INFORMATION GOVERNANCE: INFORMATION SECURITY AND ACCESS WITHIN A UK CONTEXT

Elizabeth Lomas

Acknowledgements
This article is an expression of my own personal and professional viewpoints but I am enormously indebted to each and every one of the 80 co-researchers in the Continued Communication Research Group for their lively discussions and expertise which have influenced my opinion and expanded my knowledge (www.continuedcommunication.org). I must also thank Dawn Diggines, Sonja Gabriel, Suzie Mereweather and Victor Parry for their expert information security advice and commonsense.

Purpose – *The purpose of this paper is to demonstrate that records management frameworks need to be risk based, flexible and aligned to wider information management objectives. The article outlines some of the changes, challenges and opportunities now and on the horizon for records managers. The article argues that through embedding the international information security standard ISO 27001 in conjunction with the records management standard ISO 15489 holistic information governance strategies will be delivered that are responsive to change.*

Design/methodology/approach – *The paper provides a discussion on the challenges facing records and information management professionals and suggests that ISO 27001 provides some of the systems' solutions lacking from ISO 15489.*

Findings – *The alignment of ISO 27001 to ISO 15489 strengthens the delivery of existing records management systems and its drivers. This is critical to build strong information governance programmes, which enable risks to be assessed in an ever changing information management world.*

Practical implications – *Successful implementation of records management requires alignment with wider information standards and strategies to deliver holistic information management and governance.*

Originality/value – *This research will assist in promoting best practice in records management and information governance.*

Article Type: General Review

Keyword(s):
Records Management, Information Management, ISO 15489, information security; Risk, Standards.

INTRODUCTION

"It is not the strongest of the species that survives, nor the most intelligent, but the one most responsive to change". Charles Darwin

Over the last 20 years records management professionals have had to make a paradigm shift in their roles and responsibilities in order to remain relevant within public and private sector organisations. This shift has involved moving from the physical management of largely paper filing, controlled and appraised at key stages through a records management lifecycle, to managing and valuing electronic records from capture in line with the records continuum model. Within this timeframe records management concepts have gained international recognition through the publication of the international records management standard ISO 15489-parts 1 and 2. (2001) *Information and documentation – records management.* (subsequently referred to within this article as *ISO 15489*). However, records managers are currently moving through another paradigm shift, with larger seismic tremors on the horizon.

Records managers have moved from a world in which they have been able to control and maintain information within an organisation's boundaries (albeit sometimes through server networks spread across the globe) to a world in which individuals may often create organisational records from beyond that organisation's boundaries through Web 2.0 technologies or business applications which are hosted and supported within a third party 'Cloud'. This makes the case for rethinking how information is captured, audited and managed for operational purposes, accountability and use over time. It also raises additional questions about information ownership (e.g. information created and held in Web 2.0 software or the Cloud may not be owned by the creator), information rights legislation (e.g. dispersed information will be impacted upon by wide ranging information rights legislation across the globe with many different permutations) and information reuse (e.g. information gains new value through new uses in its original form and new forms such as mashups and 'linked data' schemes). Within this context many of the key information management questions relate to issues around information value, access, security and risk management over time. It is the contention of this article that information governance solutions and thinking, which balance risks, present many of the practical answers for the development of records and information management systems within the context of current and future challenges. The implementation of the international standard on *Information Security Management Systems Requirements ISO 27001* published in 2005 (subsequently referred to within this article as *ISO 27001*), which devises a governance framework, holds many answers to strengthening records management systems.

ISO 27001 is a more holistic standard than *ISO 15489* focusing on wider information risks that link closely to organisational goals. *ISO 27001* is designed to "provide a model for establishing, implementing, operating, monitoring, reviewing, maintaining and improving an Information Security Management System (ISMS)" (ISO, 2005, p.v.). In particular, its approach marries organisational goals with human factors. The emphasis on the latter is an important part of the standard's focus that is lacking from *ISO 15489* although it has been noted by researchers that culture and human factors are a key requirement if *ISO 15489* is to be successfully implemented (see, for example, McLeod, 2004 and Oliver, 2007). Furthermore, *ISO 27001* has a systems approach built around risk management, which enables information managers to build flexible frameworks for evaluating the appropriate organisational use and impact of new storage and software systems within and outside organisational boundaries based on the nature and cultural context of the organisation. Within the UK context the risks and benefits associated with managing online information are at the forefront of public and business consciences. It is understood that information governance is a critical consideration for any organisation's success.

INFORMATION GOVERNANCE

Information governance is about putting in place information management programmes to ensure that information is controlled to ensure it is 'appropriately' available but that its security is not compromised. Governance also implies that processes are in place to ensure an organisation is able to account for its actions through its records/information. Willis has charted the links between corporate governance and information and records. He proposes that there are six components to information and records management required to deliver corporate governance: transparency, accountability, due process, compliance, meeting statutory and common law requirements, and security of personal and corporate information. (Willis, 2005, p.86-87). A wider definition of corporate governance also deals with authority, stewardship, systems and processes (Willis, 2005, p.87). All of these aspects of information management are embedded into the *ISO 27001* framework, which deals with the balance between access and security. Although it is known as the information security standard it is not intended to stop information access, it deals with establishing information governance systems that ensure information is controlled and made available as appropriate. Information governance requires organisations to take responsibility for their information management. *ISO 27001* provides a framework for information governance and aligns to strengthen *ISO 15489* implementation.

