A Corporate Information Management Framework for the European Public Sector

Declan Deasy, formerly European Commission, DG Informatics
Declanjdeasy@gmail.com

Frank Bannister, Trinity College Dublin
Frank.Bannister@tcd.ie

Vassilios Peristeras, European Commission, DG Informatics
Vassilios.PERISTERAS@ec.europa.eu

Abstract

This paper proposes a framework for Corporate Information Management (CIMF) tailored for the European Public Sector. The CIMF consists of a structured, holistic set of principles which encompass the different phases of the information lifecycle. The framework reflects the importance of information as a critical public asset, the quality of which is paramount. The principles focus on how information should be generated, managed, shared, protected and preserved. The approach emphasises the necessity to establish, implement and manage this framework at the corporate level. The framework has been influenced by references found in governmental policies from the UK, New Zealand, Australia, Estonia, USA, and Canada as well as a number of other academic and practitioner sources. For each principle both objectives (i.e. what is to be achieved) and enablers/action types (how to achieve the objectives) are presented. It is argued that adopting and promulgating this framework at a corporate level in European public administrations would be a paradigm shift in information management for the European public sector and would provide the basis for a veritable revolution in how public administrations manage information.

1. Introduction

Fast, reliable access to relevant information for better decision-making has been one of the primary drivers of successive waves of computerization in the public sector from early mainframes through networks, PCs, the Internet, the Web to today's cloud computing and digital services. This has resulted not just in a rich portfolio of information systems across governments (including policy support, administrative and office systems), but also in the emergence of digitally literate staff with high expectations of their organisations's information systems. Since the 1960s, technology has had the capacity to transform the way we create, share, process, exploit, disseminate, preserve and protect the information stored in these systems. As new technologies have emerged, these capacities have expanded to the point where many organisations struggle to cope with the sheer volume of data they create, gather, process and store.

In addition to this general challenge, information systems in public administrations around the world suffer from two particular problems which, while not unique to the public sector, are certainly more significant in that sector. These problems are siloisation and lack of interoperability. Although local collaborative initiatives exist and progress has been made on internal integration using technologies such as Enterprise Resource Planning (ERP) systems and data warehouses, both silo systems with little data sharing or reuse and data stored in local file systems persist in all public administrations. Silos and lack of interoperability are the norm especially when the situation across different departments, agencies and ministries is analysed. The situation is even worse when it comes to cross-border exchanges of information and services. These problems hinder the availability of information at the corporate level and the seamless delivery of modern digital services. For many years the challenge has been to better manage this information infrastructure/ecosystem in a holistic way at the corporate level so as to maximise its value for both the citizen and the state. It is a challenge shared by all organisations in the public sector which is reflected in the modernisation agendas of most EU Member State public administrations where there is a widespread realisation that the potential for leveraging each administration's information to create new digital public services has not yet been fully exploited.

There are numerous potential benefits to be realised from better information management in the public sector, for example in:

- evidence based policy and decision making;
- innovation and creation of new digital public services;
- knowledge management and the retention of corporate memory;
- increased trust in government's management of citizen data;
- day to day efficient operation of the public sector;
- delivery of appropriate levels of transparency both internally and externally;
- collaborative working within and across Government departments;
- co-creation between the public sector and citizens, community groups and the private sector;
- cooperation and coordination across the European Union;
- minimising the risk of non-compliance with regulations;
- managing the costs of collection, storage and securing of information.

The challenge is to develop a suitable framework for better management of the information underpinning an administration's activities so as to contribute to achieving these benefits. This paper proposes one such approach.

1.1 Terminology

The words 'data' and 'information' are often used interchangeably although they mean different things (Ackoff 1989). Furthermore, they have different meanings to people working in different disciplines (e.g. archivists, data scientists, statisticians, document management experts and so on). Data are commonly defined as elementary objective facts. Individual data items are discrete and often measurable. Data may or may not have meaning in isolation. Traditionally the data captured and stored in computer systems have been almost exclusively textual or numeric, but increasingly other forms of data are being captured and stored (e.g. video, audio, pictures and images).

Information is here defined as data placed in a context which creates meaning. This may be as simple as combining two data sets or as complicated as placing it in a political scenario. Both data and information may be stored and manipulated digitally in lightly structured documentary systems and/or highly structured data systems. The growth of both use and storage of unstructured information has been a trend during recent years.

For ease of reading, throughout this paper the word information will be used to encompass both information and data. The word 'data' will be used only where specifically required by the context.

2. The European background

Within the European Union (EU) the so-called "Information Society" has been an important driver of economic and social progress since the publication of the Bangemann Report in 1994. Since then the EU has been putting in place the legal and policy framework to support the emerging Information Society. As this supportive framework becomes more complex, the need for sound and effective information management in the Member States' public administrations increases.

While there are many detailed aspects to this legal and policy framework, the following are salient elements of it:

1. The *EU Lisbon Treaty* (Official Journal 2008) enables support from the Union for the efforts of Member States to improve their administrative capacity to implement Union law by facilitating the exchange of information amongst them.

2. The *EU Charter on Fundamental Rights* (Official Journal of the European Parliament 2000) introduces the right of every citizen to access data that has been collected concerning her or him and, if it is inaccurate or incomplete, the right to have it corrected. Where such data are inappropriately held, citizens have to right to request that they be deleted. In line with this right, highly developed data protection regulations are now in place across the EU. The core underlying legislation is Regulation (EU) 2016/679 (repealing Directive 95/46/EC) and Directive (EU) 2016/680which regulate the protection of natural persons with regard to the processing of personal data and the free movement of such data.The regulation and the directive, transposed into national laws, apply to all EU Member States as well as to Iceland, Liechtenstein and Norway.

3. The revised *Public Sector Information Directive* (European Commission 2013) encourages public sector bodies to make data/information, together with the relevant metadata, publicly available. The Directive requires that this be done in both open and machine-readable formats, at the lowest feasible level of precision and granularity and in formats that ensure interoperability. It is worth noting that there is a potential for conflict between this and the preceding directive – particularly given the growing power of modern data analytics (Barocas and Nissenbaum 2014). This creates some specific challenges for information security management which are discussed below.

