1.0 Introduction

When I started to write this article I had a particular objective in mind, as a result of my own experiences in records and information management from 1975 to 2015. And like our world, that changed. When I consider that I have been involved in Archives and Records Management for 40 years, I decided that my career, through a variety of organizations, had exposed me to all aspects on information governance, albeit under different names. And I have a strong belief that it helps to understand where we have come from, to put some perspective into where we are going.

This is not a comprehensive, all-inclusive study. Rather it is an overview, from a personal perspective, of how we have evolved from records management to information governance and describes some Canadian initiatives which have both influenced and impacted that evolution. It's fair to say that I was fortunate in working in organizations that varied in their records issues and I participated in everything from strategy development to records centre operations to building an archival facility and playing internal RIM consultant to one of Canada's largest financial institutions. Needless to say they exposed me to many different learning opportunities and facets of what now falls under the umbrella of information governance.

I have attended a number of ARMA International Conferences over the years (the first one in Toronto in 1975!!) and heard speakers discuss many different topics. One of the presentations that struck me the most was at the 2005 ARMA International Conference, in Chicago, when Daniel Burrus, the keynote speaker, talked about the future being visible in his presentation, *Future View, A Look Ahead*. One of his key themes is articulated in this statement:

> You need to visit a place that I call the *visible future*™. It is a place you can clearly see, but you have to take the time to look. Most of us never take the time to look. The *visible future* is the fully predictable future. The more you look and ponder the future that you know is coming, the more you can capitalize on that future.

In 1995, at an ARMA International conference in New Zealand, one of the speakers was demonstrating what would happen to telephones in the future, based on research being done in the field. It looked totally impossible….seeing the people we were talking to??? And where are we today? It was the visible future! Daniel Burrus' point was that if we pay attention to innovation and research being done in such places as MIT or CERN, these organizations give us a look into what is coming down the road.

If we look back at how we got to where we are today, it is not difficult to see that the evolution of technology created the big data environment we now live. It is hard to imagine a world without email and the world-wide web. But 50 years ago, that was the reality. How did technology change our workplace and lead to the era of information governance? Did it suddenly happen or was it an evolutionary process? Look at these key dates[1]….innovation that just kept going and it continues today.

- 1930's – mainframe computer is created
- 1969 – ARPANET – predecessor of the internet first created.

- 1976 – Apple 1 home computer is created
- 1979 – first cell phone network created in Japan
- 1981 – first IBM PC sold to the public
- 1989 – Tim Berners-Lee and Robert Cailliau build the prototype of the World Wide Web at CERN, the European Organization for Nuclear Research.
- 1994 – American Government releases control of the internet and the World Wide Web is born - just over 20 years ago. And how did that impact the workplace?

What changed and why now? The early 1990s saw the introduction of personal computers in the office, bringing with them the idea that records management would no longer be required. Computers could do it all. At that point, the web was in its infancy and used to transmit emails. Organizations were still sending letters and reports through inter-office mail and via Canada Post. Pre the internet, information generated through computers was managed internally and protected by IT departments. It was some time before information was shared and transmitted electronically between departments, business units in different locations and in different countries. The Internet changed everything.

And Now We Have Big Data

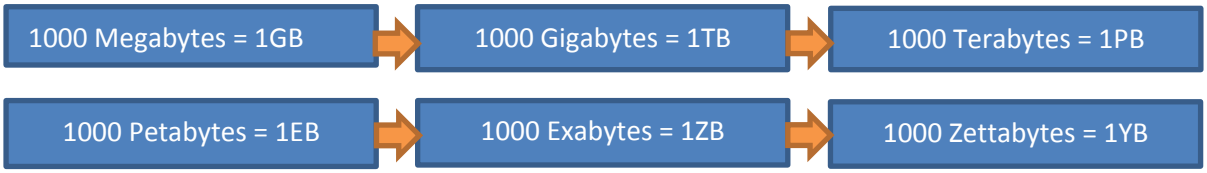
And big data didn't just happen! People have been writing about the volumes of data being created and stored since the mid 1940's[2].

Think about your organization – how is information received, used, transmitted and where is it stored? It's the same with your personal life. How many different devices does YOUR home have? How many different ways are there today to create and share information with each other? The following list gives examples of why data volumes are increasing daily. And if it supports your business, then it needs to be managed.

- The internet and wireless transmissions allow us to create and share information through text messages, blogs, Twitter, Instagram, Facebook and a myriad of other social media connections.
- Smart devices communicate with each other. Hydro and gas companies have smart metres; OnStar can provide updates on your car's maintenance status from data it has captured on the car's computer system. GPS Locators on your phones, iPad, etc. can tell where you are. All that data is being collected by the organizations that are tracking it.
- Large organizations such as financial institutions and insurance companies capture huge volumes of transactional data daily as customers do their banking online, through bank machines or any other technology that financial institutions have provided to interface with clients.
- In addition to all the structured data in systems we are still faced with the unstructured data generated by employees in their day to business in network directories, emails and system applications that support content management, etc.

In 2007 EMC and IDC[3] published their first study on the Digital Universe in an attempt to project the growth of data creation as a result of the World Wide Web. In its 2014 report the projection is that

By 2020 the digital universe – the data we create and copy annually – will reach 44 zettabytes, or 44 trillion gigabytes[4].



And the old adage, storage is cheap, keep everything forever has now come back to bite IT departments who find themselves with terabytes and more of data that is old and even inaccessible. There are costs of managing electronic data over time as software changes and is no longer supported. Disposal, as part of an overall business activity, is a necessity in reducing costs and risks and improving efficiency in any organization. And if you cannot find the right information when the judge asks for it, it can lead to out of court settlements in the millions of dollars in today's litigious environment.

How Old Is Information Governance?

Information has been around for a long time, whether it was referred to as non-record, transitory, or publications and databases. For years, organizations relied on paper as "records" (and still do) as the major source of evidence of transactions and business decisions. With the advent of technology and the proliferation of trans-border dataflow, issues such as privacy, information/data ownership, and security all started to take on a new meaning with the realisation that electronic information assets are much easier to access.

Information, like records, is stored in so many different places as organizations move to serving clients though social media and the Cloud. It is created every day and still needs to be managed, used, stored and disposed of in accordance with business and regulatory requirements. As more and more records, data and information are stored electronically the practices that were applied to paper are now required in the electronic world and are being built upon to embrace this new workplace.

Many of us are members of North American organizations and articles we read are often presented from that perspective. How long has "information governance" been on the radar? At the 2015 Information Governance Initiative (IGI) conference in Hartford Connecticut, the question was posed to the audience….5 years? 10 years? More than 10 years? The majority of the audience responded to number one – 5 years. From the perspective of what we mean by information governance, the actual answer is "longer than 15 years", driven initially by the need to ensure privacy of personal information.

Privacy, security, records retention and disposition are needed, regardless of what medium records, information, data are created and stored. Organizations now recognize the need to bring together what have previously been siloed departments and groups as cross-functional teams, to address the issues from an organization-wide perspective, because of technology and information transmission and exchange globally. Policies and procedures for each component cannot be drafted in isolation based on

a particular area of interest, such as IT, Privacy, Business, Legal and Risk and Information Management. The requirements overlap and have to be addressed as part of the whole. And an information governance framework is now where the pieces come together. Components of IG have been in place for a long time, albeit in separate departments. So how is it defined today?

Information Governance: Some Perspectives

As information governance has evolved, the definition has varied, depending on the particular source and perspective. There are, however, consistent themes across all the definitions.

