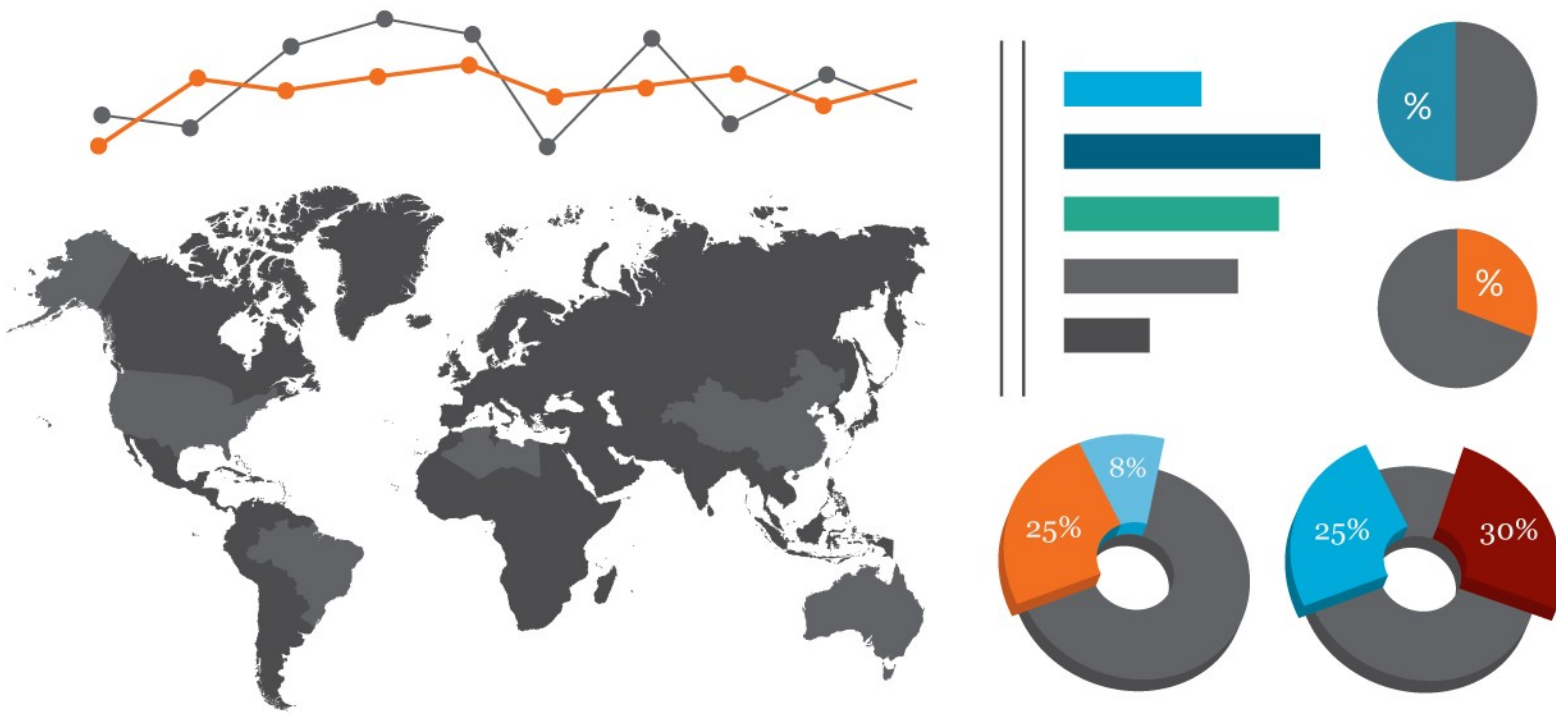


# Information Governance Process Maturity Model



Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or purposes. Time limits should be established by the controller for erasure or for periodic review.

— Regulation (EU) 2016/679 of the European Parliament and of the Council, 27 April 2016

## About CGOC

CGOC (Compliance, Governance and Oversight Council) is a forum of over 3,800 legal, IT, privacy, security, records and information management professionals from corporations and government agencies. CGOC publishes reference guides and articles and conducts primary research. Its Benchmark Reports have been cited in numerous legal opinions and briefs and its ILG Leaders Guide has been widely referenced and adopted by organizations. CGOC members convene in small working groups, regional meetings and its annual strategy summit to discuss information governance and economics, eDiscovery, data disposal, retention, and privacy. CGOC has been advancing governance practices and driving thought leadership since 2004. For more information go to [www.cgoc.com](http://www.cgoc.com).

Written by Heidi Maher, Esq and CIPM, CGOC Executive Director and Jake Frazier Esq and CIPP/US, CGOC Faculty Chair. Special thanks to Deidre Paknad, CGOC Founder and Rani Hublou, CGOC Faculty.

© Copyright CGOC Forum LLC, 2017.

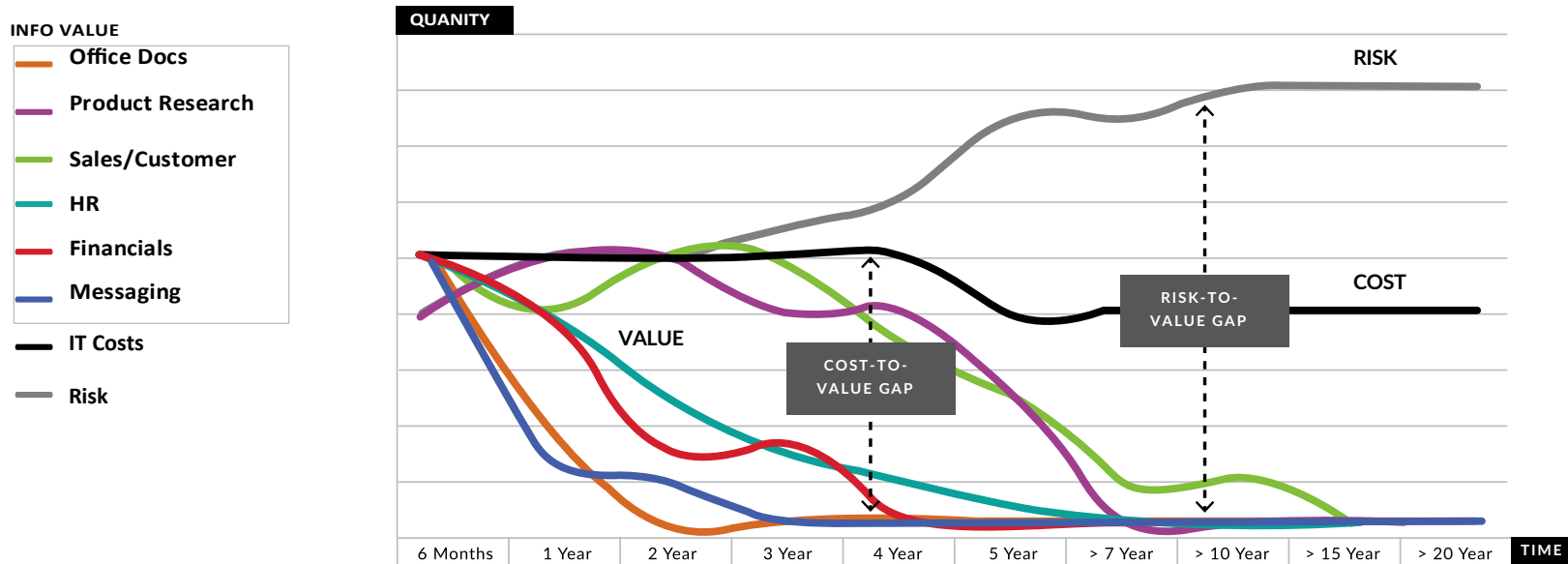
The information contained in this publication is provided for informational purposes only. While efforts were made to verify the completeness and accuracy of the information contained in this publication, it is provided AS IS without warranty of any kind, express or implied. Nothing contained in these materials is intended to, nor shall have the effect of, state or imply that any activities undertaken by you will result in any specific sales, revenue growth, savings or other results. Do not copy, cite or distribute without permission of the CGOC.

For inquiries, please contact us at [cgoc@cgoc.com](mailto:cgoc@cgoc.com) or go to [www.cgoc.com](http://www.cgoc.com) for more information. Information Governance Process Maturity Model

July 2018

# Improving Information Economics and Defensible Disposal of Unnecessary Data

Improving information economics is imperative for most organizations. As information volume rises rapidly, business users face greater challenges to extract value, IT costs for basic infrastructure rise beyond budgets and legal risks and cost increase as well. To make way for new and more useful information, ensure businesses get value from data, control IT and legal costs and lower risk and exposure, companies should dispose of unnecessary data debris. As information ages, its value declines. Unfortunately, the cost to manage it is relatively constant and eDiscovery costs and risks rise with time. When information is no longer needed, information “supply” exceeds information “demand”. This creates a widening gap between the value the information provides an organization and its cost and risk. Closing these gaps is important to legal, IT, security, privacy and business stakeholders. When processes and stakeholders are siloed and operate without a high degree of interlock and transparency, it is very difficult to tie actual need for information (demand) with information assets (supply).



