Castlepoint

Records and Information Management Solution

Use Cases

Executive Summary

This document identifies key use cases for records and information management in organisation, based on the records management lifecycle as described in ISO/TR 15489:2-2001, *Information and documentation – Records Management – Part 2, Guidelines*.

Each use case describes the current state issues, the target state using Castlepoint, and the expected target state benefits. Each slide includes a linked video demonstrating the capability.

The purpose of this document is to support executive decision making, by providing sufficient information to show that Castlepoint can meet organisation requirements, as well as sufficient justification of the business case for Castlepoint.

Compliance	Cost	Quality	Risk
Increased – to 100% of records, across all systems, for the whole records lifecycle	**Reduced** – by automating effort currently done by staff and records managers	**Increased** – by ensuring all records are classified, discoverable and consistently managed	**Reduced** – by defensibly and appropriately managing record retention and security

Records and information lifecycle – ISO 15489

ISO 15489 includes the following nine stages of the information lifecycle:

1: Capture
2: Registration
3: Classification
4: Access and security classification
5: Identification of disposition status
6: Storage
7: Use and tracking
8: Implementation of disposition
9: Monitoring and auditing

1: Capture

Current State	Target State
‘Capture’ is the process of determining that a record should be made and kept. Users may capture records into the EDRMS on an ad hoc basis. However, most records of business are not in fact saved into the EDRMS, meaning they are not formally ‘captured’ per NAA requirements. Records are created and saved into Business Information Systems (BIS), but the required ‘context, content and structure’ metadata is not consistently saved with them.	Using Castlepoint, records stay in the source system and are ‘managed in place’, so they do not need to be saved into the EDRMS if they are more naturally or appropriately stored in another BIS. Castlepoint will ensure that the required ‘capture’ metadata is captured for all records – ensuring that the records are contextualised, retrievable, meaningful, and provide fixed representations of actions undertaken.

Compliance	Cost	Quality	Risk	Compliance	Cost	Quality	Risk
Low – most records are not ‘captured’	Moderate – the impost of ‘making a record’ falls on staff	Low – records cannot be relied on as evidence	High – important records are not captured	High – all records are ‘captured’ in place	Low – records are captured automatically	High – records in BIS can be found and relied upon	Low – full coverage of records for IM and RM purposes

2: Registration

Current State				Target State			
Registration is the formalisation of records capture, and includes assigning at minimum a unique identifier, date/time of registration, title, description and author. Currently, each organisational system registers its own records independently, and may or may not assign these properties. Where records are registered manually by users in recordkeeping systems, the users may have to add metadata in order to register the record.				Castlepoint registers each record in a central information asset register, regardless of the source system, and assigns a consistent unique identifier. Castlepoint captures the required registration metadata, regardless of whether the source system is capable of recording it. Users do not have to manually register records or select appropriate metadata properties, reducing the risk of mislabelling, and the cost of doing business.			
Compliance	**Cost**	**Quality**	**Risk**	**Compliance**	**Cost**	**Quality**	**Risk**
Low – not all records are compliantly registered	Moderate – EDRMS users have to manually register	Low – registration data quality inconsistent	Moderate – records captured may not be traceable	High – all records in all systems are registered	Low – registration is automatic	High – all required registration metadata is captured	Low – AI ensures that registration details are correct

3: Classification

Current State				Target State			
Classification is the process of grouping a record into a meaningful aggregation, along with other records of its type. Classification uses the Records Authorities (RAs) and other ontologies to assign records to one or more functional categories, and so to sentence them. Currently, only records in an EDRMS are classified against an RA, and only at one point in time. No other electronic records of business are classified and sentenced – meaning they cannot then be compliantly disposed of.				Castlepoint uses AI to read each record in the organisation, and apply the most appropriate sentence, based on its context and content. Castlepoint constantly reviews sentences, meaning that if a record changes, its sentence will update automatically if needed. This provides full coverage of NAA-compliant sentencing to organisation records, meaning both that more records can be destroyed with confidence, and also that high risk records can be better protected.			
Compliance	**Cost**	**Quality**	**Risk**	**Compliance**	**Cost**	**Quality**	**Risk**
Low – only a small % of records are sentenced	Moderate – storage costs increase if records are not disposed	Low – sentencing decisions are point in time and degrade	High – records can be kept too long or lost too soon	High – all records of business are sentenced	Low – sentencing is automatic (no user or RM effort)	High – AI ensures records are resentenced constantly	Low – sentencing and disposal decisions are justifiable

4: Access and Security Classification

Current State				Target State			
This process assigns security rights and restrictions to records, based on their content. Currently, organisation controls access at the system level, as well as the file level. Classifications on individual items are either inherited, selected by the user, or absent. Classification is inconsistent across systems, as there is no single view of all classified content, or of any content that may be under or over-classified.				Castlepoint includes classification, where available, in the central information asset register, ensuring that security staff can see all classified content in the organisation via one interface. Additionally, Castlepoint uses natural language processing to identify records that have sensitive keywords, and surfaces these to security personnel to help them ensure that all records with a potential security risk are accounted for.			
Compliance	**Cost**	**Quality**	**Risk**	**Compliance**	**Cost**	**Quality**	**Risk**
Moderate – classification may not reflect content	Moderate – discovery of sensitive records is not efficient	Low – confidence in record security is low	High – sensitive information can't be well controlled	High – all classified records can be found/ managed	Low – discovery of sensitive records is simple	High – confidence in record security is high	Low – sensitive information can be well controlled