Information security and records managers

Since the dawn of record keeping there have been information losses and data manipulation. Archivists could relate the history of information security developments; the application of wax seals to prevent and detect opening, the development of codes to prevent reading a document and the requirement to maintain copies in case information was tampered with. The Romans had evidence of all these aspects of an information security system. In fact Caesar is credited with developing the first Cipher and Suetonius in the *Lives of the Twelve Caesars* discusses the requirement to copy information to ensure its integrity (Graves, 2007). Tally stick disputes, fake charters and now manipulated digital data could be traced as a strand of diplomatics. Yet few records managers have taken on management responsibility for information security.

In 1998 when the Data Protection Act (Great Britain. Parliament. House of Commons, 1998) was passed as law, many records managers took responsibility for implementing their organisations' data protection policy and practice. As the new legislation encompassed the requirement to manage personal information in paper and electronic records, it presented the opportunity for records managers, within the public and private sectors, to raise the records management profile above the technology driven agenda. However, although the Act required personal information to be kept securely and safely in accordance with the Act's seventh data protection principle, this was not articulated as a key records management driver. Instead records managers tended to focus on the fifth data protection principle that data must be kept no longer than necessary as this provided a further mandate for records management retention schedules.

In the UK's National Health Service (NHS), where patient confidentiality lies at the heart of administrative processes, information governance systems have been developed which encompass concepts of records management, information security, public accountability and legal compliance (Refer to the NHS Governance toolkit and website at http://www.connectingforhealth.nhs.uk/systemsandservices/infogov). However this integration has been slow to filter into records management practices across all sectors. At the UK Records Management Conference in 2009, approximately 70 delegates were asked how many had management responsibility for information security and only two delegates indicated that they held this role (Lomas, 2009). This response was in spite of the fact that in 2007 information security had risen to the top of the information management agenda as a result of a serious information security breach at the HMRC.

The HMRC Case: making the case for information governance and security

In November 2007 UK records managers suddenly woke up to the potential significance of incorporating information security into the records management business case as a news story broke which promoted information security to the top of most UK public sector organisations' administrative agendas. On the 20th November 2007 it was revealed that in October 2007 Her Majesty's Revenue and Customs (HMRC) Child Benefit Office had lost 2 CDs containing the bank account details of 25 million people. At this point the significance of information security for the UK political agenda massively shifted. This was not the first news story reporting public data loss. In the years leading up to this event there were a string of cases connected to information security (See http://news.bbc.co.uk/1/hi/uk/7103911.stm). However the scale and direct impact of the HMRC case, which had the potential to effect c.7.25 million households in the UK, transformed information security from the subject of minor political embarrassment to headline news, provoking a series of major government reviews of government data handling, regulation and legislation.

On 18th October, HMRC's Child Benefit Office (CBO) sent two discs containing the entire child benefit database, to the National Audit Office (NAO) but the disks did not arrive. They were sent by courier from the CBO in Tyne and Wear, unregistered and unencrypted, to the NAO in London. The Police were informed and searches for the disks were carried out on government premises and in several rubbish tips around London but the disks were not located. The disks contained the details of all current and some past child benefit recipients including their names, addresses, dates of birth, National Insurance numbers and in many cases bank details.

Over a month later, on 20th November 2007, Alistair Darling, the UK Chancellor of the Exchequer, issued an emergency statement to Parliament declaring the loss of two disks. (The full statements by Alistair Darling and the Prime Minister Gordon Brown can be viewed at http://news.bbc.co.uk/1/hi/uk/7103911.stm).) In a political context this incident was particularly embarrassing to Gordon Brown not only as the UK Prime Minister but because until the previous May, and for the preceding 10 years, Brown had been the Minister in charge of the Treasury Department with responsibility for integrating the CBO into this administration.

Many people reading this article in the UK will be aware of the impact of this case given that, like myself, they may have been the recipient of a letter explaining the loss of the data and the contact details of a helpline. In fact three years on the disks have never been recovered and nor has there been any evidence that the data has fallen into the wrong hands and been used for unlawful purposes. However the impact of this case has been enormous in the UK and is still very much in the public consciousness. Whenever new initiatives are discussed that involve the processing of large quantities of personal data, or particularly sensitive personal data this case is used to emphasize the risks involved in sharing and processing personal information. This case has impacted upon public perceptions of schemes to share medical data, to initiate a national identity scheme and for airports to undertake body scans. Work by a think tank the Foundation for Information Research Policy highlights the existence of these concerns and issues around large government IT projects and data collection (See http://www.fipr.org/trust.html).

The Government's response to the case was to launch an immediate inquiry into the case led by PWC's Chairman Kieran Poynter. The financial cost of this review was c. £3.6 million (Poynter, 2008, p.95). In addition, the Police's Independent Complaints Commission launched an inquiry (IPCC, 2008) and the Cabinet Office (the lead Department on UK Government security) launched wider reviews. The inquiries revealed that earlier NAO audits of the CBO in 2006 and 2007 had established the provision for the NAO to access data from the Child Benefit Computer System. Although the NAO did not always require access to the full data set it became a routine to download the data every six months for the audit. Consideration was given to extracting parts of the data but the cost was thought to be prohibitive. In fact the cost of data extraction was later proven to have been inflated (Poynter, 2008). In March 2007, two compact discs containing the full data from the system were provided to the National Audit Office to take off site. This set the precedent for the data to go off site. Thus, when in October 2007 the NAO later requested some of the data from the database it was an established process. The subsequent transfer of the discs via TNT was the result of a human error as the discs were posted via this TNT system in the belief that it was a secure and tracked postal system. The TNT did provide a separate tracked system to HMRC that was not used in this instance. In fact when the discs went missing they could not be traced.