**BUSINESS** Information volume will double every 2 years, reaching 180 zettabytes by 2025

90% of the world's data had been created in the last 12 months<sup>1</sup>

**LEGAL** It costs \$18,000 to do eDiscovery on 1 gigabyte<sup>2</sup>

eDiscovery consumers as much as half of the litigation budget

**IT** \$2.5M/per year to store 1 PB plus cost significantly add to run rate

Data storage consumers growing share of budget; sunsetting too slow

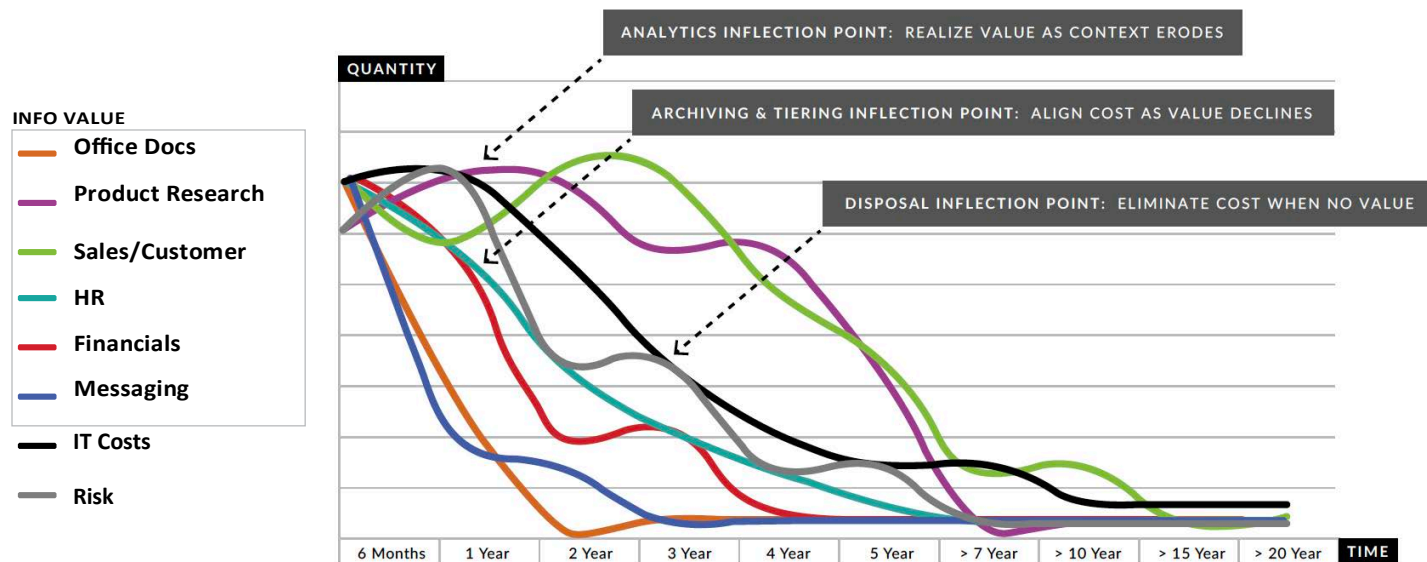
**PRIVACY AND SECURITY** Average cost of a data breach is \$3.86M

The average cost paid for each lost or stolen record containing sensitive and confidential information is \$148<sup>3</sup>

<sup>1</sup> IBM Marketing Cloud Report “10 Key Marketing Trends For 2017”

<sup>2</sup> Report from Rand Institute for Civil Justice

<sup>3</sup> Benchmark research sponsored by IBM independently conducted by Ponemon Institute LLC June 2018



**Three critical inflection points in information lifecycle drive value, cost and risk:**

1. Analytics to maximize value as context erodes
2. Archiving and tiering to ensure cost declines as value declines
3. Disposal to ensure that when need is gone, there is no remaining cost or risk

**Information lifecycle governance improves information economics for business, legal & IT**



**Leverage information for better decisions and higher revenue**

Don't waste budget on unnecessary IT or legal services



**Meet eDiscovery obligations cost effectively and efficiently for the enterprise**

Manage conflicting privacy and regulatory



**Minimize "run the shop" costs to increase investment in "grow the firm" activities**

Cut total costs even as total volume rises

To improve information economics and enable defensible disposal of data debris, organizations need to understand and optimize twenty-two processes that determine information value, cost and risk. An organization's process capabilities and maturity determine its ability to understand and extract information value, align cost to value over time, minimize information and legal risk and lower total IT and legal costs.

This CGOC practitioners model helps organizations understand and assess their process capabilities and current process risks; tools like the ILG Leaders Guide provide a roadmap to optimizing processes to improve information economics.

# Processes Capability and Maturity

A clear understanding of process maturity levels and your organization's current process capabilities and practices will help frame the work effort and change management required to improve information economics and achieve defensible disposal. The twenty-two information maturity processes incorporate the way an organization defines demand (what information is needed, why and for how long) and how it manages supply (what is provisioned, managed, decommissioned, and disposed).

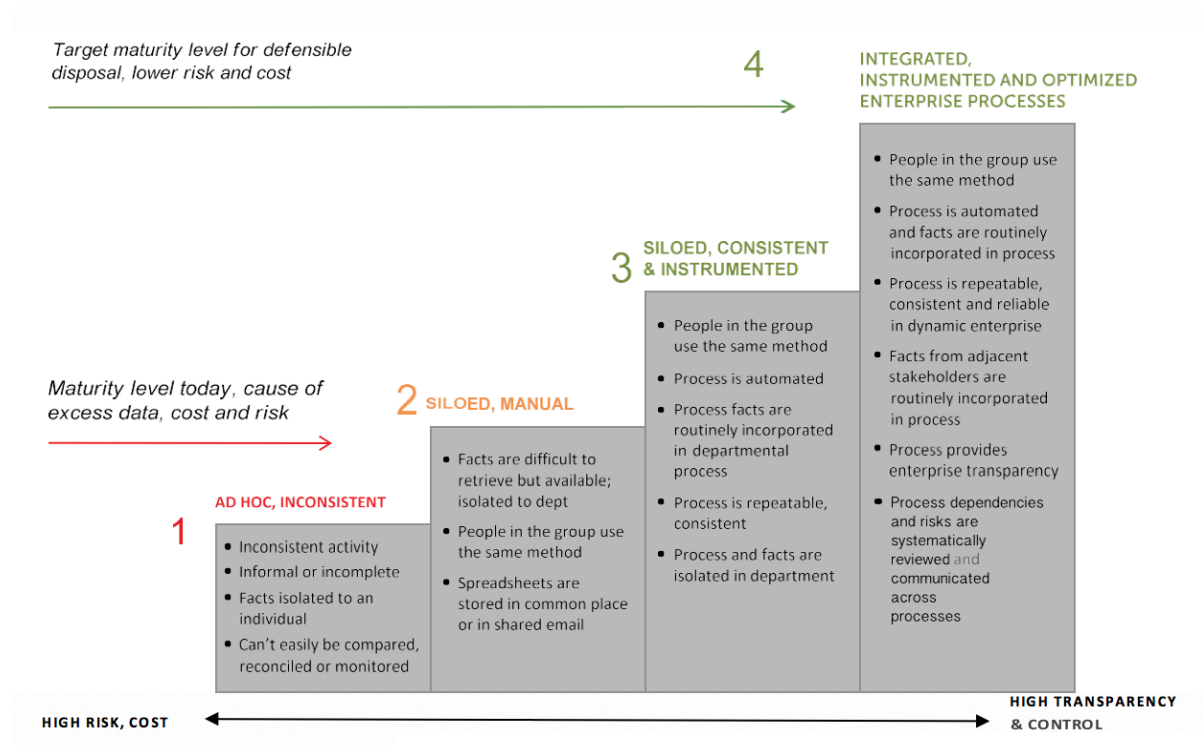
At the highest level of maturity and capability, there is a closed loop between supply and demand, information cost is aligned with its value over time and risk is limited or removed. More precise and rigorous legal holds and retention as well as consistent, defensible disposal are designed into processes at maturity level 4.

**Level 1** is an ad hoc, manual and unstructured process performed differently by each practitioner. Only the individual practitioner has access to the process facts or results. These processes are highly unreliable and difficult to audit.

**Level 2** is a manual process with some consistency in how it is performed across practitioners within a particular function or department. Only the department has access to the process facts and results, and often these are embedded in multiple spreadsheets and seldom accessed. These processes can be more reliable, but still very difficult to audit.

**Level 3** is a semi-automated process performed consistently within a department with process facts and results readily accessible to departmental stakeholders. Stakeholders beyond the department who participate in or are dependent upon the process are not integrated. These interdepartmental processes are more consistent and can readily be audited. However audit results may reflect their lack of intradepartmental collaboration.

