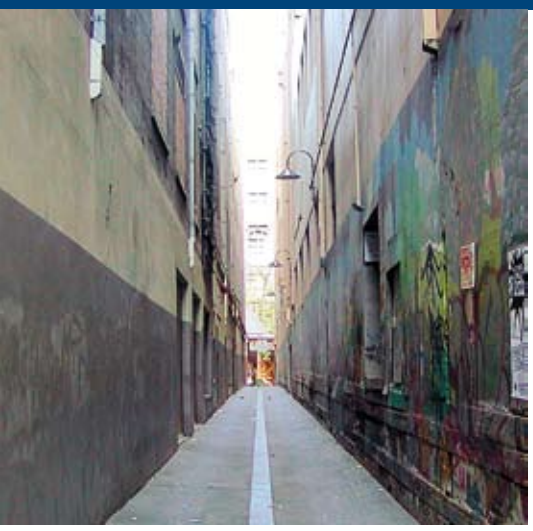


Transformational Records Management: Minimizing Risk and Liability

S. Kenny
is the KPMG Transformational Records Management champion, advising clients on the alignment of business functions necessary to minimize risk and optimise business benefit from records management investments.

kenny.steve@kpmg.nl

Steve Kenny

Many organizations today are coming to terms with the fact that the huge growth in information has created risk exposure in terms of the accessibility and integrity of data. That exposure is increasingly realized through litigation where data records are considered "discoverable" by courts. This article sets out some of the risks and challenges facing organizations today in the realm of Records Management.

Introduction

As the nature of business information becomes more complex and compliance issues multiply, every organization, large or small, regardless of its line of business, must analyze how it controls information within the enterprise, across the globe, and between product/service offerings. Sometimes corporate compliance departments and legal departments find themselves in contention with their IT departments as the former demand processes that can deliver the right information at the right time to the right person. When that repeatedly fails to happen, organizations begin re-assessing their records management programs.

Most organizations today have, in practice, a records management program based upon physical paper. They may also have an archiving strategy for electronic information. Frequently, the first is performed by a Records Management or Legal Compliance Department; the second is managed by an IT Department. The Records Management/Compliance Department concentrates on producing documents for regulatory, tax, and litigation reasons; the IT Department wants to save costs on storage and improve network performance. Getting these two groups to align their strategies is the first step toward a comprehensive global records management program that ensures safe harbor from risk and provides verifiable, defensible practices.

The development of a Global Records Management program and policy is an opportunity to set out the vision and role of enterprise-wide Records Management within an organization, as well as to create a framework for the ancillary policies. Ancillary policies need to be established to treat specific types of data content, but they must still adhere to the guiding principles of the overall policy. Ancillary policies create requirements that meet the different needs of physical records, inactive records, vital records, e-mail,

records shared across multiple regions, and electronic records for long-term archival storage. The result is an organization that mitigates risk, meets compliance demands, and realizes tangible business benefits.

Records Management Risks

Records are information created, received or used as part of a firm's transactions, processes or business activities and legal obligations (ISO15489). Records contain information created, received, and maintained as evidence by an organization or person, in pursuance of legal obligations or in the transaction of business. They include documentation pertaining to a transaction or business event that may have legal ramifications or historical value. Guided by regulations, each organization must determine the definition of what a record is and, often more importantly, what it is not.

Good records management can:

- Aid more effective disclosure and help laywers make faster decisions as to the extent of a reasonable search for documents in accordance with disclosure rules. Being able to identify relevant or privileged material quickly will also save significant costs in the event of litigation.
- Provide evidence of compliance in keeping with legal requirements as regulators pay more attention to data retention.
- Reduce time and expense incurred through document production activities associated with litigation, and increase speed and efficiency in meeting regulatory requests for documentation.

The complexity of records management has increased exponentially in recent years. Massive information production along with the complexity of processing this amount of data frequently has every level of management perplexed when the full gambit of risks are considered. For instance, a subset of this massive information contains personal information about individuals, and therefore requires increased control and recognition of how the use of data protection rights such as Subject Access Requests, interact with non-privacy related litigation, such as discrimination.cases.

Organizations are capturing information using an increasing variety of methods, including scanners, notebooks, printers, removable devices and storage area networks. The records containing this information are subject to multiple regulatory requirements, including for instance MiFID, national implementations of Directives 95/46/EC & 02/58/EC, provincial and national employment law, Federal Rules of Civil Procedure (FRCP), American Bar Association (ABA) Civil Discovery Standards, Gramm-Leach-Bliley, Health Insurance Portability and Accountability Act (HIPPA), Securities and Exchange Commission (SEC) Rule 17a-4 and National Association of Securities Dealers (NASD) Rule 3010. Failure to produce records and information to meet these regulations can be costly and damaging to an organization's reputation.

More recently, improvement programs for records management have been driven by Litigation Readiness concerns over e-discovery costs. Those costs have steadily risen as businesses deal with numerous and constant disclosure requests. The task of sifting through vast archives of e-mail and electronic data has become increasingly complex and taxing. Litigation Readiness programs hold the promise of reducing these costs. Their aim is to give companies the knowledge of precisely where and how their records are stored and over what period of time, plus the comfort of knowing they are stored in accordance with the discovery obligations of each jurisdiction in which they operate.

To help organizations realize potential benefits that could be gained from proactive programs, KPMG has designed a process called Transformational Records Management (TRM), a process that aligns records management practices with legal and business objectives. TRM can deal with widely deployed responsibilities and help gain acceptance across multiple functional lines. TRM moves processes towards broadly stated business and regulatory objectives. Technology is leveraged to address both the past (where the vast majority of exposure resides) and the future, to support long-term value preservation.

TRM aims to help organizations realize the benefits of good records management by adopting strategies across the following areas:

- Reputational risk management arising from inefficient records management processes.
- Litigation and regulatory readiness.
- Compliance transparency.
- Effective data retention.
- Controled storage costs.

Through the orchestration of these five elements TRM provides organizations with the ability to achieve business benefit from the effective and efficient management of records.

Improved management of reputational risk

Losing face can trigger a crisis of confidence in shareholders, customers, business partners and regulators, constraining a company's ability to do business. Many adverse court decisions have been publicized where findings were made against companies unable to produce admissible records. But the issue is

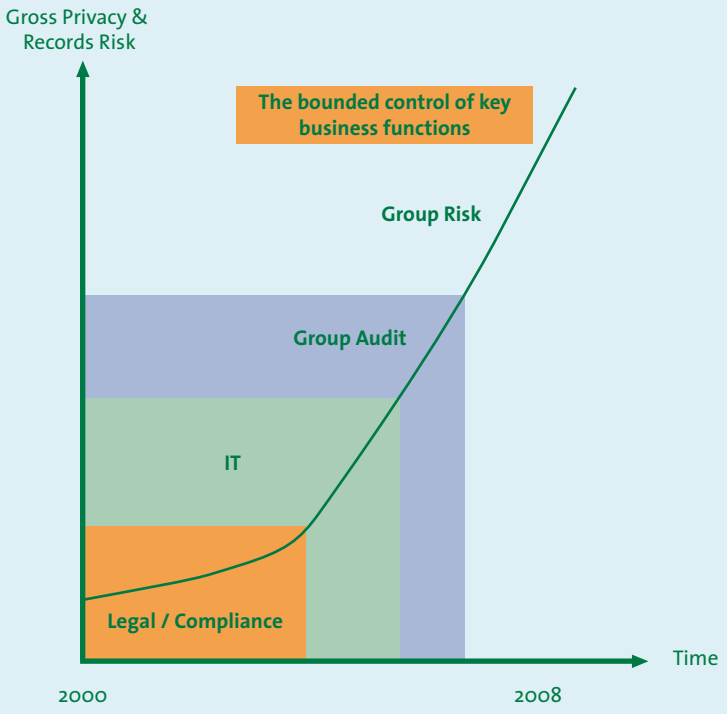


Figure 1. **The Bounded Control of Key Business Functions.**

Nothing is growing as fast as the production of information. Much of this information is linked to individuals, and some of this personal data is sensitive. At the same time, the complexity associated with processing data is also growing. These three factors are the primary constituents of privacy risk (shown here), and hence the privacy risk function is exponential. Because records management encapsulates and extends beyond personal data, a similar escalation in risk applies to records management. No single business function is equipped to manage this risk in its entirety. There can be little doubt that severe exposure is likely for those with the greatest value at stake. This is certainly the case where the legal aspects of regulation are dealt with in isolation, without also ensuring alignment with IT, assurance through audit and full integration with prevailing operational risk frameworks.

broader. Poor records management is the cause of many failures to deal effectively with customer queries and complaints. It is directly correlated to falling customer retention rates and affects customer acquisition.

Fragmented approaches tend to fail. Success depends on establishing a consistent view of information lifecycles across the organization focusing on retention, disposition and discovery. Consistency can be achieved by adopting a model centered on business activities, with similar rules applied to the records for each activity. Taking an integrated view of the approaches across several business functions can help to ensure that a consistent approach is taken to defining the categorization scheme for retention and disposition. Business users will have made decisions in the past around retention, as part of business continuity planning, and these can serve as precedents for the design and implementation of functional taxonomies that will enable category and custodial identification standards to be applied.

Litigation and Regulatory Readiness

It is a growing and significant challenge for institutions to manage the growth of data held within their systems in order to identify, preserve and manage information effectively for future use. Corporate and public bodies are increasingly subject to information requests by regulators, government institutions and the general public, whilst there is a continuing obligation to disclose electronically stored information (ESI) in legal proceedings. Having simple and immediate access to relevant information in advance of competition enquiries, regulatory investigations, Freedom-of-Information requests or litigation can save organizations time, money and inconvenience should such scenarios materialize.

Poor records management can lead to poor preparedness for the challenges of e-discovery in the US and e-disclosure in the UK. There have been various examples of records management failures that have led to heavy fines as part of legal proceedings. These include Nationwide being fined £980k by Financial Services Authority for information breaches (information security lapses), the SEC fining 5 broker-dealers $8.25M for violation of record-keeping requirements regarding e-mail and Morgan Stanley being ordered to pay $1.45 billion in a civil lawsuit, due in large part to failure to properly produce electronic documents.

The courts in the UK have started to take a greater interest in e-disclosure: for example, in the recent case of Digicel the defendants were found not to have properly searched back-up tapes. As such it is clear that proper records management can aid more effective e-disclosure and help lawyers make faster decisions on the extent of a reasonable search for documents in accordance with disclosure rules. Being able to identify rel-

Poor records management is the cause of many failures to deal effectively with customer queries and complaints

evant or privileged material quickly will also save significant costs in the event of litigation.

Some questions to consider:
- Are you ready to handle an information request, enquiry or raid?
- Do you have a comprehensive and consistently applied information retention strategy?
- Do you know where your business critical information is stored?
- Can you access and extract it quickly?
- Are your information systems effectively organized to ensure disclosure?
- Can you measure the cost of collecting, processing and producing ESI?
- Do you have a documented, defined, defendable and repeatable process for processing litigation and regulatory requests?

In litigation, internal counsel needs to understand precisely which records opposing counsel will receive in response to a discovery request. Predictability in these cases directly affects litigation success. For records to be admissible and defendable in court there must be evidence of their authenticity and chains of custody. Legal certainty here is entirely dependent upon the ability of the IT organization to align its records control framework to a prescribed set of legal and regulatory requirements. Legal certainty represents significant value at risk for many corporations that absorb sizeable litigation exposure each year.

The alignment of IT and legal functions needs to be conceptualized, planned, executed, measured, monitored and assured. Aligning them is not a simple task and can require significant rethinking, but it is vital that both parties understand the rationale for the linkage between them and the roles they play. For example, the Legal Department's understanding of the types of data, subject to legal holds and destruction must be connected with IT's understanding of the affected underlying data. Legal will determine the records stored and deleted, but IT will need to provide evidence that retention rules have been implemented. Such evidence creates legal certainty. Legal needs to be aware of current data organization, location and accessibility, and IT should be capable of establishing a chain of custody with provable authenticity. Allegations of delinquent response can be avoided by establishing, and consistently executing, precise communication protocols between Legal and IT.

Getting this alignment right requires methodology and process. Methodology is often overlooked, but is necessary in precisely translating legal requirements into traceable operational requirements, which can be broad and deep. Process can be substantiated through a formalized Responsible, Accountable, Consulted and Informed (RACI) framework, which articulates actions and allocates roles. As an example, policy approval is a role connecting Legal and IT, with Legal formally endorsing regulatory taxonomies. This provides legal certainty and assurance for the IT function so that retention and disposition rules can be applied to all storage devices.

Compliance transparency

In general, it is becoming more important for an organization to be able to quickly provide evidence of their compliance with regulations. Expectations are rising and there is a cultural shift in many organizations away from control frameworks dedicated to how a company dealt with exposure, toward more organic frameworks which seek to measure how risk events are controlled and how problems can be averted before exposure is realized.

The vast majority of records exposure a company faces resides in the past. The first step towards achieving compliance transparency is to make a conceptual split between the past and the future.

A technology roadmap is a logical starting point for considering past exposure. Roadmaps serve to baseline existing records technology capabilities against prevailing regulatory, business and technical requirements. Roadmaps include governance, alternative solution architectures (such as a records shared-service paradigm), implementation strategies and appropriate standards to reduce the cost and complexity of the current environment. All roadmap requirements should be derived from expected benefits, such as improved discoverability. In the case of regulatory requirements, effort is well spent in establishing traceability from legal rules to functional requirements that will withstand the scrutiny of substantive audit testing as a proxy for court scrutiny.

Selecting a robust records management application (RMA) is critical. RMA's should be capable of locating data outside the network topological map, as are SharePoint servers and online

It is becoming increasingly important for an organization to be able to quickly provide evidence of their compliance with regulations

collaboration tools such as Google Docs. They should be able to sift through unstructured content with text analysis and apply ontological classification enabling the information to be coherently indexed and classified. RMA's should be capable of categorization. This enables retention and disposition rules to be applied and enforced. It also supports legal holds by searching for relevant data then moving that data to a "legal hold categorized" repository.

In terms of the future, the vehicle of IT Governance is of particular use. Control Objectives for IT (COBIT) processes related to system development, technical change management and the service level management are worthy of focus as recipients of records management requirements. Development and implementation of records risk controls in these three areas invariably creates leading indicators of control, rather than traditional lagging indicators of exposure event trends. This directly supports the realization of compliance transparency.

Data retention

Data retention is becoming a real focus for Privacy Commissioners in Europe. This is due to rapid technological development in the areas of data mining supported by personal data fueled business models, and an increasing awareness of the impact this has on privacy rights. What many organizations are also beginning to realize is that data retention can have a substantial impact on the level of trust that exists between businesses and their customers.

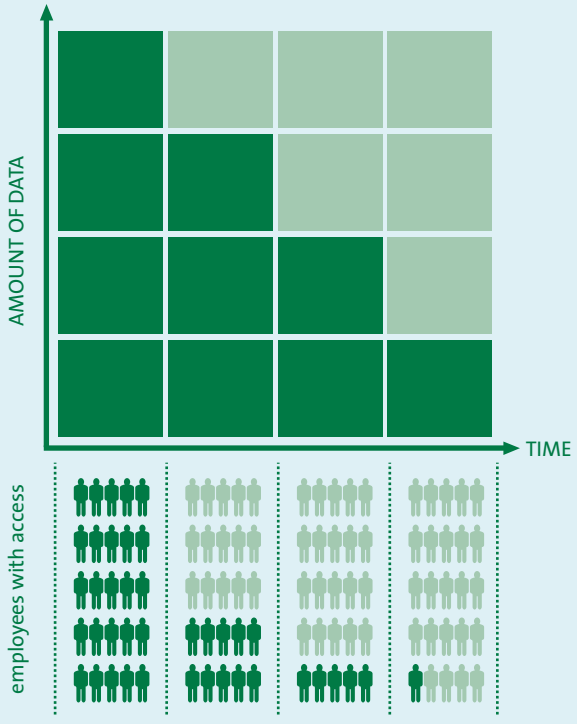
One systematic weakness in information lifecycle management, impacting upon data retention, is that in many cases the "time factor" of user access is still not given sufficient attention by organizations. The "time factor" means that there are different people with varying business needs who access information throughout the information lifecycle.

