ADS Information Security Risk Assessment

Title:	Archaeology Data Service Information Security Risk Assessment
Author(s):	Tim Evans
Responsibility of:	ADS Deputy Director, ADS Systems Manager
Derivation:	No derivation
Origination Date:	2nd July 2019
Reviser(s):	Tim Evans (inc. comments from Arthur Clune)
Date of last revision:	8th July 2019
Date of next revision:	1st July 2020
Version:	1.1
Status:	Current version for circulation
Summary of changes:	

Executive Summary

The ADS Information Risk Assessment acts as an actively updated overview and assessment of risks to the technical infrastructure of the Archaeology Data Service and the data held thereon. As such it may also be termed the organisation's policy on information risk management. This document is meant to act as a separate document to the Security Overview and Risk Register documents, which deal with policy, oversight and response to specific issues regarding day-to-day IT security/best practice in regard to local and remote systems, and wider strategic threats respectively. The Risk Assessment is intended to feed into/necessitate updates in these documents where required.

ADS Information Security Risk Assessment

1. Introduction

1.1 Purpose

This document is intended to outline the policy procedure for assessing risks to the ADS Information Security, and then to act as an overarching assessment of all of the risks that may impact specifically upon the ADS technical systems. For the purposes of this document *technical systems* covers the following overarching elements of the ADS:

- Integrity of digital objects stored by the ADS within its Preservation system
- Technical maintenance of local and remote storage devices used by the ADS (both Preservation system and other devices used for stand-alone external applications such as OASIS or Internet Archaeology, or ADS internal applications such)
- Security of all local and remote storage devices, devices and applications used by the ADS

The document is intended to form part of a framework of policies and procedures as part of the ADS Information Security Management System (ISMS), largely based on ISO/IEC 27001:2013 and ISO/IEC 27000:2018 (see Figure 1). This assessment is designed to both act as a point of review of related Policy documents, but also to ensure that any risks and subsequent controls are fed back into the correct document. At most levels this is technical (e.g. safeguards against deterioration of storage media), but also covers governance issues and change management that should feed back into development of the ADS Strategic Plan.