**Level 4** is an automated and cross-functional process that is performed consistently with inclusion of dependent stakeholders across multiple departments. Process facts and results are readily available across organizations. These processes have the lowest risk, highest reliability and are readily and successfully audited.



# Roles and Responsibilities

A cooperative relationship is needed among stakeholder groups to achieve the desired level of information governance maturity. This shared ownership and execution of IG processes ensures that accountabilities and dependencies across the stakeholders are clearly defined by each group to promote efficient and effective management of information. As a part of the process maturity and improvement effort, responsibilities for each process owner should be defined to reflect the level of maturity, integrity and reliability required to achieve the cost and risk reduction goals.

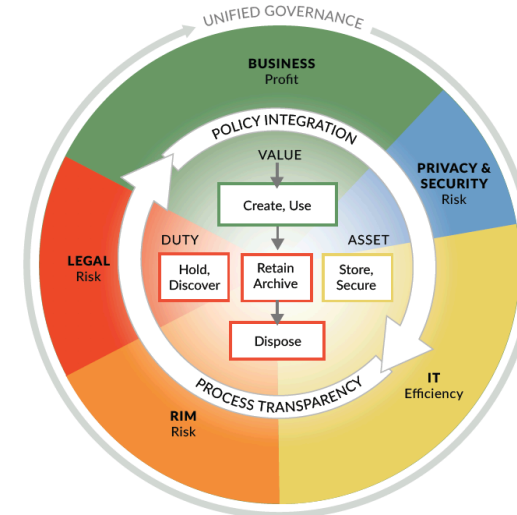
## Information Governance Reference Model (IGRM)

Linking duty + value to information asset = efficient, effective management

**Duty:** Legal obligation for specific information

**Value:** Utility or business purpose of specific information

**Asset:** Specific container of information



Information Governance Reference Model / © 2012 / v3.0 / edrm.net

### To support the objectives of the IG Program, the Legal organization will:



- Maintain an accurate inventory of legal obligations for information by case and scope of obligation including individuals involved, information scope (dates, terms, elements), and relevant records. The inventory should indicate whether the duties have been satisfied fully or partially and how.
- Precisely and timely define and clearly communicate specific requirements to preserve potential evidence to IT, records and business stakeholders for each matter including the individual employees, records and ranges of data that must be preserved as potential evidence.
- Provide real-time, continuous transparency to current legal obligations for information that can be readily understood and acted upon by stakeholders in IT, records and business units.
- Affirmatively communicate to and receive confirmation of compliance from employees, records managers or IT staff are relied upon to preserve information in their custody.
- Ensure the defensibility of its process through complete, accurate, timely record keeping and closed loop communications with custodians, IT and records staff.
- Enable defensible disposal of information through precise, consistent and timely communication of obligations to individuals, IT and records staff when the duty arises and as it changes over the course of a matter.
- Work with Internal Audit to assess enterprise preservation procedures.



**To support the objectives of the IG Program, the Records organization will:**

- Author and distribute a records management policy and provide training materials to employees or contribute content to corporate ethics training program.
- Provide an information taxonomy that can be reliably used across business, IT and legal stakeholders to define and characterize business information and information required for regulatory obligations.
- Maintain an inventory of regulatory requirements for records updated annually and identify which laws apply to which classes of information by country or jurisdiction and business area.
- Provide actionable retention schedules that can be routinely and automatically applied by IT and business stakeholders on electronic information to ensure proper record keeping.
- Maintain a network of records liaisons across the business to coordinate and communicate policy, taxonomy and schedule needs and changes; provide management visibility on liaison status
- Safeguard information of value to the business. Perform consistent, documented and precise collection and disposal (or cause to be collected and disposed) of electronic and physical records, regardless of their form, in accordance with the schedule.
- Ensure timely response to regulator inquiry, enable Internal Audit to test records and retention procedures on physical and digital records.



**To support the objectives of the IG Program, the IT organization will:**

- Retain and preserve information based on its value to the business and legal obligations and according to procedures/instructions provided by legal, RM and business, including aligning technique and technology to value.
- Dispose of information no longer needed to lower information costs and related risks.
- Author and follow backup and disaster recovery policies that limit the retention of backup media to the shortest necessary period to effectively recover from a disaster or failure.
- Maintain an inventory of systems with current business value retention, record requirements and legal hold obligations for data contained in said systems or stores and ensure that staff involved in provisioning and decommissioning have access to this inventory in the course of their work.
- Establish and provide a common data dictionary for organization and department, data source, employee, information classification, system classification, law, lawsuit for use by legal, records, business and IT in the governance program execution.
- Provision new systems, servers and storage with automated or manual processes for imposing retention, preservation and disposition of information in the ordinary course of operation (revise SLDC policies, procedures).
- Align systems and stores with the value of information contained in them, including security, privacy, confidentiality, regulatory, business, and litigation requirements.



- Develop protocols for disposal of data and protocols for storage and disposal of customer data and PII (in concert with information security and privacy stakeholders).
- Enable Internal Audit to test retention/disposition, preservation/collection and privacy procedures.
- Ensure that safeguards around information governance are applied to non-traditional procurement and provisioning channels such as cloud services.



**To support the objectives of the IG Program, the Lines of Business will:**

- Ensure a business liaison for governance is able to participate in the Program and its processes.
- Using online tools and taxonomy provided, participate in a bi-annual value inventory to articulate what information is generated by business teams or departments and the duration of its value to enable IT, records and legal stakeholders to manage accordingly.
- Work in concert with IT to optimize the archiving and storage of information based on its utility and management cost in the interest of shareholders, regardless of charge back procedures.
- As business processes and practices change, proactively initiate changes to the taxonomy, records and value procedures to reflect business practices and needs.
- Enable timely disposal of information without value and active participation in the governance program via business leader transparency and accountability for the total unit cost of information (its storage, management and eDiscovery).
- Participate in Internal Audit on business value inventory procedures.
- Ensure data is accurate and fit to serve the business or compliance purpose by controlling data from its trusted original source and form throughout its usage by other applications.




**To support the objectives of the IG Program, the Privacy and Security organization will:**

- Establish a catalog of privacy laws and policies that is accessible to litigation, records and IT staff.
- Align with RM to associate privacy requirements during retention of records and business information.
- Coordinate with litigation in advance of data preservation and collection to ensure that appropriate measures are used for data subjects and jurisdictions.
- Require education and training to employees on relevant privacy obligations and best practices for securing information.
- Create a framework for deterring, thwarting and identifying bad actors attempting to gain access to enterprise or unauthorized data.
- Enable Internal Audit to effectively test privacy and security procedures.





	Process	Brief Description	Process Risk or Immaturity or Consequences	Level 1: Ad Hoc, Manual, Unstructured	Level 2: Manual, Structured	Level 3: Semi-Automated Within Silo	Level 4: Automated and Fully Integrated Across Functions
<b>A</b>	<b>Employees on Legal Hold</b>	Determining employees with information potentially relevant to an actual or anticipated lawsuit or government investigation.	Custodians are not identified and potentially relevant information is inadvertently modified or deleted.	Multiple custodian spreadsheets managed by the individual paralegal or attorney.	Custodian lists are kept in Word or Excel in a shared location or in a shared mailbox. Questionnaire mailed to custodians, responses, compiled manually for collection/ counsel follow up.	Systematic scope and selection by organization, people from current and historical organization data. Systematically track all custodians in all holds including multiple holds per custodian. Scope terminated/transferred employees involved. Interviews are systematically done, responses compiled and responses are automatically flagged and escalated as appropriate.	Real-time update of custodian roles, transitions, responsibilities, automatic employee transition/transition alerts by attorney and matter; copy or cross reference custodian lists across similar matters. Scope is revisited and refined at least quarterly to release or include custodians. Individual responses to interview questions are propagated to hold scope and interview results shared with outside counsel to interview by exception.
<b>B</b>	<b>Data on Legal Hold</b>	Determining information, records and data sources that are potentially relevant to an actual or anticipated lawsuit or government investigation.	Actual, rogue or IT managed data sources missed in hold execution; potentially relevant information is inadvertently modified or deleted.	Limited collection from data sources, custodian rather than information based; spreadsheet tracking/ lists.	Identify data sources by organization; understand back up procedures. Questionnaire emailed to custodians, responses compiled manually for collection/counsel follow up.	Have linked legacy tapes and data sources to organizations and open holds/ collections.	Automatically scope people, systems, production and backup data, information and records in holds; scope terminated employee data and legacy data/tapes where applicable. Scope is revisited and refined at least quarterly to release or include data. Can scope directly from a data source catalog shared with business liaisons, IT, Info Sec and other data quality stakeholders with reliability. IT interviews are done both periodically and in matter context and responses are aggregated for individual matters and across the legal team.
<b>C</b>	<b>Hold Publication</b>	Communicating, syndicating and executing legal holds to people, systems and data sources for execution and compliance.	IT or employees migrate, retire or modify data because they lacked hold visibility.	Manual notices, confirmations, no escalations. Description of information hold requires interpretation and manual effort to comply.	Centralize reply email box for confirmations, process well communicated, all holds on intranet.	Systematically send notices and reminders, require and track confirmations, ability to manage exceptions, employees can look up their holds at any time. Communications tailored to recipient role (IT, RIM, employee).	Publish to system, propagate hold, automate hold enforcement. IT Staff have continuous visibility to current discovery duties, holds during routine data management activities; automatically flag records in appropriate systems. Holds are timely released and release syndication is done with same rigor as hold syndication.
<b>D</b>	<b>Evidence Collection</b>	Fact finding and inquiry with employees with knowledge of a matter in dispute to determine potentially relevant information and its whereabouts and sources. Collecting potential evidence in response to an agreed-upon request with an adversary or government agency.	Dynamic, diverse information facts not considered in preservation and collection planning and data is over-looked; no follow through on information identified in custodian interviews. Collection failure from over-looked source, departing employee, incomplete prior collection inventory, communication and tracking errors.	Duplicate spreadsheets of custodians and information in IT and Legal; multiple copies of collected data.	Centralized, version controlled spreadsheets of custodians and information; evidence server organized by matter folder but no inventory by custodian and data.	System log of collection requests by matter, issuer and collector. Collection logging is done by discovery staff in a shared system. An inventory of evidence is well managed and not overlooked in scoping other matters. Interview results and insights are used to inform the collection activity.	Interview results are automatically incorporated into custodian or data source specific collection instructions without rekeying. IT or collection staff can efficiently and automatically collect by custodian and content without re-logging the request or recollecting the same data. Collection data and chain of custody is automatically logged. IT and legal share complete transparency on collections, and legal can monitor progress and process while IT can process work by custodian or data source efficiently. Evidence is not duplicated in multiple locations and it is timely disposed.

