UK Statistics Authority
Digital Economy Act Processor Accreditation Guidance

March 2021

Contents.

1. Introduction

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

- 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 de-identify 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.

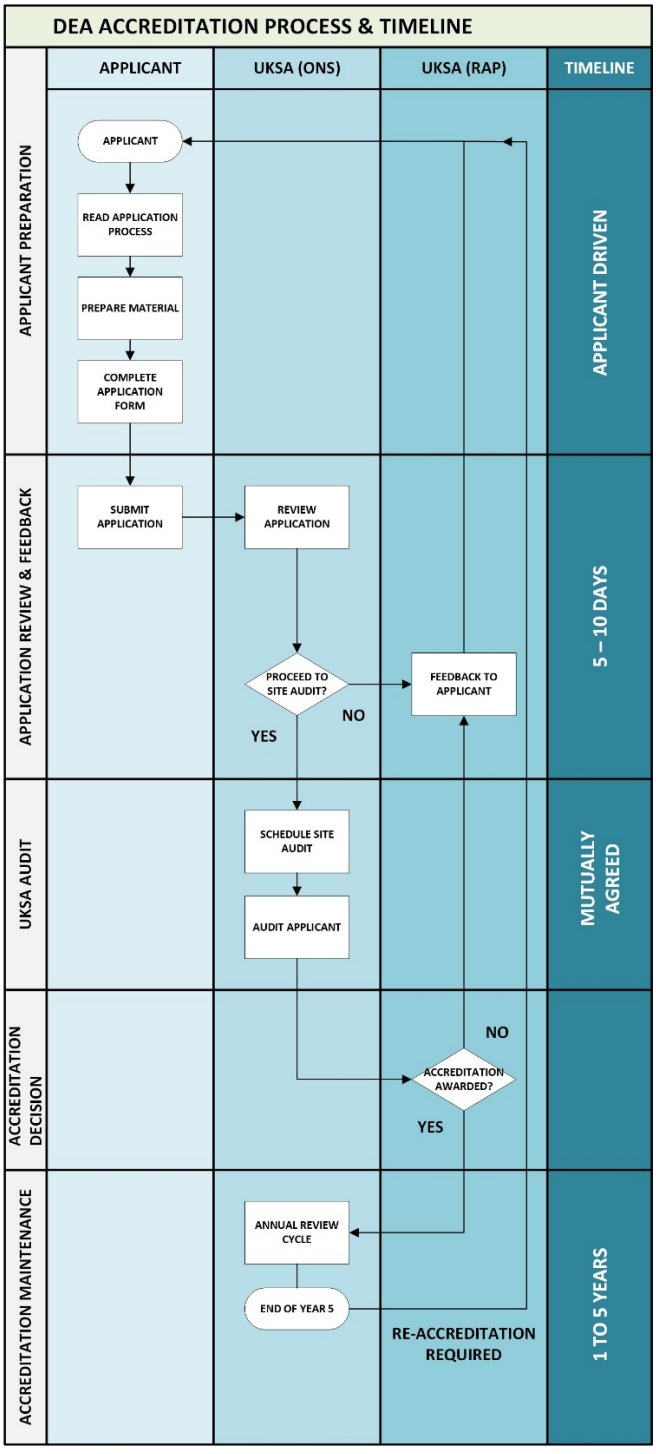
Mechanisms for the UKSA to suspend or withdraw accreditation are identified within the DEA Research Code of Practice and Accreditation Criteria. Applicants should be aware of these conditions.

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.

3.2 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

3.3 The Security and Capability assessment

3.3.1 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.

3.3.2 Capability assessment

The capability assessment considers the skills, experience, service delivery and policies 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.

There are two columns to indicate which requirements are applicable depending on whether you are applying for accreditation to prepare data or provision of data or both.

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.

Where a security or capability control is not a specific requirement for an applicant, they should indicate this on the spreadsheet as **Not Applicable** 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 tab does differentiate between the types of application by virtue of the 'Required for preparation of data' and 'Required for provision of data' columns. Only controls for the application type being made need to be addressed on this tab.

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 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 expands communications to other members within their organisation, which makes communication a challenge and potentially slows down information exchanges.

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. Presentation of the assessment to the Research Accreditation Panel who will make a decision on the application. Those organisations that are accredited as processors 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. The UKSA will provide this directly to the data provider and will inform the accredited organisation designated contact that it has done so.

