ERch

Data Audit Framework Scenario Report

Document Details
> Project name: Data Audit Framework
> Work Package:
> Document type: Draft
> Author: Stephen Grace
> Status: Interim
> Version: 0.2
> Issue Date: 16/01/2009

Change history

Date	Version	Description	Author
19/01/2009	0.2	Second draft of Scenario Report	SG

Intended Audience
> This document is written for use by the DAFD project team in evaluating the online audit tool

Introduction

This scenario plan is designed to inform the Data Audit Framework Development (DAFD) team about potential enhancements to the online audit tool developed at HATII as part of the DAFD project. It is based on the experience of using the tool during the audit of a department at King's College London (the Centre for Computing in the Humanities, or CCH), and in the expectation that data audit and the Data Audit Framework will be of wide application in organisations such as research-intensive universities.

The tool is designed to implement the DAFD methodology, and so excluded from this scenario testing is any consideration of the methodology itself.

1 Scenario

"Auditing a department using the online DAFD tool"

King's College London (King's) is a large research-intensive university with a distributed management culture in nine Schools together with a central Professional Services directorate. Beyond the current pilot phase, data audit may not be based in a single department like the Centre for e-Research (CeRch) – itself part of the Information Services and Systems department. It may be dispersed in the separate Schools, based in another part of Professional Services or come under the remit of a senior officer like the Vice-Principal (Research and Innovation). As such those managing the audit process and/or the online tool's administration will need fine-grained control of the system.

2. Roles

The online tool is designed to be used by one auditor, with the option to record other auditors involved in aspects of the work. These 'Other Auditors' are chosen from the list of those already set up with user permissions. In the scenario, it is thought that different roles would be played by the actors, with more closely defined contributions to the audit work – and accordingly, with tailored permission in the tool.

Senior Auditor: can undertake all stages of audit; can allocate permissions for stages or sections to others; can authorise or sign off the work of other auditors at section, stage or audit level; can over-ride, amend or add comments to the work of others until the audit is signed off. There may be more than one Senior Auditor in an organisation; can create and amend classification schema used in different audits.

Auditor: can undertake all stages of audit (or all those assigned by a Senior Auditor); can sign-off own work if policy/permission allows; can create and amend classification schema used in different audits.

Trainee Auditor: can undertake sections, stages or audits assigned to them by the Senior Auditor; can only proceed through stages if sign-off is given.

System Administrator: can create, configure and remove user rights for an organisation under the direction of a Senior Auditor; can create and amend classification schema used in different audits.

3. Stage One (Planning the Audit)

The auditor gathers evidence at this stage, often from printed or online sources such as websites and annual reports. It would be useful to upload documents (where available electronically) in order to have a complete record, in case the judgement of the auditor is questioned or the process is investigated or reviewed at a later date. This provides an audit trail of evidence. Websites may disappear or be amended, and documents may go missing, so attaching any electronic content to the audit will offer access to the evidence.

If a team of auditors is active in an institution, it might help to set up the administration of the auditors in advance. This would be a task for the System Administrator, who may be a separate person in a large organisation or the Senior Auditor. Also, an Auditor may delegate audit tasks to others within an audit and require rights to view and amend others' work (and then lock each entry to prevent rollback or further amendment). Some of the PI-DAF projects are using doctoral students to undertake at least some of the audit, and these students could have defined rights to contribute to the online tool.

There would need to be a clear distinction in the tool when different auditors undertake different tasks, so each element would need to be traced to its creator. A change history for each element would again show evidence of the audit process (perhaps for validation by Internal Audit departments or by external specialists). A senior auditor might want to append a comment on an audit or any element of it, without changing the original text. If a new auditor is training on the job, their manager as senior auditor may wish to approve each of the four stages – either by sanctioning each stage before the next can be started, or just as a record of accepting the work

If auditors are used from outside the organisation and that organisation manages access to the tool, access rights need to be granted to use the system. These auditors must not be able to see other audits (which may be undertaken by their competitors). In highly specialised areas, such as considering the obsolescence risk of different file formats, an expert may be contracted for just a small part of the data audit process; they could be enabled to contribute through the online tool.

4. Stage 2 (Identifying and classifying assets)

The auditor may wish to upload a spreadsheet of data for the assets or questionnaire sections of Stage 2, or Audit Form 2, for the resources under audit: this will save the auditor's time and allow them to use familiar tools (e.g. Microsoft Excel), or populate the form by automated software (using a data source such as an AHRC webpage detailing project funding, or an inhouse Current Research Information System). This will need standard design, or at least guidance to those creating spreadsheets of the worksheet structure.

An auditor may wish to amend or establish a classification scheme at the end of Stage 2.

Since the auditor may gather some of the data in the next stage of the audit, the ability to upload Audit Form 3 data would also be useful.

5. Stage 3 (Assessing management of data assets)

As with Stage 2, it is useful to upload data from a spreadsheet (such as a version of Audit Form 3) in Stage 3. The auditor may also want to make use of a characterisation tool such as JHOVE to identity and validate files, and the information reported may be usefully copied into the online tool.

In the Rights & Restrictions field, the auditor may wish to upload a document like a data management plan or contract, or include a URL (such as referencing a Creative Commons licence) as well as give a description. This will help managers and curators of digital resources, and provide data auditors with evidence over time of the context for sharing data.

An auditor may wish to amend the classification level or even revise the classification scheme at this stage of the audit, and the online tool should enable this. It is quite possible that trends in the resources under consideration will suggest a different way of classifying the assets.

6. Stage 4 (Reporting and recommendations)

Data audit is expected to be an ongoing process for universities managing research assets. As such, there will be the need to review an audit and any action taken in response to its recommendations. It would help if documents could be uploaded to the audit tool that relate this subsequent work. A mechanism for setting review dates would help the Senior Auditor gain an overview of projected work.

More generally, the tool could be used to manage audits by establishing programmes of new work, setting review dates and recording actions taken to manage risks identified in the audits.

At a more basic level, it should be possible to upload a secondary document like a corrigendum to the final report, when some information is not available at the time of the audit, or where the auditor misinterpreted data.

7. Conclusion

The online tool offers auditors a consistent way to follow the DAFD methodology, to document the audit stages and generate reports to management. It could be enhanced to enable the administration of a data audit programme in a given institution by

- adding more control over user rights management
- offering a place to upload and store more documentation
- incorporating review mechanisms, such as a log of action taken or setting review dates.