	Process	Brief Description	Process Risk or Immaturity or Consequences	Level 1: Ad Hoc, Manual, Unstructured	Level 2: Manual, Structured	Level 3: Semi-Automated Within Silo	Level 4: Automated and Fully Integrated Across Functions
<b>E</b>	<b>Evidence Analysis &amp; Cost Controls</b>	Assessing information to understand dispute and potential information sources and for determining, controlling and communicating the costs of outside review of relevant information.	Material issues in dispute are poorly understood until after strategy established and expenses incurred. Excessive data causes litigation costs to exceed dispute value.	Over collect from custodians, over scope custodians. No culling of clearly irrelevant information before sending to vendor or outside counsel. Don't assess costs prior to collection and review; no cost baseline available.	High quantity of data for review. Some basic processes for culling of irrelevant information by basic means such as date ranges used in some cases. Estimate costs on the "big matters" in spreadsheets or by outside counsel.	Quantity of data reviewed from tightly scoped custodians, leveraging prior scoping histories. Consistent & enforced culling performed by preferred vendors utilizing objective criteria such as keywords, date ranges, file types, domain names & data sources. Discovery cost forecasts available as the hold is scoped, costs are calculated continuously.	Consistently limit scope of collection and review; early case assessment performed before collection for earliest/optimized matter resolution, advanced culling techniques employed leveraging visual analytics; defined & repeatable process for providing outside counsel early case assessment before processing, manage cost at portfolio level.
<b>F</b>	<b>Legal Records</b>	Documenting the custodians and data sources identified the legal hold and collection activities over multi-year matter lifecycle.	Unable to readily assemble, understand or defend preservation and discovery record. Failures in custodian and data source management. Preservation, collection detected long after occurrence and cause unnecessary remediation cost and risk.	Each attorney tracks his or her own matters, status.	Formal, but manual reporting of open holds; no summary reporting on interviews, collections, response.	Automated reminders and escalations, online audit trail, management reporting on discovery status, visibility within legal department across custodians, collected inventory and matters.	Appropriate visibility across IT, Legal and Business; self-service dashboards for legal obligations, tasks, risk and cost reduction opportunities.
 <b>G</b>	<b>Information Retention and Disposal Obligation</b>	Defining an information classification schema that reflects the organization structure; cataloging, updating and mapping the laws that apply to each class in the countries in which the organization operates to determine regulatory record keeping obligations; establishing and managing a network of records liaisons to ascertain the existence and location of records.	Unable to comply or demonstrate compliance with regulatory record-keeping obligations. Disparate nomenclatures for records make application of retention schedules/procedures difficult to apply and audit.	Retention periods defined only for physical records. Record keeping requirements based on aggregations of similar laws and longest retention period.	Master retention policy updated to reflect physical and electronic records. Policy and schedules posted to a centrally accessible site. Jurisdictional schedules share a common taxonomy. Ability to update aspects of the policy and schedules on a regular basis.	Established retention period for regulated information. The specific or actual laws that dictate retention periods are known and clearly mapped to each record class so changes can be easily traced and decisions readily defended. Posted policy and schedules are role specific so that individuals can determine their obligations. Electronic and physical records are both retained and disposed against the schedule. Disaster recovery, retention, and preservation are all disentangled and severable in policy and practice.	Retention schedules reflect regulatory, policy and business value and encompass all forms of information enabling them to be executed on records repositories, application and archived data, backup media and physical records. Legal holds can be applied by record class and suspend automated disposal. There is a shared library of country protocols for eDiscovery, privacy, and retention to form a comprehensive view. Schedules align with and are systematically used to dispose of production and back up data whether structured, unstructured, electronic, physical, record or business information.
<b>H</b>	<b>Departmental Information Practice</b>	Using an enterprise information taxonomy, cataloging what information each business organization values, generates or stores by class, where they store it and how long it has utility to them; results in retention schedules for information and enables data source-specific retention schedules that reflect both business value and regulatory requirements.	IT 'saves everything' which increases discoverable mass, complexity and legal risk; IT disposes of information of business value undermining enterprise operation. Procedures for retention/disposal difficult to articulate and defend and unapplied by LoB.	Departmental information management needs and habits for electronic and physical information are not visible to records management, IT or legal stakeholders (who have no knowledge of actual procedures, information, location, use or value).	Inventories of departmental information management practices and source information are used to develop retentions schedules and coordinate physical records (via a network of records coordinators focused on physical records management).	Departmental liaisons work with their line of business to identify information of value, its duration of value and where it is managed; this informs more comprehensive retention schedules for all information (regulated, unregulated, electronic, physical). Business is able to request changes to master schedule and department/ country schedules at the rate of business change.	Retention schedules are automatically executed across the information environment. Cost and benefit are weighed in determining retention periods and the enterprise impact is considered. Schedule changes are syndicated to IT and directly to systems for execution of both retention and disposition. When business objectives or laws change, schedules are updated and stakeholders notified. Legal and IT have transparency to what information each line of business has where and for how long to inform eDiscovery and data management.