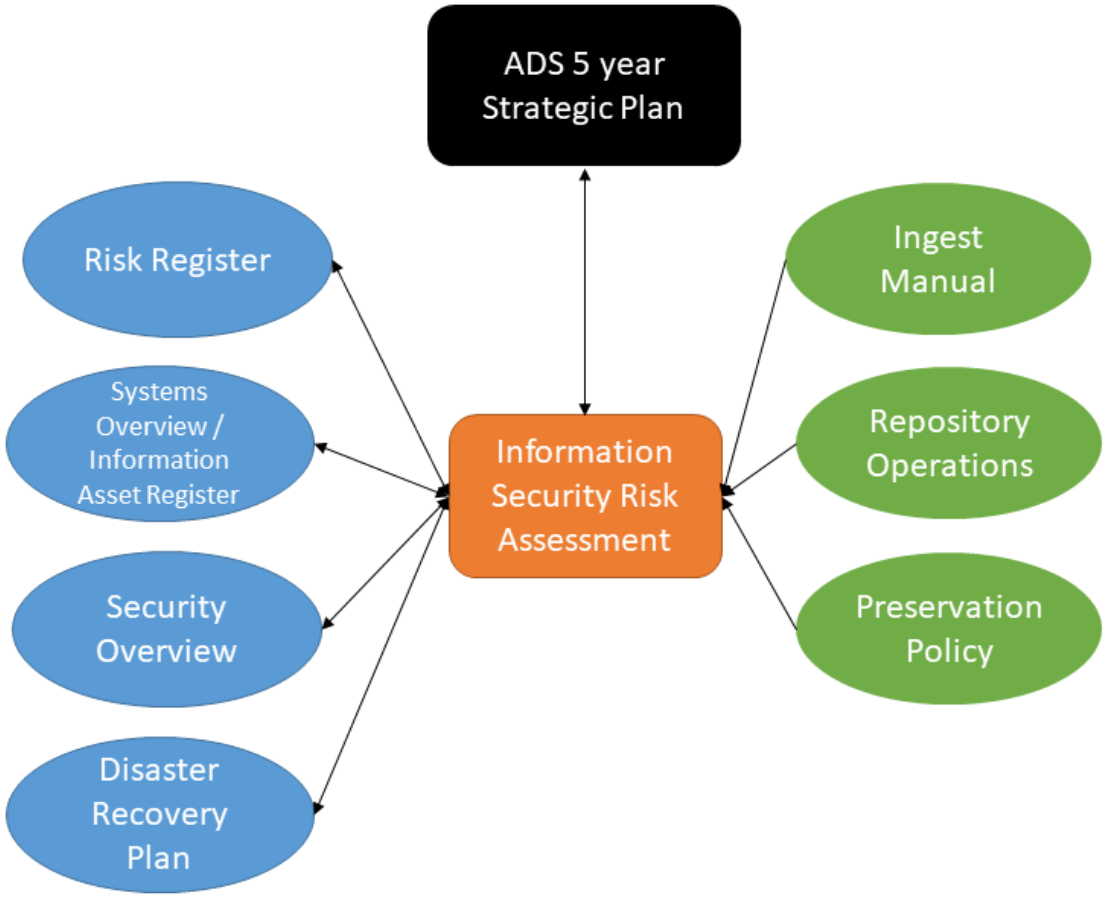

Figure 1: Relationship between this document and other core ADS Policy Documents (available at https://archaeologydataservice.ac.uk/advice/PolicyDocuments.xhtml).

1.2 Objectives of this risk assessment

- To prevent incidents of loss of digital information
- Minimise risk to wider UoY systems
- To improve information risk management generally by documenting practice
- To provide an understanding of risks to, and thereby to allow management to take informed decisions in line with existing Policy and Strategic objectives, on how to mitigate risks
- To provide a risk report which will be used to prioritise actions, tools, services and dependant Policy (for example Security overview)
- To reduce the impact of a major change event, such as loss of personnel

1.3 Scope of this risk assessment

The scope of this risk assessment is primarily on what may be termed ADS systems. As defined in Section 1.1, this includes the various storage media and devices used as part of the internal preservation system (or what may be termed our 'repository'), and the other devices and applications used for internal documentation (for example the ADS wiki), and applications hosted on behalf of external facing projects. This risk assessment also covers the information assets (be they termed files or objects) held by the ADS as part of its digital archive.

The risk assessment is concerned with all levels of risk that may impact upon our systems, this covers overarching governance and business/change management issues and specific technical issues (e.g. storage media) and threats (e.g. hacking)

Inherent risk within the ADS policy of preservation by migration is included here for the sake of completeness, and so that such risk can be evaluated at a higher strategic level Readers should be aware that full definition of the Preservation process is contained in the relevant documentation (see below).

The risk assessment timeframe will consider risks over the entire lifecycle of the information assets held by the ADS.

It should be noted that there is deliberate overlap with the ADS Risk Register, which is concerned with overarching strategic threats to the ADS such as funding. Although some risks will be raised in both documents, it is thought helpful given the specific technical work of the ADS that the risk to systems is considered separately.

1.4 Related Documents

As detailed above, this assessment interfaces with other key ADS policy documents and reporting mechanisms:

- ADS Risk Register
- ADS Preservation Policy
- ADS Repository Operations
- ADS Ingest manual
- ADS Systems Overview (aka Information Asset Register)
- ADS Security Policy
- ADS Disaster Recovery Plan
- ADS Roles and Responsibilities document (internal only)
- ADS Incident Log (internal only, located on ADS wiki)

