TECHNOLOGY DRIVES CHANGES IN RECORDS MANAGEMENT REQUIREMENTS

TECNOLOGIA IMPULSIONA MUDANÇAS NOS REQUISITOS DE GERENCIAMENTO DE DOCUMENTOS

Diane K. Carlisle | Mestre em Biblioteconomia e Informação e em Administração de Empresas; diretora executiva de Conteúdo da *Arma International*, dirige suas ações educativas e supervisiona o programa de credenciamento profissional em governança da informação.

RESUMO

As empresas de hoje dependem da tecnologia para a criação e gerenciamento de documentos e informações. Nossos marcos de gerenciamento de documentos devem mudar para abraçar a tecnologia, bem como os formatos tradicionais de documentos. Os princípios de *recordkeeping* e o modelo de maturidade de governança da informação da *Arma International*, amplamente aceitos, guiam os profissionais na reengenharia dessa mudança, e incorporam regulares aferição e auditoria dos processos-chaves.

Palavras-chave: tecnologia; cumprimento de normas; governança da informação; princípios de recordkeeping.

ABSTRACT

Today's businesses depend on technology for creating and managing records and information. Our records management frameworks must shift to embrace technology along with traditional record formats. Arma International's Generally Accepted Recordkeeping Principles and Information Governance Maturity Model guide professionals in engineering this shift, and incorporate regular benchmarking and auditing of key processes.

Keywords: technology; compliance; information governance; recordkeeping principles.

RESUMEN

Hoy en día, las empresas dependen de la tecnología para la creación y gestión de documentos e información. Nuestros marcos de gestión de documentos deben cambiar para abrazar la tecnología, junto con los formatos tradicionales de documentos. Los principios de *recordkeeping* y el modelo de madurez de gobernación de la información de *Arma International*, ampliamente aceptos, guían los profesionales en la reingeniería de ese cambio, y incorporan regulares evaluación y auditoria de los procesos clave.

Palabras clave: tecnología; cumplimiento de normas; gobernación de la información; principios de recordkeeping.

Today's business environment is dominated by digital technology. We use it to create, access, and retrieve records and information. We also use technology for communicating in a variety of formats. For example, we can use instant messaging to ask brief questions or e-mail for more complex communications. Sometimes, we even pick up the phone to have a conversation. But, if we have to leave a voice message, it might subsequently be transmitted to the person by e-mail as an audio file attachment. Digital information is here to stay – along with the advantages and disadvantages discussed in this article.

THE IMPACT OF TECHNOLOGY

Nearly all business records and documents are now "born digital", created with software applications (e.g., Word, WordPerfect, Excel, Access) or through automated reporting built into database systems. Although users may print and photocopy these records, there is no requirement to do this, so they may exist only in digital form for their entire lives. This impacts the business community in both positive and negative ways, as described below.

INFORMATION LIFECYCLE MANAGEMENT IS DIFFICULT

The exploding volume of born digital information has ramifications for information lifecycle management. Of chief concern is the difficulty of categorizing this massive quantity of information so it can be used effectively and maintained in compliance with laws and regulatory requirements. There is a need to innovate methods to facilitate categorization. Retaining and keeping digital information accessible over a long period of time is also challenging because hardware and software change frequently or become obsolete, and most media degrade rapidly and at varying rates. To ensure information's long-term accessibility and retention, the business may need to convert it to new formats and migrate it to new media.

Disposing of digital information at the end of its lifecycle is also complicated because pushing the "delete" key simply removes the index pointer to the information, not the information itself. Unless the organization destroys the media or uses technology to write over this information, it can be recovered, putting private and confidential information at risk of unintended exposure.

BUSINESS RELIES MORE ON DIGITAL INFORMATION

Various means of electronic signatures are now accepted in normal business practice and in legal and regulatory proceedings. And, increasingly – at least in many legal jurisdictions in the United States – court papers may be filed electronically.

Even in the area of health care, there is a trend toward more reliance on electronic health records (EHR). According to a report from The Office of the National Coordinator for Health Information Technology (Charles et al., 2014), more than nine in ten (93%) hospitals possessed a certified EHR technology in 2013, an increase of 29% since 2011.