The various Reviews concluded that more than 30 HMRC official from across four different departments in the HMRC, as well as a number of NAO personnel played a part in the events that led to the data loss. The Independent Police Complaint Commission concluded that there was no fraudulent or intentional misconduct (IPCC, 2008). Poynter's Review noted that the HMRC was heavily crippled by fragmentation and that information security simply was not the management priority it should have been: "HMRC had an organisational design that was unnecessarily complex and crucially did not focus on management accountability" (Poynter, 2008).

As a result of the data loss the Cabinet Office introduced new processes for handling personal data and in particular large sets of personal data (Cabinet Office, 2008a and 2008b, Cabinet Office and CESG, 2009, and Civil Service, 2008,) However, despite the inquiries that followed in the wake of the HMRC data loss and the new measures that were subsequently introduced there continue to be regular data security breaches in both the public and private sectors. The stories are the subject of heightened public interest and are reported and logged by journalists (See http://news.bbc.co.uk/1/hi/uk/7449927.stm). As a result of these continuing failings, one year on from the HMRC case in November 2008, when an HMRC memory stick that contained passwords to the online tax return website was lost, Gordon Brown made a frank admission that government cannot promise the safety of personal data entrusted by the public and implied that data security breaches were inevitable. Brown stated: "It is important to recognise we cannot promise that every single item of information will always be safe because mistakes are made by human beings. Mistakes are made in the transportation, if you like in the communication, of information." (See The Times Online, Nov 2 2008, Available at http://www.timesonline.co.uk/tol/news/politics/article5065795.ece). This is recognition that new media and the Internet have made it very difficult to balance the access and security requirements but it is a disappointing statement. In fact many of the cases that have occurred are the result of avoidable human errors. If a simple system is put in place with an onus on management and individuals to understand and maintain the system then risks can be significantly reduced. *ISO 27001* provides the mechanisms for this process. Security impacts are likely to continue as a public and operational issue. In order to ensure that information security is kept on the agenda in January 2010 it was announced that new legislation would bring into force increased penalties for data protection offences (ICO, 2010).

ISO 27001

ISO 27001 Framework

Few records managers have taken on management responsibility for information security and yet *ISO 27001* closely aligns and builds on *ISO 15489*. It provides a clear framework for information management that has the potential to explicitly embed the role of the records manager into organisational structures aligned to other colleagues linked to supporting information management objectives, e.g. IT, Facilities Managers, HR etc. Furthermore it fills the gaps within *ISO 15489* to create a holistic information management system scoped to ensure relevance to small, medium and large public and private sector organisations. Information Security Management Systems (ISMS) are built focusing on an organisations' goals, priorities and resources. The implementation of *ISO 27001* encompasses not just records and technology but the human aspects of information management and systems evolution across a whole organisation. People sit at the heart of the process as assets which must be both managed and integrated at all levels into the processes of the ISMS. HR systems for recruiting, vetting and employing individuals must be robust. All personnel must be trained and supported to understand the information management requirements that align to their personal role. The acknowledgement of the critical human role of information systems management is essential to design and maintain a successful and secure information management system. Analysis of many of the key information security failings within both the public and private sector reveal a catalogue of human errors e.g. in the case of lost data disks, memory sticks and laptops linked to individual errors or the cases of bank employees disposing of confidential client information in dustbins. These cases could be rectified and risks minimised with robust information management systems.

ISO 27001 requires the protection of information assets in their broadest form, including knowledge held by individuals. It ties in records management to current organisational drivers whilst still maintaining the links to providing robust evidential and archival records where genuinely required. Many aspects of the ISMS are mirror components of a records management system but are potentially more readily understood by a non-records management audience.

ISO 27001 System Scope

Some of the most effective implementations of an ISO 27001 system are very simple systems. The standard requires than an organisation understands what information assets it holds and then ascertains the value of these assets. This part of the process is critical as one central feature of the standard is that assets can be scoped in or out of the ISMS framework. This means that organisations can focus on directing resources towards protecting and managing their essential information assets. It may be that only one or two information assets then merit further consideration for *IS0 27001* system's management. Organisations are required to establish the scope of where the Standard should be applied. This requirement is embedded into *ISO 27001*'s very early conception.

The history of the development of the *ISO 27001* dates back to commercial initiatives. Its roots lie in the work of a large multinational oil company that developed a security framework designed to protect key commercial information, such as the location of oil fields prior to their registration. The framework developed in this sector set up an approach to information systems management that focused on assigning resources to apply protections to the organisation's most valuable information assets. In 1995 the UK's Department of Trade and Industry took this framework and developed it into a more widely applicable Code of Practice and it was from this that a British Standard on information security management was developed (*BS7799*), which five years later was evolved into an international standard *ISO 17799*, now renamed as *ISO 27001*.

