Published in KATUU, Shadrack (ed.). Diverse Applications and Transferability of Maturity Models. IG Global, pp. 61-91. ISBN 9781522570806., which should be cited to refer to this work.
DOI: 10.4018/978-1-5225-7080-6.ch003

An Information Governance Policy is required for my Institution, What to do?

Practical Method and Tool enabling Efficient Management for Corporate Information Assets

Prof. Basma Makhlouf Shabou, PhD
University of Applied Sciences and Arts Western Switzerland (HES SO), Geneva School of Business Administration (HEG), Switzerland

ABSTRACT

Effective business management within organizations depends, among other factors, on the availability and proper management of appropriate resources. Information resources are one of those resources. This chapter offers practical answers to the many questions that information professionals in an institution may have about how to ensure performant, secure and rational management of corporate informational assets. After a brief presentation and discussion of main concepts, it defines and describes the information governance policy, which is the key tool of an advanced information governance approach. It specifies how and when a maturity model should help to develop and update a corporate Information governance policy. In addition, it presents the main practical guidelines including specific recommendations on the structure, content and format of an information governance policy. A discussion of the development and implementation process is then proposed.

Keywords: Information, Data, Information Governance, Information Governance Policy, Corporate Governance, Information Assets, Maturity Model, Information Risks, Information Value, Information Governance Principle, Corporate Information Assets.

INTRODUCTION

Corporations continuously produce massive amounts of information in a variety of formats. Their content has different values and different levels of significance for corporate functions and can therefore present many challenges. These may have several different natures. For example, legal issues may be a priority if there is a specific willingness to tackle e-discovery issues in a specific sector such as finance and banking. Technical and technological aspects could be the focus of other institutions facing the needs in the health and medical sectors for long-term and secure preservation. The lack of a big capacity for information-assets storage seems a ridiculous need that small companies still consider an important issue. Deciding what information is worth conserving is another serious question for all companies. Many other examples illustrate the need for high-performance management of corporate information assets, for which an investment in the information governance approach and appropriate tools becomes worthwhile. After introducing the nature and relevance of information governance, this chapter proposes to identify and describe the different components of information governance policy

(IGP). It also specifies the relationship between information governance policy and use of maturity models. In addition, it recommends an implementation method that includes the whole life cycle of an information governance policy and its steps, as well as various contributors and their roles.

BACKGROUND: INFORMATION GOVERNANCE—WHAT IS IT AND WHY IS IT NEEDED?

IG Nature

One working definition of information governance (IG) sees it as a

> *senior-level administrative structure that establishes roles and responsibilities, decision-making processes, policies and procedures that promote effective decisions that align with business outcomes. (…) In some organizations, information governance seeks to integrate and coordinate a range of relative activities, such as data management, knowledge management, and records management. Sometimes referred to as information technology and communications governance (InterPARES, 2018a).*

Considering this definition, an IG domain will fall within large perimeter that is likely situated at strategic and decisional corporate levels. It offers a strong connection between corporate governance and the strategic management of information resources in a given institution.

IG Relevancy

Many reasons exist for organizations to develop such an IG approach. They divide into three categories: short term, mid-term, and long term.

Among the **short-term** reasons that would lead an organization to adopt an information governance policy are that such a policy:

- Formalizes the rules and organizational conventions defining the informational behaviours required for the good conduct of business carried out by the organization's units;
- Recalls the rights and obligations with which the various organizational actors must comply;
- Provides support to conduct high-performance organizational activities and processes while optimizing the use of human, logistical, and financial resources necessary to access and exploit the information on which these same organizational activities and processes are based;
- Aligns information-management policies with the requirements of the organization’s governance policy.

From a **mid-term** perspective, an IG approach helps to:

- Guard against legal and technological risks related to information, as well as various other threats resulting from human error;
- Bring together the various information management (IM) sectors of an organization, such as information technology (IT) and records management (RM), around the same objectives;
- Identify the organization's information assets;

- Control the quality of information and the mechanisms protecting it; and
- Harmonise the definition of terms and standardise the practice of information resource management

Finally, among the **long-term** reasons that would lead an organization to adopt an information governance policy are to:

- Increase the visibility of information professionals (e.g., archivists, competitive intelligence specialists, record managers, content managers, knowledge managers);
- Enable these professionals to participate more easily in decision-making; and
- Enhance the organization's information assets through appropriate means and methods.

Maturity Models as a Support for Corporate Information Governance

Generally, the maturity of a given practice in different domains takes its significance from the perspective of what ideally should be followed, as a behaviour and as a system that includes processes and resources. The highest level of corporate information-management maturity that corresponds to information-governance maturity is already examined through an explicit process of ranking 'the reliability and sustainability of an entity's behaviours, practices, and processes, relative to some function or outcome' (InterPARES, 2018c). Many definitions mention that maturity models use levels to provide an assessment basis for ranking that indicates the position of the institution and its distance from the best position (i.e., the highest maturity level). Some models use capability instead of maturity (Crowston & Qin, 2011). In fact, it is difficult to confirm that those two concepts are fundamentally different.

In their very comprehensive report, Proença, Vieira, Borbinha, Calado, and Martins (2017) list 27 maturity models that they divide into several categories: Information Governance; Process Management; IT Governance; Risk Management; and Software-Engineering Governance. Twelve models are dedicated to information governance (see Table 1), divided into several categories: those dedicated to Information Governance in general, and those that focus on one aspect such as Digital Preservation, Data Management, or Records Management.

Table 1. An overview of existing information-governance maturity models

Maturity Model	**Attributes**		**Maturity Levels**
	Name	**Number**	
Information Governance - General			
Asset Management Maturity Model (Lei, Ligtvoet, Volker, Herder, 2011)	Dimensions / Category	4	Initial; Repeatable; Defined; Managed; Optimizing
Digital Asset Management (DAM) Maturity Model (Real Story Group, DAM Foundation, 2017)	Categories / Dimensions	4/15	Ad-Hoc; Incipient; Formative; Operational; Optimal
ECM Maturity Model (Katuu, 2018, Pelz-Sharpe et al., 2010)	Categories / Dimensions	3/13	Unmanaged; Incipient; Formative; Operational; Pro-Active
Gartner Enterprise Information Management Maturity Model (Newman & Logan, 2008)	-	-	Unaware; Aware; Reactive; Proactive; Managed; Effective

Information Governance - Digital Preservation			
Brown Digital Preservation Maturity Model (Dollar & Ashley 2014)	Process Perspective	10	No Awareness; Awareness; Roadmap; Basic Process; Managed Process; Optimized Process
Digital Preservation Capability Maturity Model (DPCMM) (Brown, 2013)	Domains / Components	3/15	Nominal; Minimal; Intermediate; Advanced; Optimal
Preservica Digital Preservation Maturity Model (Preservica, 2014)	-	-	Safe Storage; Storage Management; Storage Validation; Information Organization; Information Processes; Information Preservation
Information Governance - Data Management			
Capability Maturity Model for Research Data Management (CMM for RDM) (Crowston & Qin, 2011)	Key Process Areas	5	Initial; Managed; Defined; Quantitatively Managed; Optimizing
Data Management Maturity (DMM) Model (CMMI Institute, 2018)	Categories / Process Areas	6/25	Performed; Managed; Defined; Measured; Optimized
Stanford Data Governance Maturity Model (Stanford University, 2013)	Dimensions/ components	3	5 criteria unnamed
Information Governance - Records Management			
Information Governance Maturity Model (ARMA International, 2017)	Principles	8	Sub-standard; In Development; Essential; Proactive; Transformational
JISC Records Management Maturity Model (JISC infoNet, 2013)	Sections	9	Absent; Aware; Defined; Embedded

Based on and adapted from Proença et al. (2017)

A maturity model consists of several categories or domains. The terms vary according to the models, and the level of maturity at which they are evaluated is represented by a number that varies by model between 4 and 7, with a strong majority evaluated at 5 or 6. Each category has its own criteria.

Pointing out the major strengths and weaknesses in information-management practices should better guide organizations on improvements necessary to achieve higher strategic and operational performance. The maturity models provide very useful support for information governance. Developing an information governance policy utilises the maturity models to help establish its objectives, and then at the time of the assessment, to determine which have been achieved and which remain to be achieved (Proença et al., 2017).

