that stakeholder engagement matters were addressed in any other planning documents.

2.32 There is evidence that communication plans were developed for a small number of the individual projects initiated to support entities implement the policy, however the Archives does

not have an approved communications or stakeholder engagement strategy to administer the implementation of the Digital Continuity 2020 policy as a coordinated program of work.<sup>29</sup>

## **Stakeholder engagement and communication — in practice**

2.33 In practice, the Archives engages with stakeholders using the following channels.

- Social media updates — where the Archives promotes events, and seeks community feedback on initiatives, including initiatives related to the Digital Continuity 2020 policy such as information awareness month.
- The Archives' website — where the Archives releases supporting products, guidance and advice to assist and encourage entities to implement the targets of the Digital Continuity 2020 policy.
- The Government Agencies Information Network (GAIN) Australia<sup>30</sup> — GAIN holds forums, and issues regular e-bulletins. Forums are face-to-face meetings used to provide an avenue for information managers to share expertise and experience. The GAIN forums and e-bulletins are also used to provide updates on information management initiatives, standards, and policies including the Digital Continuity 2020 policy.<sup>31</sup>
- The Archives' Agency Service Centre (ASC) — logs queries received in relation to all the functions of the Archives, including queries related to the implementation of Digital Continuity 2020 targets (and associated responses). Between 2017 and 2019, the ASC has logged 1208 queries, with 287 (24 per cent) related to Digital Continuity 2020 or a supporting product<sup>32</sup>, guidance material<sup>33</sup> or target.<sup>34</sup>

### *Targeted support for stakeholders*

2.34 The Digital Continuity 2020 policy states:

the Archives will use annual agency reports [surveys] and other information as part of performance monitoring. This includes identifying agencies that need assistance to complete the recommended actions. The Archives will work with these agencies to improve their digital information management.

2.35 The annual agency surveys are examined in detail in paragraphs 3.12 to 3.17. The Archives uses the results of the annual surveys to inform its annual planning cycle and support the

---

29 In addition to the entities responsible for implementing the policy, key stakeholders include other agencies that oversee related whole of government policies and standards, such as the digital service standard, digital transformation strategy and digital marketplace: <https://www.dta.gov.au/> [accessed 17 July 2019]. Key policies and initiatives that have information management implications are outlined in Appendix 3, Table A.3.

30 The Archives initiated and facilitates the GAIN initiative, which is a national network supporting agency information and records managers in the Australian Government.

31 GAIN e-bulletins are issued to subscribers with current and previous bulletins accessible on the Archives website: <http://www.naa.gov.au/information-management/support/gain/gain-australia-e-bulletin/index.aspx> [accessed 4 July 2019].

32 The supporting products include the Check-Up survey, metadata and standards, and records retention, transfer or disposal.

33 The guidance material includes information governance and management, machinery of government changes, and records authorities.

34 Targets include: professionalisation targets, support and professional development.

identification of activities in business plans throughout the year. For 2016, the Archives used the results from the Check-Up Digital survey to identify entities that required further assistance. However, there is no evidence that action was subsequently taken to provide targeted assistance to the entities identified through this process.

2.36 The Archives has acknowledged that, to date, there has been no formal process to support entities that are experiencing difficulties in implementing digital information management practices and provide targeted assistance to implement the targets of the Digital Continuity 2020 policy. To address this gap, the Archives approved a program of work entitled 'Join-the-Dots' in July 2019.

2.37 The 'Join-the-Dots' initiative intends to analyse data from the annual surveys to identify and prioritise entities that require additional support to drive improvement. The Archives has completed an analysis of survey data from 2014 to 2018<sup>35</sup>, identified the entities that require assistance, and is in the process of determining the most appropriate methods to deliver assistance and establish priorities. To assess the impact of the project, the Archives intends to analyse the annual survey results for the remaining duration of the Digital Continuity 2020 policy. The next survey has been released and is to be completed by entities by 30 September 2019, with analysis and reporting due to occur in the subsequent months.

## Recommendation no.2

2.38 The National Archives of Australia should develop and implement a stakeholder engagement and communication strategy that:

- (a) includes measures to ensure that entities are appropriately consulted when introducing new or revised targets; and
- (b) establishes mechanisms to ensure targets are clearly identified and consistently communicated as either mandatory, suggested, or optional.

**National Archives of Australia response:** *Agreed.*

2.39 *The draft stakeholder engagement and communication strategies will be reviewed to meet this recommendation, and formally approved. Additionally, existing targets will be reviewed to clearly identify them as mandatory, suggested or optional and the outcome communicated to all entities. The Archives notes that the majority of targets are not compliance measures and are provided as a pathway to assist agencies to achieve policy outcomes.*

---

35 The Archives has conducted annual surveys of entity information management and maturity since 2007. As outlined in paragraph 3.13, surveys with a relationship to the principles of the Digital Continuity 2020 policy commenced in 2016.



## Are risks to the implementation of the Digital Continuity 2020 policy being effectively identified, managed and reported?

Risks to the implementation of the Digital Continuity 2020 policy are not being effectively identified, managed, and reported. A risk management plan for the implementation of the policy as a coordinated program of work was not established. Risks for a small number of individual projects associated with the implementation of the policy have been identified, however there is no evidence that these risks are being appropriately managed and reported.

2.40 In its 2015–16 corporate plan, the Archives identified the Digital Continuity 2020 policy as a key strategy to address risks relating to the Archives' ability to provide leadership and continued support for digital information and records management capability across the Australian Government.

2.41 In October 2015, work to develop a risk register for the implementation of the policy commenced. This work was not completed.

2.42 In November 2016, the Archives established the project implementation register (PIR) to track the progress of the projects established to develop the products, advice, and guidance material to support entities meet the targets of the policy. Of the 20 individual projects listed in the PIR, project briefs and associated project management documentation have been located for eight projects, and these include risk assessment information. The risk assessments within the documentation identify the risk controls and a risk rating, however do not include a risk management action plan that identifies how the effectiveness of the risk controls will be assessed or tested. In accordance with the Archives' April 2016 risk management framework and policy, the strategic and operational risks associated with the achievement and promotion of the Digital Continuity 2020 policy targets should have been formally assessed and regularly reviewed. However, there is no evidence that this occurred.

2.43 In 2017–18, the Archives' strategic risk register included the risk that 'Archives fails to impose records creation requirements and the minimum standards for digital Government records', and identified the following risk mitigation strategies.

- Continuing to develop tools, strategies, guidance and standards to assist entities transition to digital information management.
- Continued achievement and promotion of Digital Continuity 2020 policy targets up to 2020.
- Implementation of a new policy to guide digital information management — to succeed the Digital Continuity 2020 policy.
- A new survey reporting tool to assess entities progress towards digital information management.



2.44 As at July 2019, there is no evidence of any activity to monitor and report on the effectiveness of these strategies in the subsequent period.

### Recommendation no.3

2.45 The National Archives of Australia should develop and implement a risk management plan for the successful implementation of the Digital Continuity 2020 policy, and any successor policies.

**National Archives of Australia response:** *Agreed.*

2.46 *Existing risk management arrangements will be reviewed and a comprehensive and coordinated risk management plan will be developed for the implementation of the Digital Continuity 2020 policy, and any successor policies.*

### 3. Monitoring and evaluation arrangements for the Digital Continuity 2020 policy

---

#### Areas examined

This chapter examines whether the National Archives of Australia (the Archives) has implemented effective monitoring and evaluation arrangements for the implementation of the Digital Continuity 2020 policy.

#### Conclusion

The effectiveness of the arrangements for monitoring and evaluating the implementation of the Digital Continuity 2020 policy are limited. The priorities, objectives, and targets utilised by the Archives to measure its performance in overseeing the implementation of the policy have not been designed to appropriately align with the policy's objectives. Monitoring and reporting processes have been integrated into an annual whole-of-government survey, however the performance information is not clearly aligned with the policy itself, is not subject to sufficient quality assurance processes, and does not include clear and consistent benchmarks to measure success.

#### Recommendations

This chapter includes two recommendations to improve the Archives' approach to monitoring and evaluation.

#### Has the National Archives of Australia designed appropriate monitoring and evaluation arrangements?

Monitoring and evaluation arrangements were not designed appropriately. The Archives has not maintained consistent priorities and objectives in relation to the implementation of the policy since 2015–16, and the measures selected by the Archives to assess its performance in the roll-out of the policy require improvement in relation to relevance, reliability, and adequacy. The Archives has not obtained consistent and comparable data to enable an accurate analysis of entity progress to implement the policy over time, and has not taken action to define clear and consistent measures of success.

3.1 When undertaking planning processes for the implementation of a policy, better practice guidance<sup>36</sup> states that monitoring and evaluation arrangements should:

clearly define the objectives and outcomes of the policy that is being implemented, [and] determine what successful outcomes will look like and what evidence will be needed to demonstrate success. As this has planning implications, thinking needs to occur from the outset and ensure activities are fit-for-purpose.

---

36 Best practice is detailed in the Department of the Prime Minister and Cabinet's policy implementation guidance, available from <https://www.pmc.gov.au/sites/default/files/files/pmc/implementation-toolkit-5-monitoring.pdf> [accessed 02 May 2019]. The best practice guidance was available at the time that the Archives was developing the Digital Continuity 2020 policy.

## Objectives, outcomes, and performance measures

3.2 The objectives of the Archives in relation to the Digital Continuity 2020 policy (policy) have been identified using various language in successive corporate plans since 2015–16.

- In 2015–16, the implementation of the policy was not specifically identified, rather it was captured under strategic priority three (of three), to ‘provide leadership and continued support for digital information and records management capability across the Australian Government.’ A single quantitative measure — a 95 per cent participation rate by entities in an annual survey on digital information maturity — was used to measure performance.
- In 2016–17, implementation of the policy was listed as a ‘delivery strategy’ under purpose three (of four) to ‘provide leadership on information management to the Australian Government’. Two qualitative measures relating to the development and delivery of guidance material and advice to support entities achieve the targets were included to measure performance. In addition, a quantitative measure aiming to have 90 per cent of entities managing information ‘digitally by default by 2020’ was also included.
- In 2017–18, implementation of the policy was listed underneath purpose one (of four) to ‘demonstrate leadership and best practice, to promote the creation, management and preservation of authentic, reliable and usable Commonwealth records.’ Four targets were identified. Australian Government entities transition to digital information management in accordance with the Digital Continuity 2020 Policy. Archives reports to the Minister (annually) and Prime Minister (2018) outlining entities’ progress towards digital transition, the support provided, and additional support needed, by the Archives to further drive improvement. A new survey reporting tool is issued to assess entities’ progress towards digital information management. Entities participate in annual survey reporting requirements. However, there were no specific qualitative or quantitative measures included within the plan to measure performance against these targets.

3.3 The latest corporate plan (2018–19 to 2021–22) identifies the policy as one of three central strategies the Archives is to implement to deliver its purpose and achieve its vision. The relevant strategy is ‘establish frameworks for best-practice management of Australian Government information and data by Australian Government agencies toward achievement of the Digital Continuity 2020 policy targets.’ The three activities that the Archives will undertake to achieve this strategy are:

- The development of standards, policies, guidance, information and services to assist entities adopt good information and records management practices and implement the Digital Continuity 2020 policy and targets.
- Survey entities and report on transition to digital information management.
- Report to the Minister and Prime Minister outlining entities progress towards digital transition, the support provided, and additional support needed, by the Archives to drive further improvement.

3.4 The measures to evaluate performance against this strategy are:

- the percentage of agencies completing the annual survey (with a target of 96 per cent) — measure one; and






- qualitative evaluation of progress towards Digital Continuity 2020 policy outcomes (to be measured using survey responses and case studies) — measure two.




3.5 As such, the Archives has not maintained consistent priorities, objectives and targets in relation to its work on the implementation of the policy.

### Appropriateness of performance measures

3.6 To determine if the current performance measures for the Digital Continuity 2020 policy implementation are appropriate, they have been assessed against better practice principles in relation to relevance, reliability and adequacy<sup>37</sup>, with the results summarised at Table 3.1.

**Table 3.1: Appropriateness of the Archives' performance measures for the Digital Continuity 2020 policy implementation**

Performance measure	Relevant	Reliable	Adequate
Measure one — Entity participation rate in annual survey			
Measure two — Qualitative evaluation of progress towards Digital Continuity 2020 outcomes			

Legend:  the measure fully aligns with the relevant principle  
 the measure partly aligns with the relevant principle  
 the measure does not align with the relevant principle

Source: ANAO analysis of the Archives' Digital Continuity 2020 performance information included in the 2018–19 corporate plan.

### Relevance

3.7 Measure one is not relevant. The fact, or not, of a high participation rate in the annual survey does not enable the Archives or external users to assess: the extent to which entities are implementing the policy; the effectiveness of the standards, policies, guidance, information and services to support entities implement the policy; or to what extent the expected benefits of implementing the policy are being realised.

3.8 Measure two is relevant. It uses survey responses and case studies to evaluate entity progress towards policy outcomes, and has a stronger alignment to the strategic objectives associated with successful implementation of the policy.

