ARCHAEOLOGY DATA SERVICE

Information Security Risk Assessment

Tim Evans

06/08/2021

archaeologydataservice.ac.uk

Document Control Grid

Title:	Information Security Risk Assessment
File name:	ads_techincal_risk_assessment_v1-4
Location:	/4-2_preservation/techincal_risk_assessment
Status:	LIVE
Version:	1.4
Last updated:	06/08/2021
Created date:	02/07/2019
Review due:	01/02/2022
Authors:	Tim Evans, Paul Young
Maintained by:	Deputy Director
Required Action:	See 3.12

Contents

Glossary

ADS	Archaeology Data Service
AWS	Amazon Web Services
ISO	International Organization for Standardization
ITS	IT Services (University of York)
Metadata	Descriptive information about data
NFS	Network File System
OASIS	The OASIS online form fhttps://oasis.ac.uk
SysAdmin	Systems Administrator
TNA	The National Archives
VM	Virtual machine

1. Introduction

1.1. Purpose of this document

This document outlines the policy and procedure for assessing risks to the ADS Information Security, that is all 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).
- Security of all local and remote storage devices, devices and applications used by the ADS.

The document is an integral part of the framework of policies and procedures that form the ADS Information Security Management System (ISMS), which is largely based on ISO/IEC 27001:2013 and ISO/IEC 27000:2018 (see Figure 1).

The assessment procedure outlined in this document acts as a single pragmatic review that incorporates key points from these other Policy documents and presents a holistic overview of the risks to ADS systems that can clearly be understood by key staff, namely the Systems Manager and Deputy Director.

It is important to note that a key element of this procedure is to ensure that risks and subsequent controls identified are then fed back into the correct Policy. 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.

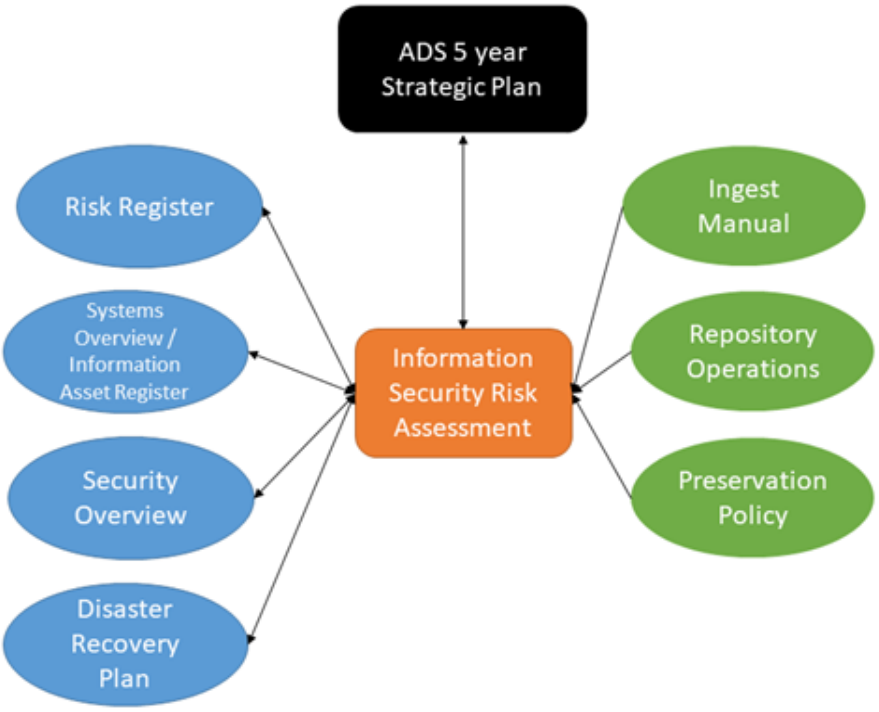

Figure 1: Relationship between this document and other core ADS Policy Documents.

1.2. Objectives of this risk assessment

- To prevent incidents of loss of digital information.
- Minimise risk to wider University of York 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

- Director: General oversight
- Deputy Director: Scheduling and implementation of Risk Identification Process. Responsibility of delivering reports to higher management and ensuring resources to deliver control are implemented. Oversight of information assets held specifically within the ADS repository system, maintainer of Policy documents.
- Systems Manager: Oversight of systems architecture, assets/devices and responsibility for local (ADS) maintenance/backup of devices etc.
- 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.

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

The risk identification process should happen twice a year (normally Spring and Autumn), and consist of the following events.

2.3.1. Biannual review of incidents

A biannual meeting of Deputy Director and Systems Manager to review ADS Incident Log. Discuss causes of any issues and required control procedures that could be introduced to prevent reoccurrence.

2.3.2. System Characterisation review

Deputy Director and Systems Manager to review the list of technology components, locations and users (including access) is up to date.