ISO 27001 Certification

Unlike *ISO 15489*, *ISO 27001* has a framework for certification. Certification against the standard enables analysis on take up to be monitored. At the end of 2008 9246 certificates for *ISO 27001* compliance were issued in 82 countries (Nielsen, 2009). Certification against the Standard requires an external audit by a certifying body such as the British Standards Institute (http://www.bsigroup.com/) or Bureau Veritas (http://www.bureauveritas.co.uk/wps/wcm/connect/bv_couk/Local). During an audit the full information security system (against its scope) would be checked and a selection of stated procedures verified. Certification against the *ISO 27001* standard requires an organisation to establish systems of information management which deliver the following components:

- a policy, objectives and activities that reflect business objectives;
- asset classification and control;
- physical and environmental security;
- HR security;
- an approach and framework to implementing, maintaining, monitoring, and improving systems consistent with the organisational culture;
- incident reporting systems;
- systems development and maintenance protocols;
- business continuity management;
- legal compliance frameworks;
- visible support and commitment from all levels of management, including the provision of appropriate funding;
- provision of appropriate awareness, training and education to all managers, employees and other parties to achieve awareness.

A system could fail a certification audit if there were a single major non-conformity or a number of minor non-conformities undermining the system as a whole. Any failure to comply with a legal requirement is deemed to be a major non-conformity and thus the system could not be certified.

As noted, the system may be scoped and built around a small selection of key assets. This does mean that when an organisation presents evidence that it has been certified against the standard it is necessary to ensure which parts of its organisation/assets are within its certification scope.

ISO 27001 Information Asset Registers

The starting point for evolving the ISMS is the information asset register. A records manager taking on the role of developing an information asset register would have probably over 80%

of the data for the register already compiled within records retention schedules. In addition, the knowledge that individuals hold must be captured if it is significantly valuable and the future potential lack of availability of that knowledge presents a risk to organisational processes. In essence, *ISO 27001* links knowledge management concepts (which focuses on human knowledge of organisational value) and records management. Furthermore, any other key components that are part of the delivery of information assets value must be listed, including software suppliers, systems hardware and other non-technological information components.

ISO 27001 framework terminology

The next step of implementing an *ISO27001* system is to risk assess information assets scoped within the system against three key information security requirements. The risk assessment requires evaluation of risks that would compromise an information asset's confidentiality, integrity and availability of information (memorable by the acronym CIA). These definitions have a great deal of synergy with the *ISO 15489* characteristic requirements for a 'good' record of useability, integrity, reliability and authenticity. A central component of *ISO 15489* is to build a records management system whereby 'good records' are created with key characteristics. *Table 1* helps to compare these requirements that sit at the heart of the two standards.

ISO 15489	***ISO 27001***
Useability It should be possible to locate, access, understand and utilize a 'good' record.	**Availability** Information assets should be accessible and useable upon demand by an authorized entity.
Integrity Characteristic that confirms that the record is complete and has not been altered.	**Integrity** The property of safeguarding the accuracy and completeness of assets.
Reliability Characteristic that ensures that the record contents (information) can be confirmed as a dependable, full and accurate representation of the business transactions to which they relate.	
Authenticity Characteristic that ensures the record is: - proven to be what it claims to be; - proven to be created or sent by the person claiming authorship and/or responsibility for transmitting the record; - proven to have been created/and or sent at the time stated.	**Authenticity** The overarching definition of 'information security' within the context of the standard is the: "preservation of confidentiality, integrity and availability of information; in addition, other properties such as authenticity, accountability, non-repudiation, and reliability can also be involved" (2005, p.2). This recognises the additional requirements surrounding the provision of evidence that information is 'authentic' and thus ensuring that the requirement is built into the system development

Confidentiality and access are dealt with in the implementation of the system that ensures ‘integrity’. Section 8.2.3 of *ISO 15489-1* on integrity requires that ‘control measures are in place such as access monitoring, user verification, authorised destruction and security to prevent unauthorized access, destruction, alteration or removal of records’ (2001, p. 9). Additional parts of *ISO 15489* make provision for other aspects of control including auditing, protective labelling, tracking and secure storage,	**Confidentiality** The property that information is not made available or disclosed to unauthorized individuals, entities, or processes.

Table 1: Representation of the synergy between the central terms in ISO 15489 and ISO 27001.

Within the context of *ISO 27001* the system’s development and implementation evolves around balancing the key, and sometimes competing, CIA objectives.

