CASTLEPOINT™ DIGITAL CONTINUITY 2020 WHITEPAPER

'Impossible Options' – why agencies are failing to manage government records in Business Information Systems using the four current approaches, and a new 'fifth' option to compliantly manage systems easily and economically

OVERVIEW

To date, available evidence shows that government agencies have not been able to achieve significant progress against the requirements of the Digital Continuity 2020 (DC2020) policy for their business information systems (BIS). This paper examines the root causes of the slow realisation of BIS compliance against the DC2020 targets, and proposes a new approach which will overcome the current cost, risk and cultural impediments encountered by agencies attempting to address the DC2020 using the four current paradigms.

The Current Issues

Agencies are required to make their business information systems records-management compliant by 2020, but so far are not succeeding. We have undertaken an analysis of the four options currently available to agencies:

- reconfiguring systems to be compliant with ISO 16175 and 15489
- integrating business systems with an existing EDRMS
- exporting records to an existing EDRMS
- using a manual 'governance' approach

Each option promises to achieve standards compliance, but fails to deliver it effectually, efficiently and cost-effectively. Each option introduces significant risk, cost, and impact to operations and users. This imbalance of cost against benefit is what has prevented agencies from making inroads on Digital Continuity 2020. Until these issues are overcome, government will not realistically be able to meet the DC2020 targets or achieve the expected benefits.

The Objective

In response to this problem, Castlepoint have developed a 'fifth option', which achieves full standards compliance with very low cost, and no business or technical disruption. The goals of the new paradigm are to:

- Avoid high cost for business information systems customisation and EDRMS integration
- Avoid the operational and sustainment risk of complex technology interdependence
- Ensure records management compliance with all requirements of ISO 16175, 15489 and other standards
- Provide additional value for normal business users, without any detrimental impacts to them

The Opportunity

By applying the new fifth paradigm in their approach to achieving BIS compliance as required by DC2020, agencies can meet their obligations rapidly with minimal cost, and avoid negative impacts on business users, processes, and systems sustainability and supportability. Agencies can actively manage their important business records in each of their document management, collaboration, email, social, transactional and line of business systems through a single interface, without the need to make changes to those systems, or to the way their users interact with them.

FAILURE TO LAUNCH

To comply with the Digital Continuity 2020 Policy, by 31st December 2020, all agencies' business information systems (any systems that create, process, manage or store information related to government business) must meet functional requirements for information management, found in ISO 15489, *Information and documentation -- Records management is an international standard for the management of business records* and ISO 16175:3, *Principles and functional requirements for records in electronic office environments*. To date, agencies have not been able to make significant progress towards this goal.

Analysis of current compliance

The *2016 Survey of Information and Records Management Practices in Australian Government Agencies* provides valuable insight into the current status of 158 agencies, and the reasons provided for non-compliance with a digital information and records management model.

The scope of the requirement

Agencies have an enormous number of business information systems (BIS). The 2016 Survey only asked agencies questions about their BIS that hold some RNA records, excluding the majority of BIS in use. However, some key findings relating to the scope of RNA records management can be extrapolated to give a fuller picture of the wider BIS environment across Australian government:

- Of 110 agencies with records designated as Retain as National Archives (RNA), 58% have digital RNA records, and 39% manage at least some of these digital RNA records in business systems
- 19% of these agencies manage at least 70% of their RNA records in BIS, and 6% manage all of them in BIS
- RNA records comprise only an estimated 14.5% of all digital records, equating to 53TB per agency. As such there are approximately 365TB of digital records in total per agency, and agencies are managing at least 39%, or 142TB of these, in BIS

Digital RNA TB	RNA % of Total	Total Digital TB	% of Total in BIS	Total TB in BIS
53TB	14.5%	365TB (53 / 0.145)	39%	142TB (365 * 0.39)

Table 9: Of the digital records that are identified as, or estimated to be, RNA, what percentage of records is held in the following systems: (q46)

Base: Agencies with digital RNA records (n=90)

	Agencies with at least 70% of digital RNA records managed this way		Agencies with all digital RNA records managed this way	
	Number	Percentage	Number	Percentage
Electronic records management system (e.g. EDRMS)	55	61%	33	37%
Business systems	17	19%	5	6%
Other (e.g. email archiving solution)	3	3%	1	1%
Mixture of systems (no one type of system manages all records)	15	17%	51	57%

Using the National Archives of Australia (NAA) conversion rate of 1TB = 98,419 records, this approximates 14 million digital records managed in BIS in each agency – assuming unstructured. Structured would be ten time this amount.

