Information Lifecycle Governance (ILG)

Maximise data value, reduce data growth, cost and risk

Jan Lambrechts
Information Lifecycle Governance, eDiscovery and Privacy
Consultant

Summary: Over-retention of data with no value leads to increased cost and risk, and reduces the capacity of organisations to identify and leverage valuable business data. Information Lifecycle Governance (ILG) provides a structured, strategic approach to reducing data growth, cost and risk, while providing the policies, processes and technology to move from a reactive to a proactive state of information management and maximise the value of information.

Introduction

Information Lifecycle Governance (ILG) is a strategic, structured approach which addresses the increasing volume and complexity of electronic information, and the associated increase in cost and risk to manage that information.

As the volume and complexity of electronic data increases, organisations face greater challenges in extracting business value, managing IT costs, and limiting the legal risks associated with managing and retaining that data.

Organisations without policies, processes and technology in place to address these issues will increasingly face the situation where their data becomes a costly liability to the effective operation of the business, rather than an asset to be leveraged.

Data may be located across multiple platforms, in various formats, across numerous geographical locations, and be the subject of a combination of business, legal, regulatory, security and privacy requirements.

The most effective way to manage this complexity is by implementing an ILG program, which takes a transparent, enterprise-wide approach to the management of data.

The outcomes of an ILG program are:

- Defensible disposal of data debris;
- Reduced risk and cost exposure from a legal, regulatory and privacy perspective;
- Improved business processes and efficiencies; and
- Reduced exposure to financial, reputational and operational threats.

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n3.46

Data debris

In 2004, the Compliance, Governance and Oversight Council (CGOC) was founded in the U.S. as a discussion forum and professional think tank to address information governance issues. CGOC has over 2,900 legal, IT, records, privacy and information management professionals and hosts regular meetings in the U.S. and Europe to discuss discovery, retention, privacy and governance.

At the 2012 CGOC Summit, a survey of corporate CIO's and general counsels revealed that typically 1 percent of corporate information is on litigation hold, 25 percent has current business value, and 5 percent is in a records retention category. This means that approximately **69 percent** of the data most organisations keep has no legal, regulatory, privacy, security or business value. (See Figure 1).

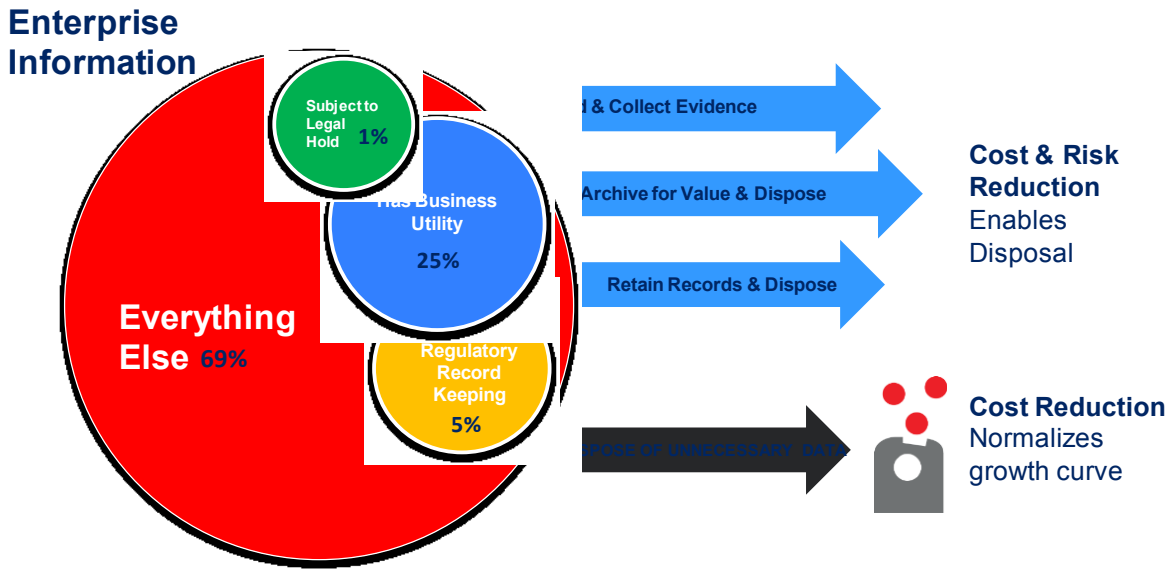

Figure 1 – CGOC Summit 2012 Survey

This overwhelming volume of data debris, i.e. data with no or low value, which still carries cost and risk, has significant implications for the business, legal, IT, records management, privacy, risk and compliance stakeholders in an organisation.