The National Health Service in the UK has created an Information Governance Toolkit[5] to ensure that the information collected as part of the overall operations of the health system in the United Kingdom is managed in accordance with the Caldicott principals (discussed later in this paper). It states that:

- Information governance is to do with the way organisations 'process' or handle information. It covers personal information, i.e. that relating to patients/service users and employees, and corporate information, e.g. financial and accounting records.
- Information governance provides a way for employees to deal consistently with the many different rules about how information is handled…

Gartner, Inc

Founded in 1979, Gartner is well known for its research and reports that are widely referenced in the IT and information management communities. In 2007, Gartner identified information governance as being a "top of mind issue" for its clients describing it as:

- The specification of decision rights and an accountability framework to ensure appropriate behaviour in the valuation, creation, storage, use, archiving[6] and deletion of information. It includes the processes, roles, standards and metrics to ensure the effective and efficient use of information in enabling an organization to achieve its goals

The Sedona Conference[7]

In the Sedona Conference Journal, Volume 15, Fall, 2014, an article titled *The Sedona Conference Commentary on Information Governance* proposed the following definition:

- (Information Governance) means an organization's coordinated, inter-disciplinary approach to satisfying information compliance requirements and managing information risks while optimizing information value. As such, information governance encompasses and reconciles the various legal and compliance requirements and risks addressed by different information-focused disciplines, such as records and information management ("RIM"), data privacy, information security, and e-discovery. Understanding the objectives of these disciplines allows functional overlap to be leveraged (if synergistic); coordinated (if operating in parallel); or reconciled (if in conflict)

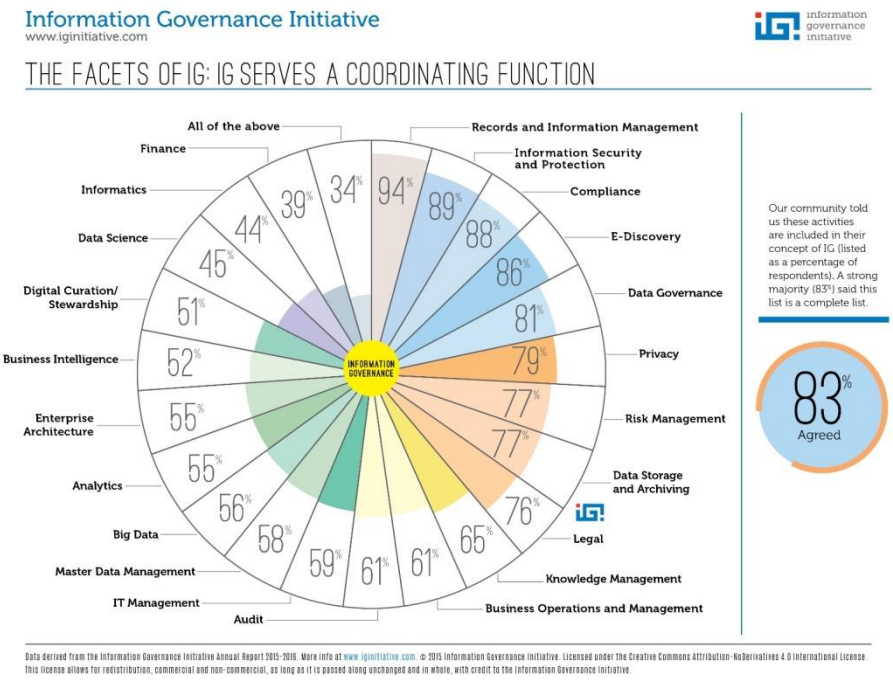
The Information Governance Initiative (IGI)

The Information Governance Initiative (IGI), established in 2013, is a cross-disciplinary consortium and think tank dedicated to advancing the adoption of information governance practices and technologies through research, publishing, advocacy and peer-to-peer networking. In its 2015-2016 Annual report IGI presented its definition of and set of components for information governance based on its IGI community input:

> Information governance is the activities and technologies that organizations employ to maximize the value of their information while minimizing associated risks and costs.

The Components of Information Governance[8]

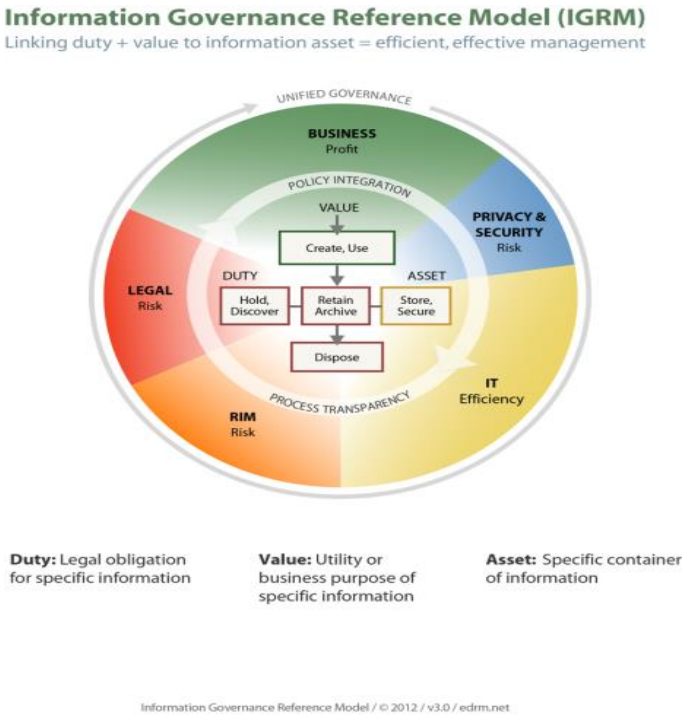
In its Annual Report 2015-2016, the IGI presented its findings from a research survey sent out to its IG community members asking them to highlight which of twenty-two activities they felt fit into the domain of information governance. The following graphic reflects the results of the survey:



A number of these components, consolidated, would fall under the information governance Reference Model, as defined in a 2011 whitepaper - How the Information Governance Reference Model (IGRM) Complements ARMA International's Generally Accepted Recordkeeping Principles (GARP®)[9]:

- The IGRM supports ARMA International's GARP® Principles by identifying the cross-functional groups of key information governance stakeholders and by depicting their intersecting objectives for the organization.

The Information Governance Reference Model depicts areas who have interest in the organization's information assets and which require collaboration in today's environment, with RIM as one element in the cross-functional approach.



The reality is that depending on where you practice records management, what your responsibilities are or the type of organization in which you work, your exposure to the components of information governance will have varied. Someone working in a school board environment in Canada for the past number of years could have had responsibility for privacy, records management and compliance. In a financial institution you may have been the records manager who had to ensure that security, retention and privacy requirements were built into a system design process.

A Look in the Mirror

The Evolution from Records Management to Information Management: 1960 - 2000

To understand the transition from records management to information governance, it is helpful to look at how each has been and is being defined. In 1969, Bill Benedon[10], considered one of records management's luminaries, published *Records Management*[11], devoted to, as the title implies the component of records management program design and implementation. Benedon writes:

Records Management is a term well chosen for covering information processing activities now and in the future. New innovations, such as magnetic tapes and other forms of miniaturized documentation, while changing the complexion of the record, still present the same problems of retention, storage, forms design, reporting needs, protection and of course, the oldest of all, filing requirements, now referred to in a much more fanciful manner – retrieval.

He goes on to add "it will be quite some time before accounting and auditing people are willing to say that once you have your information in machinable form, you can throw away the source document".

Close to 50 years later we are now dealing with having seen the source document changing from slowly to paper to digital….and we need to start disposing of the digital format!

1981 saw the publication of the Second Edition of *Information and Records Management* by Maedke, Robek and Brown, a book which became the basis of many records and information management course curricula. It defined records management as:

- The application of systematic and scientific control to the ***recorded information*** that is required in the operation of an organization's business. Such control is exercised over the creation, distribution, utilization, retention, storage, retrieval, protection, preservation and final disposition of all types of records within an organization.

