UK Statistics Authority

UK Statistics Authority
Digital Economy Act 2017 Processor Accreditation Guidance

October 2024

Contents.

1. Introduction

The Digital Economy Act 2017 (DEA) facilitates the linking and sharing of datasets held by public authorities for accredited research for the public good.

The Act provides a requirement that organisations wishing to become processors or obtain personally identifiable data and then link, match, or process this, must be accredited to ensure that their security environment, controls, and processes are satisfactory to protect data.

Under the DEA the UKSA is the statutory accreditor of processors, researchers, and projects. To oversee this role, the National Statistician has appointed a Research Accreditation Panel (RAP), with an independent chair and members, representatives of Government Departments, the Devolved Authorities and United Kingdom Research and Innovation (UKRI).

This document provides a guide to the accreditation process for processors under the DEA. The UKSA has designed the approach based on industry standards to enable organisations to meet the accreditation requirements but then provide for regular reviews so that the accreditation is maintained at the correct level.

2. Accreditation options

Under the DEA, there are two types of processor accreditation that apply, depending upon how organisations prefer to operate (scope of accreditation):

- Preparation of data – the ability to receive data for matching, linking and de-identification;
- Provision of data – the storing and provision of de-identified data.

An organisation can be accredited for both if required so they can store data but also link, match and deidentify data.

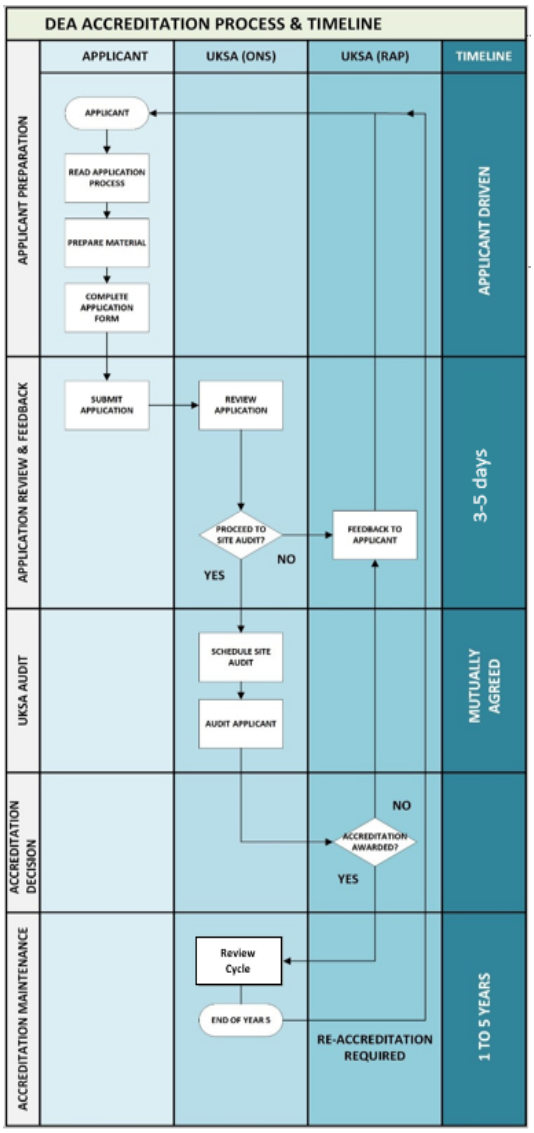
Applications to obtain accreditation can be submitted at any time. Note that applicants cannot process data under the DEA unless they are accredited. Once obtained, this accreditation covers processing activity that an applicant performs under the DEA for the period of the accreditation granted.

Ongoing reviews of the applicant will be performed at scheduled intervals when a significant incident is reported or when significant changes have been made within the applicant's systems.

Mechanisms for the UKSA to suspend or withdraw accreditation are identified within the DEA Research Code of Practice and Accreditation Criteria. Applicants should be aware of these conditions.

3. Accreditation Coordination, Process & Timeline

3.1 Application Coordination



UKSA have a coordination team to support applicants though the process of applying and ongoing in life support for accredited organisations. All correspondence in relation to DEA applications and in life support should e-mail - Research.Accreditation@statistics.gov.uk.

Application Process & Timeline

This workflow illustrates an *ideal* timeline that is a projected best-case scenario where the applicant has a fully completed evidence pack and an audit of the applicant, including an on-site visit. An applicant should factor this into their submission and plan for relevant staff to be available within this time period.