The amount is likely to be even higher. Common BIS in government agencies include line of business systems, case management, content management, document management, email, human resource management, financial management, and social media. All of these systems store Commonwealth records, and are often the primary repository for operational (core business) information in an agency. For example:

- The **Department of Defence** currently has 3,334 systems on its Defence Approved Software List (DASL). Of these approximately 1,700 are data storing systems[1]. Note that the DASL only lists the supported software type, and does not enumerate each instance of that software in use as a BIS in the organisation.
- Analysis of digital information systems usage at **Airservices Australia** shows that as well as outnumbering EDRMS in scale and size, BIS also have higher usage than EDRMS. The Airservices EDRMS is actively used by approximately 250 of its 3,000 staff. It contains approximately 250,000 documents, compared to over 8 million in one of its medium sized BIS, ORBIT. ORBIT is one of approximately 1,200 BIS in use at the organisation.

The key impediments to compliance

The amount of BIS that need to meet the functional requirements of the Standards are likely to be over 1,000 per agency. Agencies have not been able to meet these requirements. Some key findings of the 2016 Survey relating to issues with achievement of adequate digital records management were that:

- A total of 105 agencies, (66% of agencies in the Survey) had sentenced records in the past year; almost all of these had sentenced physical records, and just over half had sentenced digital records
- Nearly one quarter of agencies (39 agencies or 24%) have not transitioned effectively to digital information and records management (i.e. over 70% digital). The main reasons cited were funding or resource constraints
- 19% of agencies have not adopted any approach to ensuring the preservation of digital RNA records
- Only 14.5% of the 158 surveyed agencies had undertaken any electronic record destruction in the previous year, and none of these had undertaken any destruction of records in BIS:

Table 10: Please specify the quantity of digital records your agency (or contractor on behalf of your agency) destroyed over the last 12 months. (q52)

Total of items and total storage space across agencies (n=158)

	Number of agencies	TB
In an electronic records management system	16	4.3
In a business system	0	0.0
Other digital records	3	0.8
Total	**18***	**5.2**

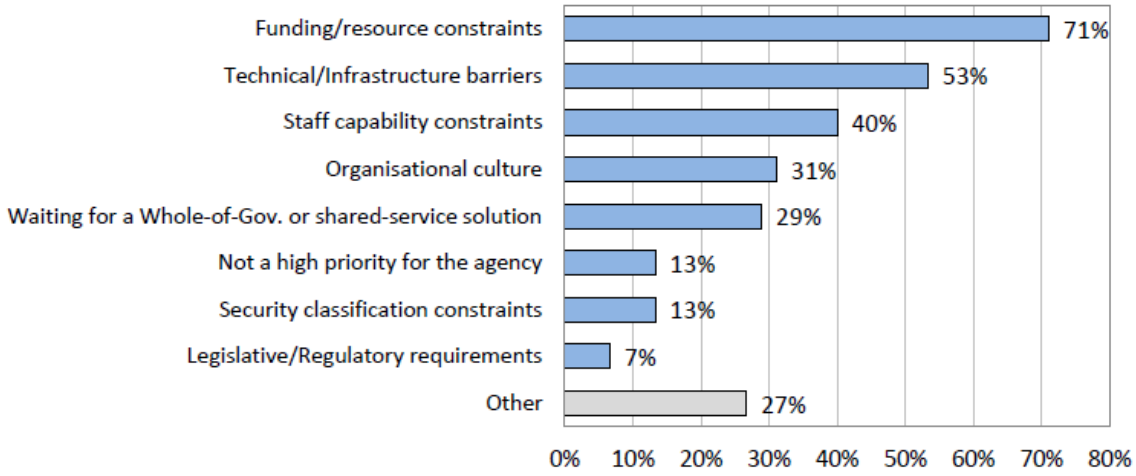
* One agency indicated destroying digital records in both an electronic records management system *and* "other" digital records (in neither an ERMS nor a business system).