2. Risk Assessment Process

2.1. Roles and Responsibilities

Role	Responsibilities
Director	General oversight
Deputy Director	Scheduling and implementation of Risk Identification Process. Responsibility of delivering report to higher management and ensuring resources to deliver control are implemented
Systems Manager	Oversight of systems architecture, assets/devices and responsibility for local (ADS) maintenance/backup of devices etc.
Archives Manager	Oversight of information assets held specifically within the ADS repository system; maintainer of Policy documents
Director of Infrastructure and Faculty IT Services	Consultation on best practice and UoY requirements; Responsibility for off-site storage, maintenance of databases

2.2. Risk Model

The approach here has been primarily derived from The National Archives guidance on *Managing Digital Continuity* namely the TNA Risk Assessment Handbook.[1]

Particular elements have also been adapted and simplified, from ISO/IEC 27005:2018 Information technology - Security techniques - Information security risk management (third edition).

2.3. Risk Identification Process

Users	Description
Annual review of incidents	An annual meeting of Deputy Director, Systems Manager and Archives Manager to review ADS Incident Log. Discuss causes of any issues and required control procedures that could be introduced to prevent reoccurrence.
System Characterisation review	Deputy Director and Systems Manager to review list of technology components, locations and users (including access) is up-to-date.
Review documentation + policy	Review the documents listed in Section 1.3
Staff interview	Individual interviews with *all* ADS staff to gauge knowledge of existing policy and best practice, and where documentation can be found.

[1] http://www.nationalarchives.gov.uk/documents/information-management/Risk-Assessment-Handbook.pdf (Accessed 2nd July 2019)

Consultation with ITS	Consultation with UoY ITS Directorate to identify any new or developing risks, how the UoY is responding and best practice/impact for ADS

2.4. Risk Analysis

1) Each risk is assessed for probability and potential impact. The probability is the chance that the risk will occur. The impact is a measure of the consequences if it does occur. This is scored on a scale of 1–5.
2) The probability and impact scores should be multiplied to give an overall risk priority number.
3) The timeframe in which action may be required is assessed – a higher score indicates more immediate action.

The ADS have defined a threshold risk priority score of **15**. Any score above this is one which ADS consider a significant risk, and requires an immediate action (see Critical below). This threshold is based on the ADS Risk Assessment Objectives, primarily any risk that would lead to loss of data from the ADS Repository systems, or pose a Risk to wider UoY systems.

Identified risks are/should be split into the following broad categories:

- *Governance*: Policy documents are fit for purpose; requirements and knowledge are embedded within ADS structures
- *Alignment*: information systems are understood, both in terms of architecture (where are things?), process (how do they work/what do they do?); the technology and resources required to support current use are available, and is agile enough to meet changing requirements.
- *Change*: Business + technological change
- *Information assets*: the stuff we hold basically

Responses are split into the following:

- *Review*: no immediate action is required, but Risk should be reviewed at next scheduled Assessment
- *Action*: some action is required over the forthcoming reporting year
- *Critical*: a critical action is required. This should be scheduled at next ADS Planning meeting with adequate resources.

ADS Information Security Risk Assessment

3. Risk Assessment Results

Item	Risk Area	Risk	Current Controls	Likelihood	Impact	Risk Rating	Response	Notes / further controls
1	Governance	Risk management is not defined or understood across ADS	Clear structure/roles and responsibilities defined Internal support Clear documentation Management aware of current issues	2	4	8	Review	All staff are made aware of current documentation. Raise awareness of channels of communication, procedure Consider scheduling a staff seminar (all levels) to highlight risks and current controls. Introduce post-incident reviews of any incidents (e.g. system compromise or downtime/degraded service). Examine all issues that contributed to the incident.
2	Change	Systems manager leaves	Ring-fenced position Documentation	3	4	12	Review	Criticality of position – and contribution – to effective risk management communicated to Management Board. Another member of staff (Developer) should review

