Model Policy for the Retention of Court Information

First edition, September 2022

FOR CONSULTATION PURPOSES ONLY

Prepared by Martin Felsky, PhD, JD – Special Advisor to the CJC on Information Technology

TABLE OF CONTENT

BACKGROUND

This Model Policy follows upon the Council's 2013 initiatives concerning court information including the Blueprint for the Security of Court Information. All courts, and the Council, recognized that the modern concept of "court information" was no longer merely a matter of official or administrative court records acquired or created intermittently, with limited bespoke content, and with practical obscurity arising from its documentary character and its ease of destruction.

A decade on, it is even more obvious and pressing that courts must recognize that "court information" is a far more encompassing concept and is far more accessible and far more durable than it once was. Accordingly, and in addition to its other responsibilities as to court information, each court needs to create, maintain, and review a systematic approach to the audit and regulation of the life cycle of court Information. This Model Policy proposes a framework for courts to consider in that effort.

Using the Council's Model Definition of Judicial Information[1] as a guide, this Model Policy is aimed at the life cycle of court information and should not be read to alter the Blueprint for the Security of Court Information,[2] nor alter the distinction between court information that is exclusively owned and controlled by the court, and any court information which by its nature can be delegated to or acquired by the executive branch directly or indirectly.

ACKNOWLEDGMENT

The author would like to thank members of the CJC Technology Subcommittee for their valuable feedback on an earlier version of this Model Policy.

[1] *Model Definition of Judicial Information* (CJC, 2020). In French: *Définition modèle des renseignements de la magistrature*.
[2] *Blueprint for the Security of Court Information* (6th edition, CJC 2021). In French: *Plan directeur pour la sécurité de l'information judiciaire*.

CURRENT STATE OF RECORDS MANAGEMENT

For any organization, implementing a records retention and disposition policy is not easy. Conventional practices based on paper collections often do not work, because the burden of identifying and retaining records worth keeping falls on individual employees. Making these decisions is time-consuming, complicated, and thus often neglected. Enforcement is almost impossible, as business heads have more important concerns than document retention. Retention schedules are granular, can run to hundreds of pages, and are stale dated as soon as they are published.

For these reasons, many courts are in the same position as any other organization: records at the end of their life cycle are treated in an unregulated fashion. By some estimates only 20% of records are disposed of in accordance with their applicable retention schedules.[3]

DIGITAL IS DIFFERENT

The conventional approach to records management does not translate to email and other electronic forms of communication such as text messaging, where billions of bits of data are stored in dynamic databases. Digital information can be structured or unstructured and exist in many different formats. Transactional records, which used to be compiled in a single file folder are now distributed in email threads, word processing files, SharePoint sites, online court registries and e-filing applications. The fact that many applications, including essential communications tools, were not designed with retention needs in mind adds to the challenge. Users must apply policies and schedules manually after the fact, unless the software is designed, configured, and deployed with the appropriate features in place.[4]

---

[3] Stephens, *Records Management: Making the Transition from Paper to Electronic* (ARMA, 2007).
[4] Over time, more software will include retention management features if customers demand it. For example, see the Microsoft 365 Purview feature set designed for records retention management.

Digital information may not require warehouse space, but it does require disk space. While the price per terabyte has been decreasing over time, the rate of data volume growth outpaces any savings, especially in cloud hosting services. Holding too much information slows down information access and retrieval, increases the risk of a security or privacy breach. As one expert wryly points out, keeping everything online "turns data management into waste management".[5]

On the other hand, in contrast with paper, digital information can be cost-effectively researched, analyzed and reused. Advocates of information mining argue that it is no longer necessary to enforce a complex matrix of varying retention periods.

COURTS ARE DIFFERENT

Managing retention and disposition in courts is more challenging than in most other organizations for several reasons, some of which are outlined below.

THE COURT RECORD

Courts are not like other organizations. First, "courts of record" are required to preserve the record of proceedings, generally to ensure than an appeal court can effectively perform its review function and other courts can follow precedent.[6] Second, the Court Record is considered a "source of truth'" in the sense that unlike records of other persons or organizations, information upon which the court has acted to make a determination thereby receives an imprimatur of reliability and accuracy. When a court finds a fact in a record of a proceeding to be true on the balance of probabilities, it is generally taken to be true thereafter.