4. Since 2000 there has been a series of EU Ministerial declarations on eGovernment and eGovernment Action Plans complemented by the European Commission's internal e-Commission initiative. Their common objective is the effective and cost efficient exploitation of digital technologies to transform public administrations and to deliver user-centric digital public services (European Union 2009; European Commission 2010b; European Commission 2012). The latest Eu eGovernment Action Plan 2016-2020 (adopted in April 2016) aims to accelerate the digital transformation of government. Interoperability and de-siloisation are key success factors for these plans.

5. The European Commission explicitly promotes interoperability and has facilitated European public services and the exchange of information between the EU Member States since the mid-1990s with a series of programmes namely:

   - *The electronic interchange of data between administrations* (IDA/IDAI/IDAII);
   - *Interoperable Delivery of Pan-European eGovernment Services to Public Administrations, Business and Citizens* (IDABC) and
   - *Interoperability Solutions for European Public Administrations* (ISA)

   The ISA programme (2010-2015) (European Commission 2015) has already delivered important results (Bovalis *et al* 2014) including interoperability frameworks, reference architectures, data standards (Peristeras 2013) and maturity models (European Commission 2010a; European Commission 2011; European Commission 2015c; IDBAC 2010). This work will continue with the ISA^2 Programme (2016-2020) (European Commission 2015b).

6. The recently published *Digital Single Market* policy (European Commission 2015d) defines priorities for interoperability and standards in areas critical to the digital single market, such as e-health, transport planning and energy. Moreover, a new e-government action plan will connect base registers across Europe and ensure ease of information exchange between different national systems and authentic data sources. Businesses and citizens should only have to communicate their data once to public administrations (this is sometimes referred to as the once-only strategy).

7. More generally the European Council has repeatedly emphasised in recent years the need for modernising member states' public administrations as part of the Structural Reforms essential for jobs, growth and investment. The European Commission in its Annual Growth Survey 2015 called for improved efficiency in public administrations emphasising the challenge of "*adapting to the needs of the digital economy*" and recommending "*a more digital approach to public administration*" (European Commission 2014, p14)

The implementation of these policies in the EU Member States has turned out to be more difficult than

expected, especially at European level. It implies cross department projects, increased collaboration and knowledge sharing, an emphasis on transparency and data exchanges with the EU institutions, other states, international organisations, citizens and businesses. However siloisation and lack of interoperability remain remarkably difficult to eradicate. Analysis of the difficulties in overcoming them has led to the insight (if not epiphany) that progress at both transnational and national level in these domains is predicated on better information management especially at corporate levels. This creates the need for a suitable universal framework.

3. State of the art on information management frameworks

The concept of an information management framework as envisaged in this paper appears under a number of different guises including corporate information management (CIM), enterprise information management (EIM) and even enterprise architecture. Van de Lans and van Til (2012, p80) define enterprise information management as:

"*… an integrative discipline for structuring, describing and governing information assets across organizational and technology boundaries to improve efficiency, promote transparency, support agility and enable business insight*."

The CIM/EIM concept goes back several decades. An early text on this topic is by Jackson (1986). More recently, a number of books on EIM have been published many of which are related to specific products (such as SAP), technologies (such as the Internet) or topics (such as content) (see, for example, Brague and Champlin 2014; Jenkins 2012; vom Brocke and Simons 2013). Ideas such as treating information as an asset and the need for good data and information governance have long been understood (see, for example, Moody and Walsh 1999; Brynjolfsson 1994; Glazer 1993; Kopper et al 2011; EIU 2008; Khatri and Brown 2010; Sarsfield 2009).

Various frameworks and definitions have been proposed over the years mostly emphasising the information technology aspects of information management. They contain certain common features or components such as data management and security, but in other ways they can be quite diverse in their understanding of what comprises EIM. For example, until recently little priority was given to preservation or data protection issues.

A study by Hausmann et al (2014) reviewed the current state of EIM readiness in a number of countries (though primarily in Australia). The authors reported that less than 35% of respondents said that they now have an EIM strategy in place. Another recent survey by the Gartner Group (Geragas 2015) reported similar findings. It confirmed that Enterprise Information Management (EIM) and Master Data Management (MDM) are moving up the corporate agenda although less than 5% of firms surveyed have fully deployed multi domain operational solutions. Gartner's conclusion, that successful enterprise information management requires "*a political power shift …and …a deliberate and architected approach"* in organisations, underlines the need for a framework for information management at corporate level.

Recent research commissioned by BT Ireland (Amárach 2016), in revealing the growing importance of data at board level has confirmed this trend: *"As technology transforms businesses globally, it is clear that data management, specifically how data is used and secured is going to be crucial for companies, their investors and shareholders alike"* (Walsh 2016).

This realisation that data management is key to meeting the challenges of the digital revolution has been articulated at the highest political level with the call by the President of Estonia to add a Fifth Freedom - the Free Movement of Data - to the Four Fundamental Freedoms of the single market - People, Goods, Capital and Services - enshrined in the European Treaties. Data must be able to cross borders but the free movement of data is not just about commerce - " *it must become an abiding value of the internal market* " (Address by President Ilves to the European Parliament, 2 February 2016).

The situation in the public sector regarding information management is broadly similar to that in the private sector. Many countries, dissatisfied with the return on IT investments in their public administrations and faced with increasing expectations for digital public services, have begun to address the issues surrounding information management in the public sector. Doing this implies a need for national frameworks for policy formulation and execution in the information management domain. No such frameworks exist at the moment. An analysis of the policies of six countries – the UK, the USA, New Zealand, Australia, Canada and Estonia - has revealed common themes and preoccupations which should be addressed in such a framework. All of these countries recognise information as an asset that should be managed and shared. They emphasise, in varying degrees, the need for information to be fit for purpose and meet business needs, to be trusted and authoritative and to be reusable. Information should be open, accessible, easy to discover and easy to use. Preoccupations found in each of these countries include the necessity for information to be standardised and linkable, readily available, protected, reasonably priced and accessible in an appropriate manner. All six emphasise governance, guidelines and training as critical to successfully implementing information management.

The European Commission is addressing some of these issues through the ISA Programme (European Commission 2014b) which promotes interoperability amongst the EU member states and the EU institutions. In this context, several results of the programme (Bovalis et al 2014) contribute to improved information management. These include:

- The *European Interoperability Framework* (EIF) which provides the basis for developing interoperable European public services (European Commission 2010a);

- The *European Interoperability Reference Architecture*, which is a blueprint to be used when designing interoperable systems supporting public services (European Commission 2011);

- The development of horizontal data standards (Core Vocabularies) to support cross-domain exchange of information and open data policies (Peristeras 2013);

- Work in the area of Base Registries to ensure that public administration master data is managed in a coherent way and becomes available for reuse by the whole administrative ecosystem;

- Maturity and assessment models for interoperability and standards like the Common Assessment Method for Specifications and Standards and the Interoperability Maturity Model;

- Joinup – ISA's collaborative platform where public administrations businesses and citizens can share and reuse interoperability solutions, including open source software and semantic assets (see www.joinup.ec.europa.eu).