BUSINESS TERRITORIES HAVE EXPANDED

One advantage of electronic record technology is that it allows companies to deliver products and some services to a global marketplace. No longer limited by time and distance, a supplier can serve a customer anywhere in the world.

Thomas Friedman, author of *The World Is Flat*, said in an undated interview with Amazon.com senior editor Tom Nissley that it was the convergence of the creation of several digital technologies with political events that "created a global platform that allowed more people to plug and play, collaborate and compete, share knowledge and share work, than anything we have ever seen in the history of the world".

IT MOBILIZES THE WORKFORCE AND CUSTOMERS

Another impact of technology is that it has made both employees and customers increasingly mobile. Mobile devices make it possible for employees to be productive from remote locations and more convenient for customers to make business transactions when they are away from their homes or office.

According to Cisco (2014), mobile use will grow significantly over the next four years. When the report was released, the number of mobile-connected devices was expected to exceed the world's projected population of 7.6 billion in 2014, reaching 11.5 billion – or 1.5 devices per capita – by 2019.

MORE DEVICES ARE NETWORKED

The projected number of mobile devices referred to above includes machine-to-machine (M2M) technologies that automatically transfer data between or among themselves via wired or wireless networks. Current examples of M2M technologies, which are part of what is referred to as "the Internet of Things," include heart sensors that send patient data to hospital monitors or inventory control devices that send automatic messages when inventory items need to be replenished.

This mobile device growth means that corporate information is distributed across multiple platforms and devices, greatly complicating an organization's ability to control and govern it.

LEGAL AND REGULATORY REQUIREMENTS FOR INFORMATION

Governing information is also affected by the complex web of regulatory and legal requirements organizations must meet. Although there have long been legal and regulatory requirements for information, complying with them is increasingly complicated by the fast-increasing volume of digital information and the global reach of business.

For example, multi-national organizations are faced with stark contrasts in regulatory requirements in the various geographic areas in which they do business. Consider, for example, privacy regulations that exist but vary greatly in all jurisdictions. Several U. S. examples are provided below.

The federal regulatory privacy framework in the United States consists of several individual privacy acts, each of which focuses on specific types of information and unique situations:

- The Health Insurance Portability and Accountability Act, more often referred to as HIPAA, regulates the use and disclosure of personally identifiable health information.
- The Fair Credit Reporting Act, or FCRA, is focused on the collection, dissemination, and use of consumer credit, financial, and lifestyle information.
- The Fair and Accurate Credit Transactions Act, or FACTA, helps protect consumers against identity theft through its limitations on companies sharing their data and its requirement for companies to disclose if they use an applicant's credit report information in their employee hiring decisions.
- The Gramm-Leach-Bliley Act, or GLBA, requires companies to notify customers regarding the use of their personal information, and it gives customers an "opt-out" option, unless disclosing this information is required by law.

In addition to being required to protect information from disclosure, many government agencies at all levels in the United States (federal, state and local) are required to provide information regarding their proceedings to those who request it. This means that many organizations must not only *protect* information from unauthorized access, they also must *ensure ready access* to information when it is legitimately requested by outside parties.

TRADITIONAL RIM FRAMEWORKS

Traditional records and information management (RIM) frameworks are insufficient in this context of the rapidly changing business environment and legal and regulatory compliance requirements. The sheer volumes of information many organizations have to manage and govern are crippling the systems and tools the professional RIM community has traditionally used. A quick overview of these shortcomings will make the point. In a traditional RIM framework:

- The focus is on controlling only *records*, which the *Glossary of Records and Information Management Terms* (Arma International, 2012) defines as "any recorded information, regardless of medium or characteristics, made or received and retained by an organization in pursuance of legal obligations or in the transaction of business"; other information is ignored.
- RIM requirements are not an integral part of business processes, workflows, and systems integration efforts.
- RIM is viewed as a "back office" operation and not valuable for contributing to the organization's success.
- Records controls tend to be focused on the format of the information, rather than on how the information is used.

- Compliance requirements are often limited to records retention/disposition and government and industry regulations.

HOW INFORMATION GOVERNANCE CAN HELP

Information governance (IG) fills the gaps left by traditional RIM programs. In its *Glossary*, Arma International (2012) defines IG as: "A strategic framework composed of standards, processes, roles, and metrics that hold organizations and individuals accountable to create, organize, secure, maintain, use, and dispose of information in ways that align with and contribute to the organization's goals". This definition emphasizes several distinctive elements that are important to the governance of information as described below.