2.3.3. Review documentation + policy

Review the documents listed in Section 1.3 for any relevant updates that need to be factored into the overall risk assessment.

2.3.4. Staff interview

Individual interviews with all ADS staff to gauge knowledge of existing policy and best practice, and where documentation can be found.

2.3.5. Consultation with ITS

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

2.4. Risk Analysis

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.

The probability and impact scores should be multiplied to give an overall risk priority number.

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 University of York 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 are agile enough to meet changing requirements.
- Change: Business + technological change.
- Information assets: the data we hold.

Responses are split into the following:

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

3. Risk Assessment results

Each risk has been recorded under a subheading.

3.1. Risk management is not defined or understood

Risk Area: Governance

Current Controls:

- Clear structure/roles and responsibilities defined.
- Clear documentation and awareness of documentation amongst all existing staff.
- Risk management is part of new staff induction.
- All Managers are aware of this document and current issues.
- Staff seminar scheduled for each year

Likelihood: 2

Impact: 4

Risk Level: 8

Response: REVIEW

Notes or further controls: Next staff seminar scheduled for October 2022

3.2. Systems manager leaves

Risk Area: Change

Current Controls:

- Ring-fenced position.
- Documentation of all systems is undertaken regularly.
- Key code backed up to ADS GIT repository

Likelihood: 3

Impact: 4

Risk Level: 12

Response: REVIEW

Notes or further controls: Criticality of position – and contribution – to effective risk management communicated to Management Board and University, and any external funders, with a view to keeping this as a core ADS role.

3.3. Application Developer leaves

Risk Area: Change

Current Controls:

- Ring-fenced position.
- Documentation of all systems is undertaken regularly.
- Key code backed up to ADS GIT repository

Likelihood: 3
Impact: 3
Risk Level: 9
Response: REVIEW
Notes or further controls: Criticality of position – and contribution – to effective risk management communicated to Management Board and University, and any external funders, with a view to keeping this as a core ADS role.

3.4. Risk management falls down list of priorities

Risk Area: Governance
Current Controls:

- Biannual review is scheduled (new in version 1-4).
- Incident log is actively updated and reviewed once a month by the Deputy Director.

Likelihood: 2
Impact: 4
Risk Level: 8
Response: REVIEW
Notes or further controls: With increase in staff, consider increasing this risk assessment to quarterly.

3.5. Policy documents are not kept up to date

Risk Area: Governance
Current Controls:

- Policy documents are reviewed and updated (at least) annually as a designated Role and Responsibility of the Directory Director. Oversight of all Policy documents is a part of monthly planning meetings.
- A designated Policy document review schedule is in place on the ADS internal wiki. This provides a link to current and previous versions, review date, and indicates member(s) of staff with responsibility for reviewing.

- Monthly meetings of technical staff to discuss issues that have arisen over a working month should refer back to Policy documents, with issues and updates raised directly with the Deputy Director.

Likelihood: 2
Impact: 4
Risk Level: 8
Response: REVIEW
Notes or further controls: Review and impact of any issues needs to be flagged as early as possible to ensure staff resources are available.

3.6. Obsolescence/deterioration/security vulnerabilities in wired devices and applications hosted by ADS

Risk Area: Alignment
Current Controls:

- 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 an internal reporting device system (men+mice).

Likelihood: 2
Impact: 5
Risk Level: 10
Response: REVIEW
Notes or further controls: No change since last review - have changed the risk name.

3.7. Loss of information during (pre)accession stage

Risk Area: Alignment
Current Controls:

- Managerial staff (Deputy Director, CDM), are aware of guidelines on how to record and store information pre-ingest, and how to alert staff to need to transition to ingest.

Likelihood: 2

Impact: 5
Risk Level: 10
Response: ACTION
Notes or further controls: Flagged at last review. A defined policy on Assessment and Appraisal that also covers how to handle unusual or singular deposits of data outside of the regular deposit/accession process should be written.

3.8. Dependency on ITS leads to lack of access to information assets

Risk Area: Alignment
Current Controls:

- 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 via email/slack/phone and will be prioritised.

Likelihood: 2
Impact: 5
Risk Level: 10
Response: REVIEW
Notes or further controls: No change since last review.

3.9. (Lucee) Coldfusion has to be withdrawn

Risk Area: Change
Current Controls:

- 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.

Likelihood: 2
Impact: 5

Risk Level: 10
Response: ACTION
Notes or further controls: Plan for change to feed into next 5 year Strategic Plan (2021+).

3.10. Withdrawal of UoY licence for Oracle

Risk Area: Change
Current Controls:

- ADS have started using PostGreSQL for certain applications.
- ADS databases are centrally managed, with any move away from Oracle will be clearly signalled by ITS at the opportunity and the impact on ADS factored into the change timetable.
- ADS backup all Oracle databases into non-proprietary format.

