BIR

Business Information Review
2015, Vol. 32(4) 212–219

DOI: 10.1177/0266382115616301
bir.sagepub.com
SAGE

Why is information the elephant asset? An answer to this question and a strategy for information asset management

Reynold Leming
Managing Director, Informu Solutions Ltd and *Conference Director of the Information and Records Management Society, UK*

Abstract
Information is a vital asset for any organization, but information does not often appear in definitions or descriptions of asset management. This article addresses the development of information asset management techniques and strategies and the various issues and problems that impact on that development.

Keywords
Information Governance, Asset Records Management

Introduction

Information is a vital business asset for any organization. Everything we do does involve using information in some way. It is used to support and inform effective decision-making and facilitate ongoing operations and the delivery of programmes, products and services, as well as evidence activity, performance, rights and obligations. In the age of both ever increasing information volumes and evolving legal obligations, as an organization seeks to leverage their information content to unlock value and identify risk, it is increasingly important for their data to be suitably protected, readily accessible and properly governed.

However, information does not often appear in definitions of asset management. For example, on Wikipedia, at the time of writing, it offers a definition of 'tangible assets such as buildings and to intangible assets such as human capital, intellectual property, and goodwill and financial assets', with a further explanation of tangible physical and infrastructure assets as for example 'structures, production and service plant, power, water and waste treatment facilities, distribution networks, transport systems, buildings' (Wikipedia, 2015). Given our tacit understanding of the importance of information, why is it the elephant in the room when we look at formal asset management processes?

It's all about money

There is a great quote by Gartner analyst Doug Laney who explains the problem of information asset management: 'It's frustrating that companies have a better sense of the value of their office furniture than their information assets'. Or as I spin it: *Do we know more about our filing cabinets and computers than about the information they contain*? Perhaps it is because we do not know how to value information?

The business value of information as an intangible asset/goodwill is undoubted and of course increasingly we are seeing the productization of data and information, especially with the 'big data' generated by the Internet of things and so on. Infonomics as a concept is rapidly developing, particularly with the work being undertaken by Gartner. Also the software company RSD is currently conducting an Infonomics project with Haute Ecole de Gestion de Genève (HES-SO University of Applied Sciences Western Switzerland).

However – aside from acquisition and maintenance costs – currently there are a lack of established models for information to determine revenue contribution, market value and depreciation as well as other impacts on the balance sheet. But let us not give up hope now. There hopefully will be a time when part of our role will be that of *information accountant*. Until then, this article discusses other ways to ensure that information management best practices are embedded into the corporate psyche in the same way that health and safety are.

Corresponding author:
Reynold Leming.
Email: reynold@informu-solutions.com

Musings on the definition of information

If information asset management is a systematic process of valuing, classifying, deploying, securing, utilizing, maintaining, measuring, monitoring and disposing of assets efficiently and cost-effectively, then we must understand the scope of 'information' in business processes.

Information units contain facts and knowledge presented in physical or digital 'content' containers, a primary one of which within business is the document. To ensure the consistent application of processes and governance we must therefore look at information holistically, irrespective of format or medium. We must also, therefore, include the underlying data sources that generate computer reports and other information types. Thus, information assets can cover a broad range, including:

- 3D objects such as samples that form part of an audit trail;
- audio and video recordings;
- backup tapes and media;
- books and journals;
- drawings, physical and CAD;
- emails;
- glass plates;
- instant messages and chat;
- lantern slides;
- manuscripts;
- maps and plans;
- microfilm/microfiche;
- paintings;
- paper files;
- photographs;
- social media content and posts;
- structured data;
- text messages;
- unstructured and semi-structured data;
- Web content on intranets, extranets and Web presences; and
- Wiki pages and blogs.

You really need a corporate function

I would like to see all organizations, where their size justifies this, having a dedicated corporate function for information (asset) management, covering strategy, governance and service delivery.

Information management should ideally be a central function, cross-cutting of the organization, subject to controls and given resources in the same way as other functions that involve management of assets, such as finance, human resources and property. This ensures that a consistent purpose, role and vision are delivered that aligns with the overall purpose and the strategic goals and themes of the organization.

You can also achieve ongoing efficiency savings by removing the duplication of roles and increasing collaboration across traditional departmental boundaries.

Records management, information security, business continuity and data management are all interrelated disciplines, requiring coordination to ensure that the confidentiality, integrity, availability and disposition of data and content are robustly and consistently managed throughout their life cycle. All these disciplines are fundamental to information asset management and risk mitigation.