This work is undertaken with the EU Member States and will be continued through to 2020 with the ISA^2 programme adopted in November 2015 (Decision (EU) 2015/2240) and establishing a programme on interoperability solutions and common frameworks for European public administrations, businesses and citizens as a means for modernising the public sector.

The US Government also has a programme to ensure information interoperability in the context of national security. The responsible agency, the Information Sharing Environment(ISE), has recently published tools including :

- DARA – Data Aggregation Reference Architecture designed to address shortfalls in data interoperability, aggregation and correlation (ISE 2014);

- GIRA - Geospatial Interoperability Reference Architecture leverages open standards to improve information sharing primarily of geospatial information (ISE 2015a);

- ISE Interoperability Framework – a start-up guide that makes tools and resources available to government and the private sector for improving information interoperability (ISE 2015b).

These tools primarily facilitate information sharing on security matters across US government agencies and underscore the need for an all embracing overarching framework for information management.

In summary while there is much ongoing work on information management and there are broad areas of commonality in its conceptualisation, there is no one agreed framework. Nonetheless, information management is recognised as an increasingly important challenge both in the private and public sectors. In almost all cases it has not yet been adequately addressed particularly at corporate level – in fact one could, to borrow a colloquial expression, say that it is an elephant in the corner of the corporate suite. The need for a corporate framework for information management that is independent of any underlying technology is clear and unambiguous.

4. A Corporate Information Management Framework (CIMF)

Drawing on the actions outlined above and the current state of the art of information management in the public and private sectors a Corporate Information Management Framework (CIMF) is presented. The framework identifies and is developed around a structured set of six principles based on the information life cycle. It adopts a corporate and holistic view of information management for public administrations similar to the discipline of Enterprise Information Management discussed in the context of private organisations The CIMF proposes an important change in current public sector information management practices namely moving from micro and *ad-hoc* management at the local level designed to optimise local functions and services to corporate and holistic information asset management designed to achieve global organisational objectives. This transition is not trivial and constitutes a paradigm shift in how many public organisations in the EU currently perceive, manage and exploit information.

The figure below presents a high-level view of the framework as a logical, structured set of principles which encompass the phases of the information lifecycle.

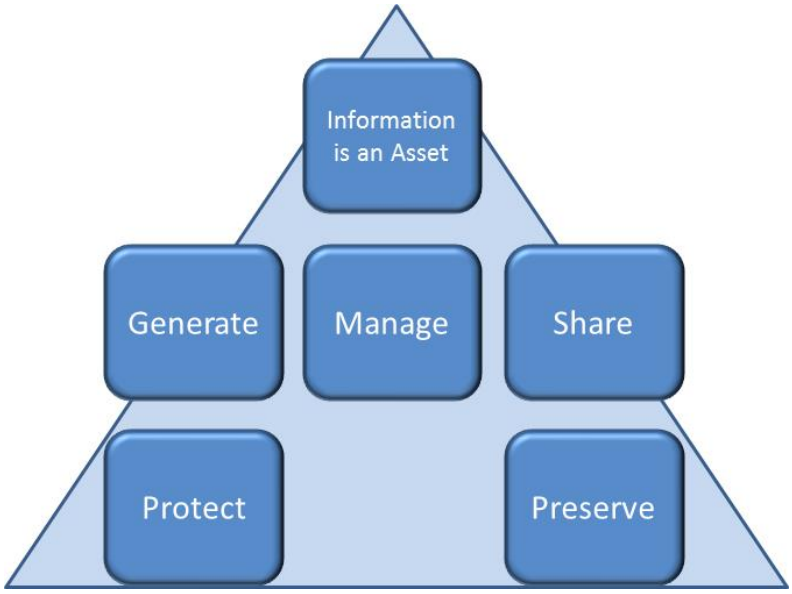

Figure 1: A Corporate Information Management Framework (CIMF)

The CIMF consists of the holistic set of principles in the following table.

Principle 1: Public Sector Information is a public asset held in trust for citizens. Public Administrations have an obligation to ensure that information retained by the public sector is accurate, integral, protected, accessible and up to date at all times.

Principle 2: Information should be generated to aid policy formulation and to support policy execution using standardised formats and exploiting both internal and external sources.

Principle 3: Information should be managed so as to optimise its quality and its relevance to good public administration and to maximise the creation of public value applying 'once-only' strategies where appropriate.

Principle 4: Information should be shared in ways that make it easy to (re)use, deliver and exchange and it should be made available through multiple channels.

Principle 5: Information should be protected as prescribed by both the EU and national legal codes as well as public administrations' data privacy and IT security policies.

Principle 6: Information should be preserved to ensure continued access for as long as is appropriate in accordance with national and international legal, regulatory and archival requirements. Information which is unlikely to serve any future public purpose should be deleted.

This framework provides a context for both theoretical and practical issues related to information to be addressed independently of any underlying systems or technologies. This ensures that the focus is on information management, information interoperability and data quality. The principles are discussed in more detail below. For each principle the rationale underlying that principle is presented, associated objectives (what) are presented and the enablers (how) to achieve the objectives are identified. These objectives and enablers allow the implementation of the CIMF to be tailored to an administration's specific needs and requirements. Some high level objectives are common to several principles but the emphasis and actions to achieve them will be different in each case.

4.1 Principle 1: Information is an Asset

Public Sector Information is a public asset held in trust for citizens. Public Administrations have an obligation to ensure that information retained by the public sector is accurate, integral, protected, accessible and up to date at all times.

A defining characteristic of public sector information is that it is held in trust for the citizens. It is a public asset the quality of which is paramount. It is worth noting that this principle has not always been accepted in all areas. Even today government agencies sometimes regard their information as proprietary. It is also worth noting that while this principle states that all public information belongs to the public, it is a collective right with associated responsibilities particularly concerning access; it does not mean that all citizens have a right to see all information.