Agencies that are managing and sentencing digital records are largely doing so in the EDRMS. However, the EDRMS is usually not the largest store of digital records in an agency – business information systems significantly outnumber and outweigh EDRMS in terms of scale.

[1] *Client server systems, enterprise databases, uncategorised systems and web applications.*

The following graphic shows the reasons provided for failure to effectively transition to date:

Figure 4: Main reasons for not having completed the transition to a digital information and records management environment



Source: 2016 Survey of Information and Records Management Practices in Australian Government Agencies. National Archives of Australia / Orima

In summary, the main reasons for agencies not effectively managing digital records are given as:

- **Cost impacts –** funding constraints prohibit expensive investments **(71%)**
- **Technical impacts –** barriers in the current technical environment prevent complex changes **(53%)**
- **Staff impacts** – constraints in staff capability and organisational culture prevent the introduction of new or changed records and information processes **(40% and 31% respectively)**

These are the three main issues that the current four options all exacerbate. In trying to achieve compliance, the four current paradigms introduce cost, technical and staff impacts. The root cause of low uptake of digital records management in business systems is that these negatives outweigh the perceived benefits.

Compliance is important, but not usually a high executive priority. Penalties for non-compliance *per se* are low. Increased accountability through reporting to the NAA helps with the compliance business case, but does not give it sufficient leverage over cost savings and minimising change impact. Any activity to ensure compliance will necessarily have some cost and change impact, but in the case of BIS compliance, the trade-off has been too high.

The requirements in more detail

Agencies have a large amount of BIS, and are being prevented by cost, technical overhead and staff impacts from ensuring they meet the functional requirements from the Standards. To meet the functional requirements, each BIS must be given the ability to:

- **create records in context**: the functionality required to create and keep records that are valid, accurate and protected from both accidental and deliberate unauthorised change.
- **manage and maintain records**: the functionality required to ensure records do not lose their evidential value during management processes including classification, retention, disposal, security and access.
- **support import, export and interoperability**: the functionality required to exchange, import or export records both within and between systems, without the loss of content or metadata.

- **retain and dispose of records as required**: the functionality required in business systems to dispose of records in a managed, systematic and auditable way.

ISO 16175:3, supported by the NAA *Business Systems Assessment Framework* (BSAF), gives four options for making these capabilities available in BIS. The following analysis of the four options shows that the cost, technical and staff impacts cannot be easily absorbed by most organisations using the suggested approaches.

Option One: Build In

Designing the business system to internally perform the records management functions

*BSAF: **Solution 1: Build in** – configuring, modifying or upgrading the business system to manage the risk or gap. For example, if you have identified that you cannot prove the information is authentic, you might build in this functionality by configuring metadata fields to capture additional information to support authenticity*.

The **Build in** option has the following inherent issues:

Cost Impacts

Making changes to existing systems is costly. Most agencies have hundreds or thousands of business information systems, with several more coming online every year. The cost of not only enhancing all existing systems, but making each new one compliant, is a large body of work requiring specific skill sets and long periods of development, testing and implementation.

Designing and building-in compliance requirements to new business systems is ideal, but can add significant overhead to the design and development process for bespoke systems. For Commercial Off the Shelf (COTS) products, international vendors are not motivated to develop records management controls for a relatively small customer base, to Australian continuum-model standards. Systems that do build in records management controls usually base them on a 'recordisation' approach, which is not compliant for Australian government. It will rarely be possible to achieve standards compliance with COTS products, without customising them in some way.

Technical Impacts

Customising an off-the-shelf system introduces significant risk, including failure of the vendor to continue to support the implementation, and interference with patching and upgrade paths for software.

Changes to in-flight COTS or bespoke systems can cause breakages to unrelated functionality that may not always be foreseeable. Additionally, whole of government Digital policy directs agencies to use COTS where possible, and avoid customisation and bespoke development. Each agency separately undertaking projects to customise each of its COTS products is not in keeping with the Digital Transformation Agency strategy.

Staff Impacts

Changes to a business information system's core functionality, in order to introduce additional administrative capability, places a burden on systems administrators that they may not be skilled or resourced for.

Additionally, unless records management capability can be introduced to a system in a way that is invisible to its users, the change will have an impact on their productivity in the short and possibly longer term.