Relationship between Maturity Models and Corporate IG Policy

The relationship between maturity models and IG policy is very iterative and dynamic. Broadly speaking, two situations illustrate these aspects. The first is the organization that has no IG policy. This case requires an analysis of organizational information practice. The use of an information governance maturity model remains a very defensible approach to conducting this analysis, which offers a transversal, exhaustive, and multidimensional vision of organizational information practices. Thus, priorities are easily defined and represented as axes of IG policy (Katuu, 2016).

In the second situation, the organization already has its IG policy and requires the use of a maturity model to better qualify the performance of practices and help the organization to see its strengths and weaknesses; target adjustments and identify updates to consider. It helps organization to structure the assessment of existing corporate information practice by offering a facilitating methodology and tool to ensure appropriate management of corporate information assets.

Information Assets and Information Governance

The following sections discuss information assets by their nature, typology and characteristics, and related concepts.

Information Assets: Definition and Characteristics

Information is contextualized data collected or created, and processes to support and manage various corporate tasks, activities, and functions. Information considered a valuable resource qualifies as a corporate asset. Consequently, information assets are intangible assets having no physical form, identified singly or collectively, and when arranged systematically or logically, could give an organization a competitive advantage and the necessary leeway to innovate (Adesemowo, von Solms, & Botha, 2016, p. 10). However, information assets are not broadly and conventionally defined (Adesemowo et al., 2016). For instance, Information Assets Development, Inc. (2018) specifies that:

> *An Information Asset is organized information that is valuable and easily accessible to those who need it. Information Assets comprise a wide range of corporate product, service and process information. In raw form Information may be nonarchived product data, uncaptured customer information, a partially documented engineering process or unshared corporate intellectual property. In typical day-to-day business activity, products are designed, services are sold, customers are supported and the necessary Information moves in a more or less efficient fashion to facilitate these actions (para 1–2).*

The National Archives of the UK states:

> *An information asset is a body of information, defined and managed as a single unit so it can be understood, shared, protected and exploited efficiently. Information assets have recognisable and manageable value, risk, content and lifecycles (National Archives, 2017, p. 1).*

Many institutions in the UK, but also throughout the Commonwealth, adopt these definitions, among them the National Institute for Health and Care Excellence (NICE) (2015, p. 4); the Council of Islington (2015, p. 4); the Oxfordshire County Council (2015, p. 18); the Victorian Government (2017, p. 8); the Tasmanian Archives and Heritage Office (TAHO) (2015, p. 2); and the University of Tasmania Records Management Unit (2018, p. 1). Surprisingl*y*, as shown in Table 2, the majority of financial, IT, and managerial standards, regulations, and guidelines do not propose an explicit definition for information and information assets.

Table 2. Comparative study of information assets across financial standards and regulations

Standard/framework/regulation	Information asset	Comment
ISO/IEC 27000:2012(E)	Implied	Last defined in ISO27000:2009
ISO/IEC 27000:2014(E)	Not defined	Sections 3.1, 3.2.1, 3.2.5, 3.2.3/3.5.5 (identified information assets!), 3.2.4 (organization's information assets), 3.4/2.68 (associated risks), 3.6 (protect information assets), 0.1 (security of information assets)
COSO (integrated framework)	Implied	SEC financial reporting, hence IASB
IASB/IFRS	Implied	Intangibles (IAS38, IFRS3)
GRAP 31	Implied	Intangibles (IP, software)
ISO5500x	In context	Intangibles explicitly out of scope
ISO19770	Define	Records, software related assets (media, documents, data)
SOX (US Sarbanes-Oxley 2002)	Implied	Software (SEC, IFRS/IASB)
King III/ISO38500	Implied	King III Principle 5.6, paragraph 36
ISO2000x/ITIL2011	In context	CI relating to service, security and other documentations
COBIT5	Implied	Information and/or IT assets
POPI	In context	Personal information, public records, special personal information

Source: Adesemowo et al., 2016, p.7

The lack of explicit and consensual comprehension of corporate information assets creates the difficulty of identifying and distinguishing what should be protected and controlled as a valuable resource. Consequently, definition is not a single aspect to specify; various characteristics and types of information assets need to be known and commonly understood. Considering the character of a corporate asset, information assets are:

- Identifiable and valuable data, information, or knowledge for corporate activities, processes, and functions;
- Mostly intangible assets, but could be related to tangible assets (e.g., software and hardware);
- Maintained, updated, and processed by various corporate units;
- Increasing the value and benefit of the institution;
- Possibly able to be monetized (e.g., patents, rare manuscripts).

Corporate Information Assets as a Focus of IG

As Smallwood argues:

> *The focus on IG comes not only from compliance, legal, and records management functionaries but also from executives who understand they are accountable for the governance of information and that theft or erosion of information assets has real costs and consequences (2014, p. 6).*

However, it would be a mistake to limit the relationship between information assets and information governance to risk management. Information valuation is an element not to be neglected. ‘Information governance has been proposed by many authors as a necessary prerequisite for the establishment of an information valorisation process’ (Guetat & Dakhli, 2015, p. 1089).

Information valuation is integrated into and recognized as an important dimension of an IG approach, based on the information’s business value, its cost, and the potential risks that could be related to different phases and actions applied during the whole information assets life cycle. Although executives in several companies claim that information is a corporate asset, few really manage it as such.

Accounting standards, particularly the International Financial Reporting Standards (IFRS) and the U.S. Generally Accepted Accounting Principles (GAAP), severely restrict the recognition of internally generated intangible assets. Consequently, under financial accounting rules, information cannot be recognized as an asset and cannot be presented on an annual corporate balance sheet, except in very specific and limited cases such as patents or development costs that meet specific criteria (e.g., IFRS Conceptual Framework; IAS 38 Intangible Assets). As a result, information is left unaccounted for as an asset, even though it is a major source of value creation within companies. But this is not the uniquely challenging aspect of being active in valuation methods and techniques. The information culture for employees, users, and executive managers is not aligned with considering information as a valuable resource because of its predominantly intangible nature. Rigorous and systematic processes for capturing and managing corporate information, added to conventional, well disseminated, and controlled principles, rules, and roles, could undeniably help to establish an effective and rational way to ensure information asset valuation, the main concrete objective of an information governance policy.

INFORMATION GOVERNANCE POLICY

IG Policy Nature

As mentioned, IG is an extended domain whose application will depend on a policy that enables appropriate practice. Worth recalling here is the difference between a directive, a procedure, and a policy (Gagnon-Arguin & Mas, 2011). The directive usually comes from the hierarchy, proposed as a documented instruction for an organizational activity or type of record. The administrative procedure is a succession of tasks that make it possible to comply with organizational formalities, and its objective is to define a specific approach. The directive could propose procedures—for example, the directive on the ‘Obligation to inform and preserve documents relating to persons’ issued by the *Service des ressources informationnelles et archives* (UNIRIS) of the University of Lausanne (University of Lausanne—Direction, 2007). As Scott (2013) defines it:

> *The policy document is exactly that—a simple statement of the business position on the chosen topic (the “why”), not to be confused with the procedural documentation which deals with “how” the policy is to be enacted. Procedures are sometimes necessarily much longer documents if they are describing complex processes which must be followed.*

Thus, a policy is a more inclusive strategic document. It provides the general framework within which these directives and procedures are proposed.

In her recent study (2013–2016) following this thought, the author reviewed the definition, scope, and main topics mentioned and discussed in a set of 13 IG policies. The following section presents a brief description and the study results.

IG Policy Components

The process of this recent study began with the review and description of a sample of existing IG policies (Appendix 1: Table of the 13 IG Policies). This entailed applying a descriptive qualitative methodology, given the exploratory nature of the object studied (Fortin & Gagnon, 2016). Thus, the design process for this model was carried out between mid-2014 and the end of 2016 in the following five stages:

Step 1: Review of a set of published and web-based IG policies. The identified sample, composed of 13 IG policies from different countries (Appendix 1), was constituted according to a sampling by convenience according to accessibility (Fortin & Gagnon, 2016);

Step 2: Analysis of the 13 IG policies sample based on the validated IG policy analysis grid. The description and analysis of the 13 IG policies identified trends and recommendations for IG policy design;

Step 3: Identification of criteria and indicators for the structure and content of an IG policy;

Step 4: Proposal of an IG policy model with recommendations regarding the content, format, dissemination, and validation of an IG policy.