---

[5] Stephens, *supra*.
[6] "The term "record" and other expressions such as "court of record', "on the record", "for the record" are used regularly and frequently in legal parlance and have been for years without, in my opinion, a clear consistent understanding of what those expressions mean." *R. v. H. (K.), Re*, 1985 CanLII 3577 (ON CJ). Per Nevins, Prov. Ct. J.

OPEN COURTS

As public bodies, and in accordance with the open courts principle, courts have a responsibility to ensure that a record of their activities is permanently and publicly accessible.

At the same time, courts are guardians of the copious records submitted by third parties (voluntarily or otherwise), including members of the public and justice partners, some of which are provided conditionally and may be subject to being returned at the end of a proceeding.[7] A great deal of this information routinely contains personal, sensitive, confidential, and privileged information.

INDEPENDENCE

The judiciary is conferred with institutional and individual independence, which adds an important layer of delicate governance and cooperation. The judiciary and executive branch, or other non-judicial administrators, involved with facilities management, human resources, infrastructure or supply, administer Canadian courts jointly. At the same time, any form of court business intelligence that the court finds appropriate to its mandate or capacity, falls into the category of judicial administration. Chief Justices are looking at matters like judgment delay, load balancing, judicial education, judicial conduct, wellness, public outreach and many other issues that are common to courts but not covered by business processes like "human resources." Thus, while court information is subject to broad-based legislation[8] and established government policies, it is also subject to individually negotiated Memoranda of Understandings, judicial discretion and the court's jurisdiction over its process and its records.

---

[7] Different courts have rules respecting access or control of specific documents: see, for example, *MediaQMI inc. v. Kamel*, 2021 SCC 23 (CanLII).

[8] Examples of relevant legislation include Official Secrets, Archives and Public Records, *Criminal Code* and Provincial Offences, Judicature acts, Evidence, Electronic Commerce and Privacy, Freedom of Information or Access to Information.

LEGACY

Courts have long histories, and truckloads of physical records including paper are stored in courthouse basements and suburban warehouses. Costs of storage are high, and the corresponding public benefits hard to quantify.

As courts steadily transform their operations from paper to digital, they are now faced with the novel complications of long-term, cost-effective secure data storage in the cloud.

The purpose of this Model Policy is to assist courts in addressing these challenges, by proposing an innovative, practicable approach to retention and disposition. For some courts this may help in the development of new policy, while for others it may contribute to existing policy amendments.

RECORDS MANAGEMENT IN TRANSITION

Records and information management is amid a decades-long transition from paper to digital. The challenge for all organizations including courts is to manage this transition without compromising the principles and values underlying sound information governance practices.

GLOSSARY

Case File

A Case File contains the Information that relates directly to a single court proceeding or to a number of related court proceedings that have all been assigned the same case file number. It includes the Information that comprises the Court Record and any other Information that has been captured or placed in the Case File.[9]

[9] See Canadian Judicial Council, *Model Definition of Judicial Information* (2020).

Court Record

Information and other tangible items filed in proceedings and the information about those proceedings stored by the court.[10]

Information asset

"An information asset is a body of information, defined and managed as a single unit so it can be understood, shared, protected and exploited efficiently. Information assets have recognizable and manageable value, risk, content and lifecycles."[11]

Information assets include physical information assets (such as paper documents, film, photographic prints) or digital assets stored electronically. An information asset can be a hardcopy document or a box of documents, a spreadsheet, or the contents of a shared network drive; a database, an operating system, an e-filing system or a PDF file uploaded to such a system; a Case File, a Court Record, an email or an entire email account.

Depending on the context, some courts may wish to categorize non-documentary physical evidentiary objects (for example forensic samples) as information assets.

Record

Elsewhere used interchangeably with information asset, in this policy record is used to denote an individual physical document or digital file, including those in the Court Record. Many leading information governance authorities refer to "records", though the broader, more modern and more technology-friendly term "information asset" is emerging. All records are information assets, but not all information assets are records.[12]

Though the definition of record can be expanded to include digital assets, it originates and resonates in the concept of recorded information as a physical object.

---

[10] The use of the terms "Judicial Information" and "Judicial Officer" also conform to the Model Definition paper. See footnote 9.
[11] UK National Archives factsheet.
[12] The conventional definition is provided by way of *ISO 15489 Information and documentation—Records management*, which defines "record" as "Information created, received and maintained as evidence and information by an organisation or person, in pursuance of legal obligations or in the transaction of business."