Option Two: Integration

Integrating with an identified records management system, such as **an electronic records management system**

BSAF: ***Solution 2: Integration –*** *integrating the business system with another system to manage the risk or gap. For example if disposal is not controlled, systematic and recorded in a particular system, you could manage the gap by integrating the business system with your agency's EDRMS and manage the disposal process there.*

The **Integration** option has the following inherent issues:

Cost Impacts

This model requires technical configuration or customisation to both the BIS and to the EDRMS. The costs are similar to the Build in model, as the process of interfacing and integrating systems usually requires extensive design and development time. Most agencies will require the services of system SMEs and/or vendors for both the BIS and the EDRMS. Existing EDRMS systems can integrate with many BIS via application programming interfaces and web services, but require changes to each BIS to push data to them. As with the Export model, EDRMS solutions will support unstructured data, but would not easily integrate with structured data systems that represent the bulk of BIS.

Technical Impacts

The technical risk of closely integrating systems is high. Once systems are closely coupled, they become interdependent. Necessary upgrades to one system may be held back by the current version of the integrated system, and agility for enhancements is limited. It is also important to note that many vendors (such as Microsoft) will not support their systems when issues arise until third party integrated systems are excluded from the equation. Internal SLAs and SLOs may also be affected. Configuration management complexity of closely integrated systems increases, as does cascading technical risk.

Staff Impacts

This option can have a low impact on general staff if the integration is invisible to users. However, most integration models require changes to the user experience in the source system in order to enforce capture of the requisite metadata that the EDRMS relies upon in order to effectively manage the records. In this way, integration of an EDRMS with a business system may result in the usability and efficiency of the BIS being degraded.

Integration between two or more systems with different access control models is highly complex, and any instability or misconfiguration affects user search, editing and document integrity. The impact on administrative staff with integrated systems can be high, as the increased effort of managing an interdependent suite of systems, coupled with reduced vendor support, can make the task of supporting and sustaining the environment much greater.

Option Three: External (export)

Designing export functionality into the business system to directly export records and their associated metadata to an identified records management system.

BSAF: ***Solution 3: External (export) –*** *managing the risk or gap by exporting the relevant data so it can be managed in a separate system. For example, if the system cannot generate reports of its information management processes, consider exporting the data periodically into a format that allows you to interrogate the data (for example spreadsheets).*

The **Export** option has the following inherent issues:

Cost Impacts

This solution also requires development, which may incur significant costs. However, it may not be able to achieve any return on investment, as it will not meet the requirements of the 16175 standard. The NAA requires that records are managed ‘whole of life’ from the point of creation or capture as per the continuum model, not ‘made a record’ at a later point in their life cycle:

> *Continuum: The whole extent of a record's existence. The related theory replaces the life cycle model by considering that* ***records require management starting before they are created****, e.g. in systems design.*

> *This theoretical model more effectively allows for p**reservation and management processes to be applied to a record at any point in time**, which is particularly relevant when dealing with digital records*[2]

The retention phase of the records lifecycle of exported digital records can in principle be managed by the EDRMS in accordance with the expectations of ISO 16175:3. However ISO 16175:3 states that the system must:

> 109: Be able to detect any metadata changes that affect the retention period of an electronic record, and calculate a new disposition date according to the disposition class (Mandatory).

Lack of dynamic linkage between the record and its metadata changes in the business system, and the retention rules engine in the EDRMS, would breach this control.

Migration between the business system and EDRMS introduces risks related to metadata compliance. For an export model to be successful, the system would have to import not only the file itself, but also its metadata:

> 53: Be able to import any audit trail information that may be directly associated with electronic records, and where applicable aggregations of electronic records, captured and maintained by the system and guarantee the integrity of the imported information (Highly Desirable)
>
> 57: Ensure that any export action is able to include:
>
> - All metadata associated with exported electronic records and, where applicable, aggregations of electronic records
> - All audit trail data associated with exported electronic records (Mandatory)
>
> 58: Be able to export electronic records, and where applicable aggregations of electronic records, in one sequence of operations such that:
>
> - Associations are retained between electronic records and their associated metadata
> - Relationships are maintained between exported components of an electronic record, between exported electronic records, and where applicable aggregations of electronic records, so that their structural links can be rebuilt in the receiving system (Mandatory)
>
> 61: Ensure that any export action is documented in metadata associated with the record (Mandatory)

Transferring a record to a new system to re-enter the 'Create' phase, effectively creating a new record without also transferring audit trail, relationships and metadata, would breach these controls.