After the completion of Steps 1 and 2, the author turned her attention to the identification of the general criteria that make it possible to define the broad lines of development of an IG policy. Step 3, and more specifically the literature review and the 13 IG policies, identified four criteria: content, presentation format, dissemination and promotion, and validation.

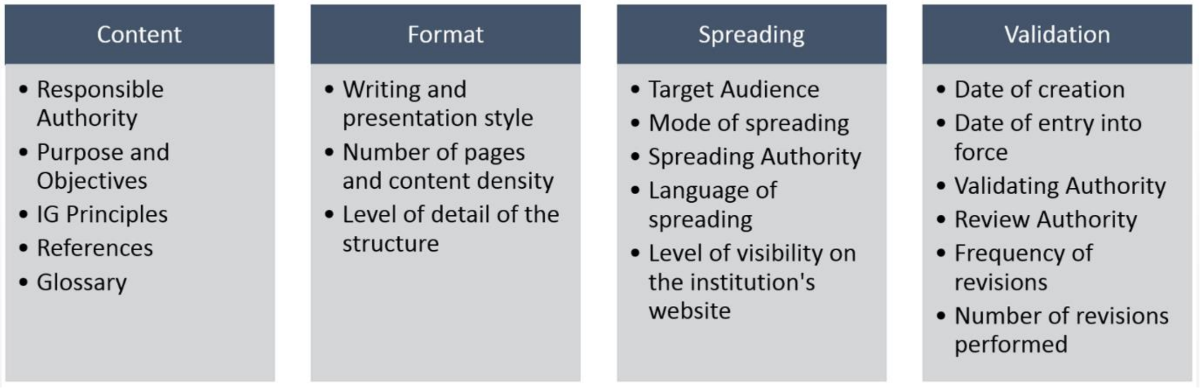
With respect to IG policy content, the policy makes it possible to identify the themes addressed, as well as their level of development and completeness. First, the purpose and objectives of IG policy must be made explicit in a precise and concise manner (Scott, 2013). For example, the clear indication of objectives has been recommended both by ISO 27000 and by authors who have taken an interest in the content of information policies (Sutter, 2006; Orna, 2008; International Organization for Standardization, 2016b). In addition to the goals and objectives, we note the value of citing legal and normative references (e.g., laws, regulations, standards) based on the analysis of IG policy. This provides strong support for the guidelines proposed in the policy. The author also examined the overall consistency of the IG policy (i.e., a link to the organization's mission and policies where these were publicly available, consideration of general IG principles); and also the adequacy of guidance on data access, corporate information security (Braman, 2011; Garde, 2014; Larrivee, 2017), and information risk management. This exploration led to identifying five indicators: responsible authority; purpose and objectives; IG principles (e.g., access and information security, informational risks); legal and normative references; and glossary.

The format of the IG policy presentation consists of first looking at the form of the policy. From there, we were interested in the layout of the text, its visual structure, and the form of its presentation. To understand format, three indicators were identified: style of writing and presentation; number of pages and density of content; level of detail of the structure.

Dissemination and promotion of IG policy addresses dissemination of the policy, as promoting the Information Management program is an important element for the organization. Indeed, its objective is to be sufficiently present in the minds of employees so that they integrate it into their daily practices (MacLennan, 2014; Smallwood, 2014). In that regard, five indicators were identified: target audience; dissemination mode; dissemination authority; language of dissemination; level of visibility on the institution's website. However, with respect to the visibility of the IG policy, the author only had access to the institution's external website and was unable to validate the policy's promotion internally.

Validation of the IG policy includes the elements that enable a policy to be validated. Chebbi (2012) states, ‘a policy must be dated, approved by the organization's senior management and regularly updated’ (p. 209). On this basis, six indicators were identified: date of creation; date of entry into force; valid authority; revising authority; periodicity of revisions; number of revisions made (to validate the announced periodicity of revisions). At the end of Step 3, the indicators for each of the four criteria mentioned above are proposed (Figure 1).

Figure 1: Information Governance: Criteria and related indicators



Content

- Responsible Authority
- Purpose and Objectives
- IG Principles
- References
- Glossary

Format

- Writing and presentation style
- Number of pages and content density
- Level of detail of the structure

Spreading

- Target Audience
- Mode of spreading
- Spreading Authority
- Language of spreading
- Level of visibility on the institution's website

Validation

- Date of creation
- Date of entry into force
- Validating Authority
- Review Authority
- Frequency of revisions
- Number of revisions performed

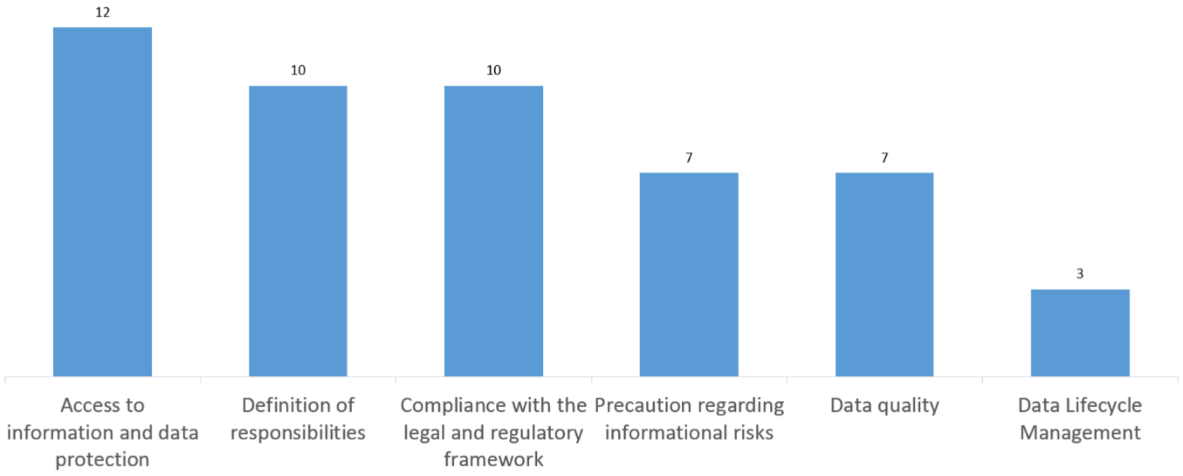
Content of the IG Policy

A policy is a more comprehensive strategic document that provides the general framework for proposing these guidelines and procedures. Therefore, the creator of the IG policy document must carefully choose the content to address, and in the same sense maintain a balance between a text that is neither too general nor too detailed. To assess the content criteria, five indicators are used to better characterize it, as shown in Figure 2. (References and Glossary appear below in the context of the actualization of the principles.)

The responsible authority identifies responsibility for developing the IG Policy, generally a body that could be a branch, a committee or a working group. The purpose and objectives of the policy are, on the one hand, to verify that the goals and objectives appear clearly in the document; and on the other hand, to analyse their purpose. Setting goals and objectives is a key step in discerning the purpose and scope of a policy.

Consideration of IG principles supports assessing the coverage of the central axes, namely access to information and data protection; information risk precautions; document life cycle management from creation to disposition; data quality; definition of responsibilities for different aspects of data management and use; and compliance with the legal and regulatory framework. Figure 2 summarizes the coverage of the principles outlined in the content of the 13 IG policies analysed. The principles most clearly mentioned are access to information and data protection, followed by the mention of data-management responsibilities, as well as the reminder of and respect for the legal, regulatory, and normative framework.

