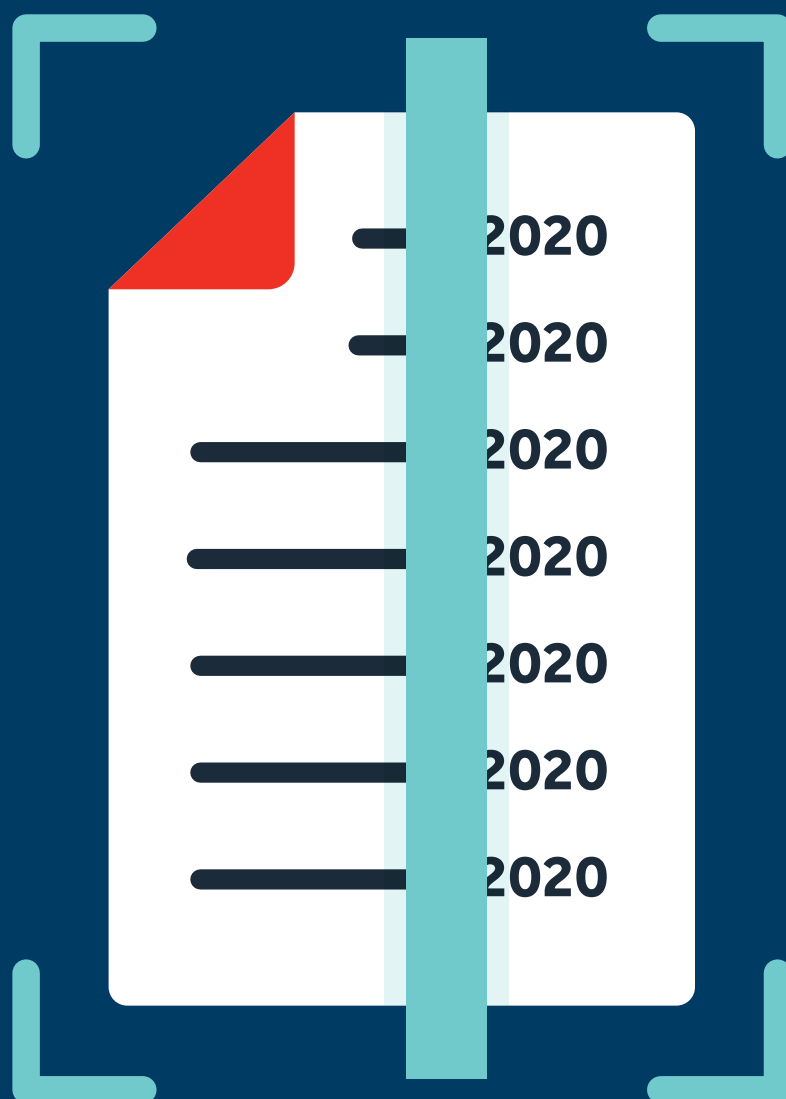


The Challenge of Change

Digitisation, privacy and connection
– 2020 and beyond



grace:

Always more.

We always offer you more.

As the 2020 digitisation deadline approaches, Australian government agencies face a range of new information management challenges. Agencies relying heavily on paper records must convert vast amounts of data into digital formats and arrange sentencing for years of paper archives.

Staff must be retrained to use new systems and interact with information resources in new formats. Datasets that were previously the domain of a single agency may need to be aggregated with other information assets towards the goal of inter-agency sharing or “interoperability”.

Exponentially increasing data volumes are also a growing concern for many agencies, especially those second-tier organs that accumulate the information assets of many other agencies. Not only is the risk of important material being mishandled steadily increasing, but the physical and temporal limitations of paper-based records have the potential to hamper productivity.

Fortunately, private sector solutions are emerging with the goal of helping government agencies optimise information management

in line with current data security guidelines (such as the Protective Security Policy Framework) and future digitisation milestones. This report will address the key areas of weakness presented by current information management practices in government and evaluate the solutions.