Additionally, re-entering the 'create' phase when the record is moved to the EDRMS would contradict the requirements of ISO 16175 for a system to maintain the whole-of-life metadata of its records:

> 18: Be able to store selected metadata over time, regardless of whether the related record has been archived, deleted or destroyed (Mandatory)
>
> 32: Be able to manage a metadata profile over time – maintaining links to the record and adding process metadata about records management activities (Mandatory)

Finally, most EDRMS systems are not able to import and manage structured data, which comprises the bulk of the records in business information systems. While an EDRMS may be able to import documents, images and potentially web pages, it is not able to manage table data from finance systems, HR systems, CRMs, ticket and process management systems, social media, Web 2.0 and other operational systems.

Technical Impacts

In order to achieve adequate compliance in a continuum model, a EDRMS would need to import data as close to the point of creation or capture as possible so that it was sentenced and controlled early. The BIS would also need to

[2] See http://www.naa.gov.au/Images/Sentencing_tcm16-47302.pdf page 5 (accessed February 2016).

export all the versions, audit trails and metadata, not just the final version; and between the EDRMS and the BIS a single metadata profile for the record must be maintained over time. However, early migration of the record would remove it from its context in the BIS. Export and import would as such need to be recurring – once when the item was created so that it could be sentenced, again dynamically each time the content of the record changed sufficiently in the BIS to require an update to the classification, and finally when the record was considered complete.

Staff Impacts

In a continuum model, where the record was retained in the BIS while also being captured into the EDRMS, staff would not have their operations impacted, as the BIS where they do their work would remain unaffected. However, issues with discovery arise when there is more than one copy of a record. Records must be reliable, authoritative and trustworthy, and this aspect of record integrity is affected in a model where the 'official' record is not the most current one, and is not seen in context with other operational information from its source system.

In a recordisation model, where the record is moved to the EDRMS later in its life, discovery and reuse becomes problematic for staff. While obsolete records can cause unnecessary 'noise' in searches for information in an organisation, missing records have a greater impact on information discovery. Information that is archived and removed from its business context can become effectively 'lost' to users who could have reused or referenced that information.

In either model, if staff are required to interface with the EDRMS at any point in the records life cycle, they will be confronted with a less usable interface to that of their BIS. The August 2017 Department of Finance *Feasibility Study into a Whole of Government Digital Records Management Solution* found that 80 agencies reported that their EDRMS systems[3] were not user-friendly, and required training to be able to navigate correctly.

Option Four: External (governance)

BSAF: ***External (governance)*** *– managing any risk or gap by implementing procedures and business rules. For example if the system cannot prevent unauthorised changes, consider controlling access to the system by using business rules and security protocols (note this option is listed in the BSAF only and is not in the Standard).*

The **Governance** option has the following inherent issues:

Cost Impacts

This model has a high resource cost to achieve. It requires agencies to manually compensate for a lack of automated functions. The governance model has to achieve the following primary records management outcomes:

- **Information is trusted** – information in a BIS has to be protected from unauthorised disposal, and have its history and chain of custody adequately documented. In this model, the agency must ensure data integrity inside a system from the outside of that system. Whether using preventative or corrective controls, there will be some risk of loss of integrity if the system itself cannot adequately set, enforce and log information access and privileges authorisation.
- **Disposal is accountable** – BIS information has to be appropriately classified against a Records Authority, and protected from disposal or deletion by unauthorised users. The agency must be able to classify and sentence records on creation, from outside the BIS. This requires knowing whenever a record is made, and manually registering it somewhere else. Additionally, the classification and sentence date must be recalculated every time the function, relationships with the rest of the aggregation, and dates of last action change. For large volume transactional systems, this will not be possible with existing resourcing.
- **Import/export** – a system that cannot generate an extract of all records with their versions, audits, metadata and relationships in a manner that can be ingested by another system will require a significant amount of manual effort to achieve any effective, compliant information transfer.