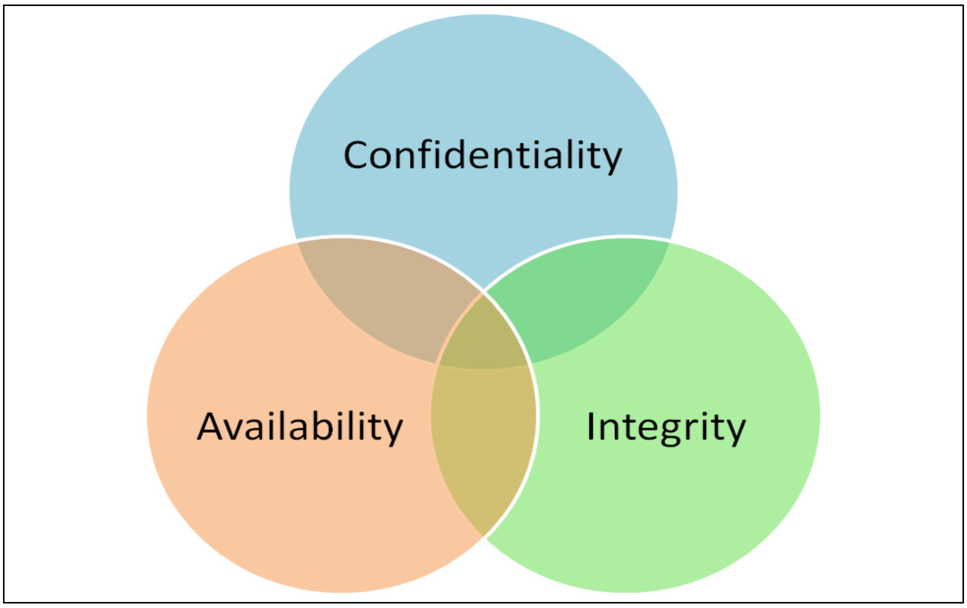

Figure 1: Representation of the information security dimensions that must be assessed and balanced within an ISMS in ISO 27001.

It may be argued that *ISO 27001* requires a more sophisticated and potentially more appropriate approach to information management than *ISO 15489*. It establishes a value for analysing competing organisational requirements, e.g. availability vs. confidentiality. *ISO 15489* lacks the same emphasis on balancing objectives and does not acknowledge the fact that there may indeed be requirements that conflict. Nor does *ISO 15489* have a scoped approach to ascertain where only certain information should be captured and set as ‘good’ records. *ISO 15489* requires that the characteristics of ‘good’ records are developed to underpin and fix information across the records management system. The four characteristics equally interlock.

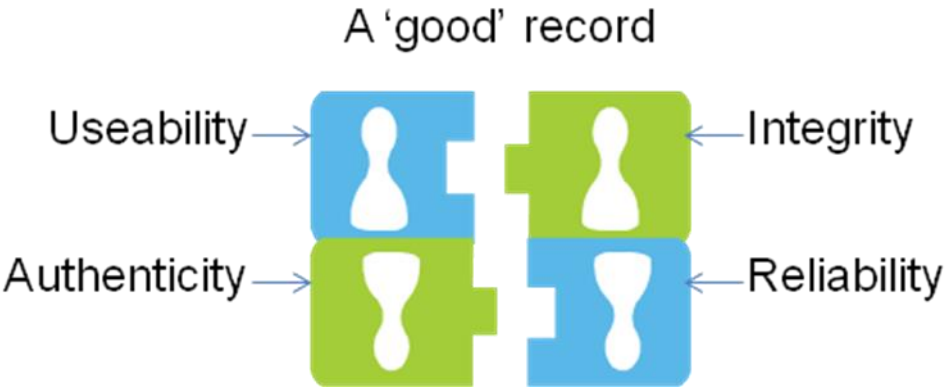

Figure 2: ***Representation of the interlocking dimensions of the characteristics of a 'good' record as defined in ISO 15489.***

However, sometimes the components of a 'good' record do compete in a wider information management context and it is critical to ensure that records managers can have sophisticated systems that acknowledge and enable the evaluation of conflicting demands, e.g. useability vs. integrity and authenticity. An organisation may want certain information to be retained in fluid formats for reuse and other information to be fixed and set to ensure its value as a legal record. A further component of *ISO 27001* that establishes the framework for balancing objectives is its central application of risk processes. A weakness of *ISO 15489* is its limited reliance on risk management strategies, which are a mandatory core requirement within *ISO 27001*. *ISO 15489* does discuss the possibility of establishing a risk framework in order to implement a records management system but the requirement is optional and only minimally covered.

Risk assessment and treatment

Risk assessment and risk frameworks are a mandatory part of the *ISO 27001* framework. The risk methodology requires the development of the information asset register to ensure that the threats and vulnerabilities for each information asset's CIA are identified and documented. It is also important to remember that risk assessment should involve the identification of information opportunities in addition to potential negative consequences from system's failures. For example, the implementation of Google's Gmail means that organisations lose control of their email accounts but equally they lose some of the costs of email storage and Gmail may be a more reliable system than some internal email systems. These factors need to be weighed up and records and information manager should be informing and influencing information creation and storage into new and diversifying arenas.

The overarching risk management process requires the following stages:

- review the organisation's strategic objectives and establish the organisation's risk appetite (the level of risk exposure the organisation will accept);
- risk assessment and risk analysis (including risk identification, description and estimation);
- risk evaluation (business impact analysis);
- risk reporting (threats and opportunities);
- risk decision (tolerate risk, terminate risk, treat risk, transfer risk);
- risk treatment;
- residual risk reporting;
- ongoing monitoring.

The organisation's risk appetite will be critical to evaluating and implementing the appropriate risk approaches. However, although a risk framework is a mandatory part of the standard, the actual risk structure is not prescribed provided that scoped assets are risk assessed for their CIA. The relevance of high, medium and low risk profiles as meaningful measures has increasingly been called into question (Gilb 2005, Brown, Demb and Lomas, 2009 and Hubbard, 2009). In the wake of the 2008 banking crisis risk profiling was shaken to its roots and new models of risk have evolved. In addition there has been a greater emphasis on creating corporate cultures that have a social responsibility when managing risk.