: Digitising and Optimising

The Digital Continuity 2020 Policy is a primary driver of the Australian Government's digitisation goals – and potentially the biggest information management challenge the public sector has ever faced. It is structured on three principles: 1) information is valued, 2) information is managed digitally, and 3) information, systems and processes are interoperable.¹

For most agencies, larger ones in particular, the second and third principles pose the greatest hurdles. With the agency set up to oversee the digitisation process – the Digital Transformation Agency (DTA) – less effective than had been hoped, agencies have been largely left to their own devices when it comes to digitisation². While they remain tasked with realising the second principle by 2020, they lack a clear directive on how to achieve it.

"There's uncertainty in some agencies about how to digitise," said Scott McMenemy, a government ICT support technician based in Canberra. "They're keen to do it, they just need someone to come in and guide them through the solution."

An Administrative Appeals Tribunal employee who spoke to us on condition of anonymity was frank: "We'd like to get these things in place, but with minimal support it's just not that easy."

The third principle (interoperability) refers to creating information, systems and processes that are common to multiple government agencies. "[This] takes time," the Digital Continuity 2020 Policy explains, "and requires interoperability to be planned, designed and

integrated from the initial stages... there is still much to be done."³ Being largely contingent upon the second principle, this planning, design and integration of inter-agency assets can only occur to the extent that the initial digital transformation succeeds.

The other major obstacles to complete digitisation by 2020 are the twin issues of operating budget limitations and staffing caps. Caps can mean that agencies are unable to dedicate personnel to establish new initiatives or training programmes, or to engage in other non-official functions. While smaller agencies find it easier than large ones to change their processes, they are more often restricted by cost. Efficiency dividends can add to this difficulty. Despite being designed to help government departments make better use of existing resources, they can make budgets unpredictable and inflexible, limiting the ability of agencies to commit meaningful resources to cross-agency cooperation.

**The Digital Continuity
2020 Policy is the
biggest information
management challenge
the public sector has
ever faced.**

1. National Archives of Australia, *Digital Continuity 2020 Policy – October 2015*, p. 4

2. "Turnbull's ex-tech guy Paul Shetler slams 'predictable' government IT disasters" in *Australian Financial Review* on 3/2/2017 [www.afr.com/technology/enterprise-it/turnbulls-extech-guy-paul-shetler-slams-predictable-government-it-disasters-20170203]

3. National Archives of Australia, *Digital Continuity 2020 Policy – October 2015*, p. 6

• Security and Privacy

Information security and privacy is another significant challenge in government information management. The OAIC Community Attitudes to Privacy Survey Research Report 2013 found that public confidence in the ability of government to handle personal information had fallen since 2007 – with financial institutions now viewed as more trustworthy than government agencies.⁴ This is certainly understandable in light of the high-profile political data breaches that have been making headlines with increasing frequency since the 2010 Wikileaks scandal. It puts pressure on government agencies to not only tighten up any security loopholes but, perhaps more importantly, to prove to the public that sensitive information is being managed properly.

This starts with the Protective Security Policy Framework (PSPF) – a multi-tiered collection of guidelines covering the management of personnel, information and physical security across the whole of government. The part of this framework that deals with electronic information security is in turn based on the Australian Signals Directorate's Information Security Manual (ISM), a sizeable document that outlines a risk-based approach to information and ICT system security.

Public confidence has fallen since 2007 – with financial institutions now viewed as more trustworthy than government agencies.



⁴ Office of the Australian Information Commissioner, Community Attitudes to Privacy Survey, Research Report 2013.

Despite having access to these resources, many agencies can find it difficult to know whether an information management initiative meets the detailed stipulations of the guidelines. Contractors dealing with the inter-agency transfer of physical information alone need to be vetted by the Security Construction and Equipment Committee (SCEC) in accordance with a range of requirements that can be difficult to assess:

- Operated as a commercial courier service for a minimum of two consecutive years and meet the majority of the SCEC Endorsement Criteria - Safe Hand Courier Services A11995602 requirements.
- Agree to initial and ongoing examination of its services to ensure compliance with criteria requirements.
- Agree to initial and ongoing assessment of foreign ownership.
- Nominated couriers agree to be subject to initial and ongoing personal background checks; prejudicial results will exclude an individual from undertaking the safe hand courier duties.

- Company is ISO 9001 Quality Management Systems certified by a third party registrar.
- A facility that holds a Transported Asset Protection Association Freight Security Requirement certification.⁵

Many agencies prefer to stay with something familiar rather than step into territory that can seem complicated and time-consuming.

For those still dealing with physical archives, there are two major security issues. In-house archives rely on agencies themselves to maintain a level of security on premises that is costly and would otherwise be unjustified. Off-site archives, while more secure, can expose information to compromise during transit, especially over long distances where multiple handovers are involved. Very few information management firms have a secure chain of custody across all their delivery locations. Instead, when they have to deliver outside certain geographical boundaries or times of day, they outsource to contractors.

⁵. <https://www.scec.gov.au/scec-couriers>



Many agencies prefer to stay with something familiar rather than step into territory that can seem complicated and time-consuming.

This adds one or more unnecessary steps to the information transmission process. While it may only increase the risk of breach by a slight margin, it elevates the risk of data loss significantly. "Complexity is fertile territory for error," says researcher Matthew C. Holtman.⁶ When the human element in a system increases, so does the possibility that something will go wrong.

Maintaining compliance by ensuring documents are destroyed at the right time is another area that agencies can struggle with. Many are aware of where their document retention obligations end, but can be unwilling to commit to sentencing schedules. There are a number of reasons for this, the most common being uncertainty over what their archives contain – especially if those archives date back to the pre-digital era. From a liability perspective, the relatively small cost of ongoing storage is more than justified by the possibility that an arbitrary sentencing mechanism might accidentally destroy mission-critical documents. Why not audit the documents? The time-and money-consuming task of going through the archives would require a financial investment equivalent to the cost of decades of static storage.

This means that agencies can end up hanging onto many times the amount of data that retention regulations demand, potentially complicating search and retrieval processes, and creating issues of compliance with the *Privacy Act*.

For smaller agencies, security and privacy concerns are limited by more modest information volumes and a greater ability to keep records in-house. For larger government departments, the risk is greater. With the confidential information of thousands of individuals in their possession, large-scale mismanagement can have an ongoing negative effect on public confidence.



Maintaining compliance by ensuring documents are destroyed at the right time is another area that agencies can struggle with.

⁶ Holtman, M. C., "Paradoxes of professionalism and error in complex systems", in *Journal of Biomedical Informatics*, Volume 44, Issue 3, June 2011, pp. 395–401

• Speed and Sharing

The third major obstacle to government information workflows is speed of access. This can be broken into two categories: the efficiency of intra-agency personnel and systems, and the efficiency of inter-agency information transfer.

In a study published by the IDC in 2012, Melissa Webster exposed the amount of time information workers were spending just on document-related challenges: more than 11 hours per week – with 2.3 hours being spent looking for things that were never found.⁷

Information processing practices have progressed rapidly since then, revolutionising the way agencies operate, so we might expect efficiency of access to have increased accordingly. Not so, say the information management experts. Staff are still spending up to 30% of their day chasing down physical copies of documents. Delays that were once the result of a lack of automation are now caused by a dearth of information that is indexed poorly, or not at all.

One cause of this is the inflexibility and inaccessibility of physical records. While the government is seeking to address this through the Digital Continuity 2020 Policy, the reality is that agencies will be reliant on paper for many years to come and still need processes capable of managing this. “The computer system is fast. Everything is right there,” the Administrative Affairs Tribunal employee told us. “But paper files get lost – especially when we have to move offices. Then everything just stops [until they’re found].” The opportunity cost of unnecessary legwork is a burden on government as a whole. But more significantly, it has a major impact on agency response times – and therefore the experience of the public.

“Paper files get lost – especially when we have to move offices. Then everything just stops [until they’re found].”

Information asset sharing issues present another unique challenge. With the volume of information passing between agencies unparalleled by other business sectors, inefficiencies in one agency can have a profound knock-on effect. For physical documentation there is the relatively simple issue of transit times, which results in the accessibility issues that the Digital Continuity 2020 Policy seeks to address. More significantly, however, are the sharing issues related to electronic information. With cooperating agencies using different systems that generate a variety of file types, shared information assets must often be converted for compatibility before or after they are transmitted. Directly commenting on this issue, the IDC study notes: “[Challenges related to collaboration add] up to seven hours of wasted time each week (or 14.2% of the workweek) at an annual cost of [AU\$10,629] per information worker.”⁸

Even if the cost isn’t an issue, across the whole of government these delays can have a detrimental effect on agencies’ ability to meet their KPIs, and can ultimately hamper the ability of government to deliver services to the public.

7. Webster, M., (September 2012) *Bridging the Information Worker Productivity Gap: New Challenges and Opportunities for IT*, <http://www.idc.com>

8. Ibid

The Solution: Simpler, Safer and Smoother Information Management

To tackle the challenges presented by digitisation goals, security requirements and efficiency demands, government agencies are increasingly turning towards external information management solutions. Although the third-party solutions currently used by agencies are not interconnected, their adoption is an important step towards satisfying the goals of the Digital Continuity 2020 Policy and the requirements of the PSPF.

In terms of their ability to help agencies digitise, experienced information management firms can rapidly convert many years of paper archives into a variety of digital formats, making these files available electronically within intuitive systems that can be precisely customised to agency needs.

Information management companies already have the expertise and infrastructure in place to help government agencies achieve full digitisation by the end of 2020.

The best solution providers will also store and transport data according to the strictest government standards – fully satisfying all PSPF requirements. Their physical storage facilities are secured with advanced fire-protection and surveillance systems, with all employees undergoing a Police Criminal Security check before being allowed to handle client information. The same vetted staff also operate a secure fleet of vehicles and ensure that document chain of custody is unbroken by anyone outside the company, such as a generic courier or other third-party contractor. Their digital offering will provide an administrative console with airtight security configurations, function-level verification on transactions, and application-level security that limits users to accessing only the functionality and data they need.

In addition, these companies are conscious of the evolving legislative environment and can keep track of stored information over time, setting up retention and sentencing schedules that ensure destruction occurs when documents reach the end of their lifespan. They can also assist with proof of compliance by providing certificates of destruction.

Finally, the secure in-house fleet and workforce model helps good information-management companies deliver solutions faster, and with greater frequency. They are similarly speed-conscious when it comes to making their systems easy for clients to access and utilise, automating much of the document retrieval and management process. Interfaces are intuitive and responsive, with indexing that integrates seamlessly with that of their clients. A smart solution not only makes searching faster, but delivers information in a way that eliminates long wait times and the need for document reformatting.

Benefits

A good information management solution directly addresses the major record-keeping challenges of government as well as providing additional benefits for digitisation, security and efficiency.

• Simpler Digitisation

For most government agencies scrambling to meet the 2020 digitisation deadline, engaging a competent information management provider will ensure they reach their goals well ahead of schedule. Where agencies may have struggled to allocate sufficient staff due to staffing caps, a third-party solution removes that obstacle.

An important point to note is that rather than affecting operating budgets, the cost of contracted digitisation can be absorbed by much larger capital budgets. It also allows additional services to be requested at the same time, such as a full audit of existing paper files.

The tailored access systems provided by the best information management companies have the added advantage of integrating with existing systems and indexing conventions to dramatically reduce the cost and time of retraining staff.

• Safer Handling

A government agency that can assure people that their information is safe is one that will stand out for all the right reasons to the privacy-conscious public.

Accredited information management companies are a boon for agencies because they don't need to go through the lengthy vetting process. PSPF-compliant firms are able to take custody of information assets immediately.