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. Annual Review

Under the DEA an accreditation is valid for up to five years from the date of award. It is recognised that elements of an organisation's services, systems and processes will change or mature through the accreditation period. To enable for ongoing maintenance of the accreditation and to ensure improving security and capability controls there is an annual review.

The annual review initially focuses on the security and capability controls that were identified as being Good (Level 3) at the point of accreditation and any changes to the services, systems and processes performed during the year. Over the five-year period the reviews will sequentially cover all security and capability controls to measure progress towards Mature (Level 4).

The annual review process is:

1. Three months before the accreditation anniversary, the organisation is contacted by the Secretariat to provide dates for a one day visit to perform the annual review.
2. UKSA Security and Capability teams confirm availability and agree a date for a one-day 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. One month before the review, 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 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.

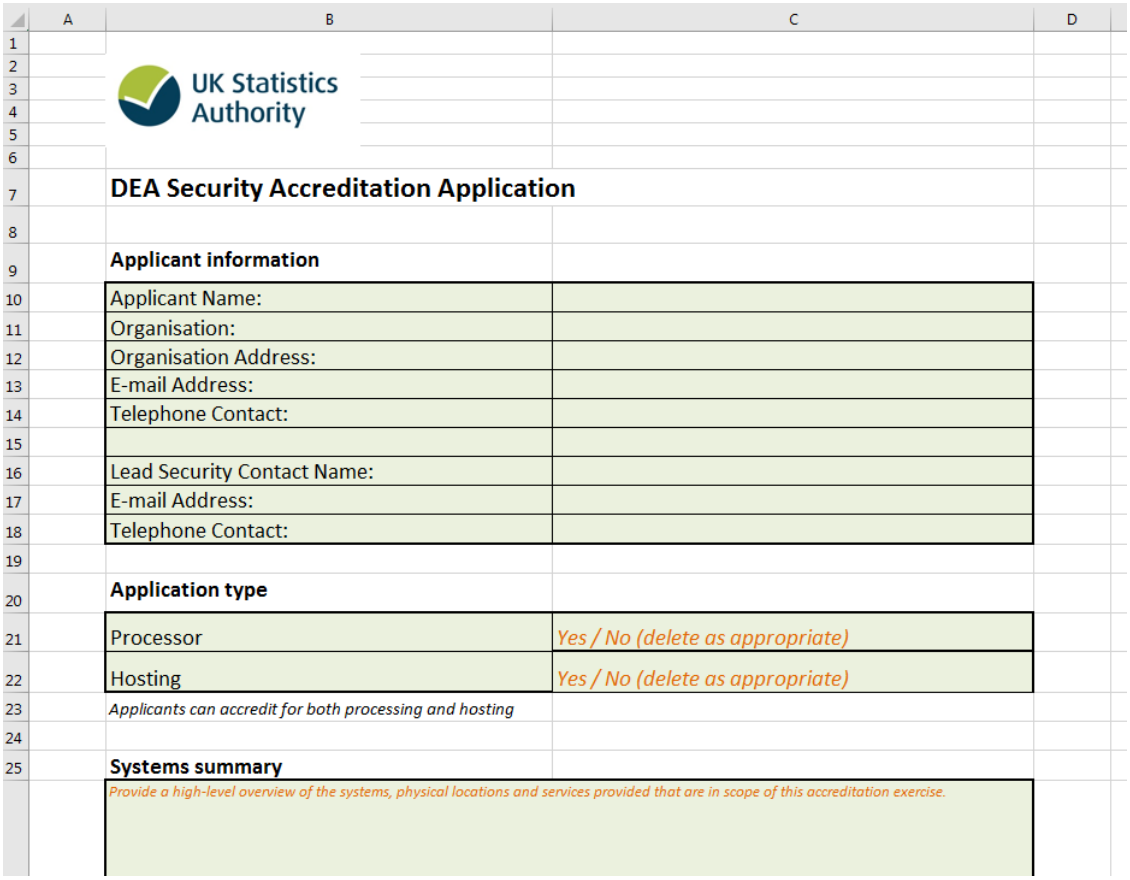
Annex A. Using the assessment form

The DEA Accreditation Spreadsheet has three 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;
- **Applicant Capability Controls** - the implementation of applicant capability 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