Figure 2: Coverage of IG principles in the IG policies analysed (N=13 policies)



Regarding the content, the IG policy should explicitly mention at least the following principles and considerations:

- Responsibility for the management and use of information—assigning responsibilities to stakeholders according to the information, its typology, and specificity. This involves developing procedures and conducting audits to ensure the proper application of IG (Mêgnigbêto, 2010; Scott, 2013);
- Information quality—definition of its characteristics and qualities based on Record Management best practices and standards (International Organization for Standardization, 2016);
- Security—definition of levels of information protection (private, sensitive, confidential, and essential). A synergy of legal, archival, and IT tools will ensure that this element is respected (Canton of Geneva, 2000, 2001; Swiss Confederation, 2014);
- Compliance with the institution's laws, regulations standards, policies, and directives;
- Availability—ensuring timely, systematic, and adequate access to information for authorized persons (i.e., levels of access such as public, restricted, confidential); ensuring access to information throughout the life cycle through appropriate and controlled information media;

- Life cycle definition—assessment (disposal or retention) of information according to legal, fiscal, operational, and historical requirements, using a retention schedule that plays a central role;
- Transparency—documentation and accessibility of organizational processes and activities to staff and stakeholders. Communication campaigns, as well as their tools, will be of great help in responding to this principle (Canton of Geneva, 2001; Swiss Confederation, 2014);
- Risk management—identification and assessment of informational risks, choice of means and mechanisms for their management, as well as the roles and responsibilities of each person in the organization (International Organization for Standardization, 2009, 2014; Smallwood, 2014; Desroches, 2013; Léger, 2015a, 2015b; Lemieux, 2004; Lemieux & Krumwied, 2011).
- References—drafting an IG policy must comply with the normative framework and its various elements, including laws, regulations, standards, and guidelines. The author identified the types of sources on which the drafters of the policy relied and checked whether these citations were properly referenced (for example, in the form of a bibliography). This is important because at first glance it provides additional validity to the content, as well as initial information about the professionalism with which the document was developed.
- Glossary—the author highlighted whether the document should include a glossary. This tool makes it possible to explain the important terms that facilitate understanding, but also and especially to fix a common vocabulary for all the actors participating in IG.

Format of the IG Policy Presentation

The format criterion focuses on the visual presentation and layout of policy content. It is important to take this into account when analysing this type of document, because it is intended for all stakeholders in IG, including information-management professionals, management, employees in various sectors, and even suppliers and clients. However, to implement a policy requires validating it, as well as communicating, reading, and integrating it into daily tasks. The visual aspect must therefore attract the reader, leading him or her to browse and understand the document. The study's IG policy observation yielded the following three indicators for the format criterion:

- Style—the overall visual aspects used to present the document. For example, the author examined the level of use of enumerations, page ventilation, the use of colours, and the layout of the title page. An engaging visual will have a better chance of reaching the target audience. Thus, for example, the use of smart lists, tables, or graphic diagrams to summarize or illustrate content could facilitate the understanding of IG policy. This component also includes an examination of the drafting style of the text (e.g., administrative, technical).
- Number of pages—the author noted the number of pages in a policy to assess the level of brevity of the information. A very long document can cause complexity of content and an unnecessary level of detail, especially since a policy is a general document that outlines and orients institutional information practices.
- Level of detail—the author first tried to estimate how deep the content treatment was in each section. For example, by examining into how many levels the sections had been broken down—and to bring these conclusions to the overall policy level. These data provide a complementary view of the previous indicator on the number of pages. The author decided to include this

indicator in the format criterion rather than in the content criterion, because too detailed or too general a text will influence the reader's intention to read the document.

Dissemination and Promotion of IG Policy

The dissemination and promotion criterion provides information on the accessibility and visibility of the policy in relation to the intended audience. Communication is always an important step in getting the text out to target readers. Indeed, a document must be visible to inform the public that it exists, and to demonstrate the importance of its content. It must also be accessible so that the target audience can consult it. To study this criterion, the following five indicators were applied:

- Target audience—this is a list of reader groups to which the policy is addressed. This indicator is crucial because content, form, and delivery will be tailored to meet the needs and expectations of the target audience.
- Method of dissemination—the tools used to communicate the document to the target audience. The quantity and modes of dissemination reflect the importance placed on promoting the policy.
- Dissemination authority—the author tried to identify the institution and, if possible, the unit or even the function responsible for disseminating the policy. This data makes it possible to evaluate the power attributed to disseminating the document. The disseminator is not necessarily the responsible authority for the IG policy. Some institutions have a centralized communication culture in which all documents or messages for internal or external publication must go through the communication service/unit/directorate for dissemination to target audiences.
- Language of distribution—the availability of the document in the official languages of the institution. The translation of the policy demonstrates an effort to disseminate it to a wide audience.
- Level of visibility on the institution's website—the author found how easy or difficult it was to access the policy from the home page of the institution's website. To do this, the number of clicks to reach the document was counted. Studies show that these should be between 3 and 7 (Laloux, 2013; Boucher 2011; Robert, 2015). A reduced number of clicks must be sufficient to access the IG policy. The "principle of 7 plus or minus 2," also called Miller's rule, explains this, because it "is based on cognitive psychology and stipulates that the human brain is capable of simultaneously processing a maximum of 7 elements on average. Applied to the Web, this translates into the idea that a navigation menu for example should have a maximum of 7 entries" (Laloux, 2013).

Validation of the IG Policy

This criterion indicates the evolution of the validation and updating of the policy since its creation, as well as the responsibilities associated with it. Validation is an extremely important aspect because it emanates from the institutional executive sphere. Updating is also essential, as a policy must reflect and respond to changing needs. The following six indicators compose the main axes of IG policy validation:

- Creation date—this is the date on which the document was created (that is, the date of an invalidated version). Measuring the difference between the creation and validation dates of the document may partly reflect the willingness of the validating authority to have implemented the policy.
- Effective Date—this is the date on which the document was validated by a responsible authority, and therefore the date from which the policy must be formally implemented.
- Validating authority—either the unit or the function responsible for validating the policy. That individual's position in the institution indicates the importance attached to this document.
- Revising authority—either the unit or the function responsible for revising or updating the policy.
- Frequency of revisions—this identifies the frequency with which the document is revised. The accuracy of this information reflects the guideline adopted by the validating authority.
- Number of revisions—the number of times the policy has been validated since its inception. This indicator makes it possible to check whether the indicated periodicity has been respected.

IG POLICY LIFE CYCLE: FROM CREATION TO IMPLEMENTATION

This section will present the steps involved in the life cycle of creating and implementing an information governance policy within an institution. It will first outline the requisites to be met, then map out the steps in creating the policy, and finally look at the process and practical recommendations that should facilitate its implementation.

Prerequisites for IG Policy Conception

Two prerequisites seem fundamental for the implementation of an IG policy. First, is a need to ensure full management support for the project leading establishment of this strategic tool. Senior managers must support the process and be active, in the event of complications (Sutter, 2006). This demonstrates to the target audience the great importance attached to policy and its follow-up. Second, a cross-disciplinary and multidisciplinary Information Governance (IG) team should be created, ideally comprising representatives of the legal sector, the IT section, the information-security field, management units (human, financial, and logistical resources), and an IG expert who could be a business document manager (Sutter, 2006; Hagmann, 2013). In the latter case, if the institution does not have one, it must hire an expert. If a business-records manager were chosen, broadening his or her view of IG would be imperative. The content of a policy resulting from such a committee, the fruit of a common vision, would therefore be more relevant (Garde, 2014; Larrivee, 2017). This would also facilitate the adoption of the tool by both managers and employees of the organization.

IG Policy Life Cycle

The following sections present a set of capital steps to consider in the process of establishing a corporate IG policy. It will focus mainly on five steps. This proposition is to be applied after adaptation and consideration of domain particularities, data and information characteristics, and undeniably the information-management maturity and information user's culture.

Conception

The first step in developing an IG policy is to identify its goals. This requires an examination of the institution's information-management practices and culture (Orna, 2008; Smallwood, 2014; Sutter 2006). As such, it is important to examine the maturity of information resource management and analyse the level of advancement of document practices in the organization. At this stage, the target audience must also be determined (Sutter, 2006). This makes it possible to adapt the message and discourse that will form the backbone of the IG policy. On this basis, an approach to IG must be formulated and priorities for good practice and local, national, and international standards must be determined (Scott, 2013; Sutter, 2006; Hagmann, 2013). This approach, designed and validated by the IG team, needs to be documented and presented to stakeholders to gather their views. The general idea is to establish a common vision of IG that is strong and consistent with the institution's policies. This framework will serve as a reference throughout the creation, validation, dissemination, and implementation phases of the policy.