Likelihood: 2
Impact: 5
Risk Level: 10
Response: ACTION
Notes or further controls: Plan for gradual change to PostGreSQL to feed into next 5 year Strategic Plan (2021+).

3.11. Manual intervention in databases leads to loss of data

Risk Area: Information assets
Current Controls:

- All core databases are now subject to scheduled backup.
- Web-based applications (CMS, ADS Library) exist for minor edits 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 Manager or Applications Developer in complicated or extreme cases.

Likelihood: 3
Impact: 3
Risk Level: 9

Response: REVIEW
Notes or further controls: No clear incidents recorded in this review.

3.12. Files are accidentally altered and cannot be recovered.

Risk Area: Information assets
Current Controls:

- 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 months; recovery from local backup; recovery from remote backup are in place

Likelihood: 3
Impact: 5
Risk Level: 15
Response: ACTION
Notes or further controls: Incident in July 2021 highlighted improvement in the current checksum procedure to increase issue identification time. This will be to improve the checksum tool within the CMS to perform two tasks:

- A 'Simple Check' that will validate a manifest file path i.e. quickly check that each file within the manifest exists. This would be a frequent fast check (monthly) primarily to identify if files have been deleted or moved (e.g. accidental changes).
- A more robust Fixity Check that will check that both a file exists and that it is unchanged i.e. verify the paths and fixity values in the manifest against the current file store. Due to the time involved in calculating and checking these checksums, this would be a three monthly check in line with current back-up availability.

Manifest details also to be recorded within the relevant section of the AIP.

3.13. Update of collection leads to overwrite/loss of data

Risk Area: Information assets
Current Controls:

- Preservation Policy stipulates clear procedures for updating collections. AIP checks are in place to ensure that work is quality checked.

Likelihood: 1
Impact: 5
Risk Level: 5
Response: REVIEW
Notes or further controls: No change since last review

3.14. AWS for off-site storage proves too expensive

Risk Area: Information assets
Current Controls:

- This service is covered by an SLA with UoY.
- Monthly review of costs in place (Deputy Director)
- ADS can leave AWS at any point. Removal of all data will take a maximum of 48 hours to resolve. Price of removal of data is minimal.

Likelihood: 1
Impact: 5
Risk Level: 5
Response: REVIEW
Notes or further controls: No change since last review.

3.15. Vulnerability is identified in ADS external facing application

Risk Area: Information assets
Current Controls:

- All ADS servers are subject to vulnerability scanning, regular automated patching with any software subject to requisite planned migration.
- ADS have moved to formal SLAs for externally funded applications, with a view to having a 'shelf life' for specific items, or with resources to facilitate wholesale migration when required.

Likelihood: 3
Impact: 5
Risk Level: 15

Response: ACTION
Notes or further controls: Management to schedule secure development training for Developers.

3.16. Deterioration of Storage media leads to loss of data

Risk Area: Information assets
Current Controls:

- 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 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 has a remote storage facility (AWS).

Likelihood: 1
Impact: 5
Risk Level: 5
Response: REVIEW
Notes or further controls: No change since last review.

3.17. Viruses or malware introduced from data deposit

Risk Area: Information assets

Current Controls:

- Virus Scanning is part of procedure in repository operations.
- UoY ITS runs a virus scanner of ADS NFS.
- Files uploaded to external facing applications (ADS EASY, OASIS) are stored on UoY ITS runs and thus subject to virus scanning.
- Files attached to email are subject to virus scanning by ADS staff.
- All ADS staff undertake ITS training for online security and best practice.

Likelihood: 2

Impact: 3

Risk Level: 6

Response: REVIEW

Notes or further controls: No change since last review.

3.18. Breach in password security (including phishing)

Risk Area: Information assets

Current Controls:

- Passwords for ADS systems are now centrally managed in an encryption-based password manager.
- 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 reviewed at least once a year.
- Personal (UoY) passwords are subject to the University's policy on password renewal (strong, unique, updated).
- All ADS staff undertake ITS training for online security and best practice.

Likelihood: 2

Impact: 5

Risk Level: 10

Response: REVIEW

Notes or further controls: No change since last review.

3.19. Insider threat (e.g. sysadmin deletes data)

Risk Area: Information assets

Current Controls:

- Sysadmin access is restricted, logs of access are kept.
- All staff are aware of basic best-practice (personal password security, locking computers when away from desk).
- UoY backups cannot be deleted by ADS sysadmin.

Likelihood: 2

Impact: 5

Risk Level: 10

Response: REVIEW

Notes or further controls: No change since last review.

3.20. Ransomware encrypts data

Risk Area: Information assets

Current Controls:

- Key ADS servers are Unix based.
- Desktops are automatically patched.
- Filestore (NFS) is subject to hourly snapshots

Likelihood: 3

Impact: 4

Risk Level: 12

Response: REVIEW

Notes or further controls: No change since last review.