### Reliability

3.9 Measure one is reliable. It is a quantitative measure with a target that can be verified. The measure is simple to assess — percentage of entities that complete the survey, measured using

37 Department of Finance, *Resource Management Guide No. 131 Developing good performance information* [Internet], Canberra, 2015, available from <https://www.finance.gov.au/sites/default/files/RMG%20131%20Developing%20good%20performance%20information.pdf> [accessed 2 August 2019]. The basis for the ANAO's assessment was drawn from the characteristics of 'good' performance information as defined by Finance. Guidance from Finance notes that 'appropriate' performance information is relevant, reliable, and complete. See Appendix 5 for more information. The ANAO assesses if performance information is relevant (benefit, focus and understandable), reliable (measurable and free from bias) and complete (balanced and collective). If an assessment is made against a subset of an entity's performance information, 'complete' is replaced by 'adequate' to reflect that the assessment of balance and collectiveness is made at a level below the purpose.

data obtained from the Archives' annual surveys. The corporate plan identifies the types of entities that are invited to complete the survey, with internal documentation clearly defining the parameters of the measure, identifying entities that are out of scope and specifying how survey responses are to be counted.

3.10 Measure two is partly reliable. Combining quantitative data (survey data) with qualitative data (case studies) can enrich the performance story<sup>38</sup>, however, the Archives has not defined a methodology that will be used to collect information and determine how case studies will be selected for inclusion in the annual report to ensure that the case studies selected are free from bias.

### *Adequacy*

3.11 The Archives' performance measures have the potential to provide an adequate basis to assess its performance against the strategic objective to 'establish frameworks for best-practice management of Australian Government agencies toward achievement of the Digital Continuity policy targets.' However, the current measures do not enable users to assess how effectively the standards, policies, guidance, information and services developed by the Archives support entities to implement digital information management practices, and to what extent entities have implemented the targets of the Digital Continuity 2020 policy. Additionally, a methodology to select case studies for inclusion in the annual report has not been defined.

### **Quality of performance information**

3.12 The Digital Continuity 2020 policy states that 'the Archives will use annual agency reports [surveys] and other information as part of performance monitoring'.

3.13 Since the launch of the policy in October 2015, the Archives has utilised three different annual agency surveys, the:

- check-up Digital survey — 2016<sup>39</sup>;
- digital continuity statement — 2017<sup>40</sup>; and
- check-up Plus survey — 2018.<sup>41</sup>

3.14 The nature of these surveys and their relationship with the actions and targets of the policy are outlined at Table 3.2.

---

38 Department of Finance, *Resource Management Guide No. 131 Developing good performance information* [Internet], Canberra, 2015, available from <https://www.finance.gov.au/sites/default/files/RMG%20131%20Developing%20good%20performance%20information.pdf> [accessed 2 August 2019], p. 23.

39 The Check-Up Digital survey commenced in 2014, prior to the issue of the Digital Continuity 2020 policy, and was a measure of digital information management transition.

40 The 2017 Digital Continuity Statement was used as an opportunity to collect 'hard data' on agency progress against the Digital Continuity 2020 policy targets.

41 The Check-Up Plus survey was designed to address the principles of the Information Management Standard and includes the Digital Continuity 2020 policy.

**Table 3.2: The relationship between the annual surveys and the Digital Continuity 2020 policy**

Survey	Relationship with the Digital Continuity 2020 policy
2016	<p>The 2016 <i>Check-up Digital</i> survey spanned the years 2014 to 2016 and had a total of 16 questions designed to gauge the 'digital information management maturity' of each entity. The Digital Continuity 2020 policy targets which were due in 2016 were listed against 14 of these questions. Entity performance against key information management principles was measured on a maturity scale from Level 1 'Initial' through to Level 5 'Optimising'.</p> <p>The links between the questions and the policy were insufficiently direct to allow the Archives to accurately assess entity performance in implementing the Digital Continuity 2020 targets. In internal discussions the Archives observed that: 'The current version of Check-Up Digital was developed in alignment with the Digital Transition policy (2011) [...] Continuing to use the current survey...will not: be in alignment with, or provide agencies with, a roadmap to assist them with measuring progress against and meeting the Digital Continuity 2020 targets and implementation pathways'.</p>
2017	<p>The 2017 <i>Digital Continuity Statement</i> comprised 10 questions. The statement requested that entities respond to each survey question using a simplified scale comprised of three categories: completed; in progress; or not started.</p> <p>While the survey aimed to assess the progress of entities in implementing the '10 targets of the Digital Continuity 2020 policy', the survey questions were not directly aligned to the 10 recommended actions of the policy. They were a mix of recommended actions from the policy and the associated targets. In practice, six of the 10 recommended actions from the policy were assessed.</p> <p>The limitations of this survey were identified by the Archives in an end-of-project report, which included an observation that 'the broad nature of the statements and the chosen metric produced little useful information on which to report'.</p>
2018	<p>The 2018 <i>Check-up Plus</i> survey consisted of a series of questions primarily focused on assessing entity implementation of the Archives' broader Information Management Standard<sup>a</sup>, which is intended to reflect the Archives' expectations for the management of business information to enable agencies to meet business, government and community needs and expectations.<sup>b</sup></p> <p>The survey had a secondary focus on the Digital Continuity 2020 policy, and included 11 questions that link to, but do not directly align with, eight of the 10 recommended actions of the policy. Overall, the links between the 2018 survey questions and the Digital Continuity 2020 targets is stronger than the 2016 survey.</p>

Note a: National Archives of Australia, 'Information Management Standard,' available from <http://www.naa.gov.au/information-management/information-management-standard/index.aspx> [accessed 8 March 2019].

Note b. In 2016, the annual survey was aligned to the Digital Transition policy, and in 2018 the annual survey was aligned to the Information Management Standard launched in 2017.

Source: Analysis of documentation, surveys, survey reports.

3.15 The varying questions<sup>42</sup>, measures, and rating scales used to gauge performance since the launch of the policy has meant that the Archives has not collected consistent and comparable data

42 The Archives stated that the changes to the survey questions over the years 2016 to 2018 were in response to acknowledging the rate of digital uptake by agencies and their general improvement towards managing digital information. The value of the 2014 questions had diminished by 2016 and the necessary changes were improved to fine tune future surveys.

sets across the three surveys to enable analysis of entity progress to implement the targets over the life of the policy.<sup>43</sup>

3.16 To address this, the Archives has reviewed the 46 questions from the 2018 survey and identified 11 questions as ‘critical statements’ associated with the Digital Continuity 2020 policy. For 2019, a shortened survey of 15 questions has been released, 11 of which are the critical statements.

3.17 For 2020, the Archives intends to conduct a broader survey, similar to that conducted in 2018, with the shorter 2019 style survey to be issued again in 2021. This approach is intended to reduce the administrative burden on entities, while maintaining a common core of questions to facilitate longitudinal analysis of the data and assess entity progress over multiple reporting periods.

### **Benchmark measures of success**

3.18 In 2016, the Archives attempted to define ‘what success looks like’ in relation to whole-of-government take up of the Digital Continuity 2020 policy. In the 2016–17 corporate plan, the Archives selected the benchmark that ‘90 per cent of entities will manage information digitally by default in 2020’ for this purpose.

3.19 Internal briefings indicated an agreement that if an entity reported a level 3 maturity rating (‘defined’) or higher, the entity would be deemed to be ‘working digitally by default’.

3.20 It was subsequently identified that using this maturity scale to measure success was potentially inaccurate. According to the annual survey for 2016 the level 3 digital maturity rating is described as: ‘having implemented some digital business processes, systems, technologies and tools, as planned’. As such, the entities that may have only commenced or partially implemented the relevant strategies and plans to move to digital information management could be considered to be operating ‘digitally by default’.

3.21 It was subsequently discussed within Archives that a level 4 digital maturity rating of ‘managing’, defined as ‘my agency has systematically transformed many business processes, systems, technologies and tools to digital as planned’, was a more accurate measure of success. However, for reporting purposes, the level 3 digital maturity rating of ‘defined’ continued to be identified as the measure of success. In February 2019, the Archives advised entities that the ‘Join the Dots’ program (examined in paragraph 2.37) aims to support all agencies achieve a level 3 maturity<sup>44</sup> rating or above by the end of 2020.

3.22 Accordingly, the Archives has not established clear and consistent measures of success to evaluate and accurately report on the progress of entities to implement the targets of the Digital Continuity 2020 policy.

---

43 In 2016, the annual survey was aligned to the Digital Transition policy, and in 2018 the annual survey was aligned to the Information Management Standard launched in 2017.

44 Level 3 maturity is defined in the 2018 survey as ‘that entities have ‘often’ implemented practices, behavioural change is in progress, plans are established, resources have been identified and some change is occurring in parts of the agency.’

## Recommendation no.4

3.23 The National Archives of Australia should establish appropriate monitoring and evaluation arrangements for the Digital Continuity 2020 policy, and any successor policies that:

- (a) include performance measures that are relevant, reliable, and adequate in order to enable an accurate assessment of performance against strategic objectives, and the effectiveness of the administration and oversight arrangements to support achievement of policy objectives;
- (b) capture consistent performance information to enable accurate analysis of the performance of entities to implement targets over the life of the policy; and
- (c) clearly define how success will be measured and reported.

**National Archives of Australia response:** *Agreed.*

3.24 *The National Archives notes the need to establish clear and relevant performance measures for both:*

- (a) *its own delivery of policies and the support provided to Australian Government agencies to assist them to achieve the intended outcomes of the policy; and*
- (b) *progress made by Australian Government agencies towards achieving the outcomes of the policy.*

3.25 *The National Archives will identify performance measures to assess the effectiveness of its delivery of the Digital Continuity 2020 policy. These measures will be included in relevant internal reporting frameworks. Performance measurement will also be built into the development of any successor policies.*

3.26 *The National Archives has invested in a 4-year survey tool (2018/19-2022/23) which assesses agencies against the core information management requirements for Australian Government agencies, as well as to some extent Digital Continuity 2020 principles. The survey will be reviewed and revised where possible, noting the investment in the current tool and the need for consistency in reporting, to improve the ability to assess progress against Digital Continuity 2020 principles.*

3.27 *The monitoring and evaluation of any successor policies will take into account the lessons learned from the Digital Continuity 2020 policy and the recommendations of the audit report.*

## Do the monitoring and evaluation arrangements accurately assess the extent to which entities are meeting the targets of the Digital Continuity 2020 policy?

There are limited arrangements to accurately assess entity progress to implement the policy. Performance information is collected using an annual survey process, however the surveys have not been structured in a way that enables a direct view of entity progress to implement the policy. An analysis of a selection of questions from the 2018 survey, which could be linked to the policy, indicates a large portion of entities across government are at lower levels of maturity against the policy principles. The Archives has achieved high participation rates for the survey,



however the absence of any processes in 2017 and 2018 to verify the accuracy of entity self-assessments means that there is minimal assurance regarding the accuracy of these results. The 2018 progress report to the responsible Minister is ten months overdue.

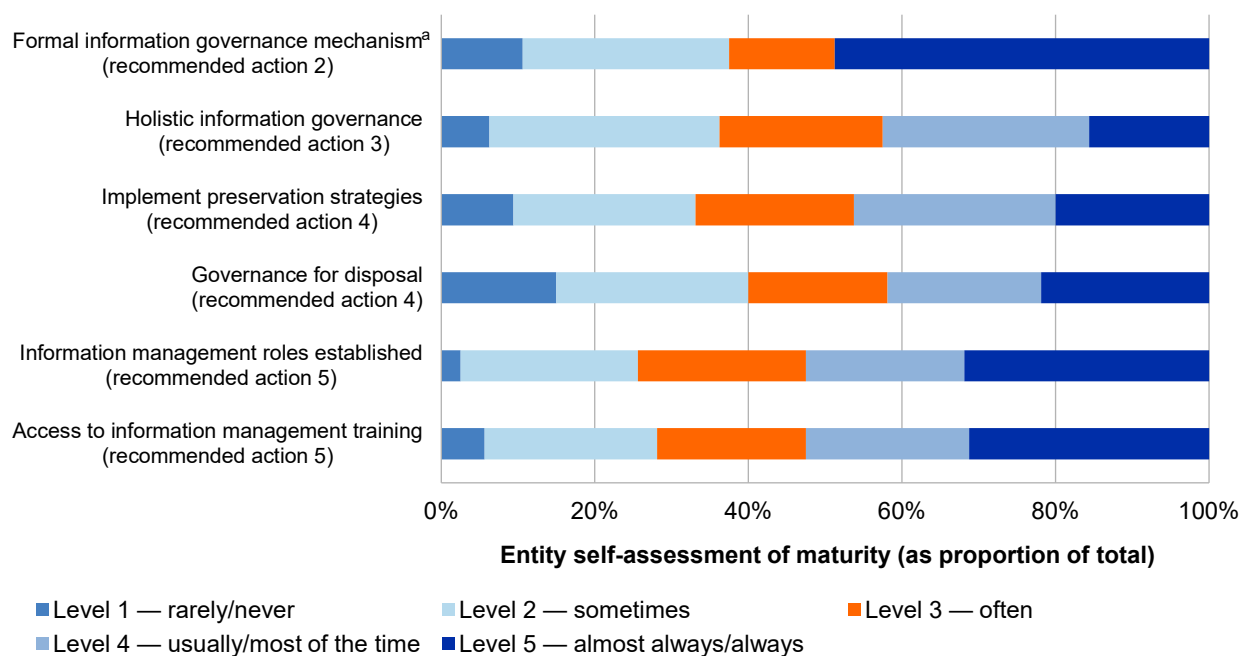
### Current data on entity progress in the implementation of the Digital Continuity 2020 policy

3.28 The annual survey for 2018 was focused on assessing entity compliance with the Archives' broader Information Management Standard, and as such is not structured in a way that enables a direct comparison of survey results with the targets of the Digital Continuity 2020 policy. The Archives has reviewed the 46 questions from the 2018 survey and identified 11 questions<sup>45</sup> as critical statements. An analysis has therefore been undertaken of the data associated with these 11 questions with the objective of gauging entity progress to implement the policy. The results of the analysis is detailed at Figure 3.1 to Figure 3.3.