In 2001, the first International records management standard (ISO 15489) issued through the International organization for Standards (ISO) defined records management as:

- The field of management responsible for the efficient and systematic control of the creation, receipt, maintenance, use and disposition of records, including processes for capturing and maintaining evidence of and information about business activities and transactions in the form of records.

The common element in all the definitions was the need for a systematic approach to managing records and recorded information. So what has changed? Did records disappear or were they absorbed into information management as technology began to emerge in the workplace?

Records and Information Co-exist

Information has always been created on many different media and in a variety of formats as have records. In the paper world, we had records and non-records or transitory records (information!). Convenience copies, drafts of reports, reference and research reports were all created in the day to day business of the organization, had different retention periods and were disposed of in accordance with the agreed upon policies. However they were not records because they did not provide evidence of decisions made by the organization.

Before personal computers, the internet and social media, databases stored data and generated printed output from those databases. Financial reports, payroll summaries, inventory listings, etc. were considered records and subject to corporate retention periods. From an IT perspective retention was focused on the period of time for which data was kept on servers or on tapes, rather than on the information content.

As more and more information was created at the desktop by knowledge workers[12] and data was stored in systems rather than printed to paper, legislation changed to allow for electronic transactions in place of paper. The internet impacted everyone, less time was spent printing and filing and more information was left in shared files on networks, in legacy systems, on backup tapes, etc. And so began the CIO's

nightmare. Not only was more information being created electronically but what about all those old systems that contained obsolete data and all those old tapes in the data centre that no-one had indexed? How could data be disposed of?

Addressing Data in Systems: The Archivists Started It!

Machine Readable Archives Division: Public Archives of Canada.

I was first introduced to the concept of electronic records as an Archivist at the Toronto Harbour Commission. During a visit to the Public Archives of Canada in the mid-1970's to learn about records centre operations, records management policy and procedure development and various aspects of archival operations, I met with staff in the Machine Readable Archives Division. Archivists were dealing with challenges of managing and ensuring the long-term preservation of data in systems many years before records managers and IT departments and Canada was among the leaders in dealing with machine readable records. In his article *FOCUS: The Machine Readable Archives Division of the Public Archives of Canada* (Archivaria, 1978 (176-180)) Harold Naugler reported that:

> "As part of the Federal Government's EDP records management program…the Office of Records Management Services of the Public Archives of Canada undertook in 1976-77 an inventory of machine readable records in some sixty-seven government departments.

Naugler further stated that:

> "There are vast amounts of information in machine readable form covering such varied aspects of national life as employment, crime, disease, immigration, emigration, climate, geology, food production and consumption, housing, transportation, communication, and the cost of living.

The methodology used in the inventory process was subsequently developed into a set of guidelines created by the Machine Readable Archives (MRA) Division[13] which later became part of the government's Guide on EDP Administration.

In 1984, recognizing digital preservation as a global issue, Harold Naugler authored *The Archival Appraisal of Machine-readable Records: a RAMP study with guidelines* published under UNESCO's General Information Programme and UNISIST. At that time it was viewed as one of the leading publications addressing electronic data management.

Groups such as the Association of Canadian Archivists, the Society of American Archivists and the International Council of Archives were appraising records and data in systems for long term preservation. Did managing data in systems need someone to understand what the systems were and what data was created, apply retention requirements and ensure that the formats and storage media were appropriately preserved? Yes. Did we call it information governance? No. It was a piece of the puzzle.

RM becomes IM becomes IG: Revolution or Evolution?

In 1989 when I joined CIBC as the Manager of Archives and Records Management, I was part of the Corporate Governance Group, the components of which reflected the current view of information

governance. The Corporate Governance Group consisted of individuals involved in Records Management and Archives, Legal, Compliance, Privacy, Audit and the Corporate Security teams. The Records Management group collaborated with other members of the department, depending on the specific projects. The issues were cross functional and too big for one group to address. The Records Management Group worked with the IT group to incorporate records retention into the Application Development Lifecycle and software selection included members of the RIM team. The RIM group were internal consultants and participated in decisions about electronic records and transactional data, hardware and software selection.

Many articles and publications which reference the beginning of the concept of information governance point to the National Health Services (NHS) in Great Britain as one of the leaders in establishing an information governance framework. In 1997, as a result of concerns over privacy and the impact of technology on patient data, Dame Fiona Caldicott chaired a panel to look at patient identifiable data and how patient information was handled across the NHS. As a result of that review and subsequent work, seven principles, known as the Caldicott Principles[14] were created. Those Principles continue to be used today to assess whether or not information containing patient information is being managed and protected properly. Information governance has now become the mainstay of the NHS and is supported by toolkits, policies and procedures and guidelines.

The level of involvement RIM professionals have had with some or all of the components of information governance has been driven by the type of organization in which they work. Someone working in a small municipality as the City Clerk may find themselves responsible for RIM, Privacy and Legal. In a large financial institution, the RIM professional may be part of a cross-functional team where individuals are responsible for the IG components. As a RIM professional in a law firm, eDiscovery might be the driving factor behind IG for clients. The regulatory environment under which the organization operates may create a stronger need for a focus on different IG elements but in the final analysis a successful IG program is the sum of its parts.

Information Management in the Government of Canada

Information management and records management have coexisted for many years in the Federal Government of Canada. The Government of Canada's Information Management program grew out of the 1989 issuance of the Management of Government Information Holdings Policy, an initiative of the Treasury Board Secretariat, which "consolidated existing policies on records management, information collection and public opinion research, micrographics, EDP records management and forms management".

In 1995[15], Treasury Board Secretariat issued guidelines on Managing Government information and included a model which showed the lifecycle of the information holdings stating that information management programs were responsible for:

1. Planning
2. Collection, creation, receipt
3. Organization, transmission, use and retrieval

4. Storage, protection and retention
5. Disposition through transfer or destruction

At that time, a 55-page user manual supported the overall implementation of information management in Federal Government departments. As the workplace has changed, so too has the policy title – 2003 saw the creation of the Policy on the Management of Government Information which was replaced in 2007 by the Policy on Information Management.

To explain the relationship between records management and information management in the Government of Canada would be a study unto itself, requiring a detailed look at the policy development roles and responsibilities of the Public Archives of Canada (later to become the National Archives and now Library and Archives Canada) and the Treasury Board Secretariat. What was previously known as records management within the Federal Government has now become Recordkeeping Practices under the Directive on Recordkeeping, first issued in 2009:

> Recordkeeping is a resource management function through which ***information resources of business value*** are created, acquired, captured, managed in departmental repositories and used as a strategic asset to support effective decision making and facilitate ongoing operations and the delivery of programs and services.

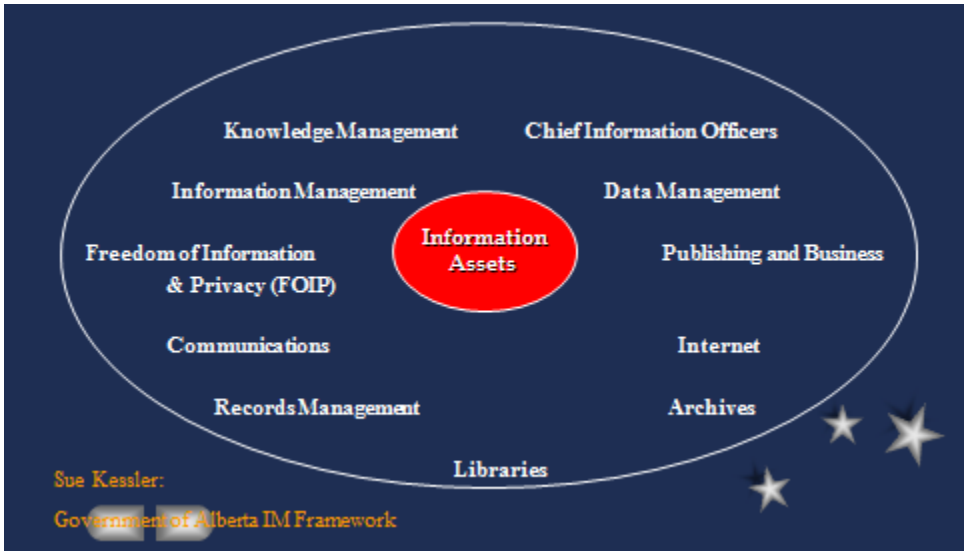
What has changed? Information resources are created across every organization. Some need to be kept to meet legal and compliance requirements and others can be disposed of. In the case of the Federal Government's recordkeeping policy, records have now become information resources of business value. Can we project what will be next?

The Government of Alberta Information Management Program

Many records management programs were created as part of a facilities management function, since paper was transferred to a records centre at the end of its active phase in the office. Typically, the perception was that managing records was a physical activity in a storage warehouse. As technology was introduced into the workplace, the perception of records management continued to focus on paper! The fact that computers were now creating and storing data and information, some of which were records, was difficult accept, as records management continued to be viewed as paper-based supported through records centre operations. Organizations began to transition from records management to information management as computers became more and more prevalent.

How was the information to be managed? In the paper world it had been defined as non-record or transitory records. In the electronic world it was all captured and stored together as a set of ones and zeroes. And it was necessary to change the concept of records to address the changing needs of the workplace. It was the content that mattered, not the medium on which it was stored, and the legal environment began to address the electronic workplace through such legislation as Electronic Transactions Acts.

In Canada, one of the leading government information management programs was that of the Government of Alberta whose Information and Technology Strategy was adopted by the Deputy Ministers' committee in 2001. The main reason for the transition from records to information was that "records" were perceived as paper only and the workplace was moving towards a much broader context of electronically stored information, some of which was identified as a record.



Recognizing the need to manage the Government's information assets, including its records, the then Director of Information Management, Sue Kessler, working closely with Dr. Mark Vale,[16] created an Information Management Framework[17], which from today's perspective covers the majority of the pieces as defined in an information governance model.

The Government of Alberta's Information Management guidance and resources were, and continue to be, used not only by the Government of Alberta's departments but by both the private sector and other governments, to transition from records management to information management.

As records management has evolved to information management to information governance, the scope has expanded even though the fundamental activities required for program management have not changed. Regardless of what we are managing, we still require:

- Strategies and frameworks
- Policies and procedures
- Standards and guidelines
- People,
- Processes and
- Technology

The medium through with the records and information are transmitted is changing and the volume is increasing daily but the concept of the lifecycle or continuum still exists and the need for organizations to be accountable and compliant has not gone away.

Data Protection and Privacy

Early Drivers towards Privacy Controls: OECD Model Privacy Guidelines[18]

The need to provide oversight to data in systems has been of concern for some time in international organizations such as the Organization for Economic Cooperation and Development (OECD), an organization which Canada joined in 1984. In 1980, the OECD created its Guidelines on the Protection of Privacy and Trans-border Flows of Personal Data stating that:

> The development of automatic data processing, which enables vast quantities of data to be transmitted within seconds across national frontiers, and indeed across continents, has made it necessary to consider privacy protection in relation to personal data.

The OECD was concerned that the amount of personal data being captured through large data processing systems would put privacy at risk and encouraged the member countries to create their own national data protection and privacy legislation, which Canada did in 1983.

With technology, not only was privacy a concern but also data could now be easily transmitted across international borders, raising concerns about country specific legislation in such areas as data ownership. Local laws around data ownership could limit the ability to share information within an organization doing business globally. Industries such as banking and insurance were particularly concerned about restrictions on trans-border data flow created by country-specific laws, given the nature of their international businesses.

The OECD model guidelines were intended to support harmonization of privacy laws while supporting trans-border data flows as technology changed the way data was transmitted and shared. In celebrating the OECD Guidelines 30 year anniversary in 2011, OECD stated that:

> The stand-alone technologies of the 1970s have become a ubiquitous, integrated global infrastructure. Occasional global data flows have given way to a "continuous, multipoint global flow," highlighting the need for privacy enforcement authorities around the world to work together to develop globally effective approaches to protecting privacy. Advances in analytics and the monetisation of our digital footprints raise challenging questions about the concept of personal information and the appropriate scope for the application of privacy protections.

Canada, driven by the need to comply with the OECD guidelines as a result of being a member, created Privacy laws at the national and provincial levels, together with a strong privacy infrastructure in government departments. Recognizing the need for access to information, alongside data protection and privacy, the Federal government enacted two separate laws in 1983: The Access to Information Act and The Privacy Act[19]. As more and more information was captured in databases and systems across government departments, policy frameworks, as discussed earlier in the paper, incorporated the necessary security and controls to ensure that personal information was appropriately collected and managed.

How did the legislation impact non-government departments? Why would non-government records managers have to be aware of the Access to Information Act? Any organization which was required to

send records to the Federal Government, for example, the Salvation Army[20], had records in Canadian Government departments and as Access to Information legislation was being enacted the Records Managers in non-government organizations had to be aware of what records were shared with the Government of Canada and the measures in place to control access to and manage the privacy of third party records as part of their overall RM activities.

Being Proactive: Building Privacy into Technology

Privacy by Design[21]

As more and more information was collected and stored in systems, the need to ensure that privacy was protected to meet the requirements of the various federal and provincial privacy acts resulted in the development of privacy guidance and controls.

Ontario has played a leading role in the privacy domain both in Canada and internationally as a result of the work of Dr. Ann Cavoukian, who served as Information and Privacy Commissioner (IPC) of Ontario from 1997 to 2014. Dr. Cavoukian believed (and still believes strongly) that rather than wait until privacy became a problem in technology, it was necessary to build privacy protection methods into the overall technology development and design and outlined her position in her 1995 paper: *Privacy-enhancing Technologies – A Path to Anonymity*[22], written in conjunction with the Netherlands Data Protection Authority. Committed to ensuring that privacy is an integral part of everyday business practice, Dr. Cavoukian created *Privacy by Design* which incorporates the following seven principles to be applied to privacy and technology:

- Proactive not reactive; preventive not remedial
- Privacy as the default setting
- Privacy embedded into design
- Full functionality: positive-sum, not zero-sum
- End-to-end security: full lifecycle protection
- Visibility and transparency: keep it open
- Respect for user privacy: keep it user-centric

The Privacy by Design framework was adopted as an international framework for privacy and data protection in 2010.

Dr. Cavoukian's work on *Privacy by Design* continues today at Ryerson University in Toronto where she is the Executive Director of the Privacy and Big Data Institute. Her work has led to the creation of a program, in partnership with Deloitte Canada, against which companies and organizations, which have embedded privacy into their day to day operations and comply with the 7 *Privacy by Design* Principles, can be certified.

Information and Data Security

For many of us who started in records management before the impact of technology, *security* referred to locked offices, filing cabinets and work spaces. Security classifications were determined by the importance of information to the organization whether on paper or in electronic form. The most common designations included confidential, restricted, internal use and public. Organizations might

have additional designations depending on the information, such as top secret and secret in government organizations.

Before the implementation of systems security controls, access and retrieval rights to online information and data were controlled through designated individuals, to ensure that appropriate persons were given access to the right documents, depending on what permissions they had.