The accreditation process can be considered as being made up of two areas of assessment:

- Security
- Capability

3.2 The Security assessment

The security assessment is based on the ISO/IEC 27000 Information Security Management standard to provide a high-level baseline for organisations to indicate their level of implemented security. Additional elements have been added to this that reflect requirements specific to the DEA Code of Practice. This approach has been selected because of its wider coverage of security including governance, risk management, personnel in addition to standard technical areas.

The security assessment incorporates the key security areas required for accreditation. Where possible this links to UK Government resources such as NCSC and CPNI, to help organisations better understand the available best practice and advice in the areas of the required security control.

Applicants should populate the assessment with their security control information for the relevant areas and provide the appropriate documentation to support the statements made, such as plans, policies, risk assessments, privacy impact assessments, reviews etc.

For applicants whose organisation has an existing, valid ISO 27000 certification, this can be taken into account as part of the assessment performed by UKSA but cannot be used as a waiver for the security element of accreditation. This is due to the varied nature of an organisation's ISO 27000 management system scope and how this aligns to the requirements of the DEA accreditation requirements. An applicant is still required to submit a completed DEA assessment, but it is expected that the evidence for this is easier to collate and present to UKSA from the ISO 27000 management system implemented.

3.3 Capability assessment

The capability assessment considers the skills, experience, service delivery and practices in place to demonstrate the organisation can perform the functions of a processor. The assessment for capability is not based on any current standard so, although it contains control references, these do not refer to anything outside the DEA requirements. The processor's capability will be measured and assessed against the accrediting body's data capability control and maturity assessment frameworks.

UKSA assessment staff will arrange for a first on-site review of the applicant's implementation based on the information they have supplied. Follow up audits and reviews of the implemented will also be arranged as a requirement for maintaining accreditation.

3.4 What an Applicant Needs to Do

Applicants need to complete three sections of the assessment.

- **Applicant Details** – basic information about the organisation including the security point of contact and the address(es) from where the data activity takes place;
- **Applicant Security Controls** – the implementation of an applicant's security controls and the evidence that exists to demonstrate this.

- **Applicant Capability Controls** - the implementation of an applicant's capability controls and the evidence that exists to demonstrate this. This is in a separate spreadsheet.

Where a security control is not relevant to the context of the organisation or if a data capability control is optional and has not been fulfilled, an applicant should indicate this as **Not Applicable** and N/A respectively, with the specific reason this is the case.

There is no distinction on the Applicant Security Controls sheet for the type of application being made – that is, preparation of date, provision of data, or both. All controls need to be addressed regardless of the type of application. The Applicant Capability Controls has its own dedicated applicant spreadsheet for applicant's to complete and non-applicable controls are annotated accordingly based on accreditation scope (preparation, provision, or both).

Applicants should place particular emphasis on their controls where personal data is being processed or hosted, such as any particular handling instructions for data of this sensitivity or personnel screening implemented.

See Annex A for an outline of how to structure the security evidence submission. **It is important that the evidence pack is appropriately structured to aid the review.**

In the experience of the assessors, key items that have delayed assessments in terms of data security include:

- **Security control evidence** – some applicants submit evidence in relation to demonstrating a specific security control but the associated commentary does not specifically state where in that evidence.
  Assessors have spent significant time trying to match up the specific evidence to the specific control. This slows the initial assessment view and feedback to the applicant.
- **Application evidence** – this needs to be collated as per Annex A in this guidance and match the requirements for the 'DEA_Evidence_Pack.zip'. Evidence that is not collated in the standard structure will be returned to the applicant and not progressed at that stage. This avoids significant time to match up the specific evidence to the specific control.
- **Security control commentary** – this needs to be specific against each accreditation requirement within each security control. On occasion some applicant's commentary is not specific against the accreditation requirement and is more generic.
  Applications that do not hold commentary against each accreditation requirement will not be assessed and returned to the applicant.
- **Application owner** – a single point of contact is required within the applicant's organisation to coordinate the assessment. On occasion some applicants expand communications to other members within their organisation, which makes communication a challenge and potentially slows down information exchanges.

The Applicant is expected to fill in the dedicated DEA capability evidence spreadsheet and reference evidence to demonstrate implementation and capability of data controls set out in

the data capability framework. In addition, there is guidance to direct how this evidence is structured and collated when sent to the accrediting body. Each control evidence will go through a maturity assessment by an assessor and will give the control a maturity opinion. Each control is assessed and given a level of maturity: Minimal, Partial, Capable, Maturing and Mature. Based on this, all controls will contribute to the overall weighting which will determine the total maturity of the applicant's data capability controls.