#### Principle 1 — Information is valued

3.29 The survey results for the six questions that the Archives has mapped to Principle 1 of the Digital Continuity 2020 policy are examined in Figure 3.1 below.

**Figure 3.1: Entity self-assessment of maturity against 2018 survey questions linked to Digital Continuity 2020 Principle 1 'Information is valued'**



Note a: The question, does your agency have a formal governance mechanism with broad representation ensuring information management requirements are considered when making decisions? — had a different answer scheme to the other questions. There were four possible answers. To make the rating consistent across all questions, the audit team categorised responses to this questions as: Level 1 is a “No response”; Level 2 is “Partial – mechanism planned but not fully implemented or lacks maturity”; Level 3 is “Yes for ICT-related matters only”; Level 4 is excluded; and Level 5 is “Yes for all agency information management decisions”.

Source: Analysis of data from the 2018 Check-up Plus survey.

45 The eleven questions identified as critical statements include sub-parts to questions in the Check-Up Plus survey separately.

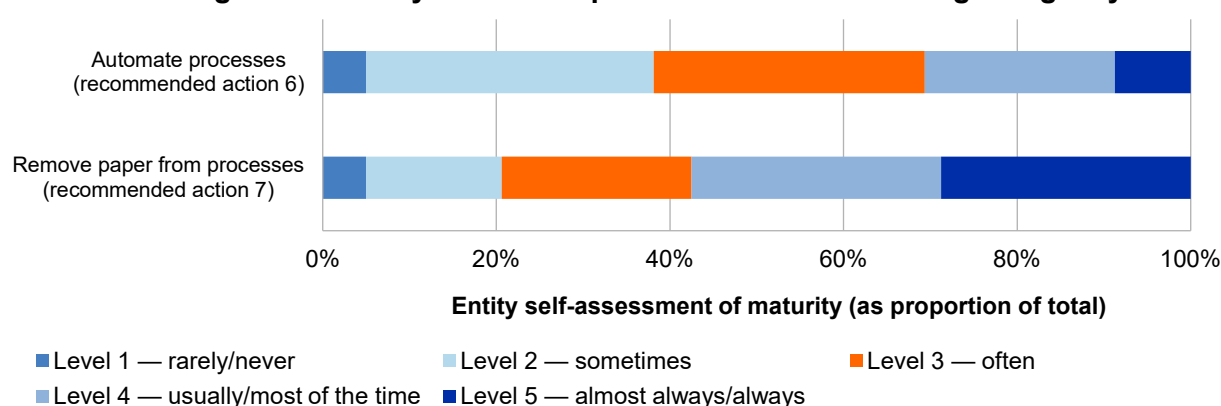
3.30 For the recommended actions associated with Principle 1 that were due by 31 December 2018, entities were to have established an information governance committee (recommended action 2) by 30 June 2016, and have an information governance framework (recommended action 3) in place by 31 December 2016. The survey results reflect that approximately two years after the associated due dates, 36 and 38 per cent of entities respectively have not implemented the two recommended actions. Recommended actions 4 and 5 are not due to be complete until 31 December 2020.

3.31 Overall, these results indicate that there is still significant progress required across Australian Government entities in order to meet the targets associated with Principle 1 of the policy.

### *Principle 2 — Information is managed digitally*

3.32 The survey results for the two questions that the Archives has mapped to Principle 2 of the Digital Continuity 2020 policy are examined in Figure 3.2.

**Figure 3.2: Entity self-assessment of maturity against 2018 survey questions linked to Digital Continuity 2020 Principle 2 ‘Information is managed digitally’**



Source: Analysis of the results of the 2018 Check-up Plus survey.

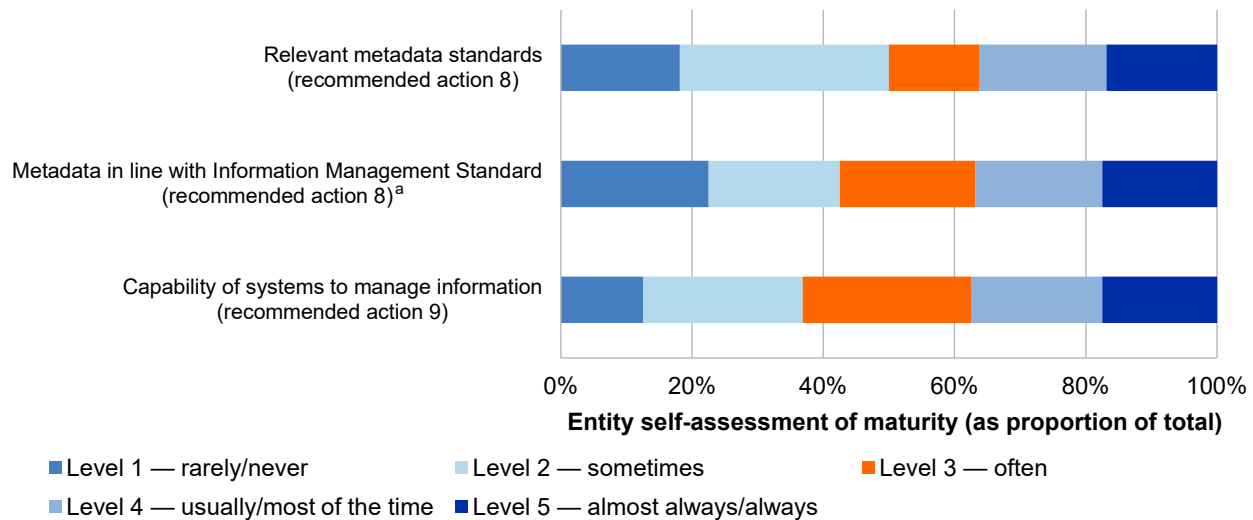
3.33 Both of the recommended actions for Principle 2 are not due until 31 December 2020. The results indicate that 38 per cent of entities have assessed their maturity at level two or below in relation to the automation of business processes.<sup>46</sup> Performance in relation to the removal of paper from existing process / digitisation of authorisations appears more positive, with 57 per cent of entities reporting that they are at maturity level 4 or above.

### *Principle 3 — Information, systems, and processes are interoperable*

3.34 The results for the three questions that the Archives has mapped to Principle 3 of the Digital Continuity 2020 policy are detailed at Figure 3.3.

46 Automating processes has been linked to recommended action no.6 of the Digital Continuity 2020 policy. This action requires that entities work digitally, with business interactions, decisions and authorisations recorded digitally. However, according to the digital authorisations and workflow framework released by the Archives in August 2018, implementing this target does not require full automation of business processes. Rather digital authorisations and workflows can include email, action tracking and system workflow approval, with digital signatures implemented as an additional layer for high risk processes, or to meet legislative requirements.

**Figure 3.3: Entity self-assessment of maturity against 2018 survey questions linked to Digital Continuity 2020 Principle 3 'Information, systems, and processes are interoperable'**



Note a: For this question, there was an additional possible answer. The sixth option was 'not measured'. To make the rating scale consistent across all questions for Principle 3, the audit team combined 'not measured' responses into Level 1.

Source: Analysis of the results of the 2018 Check-up Plus survey.

3.35 The recommended actions for Principle 3 are not due until 31 December 2020. However, for each question, between 39 and 51 per cent of entities have assessed their maturity at level 2 or below. This indicates that there is significant progress required across Australian Government entities in order to meet the targets associated with Principle 3.

### Reporting on entity progress in meeting the Digital Continuity 2020 targets

3.36 Following the completion of the annual survey by entities, the Archives produces a de-identified whole-of-government report which it publishes on its website.<sup>47</sup> The report presents summary results against five information management components.<sup>48</sup> The Archives also produces individual reports for entities. These reports have been produced since 2016 and include the individual entity's results and how these results compare to the whole-of-government population. Individual results are benchmarked against an average rating calculated using the self-reported results of all Australian Government entities that participated in the survey, however, the reports do not allow entities to compare progress against other entities with similar characteristics in either

47 Archives website reporting is available from <http://www.naa.gov.au/information-management/digital-transition-and-digital-continuity/reporting/index.aspx> [accessed 5 April 2019]. The release of the annual reports to government as part of the digital continuity policy was recommended in the Belcher review, however the recommendation did not require the report to be de-identified.

48 The five information management components addressed are: information governance; information creation; interoperability; storage; and disposal.

size or function. Similar surveys conducted by the APSC include the ability for entities to compare progress in this manner.<sup>49</sup>

3.37 The Digital Continuity 2020 policy requires that the Archives report annually to the Minister (the Attorney-General) outlining ‘agencies progress towards digital transition, the support provided, and additional support needed, by the Archives to further drive improvement.’ The Archives submitted reports to the Attorney-General detailing the results for the 2016 and 2017 surveys respectively, and has published these reports on its website. The reports outline: key survey results; areas for attention; products and advice issued in the previous year; proposed actions for the coming year; and illustrate that moderate improvement has been achieved across the Australian government between 2014 and 2016. The 2018 report was delayed from October 2018 to March 2019 to allow for an analysis of the survey data, however was then further delayed due to the election and subsequent entry into the caretaker period. The 2018 report was scheduled to be issued in August 2019.

### **Processes to manage the accuracy and validity of reporting on entity progress**

#### *Participation rate*

3.38 To date, the Archives has focused on maximising participation rates for the annual surveys across 160 Australian Government agencies. The Archives has a structured approach to tracking the responses of individual entities, following up entity progress in submitting survey responses, and has previously extended the survey period in order to maximise the response rate.

3.39 Since the launch of the policy, the Archives has had a target response rate of 95 per cent in 2016–17 and 2017–18, increasing to 96 per cent in 2018–19. These targets were met and exceeded in all three years with a 100 per cent response achieved in 2016–17 and 2017–18; and 97 per cent response rate in 2018–19.

#### *Quality assurance*

3.40 The quality assurance processes that the Archives has undertaken for each of the annual surveys are outlined at Table 3.3.

**Table 3.3: Quality assurance activities on annual survey data**

Survey	Assurance activity and results
2016	<p>An external provider was contracted to administer the 2016 Check-up Digital survey, including checking a sample of 30 entity responses (from a population of 165) to gauge consistency between the self-assessment ratings and the evidence provided by entities to support their responses.</p> <p>The 2016 consistency checks found:</p> <ul style="list-style-type: none"> <li>• high consistency for 41 per cent of entity ratings;</li> <li>• partial consistency for 28 per cent of entity ratings; and</li> <li>• low consistency for 31 per cent of entity ratings.</li> </ul>

49 The annual State of the Service Report 2017–18 includes a complete list of entities in each portfolio, categorised as policy, smaller operational, larger operational, regulatory or specialist entities and includes a headcount. The inclusion of this data allow comparisons to be made between entities of similar size and function. The report is available from [https://www.apsc.gov.au/sites/default/files/18583 - apsc - sosr - web.pdf](https://www.apsc.gov.au/sites/default/files/18583_-_apsc_-_sosr_-_web.pdf) [accessed 01 Aug 2019].

Survey	Assurance activity and results
2017	Entities were not required to provide documentation to support survey responses. The Archives advised entities that it 'reserved the right to audit entity responses', however it did not audit any of the survey responses.
2018	An external provider was contracted to administer the 2018 Check-up Plus survey to check that completed surveys were submitted by each entity and that answers to costing questions were consistent. There were no other quality assurance activities undertaken to verify the accuracy of entity responses.

Source: Analysis of Archives' documentation.

3.41 The survey process in each of the three years since the Digital Continuity 2020 policy was released has required that entities self-assess their progress to implement the recommended actions and associated targets of the policy. As part of the survey, the Archives requests that 'agency heads' approve their entity's responses prior to final submission. The Archives relies on this process to assure the accuracy of the relevant submission.

3.42 Testing conducted on a sample of 30 (18 per cent) of the respondents to the 2016 survey found that 59 per cent of the checked responses had low or partial consistency.<sup>50</sup> This data forms the basis of reporting on whole-of-government progress in the implementation of the policy. As such, activities should have been undertaken to provide assurance on the accuracy of the 2017 and 2018 survey results.

## Recommendation no.5

3.43 The National Archives of Australia should develop and implement a regime to provide appropriate assurance on the accuracy of reported data on entity progress in the implementation of the Digital Continuity 2020 policy.

**National Archives of Australia response:** *Agreed.*

3.44 *Assurance of the accuracy of agency responses to the annual survey has been achieved through agency head sign-off as the accountable authority. The National Archives will explore additional options for validation and quality assurance of survey responses within resource constraints.*

<sup>50</sup> Low consistency means that the response did not match the criteria at the stated level, or another rating is clearly more appropriate based on the evidence provided. Partial consistency means that the response matched some of, but not all, the criteria at the stated level.