---

[3] The EDRMS platforms used in Australian government per the NAA 2016 Survey of Records Management include HP Trim/CM (70% of agencies surveyed), RecordPoint (17%) and Objective (11%).

- **Reporting** – manually exporting raw data to Excel (or a third BIS) to produce reports involves significant overhead for records management staff, and time spent doing data extraction, transformation and load detracts from time records mangers can add value more strategically with their specialist skills.

Technical Impacts

The technical impacts of a governance paradigm should be negligible, as it should not require changes to the systems themselves. However, the practicalities of manual records management would require some technical changes to systems in order to achieve proper control. Full control of record integrity, disposal, import/export and reporting inside technology systems cannot be achieved using processes entirely outside of those systems.

Staff Impacts

The largest impact in this model is on records management staff. Manual control of hundreds or thousands of systems is an enormous overhead that will not be absorbable by most agencies, and goes against the recommendations of the Finance *Feasibility Study* to move to an automated model for records management.

This option also has impacts on users (who may have to change their business processes in order to satisfy requirements that cannot be met technically), and on the agency's customers and stakeholders (whose information privacy, security and integrity may be detrimentally affected due to a lack of robust and comprehensive controls).

The 'Do Nothing' Option

While most agencies are still intending to address business systems compliance, some agencies may have actively chosen to do nothing to address BIS compliance in response to the issues encountered with the four current options.

This is not an appropriate strategy. While compliance as an end goal in and of itself may not have high priority for an organisation, it is vital to understand the indirect or secondary benefits. The compliance standards are designed to enforce the 'best practice', meaning the best and most beneficial way to operate. The practice of managing records in business systems according to the standards is beneficial because it allows agencies to:

- **optimise the delivery of government programs and services** – by making sure the right information is available to the right people at the right time, helping agencies to make better business decisions with more evidence behind them, and achieve better outcomes.
- **enable information reuse for economic and social benefits** – as information is an (expensive) asset to develop and maintain, reuse and return on investment is in the agency's interest and in the public interest.
- **protect the rights and entitlements of Australians** – proper records management ensures that agencies have proper control of important information, and protect it from inadvertent or unauthorised loss or disclosure. This avoids regulatory, security and legislative breaches.

Continuing to do nothing to address BIS compliance costs the agency in terms of risk, persistent lower productivity, ongoing high impact on staff and records managers, and lost value of existing information assets that are not usable.

Analysis Paralysis

When faced with multiple options, agencies have robust methods in place to compare them in order to make the most appropriate selection. Options analysis as a discipline in government is well established and predominantly evidence-based and empirical. Options analysis generally compares relative benefit, cost, impact (technical and business) and risk, and applies weightings in making a recommendation.

When one option stands out as superior, decision making is simple. More commonly, two or more options both have similar potential to achieve benefits for the agency, and where they also have similar costs and risks, decisions can be more difficult to make and achieve consensus on.

The worst case scenario for agencies attempting to select the most appropriate option for a problem is when all of the options are unsound. This is the case with the four current options for BIS compliance. Each one is suboptimal in terms of achieving benefit, and stands to actually degrade the current state of operations if introduced. On balance, each option may cause more harm than good.

OPTION	Risk	Cost	Impact	Benefit	Score
Build in	High – 3	High – 3	High – 3	High – 1	10
Integrate	Medium – 2	High – 3	High – 3	Medium – 2	10
Export	Medium – 2	High – 3	Medium – 2	Low – 3	10
Governance	Medium – 2	High – 3	Medium – 2	Low – 3	10
Do Nothing	High – 3	Medium – 2	Medium – 2	Low – 3	10

This is the primary reason that more agencies have not progressed with their BIS compliance. When each option to move forward is effectively impossible, agencies must stay in the same place.