POLICY STATEMENTS

POLICY 1 – PURPOSE

The purpose of this policy is to ensure that court information assets are systematically preserved for as long as needed, but no longer.

COMMENTARY:

The manner in which the court receives, controls, maintains and disposes of its records is not just a part of the institutional characteristics of the court but is a crucial part of the court's reputation for integrity, accuracy, consistency and reliability in the delivery of equal justice under the rule of law. The systems created must be accessible, intelligible, coherent, explicable, predictable and accountable.

A systematic approach may also:

1. Improve access for practical uses throughout the information life cycle.
2. Minimize time wasted in searching for information.
3. Minimize the risks and costs associated with over-retention.
4. Provide a public rationale for the destruction of information assets that might otherwise be criticized as arbitrary.
5. Guide members of the court who may ask - I am allowed to delete this email? Do we need to keep these duplicate submissions?
6. Ensure compliance with applicable legislation, regulations, rules, court orders, and best practices.
7. Ease the burdens associated with conventional records retention programs by proposing a modern strategy.
8. Ensure that courts robustly address the retention and disposition of digital information, as traditional paper-based practices are not suitable.

9. Reduce unnecessary duplication of records.
10. Improve public access to information of historical value.
11. Preserve the court's legacy.
12. Ensure that confidential or private court information is not inadvertently made public when transferred to a public archive.
13. Eliminate the cost and risk of storing information for longer than is justified.
14. Address capacity limits on the storage of old, low-value paper records.

POLICY 2 – JURISDICTION

The court has jurisdiction over its own information.

COMMENTARY:

The court is sole owner of and is responsible for court information throughout its life cycle. That responsibility includes maintaining continuity, accuracy, and accessibility of the information throughout the retention period.

The information controller has legal control of information assets. This control is divorced from the concept of physical custody or possession.[13] Information controllers (or data owners), define the overarching information policies governing access, use, and retention of information assets.

[13] It is important to bear in mind the distinctions made in the 2013 CJC report: *Court Information Management Policy Framework to Accommodate the Digital Environment*, at page 6: "In a paper based world, possession of a court file is synonymous with control over that file. It was easy for the judiciary to control Case Files in such an environment because an original court file could only reside in one physical location at a time and those with possession of the physical file could easily control the ways in which information within it could be accessed.
In the digital domain however, it is quite possible to have possession of information without control and conversely, it is possible to have control of information without physical possession."

POLICY 3 – SCOPE

This policy applies to all court information assets, wherever those assets may be located and in whatever format or medium they may be transmitted or stored.

Information assets of the court do not include personal information of judicial officers, court officials or staff, which is to be segregated and clearly identified as personal.[14]

COMMENTARY:

This policy is designed to apply to all court information assets irrespective of their format, as the principles of retention and disposition should apply consistently to information based on its context, meaning, purpose, and value.

POLICY 4 – COMING INTO EFFECT

This policy is effective upon its approval by the court.

All information assets must be reviewed prior to [date] and any assets existing beyond the period indicated in the retention schedule must be destroyed within a period to be determined by the court.

COMMENTARY:

Given that the retention periods for many information assets in the custody of courts have already expired, the court must establish a timetable for clearing the backlog, so it is in compliance with its own newly established schedules.

[14] "[Personal papers … are unrelated to an organization's mission, goals, objectives, or business operations or to an employee's assigned duties. They are information-bearing objects of a private nature. … These items are the personal property of their creators and are consequently excluded from records management authority." Saffady, *Records and Information Management Fundamentals of Professional Practice* (4th edition, 2021) at p. 6.

POLICY 5 – INFORMATION ASSET REGISTER (IAR)

The court must prepare and update an Information Asset Register (IAR) that lists, briefly describes, and categorizes at a high level, all court information assets.

COMMENTARY:

The IAR forms the basis not only for decisions about retention scheduling but is also the foundation of a threat and risk assessment, the security classification of court information, and business continuity procedures. It is the first step to gaining control over court information.