## 4. Implementation of the Digital Continuity 2020 policy by the selected entities

---

### Areas examined

This chapter examines the extent to which the Attorney-General's Department (AGD), the Civil Aviation Safety Authority (CASA) and the Office of the Inspector-General of Intelligence and Security (IGIS) have implemented the Digital Continuity 2020 policy. The chapter also includes an examination of the entities internal reporting arrangements.

### Conclusion

AGD, CASA, and IGIS have partially implemented the targets of the Digital Continuity 2020 policy due by 31 December 2018. AGD has fully implemented or made substantial progress against all of the targets. CASA has partially implemented all targets except for one. IGIS has not implemented a number of targets, particularly those associated with principle two of the policy. AGD and CASA have established specific arrangements to internally monitor and report on progress against the targets of the policy. IGIS does not have such arrangements.

### Recommendations

This chapter has identified that work is required by all three entities to fully implement the policy targets due by 31 December 2018. The chapter includes two recommendations, and identifies areas for improvement to further entity progress to implement the targets and improve internal monitoring and reporting arrangements.

### Have the selected entities achieved the targets of the Digital Continuity 2020 policy?

AGD, CASA, and IGIS have partially achieved the 17 Digital Continuity 2020 targets due by 31 December 2018. All entities have implemented the majority of targets under principle one associated with information governance. AGD and CASA have made progress in the management of information digitally under principle two. Although IGIS may be unable to digitise a selection of analogue records due to originator entity restrictions, it has not implemented any of the general targets associated with the management of information in digital format. Work is required by all entities to implement the interoperability targets under principle three. However, AGD and CASA have commenced work to transfer remaining paper-based processes to digital, identify all information assets, and ensure that business systems will meet the minimum metadata and information management functional requirements.

4.1 The *Digital Continuity 2020 – Agency Implementation and Pathways* document (implementation guidance) lists the recommended actions under the Digital Continuity 2020 policy (policy), and breaks down these recommended actions into smaller 'targets' that entities should progressively implement. The implementation guidance lists a total of 29 targets, 17 of which were to have been implemented on or before 31 December 2018. This audit has assessed the progress that the Attorney-General's Department (AGD), the Civil Aviation Safety Authority (CASA) and the

Office of the Inspector-General of Intelligence and Security (IGIS) have made to implement these targets<sup>51</sup>, and the results are presented at a summary level in Table 4.1 below.

**Table 4.1: Extent to which entities have implemented targets due prior to 31 December 2018 (as at July 2019)**

	AGD			CASA			IGIS		
	Fully	Partial	Not	Fully	Partial	Not	Fully	Partial	Not
Principle 1	8	0	0	6	1	1	7	1	0
Principle 2	4	1	0	3	2	0	0	0	5
Principle 3	2	2	0	1	3	0	0	3	1
Total	14	3	0	10	6	1	7	4	6
<b>Total Targets</b>	<b>17</b>								

Source: ANAO analysis of selected entities' documentation against the Archives' 'Targets and Pathways' document.

Note: Principle 1: Information is valued; Principle 2: Information is managed digitally; Principle 3: information, systems and processes are interoperable.

## Principle 1 — information is valued

4.2 Principle 1 — *Information is valued*, identifies 13 targets that entities are to meet in order to implement the five recommended actions under this principle. Eight of the 13 targets were to have been implemented by 31 December 2018. The remaining five targets are due between September 2019 and December 2020. Table 4.2 lists the eight targets due by 31 December 2018, details the average digital maturity rating as self-reported by each of the selected entities in the 2018 Check-up Plus survey, and compares it with an assessment of the actual progress that the selected entities have made to achieve the targets associated with Principle 1 of the policy.

**Table 4.2: Extent to which entities have implemented the targets of Digital Continuity 2020 policy Principle 1**

Recommended action	Target	Target date	AGD	CASA	IGIS
Entity self-assessment — Principle 1 — average rating (out of 5) <sup>a</sup>			4.2	3.1	3.9
Information Governance Reporting	Agency senior management drives change to digital information and records management. Survey reports to the Archives are authorised by agency heads.	31 December 2015	◆	◆	◆
	Annual agency survey reporting	30 September 2016	◆	◆	◆

51 The benchmark is the Agency implementation and pathways guidance issued by the National Archives in October 2015. This implementation guidance was revised in October 2017 and again in February 2019. The revisions to the implementation and pathways document introduced four new targets. Three of the targets are aligned with Principle 1, and one target is aligned to Principle 2.



Recommended action	Target	Target date	AGD	CASA	IGIS
	Annual agency survey reporting	31 August 2017	◆	◆	◆
	Annual agency survey reporting	30 September 2018	◆	◆	◆
Agencies have an information governance framework	Agencies have an information governance framework	31 December 2016	◆	▲	▲
Agencies have established an Information governance committee	Agencies have established an Information governance committee	30 June 2016	◆	◆	◆
Agencies meet targets for skilled staff	Agencies have a Chief Information Governance Officer	31 December 2017	◆	◆	◆
	Agencies establish and implement a program of continuing professional development of information management staff for professional recognition	31 December 2018	◆	■	◆

Legend: ◆ fully implemented  
▲ partially implemented  
■ not implemented

Note a: The entity's self-assessed average rating has been determined by mapping the recommended actions outlined in the policy to the 11 relevant questions in the Check-Up Plus 2018 annual survey (See Appendix 6). It uses a rating scale of 1 to 5, where Level 1 means rarely/never (not implemented), Level 2 means sometimes (partially implemented); Level 3 means often (partially implemented); Level 4 means usually and/or most of the time (fully implemented); and Level 5 means almost always or always (fully implemented).

Source: Analysis of department documentation.

4.3 The results of this analysis reflect that AGD has implemented all eight targets associated with Principle 1 which were due by 31 December 2018. CASA has implemented six targets, partially implemented one target, and has not implemented one target. IGIS has implemented seven targets, and partially implemented one target.

4.4 Given that the entity self-assessments were completed through the Check-up Plus survey in September 2018, and that a number of activities have been undertaken by entities to progress the implementation of the recommended actions and targets during the course of the audit<sup>52</sup>, the self-assessment ratings for AGD (4.2 out of 5), CASA (3.1) and IGIS (3.9) broadly align with actual progress.

<sup>52</sup> Audit fieldwork occurred from December 2018 to June 2019.



*Information governance reporting*

4.5 All three of the selected entities submitted responses to the Archives annual agency surveys associated with digital information management between 2016 and 2018 (see paragraphs 3.12 to 3.16) for detail on the associated surveys conducted each year. Each survey response was approved by the relevant agency head. Therefore, all three entities have fully implemented this recommended action, and the associated targets.

*Entities have an Information governance framework*

4.6 The implementation guidance on the Archives' website states that an information governance framework 'is the legal, regulatory and business context within which information assets are created, used and managed.' Entities are required to set out an approach and commitment to implementing an effective governance framework, and the controls required to maintain it.<sup>53</sup> The target associated with this recommended action was due 31 December 2016.

4.7 AGD has a documented information governance framework. The framework is supported by an information management policy, with additional supporting guidance hosted on the department's intranet. As such, AGD has fully implemented this target.

4.8 CASA does not have a documented information governance framework. However, CASA does have an information management manual that details the legislative, regulatory and policy framework associated with its information governance. Following a 2015–16 internal audit, CASA developed an Enterprise Information Management Strategy that was issued in October 2017. The strategy states that CASA will identify and implement a program of work including:

- completing an information review;
- developing an enterprise information management model;
- developing and implementing an information governance framework; and
- achieving key milestones of the service delivery transformation project.

4.9 Work to implement the components of the strategy relevant to establishing an information governance framework commenced in January 2019 when CASA engaged an external contractor to review the current state of information governance, develop an information governance model, and an implementation plan to guide the development of information governance into the future. This work is not yet complete, and as such, CASA has partially implemented the recommended action and associated target.

4.10 IGIS has an information and records management policy that details: how records are to be created and maintained; procedures for carrying out information management functions; general records management practices; legislation; and a description of the operating environment. However, the policy applies to paper-based (hard-copy) files and information only. The policy has

---

53 The implementation guidance also specifies that the documented information governance framework should: outline the broad environment within which information is created and managed; describe the factors and business drivers that determine or influence the creation, management and use of information, including legislation, regulations, compliance, risk, and business needs; document the principles that guide the creation, management and use of information; provide an overarching description of how information is governed; and documents the commitment to information governance with senior management endorsement.

not been updated since 2014, however has been extended while changes to IGIS' service delivery arrangements and operations are underway, including the transfer of IGIS into the Attorney-General's portfolio<sup>54</sup>, subsequent move to new premises, the purchase of licenses to install an Electronic Document Records Management System (EDRMS), and steps taken to establish digital information management practices. The existing framework will remain in place until planned changes to IGIS' operating environment<sup>55</sup> to implement the recommendations of the 2017 Independent Intelligence Review have been completed.<sup>56</sup> Therefore, IGIS has partially implemented the recommended action and associated target.

#### *Entities have an Information governance committee*

4.11 The implementation guidance on the Archives' website states that an information governance committee can be established as a board, a working group, or its responsibilities can be absorbed into an existing governance committee. The recommended action and associated target was due 30 June 2016.

4.12 AGD has utilised an existing governance committee — the Information, Communication and Technology Committee (ICTC) — for the purpose of information governance. The terms of reference for this committee state that the purpose of the ICTC is to provide:

- strategic direction for AGD's ICT environment;
- strategic oversight and governance of the department's ICT operations, strategies, information governance framework, policies and practices; and
- monitor the implementation of the ICT strategic plan and support compliance with the Digital Continuity 2020 policy.

4.13 AGD revised the terms of reference of the ICTC to include information management responsibilities in February 2016, and again in May 2018. Therefore, AGD has fully implemented the recommended action and associated target.

4.14 CASA has also utilised existing governance structures, however initially elected to split the information governance responsibilities across four committees:

- the Enablement and Capability Group<sup>57</sup>;
- the Protective Security Subcommittee;

---

54 On 10 May 2018, the Office of the Inspector-General of Intelligence and Security was subject to a machinery of government (MoG) transfer out of the Prime Minister's portfolio into the Attorney-General's portfolio.

55 The 2017 intelligence review recommended that the remit of the Office of the Inspector-General of Intelligence and Security be expanded to cover the ten agencies that constitute the national intelligence community.

56 Implementation of the expansion of the Office of the Inspector-General of Intelligence and Security's remit as recommended in the 2017 intelligence review is subject to Parliament passing the relevant amendments to the *Inspector-General of Intelligence and Security Act 1986*.

57 The Enablement and Capability Group is chaired by the Chief Information Officer and is responsible for reviewing and prioritising proposed change initiatives and providing advice on issues impacting delivery of agreed ICT and non-ICT projects and business changes.

- the Service Delivery Transformation Program Board<sup>58</sup>; and
- the Business Improvement Program Board.<sup>59</sup>

4.15 CASA has now consolidated, the Service Delivery Transformation Program Board, and the Business Improvement Program Board into a single committee — the Business Improvement Program and Oversight Board. This board was established, and the first meeting held in April 2019. The terms of reference for this board include providing strategic direction and oversight of programs, projects, and business improvement initiatives aimed at improving the efficiency of operations and processes, including the enabling activities required to support successful implementation such as records and information management. As such, CASA has fully implemented the recommended action and associated target.

4.16 IGIS' information governance arrangements are comprised of weekly senior staff meetings and monthly all staff meetings.

4.17 These arrangements are sufficient given the small size of the entity and co-location of staff. As such, IGIS has fully implemented this action and associated target. However, the size and jurisdictional responsibilities of IGIS as outlined in the 2018–19 corporate plan are planned to expand in line with recommendations from the 2017 Intelligence review. As such, there would be benefit in IGIS establishing fit-for-purpose governance arrangements, particularly as the management and security of information is a key priority for the entity.

#### *Entities meet targets for skilled staff*

4.18 The implementation guidance available on the Archives' website states that agencies should increase support for their information practitioner's development 'to effectively deal with today's dynamic digital environment, identifying that qualified and skilled information professionals are required.' The targets associated with this action are intended to support entities meet targets for skilled staff, by:

- establishing a Chief Information Governance Officer (due 31 December 2017); and
- establishing and implementing a program of continuing professional development (due 31 December 2018).

#### Chief Information Governance Officer

4.19 AGD and CASA have established a Chief Information Governance Officer (CIGO) role. AGD has expanded the Chief Information Officer (CIO) role to include the responsibilities of the CIGO, whereas CASA has elected to split the responsibilities of the role across two existing positions —

---

58 The Service Delivery Transformation Program Board provides oversight and strategic advice for implementation of the Service Delivery Transformation Program. The program is intended to embed information management processes into CASA business processes, reduce the frequency and effort for data entry, provide real time status updates on client requests, and timely and accurate provision of information.

59 The purpose of the Business Improvement Program Board is to provide oversight, strategic advice and direction of CASA's business improvement program by monitoring milestones, dependencies, risks and issues, and ensuring sufficient resourcing is allocated to support efficient delivery of the improvement programs.

the CIO and the Branch Manager for Governance.<sup>60</sup> Therefore, AGD and CASA have fully implemented this target.

4.20 The responsibilities of the CIGO role in IGIS have been allocated to the Director of Enabling Services. For small or micro agencies such as IGIS, CIGO responsibilities can be included into the most senior information management role available. As such, IGIS has fully implemented this target.