								existing documentation to make sure it is fit for purpose
3	Change	Developer leaves	Ring-fenced position Documentation	3	3	9	Review	Criticality of position – and contribution – to effective risk management communicated to Management Board. Another member of staff (Developer) should review existing documentation to make sure it is fit for purpose
4	Governance	Risk management falls down list of priorities	Annual review is scheduled. Incident log is actively updated and reviewed once month by Deputy Director	1	4	4	Review	Raise awareness at all levels (including ADS Management Board) of how we control Risk, and resources required to do so.
5	Governance	Policy documents are not kept up to date	Policy documents are reviewed and updated annually as a designated Role and Responsibility of the Archives Manager, with support from Directory Director where needed.	2	4	8	Review	Consider moving to a designated block of time where resources (Archives Manager) are available for a full, comprehensive review, with other responsibilities moved to other members of staff.

			Monthly meetings of technical staff to discuss issues that have arisen over a working month should refer back to Policy documents, with updates raised, reviewed and implemented as wider static priority					
6	Alignment	Lack of knowledge about the spread of wired devices and applications hosted by ADS leads to obsolescence/deterioration/security vulnerabilities	Systems manager keeps an active register of *all* devices used by ADS (ADS internal wiki). This feeds into a public facing Systems Overview (or AIR) which is reviewed and updated annually Devices are also monitored by ADS + UoY ITS using internal reporting device system (men+mice).	2	5	10	Review	

7	Alignment	Staff are unaware of ADS business purpose, policy + guidelines (especially during pre- ingest process where files may be sent direct to management), leading to loss of information	Managerial staff (Deputy Director, CDM), should be aware of guidelines on how to record and store information pre-ingest, and how to alert archives manager to need to transition to ingest.	2	5	10	Action	Although best practice is ingrained in curatorial workflow, we should make sure that managerial staff are aware of best practice. Schedule internal seminar.
8	Alignment	Dependency on UoY ITS leads to lack of access to information assets	ADS have full control over file assets stored on local (UoY) devices (primarily NFS), this includes snapshots. ADS also keep their own backups of core service databases. A Service Level Agreement (SLA) exists between UoY and ITS and ADS outlining the specifics of service, response time etc. Issues can be raised	2	5	10	Action	Any request for retrieval of information asset from tape backup is undertaken within UoY ticketing system, so some delay in retrieval is inherent. SLA is due for renewal in Summer 2020. Flag this with UoY ITS at earliest opportunity.

			via email/slack/phone and will be prioritised.					
9	Change	(Lucee) Coldfusion has to be withdrawn	Moving towards Java for many internal/external facing applications (CMS, ADS-EASY, OASIS, ADS Library). Use of custom/bespoke Coldfusion pages has been reduced, with move to either plain XHTML of CFM templates for	2	5	10	Action	Still a risk for many legacy pages Plan for change to feed into next Strategic Plan
10	Change	Withdrawal of UoY licence for Oracle	ADS have started using PostGreSQL for certain applications. ADS databases are centrally managed	2	4	8	Review	
11	Information assets	Manual intervention in databases leads to loss of data	All core databases are now subject to scheduled backup.	3	3	9	Action	This is still happening (in many cases it is unavoidable), and undesirable both for information governance and internal efficiency.

			Data loaders (Java apps) exist for metadata loading Web-based applications (ADS Library) exist for tweaks to data If direct use of SQL is still required, ADS wiki contains clear examples of how code is to be written. Staff are aware that they should escalate difficult functions to Systems team.					Action for management is to prioritise and resource more work on creating data loaders and editors outside of SQL Clients.
12	Information assets	Files are accidentally altered and cannot be recovered.	Access to NFS is limited to specific users, and subject to training and procedures on how tasks should be performed. Regular comparisons of checksums are undertaken every 3	2	4	8	Action	Schedule a test scenario 19/20 to make sure process is fit for purpose.