UK Statistics Authority

DEA Security Accreditation Application

Applicant information

Applicant Name:	
Organisation:	
Organisation Address:	
E-mail Address:	
Telephone Contact:	
Lead Security Contact Name:	
E-mail Address:	
Telephone Contact:	

Application type

Processor	*Yes / No (delete as appropriate)*
Hosting	*Yes / No (delete as appropriate)*

Applicants can accredit for both processing and hosting

Systems summary

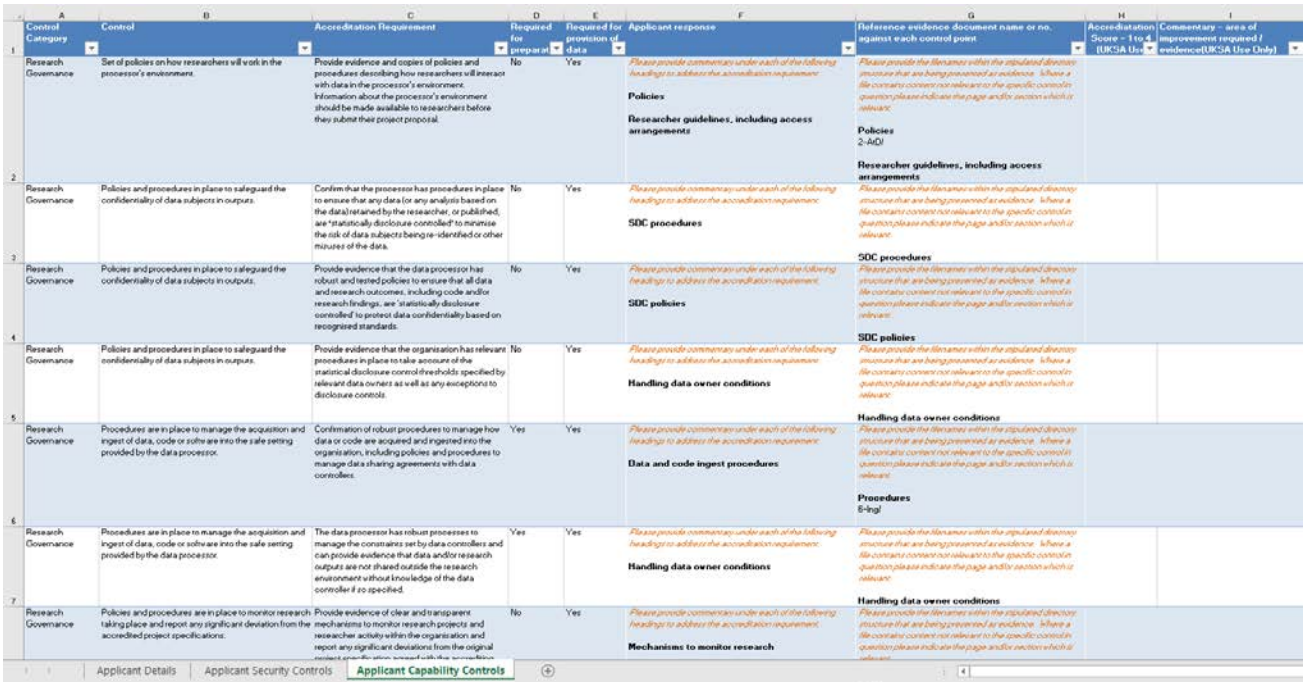
Provide a high-level overview of the systems, physical locations and services provided that are in scope of this accreditation exercise.