Implementation of a program of continuing professional development for information management staff

4.21 As discussed at paragraph 2.16, the Archives released an information management and data capabilities matrix in May 2018 detailing the skills, knowledge, and information management experience required by all staff, information management professionals, and senior executives. This tool was launched to assist entities identify and prepare professional development strategies for their information management workforce.

4.22 AGD developed a continuing professional development strategy for information management staff in December 2018, and the strategy was approved in January 2019. AGD also established all-staff learning and development themes for 2018–19 that include digital and data skills. Therefore, AGD has fully implemented this target.

4.23 CASA has established a project plan to develop e-learning courses for information governance and records management including EDRMS specific courses. According to the project plan, information governance and records management courses were to be finalised and released by mid July 2019. In response to an internal audit, issued in May 2019, CASA stated that development of an information management curriculum to cover information governance and records management was still underway. Therefore, CASA has not implemented this target.

4.24 IGIS has not developed or established a formal program of continuing professional development for information management. However, continuing professional development requirements relating to information management have been included in the personal development agreements for the Director, and Assistant Director of Enabling Services. Given IGIS' status as a micro agency, there is little value in establishing a formal program of continuing professional development for the limited number of staff with information management responsibilities. As such, IGIS has fully implemented this target.

## **Principle 2 — Information is managed digitally**

4.25 Principle 2 — *Information is managed digitally*, identifies nine targets that entities are to meet in order to implement the two recommended actions of the policy. Five of the nine targets were to have been implemented by 31 December 2018. The remaining four targets are due between 30 June 2019 and 31 December 2020. Principle 2 identifies that entities are to manage their information digitally with business interactions, decisions, and authorisations recorded digitally, and migrate information in analogue to digital format where there is value for business. Table 4.3 lists the five targets that were due by 31 December 2018, details the average digital maturity rating as self-reported by each of the selected entities in the 2018 Check-up Plus survey,

---

60 CASA has since identified that while the CIGO role was split across the CIO and Branch Manager for Governance, the split of responsibilities needs to be finalised, and the role descriptions updated to ensure agreed arrangements are accurately reflected.

and compares this with an assessment of the actual progress that the selected entities have made to achieve the targets associated with Principle 2 of the policy.

**Table 4.3: Entity progress to implement the targets of Digital Continuity 2020 policy - Principle 2**

Recommended action	Target	Target date	AGD	CASA	IGIS
Entity self-assessment — Principle 2 — Average rating (out of 5) <sup>a</sup>			3.0	2.5	1.5
Agencies work digitally, with business interactions, decisions, and authorisations recorded digitally.	Agencies have reduced reliance on paper and duplication of information in digital and physical formats. Agencies have identified paper-based business processes.	31 December 2015	◆	◆	■
	Agencies identify high-value and long-term information assets, evaluate risk and management requirements, and implement strategies to support digital continuity.	31 December 2016	◆	◆	■
	Agencies transform most paper-based business processes to digital, and routinely make and record decisions using digital authorisations and workflows.	31 December 2017	◆	▲	■
	Agencies identify all information assets, evaluate risk and management requirements, and identify strategies to support digital continuity.	31 December 2018	▲	▲	■
Information in analogue formats is migrated to digital format where there is value for business	All records created in digital formats after this date are managed digitally.	1 January 2016	◆	◆	■

Legend: ◆ fully implemented

▲ partially implemented

■ not implemented

Note a: The entity's self-assessed average rating has been determined by mapping the recommended actions outlined in the policy to the 11 relevant questions in the Check-Up Plus 2018 annual survey (see Appendix 6). It uses a rating scale of 1 to 5, where Level 1 means rarely/never (not implemented), Level 2 means sometimes (partially implemented); Level 3 means often (partially implemented); Level 4 means usually and/or most of the time (fully implemented); and Level 5 means almost always or always (fully implemented).

Source: Analysis of department documentation.

4.26 Of the five targets due by 31 December 2018, the results of this assessment reflect that AGD has implemented four targets and partially implemented one target. CASA has implemented three targets and partially implemented the remaining two, whereas IGIS has not implemented any of the targets. Overall, the average self-assessment ratings for AGD (3.0), CASA (2.5) and IGIS (1.5) broadly align with actual progress.

*Entities work digitally, with business interactions, decisions, and authorisations recorded digitally*

4.27 To achieve the targets of the policy entities are to: transform most paper-based business processes to digital; routinely make and record decisions using digital authorisations and workflows; have identified high value and long-term information assets by 31 December 2016; and identified all information assets, evaluated risk and management requirements, and implemented strategies to support implementation of the policy by 31 December 2018.

4.28 To assist agencies implement this target, the Archives released a digital authorisation framework (see paragraph 2.21), and a business systems assessment framework (see paragraph 2.23). The digital authorisation framework is a risk-based assessment tool for transforming analogue approval processes to fit-for-purpose digital approvals. The tool identifies four approval methods that can be applied to transfer paper-based processes to digital — email, action tracking, system workflows and digital signatures. The target associated with this recommended action was to have been implemented by 31 December 2017. The business system assessment framework provides entities with a structured approach to the assessment of information management functionality in business systems based on the value of information and the associated level of risk.

4.29 In April 2016, AGD identified 160 paper-based processes within the department. Of these paper-based processes, 117 required that the associated documents be digitised at the conclusion of the process. In August 2016, AGD released its information management policy which identified that emails are to be used to record business decisions and then transferred into the department's EDRMS. AGD's financial, human resource and case management systems have digital workflows embedded. AGD has identified that the 43 remaining paper-based processes will have digital workflows and authorisations embedded where practical as supporting business systems are upgraded or refreshed.

4.30 In March 2019, AGD determined that there was no requirement to complete an information stocktake to identify all information assets, stating that information assets and associated management requirements are identified and evaluated in accordance with agency specific and relevant general records authorities<sup>61</sup>, privacy impact assessments<sup>62</sup>, and business continuity and disaster recovery plans.<sup>63</sup> The strategy to support digital continuity is for information management requirements to be incorporated into the business system upgrades and/or redevelopment processes (see paragraph 4.56). Work to review the records authorities for AGD has been proposed

---

61 A records authority is a legal instrument that allows agencies to make decisions about keeping, destroying or transferring Australian Government records. There are two types of records authorities – General Records Authorities and Agency-specific records authorities. Information available from <http://www.naa.gov.au/information-management/records-authorities/index.aspx> [accessed 9 June 2019].

62 Privacy impact assessments are a systematic assessment of a project that identifies the impact that the project might have on the privacy of individuals and sets out recommendations for managing, minimising, or eliminating that impact. Privacy Impact Assessments assist entities to: describe how personal information flows in a project; analyse the possible impacts on individuals' privacy; identify and recommend options for avoiding, minimising, or mitigating negative privacy impacts; build privacy considerations into the design of a project; and achieve the project's goals while minimising the negative and enhancing the positive privacy impacts. Information available from <https://www.oaic.gov.au/agencies-and-organisations/guides/guide-to-undertaking-privacy-impact-assessments> [accessed 9 June 2019].

63 The business continuity and disaster recovery plans identify how business systems and the information within them will be protected.

as the current agency specific records authorities are out of date and do not reflect the full span of information types currently in use. As at June 2019, approval to commence the review and update the records authority has not been provided by AGD.

4.31 As outlined in the paragraphs above, AGD has:

- fully implemented the two targets associated with reducing reliance on paper processes, identifying and evaluating high-value information assets, and identifying strategies to support digital continuity;
- fully implemented the target associated with transforming most paper based business processes to digital processes; and
- partially implemented the target associated with the identification and evaluation of all information assets and implementation of strategies to support digital continuity.

4.32 CASA's Electronic Transactions policy allows for electronic approvals and deems them the equivalent of a physical signature. The Electronic Transactions policy was due to be reviewed in 2016. However, the review did not take place and the policy does not align with the Digital Continuity 2020 policy. As part of a broader Service Delivery Transformation Project, CASA has commenced work to develop and implement digital authorisation and workflows into ICT systems, and has commenced a forms improvement project. This work is ongoing, and a recent internal audit identified instances where new hard copy files were being created, and of decisions being stored in personal drives. As such, CASA has partially implemented this target.

4.33 To identify information assets and strategies to support digital continuity, CASA has developed an information asset register, and completed a business assessment for eight high value business systems. The information asset register states that 99.5 per cent of CASA's information assets are in digital format; and identifies the desired future state for each remaining information asset. As part of the Enterprise Information Management Strategy, CASA has engaged an external contractor to assist identify information assets and implement strategies to support digital continuity. While work has commenced, it is not yet complete, and has not been rolled into business as usual practices.

4.34 CASA has therefore:

- fully implemented the two targets associated with reducing reliance on paper, and identifying high-value information assets and strategies to support digital continuity;
- partially implemented the target to transform paper based processes to digital processes; and
- partially implemented the target to identify all information assets, evaluate risk, identify and implement strategies to support digital continuity.

4.35 IGIS has not developed or implemented digital authorisations and workflows into business processes. While emails may record decisions, the email record must then be printed and filed in accordance with IGIS' information and records management policy, which states that 'the electronic version of any document is regarded as an unreliable reference and must not be used for decision making'. As at June 2019, IGIS has procured licences for, and is in the process of building and installing an EDRMS, and finalising the design and functional specifications of a case management system. When completed, the installation of these two systems should allow IGIS to incorporate digital authorisations and workflows into some business processes. However, work to implement

these systems is not yet complete and as such IGIS cannot be considered to have implemented this target.

4.36 In March 2019, IGIS conducted a stocktake of its hardcopy information assets as part of moving to new premises. As at June 2019, IGIS has procured licences for, and is in the process of building and installing an EDRMS, and finalising the design and functional specifications of a case management system. IGIS has stated that a digital transformation project is planned for the second half of 2019 and that it intends to establish a process whereby all new records will be managed digitally by the end of 2019.

4.37 IGIS handles classified and sensitive data on behalf of other agencies. The Protective Security Policy Framework (PSPF) states that material which is subject to an information security caveat must be handled in accordance with any special handling requirements imposed by the originator and caveat owner. Accordingly, there are instances where IGIS is subject to policy direction by an originating entity to retain particular information in hard copy only.<sup>64</sup> IGIS has indicated, therefore, that some paper-based records may not ever be suitable for digitisation.

4.38 Whilst noting this context, IGIS cannot be considered to have met the recommended action and associated target in relation to this principle of the policy.

*Information in analogue format is migrated to digital format where there is value for the business*

4.39 To implement this recommended action, entities are to have achieved targets in relation to digitally managing all records created after 1 January 2016.

4.40 AGD's information management framework stipulates that all business records must be captured into the approved EDRMS, unless there is a specific exemption in place<sup>65</sup>, and a digitisation guide has been created to support the migration of analogue documents into digital formats. In June 2017, AGD reported that 90 per cent of the department's information is created and managed digitally, with the remaining 10 per cent of files created and managed physically. AGD has therefore fully implemented the target to appropriately manage records created in digital format.

4.41 CASA's information management manual requires that staff capture and manage all business records in electronic format in a compliant recordkeeping system<sup>66</sup>, and CASA has created a digitisation guide to support the migration of analogue documents into digital formats. In 2017, CASA developed an Enterprise Information Management Strategy, which sets out a program of work over three years (2017–2020) that includes ensuring that information in analogue formats is migrated to digital format where there is value for money. CASA has also commenced work to identify and catalogue physical records holdings. CASA has therefore fully implemented the target to appropriately manage records created in digital format.

---

64 For example, the Australian Signals Intelligence Security Regulations and Orders (ASSRO).

65 Exemptions that are in place currently include documentation required internationally or domestically for litigation, international transfer of prisoners, and abduction cases, or where the relevant record has a security classification of secret or higher.

66 The policy includes a small register of records which are exempt from these requirements. Staff are nonetheless required to obtain approval for the creation and / or maintenance of exempt records.



4.42 All IGIS information assets are currently paper-based, with any records created digitally required to be printed and stored in hardcopy. IGIS' information and records management policy states that 'the electronic version of any document is regarded as an unreliable reference and must not be used for decision making'. As such, IGIS has not implemented this target.

### Principle 3 — Information, systems and processes are interoperable







4.43 Principle 3 — *Information, systems and processes are interoperable* identifies seven targets that entities are to satisfy in order to implement the three recommended actions under this principle. Of the seven targets, four were to have been implemented by 31 December 2018. The remaining three targets are due to be implemented by 31 December 2020.

4.44 Under Principle 3, entities are to have interoperable information systems and processes that: meet standards for short and long-term management; improve information quality; and enable information accessibility, management, and reuse. The Archives have developed two tools to support entities achieve the associated targets due by 31 December 2018 and embed the principles of the policy:

- a business systems assessment framework<sup>67</sup>; and
- a minimum metadata set.<sup>68</sup>

4.45 Table 4.4 lists the four targets which were due by 31 December 2018, details the average digital maturity rating as self-reported by each of the selected entities in the Check-up Plus annual survey conducted in 2018, and compares it with an assessment of the actual progress that the selected entities have made to achieve the targets associated with Principle 3 of the policy.

