



UK Statistics Authority Digital Economy Act 2017 Processor Accreditation Guidance

September 2022



Contents.

1. Introduction	2
2. Accreditation options	2
3. Accreditation Coordination, Process & Timeline	3
3.1 Application Coordination	3
3.2 The Security assessment	4
3.4 Capability assessment	4
3.5 What an Applicant Needs to Do	4
4. Applicant Assessment	5
5. Data provider access to accreditation evidence	6
6. Accreditation Review	6
Annex A. Using the security assessment form	9
A.2 Applicant Security Controls	10
A.4 Detailed example around the right level of response and evidence	11
A.4.1 Example 1	12
A.4.2 Example 2	12
A.4.3 Example 3	13
Annex B. Compilation of security evidence packs	14
Annex C. Frequently Asked Questions	16

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, 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.

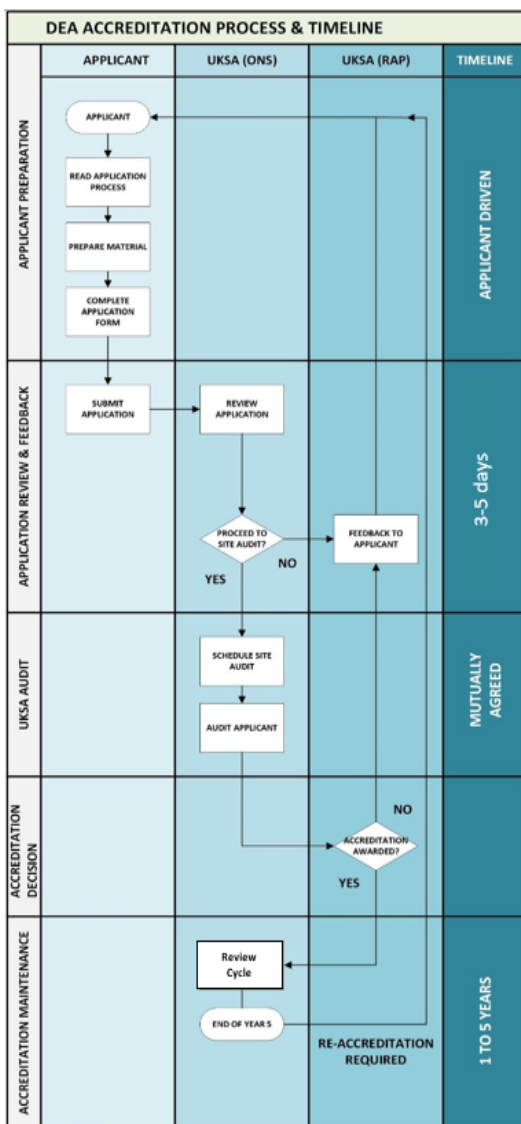
Applications to obtain accreditation can be submitted at any time. Note that applicants cannot process data under the DEA unless they are accredited. Once obtained, this accreditation covers processing activity that an applicant performs under the DEA for the period of the accreditation granted.

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 through 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 security controls and the evidence that exists to demonstrate this.
Note – DEA Code of Practice the processor must agree to publish and maintain appropriate data policies – the existence of these policies and that they are publicly available will be checked during the assessment process.
- **Applicant Capability Controls** - the implementation of an applicant capability controls and the evidence that exists to demonstrate this. This is in a separate spreadsheet.

Where a security control is not a specific requirement 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 tab for the type of application being made – that is, process, host 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 examples of how to complete the application form, assessment and to prepare the evidence pack for streamlined review. **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 B 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. The Secretariat will contact the applicant and highlight these areas for further investigation during the site visit. 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. 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 Research Accreditation Panel who will make a decision 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 Research Accreditation Panel 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 capability 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 initially focuses on the security controls that were identified as being Capable (Level 3) at the point of accreditation and any changes to the services, systems and processes performed during the time they are accredited.