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n3.46

Stakeholders

Business

Business stakeholders generate and use data for multiple purposes, including identification of new business opportunities, analysis of customer behaviours and preferences, competitors and market trends, and strategic decision making.

In order to maximise the value of business information as a strategic asset, the effort to locate the most relevant, valuable data must be reduced. In a scenario where 69% of data has no value, finding what you need becomes an onerous task. This can lead to lost opportunities, duplication of effort, lack of awareness of existing information, reduction in business efficiency, and inadvertent deletion of valuable data.

What is required is a more focused, managed, stable body of business information that can be leveraged to increase efficiency and profit. Improved access to and handling of information will allow the business to become less reactive and move towards a more proactive, even predictive management of information assets.

Legal

Legal stakeholders require potentially relevant data in anticipation of litigation or regulatory investigations to be identified, preserved (via legal hold), collected (in a forensically sound manner), processed, reviewed, analysed, and potentially produced and presented.

The typical steps in the eDiscovery process are encapsulated in the **Electronic Discovery Reference Model** as created by the EDRM (edrm.net) shown in Figure 2).

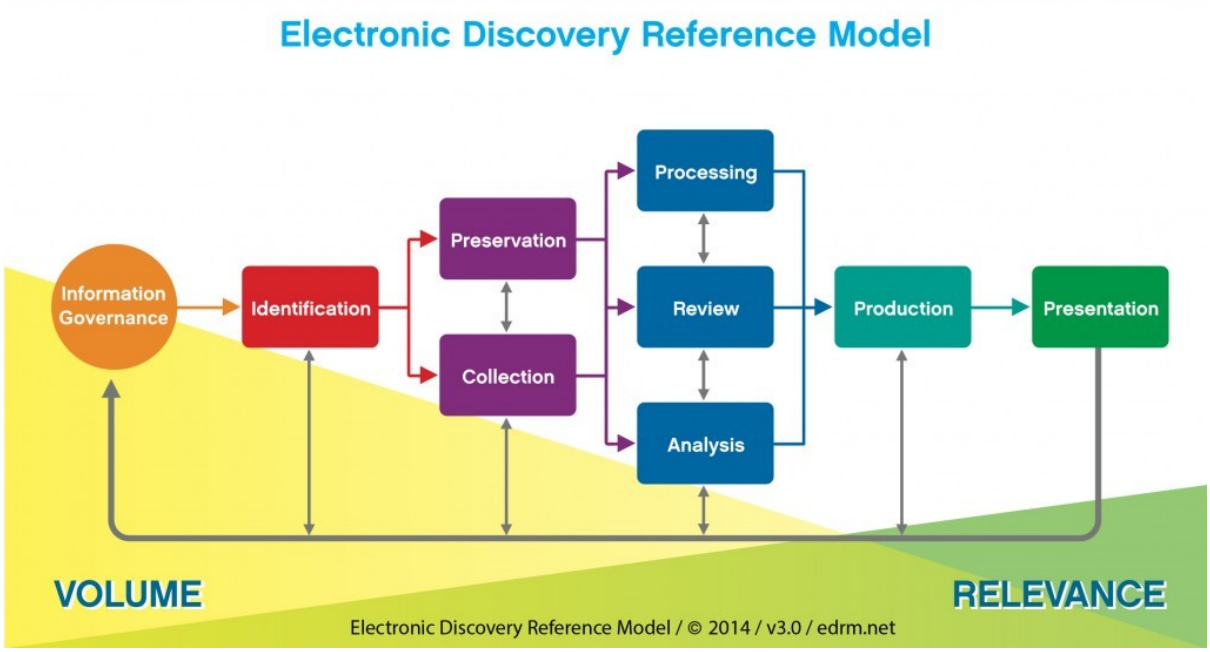

Figure 2 – Electronic Discovery Reference Model – Source: EDRM (edrm.net)

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n3.46

The higher the volume of data debris, the higher the cost and risk associated with these processes. Increased legal costs will result from the legal department having to wade through a mass of irrelevant data to find the relevant data for each legal matter.

Increased legal risks could result from:

- Potentially relevant data being inadvertently modified, deleted or overlooked;
- Damaging evidence being exposed that should have been defensibly disposed;
- Data custodians and sources being missed in legal hold execution;
- Ineffective early case assessment and matter scoping; and
- Inefficient estimation of ongoing litigation exposure.