	Process	Brief Description	Process Risk or Immaturity or Consequences	Level 1: Ad Hoc, Manual, Unstructured	Level 2: Manual, Structured	Level 3: Semi-Automated Within Silo	Level 4: Automated and Fully Integrated Across Functions
I	Realize Information Value	Gaining timely access to and ability to apply information in the course of their work, including the ability to harness information of quality as it ages and the ability to use relevant information with or without author context to maximize the enterprise value of information.	Important business decisions are made on missing information or poor quality information, resulting in poor decisions. Information is not used shortly after its creation because business has forgotten the source or location of information or can't find it, resulting in cost without corresponding value.	Information is difficult to retrieve or search. After creator loses initial context, it is forgotten and no value is realized. Staff must mine, open and view files on their individual drives to find what they need and access to relevant information they didn't create is exchanged via email.	Information for a group is organized in shared drives and collaboration sites. Employees must search multiple drives and collaboration sources to find what they need; relevant information is extracted by opening multiple files, emails, documents or reports; structured and unstructured data must be harvested separately and manually correlated.	Application data and business process data can be searched by departmental staff in the course of their work from within the system.	Search and analytics enable employees to realize value and to apply information to decision-making in real time even as context erodes across information sources and types; assertions on value and sources of information made in processes H, I and J are used to ensure accessibility and authenticity of information the business defined as valuable. The cost of information to the enterprise is consistent and appropriate over its lifecycle.
J	Data Quality & Data Lineage	Ensuring data is accurate and fit to serve the business or compliance purpose for which it was designed or captured. Understanding and controlling data from its trusted original source and form throughout its usage by other applications.	Data elements in various systems cannot be trusted to be accurate and fit for the purpose it was designed or captured to serve. Inability to trace data elements throughout their lifecycle to determine containment of a data quality issue.	Lack of proactive understanding or tracing of data elements to ensure quality. No Master datamap. Reactive investigations by silo as data quality issues are raised in production or testing only.	Individual business units taken ownership for preserving quality of data. Quality is managed record-by-record. Master datamap showing ETL processes between one or two silos. Data lineage can be determined and demonstrated through a manual process.	Data quality assessment conducted resulting in a management strategy tailored to its needs, and governance policies addressing specific data management requirements. Master datamap for 50% or more silos. A virtual data quality firewall is implemented to detect and quarantine bad data at the point of entry. "Golden Sources" of key data elements identified, monitored and updated. Business intelligence solutions determine which data sets are most likely to be utilized and targeted for quality management and governance.	Data quality management processes are fully automated with complete audit trails. Master datamap is fully integrated and ubiquitous. Astute data management processes can collect and move data to a repository for cleansing. Advanced analytics used to predict the use and misuse of data.
K	Privacy and Data Protection Obligation	Determining privacy obligations by type of data, data subject and data location, including overlapping obligations for information and a means of communicating requirements to employees and 3rd parties who process and control information.	Access, transport and use limitations not understood and customer or employee rights are impacted. Large fines levied for non-compliance, eg. up to €20 million or 4% of global turnover for violations of General Data Protection Regulation (GDPR).	Each country and business keeps a list of applicable privacy rules. Reviews and comparisons with applicable laws and regulations are performed sporadically. Procedures for the use, retention and disposal of personal information are inconsistent, informal or incomplete.	All privacy requirements are tracked in the privacy office and corporate policies are published. Implementation decisions are left to local business and system owners. Some use of privacy zones in infrastructure and storage is deployed.	An up-to-date and accurate catalog of privacy laws and policies by country is readily accessible to all relevant employees. Policy communications are routine and semi-automated. Privacy controls are included on any provisioned system. A comprehensive privacy zone schema is deployed.	There is a process to continually monitor and update privacy obligations arising from changes to legislation, regulations, business practices and industry requirements. Privacy by Design is incorporated into design specifications and architecture of new systems and processes.
L	External Intrusion	Creating a framework for deterring, thwarting and identifying external bad actors attempting to gain access to enterprise data.	Information assets and related systems are compromised resulting in stolen trade secrets, violation of privacy restrictions, lessened performance or loss of access to rightful parties.	Fortress approach used with a single barrier or patchwork of barriers designed to keep intruders out. Framework is not flexible enough to adapt to intruder behaviors quickly.	A comprehensive data breach response plan is in place. Employees are trained on the plan with clearly assigned responsibilities. In-house simulated phishing attacks are regularly conducted on employees to identify and monitor high risk users. Back-up systems are segregated from other company systems with mechanisms for quick system restoration when required.	Periodic cyber-risk audits or penetration testing are performed to identify areas of weakness and include "table-top" exercises, with participants from key areas that would be affected by an incident. There is dual factor authentication and encryption at rest of repositories. Sensitive and proprietary data is discovered, classified and segregated in repositories with strict access and security controls such as masking.	Risk assessments and threat intelligence sharing are automated. There is an integrated view of log and event data, with network flow and packets.

	Process	Brief Description	Process Risk or Immaturity or Consequences	Level 1: Ad Hoc, Manual, Unstructured	Level 2: Manual, Structured	Level 3: Semi-Automated Within Silo	Level 4: Automated and Fully Integrated Across Functions
M	Accidental Data Leakage	Developing safeguards around classifying confidential information and preventing it from leaving via the network or employee devices.	Employees accidentally expose data to 3rd parties; including trade secrets, information with associated privacy or data protection obligations or information that can harm the organization brand equity.	Employees offered training on best practices for securing confidential information.	Employee training on information classification and handling and social media policy is mandated. Mobile workstation and devices are encrypted. Automatic notification for external email.	Employees can designate sensitive or confidential information. Endpoint data protection including encryption, remote wiping and backup is implemented. Access controls are enforced for users across multiple channels, including mobile, social, and cloud.	Messaging and other systems provide both automatic and easy-to-use manual designation of sensitive information.
		Preventing employees from stealing information assets.	Employees steal information of value, such as customer lists or proprietary trade secrets.	Investigation of potential trade secret theft initiated solely on a reactive basis when reason to suspect an insider is found.	Employee agreements define the boundaries and outline ramifications for breaches in privacy and security of all proprietary data and information. Agreements clearly outline policies for using personal devices for company duties, or BYOD. Document each employee's set of tools, apps and permissions for quick cancellation of accounts or access upon an employee departure.	Endpoint data protection including encryption, remote wiping and backup is implemented. Access controls enforced for users across multiple channels, including mobile, social and cloud.	360-degree proactive monitoring of employee behavior including email, instant messages, documents accessed and software applications is available. Ability to capture and archive evidence of incidents for forensic analysis. Ability to perform behavioral analytics to perform threat analysis.
N	Insider Theft of Data	Preventing employees from stealing information assets.	Employees steal information of value, such as customer lists or proprietary trade secrets.	Investigation of potential trade secret theft initiated solely on a reactive basis when reason to suspect an insider is found.	Employee agreements define the boundaries and outline ramifications for breaches in privacy and security of all proprietary data and information. Agreements clearly outline policies for using personal devices for company duties, or BYOD. Document each employee's set of tools, apps and permissions for quick cancellation of accounts or access upon an employee departure.	Endpoint data protection including encryption, remote wiping and backup is implemented. Access controls enforced for users across multiple channels, including mobile, social and cloud.	360-degree proactive monitoring of employee behavior including email, instant messages, documents accessed and software applications is available. Ability to capture and archive evidence of incidents for forensic analysis. Ability to perform behavioral analytics to perform threat analysis.
		Preventing employees from stealing information assets.	Employees steal information of value, such as customer lists or proprietary trade secrets.	Investigation of potential trade secret theft initiated solely on a reactive basis when reason to suspect an insider is found.	Employee agreements define the boundaries and outline ramifications for breaches in privacy and security of all proprietary data and information. Agreements clearly outline policies for using personal devices for company duties, or BYOD. Document each employee's set of tools, apps and permissions for quick cancellation of accounts or access upon an employee departure.	Endpoint data protection including encryption, remote wiping and backup is implemented. Access controls enforced for users across multiple channels, including mobile, social and cloud.	360-degree proactive monitoring of employee behavior including email, instant messages, documents accessed and software applications is available. Ability to capture and archive evidence of incidents for forensic analysis. Ability to perform behavioral analytics to perform threat analysis.
O	Data Source Catalog & Stewardship	Establishing a common definition and object model for information and the people and systems with custody of it for use in determining, defining, communicating, understanding and executing governance procedures.	The type and nature of data in a system or process is poorly understood, leading to incomplete or inaccurate application of retention, preservation, privacy, and collection and policy.	No common definition of data sources and data elements exists across IT, legal, business and records. No linkage of asset to the specific applicable business value or legal duties.	IT has an asset tracking system. IT does not have visibility to holds or retention schedules for any given asset.	IT maintains an asset database for its use; IT manually enters legal holds, business liaison and retention rules for each asset/ system. Legal maintains its own data map for eDiscovery purposes.	Shared data source catalog across IT, legal, records and business stakeholders which is used to express information assets and relevant business needs and legal obligations. Catalog as source of truth for provisioning and back up retention/ disposition requirements and all back up, archiving and provisioning procedures and decisions are transparent in the catalog. Common definitions are used to describe duties, needs, stewards, employees, laws and lawsuits across ILM&G stakeholders.
		Establishing a common definition and object model for information and the people and systems with custody of it for use in determining, defining, communicating, understanding and executing governance procedures.	The type and nature of data in a system or process is poorly understood, leading to incomplete or inaccurate application of retention, preservation, privacy, and collection and policy.	No common definition of data sources and data elements exists across IT, legal, business and records. No linkage of asset to the specific applicable business value or legal duties.	IT has an asset tracking system. IT does not have visibility to holds or retention schedules for any given asset.	IT maintains an asset database for its use; IT manually enters legal holds, business liaison and retention rules for each asset/ system. Legal maintains its own data map for eDiscovery purposes.	Shared data source catalog across IT, legal, records and business stakeholders which is used to express information assets and relevant business needs and legal obligations. Catalog as source of truth for provisioning and back up retention/ disposition requirements and all back up, archiving and provisioning procedures and decisions are transparent in the catalog. Common definitions are used to describe duties, needs, stewards, employees, laws and lawsuits across ILM&G stakeholders.
P	System Provisioning	Provisioning new servers and applications, including associated storage, with capabilities for systematically placing holds, enforcing retention schedules, disposing, collecting evidence, and protection data elements subject to privacy rights.	Systems are unable to comply with or execute defined procedures for retaining, preserving, collecting, protecting and disposing of information, exposing the company to significantly higher costs and risks.	Retention, preservation, collection and/or disposition are not considered prior to provisioning.	Some systems are manually configured with capabilities to retain and collect, but policy and capability to dispose or preserve are lacking.	Some systems are configured to retain, dispose, preserve and collect data but schedules and instructions are manually applied and configured. Instructions from legal, records and the business on duties and values are communicated in disparate tools and techniques and must be reconciled within IT.	Systems are provisioned with protocol and technical capability to retain/dispose and hold/collect, including a properly authorized retention schedule and business value inventory. Systems are provisioned with the capability to archive data to lower cost storage at the earliest point in time, archive procedures are well defined and archives execute retention/ disposition of approved schedules. Back up is used for disaster recovery only and does not function as long term archive. Retention schedules, legal holds and collection requests are systematically propagated from their respective initiators; data source catalog is updated to reflect the provisioning, archiving and back up mechanism.
		Provisioning new servers and applications, including associated storage, with capabilities for systematically placing holds, enforcing retention schedules, disposing, collecting evidence, and protection data elements subject to privacy rights.	Systems are unable to comply with or execute defined procedures for retaining, preserving, collecting, protecting and disposing of information, exposing the company to significantly higher costs and risks.	Retention, preservation, collection and/or disposition are not considered prior to provisioning.	Some systems are manually configured with capabilities to retain and collect, but policy and capability to dispose or preserve are lacking.	Some systems are configured to retain, dispose, preserve and collect data but schedules and instructions are manually applied and configured. Instructions from legal, records and the business on duties and values are communicated in disparate tools and techniques and must be reconciled within IT.	Systems are provisioned with protocol and technical capability to retain/dispose and hold/collect, including a properly authorized retention schedule and business value inventory. Systems are provisioned with the capability to archive data to lower cost storage at the earliest point in time, archive procedures are well defined and archives execute retention/ disposition of approved schedules. Back up is used for disaster recovery only and does not function as long term archive. Retention schedules, legal holds and collection requests are systematically propagated from their respective initiators; data source catalog is updated to reflect the provisioning, archiving and back up mechanism.