**Table 4.4: Recommended actions, associated targets, and target dates for Principle 3**

Recommended action in the DC2020 policy	Target	Target date	AGD	CASA	IGIS
Entity self-assessment — Principle 3 — Average rating (out of 5) <sup>a</sup>			3.0	2.25	2.0
Information is managed based on format and metadata standards for information governance and interoperability.	All business systems procured after this date will meet minimum metadata standards, and will be evaluated against the Archives' business systems assessment framework to meet functional requirements for information management.	31 December 2016			
	All business systems containing high-value and long-term information assets meet minimum metadata standards.	31 December 2017			

67 This provides a consistent, streamlined, risk-based approach to the assessment of information management functionality. The Archives have also provided an online pilot tool that supports entities assess the information management functionality of their business systems.

68 This identifies the properties required for the efficient and effective management of business information, described in the Archives tools and guidance available from <http://www.naa.gov.au/information-management/digital-transition-and-digital-continuity/information-is-interoperable/metadata/index.aspx> [accessed 10 April 2019].

Recommended action in the DC2020 policy	Target	Target date	AGD	CASA	IGIS
All business systems meet functional requirements for information management.	All business systems are evaluated against the Archives' business systems assessment framework to meet functional requirements for information management.	31 December 2018	◆	▲	▲
	Functional requirements are implemented where necessary.	31 December 2018	▲	▲	▲

Legend: ◆ fully implemented  
▲ partially implemented  
■ not implemented

Note a: The entity's self-assessed average rating has been determined by mapping the recommended actions outlined in the policy to the 11 relevant questions in the Check-Up Plus 2018 annual survey (see Appendix 6). It uses a rating scale of 1 to 5, where Level 1 means rarely/never (not implemented), Level 2 means sometimes (partially implemented); Level 3 means often (partially implemented); Level 4 means usually and/or most of the time (fully implemented); and Level 5 means almost always or always (fully implemented).

Source: Digital Continuity 2020 policy, October 2015, p. 5.

4.46 Of the four targets due to be implemented by 31 December 2018, the results of this assessment reflect that AGD has fully implemented two targets, and partially implemented two targets. CASA has fully implemented one target and partially implemented three targets. IGIS has partially implemented three targets and not implemented one target. Overall, the average self-assessment ratings for AGD (3.0), CASA (2.25) and IGIS (2.0) broadly align with actual progress.

### *Information is managed based on format and metadata standards for information governance and interoperability*

#### New business information systems

4.47 The first target for this recommended action states that all business systems procured after 31 December 2016 must meet minimum metadata standards, and should be evaluated against the Archives' business systems assessment framework to meet functional requirements for information management. Digital Continuity 2020 guidance material states that for new systems the ability to capture the minimum metadata should be included as a requirement in procurement documentation.

4.48 Since 31 December 2016, AGD has purchased two new modules for an existing business system.<sup>69</sup> The procurement and solution architecture documentation did not state that the business system must meet the minimum metadata standards. In January 2019, AGD advised that checks are being built into governance arrangements to rectify this oversight. The Attorney-General's Approved Technologies Committee (AGTAC) oversees the certification process to ensure that new IT equipment and software is assessed as compatible with existing infrastructure. However, the terms of reference for the AGTAC do not identify minimum metadata and information management functionality requirements as one of the criteria necessary to achieve AGTAC certification. As such,

<sup>69</sup> The new modules were for external recruitment and on-boarding modules for the HR system (Aurion).

AGD has partially implemented this target. AGD should update the terms of reference for the AGTAC to ensure that minimum metadata standards and information management functionality requirements are addressed when procuring new business system applications, versions, or modules of software in the future.

4.49 CASA also procured two new business system after 31 December 2016, and did not confirm that the systems would meet the minimum metadata standards or evaluate the system against the Archives' business system assessment framework. Subsequently, CASA updated the documentation it uses to set out the technical requirements for new ICT products. The update includes the requirement that new products be evaluated with reference to the Archives' Business System Assessment Framework. Further, new products are required to comply with the metadata standards. This documentation is to be included with any procurement. As such, CASA has partially implemented this target.

4.50 In January 2019, IGIS procured licenses for an EDRMS and a case management system. As at July 2019, the specifications for the case management system are being confirmed. The procurement was managed by a separate government entity on IGIS' behalf. The EDRMS meets the Archives' minimum metadata and information management functional requirements. However, the system has not yet been installed, and the specifications for the case management system are still to be configured to ensure that the metadata standards are met and information management function requirements are embedded. As such, IGIS has partially implemented this target.

#### Existing business information systems

4.51 The second target under this recommended action applies to existing business systems and requires that entities' business systems containing high-value and long-term information assets meet minimum metadata standards by 31 December 2017. The Archives have developed a minimum metadata set that identifies nine properties required for the effective management of business information (see paragraph 2.17).

4.52 In April 2016, AGD identified seven existing business systems containing high value and long-term information assets that required assessment to determine if the systems met the minimum metadata standards. From October through to December 2016, AGD completed assessments, identifying that the business systems met the minimum metadata standard and captured sufficient metadata to meet business and information management needs. As such, AGD has fully implemented this target.

4.53 As at June 2019, CASA has identified eight existing high-risk, high-volume business systems and conducted assessments of these. CASA has identified that these systems meet the Archives' minimum metadata standard. Therefore, CASA has fully implemented this target.

4.54 IGIS's business operations utilise email correspondence, Microsoft Word and Microsoft Excel spreadsheets stored on group drives, and an Access database to manage complaints. There is no evidence that metadata assessments have been undertaken of these existing systems, and in accordance with the IGIS' information and records management policy, the output from the processes conducted using these systems is to be printed out and stored on the hard-copy file. As such, IGIS has not implemented this target.

### *All business systems meet functional requirements for information management*

4.55 The second recommended action under Principle 3 requires that all business systems meet functional requirements for information management. The Archives have developed a business systems assessment framework that entities can use to assess information management functionality.<sup>70</sup> The framework recommends that entities develop a systems register to: identify business systems that create, capture, and store information; prioritise those systems that hold high risk, high-value business information; and develop and implement a system information management plan.

4.56 In 2018, AGD revised its approach and ceased using the business system assessment framework developed by the Archives to determine information functional requirements for all business systems. Instead, functional requirements for information management in relation to all business systems are addressed through the systems design process.<sup>71</sup> However, information and records management requirements have not been consistently addressed in documentation submitted to, and reviewed by, the Design Authority. As such, AGD commenced work to adapt the relevant templates to incorporate records and information management requirements in July 2018, and the revised templates were released in October and November 2018. While AGD has developed processes to ensure that functional requirements for information management are evaluated as part of the systems design process, it has also identified that work to implement information management functionality into all business specific systems is not yet complete. Therefore, AGD has been assessed as having:

- fully implemented the target to evaluate the functional requirements for information management; and
- partially implemented the target to implement the functional requirements where necessary.

4.57 CASA has not yet completed an evaluation of all business systems. In 2017, CASA engaged an external contractor to begin undertaking this work as part of an enterprise information architecture review and a business systems assessment register has been developed as part of the first stage of this work. The full program of work is identified in the Enterprise Information Management Strategy, scheduled over a three year period, and due to be completed in 2020. CASA has commenced the work identified in the Enterprise Information Management Strategy and has partially implemented this target.

---

70 The Business Assessment Framework is based on Part 3 of the *ISO 16175 Principles and Functional Requirements for Records in Electronic Office Environments*.

71 The AGD's Design Authority provides oversight and approval of architectural and detailed designs for the delivery, maintenance and support of business systems, including significant variations to previously approved architectural or design solutions. In January 2018, the Design Authority was advised of its obligations to ensure that information management functional requirements are assessed as part of the system design approval process.

## Recommendation no.6

4.58 The Civil Aviation Safety Authority should:

- (a) review and update the Electronic Transactions Policy to include appropriate instruction and guidance around the adoption of digital workflows and authorisation; and
- (b) complete the assessment of existing business systems and processes to ensure that information created, captured, stored, and used to deliver services or inform decision making meets minimum metadata standards and functional requirements for the management, transferral, and disposal of information.

**Civil Aviation Safety Authority response:** *Agreed.*

4.59 *Since the completion of this audit, CASA has made progress in the review and update of its information management policies and procedures including the Electronic Transactions Policy. CASA expects to finalise this work in the first quarter of 2019–20. CASA has also completed the assessment of current ongoing business systems against the National Archives of Australia's Business System Assessment Framework.*

4.60 As discussed at paragraph 4.10, the EDRMS that IGIS is in the process of procuring and installing meets the Archives' minimum metadata and information management functional requirements. However, the system has not yet been installed, and the specifications for the case management system are still to be configured. Corporate systems, such as payroll and human resources are provided by AGD, and AGD is responsible for ensuring that these systems meet functional requirements for information management. As such, IGIS has partially implemented this target. Recommendation no. 7 at paragraph 4.67 addresses the need for IGIS to establish a plan to address this and other elements of the Digital Continuity 2020 policy targets.

## Have the selected entities established effective internal arrangements to monitor and report on progress against the targets of the Digital Continuity 2020 policy?

Two of the three selected entities have established effective arrangements to monitor and report on progress against the targets of the Digital Continuity 2020 policy. AGD has established specific reporting arrangements within existing governance structures to internally monitor progress. CASA has consolidated previously separate reporting arrangements into a single governance committee and associated reporting structure. IGIS does not have formal arrangements in place to internally monitor or report on progress against the policy targets.

### Internal monitoring and reporting

4.61 The Digital Continuity 2020 policy does not include a specific requirement for entities to monitor and report internally on progress towards achieving the policy. However, guidance issued by the Archives sets out that entities are expected to be reporting to their information governance committee or equivalent mechanism (see Appendix 7) on progress to implement whole-of-government information management initiatives (including the Digital Continuity 2020 policy).

### *Attorney-General's Department*

4.62 AGD's Information Management Framework outlines that the effectiveness of the framework will be assessed using: annual reporting as required under the Digital Continuity 2020 policy; and in-progress reports to the department's Information and Communications Technology Committee (ICTC).

4.63 In 2016, AGD expanded the terms of reference for the ICTC to include information governance. The ICTC is to receive reports on the status of activities initiated to implement the targets of the Digital Continuity 2020 policy every two months (February, April, June, August, October and December) or as required, and provide a formal report on activities to the Executive Board at least twice a year.

4.64 A review of the minutes and papers discussed at the ICT Committee meetings found that papers discussing the status of activities implemented to assist AGD in meeting the targets of the policy have been tabled and discussed at six meetings held between February 2016 and March 2019. The papers presented to the ICTC focused on reporting progress against the Digital Continuity 2020 targets and seeking endorsement, or approval of, initiatives to be implemented to meet upcoming targets.

### *Civil Aviation Safety Authority*

4.65 CASA does not have an information governance framework, or a dedicated information governance committee. However, CASA does provide regular information management input into weekly executive manager reports, and provided high-level reports mapping progress against the targets of the Digital Continuity 2020 policy to the Enabling and Capability Group. Updates on progress against the targets of the Digital Continuity 2020 policy were tabled and discussed at two meetings held in December 2017 and January 2018. Where specific business improvement projects have been initiated that will assist CASA to achieve the targets of the policy, program updates were provided to either the Enablement and Capability Group, Service Delivery Transformation Program Board, or the Business Improvement Program Board. In April 2019, the Service Delivery Transformation Program Board and Business Improvement Program Board were consolidated into a single Business Improvement Program and Oversight Board. Reports are now provided to this body on projects implemented to progress the recommended actions and associated targets of the Digital Continuity 2020 policy.

### *Inspector-General of Intelligence and Security*

4.66 IGIS has not established internal monitoring and reporting arrangements for the Digital Continuity 2020 policy. IGIS's governance arrangements are outlined in its corporate plan and are comprised of weekly senior staff meetings, and monthly all staff meetings. The Digital Continuity 2020 policy, and progress against it, are not specifically discussed at these meetings, however projects related to the procurement and installation of an EDRMS and a case management system have been discussed regularly.

## Recommendation no.7

4.67 The Office of the Inspector-General of Intelligence and Security should establish a plan for the implementation of the Digital Continuity 2020 policy, with a particular focus on those targets which were due on or before the end of 2018. The plan should also include clear processes for ongoing monitoring and reporting of progress.

**Office of the Inspector-General of Intelligence and Security response:** *Agreed.*

4.68 *Recommendation no.7 of your report relates to my agency, and the establishment of a plan for the implementation and reporting of Digital Continuity 2020 (DC 2020) targets. I accept that recommendation.*

---



Grant Hehir  
Auditor-General

Canberra ACT  
31 October 2019





## **Appendices**

## Appendix 1 Entity responses



FROM THE OFFICE OF THE DIRECTOR-GENERAL

**Our reference: 2019/2293**

Mr Grant Hehir  
Auditor-General for Australia  
Australian National Audit Office  
GPO Box 707  
CANBERRA ACT 2601

Dear Mr Hehir

Thank you for providing the National Archives of Australia with the opportunity to comment on the proposed audit report on the implementation of the Digital Continuity 2020 policy.

The National Archives agrees in principle with the recommendations made in the proposed report. These, and the findings of the audit more generally, will assist the National Archives to adjust its governance of the Digital Continuity 2020 policy in the lead up to its conclusion at the end of next year. The results of the audit will also inform the development of a successor policy, currently underway, and its implementation from 2021.