Privacy, Risk and Compliance

Privacy, Risk and Compliance stakeholders need to know what data an organisation holds, where it is stored, who has access to it, how it is secured, and how easily it can be retrieved, accessed and produced when required. This forms the basis for implementing the required practices, procedures and systems to ensure compliance with relevant legislative requirements.

The Australian federal *Privacy Amendment (Enhancing Privacy Protection) Act 2012* which came into effect on 12 March 2014 introduced significant changes to the existing *Privacy Act 1988* and places more onerous demands on organisations and agencies to manage their and their customer's personal information. Maintaining personal information beyond the end of its lifecycle increases the risk of privacy breaches occurring.

The *Australian Privacy Principles (APPs)* as encapsulated in the Act, require organisations to destroy or de-identify personal information at the end of its lifecycle, and to protect the information from (a) misuse, interference and loss; and (b) unauthorised access, modification or disclosure.

The more complex and voluminous a data set, the more challenging to locate, secure, produce or delete personal information to ensure compliance. This could lead to significant penalties of up to $1.7 million and reputational damage.

Records Management

Records Management stakeholders maintain a retention schedule that classifies records and prescribes retention periods based on this classification.

The limitations of a traditional retention schedule are that it typically only applies to records, does not include information that has business value, is not executable against data sources,

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n3.46

does not have visibility to other stakeholders, and is difficult to keep up to date within an ever changing legislative environment.

In a data environment filled with debris, it becomes almost impossible to distinguish between data that has value and data that can be discarded, which in turn impacts the effective execution of a records retention and destruction schedule.

IT

IT stakeholders are saddled with the responsibility to store, secure, archive and delete data, typically without the necessary insight into the value and obligations associated with the data. Exponential data growth, increasing data complexity and over-retention of data with no value leads to a situation where numerous IT processes are impacted.

Managing too much data debris complicates elimination of legacy systems, reclamation of storage capacity, appropriate storage allocation according to data value, application decommissioning, and value based archiving. It further impacts application system performance, development and testing of new systems, increases back-up and processing times, and increases ongoing data storage costs.

Policy, Process and Technology

Over-retention of data with no value results from gaps in policy, process and technology.

A lack of association of value and duties to data leads to a situation where data is managed as if everything has value, where compliance is difficult to monitor and enforce, and where too much cost and effort is spent on managing, preserving and producing unnecessary data.

At a policy level, decisions have to be made with regards to what data must be kept, why, and for how long. These policies will require input from all relevant stakeholders and must have visibility across the enterprise to enable ongoing, transparent application of data retention and preservation requirements.

The main elements required at a policy level are:

- **Regulatory:** an updated and expanded retention schedule that applies across the enterprise;
- **Legal:** more precise legal hold management (data custodians and sources) and improved early case assessment
- **Privacy:** an up to date privacy policy, privacy and compliance obligations register, and business unit policies
- **Security:** a data source catalogue, data classification model, improved user and role based access controls

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n3.46

Execution of policies must be supported by a maturation of business processes across the enterprise. Ad hoc, manual data management processes need to move to a more integrated, consistent and repeatable level of maturity to ensure that policy requirements are effectively implemented.

Policy and process improvements must be supported by a technology model that allows for the syndication and execution of policies on data sources, based on the mapping and classification of that data. Ideally, the underlying technology must enable some level of automation with regards to data retention, legal hold application, de-duplication, analysing data in place, value-based tiering of storage and disposal of data debris.

Information Governance Reference Model

In 2009 the EDRM (edrm.net) created the **Information Governance Reference Model (IGRM)** (see Figure 3) to provide a common, practical, flexible framework to help organisations develop and implement effective and actionable information management programs. The model enables linking of information value and duties to data assets and ties information demand to infrastructure supply.

An effective ILG solution is achieved through unified governance, policy integration and process transparency across all data stakeholders.