	Process	Brief Description	Process Risk or Immaturity or Consequences	Level 1: Ad Hoc, Manual, Unstructured	Level 2: Manual, Structured	Level 3: Semi-Automated Within Silo	Level 4: Automated and Fully Integrated Across Functions
<b>Q</b>	<b>Cloud Computing</b>	Ensuring that safeguards around information governance are applied to non-traditional procurement and provisioning channels such as cloud services.	Individual businesses execute contracts with cloud providers and put data into the cloud with no ability to protect, hold, retain or dispose of information in accordance with other information governance safeguards.	Little is known about cloud application usage across the enterprise.	Unapproved and unsupported cloud services or “Shadow IT” used by employees is documented and remediated. Provisioning of any new cloud service must go through the designated approval process.	Current Service Level Agreements (SLAs) with cloud service providers have been reviewed for those with a standards based cloud environment and a security program that meet regulatory policies and procedures. Detailed SLAs addressing specific requirements for encryption, application design, monitoring, incident response and disaster recovery have been created for future contracts.	Regular compliance audits are performed to verify cloud service providers’ security policies, practices and procedures. Audits show whether all of the applicable regulatory requirements are met and compliance is properly documented.
<b>R</b>	<b>Active Data Management</b>	Differentiating high value actively used data by the business from aging data of value to regulators only or less frequently accessed data; results in increased accessibility, security, privacy; aligns and enables data value with storage tiering by value.	New, valuable, aging, and useless data are commingled within the data source, its back up and its non-production instances. Business users waste their time sifting through debris to find what they need without success. IT costs soar. Organization is exposed to privacy, security and legal risks.	Data is managed over time as the system was provisioned and new, valuable, aging, and useless data are comingled within the data source, its back up and its non-production instances.	End user employees perform hygiene and clean up actions on file shares and systems to ensure function and access. IT performs basic back up and availability functions.	Some archiving is performed to batch off aging data and provide business users with faster access to more frequently used data. Archive approach varies by data source and business unit. Policies for retention, privacy and security are manually applied, if at all.	Data of high value actively used by the business is differentiated from aging data of value to regulators only or less frequently accessed data. Business users have ready access to high value data and spend no time sifting through debris to find it. Data is secured and retained based on its business value. Aging data with declining value is archived or moved to lower cost locations over time; unnecessary data is routinely disposed. Private data is masked based on policy. Back up data complies with the retention schedule and is not used as long-term archive alternative.
<b>S</b>	<b>Disposal &amp; Decommissioning</b>	Disposing data and fully decommissioning applications at the end of their business utility and after legal duties have elapsed.	IT is unable to/ improperly disposes data and decommission systems causing unnecessary risk and legal or business expense.	IT ‘keeps everything’ because it has no systematic way to determine obligations or value.	Some systems are manually configured with capabilities to retain, hold, collect or dispose of data. Changes in legal requirements must be manually configured.	IT de-duplicates files and disposes of log files under its control. IT responds to business requests to decommission applications and works with legal on a manual review process to determine if any open legal matters may apply before decommissioning.	Data is automatically deleted at the end of its retention period when no legal hold has been specified; back up data is routinely and systematically overwritten. IT routinely analyzes the data source catalog to identify systems with low business value to proactively determine savings opportunities; IT can easily determine duplicative systems from the business value and taxonomy map for instance consolidation. IT performs routine disposal with transparent, reliable facts on preservation and retention obligations; looks up any asset or employee to determine value, current legal requirements.

	Process	Brief Description	Process Risk or Immaturity or Consequences	Level 1: Ad Hoc, Manual, Unstructured	Level 2: Manual, Structured	Level 3: Semi-Automated Within Silo	Level 4: Automated and Fully Integrated Across Functions
<b>T</b>	<b>Legacy Data Management</b>	Processes, technology and methodologies by which data is disposed and applications fully decommissioned at the end of their utility and after legal duties have elapsed.	IT is unable to associate data with business stakeholders or ensure legal duties are met, leading to oversight in collecting evidence and unnecessary legal and operating costs.	No hold release notification, no lookup ability.	Email hold release communication from Legal to IT.	IT initiates a process with legal to “reverse engineer” legacy data holds to dispose of unstructured data or back up data.	Legacy data on disk and tape is dispositioned using legal hold inventory enriched with custodian and data sets subject to hold. Data subject to ongoing regulatory or legal requirement is isolated and “surrounding” data is disposed. Additional legacy data is not accumulated.
<b>U</b>	<b>Storage Alignment</b>	The process of determining and aligning storage capacity and allocation to information business value and retention requirements, including optimizing utilization targets, storage reclamation and re-allocation after data is deleted to link storage cost to business need for data stored.	Storage is over-allocated, misaligned with business needs and consumes unnecessary capital; IT is unable to reclaim storage and eliminate cost after data is deleted causing unnecessary cost.	No reliable means of determining storage requirements and inability to allocate/reclaim based on retention needs. Each DBA determines capacity and capacity is not revisited.	Intensive manual effort to achieve an accurate picture of storage capacity and cost; difficulty assessing and reconciling need, allocation and utilization. Charge backs are used but not reactive of cost facts or cost accounting.	Automated storage utilization reporting and charge back mechanism and transparency to refresh cycles across the inventory. Charge back reporting by tier and organization is reliable and fact based.	Storage is provisioned for new systems commensurate with retention schedules and archive protocols; refresh accounts for capacity availability from continuous deletion and decommissioning activity. Storage cost is weighed in retention schedule approval process and archive decision-making; unit cost is available in data source catalog. Current and forecasted storage capacity and costs are transparent and align to business value and data retention schedules. Optimization practice captures benefit of deletion and decomm to avoid continuous capacity addition. Accurate charge back reporting by business unit and source and gap analysis to retention schedule, business value and information cost to inform business decision-making on the costs/benefits of storing data over time.
<b>V</b>	<b>Audit</b>	Testing to assess the effectiveness of other processes, in this instance the processes for determining, communicating and executing processes and procedures for managing information based on its value and legal duties and disposing of unnecessary data.	Unable to demonstrate reasonable efforts to establish and follow governance policies and procedures increases sanctions risks, penalties and erodes customer trust.	Do not audit retention, holds, disposal processes.	Verifies that the global retention schedule is published and visible to IT and LOB.	Audits publication of records, privacy, disaster recovery, application lifecycle and legal hold policies. Does not test execution of the policy.	Establishes and conducts testing procedures for records management, business value inventories, data sources, privacy requirements and legal holds such that information assets are properly defined and retained until their value expires and it is timely disposed when there is no longer a business need or legal duty. Sample tests of organizations and record class for retention and timely disposition. Establishes and conducts testing procedures for legal matters to ensure preservation duties are properly communicated and executed and holds are timely released. Tests data source catalog, back up data and system provisioning to ensure ability to comply and actual policy adherence. Audits storage provisioning and procurement against retention/disposition/decom schedules.