The descriptive elements of the IAR should be determined in accordance with the volume of information in the court, and the state of the court's transition from paper to digital. Key elements to consider for each asset would include:

1. Relevant category
2. Brief description including the asset's purpose and use
3. Date range
4. Controller (with contact information)
5. Custodian (with contact information)
6. Users, including internal and external sharing relationships
7. Location – cloud, on premise, database, repository
8. Form – paper, digital, other medium
9. Should this be a designated asset? See Designated Asset policy here.
10. Information Sensitivity - for example, copyright, privacy, confidentiality

Current thinking in the information governance profession is that larger, more inclusive groupings, with longer retention periods, makes more sense for digital information, which is dynamic and often stored in unstructured repositories rather than filed in discrete folders. The more detailed or granular the IAR – for example a listing by document title, the more assets need to be listed and tracked individually.

The IAR therefore should be structured with the broadest possible categories of information, grouped by function, user group, purpose, or repository.

POLICY 6 – DESIGNATED ASSET

Where duplicate copies of information assets are stored in multiple environments such as email inboxes, shared folders on file servers, cloud databases, local hard drives or mobile devices, the court may designate one of these as authoritative (and subject to the court's retention schedule), in which case copies of the duplicate assets in the other repositories are considered transitory and may disposed of accordingly.[15]

COMMENTARY:

One of the features of digital information is the ease with which it is copied, distributed and otherwise shared. This places an unnecessary onus on individuals or business units to manage and retain duplicate information assets. For example, a court's e-filing database may be designated, in which case duplicate copies of e-filed material uploaded for a virtual hearing may be deleted when no longer needed, assuming the files have not been annotated or the content otherwise altered.

POLICY 7 – ASSET APPRAISAL

To determine appropriate retention periods, the court must appraise its information assets using methods that are cogent, cost effective, and appropriate for the court's circumstances.

The ability to properly appraise information assets will be much assisted where the structure under which the court receives, controls, maintains and disposes of its records involves systems for auditing the records regularly when in place to ensure the records are being properly preserved, verified and secured.

[15] Transitory records are "records of convenience" which may be deleted when they are no longer needed by the user. There is no fixed retention period for transitory records.

Similarly, the ability to appraise information assets will be much improved if the court has a full and integrated scheme for court business intelligence derived from the records and their handling by the court.[16]

When appraising information assets, the court will consider factors including:

1) Applicable laws and orders
2) The operational needs of the court
3) The impact on the administration of justice
4) The legacy of the court
5) The needs of parties and justice partners
6) The public interest

COMMENTARY:

There are three main appraisal methodologies in use. The conventional method is a file-by-file review, now considered obsolete and impracticable given the volume and nature of digital information assets.

A more modern approach is "macro appraisal." This method is consistent with a high-level IAR and involves an understanding of the court's mission, its history, and its structure. For some courts, a functional methodology may be more fitting. Like the macro approach, it focusses on the organization, but at a business unit, activity, or transactional level (i.e., the level at which most records are created). This analysis provides a better context for the asset, through which its meaning and value can be ascertained.

The main aspect of this approach is to analyze and understand the functional context in which the records were created – a functional analysis. Kelvin Smith, in his book *Public Sector Records Management*, summarizes the importance of appraisal thus:

> *Records appraisal must not be an ad hoc exercise. It should not be undertaken in a hurry when the quantity of records has outgrown the storage space available or*

[16] Audit and court business intelligence regimes are beyond the scope of this policy and hence not elaborated upon here, but such regimes are of considerable value to an effective and secure court operation.

> *when an organisation has to move to new accommodation. If it is done in such an unplanned, non-systematic manner, the wholesale, uncritical destruction of records may take place. Similarly it is often the case that records are examined item-by-item in order to separate current, semi-current records and non-current records – a very time-consuming exercise. Some of the non-current records may then be offered to an archival institution for appraisal to determine whether any of the records have historical value. The archival institution then has to review these records without the necessary contextual information about their origins or purpose. All of these scenarios are extremely wasteful of resources.*[17]

Assets of Historical Value

The decision to designate assets as historical is often subjective. Differences of opinion may arise when stakeholders are consulted. In the recent Federal Court notice, the preamble explains that "The great majority of Court records are never consulted after being sent to the Court's archives." This may be, as implied, because they are not of much historical value after all. On the other hand, mountains of paper records are difficult to find, time consuming to review, and very difficult to compile into meaningful statistics. Digital archives provide a much better opportunity for future researchers, and courts cannot today anticipate easily how and what data will be used a hundred years from today.