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. 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. Using the security assessment form

The DEA Accreditation Spreadsheet has tabs as follows:

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

A Word version of the spreadsheet is available for the security and capability control for organisations that prefer this to Excel.

A.1 Applicant Details

	A	B	C	D
1				
2				
3				
4				
5				
6				
7		DEA Security Accreditation Application		
8				
9		Applicant information		
10		Applicant Name:		
11		Organisation:		
12		Organisation Address:		
13		E-mail Address:		
14		Telephone Contact:		
15				
16		Lead Security Contact Name:		
17		E-mail Address:		
18		Telephone Contact:		
19				
20		Application type		
21		Processor	<i>Yes / No (delete as appropriate)</i>	
22		Hosting	<i>Yes / No (delete as appropriate)</i>	
23		<i>Applicants can accredit for both processing and hosting</i>		
24				
25		Systems summary		
		<i>Provide a high-level overview of the systems, physical locations and services provided that are in scope of this accreditation exercise.</i>		

The equivalent form and guidance for data capability can be found at

A.2 Applicant Security Controls

A	B	C	D	E	F	G	H
Control Category	Control	Accreditation Requirement	Applicant Response	Reference evidence document name or no. against each control point	Links to resources related to control	Accreditation Scheme Title (UKCA Use Only)	Commentary - scope of improvement required / evidence (UKCA Use Only)
DEA Research Code of Practice	An applicant must be a fit and proper person to be involved in processing before they can be accredited as a processor.	Provide evidence to confirm they have sufficient skills, experience, technical infrastructure and policies in place to demonstrate they are fit and proper person. Demonstrate a record of appropriate compliance with UK law, in particular laws relevant to processing activities and the use of data.	<p>Please provide commentaries under each of the following headings to address the accreditation requirements:</p> <p>Sufficient Skills</p> <p>Experience</p> <p>Policies</p> <p>Appropriate legal compliance</p> <p>Security Strategy & Framework</p>	<p>Please provide the document with the required details structure that are being processed as evidence. Where applicable comment not relevant to the specific control in question please indicate the page and/or section which is relevant.</p> <p>Sufficient Skills 3-CoPI</p> <p>Experience 3-CoPI</p> <p>Policies 3-CoPI</p> <p>Appropriate legal compliance 3-CoPI</p> <p>Security Strategy & Framework 3-CoPI</p>	DEA Code of Practice		
DEA Research Code of Practice	Applicants are legally accountable for the work they carry out under the legislation. Only processors based in the UK are eligible for accreditation.	Provide a guarantee that all processing is performed within the UK and evidence that this is the case.	<p>Please provide commentaries under each of the following headings to address the accreditation requirements:</p> <p>Statement on UK processing</p>	<p>Please provide the document with the required details structure that are being processed as evidence. Where applicable comment not relevant to the specific control in question please indicate the page and/or section which is relevant.</p> <p>Statement on UK processing 4-CoPI</p>	DEA Code of Practice		
DEA Research Code of Practice	The Research Code of Practice and Accreditation Criteria requires the processor to have policies defined in key areas: secure environments, major incident protocol, de-identifying data, data confidentiality, breach/loss, data retention and destruction, data confidentiality breaches documented and maintained throughout the period for which the applicant wishes to remain accredited. These do not need to be standalone single policies but must be clearly identified within the organisation's policy framework.	Confirm and evidence the organisation policies are in place and approved by the appropriate senior management providing a copy of the policies, location and review.	<p>Please provide commentaries under each of the following headings to address the accreditation requirements:</p> <p>Secure Environments Policy</p> <p>Major Incident Protocol</p> <p>De-identifying Data</p> <p>Data Retention & Destruction</p> <p>Data Confidentiality Breaches</p>	<p>Please provide the document with the required details structure that are being processed as evidence. Where applicable comment not relevant to the specific control in question please indicate the page and/or section which is relevant.</p> <p>Secure Environments Policy 5-CoPI</p> <p>Major Incident Protocol 5-CoPI</p> <p>De-identifying Data 5-CoPI</p> <p>Data Retention & Destruction 5-CoPI</p>	DEA Code of Practice		
Information security policies	Policies for information security shall be defined, approved by management, published and communicated to employees and relevant external parties. These policies will be reviewed at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	Confirm and evidence the organisation policies are in place and approved by the appropriate senior management providing a copy of the policies, location and review.	<p>Please provide commentaries under each of the following headings to address the accreditation requirements:</p> <p>Policy Governance</p> <p>Security Policies & Guidance</p>	<p>Please provide the document with the required details structure that are being processed as evidence. Where applicable comment not relevant to the specific control in question please indicate the page and/or section which is relevant.</p> <p>Policy Governance 6-SP1</p>	https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/460006/Information_Security_Policies_and_Guidance.pdf https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/460006/Information_Security_Policies_and_Guidance.pdf https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/460006/Information_Security_Policies_and_Guidance.pdf		