Risk and the records management context

Risk is central to information management processes and needs to be a clear component of any records management framework. The following quote from Karen L. Sampson on records management and risk management is a helpful high level summary of the key requirements for risk evaluation within a records management context: "Risk analysis of records involves defining the records, assigning responsibility for the activities, identifying potential hazards, and analysing and classifying vital records. It is a strategic approach to activity developments that promotes its cost effectiveness. It weighs the cost, benefits, and risks of various record-keeping practices against the relative value of various record groups. It balances the costs of re-creation of records versus protection, and costs of preservations through backup systems or insurance versus the costs of loss prevention through facility modifications. It also balances the costs of recovery against the costs of recreating information lost or total lost of information. Such analysis identifies those practices that will provide the most flexibility within the legal, ethical, and practical constraints." (Sampson, 1992, p.169). These considerations can be seen to fit with process of risk assessing *ISO 27001*'s requirements for assigning information assets' confidentiality, integrity and availability requirements. Sampson's summarises the broad principles of risk in a records management context focusing on the negative aspect of risk. As highlighted by Egbuji it must be remembered that risk is also about identifying new opportunities (Egbuji, 1999). The recognition of information value and new technologies opens up new opportunities for records and information management and risk defines these within existing frameworks and requirements. ARMA has evolved a detailed risk process for evaluating records and information management risks through organisational objectives placing the risks into a framework which enables a cost/benefit analysis (ARMA, 2009). This risk framework could be used as a basis of an *ISO 27001* approach.

To remain employable records managers are faced with a requirement to continually analyse new risks and new opportunities for developing and implementing records and information management systems. The questions that need to be asked in these contexts are often the same but the actions taken may result in different outcomes (new opportunities or negative consequences). For example, new approaches have been developed within the context of records managers appraising and disposing of information. Macro appraisal and NARA's flexible approach to scheduling (commonly termed the 'big bucket' approach) are new ways of dealing with reviewing. Bailey has suggested that there will be new ways of automating selection using approaches developed from search engine links such as Amazon (Bailey, 2009). All of those approaches have the same thinking and questions at their roots but offer new solutions and challenges to selection decisions. Within the context of an online world it is in fact not possible to guarantee information deletion. Once something is effectively 'published' on the Web it may be copied, republished and backed up elsewhere. Tools such as The Wayback Machine (See http://www.archive.org/web/web.php) specifically focus on providing access to past Web pages. Therefore, within the context of the Web, questions about access over time rather than actual guaranteed disposal are more pertinent.

Mat-isa has reviewed records management risks in the context of hybrid records management systems which manage information across record formats (Mat-isa, 2006). Information systems may be hybrid in terms of integrating data across technologies potentially through complex linked data or combining automated and human decision making. One of the great challenges for appraisal and management lies in dealing with distributed data, linked data or dynamic data (Lomas, Shepherd and Stevenson, 2010). As technology changes and their are new ways of working there will be new risks.

Organisations may also have relationships with many outsourced components making information ownership and management increasingly complex. Sanderson predicts that many records managers may be consultants working for multiple organisations (Childs. S. et al, 2008, pp.33-41). As information management becomes layered and multi-dimensional it creates information chains with complex ownership. Information chains can be demonstrated in the production and packaging of food. Ingredient passports are being developed so that the manufacturers can trace the history of each individual ingredient in a food product. Food is tracked from the farm 'gate to plate'. In addition, in Sweden consumers can see new food labels that provide information on a health and environmental impact (Heifer Organisation, 2010, p.7). In this instance labelling, barcodes and RFID (Radio Frequency Identification) technologies make it possible to track and build complex legal pictures and relationships between, people, objects and information. Were there to be an issue surrounding a food product then this information chain takes on new significance and there might be complex permutations in the chain. In this context information management ownership and responsibilities are complicated and as Sanderson has highlighted there might be new attitudes and approaches to work.

Risk management needs to take on board new realities of information creation and thus management. As information is distributed it also needs to deal with the ethics and realities of information value, ownership and placement across legislative regimes. ISO 27001's central focus on frameworks with risk management processes at their very heart will help the future navigation of records and information management programmes.

ISO 27001 Controls and Statement of Applicability

Building on and underpinning the risk assessment process, *ISO 27001* lists 133 controls. The listed controls include policies, procedures, guidelines, practices and organisational structures, which can be of an administrative, technical, management or legal nature. Organisations can also adopt their own additional controls.

Many of the listed controls are part of a records management system. Others assist with areas where records managers must work with other colleagues to ensure the effective management of information in all its forms. The controls establish a holistic ISMS covering the full range of operations that impact upon information management e.g. HR employment, physical security, business continuity etc. The controls also ensure that the system once established is maintained. For example, listed is a 'change management' control. This is the guarantee that all the controls remain up-to-date and relevant and no procedural change that would impact upon the ISMS occurs without due process. This takes into account the development of existing systems and the implementation of new systems. It also tackles changes in workforce locations and legislative regimes. Emphasis is also placed on the design and establishment of information security incident management processes. All information security incidents, including near misses, must be recorded, reviewed, assessed and new processes established as appropriate. It would not necessarily be a security incident in itself that resulted in the ISMS's breakdown but rather failure to address the cause of the incident.

It is a requirement of the standard to create a ‘statement of applicability’. This is defined as a “documented statement describing the control objectives and controls that are relevant and applicable to the organization’s ISMS” (*ISO 27001*, 2005, p.3). Where a control is not selected then it is necessary to justify within the statement of applicability why the system does not require that particular control. This process helps put in place a structure of linked information security responsibilities, e.g. IT will be responsible for firewalls and encryption, HR for vetting, undertakings of confidentiality etc. Whilst individual controls may fall within pre-existing frameworks some will require new partnerships and the programme of reviewing these controls therefore builds an information management framework of responsibilities.