A.2 Applicant Security Controls

Control Category	Control	Accreditation Requirement	Applicant Response	Reference evidence document name or no. against each control point	Links to resources related to control	Accreditation Score – 1 to 4 (UKSA Use Only)	Commentary – area of improvement required / evidence(UKSA Use
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.	Please provide commentary under each of the following headings to address the accreditation requirement: **Sufficient Skills** **Experience** **Policies** **Appropriate legal compliance** **Security Strategy & Framework**	Please provide the filename/s 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. **Sufficient Skills** 3-CoPI **Experience** 3-CoPI **Policies** 3-CoPI **Appropriate legal compliance** 3-CoPI **Security Strategy & Framework**	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.	Please provide commentary under each of the following headings to address the accreditation requirement: **Statement on UK processing**	Please provide the filename/s 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. **Statement on UK processing** 4-CoPI	DEA Code of Practice		
DEA Research Code of Practice policies	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 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 organization's policy framework.	Confirm and evidence the organization policies are in place and approved by the appropriate senior management providing a copy of the policies, location and review.	Please provide commentary under each of the following headings to address the accreditation requirement: **Secure Environments Policy** **Major Incident Protocol** **De-identifying Data** **Data Retention & Destruction** **Data Confidentiality Breaches**	Please provide the filename/s 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. **Secure Environments Policy** 5-CoPI **Major Incident Protocol** 5-CoPI **De-identifying Data** 5-CoPI **Data Retention & Destruction** 5-CoPI	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 organization policies are in place and approved by the appropriate senior management providing a copy of the policies, location and review.	Please provide commentary under each of the following headings to address the accreditation requirement: **Policy Governance** **Security Policies & Guidance**	Please provide the filename/s 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. **Policy Governance** 6-ISPI	https://www.ncsc.gov.uk/guidance/10-steps-cyber-security https://www.gov.uk/government/publications/cyber-essentials-scheme-overview https://www.cpni.gov.uk/cyber/cyber-security-risk-management-security-culture-board-awareness		

Applicant Details | Applicant Security Controls | Applicant Capability Controls

A.3 Applicant Capability Controls



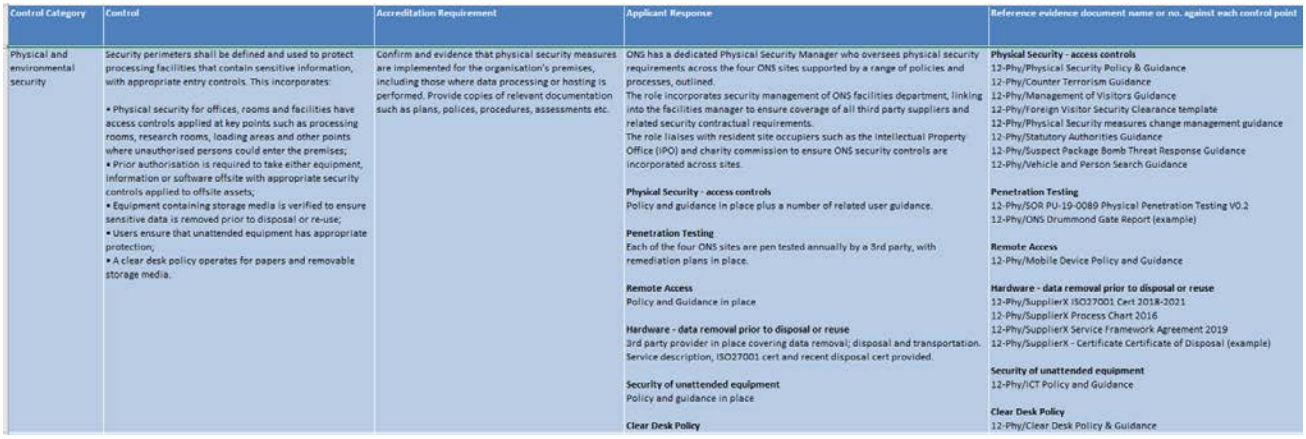
Control Category	Control	Accreditation Requirement	Required for preparation	Required for provision of data	Applicant response	Reference evidence document name or no. against each control point	Accreditation Score – 1 to 4 (UKSA Use	Commentary – area of improvement required / evidence(UKSA Use Only)
Research Governance	Set of policies on how researchers will work in the processor's environment.	Provide evidence and copies of policies and procedures describing how researchers will interact with data in the processor's environment. Information about the processor's environment should be made available to researchers before they submit their project proposal.	No	Yes	Please provide commentary under each of the following headings to address the accreditation requirement: **Policies** **Researcher guidelines, including access arrangements**	Please provide the filename/s 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. **Policies** 2-AtD **Researcher guidelines, including access arrangements**		
Research Governance	Policies and procedures in place to safeguard the confidentiality of data subjects in outputs.	Confirm that the processor has procedures in place to ensure that any data (or any analysis based on the data) retained by the researcher, or published, are "statistically disclosure controlled" to minimise the risk of data subjects being re-identified or other misuses of the data.	No	Yes	Please provide commentary under each of the following headings to address the accreditation requirement: **SDC procedures**	Please provide the filename/s 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. **SDC procedures**		
Research Governance	Policies and procedures in place to safeguard the confidentiality of data subjects in outputs.	Provide evidence that the data processor has robust and tested policies to ensure that all data and research outcomes, including code and/or research findings, are 'statistically disclosure controlled' to protect data confidentiality based on recognised standards.	No	Yes	Please provide commentary under each of the following headings to address the accreditation requirement: **SDC policies**	Please provide the filename/s 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. **SDC policies**		
Research Governance	Policies and procedures in place to safeguard the confidentiality of data subjects in outputs.	Provide evidence that the organisation has relevant procedures in place to take account of the statistical disclosure control thresholds specified by relevant data owners as well as any exceptions to disclosure controls.	No	Yes	Please provide commentary under each of the following headings to address the accreditation requirement: **Handling data owner conditions**	Please provide the filename/s 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. **Handling data owner conditions**		
Research Governance	Procedures are in place to manage the acquisition and ingest of data, code or software into the safe setting provided by the data processor.	Confirmation of robust procedures to manage how data or code are acquired and ingested into the organisation, including policies and procedures to manage data sharing agreements with data controllers.	Yes	Yes	Please provide commentary under each of the following headings to address the accreditation requirement: **Data and code ingest procedures**	Please provide the filename/s 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. **Procedures** 6-Ing/		
Research Governance	Procedures are in place to manage the acquisition and ingest of data, code or software into the safe setting provided by the data processor.	The data processor has robust processes to manage the constraints set by data controllers and can provide evidence that data and/or research outputs are not shared outside the research environment without knowledge of the data controller if so specified.	Yes	Yes	Please provide commentary under each of the following headings to address the accreditation requirement: **Handling data owner conditions**	Please provide the filename/s 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. **Handling data owner conditions**		
Research Governance	Policies and procedures are in place to monitor research taking place and report any significant deviation from the accredited project specifications.	Provide evidence of clear and transparent mechanisms to monitor research projects and researcher activity within the organisation and report any significant deviations from the original	No	Yes	Please provide commentary under each of the following headings to address the accreditation requirement: **Mechanisms to monitor research**	Please provide the filename/s 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.		