4. Applicant Assessment

The assessment of an applicant's submission is a three-stage process:

1. A review of the application and supporting pack of documentary evidence such as policies, processes, reports etc. Where sufficient evidence has not been provided, or no evidence exists for applicable controls then the assessment will proceed to stage 3.
2. Arrangements made for the on-site audit to validate the assertions made in the submission, if this is deemed necessary by the assessor.

   Applicants should factor in the ideal timescale (as indicated in the flowchart in Section 2) and ensure that they have the staff and systems available within the site visit period.

   For the on-site audit, UKSA will expect:

   - A tour of the site's physical, computing and business facilities;
   - To interview staff about operations related to DEA use of data;
   - To review records / evidence that demonstrates that the applicant has applied the controls and are operating correctly and that the organisation has the capability to perform the relevant functions (e.g. staff skills and experience, relevant policies and procedures).
3. After an assessment is made and it is deemed that the processor may be accredited a presentation of the assessment to the RAP who will decide on the application. Accredited data processors would also need to sign a declaration and they will be included within a UKSA publicly available register containing all accredited organisations

5. Data provider access to accreditation evidence

Organisations accredited to the DEA have undergone a rigorous, evidence-based assessment of their control processes that has been reviewed by the RAP as part of their accreditation deliberations. Accreditation from RAP indicates that the control processes operated by an applicant have been independently assured for research data.

An accredited organisation can request data from data providers for their approved research. In some cases, a data provider may seek further assurance for the control areas assessed. In these cases it is appropriate for the Assessment report and control assessment to be shared with the data provider. This sets out the assessed maturity of the

accredited organisation together with assessment spreadsheet detailing each control area. If requested, the UKSA will liaise directly with the data provider and accredited processor to ensure the appropriate information is provided.

In rare cases a data provider may request to review the detail of the organisation's evidence pack. Given the sensitive nature of the information held about the accredited organisation this requires the approval of RAP and a separate process to enable access to the evidence.

To request this access:

1. The data provider submits a request to RAP for access to an accredited organisation's evidence pack, together with a business case for this.
2. RAP review the business case and make a decision. Where this is approved:
    - The UKSA coordination team contact the accredited organisation and data provider to obtain suitable dates for an on-site visit – this could be on the provider or organisation site.
    - The UKSA assessment team attend the site, with a representative from the accredited organisation and presents the evidence associated with the assessment.

The organisation's evidence pack will be retained by UKSA and not passed to a data provider.

6. Accreditation Review

Under the DEA an accreditation is valid for up to five years from the date of award subject to routine accreditation reviews (full accreditation review). Security will be reviewed annually whereas data capability review frequency will be based on the accredited processor's level of maturity to enable for ongoing maintenance of the accreditation (regular accreditation review). It is recognised that elements of an organisation's services, systems and processes might change or mature through the accreditation period prompting the need for ad hoc reviews.

In relation to data capability controls the UKSA needs information and evidence to ensure processors demonstrate secure and robust data capability procedures. If an applicant's evidence does not meet the maturity standard of at least "capable" the applicant will not receive accreditation. Furthermore, if the applicant fails to provide evidence for a mandatory control, they will not be accredited.

For security controls the regular review ensures that all control areas are reviewed at least once across the lifespan of the accreditation.

For capability controls the regular review initially focuses on capability controls identified as being Capable (Level 3) or Maturing (Level 4), any improvement actions identified at the point of accreditation and any changes to the services, systems and processes performed during the time they are accredited. If an accredited processor is assessed as "Capable" in

maturity they will have a review every year, “Maturing” every two years and “Mature” every three years.

Over the five-year period the reviews will sequentially cover all security and capability controls to measure progress towards Mature. As stated previously, the timing of reviews differs between security and capability controls with the former having annual reviews and the latter having the frequency of review based of their assessed maturity level.

We also recognise that new organisations or organisations undergoing significant change would find it difficult to be fully accredited. For this purpose, we introduce the concept of provisional accreditation for data capability. This would allow organisations to be assessed on evidence they can currently provide and any future plans to attain a provisional capable organisation status. Any review will ensure that all data security controls are in place at the time of audit and data capability controls critical to safeguarding data confidentiality and data management are sufficiently evidenced. However, there might be some evidence gaps regarding data capability as monitoring systems are tested in a new operating model e.g., no management information is consistently produced.