Since the majority of the information resources were managed within the organization, the physical security issues were more easily controlled. As organizations have moved to automated systems, the Cloud and the internet, the need for security controls has increased and the ways to implement the security controls have changed.

Today's Real Threats

We all hear about security breaches. As the Records and Information Manager how involved are we in knowing where those risks to our information assets exist?

The issue of information security is not new. Recognizing it as a key element of access and privacy, in 1986 the Treasury Board Secretariat introduced the Government Security Policy intended to: "ensure that all classified and designated information or assets of the federal government are safeguarded in an appropriate manner".

As the use of technology has expanded into the internet of things, BYOD, Social Media and the Cloud, information security becomes another element of the information governance framework. International standards, such as ISO 27002: Information Technology — Security Techniques — Code of Practice for Information Security Management Standard[23] (just one of a number of standards that support information management and information security, listed in Appendix "A"). Security standards are being created to identify security control measures, practices, which include procedures or mechanisms that may:

- protect against a threat,
- reduce a vulnerability,
- limit the effect of an unwanted incident,
- detect unwanted incidents, and
- facilitate recovery.

Cyber-crime has become the number one issue that governments are now addressing. And whether the targets are governments, companies or individuals, the threat can have far-reaching implications. We hear about these breaches on the news and wonder what the impact is.

Recently TalkTalk, a telephone and broadband supplier in the UK was hacked, with the hackers gaining access to TalkTalk's client account information. While on vacation in the UK, the day after the breach was reported, we overheard a conversation in the pub telling the bar tender that his bank had called and told him that someone had gone into his bank account and attempted to clear out his money, based

on information in his TalkTalk account. What was interesting about this particular case was that the company had had an audit about two years prior to this event, in which the lack of system security was flagged and nothing was done to upgrade it.

On January 3, 2016, this note was on TalkTalk's website:

> **Welcome to TalkTalk**
> We're currently making security enhancements to our site, which should be back online soon. While we do this, our customer team are there to help you with details on the packages below or upgrades. Just give them a call.

It is no longer sufficient to assume that information security is the IT department's responsibility. Information security, privacy and disposition problems are crossing boundaries between departments which have responsibility for identifying and protecting that corporate information. Being able to understand the concepts and information security issues is critical to RIM within today's workplace.

RM Meets Technology

In my first job as Archivist at the Toronto Harbour Commission, I was responsible for purchasing a Wang word processor and learning how it functioned. That was 1978 - and some time before personal computers were adopted as a standard technology in all organizations. At the AGO in 1984, as the Manager of Administration and Archives, I was involved in the overall technology strategy because of my role in Archives and Records Management.

In 1989, as Manager of Archives and Records Management at CIBC, I worked with RIM staff to select and implement a records management software package designed to support the storage and disposition of about 400,000 boxes in the Toronto Records Centre. In addition to selecting software for our own records management purposes, the team were involved in the selection of an imaging system and worked with IT to build retention requirements into the system development lifecycle. Understanding what was happening with technology was not a nice to do…it was a must do.

For many years, the mantra "storage is cheap" could be heard in many organizations as more and more information was created electronically and IT "retention" was focused on moving live data to tiered storage, not on the value of the data to the organization. Managing data was complicated and therefore something that didn't happen, until concerns were raised about legacy systems and Y2K. At that point, organizations were still for the most part, managing "records" on paper and data was retained for disaster recovery, back up and security purposes. Given the transition from paper records to data and information in systems and the lack of retention applied to legacy systems and backups, IT organizations suddenly found themselves with terabytes of stored data that could not be disposed of because no-one knew what it was. What was the risk of deleting without any awareness of what was in those systems? How could you justify that in court? On the other hand, all those old tapes sitting in data centres, uncatalogued, not cared for in terms of preservation methods – rewinding, migrating, etc. could be a huge liability to eDiscovery. Being at the table for those discussions was part of the RIM responsibility.

Defining Software Requirements: The Canadian Influence

Canada and Canadians have played a leading role in designing specifications for records management software as well as creating software products, based on those specifications. Early work in Canada began in 1983 through an initiative of the Department of Communications and the National Archives of Canada: The Office Communications Systems Field Trial Program. Designed to study how 70 users, linked together through a local area network, created, used and disposed of electronic ***information,*** it provided important research data for ongoing solution development. Its work resulted in the creation of the Information Management Office Systems Advancement (IMOSA) project, a joint initiative between the National Archives of Canada, the Department of Communications Canadian Workplace Automation Research Centre and Provenance systems[24]. In 1990 as a result of the IMOSA project work, the National Archives published a set of functional requirements for software to manage electronic information in the Federal Government known as FOREMOST (Formal Records Management for Office Systems Technologies).

At the time the Canadian requirements were developed, the electronic records community within the International Council on Archives was collaborating on software requirements. While it would be difficult to say that Canada was number one in creating the requirements, it would be fair to say that the work undertaken through the IMOSA project was on the leading edge of defining electronic records management software requirements. A number of software requirements initiatives were subsequently developed in Australia, the US and Europe and continue to be enhanced today.

Creating Electronic Records Software Solutions

Canada, again, has played a significant role in electronic records management software development. As a result of his work with the Canadian Federal Government, Bruce Miller established Provenance Systems in 1989, and created FOREMOST, an electronic records management software package which was sold to (EMC) Documentum in 2002 forming an integral part of the Documentum Records Management product. Bruce subsequently created Tarian software as the next generation electronic records solution, the Tarian eRecord Engine, which in 2002, was acquired by IBM to become IBM Records Manager.

Records Managers globally are familiar with OpenText and its LiveLink product suite. Its evolution from its beginnings to where it is today is a great study in Canadian innovation and development. In his Forward to *Open Text Corporation: Ten Years of Innovation*[25], Tom Jenkins, then CEO of Open Text Corporation wrote:

> It's hard to imagine today, but Open Text Corporation started out in 1991 as a small three-person consulting operation, a spin-off of the University of Waterloo.

With the Internet in its infancy OpenText was responsible for creating one of the first search engines for Netscape and Yahoo. So how did they get into records management - evolution or revolution?

Before OpenText made its foray into search engines, the Canadian Federal Government departments were dealing with physical file management challenges and in 1986 a group of Ottawa-based

entrepreneurs saw an opportunity to fill the gap creating iRIMS a PSSoftware product. As a result of the changing environment iRIMS expanded its product line to address electronic, physical and image-based records. In 1999 it was purchased by OpenText and its functionality integrated into the suite of products which continue to evolve today.

And where exactly are we today? As technology has evolved, so too has the functionality of these products. Records management functionality has been built into a number of products dealing with an organization's information assets. Whether the company calls it records management, information management or information governance, at the end of the day, these software tools help manage the lifecycle of the information resources, ensure that information can be found, protected and used as required and disposed of to meet legal and compliance requirements.

The Legal Perspective: Electronic Records and eDiscovery

In any organization, the Legal group has always been critical partner with Records and Information Managers as a result of incorporating legal and regulatory requirements into retention schedule development. In the past 15 to 20 years the interest from Legal departments and law firms in records and information management has increased as a result of electronic records and the role they play in litigation and eDiscovery.

For many Records Managers, a major shift in organizational records management awareness came as a result of changes to the U.S Federal Rules of Civil Procedure in 2006, which introduced "electronically stored information (ESI) a new type of discoverable information, under Rule 34. A major concern in organizations across the US came as a result of the volume of electronically stored legacy data and back up tapes that were subject to discovery, ***if*** the organization had not had an effective program in place to dispose of its information in the normal course of business.