Examples of responses covering exactly what is required are as follows:

Control Category	Control	Accreditation Requirement	Applicant Response	Reference evidence document name or no. against each control point
Physical and environmental security	Security perimeters shall be defined and used to protect processing facilities that contain sensitive information, with appropriate entry controls. This incorporates: <ul style="list-style-type: none"> Physical security for offices, rooms and facilities has access controls applied at key points such as processing rooms, research rooms, loading areas and other points where unauthorised persons could enter the premises; Prior authorisation is required to take either equipment, information or software offsite with appropriate security controls applied to offsite assets; Equipment containing storage media is verified to ensure sensitive data is removed prior to disposal or re-use; Users ensure that unattended equipment has appropriate protection; A clear desk policy operates for papers and removable storage media. 	Confirm and evidence that physical security measures are implemented for the organisation's premises, including those where data processing or hosting is performed. Provide copies of relevant documentation such as plans, policies, procedures, assessments etc.	<p>ONS has a dedicated Physical Security Manager who oversees physical security requirements across the four ONS sites supported by a range of policies and processes, outlined.</p> <p>The role incorporates security management of ONS facilities department, linking into the facilities manager to ensure coverage of all third party suppliers and related security contractual requirements.</p> <p>The role liaises with resident site occupiers such as the Intellectual Property Office (IPO) and charity commission to ensure ONS security controls are incorporated across sites.</p> <p>Physical Security - access controls Policy and guidance in place plus a number of related user guidance.</p> <p>Penetration Testing Each of the four ONS sites are pen tested annually by a 3rd party, with remediation plans in place.</p> <p>Remote Access Policy and Guidance in place</p> <p>Hardware - data removal prior to disposal or reuse 3rd party provider in place covering data removal; disposal and transportation. Service description, ISO27001 cert and recent disposal cert provided.</p> <p>Security of unattended equipment Policy and guidance in place</p> <p>Clear Desk Policy</p>	<p>Physical Security - access controls 12-Phy/Physical Security Policy & Guidance 12-Phy/Counter Terrorism Guidance 12-Phy/Management of Visitors Guidance 12-Phy/Foreign Visitor Security Clearance template 12-Phy/Physical Security measures change management guidance 12-Phy/Statutory Authorities Guidance 12-Phy/Suspect Package Bomb Threat Response Guidance 12-Phy/Vehicle and Person Search Guidance</p> <p>Penetration Testing 12-Phy/SOR PU-19-0089 Physical Penetration Testing V0.2 12-Phy/ONS Drummond Gate Report (example)</p> <p>Remote Access 12-Phy/Mobile Device Policy and Guidance</p> <p>Hardware - data removal prior to disposal or reuse 12-Phy/SupplierX ISO27001 Cert 2018-2021 12-Phy/SupplierX Process Chart 2016 12-Phy/SupplierX Service Framework Agreement 2019 12-Phy/SupplierX - Certificate Certificate of Disposal (example)</p> <p>Security of unattended equipment 12-Phy/ICT Policy and Guidance</p> <p>Clear Desk Policy 12-Phy/Clear Desk Policy & Guidance</p>

