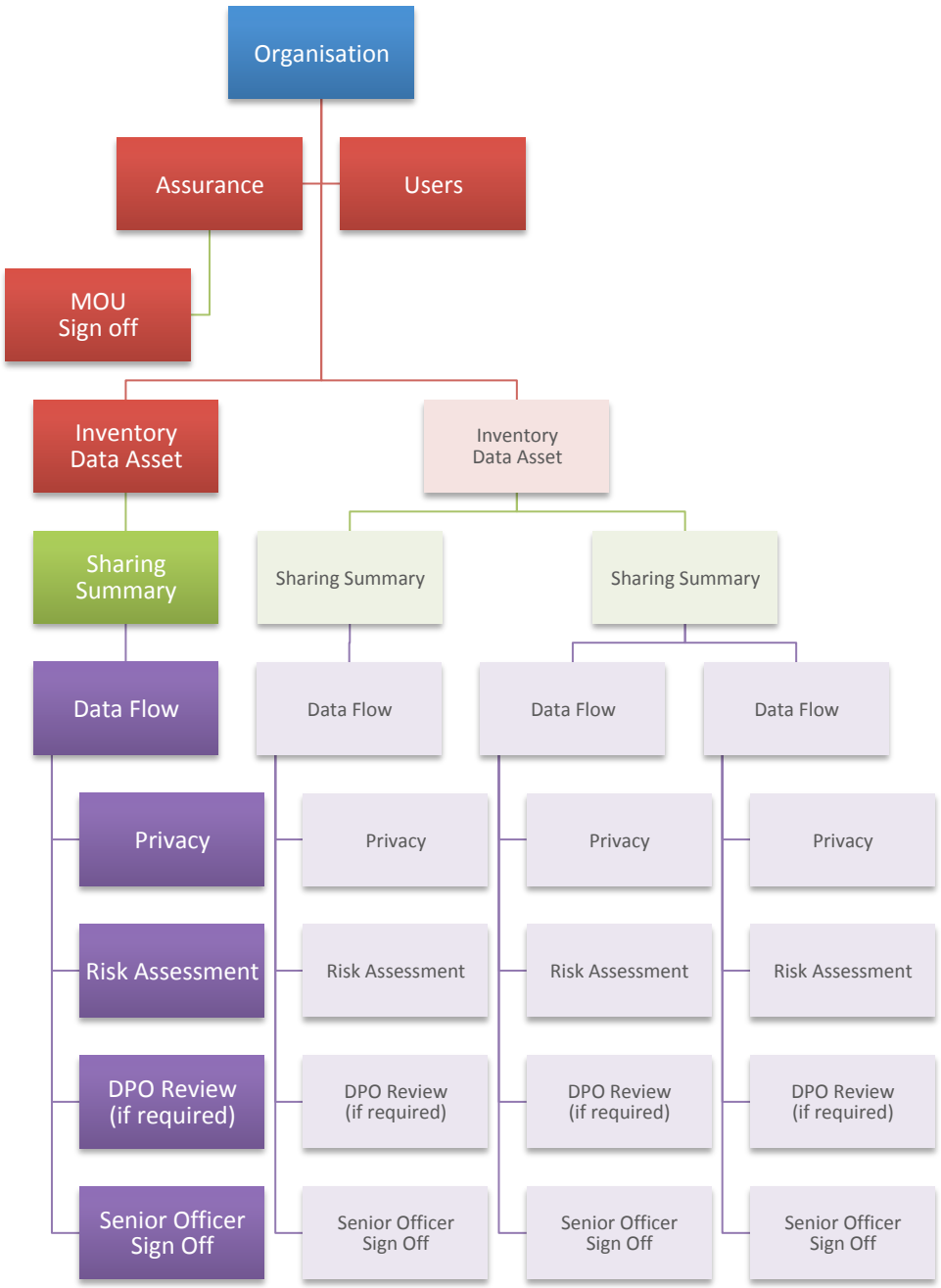
ESBT Digital – Guide to the ISG Process Flow

The below is an over view of the way the ISG process works. Please note the wording used here is merely indicative and may differ (and be more detailed, accurate and/or helpful) in the ISG itself.

The basic structure and process within the ISG is shown in the diagram below.

Frequently a Data Asset will only have one sharing summary, with one data flow (as coloured) but there can be multiple sharing summaries for each asset and multiple flows for each summary (shown faded).



ORGANISATION - (set-up)

- Create organisation
- Add users in Roles
- Complete assurance
- Sign MOU (Senior Officer confirms organisation will act as they say)

INVENTORY - (a record of organisational data assets)

- Organisational decision whether to list all data assets or just those used in ISG sharing
- Summary details of data asset a with ability to upload any relevant, associated files

---

At this point you may have an idea you may wish to share information.