			months; recovery from local backup; recovery from remote backup are in place See Preservation Policy					
13	Information assets	Update of collection leads to overwrite/loss of data	Preservation Policy stipulates clear procedures for updating collections. AIP checks are in place to ensure that work is quality checked.	1	5	5	Review	
14	Information assets	Dependence on UKDA for off-site storage	This service is covered by an SLA.	2	10	10	Action	Incident did arise in May 2017 where failure of RAID array at UKDA. Incident was picked up and resolved by UKDA within 24 hours. A synchronisation between remote (UKDA) snapshot backup and local (UoY) version was undertaken, with no loss of data recorded. This agreement is now coming to an end; Management to oversee transfer of off-site

								storage to AWS, and removal of version from UKDA.
15	Information assets	Cost of AWS becomes prohibitive	Preliminary costing based on current ADS footprint (see internal report on ADS Wiki) expects an annual cost to be within budget Monthly reports and predictive reports are available through AWS S3 console	2	4	8	Action	Implement a 3 monthly review of AWS costs (to tie in with Quarterly executive).
16	Information assets	AWS does not allow recovery of data	ADS will use Glacier for physical storage of object, and S3 for metadata. This allows comparison of local + remote versions (via metadata) and recovery of data in a few hours	2	5	10	Action	ADS to test a recovery scenario in forthcoming reporting year (19/20).
17	Information assets	Vulnerability is identified in ADS external facing application	All ADS servers are subject to vulnerability scanning, regular automated patching with any	3	5	15	Action	Management to schedule secure development training for Developers

			software subject to requisite planned migration. ADS are now moving towards formal SLAs for externally funded applications, with a view to having a 'shelf life' for specific items, or with resource to facilitate wholesale migration when required.					
18	Information assets	Deterioration of Storage media leads to loss of data	Local (UoY) storage media is subject to best practice: storage arrays are located in dispersed data centres with UPS, fire suppression, generators and alarms. Data is protected by being spread redundantly across multiple disks ("RAID"). Between data	1	5	5	Review	

			centres it is replicated asynchronously, with a maximum data loss of 2 hours. The storage arrays are automatically monitored, with logs and alerts generated that report failed disks, storage capacity warnings and other hardware and software issues. These logs are emailed to several members of the UoY ITS team for immediate action. The UoY ITS use Linear Tape-Open (LTO-6) for 90 day backups. UoY ITS plan to continue to migrate to newer LTO versions (with greater durability and storage					

			capacity) as a matter of course; migrating to newer LTO versions will help to ensure against media deterioration. The LTO media is stored in UPS, fire suppression, alarmed and secured rooms. If a tape error is reported (via a Storage Manager server), the relevant data is migrated to another tape and the tape with the error is removed from circulation. Daily logs are produced by the Storage Manager servers, which alert UoY ITS administrators of any errors or warnings.					

			ADS also have remote storage facility					
19	Information assets	Viruses	UoY ITS run a virus scanner of ADS NFS Files attached to email are subject to virus scanning Files uploaded to external facing applications (ADS EASY, OASIS) are stored on individual VMS and subject to virus scanning Ingest Manual has procedure for virus scanning of all physical media sent to ADS	2	3	6	Review	
21	Information assets	Breach in password security (including phishing)	Passwords for ADS systems are now centrally managed In an encryption based password manager.	2	5	10	Review	

			ADS passwords are subject to a strict policy in order to make them both strong and unique. Access to passwords is restricted on a need to know basis. Passwords are updated at least once a year. Personal (UoY) passwords are subject to the University's policy on password renewal (strong, unique, updated). Staff have to undertake ITS training module on IT security (including phishing)					
22	Information assets	Insider threat (e.g. sysadmin deletes data)	Sysadmin access is restricted, logs of access are kept.	2	5	10	Review	

			All staff are aware of basic best-practice (personal password security, locking computers when away from desk). UoY backups cannot be deleted by ADS Sysdmin					
23	Information assets	Ransomware encrypts data	Key ADS servers are Unix based Desktops are automatically patched Filestore is subject to hourly snapshots	3	4	12	Review	