An example of a response not providing the detail required is as follows:

Accreditation Requirement	Applicant Response
<p>Confirm that there is a policy in place covering all aspects of the UKSA provided sample secure environments policy.</p> <p>Provide a copy of the policy and detail where in the pack this is to be found here.</p>	Confirmed

This is not addressing the requirement to *Provide a copy of the policy and detail where in the pack this is to be found here.*

A.4 Detailed example around the right level of response and evidence

Let us take the following security control to work through:

Control Category	Control	Accreditation Requirement
Organisation of information security	<p>All information security responsibilities shall be defined and allocated. This incorporates:</p> <ul style="list-style-type: none"> • Segregation of duties where conflicts are identified; • Appropriate contact with authorities is maintained; • Appropriate contact with special interest groups and forums is maintained; • Information assurance is maintained within project management, regardless of the type of project; • A mobile device and teleworking policy is in place to manage associated risks. 	<p>Confirm and evidence that security responsibilities are defined and understood with consideration for segregation, authority, group contact arrangements and assurance approach. Provide copies of relevant documentation</p>
		<p>such as plans, policies, procedures, assessments etc.</p>

The Applicant Response column is pre-structured by the control areas for the respondent:

Please provide commentary under each of the following headings to address the accreditation requirement.

Segregation of duties

Appropriate contact with authorities

Appropriate contact with special interest groups

Information assurance is maintained within project management

Mobile device and teleworking policy

Let us consider responses to the **Segregation of duties** control.

A.4.1 Example 1

A.4.1.1 Applicant response

<p><i>Please provide commentary under each of the following headings to address the accreditation requirement.</i></p> <p>Segregation of duties Segregation of duties is covered within the IT Security Policy</p> <p>Appropriate contact with authorities</p>	<p><i>Please provide the filenames within the stipulated directory structure that are being presented as evidence. Where a file contains content not relevant to the specific control in question please indicate the page and/or section which is relevant.</i></p> <p>Segregation of duties 7-Org/IT Security Policy.pdf</p>
--	---

A.4.1.2 Assessment

The IT Security Policy document provided may be a length document; it may or may not be searchable and the terms used within the document may not be as per the terms used by the assessment and therefore scanned or searched for by an assessor.

The assessor does not have time to go through documents in entirety looking for what may be relevant to the control.

The improvement here is to specify exactly where the relevant information can be located within the provided document/s.

A.4.2 Example 2

A.4.2.1 Applicant response

<p><i>Please provide commentary under each of the following headings to address the accreditation requirement.</i></p> <p>Segregation of duties Segregation of duties is addressed in policy by section 2.4.1 of the IT Security Policy. The considerations around segregation of duties across the Active Directory estate are covered by Section 7 - Role and Responsibilities of the Active Directory project design document - PROJECT-0016-Design.docx The organisation maintains some break-glass accounts for several systems for use in emergency situations. These are powerful accounts that do not adhere to the policy. As such risk assessments were performed around these - as per RiskAssessment0055.pdf.</p>	<p><i>Please provide the filenames within the stipulated directory structure that are being presented as evidence. Where a file contains content not relevant to the specific control in question please indicate the page and/or section which is relevant.</i></p> <p>Segregation of duties 7-Org/IT Security Policy.pdf 7-Org/PROJECT-0016-Design.docx 7-Org/RiskAssessment0055.pdf</p>
--	---

A.4.2.2 Assessment

This addresses the problem of knowing where to looking within a document for the pertinent information. It also demonstrates that items specified in policy are being considered within projects by the reference – and inclusion in evidence pack – of a specific project which has addressed the policy items.