## Risk Heat Map

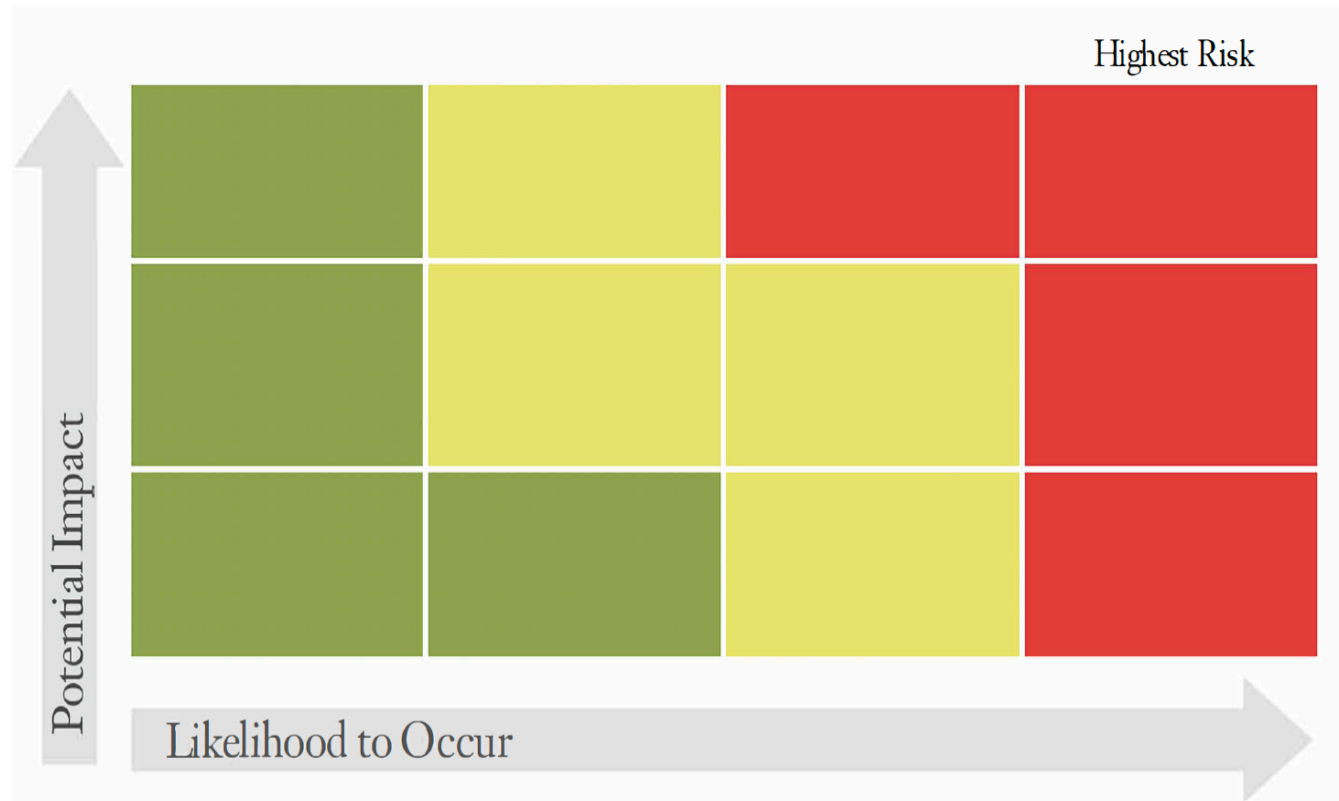
1. Using the 22 processes and their risks, consider your facts.
2. Plot the current process risks on the graph by placing the letter for each process on the grid where it belongs.
3. Plot the risk level if your organization had level 3 and level 4 capabilities.

PROCESS	
A	Employees on Legal Hold
B	Data on Legal Hold
C	Hold Publication
D	Evidence Collection
E	Evidence Analysis & Cost Controls
F	Legal Record
G	Information Retention and Disposal Obligations
H	Departmental Information Practice
I	Realize Information Value
J	Data Quality & Data Lineage
K	Privacy and Data Protection Obligations
L	External Intrusion
M	Accidental Data Leakage
N	Insider Theft of Data
O	Data Source Catalog & Stewardship
P	System Provisioning
Q	Cloud Computing
R	Active Data Management
S	Disposal & Decommissioning
T	Legacy Data Management
U	Storage Alignment
V	Audit

■ High risk requires constant monitoring and review, immediate escalation on failure or impending failure. 50% likelihood

■ Moderate risk requires frequent monitoring to prevent and detect; costly to correct or mitigate. Between 10%-50% likelihood

■ Low risk does not require constant monitoring and is easy to prevent, detect, correct, defend. Less than 10% likelihood



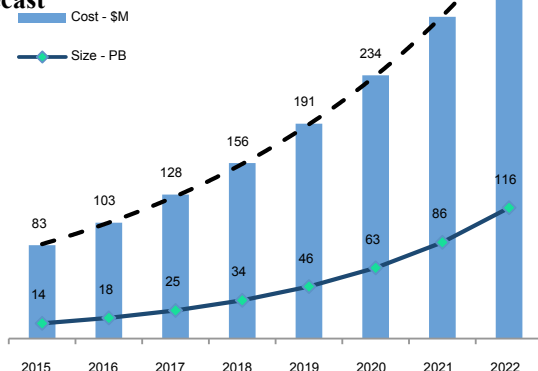


# The Business Case for Information Governance

## Cost Levers

### 1 Storage Infrastructure: Storing Data with No Utility

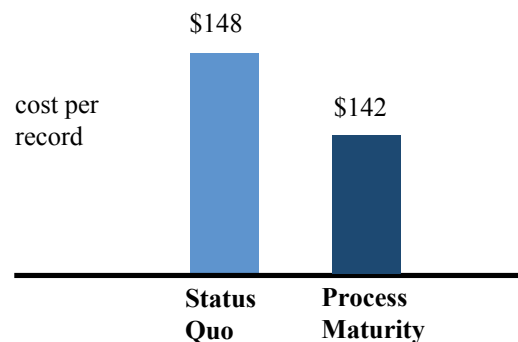
Utilized Storage Cost and Volume Forecast



### 2 Data Security: Cost Reduction through Process Maturity

Impact of process improvements on the per record cost of data breach

Consolidated view measured in US\$



## Process Drivers

Excess storage cost (processes R and U) resulting from over-accumulation and/or inability to delete data for lack of certainty on legal holds, regulatory requirements or business value. Costs correlate to capabilities in process A) employees on legal hold, B) data on legal hold, C) hold publication, G) information retention and disposal obligations, and H) departmental information practice.

Excess storage and use of data creates increased opportunities for data breaches, leakage and theft. Costs correlate to capabilities in process, H) departmental information practice, L) external Intrusion, M) accidental data leakage, N) insider theft of data theft and Q) cloud provisioning.

## Scorecard

	1	2	3	4
R				
U				
A				
B				
C				
H				
G				

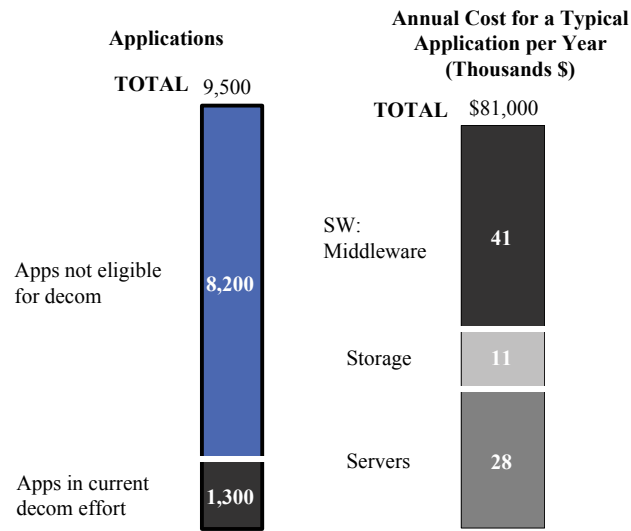
	1	2	3	4
H				
L				
M				
N				
Q				

## Scorecard

	1	2	3	4
P				
S				
A				
B				
C				
G				
H				

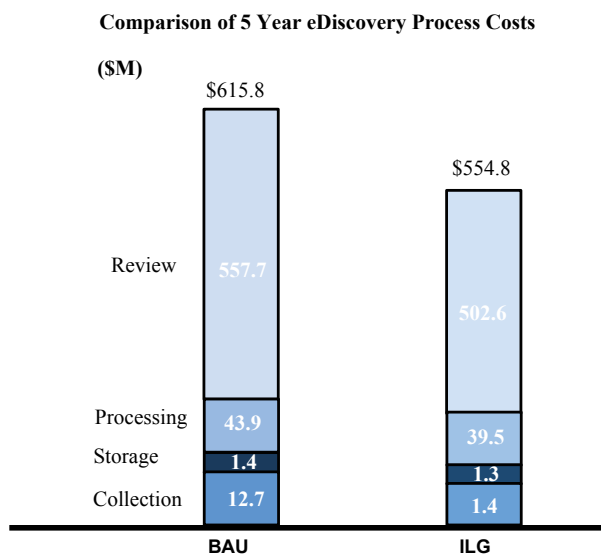
	1	2	3	4
O				
R				
S				
T				
G				
H				
D				
E				

### 3 Applications: Instances without Business Value



Delayed or partial application decommissioning (process P and S) from inability to discern which data is required by legal, regulators and business. Cycle time delays lead to excess run rate. Costs correlates to capabilities in process A) scoping people on hold, B) scoping data on hold, C) publishing holds, G) information retention and disposal obligations, and H) departmental information practices.