However, I question the conclusion of the ANAO that 'the National Archives of Australia ... has been largely ineffective in monitoring, assisting and encouraging entities to meet the targets of the [Digital Continuity 2020] policy'; indeed this statement is contradicted by the evidence produced in the report. Relevant here is the report's finding that the products, advice and guidance material issued by the National Archives are largely fit for purpose, and the report's recognition of the National Archives' stakeholder engagement through the Agency Service Centre, the Government Agencies Information Network, the Archives' website and social media updates.<sup>(a)</sup> Since the introduction of the policy in 2015, the percentage of agencies with an established digital information management capability has increased by almost 30% to over 80%.<sup>(b)</sup>

In an operating environment that requires Commonwealth entities to continuously deliver efficiency dividends; to do more with less; and to implement congestion-busting innovations within the bureaucracy, it is important to maintain a focus on outcomes over process. Of course, it is undeniably the case that without proper oversight and management any endeavour is sure to fail, equally however a disproportionate concentration on the internal mechanisms and activities of governance will divert resources from the front line work that is required to actually achieve the change that is required. The National Archives will therefore act upon all of the report's recommendations, improving our governance frameworks such that our approach to implementation engages with risk, remains agile, embraces innovation and at all times stays outcomes-focussed.

I would like to acknowledge the support of the Attorney General's Department, the Civil Aviation Safety Authority and the Office of the Inspector General of Security. Their participation in this audit

PO Box 4924 Kingston ACT 2604 | Queen Victoria Terrace, Parkes ACT 2600  
t (02) 6212 3600 | e [archives@naa.gov.au](mailto:archives@naa.gov.au) [naa.gov.au](http://naa.gov.au)



has assisted in identifying areas where the National Archives can provide further support to Commonwealth Government agencies in their implementation of the policy.

Yours sincerely



David Fricker  
2 September 2019

**Attachments:**

1. Summary Response
2. Responses to Recommendations
3. Editorial comments



### *ANAO comment on National Archives of Australia response*

(a) The Digital Continuity 2020 policy statement published by the Archives in 2015 established the objective that Australian Government entities will have embedded the principles of the policy by 31 December 2020, and stated that the Archives:

- is responsible for leading the implementation of the policy;
- will collaborate with entities to develop advice, products and tools to support implementation of the policy principles; and
- will undertake performance monitoring to identify and work with entities that need assistance in implementing the policy.

The audit assessed the Archive's performance against this objective, and its discharge of these responsibilities, and found that: the Archives arrangements to administer the Digital Continuity 2020 policy are limited in effectiveness (paragraph 8); that while the products, advice, and tools issued by the Archives to support entities are largely fit for purpose, there are material deficiencies (paragraph 12); that there are material deficiencies in performance monitoring (paragraphs 15 and 16); there are no formal processes to identify and work with entities that need assistance in implementing the policy (paragraph 13); and that Australian Government entities are unlikely to have embedded the principles of the policy by the 31 December 2020 target (paragraph 7).

On this basis, the audit has concluded that the Archives has been largely ineffective in monitoring, assisting and encouraging entities to meet the targets of the policy.

(b) The figure quoted in the above statement is based on the number of agencies that have self-assessed as having a digital maturity level of 3 or above in the Check-Up Digital and Check-up Plus surveys conducted in 2016 and 2018 respectively. As stated at paragraph 3.20, the Archives has itself identified that using this maturity scale to measure success is potentially inaccurate.



**Australian Government**  
**Attorney-General's Department**

Secretary

18/8925

29 August 2019

Mr Grant Hehir  
Auditor-General for Australia  
GPO Box 707  
CANBERRA ACT 2601

Via email: [OfficeoftheAuditorGeneralPerformanceAudit@anao.gov.au](mailto:OfficeoftheAuditorGeneralPerformanceAudit@anao.gov.au)

Dear Mr Hehir 

Thank you for providing the department with the opportunity to comment on the ANAO's proposed report on the Implementation of the Digital Continuity 2020 policy.

I am pleased that the report recognises the significant investment the department has made in meeting the targets of the policy. The department welcomes the report's conclusions and findings and continues to be committed to the effective and efficient implementation of the policy, where practical to do so.

I would like to thank your staff for their professional and collegiate conduct during the course of the audit.

Yours sincerely

  
Chris Moraitis



**Australian Government**  
**Civil Aviation Safety Authority**

CASA Ref: D19/323581

**Response to the ANAO S19 Report – Implementation of Digital Continuity 2020 Policy**

Mr Grant Hehir  
Auditor-General  
Australian National Audit Office  
GPO Box 707  
CANBERRA ACT 2601

Dear Mr Hehir

Thank you for providing the Civil Aviation and Safety Authority (CASA) with the opportunity to respond to the ANAO's proposed report under section 19 of the *Auditor-General Act 1997* on *Implementation of the Digital Continuity 2020 policy*.

CASA welcomes the recommendation related to CASA (recommendation six) and agrees with its finding without qualification.

As the audit report notes, CASA has made steady progress in delivering the Digital Continuity 2020 targets and continues to do so.

Since the completion of this audit, CASA has made progress in the review and update of its information management policies and procedures including the Electronic Transactions Policy – recommendation 6.a. CASA expects to finalise this work in the first quarter of 2019-20. CASA has also completed the assessment of current ongoing business systems against the National Archives of Australia's Business System Assessment Framework - recommendation 6.b.

I would like to thank you for the opportunity for CASA's participation in this audit and the audit team for the professional and collaborative way the audit was conducted.

Yours sincerely

A handwritten signature in blue ink, appearing to read 'A Mathews'.

Anthony Mathews  
Chairman  
Civil Aviation Safety Board

Attachment A – Correction of immaterial factual error notice.

GPO Box 2005 Canberra ACT 2601

Telephone: (02) 6217 1001

Facsimile: (02) 6217 1555



File ref: 2019/003  
Correspondence ref: OIGIS/OUT/2019/823

Mr Grant Hehir  
Auditor-General for Australia  
C/O: Electronic mail

Dear Mr Hehir

**Letter of Reply – Implementation of the Digital Continuity 2020 Policy**

Thank you for your correspondence on 05 August 2019 which contained the *Proposed Report for the ANAO Performance Audit – Implementation of the Digital Continuity 2020 policy*. I have reviewed the report and provide the following comments and attachments.

Recommendation no. 7 of your report relates to my agency, and the establishment of a plan for the implementation and reporting of Digital Continuity 2020 (DC 2020) targets. I accept that recommendation.

In 2018, this agency received an appropriation of both capital and operating funds to implement recommendations from the 2017 Independent Intelligence Review, meaning that for the first time, this Office now has some resources to dedicate to the implementation of DC2020 targets. I note that due to the security requirements of this office, there are some elements of the DC2020 policy which will not be able to be implemented (examples of which were provided during the audit process).

The contact in my office for this matter is the Deputy Inspector-General, Mr Jake Blight, who can be contacted by telephone on 02 6141 3330 or email: [jake.blight@igis.gov.au](mailto:jake.blight@igis.gov.au).

Yours sincerely

Margaret Stone AO, FAAL  
Inspector-General

2 September 2019

Attachments:

1. Summary Response
2. Editorial Matters

## Appendix 2 Digital Continuity 2020 targets and pathways

**Table A.1: Digital Continuity 2020 Agency Implementation targets and pathways**

Principle 1 — Information is valued	Principle 2 — Information is managed digitally	Principle 3 — Information, systems and processes are interoperable
<b>31 December 2020</b> <ul style="list-style-type: none"> <li>Agencies manage their information assets for as long as they are required.</li> <li>Agencies meet targets for professionally qualified or accredited information managers.</li> </ul>	<b>31 December 2020</b> <ul style="list-style-type: none"> <li>Agency business interactions, decisions and authorisations are recorded digitally.</li> <li>Information in analogue format is migrated to digital format, where there is value for business.</li> </ul>	<b>31 December 2020</b> <ul style="list-style-type: none"> <li>Information is managed based on format and metadata standards for information governance and interoperability.</li> <li>All business systems meet functional requirements for information management.</li> <li>Cross-agency and whole-of-government processes incorporate information governance requirements.</li> </ul>
<b>30 September 2020</b> <ul style="list-style-type: none"> <li>Annual agency survey reporting.</li> </ul>		
<b>31 December 2019</b> <ul style="list-style-type: none"> <li>Chief information governance officers or senior officers responsible for information governance individually join a professional association to support their continuing professional development.</li> </ul>	<b>31 December 2019</b> <ul style="list-style-type: none"> <li>Agencies implement strategies for the management of all information assets to support digital continuity.</li> </ul>	<b>31 December 2018</b> <ul style="list-style-type: none"> <li>All business systems are evaluated against the Archives' business systems assessment framework to meet functional requirements for information management.</li> <li>Functional requirements are implemented where necessary.</li> </ul>
<b>30 September 2019</b> <ul style="list-style-type: none"> <li>Annual agency survey reporting.</li> </ul>		
	<b>30 June 2019</b> <ul style="list-style-type: none"> <li>Agencies identify remaining analogue approval processes and evaluate against the Archives' digital authorisations framework to implement fully digital authorisations and workflow processes.</li> </ul>	



Principle 1 — Information is valued	Principle 2 — Information is managed digitally	Principle 3 — Information, systems and processes are interoperable
<b>31 December 2018</b> <ul style="list-style-type: none"> <li>Agencies establish and implement a program of continuing professional development of information management staff for professional recognition.</li> </ul>	<b>31 December 2018</b> <ul style="list-style-type: none"> <li>Agencies identify all information assets, evaluate risk and management requirements, and identify strategies to support digital continuity.</li> </ul>	<b>31 December 2018</b> <ul style="list-style-type: none"> <li>All business systems are evaluated against the Archives' business systems assessment framework to meet functional requirements for information management.</li> <li>Functional requirements are implemented where necessary.</li> </ul>
<b>30 September 2018</b> <ul style="list-style-type: none"> <li>Annual agency survey reporting.</li> </ul>		
<b>31 December 2017</b> <ul style="list-style-type: none"> <li>Agencies have a chief information governance officer.</li> </ul>	<b>31 December 2017</b> <ul style="list-style-type: none"> <li>Agencies transform most paper-based business processes to digital, and routinely make and record decisions using digital authorisations and workflows.</li> </ul>	<b>31 December 2017</b> <ul style="list-style-type: none"> <li>All business systems containing high-value and long-term information assets meet minimum metadata standards.</li> </ul>
<b>31 August 2017</b> <ul style="list-style-type: none"> <li>Annual agency survey reporting.</li> </ul>		
<b>31 December 2016</b> <ul style="list-style-type: none"> <li>Agencies have established an information governance committee.</li> </ul>	<b>31 December 2016</b> <ul style="list-style-type: none"> <li>Agencies identify high-value and long-term information assets, evaluate risk and management requirements, and implement strategies to support digital continuity.</li> </ul>	<b>31 December 2016</b> <ul style="list-style-type: none"> <li>All business systems procured after this date will meet minimum metadata standards, and will be evaluated against the Archives' business systems assessment framework to meet functional requirements for information management.</li> </ul>
<b>30 September 2016</b> <ul style="list-style-type: none"> <li>Annual agency survey reporting.</li> </ul>		
<b>30 June 2016</b> <ul style="list-style-type: none"> <li>Agencies have established an information governance committee.</li> </ul>		
	<b>1 January 2016</b> <ul style="list-style-type: none"> <li>All records created in digital formats after this date are managed digitally.</li> </ul>	

Principle 1 — Information is valued	Principle 2 — Information is managed digitally	Principle 3 — Information, systems and processes are interoperable
<b>31 December 2015</b> <ul style="list-style-type: none"> <li>Agency senior management drives change to digital information and records management. Survey reports to the Archives are authorised by agency heads.</li> </ul>	<b>31 December 2015</b> <ul style="list-style-type: none"> <li>Agencies have reduced reliance on paper and duplication of information in digital and physical formats. Agencies have identified paper-based business processes.</li> </ul>	

Source: National Archives of Australia, 'Agency implementation targets and pathways,' available from <http://www.naa.gov.au/information-management/digital-transition-and-digital-continuity/agency-implementation-targets-pathways/index.aspx> [accessed 10 April 2019].

## Appendix 3 The information management legislative, regulatory, and policy environment

1. The legislative, regulatory, and policy environment that applies to information management spans multiple portfolio bodies, and independent bodies, is characterised by high levels of interdependency, and is comprised of:

- legislation, legislative instruments and standing orders<sup>72</sup>;
- whole-of-government policies and strategies<sup>73</sup>;
- records and information management standards and authorities<sup>74</sup>; and
- subject matter guidance and advice.<sup>75</sup>

2. The lead agencies responsible for overseeing compliance with the key pieces of legislation that detail how Australian Government agencies are to handle, protect, and manage information are listed below at Table A.2.

**Table A.2: Lead agency and associated legislation that relates to information management**

Lead agency	Legislation	Description
National Archives of Australia	<i>Archives Act 1983</i>	The Act authorises the National Archives to: <ul style="list-style-type: none"> <li>a) identify the archival resources of the Commonwealth;</li> <li>b) preserve and make publicly available the archival resources of the Commonwealth;</li> <li>c) oversee Commonwealth record-keeping by determining standards and providing advice to Commonwealth institutions; and</li> <li>d) impose record-keeping obligations in respect of Commonwealth records.</li> </ul>
Attorney-General's Department	<i>Crimes Act 1914</i>	The Act contains provisions relating to the protection of official information and sets out penalties for unauthorised disclosure.