- *The Data Sharing summary describes what you are proposing, with whom and why.*
- *The Data Flow describes how you are proposing to share it.*

Having established this basic information, it moves to the Privacy section.

DATA SHARING section

Data Sharing Summary

This section describes, at a high level, what is proposed to be shared, between whom and for what purpose.

- Who should see this Sharing Summary
- Who might be involved on the sharing
- IS a Data Asset (in ICR) linked to the sharing
- Why are you proposing to share, for what purpose
- What is the Legal Gateway for sharing
- What information will you be sharing
    - (inc Personal and SC Personal – data items and applicable Art 6 or Art 9 condition)
- Specify which data fields
- What are the benefits to sharing
- In what format is the data being shared
- Who are the data subjects
- Who will access the information in the receiving organisation
- Give a review cycle/date
- Upload any relevant, associated files

Data Flow detail *(within a Data Sharing Summary)*

(there can be several of these under each sharing summary, although commonly there is only one)

This section describes, how you are proposing to share the information. The ability to have multiple Data Flows allows you to share the same information in different ways with different organisations (or groups of organisations).

- Who should see this data flow
- Which organisations are involved
- Direction of the flow: outbound/inward/both, is it inside/outside UK/EU/Internal – onsite/offsite
- Frequency of transfer and number of records being transferred
- Mode of transfer (e.g. paper/electronic) and controls (e.g. N£/HCSN)
- Which sharing platform is being used (limited picklist – often not helpful)
- Where will the data be stored post transfer, how will it be secured, security around access

Privacy *(within a Data Flow)*

In order to begin the privacy section (This prints under the title of "Data Protection Impact Assessment") you need to know a lot of the information in the sharing summary and data flow detail. This section carries forward some previously entered information, and adds additional considerations and detail around legal requirements and processes.

- Is there a privacy notice (upload or hyperlink)
    - Note: any organisation without will have their assurance marked as 'Limited'
- Does the privacy notice need amending/updating
- Purpose of sharing (carried forward from Sharing Summary)
- Consent model (including 'Not required') – picklist and text to elaborate
- Legal Gateways for sharing personal data (carried forward from Sharing Summary)
- Legal Gateways specific to this data flow (if different from above)
- Article 6 conditions for sharing personal data (carried forward from Sharing Summary)
- Personal data items (picklist)
- Article 9 conditions for sharing personal data (carried forward from Sharing Summary)
- Special Category data items (picklist)
- Checks regarding adequacy, relevance, necessity for collection of personal/sensitive data (text)
- Provisions for accuracy/completeness by all organisations
- Management of retention & disposal by all organisations
- How Subject access requests are dealt with and rectification/blocking/erasure/destroying
- Describe receiving organisations policies/processes and standard procedures
- Describe receiving organisations management of incidents
- Describe receiving organisations training for both system and data
- Describe receiving organisations security of the asset
- Describe receiving organisations business continuity arrangements
- Describe receiving organisations disaster recovery arrangements
- Do all 3rd party/supplier contracts contain necessary IG clauses inc DP & FOI Act.
- Will personal/sensitive data be transferred to/from outside of EEA

Risk Assessment *(within a Data Flow)*

This is optional. It is manually triggered but can then initially be automatically generate, based on answers so far that are set against pre-set 'risks' in the ISG. It also allows users to specify where acceptable but slightly different arrangements are in place to address those issues.

It also allows users as well as to add their own risks and controls, either on top of the initial assessment generated by the ISG or to create a complete risk assessment from scratch.

It can be useful as a quality check and to highlight any accidental errors/omissions.

- Automated electronic transfer is taking place over a controlled platform. Security controls should still be implemented and maintained
- Servers hosted within the UK are bound by UK Law and legislation. You must ensure that the necessary due diligence and checks are made. Make sure access is controlled.
- At least one control is in place which enables the information to be accessed securely in the receiving organisation.
- At least one control is in place which enables the information to be accessed securely in the receiving organisation
- All of the minimum recommended controls are in place relating to the accuracy and completeness of the data.
- All of the minimum recommended controls are in place relating to the retention and disposal of the data.
- All of the minimum recommended controls are in place relating to subject access requests.
- Policies, processes and standard operating procedures for the asset/data are clearly defined, up-to-date, understandable and readily available.
- Incidents are reviewed appropriately.
- Users of the data are regularly trained, aware of their responsibilities and understand what to do in the event of breach.
- The asset / data is secure, controlled and interactions recorded.
- Business continuity arrangements are clear, users are aware and trained with regular reviews and updates.
- Disaster recovery arrangements are in place with regular review and testing where appropriate

Append Documents *(within a data flow - if desired)*

DPO Review *(of data flow - if required)*

Sign Off *(sign off data flow)*