Increasing volumes of new and unique information are being generated by organizations every year. This data, in all its media forms, held within corporate groups and their business partners, needs to be retained for a finite period of time. Not surprisingly, this is presenting organizations with both practical and legal challenges.

There are two main reasons for retaining the data. Firstly, it can serve useful purposes in addition to the reason for which it was originally collected, typically including customer profiling and meeting new legislative requirements. Secondly, storing the data is often a more pragmatic solution than destroying it.

What we know from our member firms' work in this area is that search tools have improved (in particular, search technologies for unstructured text/data – a high-growth area in the Business Intelligence market), making it far easier to efficiently access large amounts of data. Furthermore, systems rarely enable the user to delete selected fields; it is often all or nothing. This results in whole data sets being retained when only subsets can be stored compliantly.

In managing the information lifecycle, many organizations still repeatedly fail to pay sufficient attention to user access, which has an impact on retention. KPMG firms often see inadequate processes, and the time factor is typically not considered when determining levels of access. However, time is an important consideration, as many users do not need access throughout the entire information lifecycle. Many staff do not need to access stored data at all in order to fulfill their business roles. For example, front-end customer support staff can comply with applicable bookkeeping regulations without the need to call up stored data. Similarly, account staff do not have a business need to access information about customers stored in CRM systems.



The Data Retention Staircase is neither a solution nor a methodology, but illustrates the challenge of access controls and data retention., assisting an organization in mitigating the risks of potentially illegal storage.

Figure 2. **Data Retention Staircase**

Insufficient access controls and deletion routines frequently lead to fundamental privacy principles being contravened, as large volumes of personal information become accessible to people with little or no business need to use the information. In the days of paper storage, this was not a problem. Records were physically moved into archives. But with data stored electronically, inappropriate access to information is now a major concern.

The vertical axis of the Data Retention Staircase in Figure 2 depicts the volume of personal data. The horizontal axis depicts time. The employees in dark blue are those with an actual need to access the data. The employees in grey have access, but no business need. Importantly, this model illustrates that legitimate access to data is required by fewer people over time, so that in planning storage and access, regular re-assessments of both employee needs and storage requirements should be made.

Data retention can be managed effectively, without the need for systems overhaul, by following a six-step process:
1. Create an overview of the personal information being processed in the company. In some cases, Operational Risk process definitions are well suited to establish information lifecycles.
2. Map all relevant legal requirements (including business needs, if they contribute to the rationale) relating to data storage and any additional purposes identified in Step 1.
3. Assess current retention levels and policies against requirements throughout the information lifecycle.
4. Identify the staff with access to information and map them against the purpose for processing the data.
5. Provide a view of all gaps:
6. Information kept without a defined purpose
7. Individuals with access but no established need.
8. Close gaps:
9. Delete excess information
10. Embed and enforce appropriate access controls.

Controlling storage costs

Nothing is growing as fast as the production of information to the extent that associated storage costs have outstripped falling per-gigabyte storage costs, improvements to drive capacity and disk performance. The "save everything" approach does not make economic sense (and neither is it a recommended litigation management strategy), while storage reduction solutions such as de-publication can create problems with legal admissibility of records. A typical organization holds between 10 and 30 copies of each document. Many of these are no longer needed; some are misplaced or even unknown. Storage optimization and process efficiency have become important business objectives.

Process improvements and a well thought-out infrastructure strategy are key factors in controlling storage growth. Records requirement, in many cases, needs to be incorporated into business processes through automatic content analysis, identification and classification.