The central function would work with a defined network of 'local' champions and experts who would ensure that activity can be embedded into 'business as usual' work. However, a robust and empowered core team will be even more important, as an organization devolves more activity and accountability into business units, providing the critical services of strategy, governance, risk and assurance.

Binding it down

To quote Thomas Jefferson, 'In questions of power, then, let no more be heard of confidence in man, but bind him down from mischief by the chains of the constitution' (Jefferson, 1798, 8th Resolution). That's a bit over the top, yet governance structures should be in place to ensure that there is leadership, direction, accountability, implementation, reporting and monitoring of information management both for active programmes and the ongoing sustainability of best practice. The things to consider to get information asset management bound down and embedded include the following:

- Information management should be recognized as a corporate function, with the organization's commitment to information governance and management (e.g. the importance of, and arrangements for, ensuring the proper management of key records) outlined in key strategic documents, such as the corporate plan.
- Central responsibility for information management, as discussed above, must be assigned within the organization, and an individual at top management level must have overall strategic responsibility. At the very least, director-level sponsorship should be in place, with delivery and reporting structures in place, ensuring monitoring and scrutiny.
- There should be an information management strategy, which includes specific objectives. The corporate objectives for information management are linked to business objectives.
- The role of the head of information management should be clearly defined and of appropriate seniority.
- The information management function, managed by the head of information management, should receive

the necessary levels of organizational support to ensure its effectiveness.
- The information management function should have clearly defined responsibilities and objectives and the resources to achieve them.
- There would be some form of information management challenge and scrutiny panel to provide independent, expert advice and opinion on the scope and direction of the organization's information management programme and delivery.

Business as usual

Information management policy should cover the roles and responsibilities of the sponsor/function head, senior management, records and other information management professionals, business unit managers, technical systems staff and individual employees.

Policies will need a related framework of supporting standards, procedures and guidelines covering all aspects of the information life cycle, irrespective of medium or format. Fundamentally, all employees are responsible and accountable for keeping accurate and complete records of their activities. Everyone needs to be an information manager as well as an information user. However, day-to-day functional responsibility for information management processes – including maintaining asset registers (see more on this below), being superusers for the Electronic Document and Records Management (EDRM) systems, collating records eligible for disposition and physical archiving – can be delegated to a departmental information/records management champion.

It is important that not only are roles and responsibilities for managing information defined and assigned at all levels of the organization to ensure effective record keeping but also that human resource (HR) policies and practices should support sustainable good practice in information management. It should be seen as being 'part of the day job' and fully integrated into planning, monitoring and reporting processes in the organization. Accountability for information management throughout the organization should be clearly and formally defined and be part of the corporate performance appraisal system.

Specific skills and responsibilities in relation to information management should be identified, and the organization should undertake an assessment of the information management skills that it has in place across the workforce and identify potential gaps. Human resource policies and practices for recruiting and retaining good quality staff should include the regular analysis of information management training needs. Roles and responsibilities below the strategic level in relation to information management should be clearly defined and documented and be incorporated into job descriptions.

Human resource policies and practices should include the establishment and maintenance of a scheme, such as the competency framework, to identify the skills and knowledge and corporate competencies required in records and information management. The competency approach should include job and person specifications and an outline of training and development issues.

Human resource policies and practices should include the regular review of selection criteria for posts with information management duties to ensure current compliance with best practice. They should also include the establishment of a professional development programme for staff with records management duties. The organization should have provided training to ensure that all staff have the necessary skills and knowledge in relation to information management. There should be corporate arrangements in place to ensure that information management training provision is periodically evaluated and adapted to respond to changing needs.

Policies and practices should include the inclusion in induction training programmes, for all new staff, of an awareness of information management issues and practices.

Any weaknesses identified through internal or external reviews of information management should be adequately addressed through the training programme or briefing sessions. The organization should be able to demonstrate that it has identified future developments that may impact on information management staff skills and capacity and is proactively managing these.

There should be regular update training for staff to ensure the latest changes in information management law, procedures, guidance and systems are disseminated and acted upon in a timely manner. Exit processes should include a handover of knowledge from staff of record-keeping 'systems'.

Communicate, communicate, and communicate!

The corporate commitment to information management must be communicated clearly, via an ongoing campaign, reinforcing the message that all staff have a responsibility for information management, in line with corporate governance, to ensure that all staff are aware of the strategy, its benefits and their obligations.