Furthermore, where an exceptional situation has arisen within the organisation, it has been explicitly recognised and risk assessed showing maturity and good record keeping.

What remains to be seen in some form is the implementation of duty segregation in live operation. An improvement would be for this to be evidenced – as per Example 3.

A.4.3 Example 3

A.4.3.1 Applicant response

<p><i>Please provide commentary under each of the following headings to address the accreditation requirement.</i></p> <p>Segregation of duties Segregation of duties is addressed in policy by section 2.4.1 of the IT Security Policy. The consideration around segregation of duties across the Active Directory estate are covered by Section – Roles and Responsibilities of the Active Directory project design document – PROJECT-0016-Design.docx. The organisation maintains some break-glass accounts for several systems for use in emergency situations. These are powerful accounts that do not adhere to the policy. As such, risk assessments were performed around there – as per RiskAssessment0055.pdf. The joiners, movers and leavers process has been included (JML Process.docx). Section 3 states that group memberships have to be specified by the line manager. Helpdesk screenshot PRIV shows a request for a privileged new user. The corresponding AD screenshot PRIV shows the current membership in Active Directory. Helpdesk screenshot REG shows a request for a regular user within the software development team of the organisation. the corresponding AD screenshot REG shows the current membership in Active Directory.</p>	<p><i>Please provide the filenames within the stipulated directory structure that are being presented as evidence. Where a file contains content not relevant to the specific control in question please indicate the page and/or section which is relevant.</i></p> <p>Segregation of duties 7-Org/IT Security Policy.pdf 7-Org/PROJECT-0016-Design.docx 7-Org/RiskAssessment0055.pdf 7-Org/JML Process.docx 7-Org/Helpdesk screenshot PRIV.jpg 7-Org/AD screenshot PRIV.jpg 7-Org/Helpdesk screenshot REG.jpg 7-Org/AD screenshot REG.jpg</p>
--	--

A.4.3.2 Assessment

Evidence of the implementation of segregation of duties has been provided in the form of regular user vs privileged user in both the requesting helpdesk requests and the resultant group membership. Additionally, the joiners, leavers and movers process has been provided.

This provides a comprehensive coverage of this control:

- Policy
- Process (result of a policy requirement)
- Policy consideration within a project (evidence of policy consideration)
- Risk assessment due to non-compliance with policy (evidence of policy consideration)
- Evidence of different users' permissions (evidence of policy consideration and adherence to the process)