The purpose of the second step is to identify policies, some aspects of which could affect the management of information already existing in the organization, and examples of IG policies from similar organizations. In the first case, it is important to review common internal records with IG-related content, such as email-management policies, cloud-security policies, or business-records management policies. This allows the alignment of IG policy with its context for application. The use of templates developed by professional information-management associations is recommended. The second case involves identifying and analysing IG policy from similar institutions working in the same sector of activity or processing the same type of data (e.g., medical data, banking data, scientific data). This will provide a more precise indication of the type of information that an agency of the same type has entered in its copy.

With respect to the previous step, new data should be collected to complement and adapt the content of the policy to the organization. This third step begins with clarifying and describing the target audiences to whom the document is addressed, and their roles. This significantly determines the form and content. The IG vision developed in the first phase should provide guidance for identifying the target audience, the external and internal users of institutional information. Among the latter, it is essential to identify employees whose role in IG influences assigning responsibilities to them. In addition, an organizational information policy must also take into account several types of resources (Orna, 2008): human resources (e.g., contact person, document manager, lawyer, computer scientist, external consultants), information management systems, financial (budget), materials and supplies for storing and processing data, real estate (e.g., current and final archive premises), logistics (e.g., assistance in organizing training courses, defining processes) and IT (e.g., servers, software). There is a need to identify existing means and tools, and to assess their relevance for integration into corporate governance in general, and IG in particular (Iron Mountain, 2014). In the same vein, it is important to look at the norms, standards, and legal frameworks relating to the domain in one way or another. The policy must fit within the legal and normative context of the institution. Finally, in agreement with management, the procedures for validating and updating the document must be established.

The fourth step is the drafting of the policy. The creation of the IG policy must be the result of a deliberative process—that is, the content must consider the opinions and views of the IG team members. In this way, the policy will be consistent with the overall goals of the institution and respond to the expectations of the various IG actors.

Test and Validation

The IG policy validation phase could depend on at least two components: user validation and hierarchical validation. In the first component, organizationally IG policy needs to be empirically tested. This step could be carried out in close collaboration with a user group that agrees to evaluate full and draft versions of the policy. The interdisciplinary group and its various members must listen to the users as they comment on the strengths and areas for improvement of this tested IG policy. Changes can then be made. Once user validation has been obtained, the second component consists of having a final version approved by the direct hierarchy, the body responsible for the mandate to implement the IG policy, and then by management. This validation marks the entry into force of the document (Hagmann 2013).

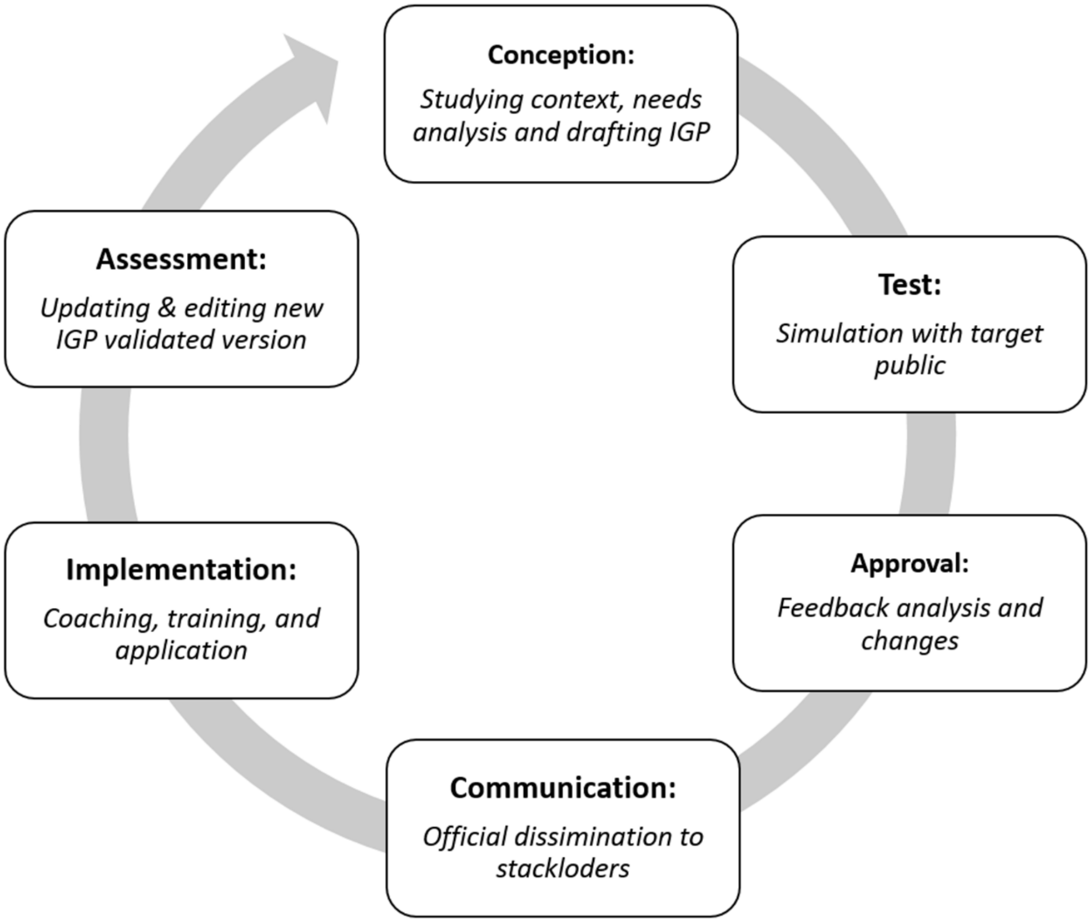
Communication

At the end of the IG policy validation, a communication and training campaign must be implemented (Scott, 2013; Sutter, 2006). The idea is to disseminate the content of the document, but also to explain this new approach to contributing to the achievement of the institution's goals, and therefore the objectives of the stakeholders, and to highlight the practical aspect of this tool and its relevance in their daily lives. This step is crucial in managing change. The goal is to create an information management culture that employees embrace and integrate into their day-to-day tasks. In practice, a communication plan must be developed. This involves segmenting the different audiences to which the document is addressed, to adapt the content of the message. The basic text will be the same for all, but some aspects should be emphasised, or the vocabulary changed in relation to the various sectors. The discourse will significantly differ when communicating with the IT department or the legal unit. Finally, the more distribution channels available to reach the target audience, the more effective and sustainable the delivery of the message (Smallwood, 2014). Usable tools include internal newsletters, intranets, the Internet, social networks, internal blogs, emails, promotional posters, meetings, and training courses. These can be designed in a variety of ways, delivered either in the classroom or online, and must be offered consistently and daily to maintain a high level of effectiveness.

Implementation

Communication and training alone are not sufficient to ensure policy implementation (Figure 3). Actors must take effective action. Therefore, based on the roles and responsibilities chapter included in the IG policy, an action plan must be developed. The purpose of this report is to present concretely the objectives for each of the IG stakeholders. As a result, tasks and an action plan must be foreseen, to give concrete expression to the content of the policy. These tasks must be assigned according to individuals' areas of expertise, integrated into their daily activities, and above all approved by the hierarchy. The implementation of the IG policy also includes awareness-raising, training, and support activities if necessary (Iron Mountain, 2014; Scott, 2013).

Figure 3: Information Governance Policy Life cycle


Conception:
Studying context, needs analysis and drafting IGP
Test:
Simulation with target public
Approval:
Feedback analysis and changes
Communication:
Official dissimination to stackloders
Implementation:
Coaching, training, and application
Assessment:
Updating & editing new IGP validated version

Assessment and Updating

Finally, the implementation of the policy must be subject to quality controls. This includes determining the level of monitoring of IG principles, assessing the impact of actions in this area on the achievement of the institution's goals, and measuring staff satisfaction. Clear and precise metrics must be defined for this purpose (Proença, Vieira, & Borbinha, 2014). For example, staff satisfaction could correspond to the evaluation of user feedback, and the level of knowledge and application of the IG policy, data for which could be collected through interviews or by observing the occurrence of informational risks after the implementation of the policy. Regardless of metrics, auditing the IG policy and its implementation and application remains an essential step in assessing the quality of the project and making improvements. As Orna (2008) points out, an information policy is a dynamic tool. In addition, since an institution and its context are in constant evolution, the content of the policy must be updated periodically (Figure 1). Iron Mountain (2014) stresses the importance of implementing a self-assessment program (p. 14). To this end, internal collaborators and users of organizational information will be consulted and involved, and their contribution will be crucial (Scott, 2013; Sutter, 2006).