With information stored off-site, much of the pressure is taken off agencies that are currently maintaining a high level of physical and cyber security in their office premises. Access to archives can then be controlled entirely through administrative systems to reduce the burden on existing departmental separation practices or clean-desk policies.

Having an information management partner paying close attention to sentencing schedules means that documents are less likely to occupy costly shelf space, allowing for a dramatic reduction in information storage overheads. Healthy sentencing schedules also help ensure all of an agency's records comply with the Privacy Act and other relevant legislation without significantly driving up costs.



PSPF-compliant firms are able to take custody of information assets immediately.

: Smoother Sharing

Perhaps the most attractive benefit to government agencies is the increased efficiency that comes from better information management. There may still be a wait time for physical documents, but the time is almost entirely taken up by the transit process, and no longer by staff searching in vain for files that may not even exist. With document retrieval outsourced, staff can get on with more productive tasks.

In terms of requesting information, a more streamlined and intuitive electronic document access system naturally increases retrieval speeds. Off-site electronic information storage doesn't necessarily need to offer a higher transfer rate to be faster either – just the knowledge that all data has been consolidated inside a single system can greatly improve staff efficiency.

Information asset sharing can be improved when two or more agencies use the same information management company. Not only does this help agencies draw more easily from the same data sets, but allows them to use common file formats, reducing the need for time-consuming conversions. Smaller agencies without the budget to engage an information management company can also piggy-back on a contract held by a larger agency. Both agencies then enjoy reduced costs at the same time as their shared information management solution helps them fulfill the interoperability requirements of the Digital Continuity 2020 Policy.



Smaller agencies without the budget to engage an information management company can also piggy-back on a contract held by a larger agency.

The 6 Principles How To Choose An Information Management Partner For Your Agency

1. Information is recognised as a valuable asset

Information assets are a crucial part of government decision-making and service delivery. To maximise the value of these assets, staff need to be able to exploit them to the fullest. This starts with good information management. Your information management partner should be able to deliver your assets on demand so that you can make use of them whenever and wherever necessary to meet the needs of your agency.

2. Significant information assets are managed by an accountable custodian

Information that is managed poorly or not at all can cause agencies to breach their legal or statutory obligations. Good custodianship helps prevent this situation, so staff should be clear on their roles and responsibilities. When evaluating potential third-party information management partners, you should ensure they are able to manage information assets throughout their entire lifecycle – and that they can meet the security, privacy, confidentiality and other statutory requirements of different types of information.

3. Information meets business needs

Information should be developed and managed in accordance with its strategic importance. This means that information assets should be assessed to see if they are fit for purpose, which is heavily contingent upon data quality. Your information management partner should be able to audit your data, digitising and aggregating key information assets to help you more easily create a “single point of truth”.



Your assets
on demand,
wherever,
whenever

4. Information is easy to discover

Government is a largely knowledge-based industry, which means it's critical that necessary information be easy to find for the public, agency staff, and contracted organisations. While it is important that agencies work towards developing a cross-government information directory, information management companies can help by providing strong cataloguing and indexing systems, and by making these accessible through fast, intuitive interfaces.

5. Information is easy to use

The best way to ensure that information is easy to use is to maintain agreed standards. These standards help determine how information is collected, described, defined, stored and shared. A good information management partner will help to unify your processes and information in a system and format that maximises the ease with which assets can be accessed and interpreted.

6. Information is shared to the maximum extent possible

An excellent way to maximise the value of an information asset is to maximise how often it is used. This reduces the burden on any one agency and limits the overall cost of information management. When choosing an information management company, it can help to align with other agencies – limiting costs, creating a more connected government, and achieving the interoperability recommendations of the Digital Continuity 2020 Policy.

Top 10 Questions to ask when looking for a solution

1. Will your documents be available “scan on demand”?

If you move your documents off-site, they need to be just as easy – if not easier – to access as they were when stored in-house. A good scan-on-demand solution should be able to retrieve the documents you need and deliver them in your choice of format within 3 hours.

2. Does the solution offer a low-cost audit?

A little-known fact about switching information managers is that the best ones will combine the relocation of your archives with a full audit of the files within them. This is an ideal way to discover which files are no longer needed and reduce your overall storage costs.