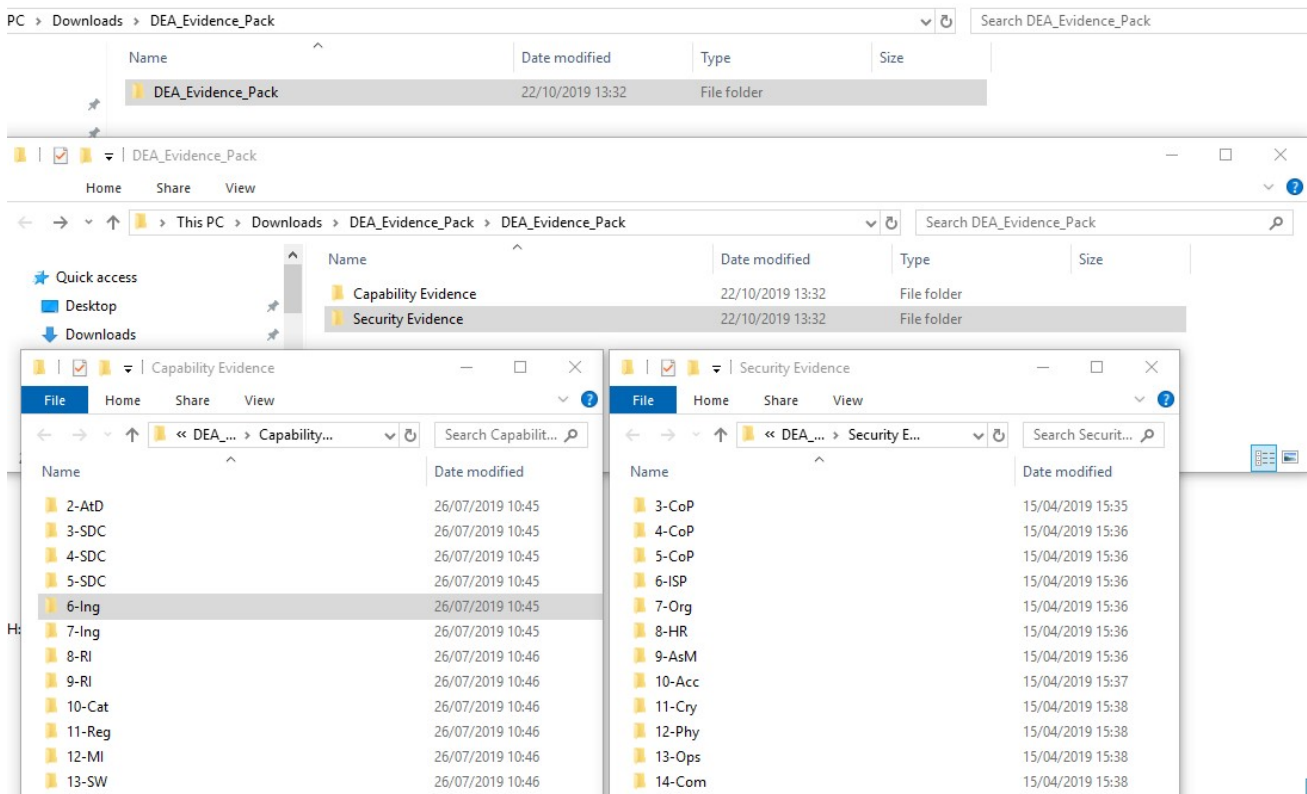
Annex B. Compilation of security evidence packs

A pack of all evidence should be collated, indexed, and provided to UKSA as part of the application. This should cover all aspects of the control requirements indicated for security and capability.

Detailed checks will be performed by the UKSA assessors to ensure the evidence exists and it matches the statements made for each control.

A zip archive file – “DEA_Evidence_Pack.zip” – will have been provided to you as part of the application process. This archive expands out to be an empty directory structure to be populated with evidence for both the security and capability parts of the accreditation.

The extracted archive file looks as follows:



This shows:

- The first level has only a single directory named “DEA_Evidence_Pack” (top window in screenshot)
- The second level has two directories: “Capability Evidence” and “Security Evidence”. This maps to the two main tabs of the accreditation spreadsheet (middle window in screenshot)
- The third levels have many directories that map to the Excel rows of the Capability and Security tabs respectively (the windows at the bottom of the screenshot)

The directories are named starting with a number that corresponds to the row on the spreadsheet tab for which corresponding evidence must be placed. The diagram on the following page depicts this using the Security tab.

The directories for the data capability assessment are named starting with a number that corresponds to the relevant control for which corresponding evidence must be placed please refer to the Data Capability application guidance for further detail.

The reference evidence columns have only a single line of evidence pre-populated under each category heading. However, as per the completed example given in section 4, it is expected that in most cases you will have multiple pieces of evidence to present under each category heading. You are free to list as many relevant pieces of evidence under each heading as is appropriate.

When the directory structure is populated and the evidence pack completed, please zip up the entire pack and send back to the UKSA via the MoveIT secure transfer system.

The image shows a screenshot of an Excel spreadsheet with columns for 'Central Category', 'Central Point', 'Accreditation Requirement', 'Applicant Response', and 'Reference evidence document name or no. against each central point'. To the right, a file explorer window shows a directory structure for 'DEA_Security_Controls_Evidence'. Arrows point from specific evidence files in the file explorer to the 'Applicant Response' column in the spreadsheet, illustrating how evidence is mapped to requirements.