This principle is inspired by similar overarching propositions enunciated by several countries for example:

Country	**Comment**
New Zealand (ICT.gov.nz 2015)	*"Data and Information held and owned by government effectively belong to the New Zealand public; are a core strategic asset held by government as a steward on behalf of the public; and should only be collected or generated for specific public policy, operational business or legislative purposes*."
Australia (Victorian Government 2011, p2)	"*Information assets are critical to decision making and service delivery in government"*
UK (The National Archives 2015)	"*Information is an asset which is fundamental to the efficient and effective delivery of public services* "
Estonia (Estonian Ministry of Economic Affairs 2014, p42)	"*Well functioning information governance is creative information governance where… information in any form, from any source, sent/received via any channel is covered*."

Administrations have traditionally put in place strategies establishing governance and management procedures at the corporate level for valuable assets like human resources, finance, technology and intellectual property. In an Information Society, high quality information has become one of these valuable assets. However, until recently few administrations have treated it as such – particularly at the corporate level. Instead the focus of investment has been more on project management, system

development and service delivery. Information management has remained a poor relation.

One possible explanation for this is that information management is often mistakenly identified with information technology management. However, the core of information management lies not in the technology as such, but in the way in which a public administration perceives:

- how information is ***created*** internally,
- how it ***collects*** information from its external environment,
- how all this information is ***processed, documented*** and ***organized*** and
- how it ***shares, delivers*** and ***exchanges*** information internally and with citizens and other organizations.

In addition public administrations have a particular responsibility to safeguard this information, thus ***protection*** and ***preservation*** are two aspects that acquire critical importance.

An Information Management strategy needs to maintain a delicate balance: it should remain to a certain extent technology-agnostic emphasising the business requirements and whilst providing the potential to exploit new, innovative and cutting-edge technological advances. The CIMF is explicitly designed to be independent of an administration's information systems and underlying IT infrastructure while at the same time providing a continual stimulus for their orderly evolution. Essentially the CIMF creates the context for corporate governance to dictate and oversee this evolution.

This overarching first CIMF principle has significant implications for regularly reviewing the processes that ensure the accuracy and integrity of data.

Keeping data up to date will also have implications for systems and resources. Where, say, data is captured and/or keyed in manually the currency of data can be problematic. In fact with the likelihood that the volume of data will continue to grow exponentially sustainable cost models for storage and access mechanisms will have to be developed so that relevant information will always be retrievable

Objectives

- Create a culture of awareness of information as a public asset
- Ensure that public information is of high quality
- Facilitate extraction of the maximum public value from public information
- Ensure that data is high quality
- Ensure compliance with relevant legislation
- Support the Digital Single Market and eGovernment policies
- Implement relevant European Council public sector recommendations.

Enablers

- Appropriate governance
- Awareness campaigns
- Organisation-wide Data Policy
- Guidelines including development and service delivery guidelines
- Training
- Regulatory supervision
- Data quality standards and processes
- The European Interoperability Framework (EIF) including reference architectures and common data models.

4.2 Principle 2: The Generation of Information

Information should be generated to aid policy formulation and to support policy execution using standardised formats and exploiting both internal and external sources.

This "*information generation*" principle refers to the way information is created within an administration or collected/obtained from outside. It highlights the importance of improving the internal information production, but also the need for interfaces between the organization and its external environment which channel information and data from outside. More specifically "create" here refers to the internal production of information - why and how an administration produces information satisfying user needs - while "collect" refers to acquiring information from the external environment.

Reviewing and streamlining both these processes is important for four reasons. The first is to avoid the reinvention of existing content (as this will lead to savings). The second is to sense and monitor what is happening in the external environment. The third is to align the organization with its environment and the fourth is to identify and exploit the huge amounts of available information for policy formulation and implementation.

This principle draws on concepts specifically elaborated by several countries:

Country	**Comment**
New Zealand (ICT.gov.nz 2015)	"*Data and information support the purposes for which they were collected and are accurate, relevant, timely, consistent and without bias in that context. Where possible there is an identified authoritative single source*"
UK (The National Archives 2015)	*"Information must be accurate, valid, reliable, timely, relevant and complete to ensure that it meets the purposes for which it is intended."*
Canada (Government of Canada 2015)	"*Ensure information is complete, accurate, current, relevant, and understandable. Avoid collecting duplicate information."*
Estonia (Estonian Ministry of Economic Affairs 2014, p42)	"*Information is filtered/organised/stored and preserved according to its value, while its quality is ensured"*

Information gathered and stored needs to be 'relevant'. Determining what information is relevant and what is not is not always simple and different stakeholders are likely to have different perspectives on relevant. The need for agility implies adopting a forward-looking approach that anticipates as much as possible future needs for collected data. There is however ample evidence that public administrations are prone to collect data and information from citizens which is above and beyond what is strictly necessary to deliver public services or to make good decisions or even than they can manager (Bennet 2012; Latham 2016). Apart from the fact that collecting and storing unnecessary information costs money and undermines public trust, irrelevant information and too much information can cloud decision making (O'Reilly 1980; Edmunds and Morris 2000; Eppler and Mengis 2004).

To comply with this principle, information and data requirements need to be reverse engineered from both decision making and policy execution perspectives. The latter is the lesser problem; the former is

more challenging because decisions, unlike much execution, are often one off and it can be difficult to know in advance of a given policy decision exactly what information will be needed.

Good decision support system design starts with the decision to be made and works back to the information and data necessary to support the decision makers. This can mean a shift in mind set from a 'what data have we got" to "what data do we need" and "how can we efficiently access/acquire this data" so as to satisfy the increasing need for on-the-fly proactive decision making in real time.

Objectives

- Support evidence based decision making
- Support the delivery of high quality public services
- Facilitate the creation of public value
- Eliminate wasteful data conversion and information interpretation activities
- Implement agreed standards
- Exploit relevant external sources of information
- Interoperability by default
- Apply the minimality approach – only data which is needed is collected and stored
- Eliminate errors arising from poor quality data/information
- Eliminate errors from out-of-date data/information

Enablers

- Training
- Process design
- Metadata systems
- Once only principle
- Search engines
- Federated, distributed and service oriented architectures
- Setup advanced interfaces between the organization and the external environment, capable of dealing with the huge amount of available (big) data from multiple sources e.g. external information systems, social web, deep web, internet of things, sensors
- Good data capture and maintenance processes

4.3 Principle 3: The Management of Information

Information should be managed so as to optimise its quality and its relevance to good public administration and to maximise the creation of public value applying 'once-only' strategies where appropriate.

