ARKIVUM
ASSURED ARCHIVING

Company Profile

Arkivum's 100% Guarantee

BACKGROUND

There are many threats to long-term data integrity when using IT systems, in particular mass storage technology, but also from the people and processes that surround the use of this technology.

Risk assessment methodologies from both the digital preservation and information security communities provide a rigorous and structured approach to identifying, assessing and managing these risks.

Arkivum has used this risk assessment approach to identify the measures needed to ensure 100% data integrity for our customers. The risks that need to be considered include:

- **Risks of loss of data authenticity and integrity.**
  These risks are mostly concerned with the loss of ability to track and record the origins of data and then everything that is done to data within our archive service. Without this provenance trail, there is the risk that changes to integrity or authenticity can happen, but go unnoticed by us or by our customers.

- **Risks of data destruction or degradation.**
  These risks are concerned with the loss or corruption of both customer data and the information needed by Arkivum to deliver its service. Risks come from imperfect storage technology (media, hardware, software) for example failures or obsolescence, the people involved in managing this technology who may cause deliberate or accidental damage, or unauthorised access by third-parties.

- **Risks to data through loss of services.**
  If there is a loss or interruption to the services and processes that are involved in retention or access to digital content, then this has the potential to put the content itself at risk of loss. For example, this might be the loss of a service that routinely checks and maintains data integrity in a storage system, or loss of access to data that needs to be migrated.

- **Risks to loss of data integrity through mismatch of expectations.**
  If archiving is provided as a service, then there is the potential for a mismatch in expectations or understanding between the providers of the service (Arkivum) and the community for which the services are being provided (Arkivum customers). If the changes in expectations are too fast, or not communicated properly, then data can be put at risk. For example, the required level of data security might not be properly defined, or the sudden need for higher levels of access might be beyond the capabilities of current systems

Data corruption and failure modes exist for all common mass storage technologies, e.g. hard drives and data tape. Software systems, no matter how carefully designed, are not without bugs. Humans are never infallible and can never be guaranteed to make the right decisions 100% of the time.

At Arkivum we take a holistic approach to assessing and managing the risks to our customers' data that come from all fronts. We make no assumption that any part of our infrastructure (people, kit or media) is 100% reliable. We do however have the processes in place to monitor and manage all aspects of our service so we can detect and counter a very wide range of threats to data integrity and can provide a 100% guarantee to our customers with absolute confidence.

OUR RISK ASSESSMENT PROCESS

A useful definition of the term “information security” is provided in the United States Code[1]. Information security is all about protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide:

- **integrity,** which means guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity;
- **confidentiality,** which means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information, and
- **availability,** which means ensuring timely and reliable access to and use of information.

Clearly all of these aspects of information security are applicable to the archiving of file-based assets.

Security standards offer guidelines and general principles for information security management within an organisation. The ISO 27001[2] standard, titled "Information Security Management - Specification With Guidance for Use", is considered as the specification of best practice for an Information Security Management System (ISMS).

The standard defines its 'process approach' as

> *"The application of a system of processes within an organisation, together with the identification and interactions of these processes, and their management".*

It employs the “Plan-Do-Check-Act (PDCA)” model to structure the processes. The ISO 27002[3] standard, formerly known as ISO 17799, is a code of practice for information security. It

[1] http://www.law.cornell.edu/uscode/html/uscode44/usc_sec_44_00003542----000-.html

[2] ISO/IEC 27001:2005, Information technology - Security techniques - Information security management systems – Requirements. http://www.iso.org/iso/catalogue_detail?csnumber=42103

[3] ISO/IEC 27002:2005, Information technology -- Security techniques -- Code of practice for information security management.

outlines hundreds of potential controls and control mechanisms, which may be implemented, in theory, subject to the guidance provided within ISO 27001. This standard established guidelines and general principles for initiating, implementing, maintaining, and improving information security management within an organisation.