3. Is the solution flexible and customisable?

Information management needs vary widely across businesses. Rather than asking you to choose a pre-packaged option, the best providers will consult with you to tailor a storage and retrieval solution that adapts to your needs, even if those needs might change over time.

4. Does the solution integrate with your existing system?

You don't want to have to retrain your staff to use a new indexing system. The ideal information management solution uses your existing organisation system and allows you request retrieval using the same filing references you've always used.

5. Is the electronic retrieval process fast and easy?

Many information management companies are able to deliver your files fast, but the system you use to request that data can be cumbersome and slow. Make sure your partner allows the right people to retrieve files easily, from any device, at any time of the day or night.

6. Will your stored information be secure?

Security is a non-negotiable element of information management. Your partner's storage sites need to be equipped with the best fire protection systems, back-to-base intruder detection, and 24-hour surveillance. Employees should also all be police-vetted.

7. Is chain of custody unbroken to all your locations?

Chain of custody is crucial to information security. To reduce the risk of a data breach or loss, ensure your information management partner uses their own fleet and staff for an unbroken, GPS-secured chain of custody to all your locations – urban, suburban and rural.

8. Is physical delivery available multiple times per day?

It's not always possible to plan ahead. A good information management partner understands this and will provide you with the option to have documents delivered more than once per day. They'll also allow you to collect directly from their storage facility if necessary.

9. What is the scope of digitisation services on offer?

Your information management partner should provide a full range of data capture solutions, with OCR, ICR and data entry indexing – helping you automate your business processes and ensuring the fastest possible access to important data.

10. Will the solution streamline your information lifecycle?

The best information management partners will actively help you limit costs and stay compliant by setting up destruction schedules for your documents. They will also always check with you before they shred anything, even if destruction has been pre-arranged.

The Grace Advantage

With over 50 years in the business, Grace is uniquely qualified to deliver excellence in information management.

Grace provides solutions for the full range of government sector requirements, from storage and indexing to retrieval and destruction. Here are the advantages your business will enjoy with Grace:

- Expert consultants to assess the precise needs of your business and tailor solutions that address your specific information management challenges.
- The speed, convenience and security of 26 information management centres across the country – more than any other provider.
- Many facilities are protected by state-of-the-art safety systems, including sprinklers and fire doors – all linked directly to the local fire brigade. Plus, electronic intruder detection with back-to-base alarms.
- Complete and customisable cataloguing, indexing and sentencing solutions for projects of any size, right across the country – with information management software that gives you total control from any device.
- A scanning and digitisation process to make searching and retrieval as fast as possible. Digital files are audited to ensure 100% accuracy, and can be delivered in any electronic format or securely hosted in Grace's online data repository.
- Fast and flexible retrieval, with a standard service that delivers documents twice per day, urgent scan-on-demand services that respond within just 3 hours, and the option to personally retrieve information on site.
- The only secure chain of custody in the industry that spans the entire country. With GPS-tracked vehicles and police-checked staff, your documents never leave Grace's sight. Their client-anonymous indexing system also ensures your confidentiality at all times.
- Real-time tracking of your documents, from anywhere in the world.
- Secure destruction of documents (either on schedule or on demand) that operates under a strict authorisation process, protecting against both accidental data loss and unnecessary storage terms.
- Innovative solutions that recruit Grace's commercial and fine-art removals expertise to cater to a wide variety of unique business requirements.

Contact Grace today to find out how their specialised information management solutions and integrated services can help you. Visit www.grace.com.au/information/contact-us for your nearest office.

HOME | CORPORATE | COMMERCIAL

Our diverse range of services are designed to be fully integrated, offering you a holistic solution. To help you identify where Grace can add immediate value for you, we categorise our services into three customer segments: Home, Corporate and Commercial. Clicking on to these sections on our website will help you easily find what you're looking for.

grace.com.au/information | 1300 164 614

grace:

grace.com.au