With the advent of technology, the challenges of the discovery process were not unique to the US although for many of us, as members of ARMA International, the Sedona Conference and the changes to the Federal Rules were probably our first introductions to the connection between eDiscovery and records management. Ontario and other jurisdictions in Canada were facing the same challenges of discovery, given the proliferation of computers in the workplace.

In 2001 the Attorney General and Chief Justice of the Superior Court of Justice appointed a Discovery Task Force, chaired by Justice Colin Campbell, Superior Court of Justice, Toronto Region, to look at existing practices and propose options for reform. The report, presented in 2003, included two recommendations in its section under the "Discovery of Electronic Documents" expanding the scope of discovery:

- Amend rules 30.01 and 31.01 to include in the definition of document "data created and stored in electronic form.
- Develop best practices with respect to retention of electronic records and the scope, cost and manner of electronic documentary production.

No longer was discovery only about paper and the issues around electronic records and information management were again, brought to the forefront.

The work of **The Sedona Conference** has been pivotal in addressing issues around eDiscovery, Data Protection and Privacy and Information Governance. Sedona Working Group One (WG1), made up of representatives from the US Legal Community and members of ARMA International among others, focused on the development of electronic document retention and production guidelines, publishing *The Sedona Principles; Best Practices Recommendations and Principles Addressing Electronic Document Production*, in March 2003. The guidelines provided detailed interpretations and insights on how organizations could apply the Principles in preparing for litigation.

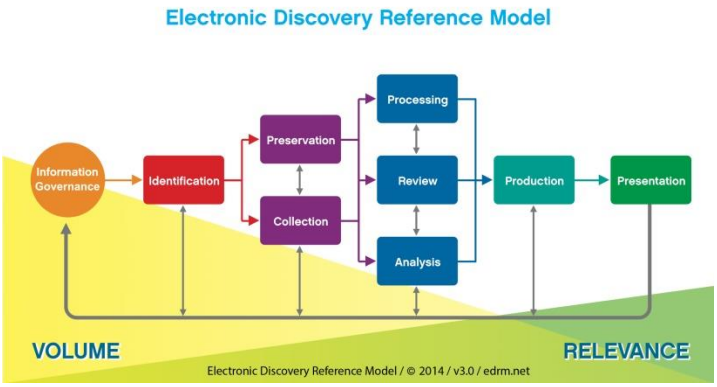
The Sedona Principles became an integral part of eDiscovery guideline development in Ontario as a result of the participation of Susan Wortzman[26], the first Canadian to attend a Sedona Conference meeting. Susan joined WG1 while a member of the Ontario Discovery Task Force. As a result of her participation on WG1, Ms. Wortzman worked with The Sedona Conference to set up Working Group 7 (WG7), Sedona Canada, which created the Sedona Canada Principles. As stated on The Sedona Conference website, WG7 was formed in 2006 with the mission:

> "To create forward-looking principles and best practice recommendations for lawyers, courts, businesses, and others who regularly confront e-discovery issues in Canada." The first edition of these *Sedona Canada Principles*[27] was released in early 2008 (in both English and French) and was immediately recognized by federal and provincial courts as an authoritative source of guidance for Canadian practitioners. It was explicitly referenced in the Ontario Rules of Civil Procedure and practice directives that went into effect in January 2010.

In November 2015, the 2nd edition of *The Sedona Canada Principles* was issued and Working Group 7, open to interested Canadian residents, continues its work on eDiscovery and information governance issues in Canada.

The Electronic Discovery Reference Model

Launched in May 2005, the EDRM[28] was established to address the lack of standards and guidelines in the e-discovery market. One of the outputs from EDRM was the Electronic Discovery Reference Model, published in 2006, designed to define the steps in an eDiscovery process in which the first step was records management. Putting records management as the first activity in the model showed the importance of ensuring that records were managed and disposed of in accordance with retention schedules and business practices. The premise was that by managing those resources effectively, there was less data/information to be waded through in case of litigation. What is interesting to note in this evolutionary process, is that while the 2014 version of the Electronic Discovery Reference Model (EDRM) shows information governance as the first box in the litigation/eDiscovery process, between 2006 and 2016, the first box changed from records management (2006) to information management (2007) to information governance (2014), showing the change in the workplace and the overall thinking about records, information and technology.



The EDRM website describes information governance as:

> "Getting your electronic house in order to mitigate risk & expenses should e-discovery become an issue, from initial creation of ESI (electronically stored information) through its final disposition."

eDiscovery has driven changes in the way organizations view their information assets as a result of the liabilities and risks associated with not managing information properly. So how does risk management fit into the picture and how do we assess our information risk?

RIM Risk Assessment Supports Business Strategies

Within any organization there are many different types of risks which are assessed to protect the organization's operations. These may be overall business risks, operational risks, financial risks and on and on. They are usually defined and quantified so that they are measurable. And behind all these risks are records and information that capture details about the business activities of and decisions made by the organization.

Many of us have applied for credit cards, loans and mortgages. We are assessed on our credit history and provided with a yes or no response, based on the risk that lending the money to us poses to the financial institution. There are measurement criteria, assessment models, and methods to weigh the results of the assessments, all of which are quantified as part of a risk management framework. In order to make a decision, people requesting the loan complete forms, staff do analyses and provide reports of their decisions and the documentation, in whatever format it is collected, create a history of the transaction. How important are those risk analysis records to the organization?

In the case of technology installations and implementation, a risk analysis looks at all the aspects of the implementation – what are the potential risk factors that may impact the project, what is the impact if one of those factors occurs and how can you minimize the impact and reduce the risks. The records created document the decisions made and provide a tracking mechanism throughout the project.

For many of us who implemented vital records programs as part of business recovery initiatives, we were involved in undertaking a risk assessment around the value of the records to the organization should some type of emergency arise, such as a natural disaster, physical damage within our facilities such as fires, burst pipes, etc. or a frustrated employee stole data or sabotaged the system. We looked at the potential occurrences and the frequency with which they might occur, analysed the scenarios and determined which of the records created and stored were either high risk, if they were lost, or required as critical to the start-up of the business post disaster.

Because of the large volumes of information created and stored in our current workplace, organizations have begun to take a risk-based approach to managing the records which are captured in *Managing Risks for Records*[29] in which the author, Dr. Victoria Lemieux, presented two approaches to records and information risk assessments:

- Event-based risk assessments such as the ones used to determine risks typically used in vital records programs,
- Records and information requirements based approach.

In the second approach, Dr. Lemieux suggests that rather than events being the basis of the risk assessment, the value of the records to the strategic business direction results in a cross-functional approach to managing information risk. Her recommendation for records and information risk management administration is to integrate it into the overall risk management function and culture, business operations, training and strategic development and budgeting, rather than have it as a separate, standalone activity within a records management program. Her book presents details about the two approaches and provides examples of the consequences of filing to manage records and information risks as highlighted below:

TABLE 1 Consequences of Failing to Manage Records and Information Risks

Sector(s)	Primary Risk	Secondary Risk(s)	Cause of Risk	Consequence of Risk
Investment Banking	Legal[a] and regulatory risk	Financial[b] and reputational risks[c]	Failure to preserve e-mail in accordance with Securities and Exchange Commission rules	$1.65 (U.S.) million fine each against five investment banks
Auditing and Management Consulting (Arthur Andersen LLP)	Legal risk	Financial and reputational risks	Inappropriate destruction of records	Found guilty of obstructing justice Subsequent corporate failure
Utilities (Transco)	Operational risk[d]	Legal and reputational risk	Lost regional records of the number of gas leaks left for repair	Engineers waste time and money as they are asked to work on pipes they cannot find Health and safety executive investigation follows
Science and Technology (NASA)	Operational risk	Environmental risk[e]	IT obsolescence leads to disappearance of valuable satellite records documenting global warming	Inability to track global warming with potential long-term environmental consequences that are, as yet, unknown

[a] *Legal risk includes loss, damage, or unrecoverability of records and information that could result in litigation or noncompliance with laws or regulations.*

[b] *Financial risk includes loss, damage, or unrecoverability of records and information that could result in financial losses or threaten the organization's financial position.*

[c] *Reputational risk includes loss, damage, or unrecoverability of records and information that could result in damage to the organization's public image, confidence, or reputation.*

[d] *Operational risk includes loss, damage, or unrecoverability of records and information needed for completing the organization's business transactions effectively.*

[e] *Environmental risk includes loss, damage, or unrecoverability of records and information documenting the organization's environmentally safe practices.*

September/October 2004 • The Information Management Journal 57

As with the other components we have discussed so far as part of the information governance Framework, managing risk is an integral part of the activities and resources, such as Dr. Lemieux' book are available to assist in the transition from the traditional view of vital records issues and risks to the business risks of the organization, something that RIM professionals need to understand and be able to discuss as part of the cross-functional team.