The International Criminal Court assesses historical value based on the asset's "use in the future for the purposes of supporting any sort of legal dispute or reconstructing the general history of the development and governance of the Court and its legacy."[18] The court may consider information shedding light on the development or organization of the court, or its impact on the community, as having historical interest.

---

[17] Smith, *supra* at p. 110.
[18] International Criminal Court, *Records retention and disposal policy* (2015).

POLICY 8 – RETENTION SCHEDULE

All court information assets are subject to a retention period as defined by the court for each category of asset.

A retention schedule setting out these periods must be published on the court's website. The court may retain any information asset after the expiry of its designated retention period should the court find it necessary to do so.

COMMENTARY:

Retention schedules must be carefully crafted by professionals in consultation with court staff, court officials, legal counsel and the judiciary. If the court's information assets are broadly defined in the IAR, then the number of different retention periods is accordingly minimized. Lengthy, complicated registers are difficult to update, complicated to explain, and therefore at risk of non-compliance. Drastic simplification is the key to compliance.[19]

Default guidance is provided in some courts. For example, the International Criminal Court provides:

1. Transitory assets must be destroyed in two years
2. Operational assets must be destroyed ten years from the date of last active use
3. Legacy assets – those of historical value – are retained permanently.

The Federal Court recently provided its guidance in an effort to reduce the cost of permanent retention:[20]

1. Court information that was ***not*** adjudicated on the merits – destroyed in seven years (with some enumerated exceptions)
2. Court information that ***was*** adjudicated on the merits – destroyed in fifteen years (with one exception)

[19] A reduction of 80% in the number of categories of information assets is not unexpected, according to some experts. For example see Kahn, "*The Incredibly Compelling Case to Rethink Records Retention in 2018 and Beyond*" (Business Law Today, American Bar Association 2018).
[20] Document Retention Schedule pursuant to Rule 23.1 of the Federal Courts Rules (2021).

POLICY – 9 TRIGGERS

Where trigger event dates cannot be tracked automatically, the court should set a reasonable retention date based on the time the asset is received, created, or last accessed.

COMMENTARY:

Trigger dates based on the expiration, termination, or completion of a process, such as the final determination of a matter and the expiry of any period for review or appeal, may be necessary but can complicate the calculation of retention periods if they cannot be tracked automatically.[21] Manual tracking is difficult and leads to non-compliance.

POLICY 10 – RETENTION BY DIGITIZATION

Requirements for retention of information assets in paper form are satisfied by retention of a reliable digitized or microfilmed copy.

COMMENTARY:

Digitization of high-value information assets is highly recommended, as it can serve to reduce long-term costs of paper storage; provide a critical backup and offers an opportunity to readily encrypt sensitive information that would otherwise be difficult to protect from unauthorized access.

Digitization of paper records, if used as a method of retention, requires attention to the quality control process to ensure that the digital version is reliable and that contextual information about the hard copy is maintained as metadata after the paper is destroyed.

Local standards may be adopted if available, such as the Digitization Standard from Service Alberta. A Canadian standard, CAN/CGSB-72.11-93, was withdrawn but contains many useful guidelines for preserving the integrity of digitized records. It has been replaced by the less

[21] Analysis of the matter type may be required to properly document the applicable trigger date. For example, in some courts the trigger for child support cases is tied to the age of the minor involved – that is, their period of dependency.

detailed CGSB 72.34-2017, Electronic Records as Documentary Evidence, and in French Enregistrements électroniques utilisés à titre de preuves documentaires. Other resources include those from Library and Archives Canada and ISO, the International Organization for Standardization.

POLICY 11 – DIGITAL VERSION AUTHORITATIVE

Unless legislation or a court order provides otherwise, digital forms of information assets are authoritative.

COMMENTARY:

Paper documents that have corresponding electronic files, for example computer printouts, are transitory records that may be destroyed when no longer needed for active use.

Paper records can be destroyed when their retention period has been reached or if they have been digitized to an appropriate standard of quality.[22]

POLICY 12 – LONG-TERM PRESERVATION

The court must take proper steps to ensure the preservation of its information assets in all forms, where the assets are scheduled for long term or permanent retention.