This principle covers the internal management and processing of information. It concerns the creation of digital ecosystems to support the complex multi-dimensional collaborative decision making that characterises modern administrations and the delivery of seamless user-centric digital public services.

Implementation of this principle should promote a knowledge-based culture and collaborative working methods across the administration. It involves the analysis, aggregation and combination of data and information, the de-siloisation of processes and systems and the implementation of interoperable solutions.

Several countries have similar concepts and preoccupations which are addressed by this principle:

Country	Comment

Australia (Victorian Government 2011, p3)	"*Government is largely a knowledge-based industry. For government to function effectively, the public, government employees and partner organisations must be able to find the information they need.*"
	"*Unmanaged information can lead to agencies breaching of their legal or statutory obligations.*"
	"Applying agreed standards to information makes it easier to use and interpret. Standards help to determine how information will be collected, described, defined, stored and shared."
UK (The National Archives 2015)	"*The opportunities for using information greatly increase when it is made available in standardised and linkable formats.*"
USA (ISE 2004)	"*Facilitates the availability of information in a form and manner that facilitates its use in analysis, investigations and operations.*"
Estonia (Estonian Ministry of Economic Affairs 2014, p42)	"*Information is separated, gathered together, systemized and presented according to the needs of the particular user – an official/partner (citizen/entrepreneur/another agency).*"

Implementing this principle requires putting in place mechanisms for identifying data sources, having catalogues, dictionaries and taxonomies set up as well as sophisticated search capabilities.

This requires the creation and maintenance of suitable metadata systems (European Commission 2014c) so that public servants can quickly find the information that they need.

Furthermore there needs to be review processes in place which continually, or at least periodically, reviews data for relevance and cost effective accessibility.

Finally to encourage reuse and facilitate ease of access a 'once-only' philosophy should be promoted and strategies adopted whereby each data item in a given system is stored once only in one location. Single instance storage and coherent distribution mechanisms eliminate the potential problems that can occur when multiple copies of the same data are held in different locations and by different organisations.

Objectives

- Support evidence based decision making
- Facilitate the creation of public value
- Promote a knowledge-based culture
- Adoption of collaborative working methods
- Eliminate silos
- Create synergies
- Digital by default
- Cross-border by default
- Implement/evolve to interoperable systems
- Ensure that information is properly

Enablers

- Standards
- Ontologies
- Master data, Reference data
- Guidelines
- Proactive communication on who produces what kind of information
- Data quality standards and processes
- Data standards i.e. formats, metadata, semantics

aggregated and combined
- Enable/ensure data integrity
- Coordinate data management to avoid overlaps
- Arrive at agreed standards
- Where possible, fe-use rather than re-invent
- Reduce storage and processing costs

4.4 Principle 4: The Sharing of Information

Information should be shared in ways that make it easy to (re)use, deliver and exchange and it should be made available through multiple channels.

This principle covers the use, exchange and sharing of information. Sharing information requires technical standards, semantic standards and legal structures. It also requires a willingness to share, something which is not always found in public administrations. A reluctance to share may arise from several concerns including (but not limited to) security, privacy and commercial sensitivity. There are two approaches to data sharing. One starts from the assumption that all data can be shared except for specific datasets which, for different reasons, cannot. The other is that no data is shared unless, for specific datasets, it is permitted. This CIMF principle is based on the first approach, 'open by default' i.e. data should be shared unless there is a specific reason for not doing so.

Most countries have concepts which are encompassed by this principle:

Country	**Comment**
New Zealand (ICT.gov.nz 2015)	"*Data and information held by government should be open for public access unless grounds for refusal or limitations exist under the Official Information Act or other government policy.*"
	"*Use and re-use of government held data and information is expected to be free. Charging for access is discouraged.*"
Canada (Government of Canada 2015)	" *Share and re-use information, respecting legal restrictions"*
UK (The National Archives 2015)	"*Public information should be published, unless there are overriding reasons not to."*
	"*The value of information can be multiplied by re-use, and therefore opportunities to re-use should be looked for proactively*."

Open and linked government data policies are gaining ground all over the world (Ding Li, 2012). However, rules about sharing may be complicated. Licensing of data can be complicated and there are numerous types of license in use ranging from Creative Common zero (CC0) which imposes no restrictions whatsoever on data use to a variety of quite limiting licences (Khayyat and Bannister 2015). Nonetheless, the principle is that government data, where possible, legal and safe to do so should be made available free of restrictions.

Data should be available through different channels to facilitate the work of different citizen groups.

Objectives:

- Make information sharing the norm and open-by-default
- Deliver to users what they need, when they need it
- Foster transparency and collaboration across the whole organization
- Provide multi-modal access (different devices, OSs, advanced GUIs and browsers)
- Foster and enable innovation
- Foster co-creation
- Facilitate the creation of public value
- Increase transparency
- Support open government

Enablers

- Data and information interoperability and standards
- Information that is published, searchable, findable and accessible across the whole organization via base registries
- Open and linked data platforms
- Incentives for information sharing and reuse
- Government commitment to and support for openness following the PSI and open data initiatives
- Multimodal access to information.

4.5 Principle 5: The Protection of Information

Information should be protected as prescribed by both EU and national legal codes as well as public administrations' data privacy and IT security policies.

Citizens and businesses must be assured that they interact with public administrations in an environment of trust and in full compliance with the relevant regulations and directives on privacy and data protection. Data must be processed "*lawfully, fairly and in a transparent manner*" and must be collected "*for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes*"(European Union 2016). Public administrations should respect fully the EU Regulation on Data Protection so as to guarantee the privacy of citizens and the confidentiality of information provided by businesses. In addition to data confidentiality attribution, data integrity, non-repudiation and data availability must all be guaranteed so that trust between the citizens and the administration is ensured. These needs should be taken into account in the design phase of systems and services and should be implemented within the context of a common IT security and data privacy policy.

It is important to note that this principle may conflict with the ideal states envisaged by a number of the other CIMF principles including freedom of access and sharing. Where that happens, this protection principle will trump others.

This principle addresses preoccupations expressed by several countries.