Particularly, this supports the management of (cultural) change in the communication of the beneficial outcomes of specific programmes.

Key principles and messages

- The vision (as it interfaces to business strategy).
- The business case and benefits realization strategy for specific programmes (continuous identification, optimization and tracking to ensure outcomes are achieved; how success will be measured).
- The quick wins achieved.

- The (new) roles and responsibilities for supporting and managing information management (so that staff know what is expected of them and why).
- Approved supporting policies, procedures, standards, FAQs and guidelines; the organization should be able to demonstrate that it is proactive in informing staff of any policy or procedure updates on a timely basis.
- Awareness of supporting processes (so that the organization is seen to have appropriate personnel available with relevant skills and experience to set-up, manage and deliver the programme).
- Decisions made at governance, programme or project board meetings and so on.
- Addressing matters and issues arising out of a staff survey of awareness and opinion regarding the principles and methods of record keeping.
- FAQs can dispel rumours as well as answer questions.
- Communication when change has happened is vital.

Thoughts on tactics and methods

- Any campaign must be memorable and probably utilize mixed media techniques.
- There must be collaborative stakeholder involvement and feedback loops (trust comes from sharing and involvement).
- Production of consolidated, cross-referenced documentation, with quick reference guides.
- Circulation of updates and briefing notes (electronic newsletter, email, notice boards and social tools).
- Maintenance of a dedicated intranet area.
- Interactive questions answered approach.
- Roadshows, surgeries and floor walking.
- E-Learning where possible.
- Using and leveraging the network of local 'Champions'.

Register, register, and register!

I propose that populating and maintaining an information asset register (IAR) is an important step in ensuring that information is understood, valued, leveraged and risk managed. It can provide a comprehensive record of all important informational and evidential physical and digital assets. The assets can be described and profiled to their information type, ownership, location, format, security, criticality, source, activity and so on; tagged to a vocabulary of functions and activities within a business classification scheme; and thus aligned to retention and disposal policies.

Your organization, including the C-suite, can be reassured that (i) there is an understanding of the legal issues and requirements for the entire corporate information landscape and 'duty of care' responsibilities are in place and (ii) that the organization is leveraging its information for insight and innovation.

There are a number of deliverables and benefits that an IAR can provide to a range of different stakeholders within an organization:

Information governance and records management: A recognition and understanding of all types of information held and maintained, together with the issues and risks. Information processes and transactions can be automated, including risk assessments, information access requests (e.g. Freedom of Information (FOI) and Data Protection), transfer and disposal actions. An IAR can also be used to create and maintain business classification schemes and retention schedules and understand the impact to assets of any future changes in law or regulation.

Information security: Identifying, protecting and risk managing confidential personal and commercially or otherwise sensitive information, particularly in helping avoid data loss and breach. It can also be deployed as an ISO 27001 Asset Register and inventory system.

Business continuity: Identifying, protecting and risk managing 'vital' records that are critical to the running of the organization and that, if the original is lost or destroyed and cannot be replaced, would seriously impair or disrupt normal business or might place the organization in legal or fiscal jeopardy.

Technology management: Being able to map, assess and manage the line of business applications in place, including aspects such as utilization, duplication, contingency, licensing, retirement, platforms, data archiving, retention and disposal. It can also be used as an asset register for systems software, computer and communications equipment.

Facilities management: Identifying paper and other physical record collections, capturing their location and metrics to support space planning, office moves and changes. It can also be used as an internal inventory management system for records held by offsite archive storage facilities if this is under the control of facilities.

Insurance management: Help in understanding the scope and risks to confidential information to support planning for cyber insurance.

Risk, audit and compliance: Providing the insight to information existence, ownership and location to enable proactive risk management and investigations. It helps meet regulatory obligations for record keeping and information security as well as ensuring that good systems and controls are in place. Also it is supporting assurance on the extent to which appropriate management and control structures are in place for managing information assets and risks, acquiring and disposing of these

assets and monitoring their use and performance. Information asset management is fundamentally a part of overall good practice for general operational risk management.

Legal affairs: In mapping the information landscape, an IAR can help both electronic and physical discovery for litigation, investigation or tribunal as well as facilitating the issue of legal hold notifications to suspend disposal processes.

Historic archiving: Use of the IAR to identify information of heritage value and record its transfer to appropriate historical archives at a suitable point in its life cycle.