### 4 eDiscovery: Costs of Collection and Review



Excess eDiscovery and outside counsel fees from over collection of data from lack of visibility to what data exists, inability to collect with precision, excess data across the information environment, and late case resolution with excess run rate legal costs or excessive eDiscovery cost relative to case merits. Costs correlates to capabilities in process O) data source catalog, R) active data management, S) disposal, T) legacy data management, H) departmental information practice, G) information retention and disposal obligations as well as D) evidence collection.

# Process Score Card

Level 1: Facts known only to individuals practitioners.

Level 2: Facts accessible with difficulty by others within the same practice.

Level 3: Facts readily available with frequently used in departmental actions and decisions.

Level 4: Facts readily available and fully integrated across related enterprises process, used by all stakeholders in decisions and actions.

	IG Process	Brief Description	Maturity Scale (1-4)				Potential Risk of Failure	Potential Impact	Likelihood to Occur
LEGAL	A	<b>Employees on Legal Hold</b> Determining employees with information potentially relevant to an actual or anticipated lawsuit or government investigation.					Custodians are not identified and potentially relevant information is inadvertently modified or deleted.		
	B	<b>Data on Legal Hold</b> Determining information, records and data sources that are potentially relevant to an actual or anticipated lawsuit or government investigation.					Actual, rogue or IT managed data sources missed in hold execution, potentially relevant information is inadvertently modified or deleted.		
	C	<b>Hold Publication</b> Communicating, syndicating and executing legal holds to people, systems and data sources for execution and compliance.					IT or employees migrate, retire or modify data because they lacked hold visibility.		
	D	<b>Evidence and Collection</b> Fact finding and inquiry with employees with knowledge of a matter in dispute to determine potentially relevant information and its whereabouts and sources. Collecting potential evidence in response to an agreed-upon request with an adversary or government agency.					Dynamic, diverse information facts not considered in preservation and collection planning, data is overlooked; no follow through on information identified in custodian interviews. Collection failure from overlooked source, departing employee, incomplete prior collection inventory, communication and tracking errors.		
	E	<b>Evidence Analysis &amp; Control</b> Assessing information to understand dispute and potential information sources and for determining, controlling and communicating the costs of outside review of relevant information.					Material issues in dispute are poorly understood until after strategy established and expenses incurred. Excessive data causes litigation costs to exceed dispute value.		
	F	<b>Legal Record</b> Documenting the custodians and data sources identified, the legal hold and collection activities over multi-year matter lifecycle.					Unable to readily assemble, understand or defend preservation and discovery records. Failures in custodian and data source management. Preservation, collection detected long after occurrence and cause unnecessary remediation cost and risk.		
RIM	G	<b>Information Retention and Disposal Obligations</b> Defining an information classification schema that reflects the organization structure; cataloging, updating and mapping the laws that apply to each class in the countries in which the organization operates to determine regulatory record keeping obligations; establishing and managing a network of records liaisons to ascertain the existence and location of records.					Unable to comply or demonstrate compliance with regulatory record keeping obligations. Disparate nomenclatures for records make application of retention schedules/procedures difficult to apply and audit.		
BUSINESS	H	<b>Departmental Information Practice</b> Using an enterprise information taxonomy, cataloging which information each business organization values, generates or stores by class, where they store it and how long it has utility to them; results in retention schedules for information and enables data source-specific retention schedules that reflect both business value and regulatory requirements.					IT 'saves everything' which increases discoverable mass, complexity and legal risk; IT disposes of information of business value undermining enterprise operation. Procedures for retention/disposal difficult to articulate and defend and unapplied by LoB.		
	I	<b>Realize Information Value</b> Gaining timely access to an ability to apply information in the course of their work, including the ability to harness information of quality as it ages and the ability to use relevant information with or without author context to maximize the enterprise value of information.					Important business decisions are made on missing information or poor quality information, resulting in poor decisions. Information is not used shortly after its creation because business has forgotten the source or location of information or can't find it, resulting in cost without corresponding value.		
	J	<b>Data Quality &amp; Data Lineage</b> Ensuring data is accurate and fit to serve the business or compliance purpose for which it was designed or captured. Understanding and controlling data from its trusted original source and form throughout its usage by other applications.					Data elements in various systems cannot be trusted to be accurate and fit for the purpose it was designed or captured to serve. Inability to trace data elements throughout their lifecycle to determine containment of a data quality issue.		
PRIVACY AND SECURITY	K	<b>Privacy and Data Protection Obligations</b> Determining privacy obligations by type of data, data subject and data location, including overlapping obligations for information and a means of communicating requirements to employees and 3rd parties who process and control information.					Access, transport and use limitations not understood and customer or employee rights are impacted. Large fines levied for non-compliance, eg. up to €20 million or 4% of global turnover for violations of General Data Protection Regulation (GDPR).		

# Process Score Card

Level 1: Facts known only to individuals practitioners.

Level 2: Facts accessible with difficulty by others within the same practice.

Level 3: Facts readily available with frequently used in departmental actions and decisions.

Level 4: Facts readily available and fully integrated across related enterprises process, used by all stakeholders in decisions and actions.

	IG Process	Brief Description	Maturity Scale (1-4)				Potential Risk of Failure	Potential Impact	Likelihood to Occur
L	External Inclusion	Creating a framework for deterring, thwarting and identifying external bad actors attempting to gain access to enterprise data.					Information assets and related systems are compromised resulting in stolen trade secrets, violation of privacy restrictions, lessened performance or loss of access to rightful parties.		
M	Accidental Data Leakage	Developing safeguards around classifying confidential information and preventing it from leaving via the network or employee devices.					Employees accidentally expose data to 3rd parties; including trade secrets, information with associated privacy or data protection obligations or information that can harm the organizations brand equity.		
N	Insider Theft of Data	Preventing employees from stealing information assets.					Employees steal information of value, such as customer lists or proprietary trade secrets.		
LT. O	Data Source Catalog & Stewardship	Establishing a common definition and object model for information and the people and systems with custody of it for use in determining, defining, communicating, understanding and executing governance procedures.					The type and nature of data in a system or process is poorly understood, leading to incomplete or inaccurate application of retention, preservation, privacy, and collection and disposition policy.		
P	System Provisioning	Provisioning new servers and applications, including associated storage, with capabilities for systematically placing holds, enforcing retention schedules, disposing, collecting evidence, and protecting data elements subject to privacy rights.					Systems are unable to comply with or execute defined procedures for retaining, preserving, collecting, protecting and disposing of information, exposing the company to significantly higher costs and risks.		
Q	Cloud Computing	Ensuring that safeguards around information governance are applied to non-traditional procurement and provisioning channels such as cloud services.					Individual businesses execute contracts with cloud providers and put data into the cloud with no ability to protect, hold, retain or dispose of information in accordance with other information governance safeguards.		
R	Active Data Management	Differentiating high value actively used data by the business from aging data of value to regulators only or less frequently accessed data; results in increased accessibility, security, privacy, aligns and enables data value with storage tiering by value.					New, valuable, aging, and useless data are commingled within the data source, its back up and its non-production instances. Business users waste their time sifting through debris to find what they need without success. IT costs soar. Organization is exposed to privacy, security and legal risks.		
S	Disposal & Decommissioning	Disposing data and fully decommissioning applications at the end of their business utility and after legal duties have elapsed.					IT is unable to/improperly disposes data and decommission systems causing unnecessary risk and legal or business expense.		
T	Legacy Data Management	Processes, technology and methodologies by which data is disposed and applications fully decommissioned at the end of their utility and after legal duties have elapsed.					IT is unable to associate data with business stakeholders or ensure legal duties are met, leading to oversight in collecting evidence and unnecessary legal and operating costs.		
U	Storage Alignment	The process of determining and aligning storage capacity and allocation to information business value and retention requirements, including optimizing utilization targets, storage reclamation and re-allocation after data is deleted to link storage cost to business need for data stored.					Storage is over-allocated, misaligned with business needs and consumes unnecessary capital; IT is unable to reclaim storage and eliminate cost after data is deleted causing unnecessary cost.		
V	Audit	Testing to assess the effectiveness of other processes, in this instance the processes for determining, communicating and executing processes and procedures for managing information based on its value and legal duties and disposing of unnecessary data.					Unable to demonstrate reasonable efforts to establish and follow governance policies and procedures increases sanctions risks, penalties and judgments and erodes customer trust.		