5: Identification of Disposition Status

Current State				Target State			
This process follows from classification, and uses the ontology selected in that stage to determine how long the record needs to be kept for. It also determines the trigger for disposition (creation, modification or expiry). Currently, organisations can only identify and manage the disposition status of their EDRMS electronic records. An organisation cannot determine the retention time or trigger of records in other systems, meaning it cannot destroy them safely without significant manual effort.				Castlepoint calculates the disposition status of all records from creation or capture, and again on every record change, meaning that sentencing is always correct and current. Castlepoint displays the disposal status (including records due, overdue and not yet due for disposal) in dashboards and reports, and alerts records managers when actions are due.			
Compliance	**Cost**	**Quality**	**Risk**	**Compliance**	**Cost**	**Quality**	**Risk**
Low – NAA requires all records have disposal status	High – BIS disposal requires extensive sampling	Low – BIS disposal status only set on start or end of life	High – BIS records are kept for too long or not long enough	High – all records are actively managed for disposal	Low – disposal status is managed automatically	High – disposal status is always current	Low – record disposal is defensibly and actively managed

6: Storage

Current State				Target State			
This part of the information lifecycle relates to ensuring that records are stored properly throughout their lifecycle – including when their systems become obsolete. Organisations may have multiple legacy systems that need to be upgraded, and many paper files that may need to be digitised, but limited capability to determine which old records have value and should be kept. The main preservation strategy is to manually review records for upgrade, to upgrade them all, or to upgrade none.				Castlepoint is able to index, classify and sentence records from legacy systems, or from paper file lists. This activity results in a clear picture of which legacy records are still required versus which have already reached their minimum retention period. Of the records that are still required to be kept per their Records Authority, Castlepoint's content analysis can help organisation to determine which have enough value to convert or migrate, versus which can be kept as archives on legacy systems for the remainder of their life.			
Compliance	**Cost**	**Quality**	**Risk**	**Compliance**	**Cost**	**Quality**	**Risk**
Moderate – records can be preserved, but may not be	High – needs manual sampling, or wholesale conversion	Low – converting end of life records adds clutter	High – key records may be lost or inaccessible	High – record preservation decisions are defensible	Low – AI can determine the records worth conversion	High – only valuable records are preserved	Low – key records in legacy systems are identified

7: Use and Tracking

Current State				Target State			
This process involves making metadata records of all key actions on a record over time, including access, modification, security changes, movements, classifications, and disposition status updates. Currently, organisations can track records in an EDRMS, but cannot effectively track actions or usage on Business Information System (BIS) records. Where BIS records do retain this metadata, each BIS has to be interrogated separately for reviews and audits.				Castlepoint will keep a register of all key actions on all records in all systems, accessible through a single interface. This includes metadata that may not be recorded in the source system in a human-readable format. Castlepoint includes various reports which can be used by records managers, security managers, auditors and quality managers to monitor usage in real time.			
Compliance	**Cost**	**Quality**	**Risk**	**Compliance**	**Cost**	**Quality**	**Risk**
Low – BIS records are not effectively tracked	Moderate – reviews audits require manual scans	Moderate – review and audit outputs are inconsistent	Moderate – lack of detective controls increases risk	High – all records have their usage and changes tracked	Low – reviews and audits can be largely automated	High – outputs are consistent over all BIS records	Low – detective controls support security

8: Implementation of Disposition

Current State	Target State
This process involves identifying records that are due for disposition, bundling them together, undertaking the disposal action (destroy, transfer or retain), and updating the sentence control record (SCR) with the outcome of the disposition action. Currently, organisations usually only have this capability in the EDRMS. Any disposition of records in Business Information Systems requires manual effort for each step.	Castlepoint will support records managers in implementing disposal requirements on all records. Castlepoint provides a single view of all records, meaning it is easy to bundle records with like disposal actions for actioning at the same time. Additionally, the interface shows records managers a summary of what content is in a record, and when/by whom it was used, meaning they do not need to open each record to confirm the sentence.

Compliance	Cost	Quality	Risk	Compliance	Cost	Quality	Risk
Low – NAA requires disposition across all BIS	High – BIS disposition requires significant effort	Moderate – 'sampling' approach to support decisions	Moderate – non-simple disposition causes inconsistency	High – disposition of all records can be managed	Low – AI manages triggers, schedule, and SCR	High – sentence is defensible and easy to confirm	Low – records can be more appropriately disposed of

9: Monitoring and Auditing

Current State	Target State
Monitoring and auditing are required by the Standard to ensure compliance; to provide assurance that records will have acceptable evidential value in court if required; and to help agencies continually improve their performance. Organisations can monitor and audit compliance, evidential weight and performance for an EDRMS, and for some BIS, but not all. Organisations can't assure the integrity, authenticity or security of many of their records.	Castlepoint provides a single, central register of all actions on all records, and is itself protected from both deliberate and inadvertent modification. As such, it provides a reliable control record for each document or data set in the organisation. Organisations can use Castlepoint to monitor for unauthorised changes, movements, deletions and additions, and to provide evidence of the same, whenever required.

Compliance	Cost	Quality	Risk	Compliance	Cost	Quality	Risk
Low – most records can not be effectively assured	Moderate – reviews and audits require manual work	Low – performance improvement opportunities are limited	High – evidential value can't be assured in most systems	High – all record actions can be assured	Low – audit and review is able to be automated	High – continuous improvement is supported	Low – evidential value can be assured in all BIS