Knowledge management: A high-performing organization consistently improves its use of data and information to increase its knowledge, thus leading to wisdom, insight and innovation. The IAR can help information scientists and data analysts fully understand the scope of what the organization holds and where it is located. Therefore, it can support marketing, research and development and so on.

So just what is an asset (within an IAR)?

One thing I am glad to see is that many organizations I speak with have created or are in the process of creating an IAR. There are many approaches to creating a register – spreadsheets, access or other bespoke databases, SharePoint lists, asset management tools within ERP systems, many EDRM systems and increasingly a number of specialist applications. It is fair to say that, in most cases, currently they are crafted within spreadsheets. I think that a database approach is ideal, overcoming limitations not accounting for variations of profiles for mixed format types, facilitating interrogation or allowing audit trails of information processes – but more on that later.

Firstly, I would like to discuss the scope of an 'asset' within an IAR. The UK National Archives (2015) 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 effectively' and that 'Information assets have recognisable and manageable value, risk, content and lifecycles' (p. 2). That is eloquently put and I will not seek to amend within this article.

They also state importantly, and again I totally agree with this, that 'Assessing every individual file, database entry or piece of information isn't realistic. You need to group your information into manageable portions'.

An asset is essentially a cognate group of data and information sharing the same rules and purpose, and it is any valuable physical or digital information unit that you wish to identify, profile and manage. This could of course be a singularly important individual thing or a related collection of stuff.

Thus, for example, you might treat the paper employee leavers' files or the digital information and communications technology help desk logs for an individual year as single asset if they are filed, archived and disposed of in a uniform manner. However, equally an important individual record, such as an insurance or other certificate, might be an asset in its own right.

Often though the asset refers to a collection. Therefore, I propose the concepts of master assets with related sub-assets. A master asset identifies and describes a related series of records sharing the same purpose. A sub-asset record, which is linked to a master asset, is used where required for detailed profiling, asset tracking and disposition processing. Thus, for example, if the accounts payable records are a master asset, the records for an individual year might be recorded as a sub-asset when they are either archived or destroyed. Sub-assets can also be used to reflect the various entities in different formats that make up a master asset – this might include for example paper correspondence files, a status tracking spreadsheet and a master contact management database. As each of these will have characteristics based upon their format, we therefore have three types of sub-asset – physical, digital and data set. There could of course be more – for example, equipment, more specialist physical types such as microform and so on.

Relevant to this is another entity – that of information system. A single system, be it a line of business application or archiving/document/content/records management system, could of course store multiple sub-assets.

Figure 1 shows an example architecture for an IAR:

The following is a list with some ideas on key assets that an organization might hold:

Audits: including internal, external and financial audit records.

Building and land records: such as maps, plans, registers, surveys, drawings, photographs, project works, contractor arrangements, deeds, leases, acquisition and disposal.

Business performance: business improvement and performance records.

Business plans: all business plans, including local delivery plans.

Committee records: agendas, minutes and reports for every individual committee meeting.

Company secretarial and corporate governance: the constitutional, accounts, board and investor administration records required under the Companies Acts, as well as establishment orders, codes of conduct, risk registers, standing financial instructions and standing orders.

Complaints: complaints and other key customer correspondence, including of course enquiries, compliments and comments.