THE FIFTH OPTION

Assessment of the four current options identifies significant issues with each that must be overcome or avoided. Overcoming the limitations of each option requires some substantial mitigations:

- **Build in**: Agencies may wish to add third party products to their BIS in order to achieve the functional requirements. This avoids the need to customise the BIS itself. However, while some products already exist to add on to SharePoint, for example, to help achieve compliance, there are no products available to address compliance of other BIS such as HR, Finance or CRM systems, or for bespoke products. A third party add-on may address one system, but not thousands.
- **Integrate**: The issues of interoperability with integration solutions can be reduced by a loose coupling, rather than tight coupling, model. This is a reasonable proposition for BIS, which will often be compatible with standardised web services or Application Programming Interfaces that can be used for inbound and outbound messages. However, EDRMS are not generally designed to support loose coupling with dozens of different system types, to manage structured, as well as unstructured, data. Less tight coupling may result in less capability. Where the EDRMS cannot get all the information it requires about the record from the BIS in order to properly classify and control it, this task will shift to the users or records managers.
- **Export**: To ensure continuum management in an import model, imports would need to be recurring. This would likely require changes to the business systems, and customisations to the EDRMS, to be manageable. In this model, there would be two copies of each record – storage for the EDRMS would need to be significantly increased, and a control system introduced to ensure that users were always presented with the current, most authoritative copy.
- **Governance**: To make an external governance option feasible, some automation would also be required. Records managers cannot manually oversee millions of records in thousands of systems without some machine assistance.

A more effective way to manage the inherent risks is to develop a fifth option – one which combines the benefits of each existing paradigm while mitigating all of the impacts and risks. This option must have the ability to:

- encompass millions of records in thousands of systems, both structured and unstructured

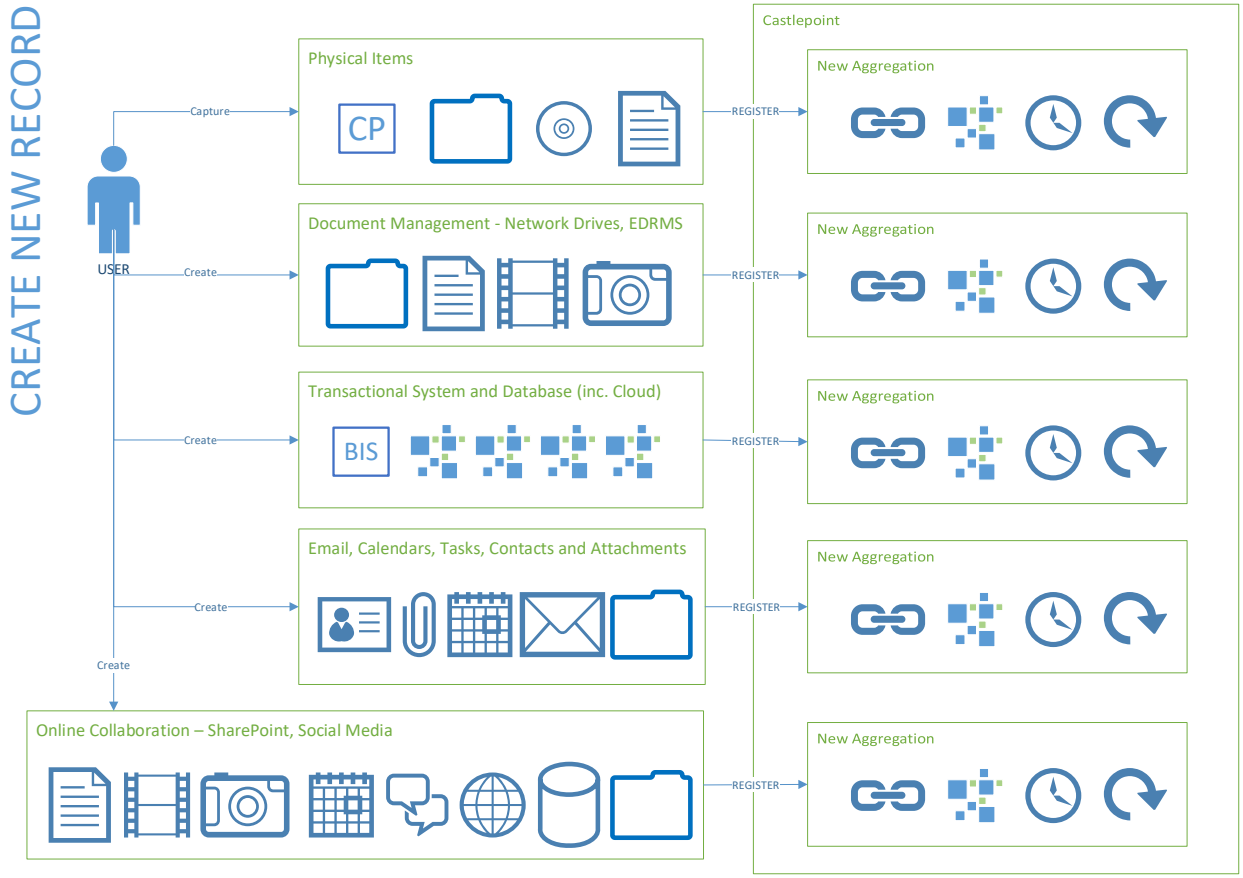
- make the management of records in those systems compliant with the standards for their entire life cycle
- avoid technical customisation or complex integration of existing BIS and EDRMS
- avoid duplication of records and expansion of records storage
- provide a simple interface for records managers to undertake their control activities
- automate the process of registration, classification, and sentencing per Department of Finance expectations