IG SUPPORTS BUSINESS IN REACHING GOALS

First, the definition stresses that IG is a *strategic* approach that begins with governing information to help an organization meet its goals.

One goal of all organizations is to be in compliance with laws, regulations, and other binding authorities. IG includes identifying these requirements and establishing policies, procedures, and audit protocols to help ensure that information is used, protected, retained, and disposed of in accordance with them.

Another goal, of course, is to be successful. IG helps ensure that information is accurate, available, and accessible so it can be leveraged in ways that will contribute to the organization's success. The primary focus of IG, then, is on business strategy and success.

IG HELPS BALANCE NEEDS AND RISKS

Second, the definition shows that the intent of IG is to be enterprise-wide in scope and perspective. Many internal entities have a vested interest in how an organization's information assets are handled. For IG to be effective across the enterprise, the organization must take a considered and intentional approach to identifying its: business needs; regulatory compliance requirements; duty to protect privacy; procedures for processing information efficiently.

These needs are sometimes at odds with one another. IG is about balancing the needs, identifying the repercussions if some needs and requirements can't be met and mitigating the risk resulting from less-than-optimal solutions.

IG PRINCIPLES

In 2009, Arma International developed the Generally Accepted Recordkeeping Principles (Principles) and detailed narratives that identify the common, essential elements of IG. In short, the Principles are:

- Accountability – which delivers a senior leader and defined roles and responsibilities to hold individuals accountable for information governance results;

- Transparency – which 1) traceable and verifiable information in support of the organization's activities and 2) complete, consistent policies and processes;
- Integrity – which requires suitable guarantee of the authenticity and reliability of the organization's information;
- Protection – which requires specific levels of protection and security for the organization's information, including personal information;
- Compliance – which requires accurate references to laws and other binding authorities and guidance on how to comply with them;
- Availability – which requires the correct information to the right person at the right time, in the right format, and with the proper protection;
- Retention – which requires compliance and defensible disposition;
- Disposition – which requires secure methods for disposal of all formats of information that is properly eligible.

Additional context for the Principles and the program controls that assist in implementing them can be found at <www.arma.org/principles>.

IG PROGRAM METRICS

To ensure that the IG framework is solid and all of its associated policies and procedures are being followed, the organization must also establish metrics by which program and employee compliance will be measured and evaluated. To this end, Arma International has developed the additional tools that are described below.

INFORMATION GOVERNANCE MATURITY MODEL

The Information Governance Maturity Model (Maturity Model) establishes a five-level scale against which to evaluate an organization's compliance with the Principles. The five levels on the Maturity Model are:

- Level 1 – Substandard: this level describes an environment where recordkeeping concerns are either not addressed at all, or are addressed in a very *ad hoc* manner.
- Level 2 – In Development: this level describes an environment where there is recognition that the organization may benefit from a more defined information governance program. However, the organization is still vulnerable to legal or regulatory scrutiny since practices are ill-defined and still largely *ad hoc* in nature.
- Level 3 – Essential: this level describes the essential or minimum requirements that must be addressed in order to meet the organization's legal and regulatory requirements.

- Level 4 – Proactive: this level describes an organization that is initiating information governance program improvements throughout its business operations. Information governance issues and considerations are integrated into business decisions on a routine basis.
- Level 5 – Transformational: this level describes an organization that has integrated information governance into its overall corporate infrastructure and business processes to such an extent that compliance with the program requirements is routine.

WHAT'S NEW IN THIS FRAMEWORK

In addition to painting a strategic and enterprise-wide focus for IG, this new framework calls for several shifts in perspective from traditional RIM structures, which are described below.

IG RECOGNIZES INFORMATION'S VALUE

This foundation for IG brings information assets into the realm of corporate assets that have value and are managed to the organization's benefit. No longer are records and information the left-over debris of organizational decision-making and transactions. No longer can records and information be hoarded by business units until their work is done and then dumped on the RIM manager to handle the retention and disposition. The IG framework calls for the value of the records and information to be maximized to the benefit of the organization while the information is *active*, when it is still being used in conducting business.