If there are known issues with asset integrity during a migration, and these issues cannot be mitigated, they should be carefully documented. Data migration must be planned and tested in such a way as to ensure the integrity of all content and metadata.[23]

[22] For guidance see Library and Archives Canada, *Destruction of Source Records following Digitization*.
[23] ARMA International TR22-2016 defines "metadata" as "The structured information that describes, explains, locates, or otherwise makes it easier to retrieve, use, or manage information resources."

COMMENTARY:

Significant volumes of data will need to be meaningfully preserved by courts beyond the typical lifecycle of the technology used to store them. Systems become obsolete quickly, and the pace of change increases over time. Many courts today are undergoing a major platform replacement as they move information from local servers to the cloud. Custom-built case management systems developed fifteen or more years ago are being replaced with commercial off-the-shelf solutions. If a court is required to keep certain assets for, say, fifteen years, it will most likely need to be migrated, converted, or otherwise refreshed at least once.[24] Conversion to archival formats such PDF/A are partial solutions, as original metadata can be lost, and these formats are only suitable for certain types of document-based assets.[25]

POLICY 13 – DISPOSITION

At the end of their retention periods, the court must promptly dispose of information assets either by secure destruction, by transfer to a storage or archive facility, or by returning them to the parties from whom they were received.

POLICY 14 – CONFIDENTIALITY

Arrangements for the conversion, retention or disposal of Court Information that are sealed or otherwise deemed confidential must preserve the level of protection and non-access required by law.

---

[24] MoReq 2010 (Modular Requirements for Records Systems) at p. 23 suggests that typically, organizations refresh their technologies every 3-5 years.

[25] There are several useful references for long-term preservation, including ISO/TR 18492:2005, Long-term preservation of electronic document-based information; ISO 19005 series.), Storing Data For The Next 1000 Years (Tom's Hardware), and many others including for example the Minnesota State Archives.

POLICY 15 – DISPOSITION BY TRANSFER

Information assets scheduled for long-term or permanent preservation may be transferred to the custody of an approved third-party entity. The court must adopt effective transfer protocols for long-term accessibility and security of information assets.

COMMENTARY:

The court should follow professional guidelines such as Guidelines on File Formats for Transferring Information Resources of Enduring Value published by Library and Archives Canada.

POLICY 16 – DESTRUCTION

Information assets may only be deleted or destroyed in accordance with the approved retention schedule and procedures.

The court ensures that information assets scheduled for destruction are disposed of in a manner that protects sensitive information and renders it unrecoverable.

Where the destruction has been carried out by third parties, written certification of such destruction should be obtained.

The court must maintain a listing of all scheduled assets destroyed. Such listing must include the category of assets from the retention schedule, a brief description of the assets, the date range during which the assets were created, the date of destruction, and the method used to destroy the assets.

COMMENTARY:

The court may classify certain types of information or data, such as personal Judicial Information, draft documents, or other things, as being subject to discretionary deletion or removal by the Judicial Officer or senior court official involved.

Deletion or removal of any specific information may be reversible or irreversible, depending on the established policies of the court. Where information is deleted or removed, a record should

be kept as to the nature of the information, the policy justifying its deletion or removal, and the date of its deletion or removal unless those policies provide otherwise.

Some courts require that notification to the affected parties be provided, depending on the nature of the assets.[26]

POLICY 17 – LEGAL HOLD

Any information subject to a lawful information access request or likely to be subject to a legal proceeding should be retained until the matter is resolved, even if its retention period has expired.

COMMENTARY:

The routine destruction of information assets at the expiry of the retention period should be paused if there is a risk of non-compliance with a lawful request for such an asset. An investigation into judicial conduct, a lawsuit by or against a contractor or supplier, or a statutory access request are examples of triggers that may, in the opinion of the court, justify a legal hold.

POLICY 18 – SENIOR COURT OFFICAL

The court must appoint or designate a senior court official accountable to the court and responsible for implementing and enforcing this policy.

The retention-related duties of this senior official would include:

1. Implementing the policy
2. Developing the IAR and retention schedules, and updating them periodically
3. Training users and system administrators and advising the court on information governance issues

[26] For example, see Document Retention Schedule pursuant to Rule 23.1 of the Federal Courts Rules (2021).

4. Contributing to systems procurement activities to ensure that court systems are compatible with automated retention processes

COMMENTARY:

The senior court official handles the administrative tasks associated with the implementation of information governance policies, including retention and disposition.