Rm to IM to IG: Changing Skill Sets

So how do we know what we need to know to be successful RIM and IG professionals, if the world and our environment are changing around us daily? As the records management profession started to change in the 1990's, there was an identified need to define what activities fell into the "records management" profession. A review of the Canadian Federal Government's job classification codes showed that there were no clearly defined categories for records managers because the profession itself was not clearly defined. Skills and competencies existed for professions such as lawyers, doctors and accountants. No such things existed in the records and information management community in North America at the time.

ALARM Competency Model

In 1994 ARMA Canada participated in the Human Resources Development Canada's (HRDC) Alliance of Libraries, Archives and Records Management[30] initiative to examine human resource development challenges facing the Information Resources Sector[31]. In its Competency Tool Kit[32], ALARM was described as:

> Unique in the fact that it has brought together the three occupation areas (Libraries, Archives and Records Management) and has begun to demonstrate the promise of collaboration among the three professions in identifying and responding to common human resource needs.

The groups met for about five years and created not only the detailed set of competencies but also supporting toolkits on using the competencies. The ALARM[33] competencies comprised seven professional competencies supported by three general sets of skills which defined at a high level, the core activities carried out in managing information resources. Committee members from the three professions agreed that, while managing a variety of information resources, Librarians, Archivists and Records Managers:

- Create and maintain programs and services
- Acquire and dispose of information resources
- Create a framework for access to information resources
- Provide reference, research and advisory services
- Provide electronic services
- Store and protect information resources

And required:

- Business/management skills

- Interpersonal skills
- Personal skills

The ALARM competencies were used for hiring, selecting, training and managing the performance of staff in addition to supporting RIM education program development and were, perhaps, ahead of their time from the perspective of collaboration between the individual professions.

Were we alone in developing competency models - definitely not. Were we, again, leaders in the process - yes, we were.

ARMA International Competency Models[34]

The first set of competency models developed by ARMA International in 2007 focused on Records and Information Management competencies and differed from the ALARM competencies in that they broke the competencies into four levels from entry-level practitioner to executive-level professional and six domains that reflect:

- Business Functions
- RIM Practices
- Risk Management
- Communications and Marketing
- Information Technology
- Leadership

As records management moved to information management, the Canadian General Standards Board (CGSB) issued CGSB-192.2-2009: *Competencies of the Federal Government Information Management Community*. Its format differed from both ARMA and ALARM and as of the date of this article[35], a review had been proposed but did not happen due to a lack of interest. The standard is still available on the CGSB website.

ARMA International began to expand its member offerings to include information governance and created the Information Governance Professional (IGP) certification program in 2012. In describing the role of an Information Governance Professional ARMA International states that:

> A Certified Information Governance Professional creates and oversees programs to govern the information assets of the enterprise. The IGP partners with the business to facilitate innovation and competitive advantage, while ensuring strategic and operational alignment of business, legal, compliance, and technology goals and objectives. The IGP oversees a program that supports organizational profitability, productivity, efficiency and protection.

To support the Information Professional designation, ARMA International created a set of competencies, complementary to ARMA International's RIM competencies, which state that an IGP has the ability to:

- Manage information Risk and Compliance
- Develop an IG Strategic Plan
- Develop the IG Framework

- Establish the IG program
- Establish IG Business Integration and Oversight
- Align Technology with IG Framework

In terms of defining what an IG program will look like the competencies provide an overview of program activities, through the domains and related knowledge and skills. They can also help records and information management professionals determine where there are gaps in their existing skill set and develop a personal career path, identifying opportunities for training and education.

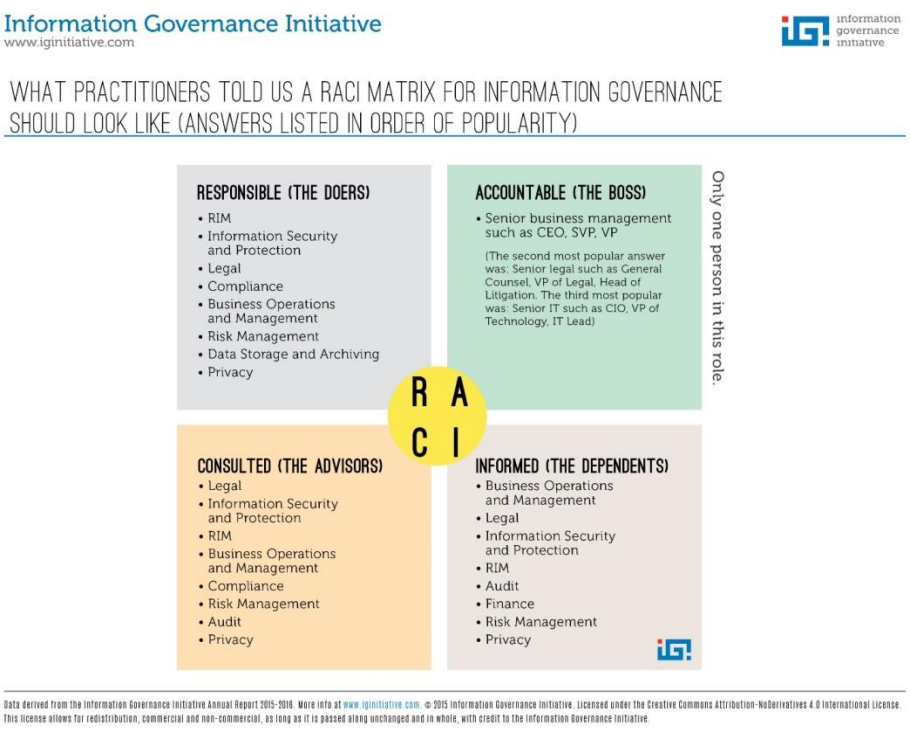
My personal belief is that information governance is a response to a changing workplace, hugely impacted by technology and requires collaboration between several groups to ensure consistency and reduce duplication of effort in managing information resources. Records and information management skills sets are being enhanced and expanded alongside other professions such as legal, privacy, risk and IT, driven by a need to address what are truly enterprise-wide issues.

Looking Ahead: Roles and Responsibilities

Looking at information governance from the 30,000 foot level, it is clear that information assets are the common element and that an information governance framework is required to ensure compliance, etc. However, unlike Records management, which has traditionally been the purview of one designated community, the information governance issues are more complex and require input from a number of different communities based on their needs and concerns. The concerns vary, depending on the specific group:

- The Privacy Officer ensures that personal information is collected, used and disposed of appropriately in accordance with privacy legislation.
- The Legal department or law firm is concerned with ensuring that the internal and external clients are aware of the retention and eDiscovery issues around all records, information and data. The costs of searching through data to support litigation have, in the past few years, resulted in an increased awareness of the benefits of effective information governance as part of ongoing business practices.
- The IT department is looking after all the systems and the data created and stored in them and has to ensure that information is secure, retrievable and accessible for as long as it is required through not only active data management but also through digital continuity and preservation to address changes in software and hardware.
- Records and Information Management provides the RIM guidelines, standards and policies and procedures which ensure that information is managed appropriately from creation to disposition.
- Employees are now far more aware of information assets and the impact of technology, although their expectations are that managing those assets will be transparent so that they get what they get what they need to do their day to day work. Anything which makes managing information onerous for the user will be rejected!