Applicant Details | Applicant Security Controls | Applicant Capability Controls

Applicants need to enter information into the Applicant Response and Reference evidence columns of the **Application Security Controls** and **Applicant Capability Controls** tabs.

The UKSA needs information on the state of the controls listed in order to assess the applicant. Every Control Category requires a response or a not applicable declaration. If a control – or part thereof - is not applicable an explanation is required as to why this is the case. If it is not understood by the assessor the control will be marked as not meeting the required standard. If information is missing from the spreadsheet or does not sufficiently address what is being asked for, this is likely to result in delays in the processing of the application.

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: ▪ Physical security for offices, rooms and facilities have 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, polices, procedures, assessments etc.	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. 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. 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. **Physical Security - access controls** Policy and guidance in place plus a number of related user guidance. **Penetration Testing** Each of the four ONS sites are pen tested annually by a 3rd party, with remediation plans in place. **Remote Access** Policy and Guidance in place **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. **Security of unattended equipment** Policy and guidance in place **Clear Desk Policy**	**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 **Penetration Testing** 12-Phy/SOR PU-19-0089 Physical Penetration Testing V0.2 12-Phy/ONS Drummond Gate Report (example) **Remote Access** 12-Phy/Mobile Device Policy and Guidance **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) **Security of unattended equipment** 12-Phy/ICT Policy and Guidance **Clear Desk Policy** 12-Phy/Clear Desk Policy & Guidance

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

Accreditation Requirement	Applicant Response
Confirm that there is a policy in place covering all aspects of the UKSA provided sample secure environments policy. Provide a copy of the policy and detail where in the pack this is to be found here.	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	All information security responsibilities shall be defined and allocated. This incorporates: • 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.	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

		such as plans, polices, procedures, assessments etc.