CONCLUSION

This chapter discusses the concept of information governance and explains how information governance policy should look. It presents some relevant examples of information governance maturity models and highlights their support in developing and updating corporate IG policies. It articulates the different sections of an information governance policy, which should indicate responsibility for the management and use of information; information quality principles and considerations; security aspects; legal and regulatory compliance; information access and availability, including life cycle assessment (disposal or retention); transparency; and risk management. References and a glossary must be specified to make sure that vocabulary is accessible for all IG-policy stakeholders.

In addition, this chapter recommends the main steps in creating and maintaining the IG policy including its design, testing and validation, dissemination, implementation, evaluation, and updating. These are very practical recommendations to help organizations develop and update such tools.

Investing in IG policy development and implementation increases not only the corporate ability to better manage information risks and their impact, but also the value and quality of corporate information. One of the objectives that justifies the development of an IG policy is precisely the desire to increase the benefit of information assets. Recent research initiatives are being developed in this field to deepen knowledge of different types of informational values and to propose appropriate approaches and methods for measuring them.

ACKNOWLEDGMENT

This research was supported by the InterPARES Project https://interparestrust.org/ and the Department of Information Sciences of the Geneva School of Business Administration (HEG). It was advanced thanks to helpful contributions of GREGI researchers and precious collaboration by Aurèle Nicolet and Gregory Nobs, research assistants at the Information Sciences department of the Geneva School of Business Administration (HEG). My sincere thanks to Yvonne Grandbois for her appreciated help and support.

REFERENCES

Adesemowo, A., von Solms, R., & Botha, R. (2016). Safeguarding information as an asset: Do we need a redefinition in the knowledge economy and beyond? *South African Journal of Information Management*, *18*(1). Retrieved from https://doi.org/10.4102/sajim.v18i1.706

Archives d'État de Genève. (2013). Bonne gouvernance des documents électroniques dans l'administration. Genève, Suisse: République et canton de Genève. Retrieved from http://ge.ch/archives/media/site_archives/files/imce/pdf/procedures/20130827_gouvernance_doc_electr_adm_1_v.pdf

ARMA International. (2017). Generally accepted recordkeeping principles—Information governance maturity model. Retrieved from http://www.arma.org/page/IGMaturityModel

Banque de Développement du Conseil de l'Europe. (2008). Politique d'information publique. Paris, France: Banque de Développement du Conseil de l'Europe. Retrieved from www.coebank.org/documents/25/Politique_information_publique.pdf

Boucher, A. (2011). *Ergonomie web: pour des sites web efficacies*. Paris, France: Eyrolles.

Braman, S. (2011). Defining information policy. *Journal of Information Policy*, *1*, pp. 1–5.

Brown, A. (2013). *Practical digital preservation—A how-to guide for organizations of any size.* London: Facet Publishing.

Cancer Institute of New South Wales. (2015). *Data governance policy, Version 2.0*, 19 October 2015. New South Wales, Australia: Cancer Institute. Retrieved from https://www.cancerinstitute.org.au/getmedia/b6a63978-f588-493c-af45-ee4716a4066b/CINSW-data-governance-policy.PDF

Canton of Geneva. (2000). *Loi sur les archives publiques (LArch) du 1er décembre 2000 (Entrée en vigueur: 1er septembre 2001)*. Retrieved from https://www.ge.ch/legislation/rsg/f/s/rsg_b2_15.html

Canton of Geneva. (2001). *Loi sur l'information du public, l'accès aux documents et la protection des données personnelles (LIPAD) du 5 octobre 2001 (Entrée en vigueur: 1er mars 2002)*. Retrieved from https://www.ge.ch/legislation/rsg/f/s/rsg_a2_08.html

Chebbi, A. (2012). *Archivage du Web organisationnel dans une perspective archivistique*. (Unpublished Doctoral dissertation, University of Montreal, Montreal, Canada). Retrieved from http://hdl.handle.net/1866/9203

CMMI Institute. (2018). *Data Management Maturity (DMM)*. Retrieved from http://cmmiinstitute.com/data-management-maturity

Council of Islington (2015). *Islington information asset owners: A council-wide information management policy*. Retrieved from https://www.islington.gov.uk/~/media/sharepoint-lists/public-records/informationmanagement/businessplanning/policies/20162017/20160418informationassetowners.pdf.

Crowston, K., & Qin, J. (2011). *A capability maturity model for scientific data management: Evidence from the literature*. Proceedings of the Association for Information Science and Technology, *48*(1), 1–9. Retrieved from https://crowston.syr.edu/content/capability-maturity-model-scientific-data-management-0

DAM Foundation (2017). *The DAM Maturity Model Version 2. DAM Maturity Model.* 14 February 2017. Retrieved from http://dammaturitymodel.org/

Desroches, C. (2013). *La gestion des risques informationnels dans l'entreprise privée: perspective des gestionnaires de la sécurité* (Unpublished Master's thesis, University of Montreal, Montreal, Canada). Retrieved from https://papyrus.bib.umontreal.ca/xmlui/handle/1866/11469

Dollar, C., & Ashley, L. (2014). *Digital Preservation Capability Maturity Model© (DPCMM): Background and performance metrics. Version 2.6.* Retrieved from http://www.securelyrooted.com/s/2014-May_DPCMM-Background-and-Performance-Metrics.pdf

Fortin, M.-F., & Gagnon, J. (2016). *Fondements et étapes du processus de recherche: Méthodes quantitatives et qualitatives*. Montréal, Québec: Chenelière Éducation

Gagnon-Arguin, L., & Mas, S. (2011). *Typologie des dossiers des organisations: analyse intégrée dans un contexte analogique et numérique.* Québec: Presses de l'Université du Québec.

Garde, J. (2014). *Information governance with MoReq.* In J. Borbinha, Z. Szatucsek, & S. Ross (dir.). Proceedings of the DLM Forum—7th Triennial Conference (p. 99). Lisbon, Portugal: National Library of Portugal. Retrieved from http://purl.pt/26107/1/DLM2014_PDF/dlm2014-Proceedings_V1.pdf

Gouvernement du Québec (2012). *Politique-cadre sur la gouvernance et la gestion des ressources informationnelles des organismes publics*. Retrieved from http://www.tresor.gouv.qc.ca/fileadmin/PDF/ressources_informationnelles/Politique___lois/politique_cadre.pdf

Guetat, S. B. A., & Dakhli, S. B. D. (2015). The architecture facet of information governance: The case of urbanized information systems. *Procedia Computer Science*, *64*, 1088–1098. Retrieved from https://doi.org/10.1016/j.procs.2015.08.564.

Hagmann, J. (2013). Information governance—Beyond the buzz. *Records Management Journal*, *23*(3), 228–240.

Information Assets Development, Inc. (2018). *What is an information asset?* Retrieved from http://www.informationassetdevelopment.com/what.html

International Organization for Standardization. (2009). *Risk management—Principles and guidelines (ISO 31000)*. Geneva, Switzerland: International Organization for Standardization.

International Organization for Standardization. (2014). *Information and documentation—Risk assessment for records processes and systems (ISO/TR 18128)*. Geneva, Switzerland: International Organization for Standardization.

International Organization for Standardization. (2016a). *Information and documentation—Records management—Part 1: Concepts and principles (ISO 15489-1)*. Geneva, Switzerland: International Organization for Standardization.

International Organization for Standardization. (2016b). *Information technology—Security techniques—Information security management systems—Overview and vocabulary (ISO/IEC 27000)*. Geneva, Switzerland: International Organization for Standardization.