Country	**Comment**
Canada	*"Support access to information, respecting privacy, policy and legal requirements."*
	"*Safeguard information against unlawful access, loss and damage."*
UK (The National Archives 2015)	"*Ensure citizens and businesses can access information about themselves.*"

USA (ISA 2014)	"*…incorporates protections for individuals' privacy and civil liberties*"
	"*…incorporates strong mechanisms to enhance accountability and facilitate oversight, including audits, authentication, and access controls*."

Objectives

- Ensure that information is secure
- Prevent unauthorised access or usage
- Ensure compliance with the General Data Protection Regulation
- Protect citizens and organisations from potential misuse or accidental release of information.
- Privacy and Security by design

Enablers

- Digital rights
- Data protection legislation and directives;
- Data protection regulators
- Information security policy and implementation plan
- Data privacy policy and implementation plan
- Public awareness campaigns
- Security and Availability

4.6 Principle 6: The Preservation of Information

Information should be preserved to ensure continued access for as long as is appropriate in accordance with national and international legal, regulatory and archival requirements. Information which is unlikely to serve any future public purpose should be deleted.

This principle covers the last phases of the Information lifecycle and should ensure that an administration has policies and services in place to preserve information for the long-term. Processes and procedures to guarantee its integrity and authenticity over time, to make it available to the public after a certain time and to cooperate with the digital archives of the State's National Archives need to be in place.

Several countries have issues which this principle addresses:

Country	**Comment**
New Zealand (ICT.gov.nz 2015)	"*Agencies are stewards of government-held data and information and must provide and require good practices which manage the data and information over their life-cycle, including catering for technological obsolescence and long term preservation and access.*"
Canada (Government of Canada 2015)	"*Preserve information in accordance with its operational, legal, financial and historical value*."

An important, but often overlooked, consequence of this principle is that maintenance of data which needs to be stored over long periods (say a decade or more) must be stored in media which will be permanent and readable in the future. This means confronting the problem of what Vince Cerf has characterised as "bit rot", i.e. the inability to access data because the medium on which it is stored is no

longer accessible (Sample 2015). Bronze Age clay tablets are still perfectly readable today. Even when all files were on paper this was, at worst, a long term problem as good quality paper has a life of several hundred years. Current forms of magnetic media may have a life of less than ten years. Implementing this principle will require development of long term storage strategies.

When data is no longer serving any useful purpose and is not going to do so at some future time it should be permanently deleted. This is not just to ensure compliance with data protection and privacy legislation, but on the ground of efficiency. Implementing this principle means that good practices for immediate deletion need to be in place as do periodic review processes.

Objectives	**Enablers**
• Ensure that information is preserved according to its historical value • Ensure the authenticity and integrity of preserved information • Avoid potential loss of data due to fragility of the medium on which data is (initially) stored • Ensure that technological obsolescence does not impact accessibility • Ensure that information is deleted when no longer needed or of value • Dispose of information that is not of historical value • Reduce unnecessary storage • Improve search and access by reducing clutter	• Information preservation policy and implementation plan • Standards-based long term digital preservation solutions • Organisational entities in charge of information preservation policy and implementation plan • • Organisational entities in charge of preservation and archiving • Preservation and archiving • Time stamping • Training • Regular Reviews of data relevance

5. Implementation Issues

It serves no purpose for a large and complex public administration to address the issues discussed independently for each principle. To achieve the potential benefits accruing from better information management, a holistic information management framework is proposed which fosters mutual understanding by all stakeholders of the challenge, creates a common space for discussion and facilitates the monitoring and follow-up of agreed actions. This is the purpose of the proposed CIMF.

The CIMF needs to be tailored to the specific needs and maturity of each administration. It is important that the resulting variant of the CIMF remains at a high level and at the same time provides practical direction and advice. To this end, both the objectives and more importantly the enablers for each principle should be elaborated and detailed taking into account the specific circumstances of each administration.

Applying this framework would inevitably introduce significant cultural changes throughout an

administration. The horizontal/corporate versus vertical/department view and the focus on local versus global optimum may require fundamental cultural re-orientation on how local managers report to and coordinate with the corporate level. This could in turn create a need for new job profiles and coordination roles, introduce new horizontal and silo-breaking processes and require coordinated local and corporate actions and project management. Resistance to change could be a reaction if such changes result in a redistribution of power within the organisation.

For these reasons it is considered critical that the framework be approved and supported by top management at corporate level and that it continue to enjoy their support, ownership and political sponsorship underpinned by permanent senior management commitment and oversight.

Corporate approval for this shift in emphasis from technology to information and from local to corporate would require a comprehensive cost-benefit analysis, a risk assessment, a road map, a communication strategy and inclusive governance structures.

CIOs (who have existed in a number of EU countries for some time and have recently been appointed in several others) should be responsible politically for the CIMF. The operational implementation may be delegated to a Chief Data Officer whose responsibility for corporate data quality across the administration is supported by the CIMF.

The framework, once tailored to an administration's specific needs, should be internally communicated in a language that is easy to understand for all stakeholders. It should remain stable over time with a change management mechanism well-described and established.

Once adopted an essential element of the CIMF implementation would be the definition of an organisation-wide Data Policy specifying elements such as classification, metadata, licensing, quality as well as more social aspects of data governance including public engagement, roles and responsibilities.

The internal communication actions should include training, guidance and the sharing of data management techniques that address day-to-day issues so as to embed the framework in everyday work practices.

Development and service delivery guidelines need to be updated and adapted so as to emphasise the CIMF and to ensure that its principles underpin all IT activities. Existing and new systems, as well as all internal and external information flows should be positioned and analysed vis-à-vis the CIMF. New corporate software systems may need to cover the gaps between the silos.

A hallmark of modern public administrations is the quality of their digital public services and associated information systems. Embedding the CIMF principles in an administration's IT design, development and delivery processes should contribute to the evolution of the portfolio of mission-critical systems resulting in better quality and more innovative, user centric, reliable and permanent eGovernment services based on common interoperable and reusable components (Coyle et al 2010; Deasy and Noel 2010).

In this context adopting an ***'Interoperability-by-design/privacy-by-design/security-by-design/digital by default/cross-border by default/open by default***' paradigm for the development of digital services based on the CIMF principles would create a culture where the '*Information Layer*' and Information Interoperability take centre stage **:**

"The Information Layer... the stuff of information...we should think imaginatively about what it could be like for computer systems not only to make such stuff available to users, but to exploit it for themselves" (Spärck Jones 2007).

These organizational and technological changes may require substantial dedicated human and financial resources.