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

Please provide commentary under each of the following headings to address the accreditation requirement. **Segregation of duties** **Segregation of duties is covered within the IT Security Policy** **Appropriate contact with authorities**	*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.* **Segregation of duties** 7-Org/IT Security Policy.pdf

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

Please provide commentary under each of the following headings to address the accreditation requirement. **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.**	*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.* **Segregation of duties** 7-Org/IT Security Policy.pdf 7-Org/PROJECT-0016-Design.docx 7-Org/RiskAssessment0055.pdf

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

Please provide commentary under each of the following headings to address the accreditation requirement. **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 Resonsibilities 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 specificed by the line manager.** **Hepldesk screenshot PRIV shows a request for a privileged new user. The corresponding AD screentshot PRIV shows the current membersip 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.**	*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.* **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 screenshort REG.jpg 7-Org/AD screenshot REG.jpg

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)

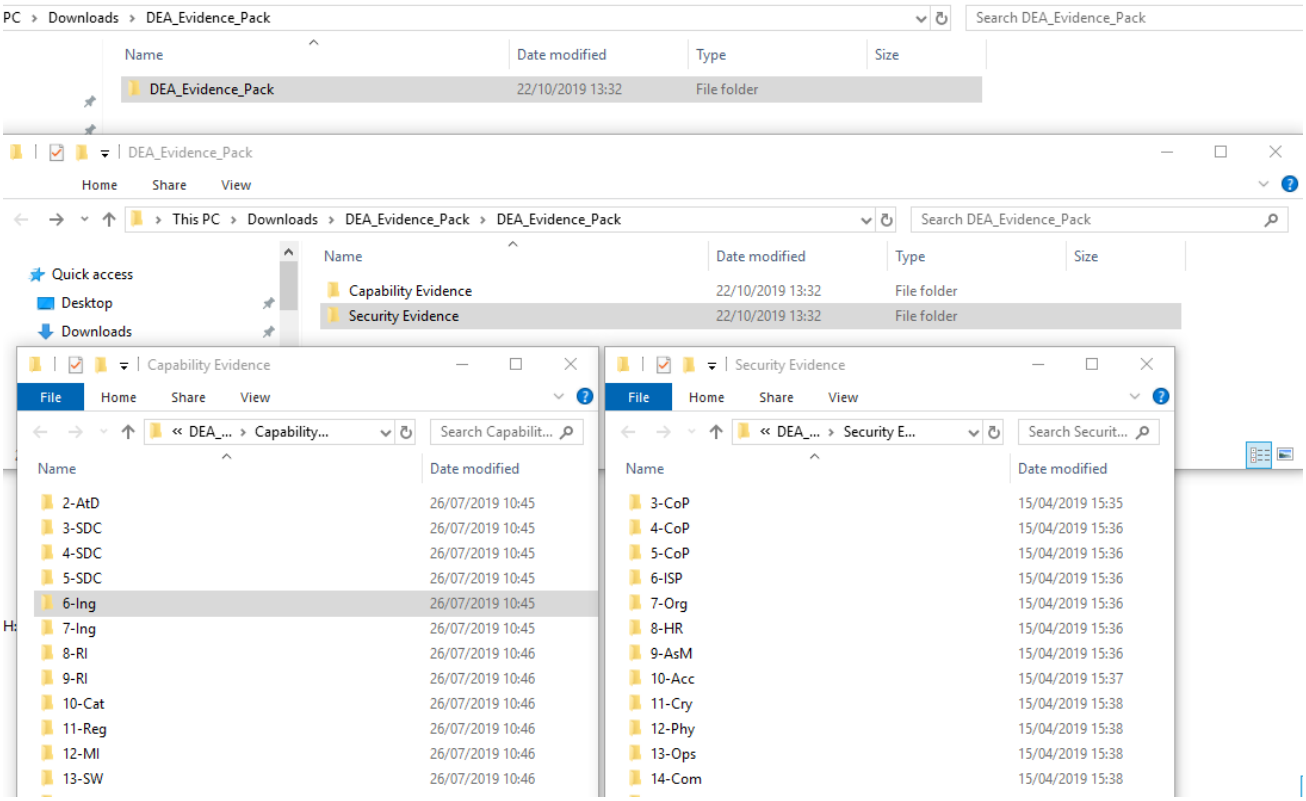
Annex B. Compilation of evidence packs

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)