InterPARES. (2018a). *ITrust Terminology: Information governance (English)*. Retrieved from http://arstweb.clayton.edu/interlex/en/term.php?term=information%20governance

InterPARES. (2018b). *ITrust Terminology: Information management (English)*. Retrieved from http://arstweb.clayton.edu/interlex/en/term.php?term=information%20management

InterPARES. (2018c). *ITrust Terminology: Maturity model (English)*. Retrieved from http://arstweb.clayton.edu/interlex/en/term.php?term=maturity%20model

Investissement Québec. (2015). *Politique de gouvernance et de gestion des ressources informationnelles (G1397)*. Retrieved from http://www.investquebec.com/documents/fr/acces_a_information/PolitiqueGouvernance.pdf

Iron Mountain. (2014). *A practical guide to information governance* [White paper]. Retrieved from http://www.ironmountain.com/resources/whitepapers/a/a-practical-guide-to-information-governance

JISC infoNet. (2013). *Records Management Maturity Model*. JISC Website. 12 November 2009–30 July 2013. Retrieved from https://www.jisc.ac.uk/guides/records-management/maturity-model

Katuu, S. (2016). Assessing the functionality of the enterprise content management maturity model. *Records Management Journal*, *26*(2), 218–238. Retrieved from https://www.emeraldinsight.com/doi/full/10.1108/RMJ-08-2015-0030

Katuu, S. (2018). A comparative assessment of enterprise content management maturity models. In N. Gwangwava & M. Mutingi (Eds.), *E-manufacturing and e-service strategies in contemporary organizations* (pp. 93–118). Hershey, PA: IGI Global.

Laloux G. (2013). *Règles d'or en ergonomie Web: toujours le bon choix ?* Retrieved from https://www.webmarketing-com.com/2013/08/01/22609-regles-dor-en-ergonomie-web-toujours-le-bon-choix

Larrivee, B. (2017). Time for organizations to get serious about governance. *Credit Control*, *38*(1), 49–51.

Léger, M-A. (2015a). *Pour une définition du risque informationnel* [Blog post]. Retrieved from http://www.leger.ca/2015/10/02/pour-une-definition-du-risque-informationnel/

Léger, M-A. (2015b). *Typologie des risques informationnels* [Blog post]. Retrieved from http://www.leger.ca/2015/10/23/typologie-des-risques-informationnels/

Lei, T., Ligtvoet, A., Volker, L., & Herder, P. (2011). *Evaluating asset management maturity in the Netherlands: A compact benchmark of eight different asset management organizations.* In Proceedings of the 6th World Congress of Engineering Asset Management. as cited in Proença et al. (2017)

Lemieux, V. (2004). *Managing risks for records and information*. Lenexa, Kansas: ARMA International.

Lemieux, V., & Krumwied, E. (2011). Managing records risks in global financial institutions. In L. Coleman (ed.). *Managing records in global financial markets, ensuring compliance and mitigating risk* (pp. 91–105). London, United Kingdom: Facet Publishing.

MacLennan, A. (2014). *Information governance and assurance: Reducing risk, promoting policy.* London, United Kingdom: Facet Publishing.

Mêgnigbêto, E. (2010). Information policy: Content and challenges for an effective knowledge society. *International Information & Library Review, 42*(3), 144–148. Retrieved from https://doi.org/10.1080/10572317.2010.10762858

National Archives. (2017). *What is an information asset?* February 2017. Retrieved from http://www.nationalarchives.gov.uk/documents/information-management/information-assets-factsheet.pdf

National Institute for Health and Care Excellence (NICE). (2015). *Information governance management framework*. Retrieved from https://www.nice.org.uk/Media/Default/About/Who-we-are/Policies-and-procedures/Information-governance-policy-and-management-framework.pdf

Newman, D., & Logan, D. (2008). *Gartner introduces the EIM Maturity Model*. Gartner Research Publication, ID, (G00160425) Retrieved from https://www.yumpu.com/en/document/view/24634038/gartner-introduces-the-eim-maturity-model-eurim

NHS Commissioning Board. (2012). *Information governance policy*. Retrieved from https://web.archive.org/web/20130510182133/http://www.england.nhs.uk/wp-content/uploads/2012/11/info-gov-pol.pdf

Orna, E. (2008). Information policies: Yesterday, today, tomorrow. *Journal of Information Science, 34*(4), 547–565. Retrieved from http://journals.sagepub.com/doi/pdf/10.1177/0165551508092256

Oxfordshire County Council (2015). *Security incident management policy*. Retrieved from https://www.oxfordshire.gov.uk/cms/sites/default/files/folders/documents/business/providers/securityincidentmanagementpolicy.pdf

Pelz-Sharpe, A., Durga, A., Smigiel, D., Hartmen, E., Byrne, T., Gingras, J. (2010). ECM Maturity Model - Version 2.0. Wipro—Real Story Group—Hartman, 22 June 2010. Retrieved from https://ecmmaturity.files.wordpress.com/2009/02/ecm3-v2_0.pdf

Perrein, J.-P. (2013). *Définition de la gouvernance de l'information par des mots: Extrait du livre GouvInfo "Océan bleu"* [Blog post]. Retrieved from http://www.3org.com/news/gouvernance_de_linformation/definition-de-la-gouvernance-de-linformation-par-des-mots-extrait-du-livre-gouvinfo-ocean-bleu/

Preservica. (2014). *Digital preservation maturity model*. Retrieved from https://preservica.com/uploads/resources/Preservica-White-Paper-Maturity-Model-2014_NEW.pdf

Proença, D., Vieira, R. & Borbinha, J. (2014). *A maturity model for information governance,* presented at DLM Forum Foundation Triennial Conference, Lisbon, Portugal. Retrieved from http://purl.pt/26107/1/DLM2014_PDF/27%20-%20A%20Maturity%20Model%20for%20Information%20Governance.pdf

Proença, D., Vieira, R., Borbinha J., Calado, P., and Martins, B. (2017). *A maturity model for information governance*. European Archival Records and Knowledge Preservation (E - ARK). Retrieved from http://www.eark-project.com/resources/project-deliverables/95-d75-1/file.

Queensland Government Chief Information Office. (2012). *Information governance*. Retrieved from https://www.qgcio.qld.gov.au/products/qgea-documents/548-information/2620-information-governance

Queen Elizabeth Hospital King's Lynn NHS Foundation Trust. (2013). *Information governance policy*. Retrieved from http://www.qehkl.nhs.uk/IG-Documents/ig-policy.pdf

Robert, S. (2015). *Le mythe de la règle des 3 clics—Ergonomie Web*. Retrieved from http://www.usabilis.com/mythe-regle-3-clics/

Scott, A. (2013). How to create a good information security policy. *ComputerWeekly.com.* Retrieved from http://www.computerweekly.com/feature/How-to-create-a-good-information-security-policy

Sedona Conference on Information Governance. (2013). *The Sedona Conference Commentary on Information Governance.* Retrieved from https://thesedonaconference.org/download-pub/3421

Smallwood, R. F. (2014). *Information governance: concepts, strategies and best practices.* Hoboken, New Jersey: Wiley.

Stanford University. (2013). *Data Governance Maturity Model.* 22 October 2013. Retrieved from https://web.stanford.edu/dept/pres-provost/cgi-bin/dg/wordpress/wp-content/uploads/2011/11/StanfordDataGovernanceMaturityModel.pdf

Sutter, E. (2006). *Intelligence économique et management de l'information: les questions les plus fréquemment posées*. Paris, France: Éditions TEC & DOC.

Swiss Confederation. (2014). *Loi fédérale sur la protection des données (LPD) du 19 juin 1992* (État le 1er janvier 2014). Retrieved from https://www.admin.ch/opc/fr/classified-compilation/19920153/index.html

Tasmanian Archives and Heritage Office (TAHO). (2015). *Information Management Advice 38 Information Asset Owner and Digital Continuity.* Retrieved from https://www.informationstrategy.tas.gov.au/Records-Management-Principles/Document%20Library%20%20Tools/Advice%2038%20Information%20Asset%20owner%20and%20Digital%20Continuity.pdf.