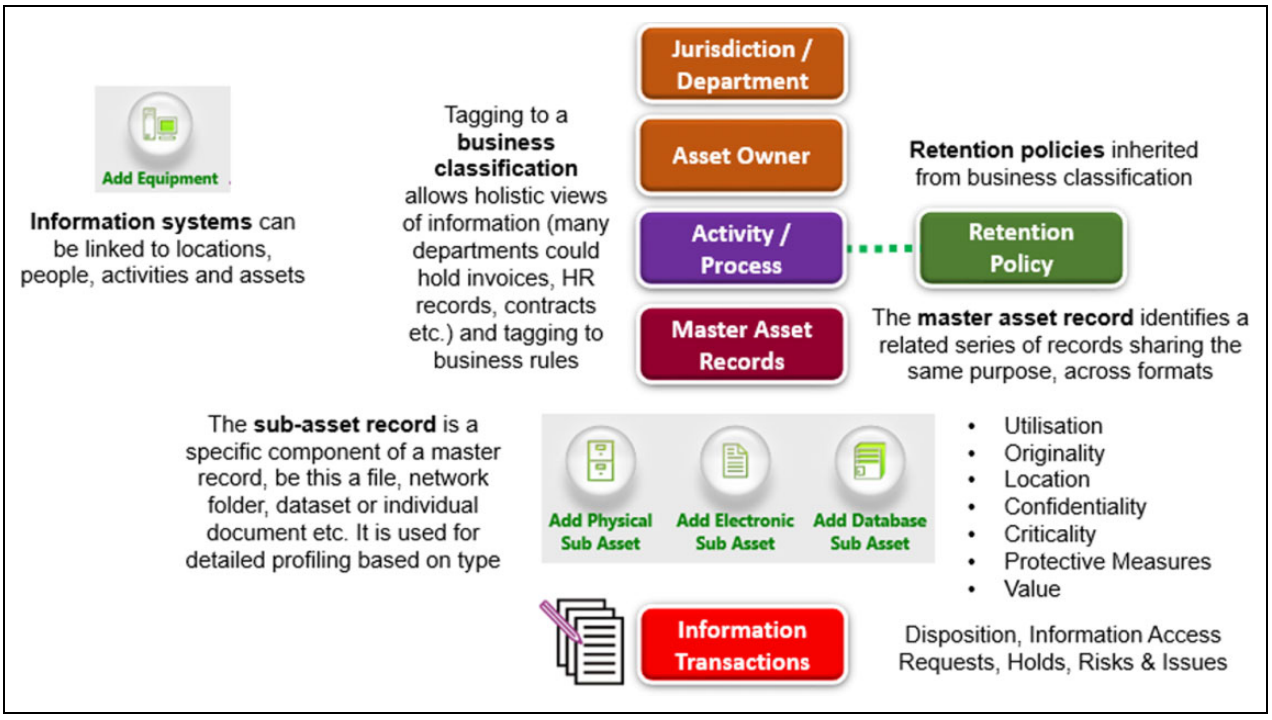

Figure 1. Architecture for an information asset register.

Contracts: all contracts, agreements, schedules and variations.

Environmental records: key environmental and waste management records.

Equipment records: all equipment and plant records – including inventories, specifications, inspections, testing and maintenance.

Establishment records: such as organization structures.

Financial records: the key sets of financial records for each financial year, including both financial and management accounting.

Funding records: all fundraising, charitable gift and benefaction records.

Health and safety: records of all inspection and occupational health processes.

Historical interest: where there are enduring cultural and/or historical considerations.

Incidents: all incident 'cases' within the organization, whether, for example, health and safety, environmental, compliance or information governance related.

Information access requests: all information access requests, that is, as applicable under Environmental Information Regulations, FOI and Data Protection.

Internal services: the work order and delivery records of internal services, such as IT and Facilities.

IT systems: related to the scope and utilization of all IT systems in the Trust, including key documentation regarding ownership and support.

Legal cases and tribunals: all open and closed legal and tribunal cases and related precedent and key reference information.

Pensions: all pensions/superannuation scheme records.

Policies and procedures: all policies, standards, toolkits and procedures.

Procurement and suppliers: all tendering, procurement management, supplier approval and stores records.

Programme and project records: all programme and project records, whether corporate or departmental.

Publications: all publications produced and used by the organization.

Records inventories: all records management indices, registry lists, publications schemes, as well as records documenting archiving, transfer and destruction.

Reports: all key reports, including statistical returns, produced by or for the organization.

Research and development: all records relating to research and development activities.

Service development: all service development records, including those relating to the commissioning of external/outsourced services.

Staff current and leavers: records of all employee and staffing records, including corporate HR and departmental staff records and those for volunteers.

Training events: all training materials and event records.

Transport: all fleet management records, including operating licences, vehicle maintenance and drivers' logs.

Web content: all Web and social media presences, including content that has been archived.

Work tracking: all spreadsheets and databases that log work and/or case instances.

A brief look at data classification

There are many ways to classify an asset or sub-asset. Fundamentally, it is about engaging with the list of stakeholders in information asset management identified above, understanding their requirements and objectives, thus leading to a determination of what to audit and identify.

I will below quickly cover three key areas: security; business continuity and retention.

Security classification

As part of risk management processes, a core objective is to ensure that suitable protective measures are in place for confidential personal and commercially sensitive information. Appropriate information handling rules and methods can then be applied to these assets when they are at rest, on the move or disposed of.