Castlepoint – Manage Information Everywhere (MIE)

Developed in response to the challenges seen with both traditional EDRMS and BIS compliance, MIE introduces a new paradigm for digital continuity. MIE is a central system that loosely couples with BIS without the requirement to make technical changes to those systems. MIE can interact with any business information system via microservices, and manage both structured and unstructured records.

Some examples of common BIS that Castlepoint MIE can manage include

- Document management systems including network drives, Dropbox, Docusign and Google Drive
- Email systems including Exchange and Gmail
- Collaboration systems including SharePoint and Office 365
- Databases including Oracle, SQL Server, DB2, Ingres, and other ODBC-compliant databases
- Social including EventBrite, Facebook, Instagram, SurveyMonkey, Twitter, Wordpress, Yammer, YouTube
- Line of business systems including Dynamics, GitHub, Jira, PostgreSQL, and Zendesk
- Other cloud systems including SalesForce, GoTo Meeting, Webinar and Training, Google Calendar and Stripe.



MIE works by silently monitoring the BIS for new items (documents, emails, tweets, rows, web pages, images or other records). When a new item is identified, MIE uses artificial intelligence (AI) to either match it to an existing record aggregation, or create a new aggregation. No user interaction is required (including additional metadata input).

MIE uses AI to understand the context of the record (who created it, and where in the organisation it arises from) as well as content analysis of keywords present in the text. It uses this information to automatically classify the record aggregation against a Records Authority, and any relevant ontologies.

MIE applies the sentence from the Records Authority when it is registered, but also continually over time as the content of the aggregation evolves and changes, to ensure the classification remains appropriate. When the retention period is met, MIE alerts the records managers, who can review the aggregation and execute the sentence.

MIE supports compliant destruction, transfer and import and export of records, and provides a full set of reports on all records across the enterprise. MIE also adds value to users by providing an interface where they can search for other records in the organisation that relate (contextually or in their content) to the ones they are working on.

Cost Benefits

- Single customisable product that doesn't require expenditure on a BIS or EDRMS in order to connect to them
- Single license for an organisation – only one product required to manage all records in all systems
- Reduced productivity costs for records managers and staff through ease of discovery and management

Technical Benefits

- Avoids the need for customisation or integration with bespoke or COTS products, affecting their supportability
- Avoids duplication of storage for millions of records by allowing them to remain in place in their source system
- Runs using a simple AI system that does not require a complex rules engine requiring ongoing support

Staff Benefits

- Allows records managers to add more strategic value by freeing time from manual classification and control
- Assists users with information discovery across the boundaries of their usual systems and silos
- Allows users to work as normal in their usual BIS, keeping all records management functions invisible to them

MIE achieves the benefits of full compliance, including reduced organisational risk and increased business benefit, without the commensurate cost, technical and staff impacts that the current paradigms introduce. Using MIE, Australian government can easily achieve its DC 2020 obligations, and improve its overall information management.

FOR MORE INFORMATION AND BLUEPAPERS

Rachael Greaves	**Gavin McKay**
Chief Information Officer	*Chief Technology Officer*
Castlepoint Systems	Castlepoint Systems
Rachaelg@castlepoint.systems	Gavinm@castlepoint.systems
http://www.castlepoint.systems	http://www.castlepoint.systems
1300 996 905	**1300 996 905**