It is reemphasised that the CIMF must be established managed and implemented at the corporate (or enterprise) level, justifying the "C" in its title. Once adopted, the CIMF has the potential to become the cornerstone for a broader corporate information management strategy for the administration which should be put in place to maximise the quality, security and accessibility of its information.

6. Conclusion

In this paper, we have outlined some of the challenges modern public administrations face when managing information. To contribute to meeting these challenges and accommodate ever-increasing information needs, the adoption and promulgation of a Corporate Information Management Framework (CIMF) is proposed. This proposal is based on experiences and best practices identified in several countries and in a number of academic sources.

The fact that the CIMF is at the global, corporate level, articulating a holistic set of information management principles to be applied across the administration, represents a paradigm shift and introduces, we argue, a revolution in how public administrations manage information. It should contribute, over time, to less siloisation, greater ease of information exchange and better data quality.

With the growing demand for digital public services, the advent of big data, the imminent arrival of the Internet of Things and escalating cyberattacks, information management will become more politically important. Widespread endorsement of this framework would send a timely message that the EU Institutions and public administrations across Europe are laying the foundations for information policies fit for purpose for the public sector in the 21st century (Irish Times 2000).

Finally the CIMF may also be considered as a contribution to the broader discussions on the changing role of digital information in public administrations including its management, protection and preservation; and the need for a new Social Contract between the State and its citizens for the Digital Age.

While designed with the public sector in mind, there is no reason why the CIMF proposed in this paper could not be considered an example of best practice applicable to the private sector. It could also be the basis for a global information management framework to address the information issues linked to climate change, trade, terrorism and civil rights.

Acknowledgements

The authors of this paper acknowledge the many stimulating discussions and contributions of European Commission staff in the Informatics Directorate General and the Secretariat General. However the opinions expressed in this paper are solely those of the authors and are not official policy of the Commission.

References

Ackoff, R. L. (1989) From data to wisdom, *Journal of applied systems analysis*, *16*(1), 3-9.

Barocas, S., and H. Nissenbaum (2014) *Big data's end run around anonymity and consent* (pp. 44-75), Cambridge University Press, NY.

Bennett, D. (2012) The U.S. Government Has Collected More Data Than It Could Ever Possibly Read, The Wire, May 10th 2012. Available at: http://www.thewire.com/technology/2012/05/us-government-has-collected-more-data-it-could-ever-possibly-read/52179/

Bovalis, K., Peristeras, V. Abecasis, M. Abril-Jimenez, R.-M. Alvarez Rodriguez, M. Gattegno, C. Karalopoulos, A. Sagias,, I. Szekacs and S. Wigard (2014) Promoting Interoperability in Europe's E-Government, Computer, 47(10), pp. 25-33. Available at: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6926660&isnumber=6926651,

Brague, C. and R. Champlin (2014) Enterprise Information Management with SAP (2nd Edition), SAP Press.

Brynjolfsson, E., 1994. Information assets, technology and organization. *Management Science*, *40*(12), pp.1645-1662

Coyle, L., L. M. Hinchey, B. Nuseibeh, J. L. Fiadeiro (2010) Introduction: Evolving Critical Systems, Computer, 43(5), pp. 28-33.

Deasy, D. and F. Noel (2010) Critical Systems Enabling European Integration, *Computer*, 43(5), p32.

Ding Li, Peristeras V., Hausenblas M., (2012), Linked Open Government Data (Editorial), IEEE Intelligent Systems, 27(3): 11-15.

Edmunds, A. and Morris, A. (2000) The problem of information overload in business organisations: a review of the literature. *International journal of information management*, 20(1), pp.17-28.

EIU (The Economist Intelligence Unit) (2008) *The future of enterprise information governance*, EIU.

Eppler, M.J. and Mengis, J. (2004). The concept of information overload: A review of literature from organization science, accounting, marketing, MIS, and related disciplines. *The information society*, *20*(5), pp.325-344.

Estonian Ministry for Economic Affairs (2014) Information Governance: Current situation analysis and implementation strategy. Available at:
www.mkm.ee/sites/default/files/information_governance_analys_strategy_oige.pdf

European Commission (2010a) European Interoperability Framework (EIF) for European public services. Annex 2 to "Towards interoperability for European public services". Available at:
http://ec.europa.eu/isa/documents/isa_annex_ii_eif_en.pdf.

European Commission (2010b) The European eGovernment Action Plan 2011-2015; Harnessing ICT to promote smart, sustainable & innovative Government, COM (2010) 743 Final. Available at:
http://www.umic.pt/images/stories/publicacoes5/action_plan_en_act_part1_v2.pdf.

European Commission (2011) European Interoperability Architecture (EIA) Phase 2 – Final Report : Common Vision for an EIA, Available at:
http://ec.europa.eu/isa/documents/isa_2.1_eia-finalreport-commonvisionforaneia.pdf.

European Commission (2012) Communication from VP Šefčovič to the Commission: Delivering user-centric digital services, SEC(2012) 492 Final. Available at:
http://ec.europa.eu/dgs/informatics/ecomm/doc/communication_sefcovic_tothecom.pdf.

European Commission (2013) DIRECTIVE 2003/98/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 17 November 2003 on the re-use of public sector information. Amended by: Directive 2013/37/EU of the European Parliament and of the Council of 26 June 2013. Available at:
http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:02003L0098-20130717&from=EN

European Commission (2014) *Annual Growth Survey 2015*, COM(2014) 902 final. Available at:
http://ec.europa.eu/europe2020/pdf/2015/ags2015_en.pdf.

European Commission (2014b) *Proposal for a DECISION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL establishing a programme on interoperability solutions for European public administrations, businesses and citizens* (ISA2), Brussels, 26.6.14 COM(2014) 367 Final, Available at:
http://ec.europa.eu/isa/documents/isa_2_proposal_en.pdf

European Commission (2014c) *Methodology and tools for Metadata Governance and Management for EU Institutions and Member States*. Available at:
http://joinup.ec.europa.eu/site/core_vocabularies/governance_and_management_of_structural_metadata/Methodology-and-tools-for-Structural-Metadata-Management-and-Governance-for-EU-Institutions-and-Member-States_v1.00.pdf

European Commission (2015a) *Interoperability Solutions for European Public Administrations: Our ISA Solutions for you*. Available at:
http://ec.europa.eu/isa/ready-to-use-solutions/index_en.htm.