Central Category	Central Point	Accreditation Requirement	Applicant Response	Reference evidence document name or no. against each central point
DEA Research Code of Practice	An applicant must be a 'fit and proper person' to be involved in processing before they can be accredited as a processor.	Provide evidence to confirm they have sufficient skills, experience, technical infrastructure and policies in place to demonstrate they are a fit and proper person. Demonstrate a record of appropriate compliance with UK laws, in particular laws relevant to processing activities and the use of data.	<p><i>Please provide commentary under each of the following headings to address the accreditation requirement:</i></p> <ul style="list-style-type: none"> Sufficient Skills Experience Policies Appropriate legal compliance Security Strategy & Framework 	<p><i>Please provide the filename within the specified directory structure that are being commented on in evidence. Where a file contains content not relevant to the specific central point in question please include the year and file version which is relevant.</i></p> <ul style="list-style-type: none"> Sufficient Skills 3-CoP Experience 3-CoP Policies 3-CoP Appropriate legal compliance 3-CoP Security Strategy & Framework 3-CoP
DEA Research Code of Practice	Applicants are legally accountable for the work they carry out under the legislation. Only processors based in the UK are eligible for accreditation.	Provide a guarantee that all processing is performed within the UK and evidence that this is the case.	<p><i>Please provide commentary under each of the following headings to address the accreditation requirement:</i></p> <ul style="list-style-type: none"> Statement on UK processing 	<p><i>Please provide the filename within the specified directory structure that are being commented on in evidence. Where a file contains content not relevant to the specific central point in question please include the year and file version which is relevant.</i></p> <ul style="list-style-type: none"> Statement on UK processing 4-CoP
DEA Research Code of Practice	The Research Code of Practice and Accreditation Criteria requires the processor to have policies defined in key areas: secure environments; major incident protocol; de-identifying data; data confidentiality breaches; data retention and destruction; data confidentiality breaches documented and contained and mitigate the processor for which the applicant wishes to remain accredited. These do not need to be standalone single policies but must be clearly identified within the organisation's policy framework.	Confirm and evidence the organisation policies are in place and approved by the appropriate senior management providing a copy of the policies, location and review.	<p><i>Please provide commentary under each of the following headings to address the accreditation requirement:</i></p> <ul style="list-style-type: none"> Secure Environment Policy Major Incident Protocol De-identifying Data Data Retention & Destruction Data Confidentiality Research 	<p><i>Please provide the filename within the specified directory structure that are being commented on in evidence. Where a file contains content not relevant to the specific central point in question please include the year and file version which is relevant.</i></p> <ul style="list-style-type: none"> Secure Environment Policy 5-CoP Major Incident Protocol 5-CoP De-identifying Data 5-CoP Data Retention & Destruction 5-CoP Data Confidentiality Research

Excel row 3 – evidence should be placed in the corresponding directory "3-CoP"

Excel row 4 – evidence should be placed in the corresponding directory "4-CoP"

Annex C. Frequently Asked Questions

Our organisation holds ISO 27001 certification, do we need to undertake the security part of the assessments?

Yes. Your certification should stand you in good stead for the security aspect of the DEA assessment. However, the assessment is evidence based, so whilst you will very likely have all the expected policies in place and appropriate content within, the assessment will quickly home in on the evidence the organisation has that proves that policy is being adhered to.

What is the cost of the assessment?

There is no cost associated with any part of the assessment. The initial assessment, annual reviews and subsequent assessments following expiry attract no direct cost. However, you should expect that a non-trivial amount of time has to be put into the application and review.

How long does accreditation last?

Accreditation lasts five years, but there are annual security reviews and reviews for data capability based on processor's maturity level within this period.

Who can I contact for more information?

Please address queries to the following address Research.Accreditation@statistics.gov.uk