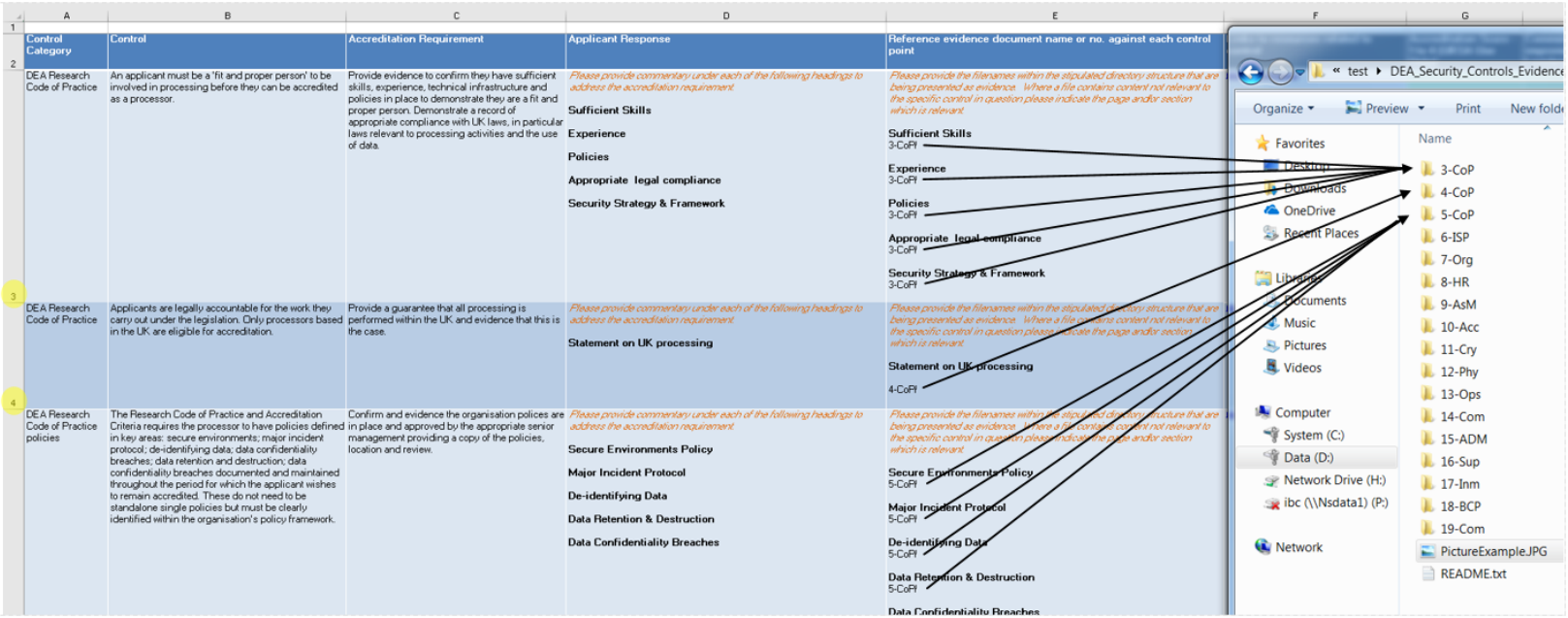
The directories are named starting with a number that corresponds to the row on the spreadsheet tab for which corresponding evidence must be placed. The diagram on the following page depicts this using the Security tab.

The 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.

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"



Control Category	Control	Accreditation Requirement	Applicant Response	Reference evidence document name or no. against each control 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.	*Please provide commentary under each of the following headings to address the accreditation requirement.* **Sufficient Skills** **Experience** **Policies** **Appropriate legal compliance** **Security Strategy & Framework**	*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.* **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.	*Please provide commentary under each of the following headings to address the accreditation requirement.* **Statement on UK processing**	*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.* **Statement on UK processing** 4-CoP
DEA Research Code of Practice policies	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 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 polices are in place and approved by the appropriate senior management providing a copy of the policies, location and review.	*Please provide commentary under each of the following headings to address the accreditation requirement.* **Secure Environments Policy** **Major Incident Protocol** **De-identifying Data** **Data Retention & Destruction** **Data Confidentiality Breaches**	*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.* **Secure Environments Policy** 5-CoP **Major Incident Protocol** 5-CoP **De-identifying Data** 5-CoP **Data Retention & Destruction** 5-CoP **Data Confidentiality Breaches**

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 is an annual review.

Who can I contact for more information?

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