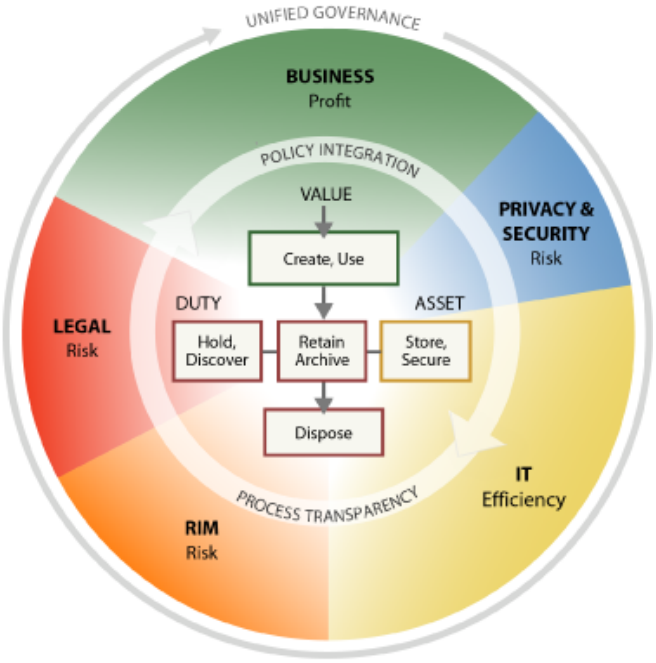

Figure 3 – Information Governance Reference Model – Source: EDRM (edrm.net)

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n3.46

ILG elements

Data source catalogue

The first step towards an effective ILG program is to establish what data resides in which systems, and to track the relationship between data sources and supporting infrastructure. An updated data source catalogue should track data sources in a way that is understandable to non-IT stakeholders.

Data classification

Once a data mapping exercise has been completed, data must be classified according to business value, retention periods stipulated by law, privacy and security obligations, and legal holds.

This process will involve the extension and automation of retention schedules and increased automation of legal hold and eDiscovery processes.

Data classification then forms the basis for applying the most appropriate security and access controls, and identifying data of no value that can be defensibly disposed.

Retention management

The retention schedule must be updated to include not only records, but also data that has business value, i.e. the schedule should be dynamically mapped to legal and business requirements.

The intention is to retain data for no longer than is required and to include retention periods for all types of data, including unstructured repositories such as email, share drives, SharePoint and others.

Legal hold and eDiscovery

A more precise, actionable legal hold process will ensure that relevant data is not deleted, modified or overlooked.

Improved data analytics will enable more efficient early case assessment and the ability to analyse data in-house and in place, saving cost and lowering risk through the avoidance of unnecessary data collection, processing and review.

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n3.46

Defensible disposal

There is no legal requirement to keep all data in perpetuity. Once data to be retained and preserved has been identified and classified, the remaining data debris can be defensibly disposed according to the relevant policy.

All relevant stakeholders should be in agreement that certain information has reached the end of its lifecycle and the resulting disposal instructions should be clearly communicated to the data owner who manages the information.

Value based archiving and tiering

Based on the classification of data, appropriate storage tiers can be applied, e.g. high value data on tier 1 storage, and low value data on lower tiers or back-up tape. This will maximise the efficiency and cost of data storage and ensure quick, easy access to key information by business users.

Storage reclamation, application decommissioning

Once data of no value has been disposed and data of low value has been archived appropriately, applications that are no longer required can be decommissioned and storage can be reclaimed.

Ongoing information governance

Once policies, processes and technology have matured, information governance practices that have been put in place for existing data should now also be applied to all new data that enters the organisation (via creation or collection). All new data should now be managed according to these upgraded policies and processes, enabling data to be managed by value, cost, risk and duties throughout its lifecycle.

Conclusion

ILG is not a stagnant process.

In order for an organisation to keep information governance policies, processes and technology up to date, it will require constant monitoring and auditing by executive management. New trends and technologies, combined with changing legal and regulatory requirements, have to be incorporated into the organisation's ILG strategy on an ongoing basis.

ISSN 2203-1693. http://doi.org/10.7790/ajtde.v2n3.46

The true benefits of an integrated ILG approach cannot be realised through occasional data clean-ups, but rather through structured, strategic implementation of governance, policy and process initiatives across the organisation.

References

Australian Privacy Principles, at http://www.oaic.gov.au/privacy/privacy-act/australian-privacy-principles

Compliance, Governance and Oversight Council, at http://www.cgoc.com/

Electronic Discovery Reference Model, at http://www.edrm.net/resources/edrm-stages-explained

Information Governance Reference Model, at http://www.edrm.net/resources/guides/igrm

Privacy Act 1988, at http://www.comlaw.gov.au/Series/C2004A03712

Privacy Amendment (Enhancing Privacy Protection) Act 2012, at http://www.comlaw.gov.au/Series/C2012A00197

ISSN 2203-1693.

http://doi.org/10.7790/ajtde.v2n3.46