To further the discussion, the IGI created a RACI chart based on responses to their research:



Who is responsible for what will depend on the organization you are in and the focus of your strategic business goals, activity and regulatory environment. My father always used to say "if you know where you are going there is more than one road to take you there". Such is the situation with information governance. However, any successful program will depend on a champion and a cross-functional team support by the necessary tools and technologies.

Conclusion

Some years ago, a session facilitator at the National Association of Government Archives and Records Administrators (NAGARA) Conference in Sacramento, California suggested that Archivists and Records Managers should change their story from one which was all about doom and gloom and full of jargon, to one which resonated with the creators of the records and information. Certainly the story is changing!

There is no doubt that information governance, under whatever name, will become a critical part of every organization given issues of privacy, eDiscovery, risk and compliance and value proposition of the information assets to the organization's strategic position.

Records management has changed, not gone away, because there is still a need to manage records as evidence of business decisions and transactions. For records, data, information, knowledge, whatever it is called, to be useful to the organization it needs to be managed throughout its lifecycle. Discussions about what IG is and who is responsible will continue as our work changes. Each organization will design and implement a program based on its strategic direction, resource availability and risk and compliance

requirements. The big shift is in the need to create cross-functional teams to address the issues from an enterprise perspective, not a siloed focus.

We have a rich resource of work that has been done in Canada as we have moved through the various challenges posed by technology and evolved from Records management to where we are today. We have a proud heritage of development and leadership in Archives, Records and Information Management. We can learn from it, build on it and look at the present research to see where we are heading in the future so that we are ready for the challenges ahead and embrace them. And our Canadian colleagues will continue to lead in different ways to enhance our understanding.

As I said at the beginning, this is not a comprehensive, all-inclusive study and I have omitted many people and projects, to whom and for which I apologize. There is much more to be added and I encourage you to build on it and prepare an article for the next ARMA Canada publication. The seeds have been planted for the flowers to grow. There is a huge opportunity to add to what has been started so let's create the visible future!

Appendix A: ISO Standards

Information Technology

ISO/IEC 20000-1:2011 Information technology -- Service management -- Part 1: Service management system requirements

ISO/IEC 27014:2013 Information technology — Security techniques — Governance of information security

ISO/IEC 38500:2015 Information Technology Governance of IT for the organization

Information Management

ISO 30301:2011 Information and documentation -- Management systems for records -- Requirements

ISO 15489-1:2001 Information and documentation -- Records management -- Part 1: General (under revision

ISO 16175-1:2010 Information and documentation -- Principles and functional requirements for records in electronic office environments -- Part 1: Overview and statement of principles

ISO/TR 17068:2012 Information and documentation - Trusted third party repository for digital records

ISO/TR 18128:2014 Information and documentation -- Risk assessment for records processes and systems

ISO 23081-1:2006 Information and documentation -- Records management processes -- Metadata for records -- Part 1: Principles

ISO/TR 26122:2008/Cor 1:2009 Information and documentation -- Records management processes -- Metadata for records -- Part 1: Principles

Endnotes

URLs checked as of February 15, 2016

[1] Canadian Atlas online source http://www.canadiangeographic.ca/atlas/themes.aspx?id=connecting&sub=connecting_technology_wireless&lang=En

[2] See Gil Press: Forbes - http://www.forbes.com/sites/gilpress/2013/05/09/a-very-short-history-of-big-data/2/#170e0de71af0

[3] http://www.emc.com/collateral/analyst-reports/idc-digital-universe-are-you-ready.pdf

[4] http://www.emc.com/leadership/digital-universe/2014iview/index.htm

[5] https://www.igt.hscic.gov.uk/Home.aspx?tk=424106365366405&cb=7e8b504b-fbb7-488d-aefd-a8894cfb45b1&lnv=7&clnav=YES

[6] Note that Gartner, as do many organizations, uses the term archiving for setting aside inactive records into cheaper storage. For those involved in the archival profession, the use of the term causes confusion when distinguishing between the 5% of records which capture the long-term corporate memory of a private/public sector organization.

[7] TSC was founded in 1997 by Richard G. Braman, is a nonprofit, 501(c)(3) research and educational institute dedicated to the advanced study of law and policy in the areas of antitrust law, complex litigation, and intellectual property rights

[8] Images for Information governance framework

[9] www.edrm.net

[10] William Benedon was President of the American Records Management Association and editor of Records Management Quarterly and was awarded the Emmett Leahy Award in 1968 for his outstanding contribution in the field of records management

[11] Prentice-Hall, Inc. 1969

[12] A term made popular in the 1980s and 1990s as PCs became more widely used in the workplace

[13] As in other National Archives programs where the issue of preserving data for historical reference and research was a major concern, in addition to preserving historical records on paper.

[14] "Information: To Share Or Not To Share? The Information Governance Review"

[15] http://www.tbs-sct.gc.ca/pubs_pol/dcgpubs/tb_h4/holdings-fonds04-eng.asp

[16] Dr. Vale later became the head of the Information Management Branch in the Government of Ontario

[17] http://www.im.gov.ab.ca/documents/imtopics/IMFrameworkSummary.pdf; http://www.im.gov.ab.ca/documents/imtopics/IMFrameworkReport.pdf

[18] http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm

[19] coincides with the principles contained in the *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* of the Organization for Economic Co-operation and Development (OECD), to which Canada agreed in 1984

[20] Including records containing personal information

[21] The concept was created by Dr. Cavoukian "to capture the notion of embedding privacy into technology https://www.ipc.on.ca/english/Privacy/Introduction-to-PbD/

[22] https://www.ipc.on.ca/english/Resources/Discussion-Papers/Discussion-Papers-Summary/?id=329

[23] Replaced ISO 17799

[24] Provenance Systems was founded in 1989

[25] Published in 2001 by Open Text Corporation. The name Open Text has become OpenText since the book was first written. The author has referenced the name as it was at that time.

[26] Susan Wortzman is the founder of Wortzmans based in Toronto, Ontario. http://www.wortzmans.com

[27] https://www.google.com/search?sourceid=navclient&aq=&oq=Sedona+Canada+Principles&ie=UTF-8&rlz=1T4AURU_enCA499CA500&q=sedona+canada+principles+addressing+electronic+discovery&gs_l=hp..1.0l2j0i22i30l2.0.0.0.5630047.....0.zGJBBlnet3o

[28] Since its launch, EDRM has comprised 400 organizations, including 195 service and software providers, 88 corporations, 76 law firms, 24 governmental entities, 12 educational institutions and 5 industry groups involved with e-discovery and information governance.

[29] Lemieux, Victoria, *Managing Risks for Records and Information*. Lenexa, KS; ARMA International, 2004

[30] The committee was made up of ARMA International, CCA, AAQ and ACA and Associations representing different types of libraries across Canada.

[31] The title was selected in an attempt to create a common terminology that would cross all three areas.

[32] Published in August 2002, by the Cultural Human Resources Council

[33] http://www.culturalhrc.ca/heritage/e/01-01-00.php

[34] http://www.arma.org/r1/professional-development/education/competencies

[35] 2016/2/2