Infrastructure strategy encompasses many elements. Duplicate management, e-mail filtering and archiving, backup, data center approach, tape restoration and data classification all play a part. But infrastructure strategy also considers the presentation layer. Records functionality will need to become abstracted into common user interfaces, particularly e-mail, providing users with support for identification and categorization. Consequently, employees will become increasingly responsible for identifying and classifying records.

In computing, virtualization is a broad term that refers to the abstraction of computer resources typically at the platform, storage, resource or network layer. In virtualization, users do not necessarily know what resources they are using. In enterprise environments those resources usually are controlled by the company, but the resources can also be external, which means that it is difficult to know where that data will be stored, processed and transferred.

Virtualization of storage helps achieve location independence by abstracting the physical location of the data. The virtualization system presents the user with a logical space for data storage and handles the process of mapping data to its actual physical location. This means that the data can reside at several locations and in locations unknown to the user. In virtual storage the host only deals with the logical space. Any changes to the meta-data mapping are transparent to the host, meaning the data can be moved or replicated to another physical location without affecting the operation of any client.

In storage virtualization the physical storage resources are aggregated into storage pools, which can be added as and when needed, with the virtual storage space scaling up by the same amount. Many data retention policies state that data must not be stored beyond the end of its lifecycle. When the data is scattered in different physical disks in the storage pool, it is difficult to physically destroy the disk containing the record. Therefore these records need to be erased from the virtual storage using other means, such as specific software that is designed to reliably erase data from disks. On the more positive side, since multiple independent storage devices appear to be a single monolithic storage device they can be managed centrally, which can help in data lifecycle management. Although a virtual storage infrastructure benefits from a single point of logical disk

Case studies

Case Study 1 – Global Financial Services Company
For a global financial services company, KPMG created an inventory of all electronic record types, defined a compliance framework in accordance with the company policy and standard operating procedures, established the internal controls for record repositories and processes, and conducted risk and gap analysis by determining nonconformity with the company's e-compliance framework. KPMG worked closely with senior management to develop a remediation strategy and a plan to correct the gaps.

Case Study 2 – Retail Correspondent Clearing Firm
KPMG performed a records retention process improvement program specifically for account records for a large retail and correspondent clearing firm. Current state policies, processes, and documentation were identified and desired state polices and processes developed with operations and technology management. The team prepared process-improvement observations with recommendations for change, and provided a roadmap for addressing open issues.

Case Study 3 – Manufacturing Company
KPMG managed the development of the regulatory and legal requirements for a corporate retention schedule for a manufacturing company. KPMG led a risk appetite workshop with key stakeholders to understand the organization's "risk appetite" and designed a corporate-wide program to meet regulatory compliance demands.

Case Study 4 – Insurance Company
As part of an overall legal and compliance process review, KPMG assessed an insurance company's policies, processes, and procedures for creating, maintaining, accessing, and destroying pertinent company records. Of particular concern were records relating to policy forms and producer licensing information, thus a comprehensive program was developed.

Case Study 5 – Utilities Company
For a large southeastern U.S. utilities client, KPMG was tasked with
a. developing an enterprise information security program,
b. developing a dynamic and sustainable compliance program,
c. developing performance metrics to be utilized in assessing operational and business performance, and
d. designing, implementing, and managing an enterprise information management and protection program.

and replication service management, the physical storage must still be managed. For example, faulty disks need to be identified, properly destroyed and replaced.

Meta-data is a key component in virtualization, since once the data has been virtualized, the meta-data is the only thing making it possible to access the information. If the meta-data is lost, so is all the actual data, since it is virtually impossible to reconstruct the logical drives without the mapping information. Hence it is important to be able to reconstruct the meta-data in the event of a failure. Meta data has also been admissible in US court proceedings.

Conclusion

As structured and unstructured records grow in both the volume and the risk they represent, it becomes more important for organizations to re-think the processes by which they manage records. Are they adequate today and will they suffice for tomorrow are questions well worth asking.