Within the UK in 2014, a new classification system, the Government Security Classifications Policy, replaced the old Government Protective Marking Scheme. In summary, this standard is:

- Top secret: information marked as Top secret is that whose release is liable to cause considerable loss of life, international diplomatic incidents or severely impact ongoing intelligence operations. Disclosure of such information is assumed to be above the threshold for Official Secrets Act prosecution.
- Secret: this marking is used for information that needs protection against serious threats and that could cause serious harm if compromised – such as threats to life, compromising major crime investigations or harming international relations.
- Official: all routine public sector business, operations and services is treated as OFFICIAL. A limited subset of OFFICIAL information that would have more damaging consequences (for individuals, an organization or government generally) if it were lost, stolen or published in the media is classified OFFICIAL-SENSITIVE.

For organizations that do not have an existing or mandated scheme, such as that above, one example is as follows:

- Restricted: information that, if disclosed to unauthorized individuals, could have a significant impact on an organization's legal or regulatory obligations or on its financial status, customers or franchise and therefore needs to be held on a specific 'need to know' basis.
- Confidential: information about or belonging to customer, employees and corporate businesses that an organization is obligated to protect, for example, by law, internal, internal policy or regulator.
- Internal: information that is commonly shared within an organization is not intended for distribution outside and is not classified as Restricted or Confidential.
- Public: information that is freely available outside of an organization or is intended for public use.

Criticality classification

Similarly, it is important for business continuity and disaster recovery purposes to identify and suitably protect any files, electronic folders, data sets or specific documents containing information that is essential to the running of the organization and that, if the original is lost or destroyed and cannot be replaced, would seriously impair or disrupt normal business, might place the organization in legal or fiscal jeopardy or might jeopardize the rights of citizens.

An example classification scheme for the criticality of information assets is shown below:

Vital: records that are considered crucial such that legal operations could not be continued without them in original form.

Essential: records that are used in day-to-day operations but can be replaced or the information retrieved or reconstructed elsewhere.

Non-essential: all miscellaneous records including available published materials that are generally used for reference and various duplicate and/or convenience copies of records.

Retention and disposal

If the organization has an approved corporate records retention schedule, then this can be incorporated within an IAR, mapped to the business classification scheme and inherited by the assets when they are added.

If not, then it is never too soon to create one in order to ensure that information is kept for the minimum period of

time required, confidential personal information is not kept too long and that defensible disposition is in place.

This article does not focus on how to create a records retention schedule, including deduction of both the time period and triggering date or event or how 'big bucket' you can go, however, some key considerations or principles in determining retention periods are given below.

Principles for determining retention periods:

- Statutory: where a specific retention period is set by a law or regulation for a particular record type;
- Legal evidence: where records are retained to support and evidence contract-related or other legally enforceable rights and obligations, including limitation periods for legal action and enforcement.
- Financial accountability: records documenting financial activity that are required to meet audit and tax requirements and/or to maintain an accurate financial picture over time.
- Internal regulation: keeping records to meet internal audit purposes and/or the implementation of company policy.
- Business need: how long a record is needed by the business to support the performance of current or future work, including longer term informational or research value
- Heritage: where there are enduring cultural and/or historical considerations.
- Data protection: personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes

A one sentence conclusion

If there is explicit, as opposed to tacit, C-level recognition of the value of information, then it need not be the elephant in the room, rather it can be an economic and transformative tiger for any organization!

Declaration of Conflicting Interests

The author(s) declared no potential conflicts of interest with respect to the research, authorship and/or publication of this article.

Funding

The author(s) received no financial support for the research, authorship and/or publication of this article.

References

Jefferson T (1798) *The Writings of Thomas Jefferson* (Edited by Andrew A. Lipscomb and Albert Ellery Bergh. 20 vols.) Washington: Thomas Jefferson Memorial Association, 1905. Available at: (accessed 09 October 2015).

The National Archives (2011) Information asset owners and digital continuity. Available at: http://www.nationalarchives.gov.uk/documents/information-management/information-assets-factsheet.pdf (accessed 09 October 2015).

Wikipedia (2015) Asset management. Available at: https://en.wikipedia.org/wiki/Asset_management (accessed 16th October 2015).

Author biography

Reynold Leming is an experienced information management professional who has worked as an independent consultant since 2000. He has worked in the financial information industry from 1986 to 1995 and then in the document and records management industry from 1995 to present. He is on the Executive board and is the Conference Director of Information and Records Management Society (IRMS), with whom he has also achieved Professional Accreditation. He was also the creator of IRMS Records Retention Wiki. He has wide experience in all aspects of physical and digital records management within private, public and voluntary sectors.