The choice of what security measures to implement is driven by risk assessment and here EBIOS[4], MEHARI[5] and OCTAVE[6] are all examples of risk management methods for information security that can be applied. OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation) is a risk-based strategic assessment and planning technique for security proposed by CERT (Computer Emergency Response Team) Coordination Centre [7]. It is self-directed, that is, a small team of people from the operational (or business) units and the IT department work together to address the security needs of the organisation. The team draws on the knowledge of many employees to define the current state of security, identify risks to critical assets, and set a security strategy. OCTAVE Allegro[8] is an OCTAVE variant that focuses on information assets in the context of how they are used, where they are stored, transported and processed and how they are exposed to threats, vulnerabilities and disruptions as a result. This makes it ideally suited to risk assessment for data integrity provided by retention and access services.

Whilst risk management has been long been used in 'mission critical' domains including information security, it is now emerging in the digital preservation domain in the context of trusted repositories.

DRAMBORA (Digital Repository Audit Method Based on Risk Assessment) provides an approach to auditing digital repositories[9] and has been developed through a partnership between the UK Digital Curation Centre[10] and the EU DPE[11] project. Other examples include the TRAC[12] (Trustworthy Repositories Audit & Certification) Criteria and Checklist as developed by the Research Libraries Group (RLG)[13] and the National Archives and Records Administration (NARA)[14] through a joint task force to specifically address digital repository certification and sets criteria to identify digital repositories capable of reliably storing, migrating, and providing access

http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=50297

[4] Expression of Needs and Identification of Security Objectives (EBIOS), http://www.ssi.gouv.fr/en/confidence/ebiospresentation.html

[5] Méthode Harmonisée d'Analyse de Risques, MEHARI 2007 Concepts and Mechanisms, CLUSIF, April 2007 https://www.clusif.asso.fr/fr/production/ouvrages/pdf/MEHARI-2007-concepts_principles_2007.pdf

[6] Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE), http://www.cert.org/octave/

[7] Computer Emergency Response Team (CERT), http://www.cert.org

[8] Richard A. Caralli, James F. Stevens, Lisa R. Young, William R. Wilson. Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process, Technical report, May 2007, http://www.cert.org/archive/pdf/07tr012.pdf

[9] Drambora interactive : http://www.repositoryaudit.eu/

[10] UK Digital Curation Centre (DCC) The DCC provides a national focus for research and development into curation issues and to promote expertise and good practice, both national and international, for the management of all research outputs in digital format. http://www.dcc.ac.uk/

[11] http://www.digitalpreservationeurope.eu/

[12] http://www.crl.edu/PDF/trac.pdf

[13] The RLG is now part of the OCLC see: http://www.oclc.org/programs/default.htm

[14] http://www.archives.gov/

to digital collections. Lead by the CCSDS (Consultative Committee for Space Data Systems)[15] another working group[16] is currently advancing the establishment of an ISO standard on which a full audit and certification of digital repositories can be based. The venture is combining the efforts of TRAC, DRAMBORA, Nestor[17] and ISO/IEC 27001:2005[18] and to standardise the results in the same way as the OAIS Reference Model (ISO 14721)[19].

At Arkivum, we combine the risk assessment methodologies of OCTAVE Allegro and DRAMBORA. This provides a comprehensive and best of breed approach that not only allows us to properly assess and manage the risks to our customer's data, but also sets us in good stead for meeting the relevant parts of ISO standards in this area, both existing e.g. ISO27001 and also emerging, e.g. ISO standards related to trusted repositories and their audit (ISO16363 and ISO16916)[20].

[15] http://public.ccsds.org/default.aspx
[16] http://wiki.digitalrepositoryauditandcertification.org/bin/view/Main/WebHome
[17] Nestor, http://edoc.hu-berlin.de/series/nestor-materialien/8en/PDF/8en.pdf
[18] International Standards Organization, http://www.iso.org
[19] OAIS Blue Book, CCSDS 650.0-B-1, http://public.ccsds.org/publications/archive/650x0b1.pdf
[20] http://wiki.digitalrepositoryauditandcertification.org/bin/view