UNIRIS. (2014). *Politique de records management et d'archivage pour une gouvernance informationnelle*. Lausanne, Suisse: Université de Lausanne. Retrieved from http://www.unil.ch/uniris/files/live/sites/uniris/files/documents/references/UNIL_POL_Records_management_archivage_VF.pdf

University of Hawaii. Office of the Executive Vice President for Academic Affairs/Provost. (2012). *Executive policy on institutional data governance*. Retrieved from https://www.hawaii.edu/policy/archives/ep/e2/e2215.pdf

University of Lausanne—Direction. (2007). *Directive de la Direction 0.5. Obligation de renseigner et conservation des documents relatifs aux personnes*. Retrieved from http://www.unil.ch/interne/files/live/sites/interne/files/textes_leg/0_aff_gen/dir0_5_conservation_document.pdf

University of Nevada Las Vegas. Office of the Executive Vice President and Provost. (2010). *Data governance policy*. Retrieved from http://ir.unlv.edu/IAP/Files/UNLV%20Data%20Governance%20Policiy%20July%202010.aspx

University of North Carolina. Information Technology Services. (2010). *Institutional data governance policy*. Retrieved from https://www.med.unc.edu/pharm/administration/it-corner/it-campus-security-policy/Data_Governance_Policy.pdf

University of Tasmania. Records management unit (2018). *RMU Information Sheet 18*. Retrieved from http://www.utas.edu.au/__data/assets/pdf_file/0020/1046243/RMU-Information-Sheet-18-Information-Assets.pdf

Vallès, L. (2015). *Le risque informationnel et l'urgence de le gérer de façon adéquate* [Blog post]. Retrieved from http://lyonelvalles.com/2015/12/20/le-risque-informationnel-et-lurgence-de-le-gerer-de-facon-adequate/

Victorian Government. (2017). *Information Management Glossary.* 1 May 2017. Retrieved from https://www.enterprisesolutions.vic.gov.au/wp-content/uploads/2017/08/IM-GUIDE-03-Information-Management-Glossary.pdf.

Virginia Polytechnic Institute and State University. (2017). *Administrative data management and access policy*. Retrieved from http://www.policies.vt.edu/7100.pdf

ADDITIONAL READING

Almarabeh, T., & AbuAli, A. (2010). A general framework for e-government: definition maturity challenges, opportunities, and success. *European Journal of Scientific Research*, *39*(1), pp. 29–42.

Bountouri, L. (2017). *Archives in the digital age: standards, policies and tools*. Chandos Publishing.

Fahy K., and Hermann, M. 2017. Case study #6: Enterprise information management at children's health system of Texas. Updating organizational policies and procedures for information governance. *Journal of AHIMA / American Health Information Management Association*, *88*(6), 46–47.

Grazhenskaya, A. (2017). *Information governance: Nature and implementation from the European public administrations' perspective* (Unpublished Master's thesis, Geneva School of Business Administration (HEG), Geneva, Switzerland). Retrieved from http://doc.rero.ch/record/306588?ln=en

Groupe d'études et de recherche en gouvernance informationnelle (GREGI). (2018). Site du GREGI. Retrieved http://gregi.org/

Leger, M-A. (2015). *Modèle de politique de sécurité des actifs informationnels*. Retrieved from http://www.leger.ca/2015/10/02/modele-de-politique-de-securite-des-actifs-informationnels

Makhlouf Shabou, B. (2011, October). *Measuring the quality of records to improve organizational documentary testimony*. In Professional Communication Conference (IPCC), 2011 IEEE International (pp. 1–6). IEEE.

Makhlouf Shabou, B., Grazhenskaya A., & Lomas, E. (2017). *Information Governance in European Public Administrations.* In: ALA-ICA Conference, Mexico City, 28 November 2017. Retrieved from http://www.alaarchivos.org/wp-content/uploads/2017/12/4.-Basma-Arina-Granzhenskaya.pdf

NHS Digital. (2017). *Information Governance Toolkit*. Retrieved from https://www.igt.hscic.gov.uk/

Richards, L. L. (2014). *Evidence-as-a-service: State recordkeeping in the cloud* (Doctoral dissertation) The University of North Carolina at Chapel Hill. Retrieved from https://cdr.lib.unc.edu/indexablecontent/uuid:028b34f2-5182-4bfc-a246-b1a3845788f6

Soma, K., Termeer, C., & Opdam, P. (2016). Informational governance—A systematic literature review of governance for sustainability in the Information Age. *Environmental Science & Policy, 56*, 89–99. Retrieved from https://doi.org/10.1016/j.envsci.2015.11.006

Southern Health NHS Foundation Trust (2016). *Information Risk Management Policy.* Retrieved from http://www.southernhealth.nhs.uk/_resources/assets/inline/full/0/41852.pdf

APPENDIX 1: THE SAMPLE OF 13 INFORMATION GOVERNANCE POLICIES

	Institution	IG Policy Title
1	Banque de développement du Conseil de l'Europe (Banque de Développement du Conseil de l'Europe, 2008)	Politique d'Information Publique
2	Cancer Institute of New South Wales (Cancer Institute of New South Wales, 2015)	Data Governance Policy
3	Gouvernement du Québec (Gouvernement du Québec, 2012)	Politique-cadre sur la gouvernance et la gestion des ressources informationnelles des organismes publics
4	Investissement Québec (Investissement Québec, 2015)	Politique de gouvernance et de gestion des ressources informationnelles (G1397)
5	National Health Service England (NHS Commissioning Board, 2012)	Information governance policy
6	Queensland Government (Queensland Government Chief Information Office, 2012)	Information governance
7	The Queen Elizabeth Hospital King's Lynn National Health Service Foundation Trust (The Queen Elizabeth Hospital King's Lynn NHS Foundation Trust, 2013)	Information Governance Policy
8	University of Hawaii (University of Hawaii. Office of the Executive Vice President for Academic Affairs/Provost, 2012)	Executive Policy on Institutional Data Governance
9	University of Nevada Las Vegas (University of Nevada Las Vegas. Office of the Executive Vice President and Provost, 2010)	Data Governance Policy
10	University of North Carolina (University of North Carolina. Information Technology Services, 2010)	Institutional Data Governance Policy
11	Virginia Polytechnic Institute and State University (Virginia Polytechnic Institute and State University, 2008)	Administrative Data Management and Access Policy
12	État de Genève, Archives de l'État de Genève (Archives d'État de Genève, 2013)	Bonne gouvernance des documents électroniques dans l'administration
13	Université de Lausanne, Service des ressources informationnelles et archives (UNIRIS) (UNIRIS, 2014)	Politique de records management et d'archivage pour une gouvernance informationnelle

KEY TERMS AND DEFINITIONS

Corporate Information Assets: Elements involved in the process of setting up and operating the company's information systems: computer hardware, processes, data, and information stored on paper or any other type of medium (Vallès, 2015).

Information: An element carried by objects allowing communication between individuals or between machines, such as paper documents, digital documents, data from databases, images, videos, sound tapes, informal discussions between individuals (Perrein, 2013).

Information asset: A portion of information, identified, defined and managed as a single and valuable unit, therefore it can be viewed, shared, protected and exploited optimally and efficiently as such. It has distinguishable able, manageable value, risk and life cycles (National Archives, 2017).

Information Governance: Subset of corporate governance, information governance is a strategic and multi-dimensional approach that aims to ensure the achievement of corporate objectives with high performance, rationalization and established authority, rules and principles. It brings together several competencies and disciplines such as records management, information security, data quality, knowledge management and business intelligence, information valuation & cost management and long-term digital preservation. (Sedona Conference Commentary on Information Governance, 2013; Smallwood, 2014; Dollar & Ashley 2014).

Information Governance Principles: Concepts, considerations, and rules of conduct for achieving effective information governance.

Information Governance Policy: A master document drawn up in accordance with the corporate governance policy, based on a collective consultation involving several corporate stakeholders, in which the objectives, rules, processes, and mechanisms necessary to optimize the efficient management of the entire corporate information assets are formalized.

Information Management: Operational management of day-to-day processing and use of information to achieve the corporate's goals and objectives, including RM, IT service delivery, information security, and business directives (InterPARES, 2018b).

Informational Risks: Any uses or actions carried out in the context of information management that occur in an unforeseen or unauthorized manner and have a direct or indirect impact, positive or negative, on the performance of institutional functions.

Maturity Model: The way to rank the ideal behaviours, processes, tools, practices enabling a rational and optima achievement of corporate functions and goals (InterPARES, 2018c).

Policy: A document setting out the guidelines for the various legal, regulatory, normative, and ethical requirements of an area of activity, and identifying the main actors involved in the implementation of governance.