72 Legislation, legislative instruments, and standing orders are mandatory and all Commonwealth entities must comply with the provisions of the Act, Instrument, or Order. Examples include: the *Crimes Act 1914*; the *Freedom of Information Act 1982*; the *Archives Act 1983*; the *Privacy Act 1988*; the *Electronic Transactions Act 1999*; the *Australian Public Service Act 1999*; and the *Public Governance, Performance and Accountability Act 2013*.

73 Whole of Government policies and strategies apply to all Commonwealth entities and identify actions that entities must, should, could, or may wish to implement. Examples of whole-of-government strategies include the Digital Transformation Strategy and Australia's Cyber Security Strategy. Whole of Government policies include the Digital Continuity 2020 policy; the Protective Security Policy Framework, and the Digital Service Standard.

74 Examples of records and information management standards and authorities include the Australian Government Records Interoperability Framework; Information Management Standard 2017; *ISO 15489 – Records Management*, *ISO 16175 - Principles and Functional Requirements for Records in Electronic Office Environments*; and the Australian Government Recordkeeping Metadata Standard.

75 Examples of subject matter guidance and advice include: implementing machinery of government changes; information security; guides to securing personal information; digitising accumulated physical records; preserving physical records; and outsourcing digital data storage.

Lead agency	Legislation	Description
	<i>Freedom of Information Act 1982</i>	This Act gives the Australian community access to information held by the Government by: <ul style="list-style-type: none"> <li>a) requiring agencies to publish the information;</li> <li>b) providing for a right of access to documents;</li> <li>c) increasing public participation in Government processes, to promote informed decision making;</li> <li>d) increasing scrutiny, discussion, comment and review of the Government's activities; and</li> <li>e) increasing recognition that information held by the Government is to be managed for public purposes and is a national resource.</li> </ul>
	<i>Privacy Act 1988</i>	The Act sets out the Australian Privacy Principles that detail how personal information is to be handled and establishes the Office of the Australian Information Commissioner.
	<i>Electronic Transactions Act 1999</i>	The Act provides a regulatory framework that: <ul style="list-style-type: none"> <li>a) recognises the importance of the information economy to the future economic and social prosperity of Australia;</li> <li>b) facilitates the use of electronic transactions;</li> <li>c) promotes business and community confidence in the use of electronic transactions; and</li> <li>d) enables business and the community to use electronic communications in their dealings with government.</li> </ul>
Australian Public Service Commission	<i>Public Service Act 1999</i>	This Act sets out the Australian Public Service Values and Code of Conduct. The Act also contains a number of sections which directly and indirectly relate to information and records management.
Department of Finance	<i>Public Governance, Performance and Accountability Act 2013</i>	This Act establishes the governance, performance and accountability requirements that apply to Commonwealth entities by: <ul style="list-style-type: none"> <li>a) setting out the duties of accountable authorities and officials of a Commonwealth entity in relation to the use of public resources, including information;</li> <li>b) specifying that the accountable authority of a non-corporate Commonwealth entity must govern the entity in a way that is not inconsistent with the policies of the Australian Government;</li> <li>c) requiring that the accountable authority of a Commonwealth entity must cause records to be kept that properly record and explain the entity's performance in achieving its purposes.</li> </ul>

Source: ANAO analysis of legislation that guides the handling and management of information by Australian Government entities. Information available from <http://www.naa.gov.au/information-management/information-governance/legislation-standards/index.aspx> [accessed 10 April 2019].

3. The supporting standards, whole-of-government policies, and strategies that Australian Government entities are to implement (including the Digital Continuity 2020 policy) to meet legislative and regulatory requirements are detailed at Table A.3 below.<sup>76</sup>

**Table A.3: Supporting standards and whole-of-government policies that apply to information management**

Standard/policy <sup>a</sup>	Legislative Authority	Lead agency	Date	Description
Digital Continuity 2020 policy	Archives Act 1983	National Archives of Australia	2015	The Digital Continuity 2020 policy identifies three principles that Australian Government entities are to meet. It is a Government endorsed policy and identifies 10 recommended actions that Australian Government entities are to implement. The purpose of the policy is to encourage Australian Government entities to complete the transition to fully digital information management and work processes.
Digital Service Standard	<i>Public Governance, Performance and Accountability Rule 2014</i>	Digital Transformation Agency	2016	The Digital Service Standard is a set of best-practice principles for designing and delivering government services. The Digital Service Standard applies to Australian Government Services that are public facing and owned by non-corporate Commonwealth entities that distribute information and/or provide transactional services. Where the result of a transaction is used to inform decision making it is to be included as part of the relevant record and maintained in accordance with the <i>Archives Act 1983</i> .
Information Management Standard	<i>Archives Act 1983</i>	National Archives of Australia	2017	The Information Management Standard identifies eight principles that Australian Government entities are to meet. The standard does not prescribe how entities should meet the principles, identifying that the principles should be implemented using a risk and value based approach. The purpose of the standard is to assist entities create and manage information, regardless of format. The standard is also intended to support entities to implement the targets of the Digital Continuity 2020 policy.

<sup>76</sup> The list of legislation, policies, strategies and advice available on the Archives' website is not exhaustive and does not include sources relevant to entities responsible for unique regulatory or business functions: <http://www.naa.gov.au/information-management/information-governance/legislation-standards/index.aspx> [accessed 10 May 2019].

Standard/policy <sup>a</sup>	Legislative Authority	Lead agency	Date	Description
Protective Security Policy Framework	<i>Directive on the Security of Government business issued by the Attorney-General</i>	The Attorney-General's Department	2018	The Protective Security Policy Framework applies to people, information and assets. All Australian Government entities are required to apply the policy as it relates to their risk environment. Core requirements identified in the policy framework that relate to information security apply to: sensitive and classified information; access to information; safeguarding information from cyber threats; and robust ICT systems. The policy framework identifies the National Archives of Australia as a key lead protective security entity responsible for Commonwealth records, information standards and advice.

Note a: The Archives has categorised whole-of-government strategies and policies as required practice. Required practices are practices that entities must be aware of, and implement to the level required as defined in the relevant strategy or policy.

Source: Analysis of the, 'Legislation, policies, standards and advice,' available the National Archives of Australia website: <http://www.naa.gov.au/information-management/information-governance/legislation-standards/index.aspx> [accessed 10 April 2019].

## Appendix 4 Criteria used to select entities

1. An overview of the entities, and the criteria used to select them for audit coverage, is provided in Table A.4.

**Table A.4: Selection of entities**

Entity	Strategic Priorities	Criteria used for entity selection		
		Size (staff)	Function	Self-assessed digital maturity level <sup>a</sup>
Attorney-General's Department	Support the Attorney-General as First Law Officer, including by providing high quality legal services to the Commonwealth.  Promote public sector integrity and strong oversight of Commonwealth intelligence and law enforcement agencies.  Delivering national security and criminal justice legislation.  Maintaining the civil and criminal Commonwealth justice system.	Large (>1001)	Policy and program administration	High
Civil Aviation Safety Authority	Maintain and enhance a fair, effective and efficient aviation safety regulation system.  Engage collaboratively with the wider aviation community to promote and support a positive safety culture.	Medium (251–1000)	Regulatory	Developing
Office of the Inspector-General of Intelligence and Security	Assist Ministers in overseeing and reviewing the activities of the intelligence agencies for legality and propriety and for consistency with human rights, through conducting inspections, inquiries and investigations into complaints. <sup>b</sup>  Assist the Government in assuring the Parliament and the public that intelligence and security matters relating to Commonwealth agencies are open to scrutiny.	Small (11–100)	Specialist	Initial

Note a: The entity's self-assessed digital maturity level has been based on their responses to the 2016 Check-up Digital survey.

Note b: When conducting inspections, inquiries and investigations into complaints, IGIS collects classified and sensitive data from the agencies involved. In accordance with the protective security policy framework classified and sensitive data is to be handled and accessed in a manner that complies with the originating entities instructions and requirements.

Source: Analysis of 2016 Check-up Digital responses.

## Appendix 5 Criteria used to assess the appropriateness of performance information

**Table A.5: Criteria to assess the appropriateness of performance information**

Finance guidance	Assessment characteristics		Explanation
<b>Relevant</b>	<b>Individual assessment</b>	Benefit <i>The performance criterion clearly indicates who will benefit and how they will benefit from the entity's activities.</i>	The performance criterion should explain who will benefit from the activity and how the recipient benefitted.
		Focus <i>The performance criterion should address a significant aspect/s of the purpose, via the activities.</i>	The performance criterion should assist significantly in informing whether the purpose is being achieved, and the attribution of the entity's activities to it is clear.
		Understandable <i>The performance criterion should provide sufficient information in a clear and concise manner.</i>	The performance criterion should be stated in plain English and signal the impacts of activities to inform users.
<b>Reliable</b>	<b>Individual assessment</b>	Measurable <i>The performance criterion should use and disclose information sources and methodologies that are fit for purpose.</i>	The performance criterion should be capable of being measured to demonstrate the progress of fulfilling the purpose. This includes documenting a basis or baseline for measurement or assessment, for example a target or benchmark.
		Free from Bias <i>The performance criterion should be free from bias and where possible, benchmarked against similar activities.</i>	The performance criterion should allow for clear interpretation of results and provide an objective basis for assessment.
<b>Complete / adequate</b>	<b>Overall assessment</b>	Balanced <i>The performance criteria should provide a balanced examination of the overall performance story.</i>	The performance criteria should reflect a balance of measurement types (effectiveness and efficiency), bases (quantitative and qualitative) and timeframes (short, medium and long-term).
		Collective <i>The performance criteria should collectively address the purpose.</i>	The performance criteria should demonstrate the extent of achievement against the purpose through the activities identified in the corporate plan.



## Appendix 6 The average digital maturity assessments of the selected entities for 2018

**Table A.6 Selected entities average digital maturity assessments for 2018**

Recommended action	Check-up Plus question	AGD	CASA	IGIS
Principle 1 average		4.2	3.1	3.9
1. Information governance reporting	<i>Not assessed as part of Check-up Plus</i>	All 3 years	All 3 years	All 3 years
2. Agencies have established an Information Governance Committee	14. Does your agency have a formal governance mechanism with broad representation ensuring information management requirements are considered when making decisions?	Yes (5)	Yes, for ICT (3)	Partial (2)
3. Agencies have an information governance framework	13a. Information governance is implemented holistically to ensure complete and consistent management of all information assets regardless of format, location, type or value.	4	3	5
4. Agencies manage their information assets for as long as they are required	24c. Implement preservation strategies, procedures and activities to ensure information can be accessed, used and understood for as long as it is required.	3	3	1
	25a. Establish governance across all business systems for the identification, destruction or transfer of agency information assets.	3	2	5
5. Agencies meet targets for skilled staff	13b. Information management roles and responsibilities are established and articulated throughout the agency.	4	2	5
	13e. Everyone has access to appropriate training to develop contemporary information management skills relevant to their role, ensuring they have the capability to manage information and data for as long as it is required.	4	2	4
Principle 2 average		3	2.5	1.5
6. Agencies work digitally, with business interactions, decisions and authorisations recorded digitally	18f. Use appropriate technologies to automate processes e.g. digital signatures and automated workflows).	3	2	1
7. Information in analogue formats is migrated to digital format, where there is value for business	18c. Continually identify and remove paper from internal and external processes to improve efficiency.	3	3	2
Principle 3 average		3	2.25	2
8. Information is managed based on format and metadata	21b. Adopt relevant metadata standards at the appropriate level (e.g. enterprise, domain, government, international).	3	4	3

Recommended action	Check-up Plus question	AGD	CASA	IGIS
standards for information governance and interoperability	22e. Collect descriptive information (metadata) in line with the Information Management Standard.	3	1	3
9. All business systems meet functional requirements for information management	18b. Ensure new or updated business systems are services have the capacity to manage information in place for its whole life.	3	2	1
10. Cross-agency and whole of government processes incorporate information governance requirements and specifications	<i>Not assessed by the Archives</i>			

Source: Check-up PLUS Survey 2018.

## Appendix 7 Internal monitoring and reporting guidance for information management

**Table A.7: Archives' guidance — internal monitoring and reporting**

Digital Continuity 2020 target	Archives' guidance
Information Governance Framework	<ul style="list-style-type: none"> <li>• The framework should detail the entity's approach to information governance compliance and reporting requirements.</li> <li>• This may include the annual reporting requirement to the Archives.</li> <li>• This framework may also include compliance with or reporting on requirements set out internally by the information governance committee.</li> </ul>
Information Governance Committee	<ul style="list-style-type: none"> <li>• The committee will be more effective if it has a direct reporting line to the head of the entity.</li> <li>• The committee should coordinate information governance reporting both internally and externally.</li> <li>• The committee should prioritise and coordinate information management initiatives. For example, address whole-of-government information management initiatives such as Digital Continuity 2020 or the Information Publication Scheme.</li> </ul>
Chief Information Governance Officer	<ul style="list-style-type: none"> <li>• The Chief Information Governance Officer is a dedicated senior executive accountable for enterprise wide information governance.</li> <li>• Responsibilities include: executive advice and reporting; best practice information management; and engagement with whole-of-government information governance initiatives.</li> </ul>

Source: The National Archives of Australia website: <http://www.naa.gov.au/information-management/information-governance/> [accessed 10 April 2019].