SEISMIC SHIFTS FOR RECORDS AND INFORMATION MANAGEMENT

“The only thing constant in this world is change” Heraclitus c. 500BC

Over the next ten years there will be new questions for records and information managers to ask about whom they are working for, what are the professional and ethical issues surrounding information management and what is the reality of information rights law. The big issues for records managers are:

1. Organisational shifts and work practice changes– who will employ records managers and where?
   As records that are borne digital can be accessed and managed from around the globe, increasingly records management processes may be dispersed or outsourced. Information management work can be allocated to workforces based on numerous considerations, e.g. employment around an organisation’s headquarters, countries with the most attractive information or employment legislation from a financial or operational perspective, the countries with the most ethical or environmental approaches to industry, the locations with the oil and power to run server and online storage, the cheapest, brightest or appropriately skilled workforces.

   Furthermore there will be new styles of working and approaches to business models. Noon and Blyton have charted recent evolutions in employment (Noon and Blyton, 2007). New technology has enabled workforces and business relationships to be established and managed in new ways. Currently only larger businesses and public sector employers have tended to employ records managers. However, small and medium enterprises may start to become a bigger employer of records and information managers as information gains additional value and complexity; provided that records and information managers sell their value and continuing relevance.

2. Technological developments – what are the foreseeable changes that will further impact upon the creation and management of information and records?
   Technology has elevated the place and function of information. Throughout the centuries, each technological advancement in record keeping has resulted in new questions, challenges, ways of working and legislation. The implications of some aspects and requirements around new technologies are only just beginning to be understood. Some studies are starting to promote a model around assessing new technologies. ENISA have conducted a study in this context of the implications for air travel and RFID/The Internet of Things (IoT) technology. For those interested in traditional records management, RFID combines information into a physical object

requiring management. The ENISA study draws up an interesting list of considerations which relate to thinking about the wider context of information systems management and the implementation of individual technologies. However, ENISA stresses the human context that takes priority over technology and ultimately controls its usage: “To fully realise the benefits of the Internet of Things, the challenges and risks that IoT implies must be identified and addressed in a proactive way. These risks do not always have to do with the technology per se but with the way we use it.” (ENISA, 2010).

3. International legislation – as information is created, distributed and held around the globe how will new legislation evolve to underpin its management?
   As the place and purpose of information itself has developed it too has become the subject of law and conflict and legislation acts as the mechanism that has evolved to create the understanding and balance between competing information demands. Within this context, the law continually redefines the relationships between information ownership, information sharing (access and accountability) and confidentiality/privacy rights. Each of these contexts continues to shift across these domains as new technologies impact upon the possibilities for information use and misuse. Information rights law currently differs enormously within different countries. For example, within the USA context e-discovery places a huge information burden to produce information in the event of a law suit. But in the USA it is acceptable to dispose of information in accordance with an approved disposal schedule. Indeed, this was an ultimately accepted defence in the case of Arthur Andersen LLP v. United States, 2005. Although information relating to Andersen’s auditing of Enron was hurriedly shredded, the Supreme Court ultimately accepted that the shredding was in accordance with approved retention schedules despite the fact that there was evidence that the disposal had been initiated only in order to cover up aspects of the Enron audit. In China retention schedules present no defence against the failure to produce information in a legal case as the burden is on providing actual information proof rather than any acceptance of why proof cannot be found. In the light of technological change and distributed information, legislative agendas may shift very quickly driven by the short term goals of global commerce; unless there is a significant large scale movement from the public and/or governments to maintain information balance. However it is to be noted that governments and individuals in different countries do have significantly differing views and expectations on their information. National and international differences need to be mapped, understood and discussed. Within this context records and information professional codes of ethics may further evolve.

In conclusion it is an exciting time to be working in the field of records and information management. The requirements for managing information are constantly shifting but in order to deliver information’s value and meet organisational and societal requirements frameworks need to be evolved to manage information and deal with these shifts. Ethics and legislation underpin all risk management evaluation, professional development and societal balance. Information governance lies at the heart of all records and information management practice and considerable work is required in this area as international legislation evolves.
By mapping ISO 27001 into ISO 15489 and developing a strong information governance framework can be delivered tailored to organisational contexts.

REFERENCES

ARMA (2009) Evaluating and mitigating records and information risks. ARMA.

Bailey, S. (2009) ‘Forget electronic records management, it’s automated records management that we desperately need’, *Records Management Journal*, 19 (2), pp. 91-97.

Bisson, J. and Saint-Germain R. (2005) *The BS 7799/ISO 17799 standard: for a better approach to information security*. Callio. p.19 contains an information security bibliography. Available at https://www.callio.com/files/wp_iso_en.pdf (Accessed: 1 March 2010).

Bisson, J. and Saint-Germain, R. (2005) “The ISO 17799 standard: for a better approach to information security” *Records Management Bulletin* 127, pp.21-23 and 36.

Brown, M., Demb, S. R. and Lomas, E. (2009) ‘Continued communication – maximising the potential of communications: the research and outputs of a co-operative inquiry’, *Proceedings of the Managing Information in the Digital Era Conference*, Botswana October 2009.