IG EMBRACES TECHNOLOGY

With this understanding of information's value underlying our RIM actions and decisions, it is clear that IG must embrace technology as the key business driver – even as it continues to manage physical information formats like paper and microfilm. This means that when an organization considers implementing new technology systems for business productivity, it must address RIM needs at the onset.

IG DEMANDS COLLABORATION

The IG framework also calls for a more holistic approach to identifying business needs from various areas of the organization. The needs of all business units, including IG stakeholders from privacy, information technology, information security, legal, risk, and compliance, must be identified and considered at the project's initiation.

Because each of these areas has a different perspective on the organization and its use of information, the approach to determining information technology system requirements must be collaborative. Only by collaborating will the IG stakeholders be able to see a complete picture of the organization's information needs and the ramifications of various de-

cisions about how it is handled. Only by collaborating will they be able to ensure that all stakeholders' information needs have been identified and the information risks mitigated to the maximum extent possible.

IG DEPENDS ON METRICS

IG puts an emphasis on using metrics to: establish expectations and priorities for employee performance; evaluate performance against established targets; document progress toward stated goals; identify opportunities for improvement; benchmark against peer organizations; show progress in IG program maturity over time.

For metrics to be meaningful, there must be a standard against which the IG program is to be evaluated. And, the metrics must drive the desired behavior; otherwise, it is just a counting exercise. Arma International used the Principles as the foundation of its Information Governance Maturity Model, which established an objective standard by which IG programs can be measured.

Arma also created a 65-question, cloud-based assessment tool called Next Level, which delves even more deeply into an organization's IG program practices. It is also based on the Principles and the Maturity Model, but it speeds up the assessment process, aggregates results, and makes recommendations for further action.

Using any of these metric tools provides an objective foundation for assessing an IG program, helps establish targets for performance, and enables an organization to demonstrate compliance with the internal IG program elements.

IG REQUIRES AUDITING

The final distinctive element to be discussed in this IG framework is the requirement that programs be audited for program compliance. It is this attention to auditing, in combination with the attention to metrics and benchmarks that enables the enforcement of IG policies and processes.

Using the Next Level assessment strengthens an organization's ability to audit its IG program by defining audit measures that are appropriate for each of its 65 questions. These measures specify the kinds of tools and documentation that will provide evidence that the IG program is an integral part of an organization's operations.

SUMMARY

When IG is integral to an organization's operations, it can stand on the foundation it has built with internal standards, processes, roles, and metrics. Through its documentation of adherence to defined IG policies and processes, an organization can legitimately state that its IG program has credibility and that its: records can be trusted to be true and accurate accounts of the events they support; disposition of records is defensible because it is conducted according to defined controls designed to ensure that records are retained as legally required and are not destroyed prematurely.

In short, with an effective IG program in place, an organization can demonstrate integrity in how it handles its information, making a positive contribution to its reputation – and its bottom line.

Bibliographical references

ARMA INTERNATIONAL. *Generally Accepted Recordkeeping Principles*. Available at: <www.arma.org/principles>. Accessed 29 Apr. 2015.

_____. *Glossary of Records and Information Management Terms*. 4. ed. (ARMA TR 22-2012). Overland Park, KS: Arma International, 2012.

CHARLES, Dustin; GABRIEL, Meghan; FURUKAWA, Michael F. Adoption of Electronic Health Record Systems among U. S. Non-federal Acute Care Hospitals: 2008-2013. *ONC Data Brief*, Washington, D. C., Office of the National Coordinator for Health Information Technology, n. 16, 2014. Available at: <http://www.healthit.gov/sites/default/files/oncdatabrief16.pdf>. Accessed: 29 Apr. 2015.

CISCO. *Cisco Visual Networking Index*: Global Mobile Data Traffic Forecast Update 2014-2019 White Paper. 2014. Available at: <http://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/white_paper_c11-520862.html>. Accessed: 29 Apr. 2015.

NISSLEY, Tom. *Where Were You When You Realized the World Is Flat? (Or Have You?)*: a conversation with Thomas L. Friedman. Undated. Available at: <www.amazon.com/gp/feature.html?ie=UTF8&docId=562744>. Accessed: 29 Apr. 2015.

Recebido em 30/4/2015
Aprovado em 24/7/2015