European Commission (2015b) *Interoperability Solutions for European Public Administrations: ISA2*. Available at:
http://ec.europa.eu/isa/isa2/index_en.htm.

European Commission (2015c) *DCAT application profile for data portals in Europe*. Available at: https://joinup.ec.europa.eu/asset/dcat_application_profile/description.

European Commission (2015d) *A Digital Single Market Strategy for Europe*. SWD(2015) 100 Final, Available at: http://ec.europa.eu/priorities/digital-single-market/docs/dsm-communication_en.pdf.

European Commission (2013) *Interoperability Maturity Model, Joinup e-Library April 23rd 2013.* Available at: https://joinup.ec.europa.eu/elibrary/document/interoperability-maturity-model.

European Union (2009) *Ministerial Declaration on eGovernment, se2009eu*. Available at: https://ec.europa.eu/digital-agenda/sites/digital-agenda/files/ministerial-declaration-on-egovernment-malmo.pdf.

European Union(2016) Regulation (EU) 2016/679 on the protections natural persons with regard to the processing of personal data and of the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)
Geragas, D. (2015) Value and Implications of Master Data Management (MDM) and Metadata Management, *SEMIC 2015*, 5th May 2015 Riga – Latvia.

Glazer, R., 1993. Measuring the value of information: The information-intensive organization. *IBM Systems Journal*, *32*(1), pp.99-110.

Government of Canada (2015) Public Works and Government Services Canada: Information Management – Knowledge Area. Available at: http://www.tpsgc-pwgsc.gc.ca/biens-property/sngp-npms/ti-it/conn-know/gi-im-eng.html#wb-tphp

Hausmann, V., S. Williams, C. Hard and P. Schubert (2014) Enterprise Information Management Readiness: A survey of current issues, challenges and strategy, *Procedia Technology*, 16, pp. 42-51.

IDBAC (2010) CAMSS: *Common Assessment Method for Standards and Specifications*. Available at: http://ec.europa.eu/idabc/en/document/7407.html.

ICT.gov.nz (2015) *Guidance and Resources*, Available at: https://www.ict.govt.nz/guidance-and-resources/open-government/new-zealand-data-and-information-management-principles/

Irish Times (2000) “Let Us Step With Hope Into Our New Century", Editorial, 1 January 2000.

ISE (Information Sharing Environment) (2004) Intelligence Reform and Terrorism Prevention Act of 2004, Sec 1016, Information Sharing. Available at: http://ise.gov/intelligence-reform-and-terrorism-prevention-act-2004-sec-1016-information-sharing

ISE (Information Sharing Environment) (2014) *Data Aggregation Reference Architecture (DARA)* Version 1.0, December 2014, Available at: https://www.ise.gov/resources/document-library/data-aggregation-reference-architecture-dara-v10

ISE (Information Sharing Environment) (2015a) *Geospatial Interoperability Reference Architecture*, (GIRA) Version 1.0, April 2015, V 1.0, Available at: https://www.ise.gov/resources/document-library/geospatial-interoperability-reference-architecture-gira

ISE (Information Sharing Environment) (2015b) *Project Interoperability Startup Guide*, April 2015, V 1.0, Available at: http://project-interoperability.github.io/

Jackson, I. F. (1986). *Corporate Information Management*. New Jersey, Prentice-Hall, Inc.

Jenkins, T. (2012) *Behind the Firewall. Big Data and the Hidden Web: The Path to Enterprise Information Management*, Open Text Corporation.

Khatri, V. and Brown, C.V., 2010. Designing data governance. *Communications of the ACM*, *53*(1), pp.148-152.

Khayyat, M., & Bannister, F. (2015). Open data licensing: More than meets the eye. *Information Polity*, *20*(4), 231-252.

Kooper, M.N., Maes, R. and Lindgreen, E.R., 2011. On the governance of information: Introducing a new concept of governance to support the management of information. *International Journal of Information Management*, *31*(3), pp.195-200.

Moody, D.L. and Walsh, P., 1999, June. Measuring the Value Of Information-An Asset Valuation Approach. In *ECIS* (pp. 496-512).

Latham, E. (2016) Is the Government Hoarding Too Much Data?, Government Technology, February 9th 2016. Available at: http://www.govtech.com/opinion/Is-the-Government-Hoarding-Too-Much-Data.html

Official Journal (2008) *Consolidated versions of the Treaty on European Union and the Treaty on the Functioning of the European Union*, 51, 9th May 2008. Available at: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:C:2008:115:TOC.

Official Journal of the European Parliament (2000) *The EU Charter on Fundamental Rights*, 2000/c 364/01. Available at: http://www.europarl.europa.eu/charter/pdf/text_en.pdf

O'Reilly, C.A., 1980. Individuals and information overload in organizations: is more necessarily better?. *Academy of management journal*, *23*(4), pp.684-696.

Peristeras V. (2013) Semantic Standards: Preventing Waste in the Information Industry, IEEE Intelligent Systems, 28(4) pp. 72-75, July-Aug.

Sample, I. (2015) Google boss warns of 'forgotten century' with email and photos at risk, Manchester, *The Guardian*, 13th February 2015. Available at: http://www.theguardian.com/technology/2015/feb/13/google-boss-warns-forgotten-century-email-photos-vint-cerf

Sarsfield, S., 2009. *The data governance imperative*. IT Governance Publishing

Semantic Community (2015) Core Vocabularies. Available at: http://semanticommunity.info/Be_Informed_for_SEMIC.EU/Core_Vocabularies.

Spärck Jones K. (2007) Natural Language and the Information Layer, in 2007 Athena Lecturer Award, SIGIR '07 Proceedings of the 30th annual international ACM SIGIR conference on Research and development in information retrieval, pp 3-6.

The National Archives (2015) *Information Principles*. Available at: http://www.nationalarchives.gov.uk/information-management/manage-information/planning/information-principles/

Van de Lans, A. and P. van Til (2013) Enterprise Information Management (EIM), in Baan, P. (Ed). Enterprise Information Management: When Information Becomes Inspiration, New York, Springer.

Victorian Government (Australia) (2011) *Information Management Principles*, Available at: http://www.enterprisesolutions.vic.gov.au/wp-content/uploads/2015/09/IM-GUIDE-00-Information-Management-Principles-2.0.pdf

Vom Brocke, J. and A. Simons (2014) Enterprise Content Management in Information Systems Research: Foundations, Methods and Cases (Progress in IS), Berlin, Springer.