BS 10008. (2004) *Code of practice for legal admissibility and evidential weight of information stored electronically*. BSI.

Cabinet Office. (2008a) *Data handling procedures in government: final report*. Cabinet Office. Available at: http://www.cabinetoffice.gov.uk/media/65948/dhr080625.pdf. (Accessed: 1 February 2010).

Cabinet Office. (2008b) *Protecting information in government*. Cabinet Office. Available at: http://www.cabinetoffice.gov.uk/media/328380/protecting-information.pdf. (Accessed: 1 February 2010).

Cabinet Office and CESG. (2009) *HMG information assurance maturity model and assessment framework.* Available at: http://www.cesg.gov.uk/products_services/iacs/iamm/media/iamm-assessment-framework.pdf (Accessed 1 February 2010).

Civil Service. (2008) *Cross government actions: mandatory minimum measures*. Available at: http://www.cabinetoffice.gov.uk/media/cabinetoffice/csia/assets/dhr/cross_gov080625.pdf (Accessed: 1 February 2010). See also Central Sponsor for Information Assurance http://www.cabinetoffice.gov.uk/csia (Accessed: 1 February 2010).

Childs, S, Hardiman, R., Hay-Gibson, N. Lomas, E. and McLeod, J. (ed.) (2008) *Examining the issues and challenges of email and e-communications exploring strategies with experts*, Proceedings of the 2nd Northumbria Witness Seminar Conference, Newcastle-upon-Tyne, 24-25 October.

Dodgson, P. (2010) ‘Information assurance for records managers’, *Records Management Society Conference*, 21-23 March 2010.

Egbuji, Anjel. (1999) ‘Risk management of organisational records’, *Records Management Journal*, 9 (2).

ENISA *Flying 2.0 – enabling automated air travel by identifying and addressing the challenges of IoT and RFID technology.* Available: http://www.enisa.europa.eu/act/rm/emerging-and-future-risk/deliverables/flying-2.0-enabling-automated-air-travel-by-identifying-and-addressing-the-challenges-of-iot-rfid-technology-2 (Accessed 1 February 2010).

European Commission (2007) *On promoting data protection by Privacy Enhancing Technologies.* European Commission, 2008.

European Commission (2008) *Early challenges on the Internet of Things.* European Commission, 2008.

Graves, R. (2007) *Suetonius The Twelve Ceasars*. Penguin Classics, 2007.

Great Britain. Parliament. House of Commons. (1998). *Data Protection Act*. London: The Stationery Office. Available at: http://www.opsi.gov.uk/acts/acts1998/ukpga_19980029_en_1 (Accessed 1 March 2010)

Heifer Organisation. (2010) 'Fat, calories, CO2?', *World Ark*, Spring 2010. Available: http://www.nxtbook.com/nxtbooks/heifer/worldark_2010spring/#/8 (Accessed:14 April 2010).

Humphreys, T. and Plate, A. (2005) *Guide to the implementation and auditing of ISMS controls based on BS ISO 27001*. BSI.

Independent Police Complaints Commission (2008) *Report into missing HMRC data CDs*. IPCC, 2008.

ISO. (2005a) *17799:2005. Information technology – security techniques – code of practice for information security management.* BSI.

ISO (2005b) *27001:2005 BS 7799-2:2005. Information technology – security techniques – information security management systems - requirements.* BSI.

ISO 15489-1. (2001a) *Information and documentation – records management. Part 1: General.* ISO.

ISO/TR 15489-2. (2001b) *Information and documentation – records management. Part 2: Guidelines.* ISO.

ICO. (2010) Press Release: data breaches to incur up to £500,000 penalty. 12th January 2010. Available at: http://www.ico.gov.uk/upload/documents/pressreleases/2010/penalties_guidance_120110.pdf (Accessed: 1 February 2010).

Lomas, E. (2009) 'The synergy of international information standards: aligning records management practice with risk and information security models', *Records Management Society Conference*, 19-21 April 2009.

Lomas, E., Shepherd, J. and Stephenson, K. (2010) ‘Continued Communication: maximising your communications in a Web 2.0 world’, *Records Management Society Conference*, 21-23 March 2010.

Mat-isa, A. (2006) ‘Risk management and managing records’, in Tough, A. and Moss, M. ed. *Record Keeping in a Hybrid Environment*. Chandos House.

McLeod, J. (2004) *Assessing the impact of ISO 15489 in practice: early indications from the UK*. 15th International Congress on Archives, Vienna, Austria, 23-29 August 2004.

The Nielsen Company (2009) *The ISO Survey 2008*. The Nielsen Company. Available at: http://www.iso.org/iso/survey2008.pdf (Accessed, 1 February 2010).

Oliver, G. (2007) ‘ Implementing international standards, first know your organisation’, *Records Management Journal*, 17 (2), pp. 82-93.

Poynter, K. (2008) *Review of information security at HM Revenue and Customs, Final Report.* June 2008. Available at http://www.hm-treasury.gov.uk/media/0/1/poynter_review250608.pdf (Accessed: 1 February 2010).

Sampson. K.L. (1992) *Value added records management: protecting corporate assets, reducing business risks.* Westport, CT.

Willis, A. (2005) ‘Corporate governance and management of information and records’, *Records Management Journal*, 15(2) pp.86-97.