In addition to the evidence review, we expect that RAP will request the following evidence from data processors:

1. justify why they require to use the Digital Economy Act legal gateway at this stage, and
2. determine when they will be able (within a six-months period) to provide evidence for a full accreditation review.

Further information relating to this, and the data capability controls can be found on the Data Capability Guidance.

The review process is:

1. Six weeks before the accreditation anniversary, the organisation is contacted by the Secretariat to provide dates for a regular review.
2. UKSA Security and Capability teams confirm availability and agree a date for a review with the organisation. A high-level schedule of the review content is provided to the organisation at this point. This content is based on the sequential schedule of controls review and any specific items from previous reviews or organisation changes.
3. Two weeks before the review date, the organisation provides a documented summary of any accreditation and process changes performed during the year, together with their progress on control improvements.
4. If required, the UKSA team visits the organisation, either physically or virtually upon agreement, and:
    - Performs a refresh tour of the site’s physical, computing and business facilities;

- Meets with staff to discuss the capability and security control operations in scope conducted over the year;
- Reviews those controls that require particular focus; and
- Reviews evidence that supports the continuing operation of controls and steps towards a Mature state.

5. The UKSA team summarises the annual review in a short report for the Research Accreditation Panel.
6. The Panel discusses the findings and highlights items as necessary for further action and follow up. Where the review has identified shortcomings in operations that weaken security and/or capability controls, RAP are able to determine sanctions including suspension of research under the DEA, temporary suspension of accreditation or withdrawal of accreditation.

Note that at any point during the five-year accreditation period, any significant change to an organisation's systems or processes may require an element of reaccreditation. In these instances, the organisation should contact the UKSA coordination team for advice.

Displaying the maturity opinion grading

As part of the accreditation review, data processors will be presented with two assessment gradings - one for the security accreditation and one for the data capability accreditation (maturity assessment opinion). For accredited data processors the security grading can be capable or mature, while the data capability rating can be capable, maturing, or mature.

Accredited data processors must

- present both gradings separately even if these are at the same level (e.g., mature), and
- include the disclaimer text provided below against the data capability rating

We also encourage data processors to display the functions they provide along with the data capability maturity rating.

Disclaimer text

The final maturity assessment opinion of the data processors is estimated as a weighted average of the data capability accreditation controls. This is an evaluation of the maturity of the data processing environment based on the evidence provided to assessors at this time. As accredited data processors might deliver various services and functions as part of their accreditation under the Digital Economy Act 2017, this opinion must not be used on its own to compare intrinsically different data processing environments.

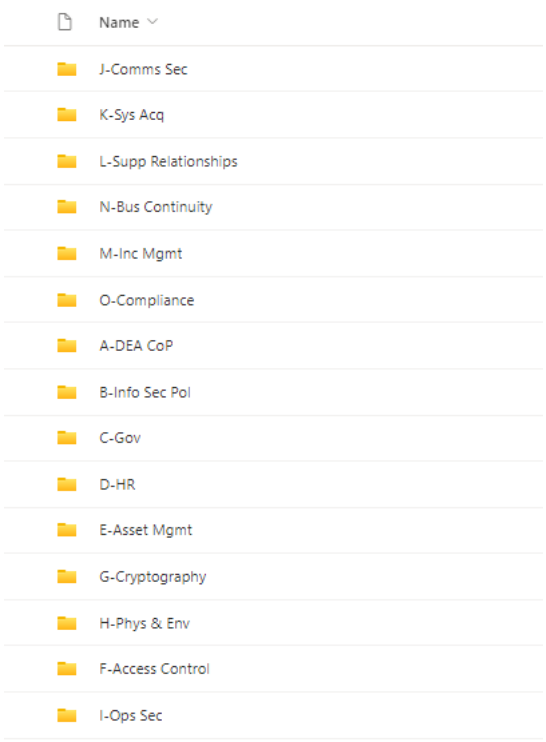
Annex A. Security Evidence File Structure

For submitting evidence for your accreditation audit, please follow the outlined file structure.

1. Top level file for each Control Category
2. Separate second level files within each Control Category for each individual control.

Please ensure each second level file contains all relevant evidence documents for that control. If a piece of evidence is relevant to multiple controls, please put it in every relevant folder.

The top level file structure should resemble:



And the second level file structure should appear as: