# Table of Contents

1. **Purpose of the Document** .................................................................................................................................................................................. 2

2. **Introduction** ................................................................................................................................................................................................... 3
   2.1 **Learning Content** ....................................................................................................................................................................................... 3

Chapter 2: **Definition** ........................................................................................................................................................................................................ 4
   2.2 **What is “Individual Data Processing”?** ........................................................................................................................................... 4
   2.3 **What is “Individual Data Processing”? - Definition** ................................................................................................................................. 5
   2.4 **Legal background of IDP – Management and Identification** .............................................................................................................. 6

3. **Roles, Responsibilities and Process Overview** ......................................................................................................................................................... 7
   3.1 **Relevant Stakeholders** ............................................................................................................................................................................... 7
      3.1.1 **CISO** ................................................................................................................................................................................................. 7
      3.1.2 **IDP Master Coordinator** .................................................................................................................................................................. 8
      3.1.3 **IDP Coordinator** ............................................................................................................................................................................. 8
      3.1.4 **IDP Process Owner** ................................................................................................................................................................. 8
      3.1.5 **IDP Developer** ............................................................................................................................................................................... 9
      3.1.6 **IDP Tester** ..................................................................................................................................................................................... 9
      3.1.7 **IDP Business Support** ............................................................................................................................................................... 10
      3.1.8 **IDP Information Owner** ............................................................................................................................................................ 10
   3.2 **IDP Lifecycle** ................................................................................................................................................................................................ 10
      3.2.1 **File Creation and Categorization** .................................................................................................................................................. 11
      3.2.2 **IDP Initial / Classification / Risk Survey** ........................................................................................................................................ 12
      3.2.3 **IDP Approval, Test and Risk Assessment** ...................................................................................................................................... 13
      3.2.4 **IDP Periodic confirmation / Re-classification / Approval** ....................................................................................................... 13
      3.2.5 **Controls; Review** ........................................................................................................................................................................ 14

4. **Chapter 4: Classification Process (and related tasks)** .............................................................................................................................................. 15
   4.1 **First Things First - Step 1** ......................................................................................................................................................................... 15
      4.1.1 **Is my file an IDP file?** ............................................................................................................................................................... 16
      4.1.2 **MS Excel Questionnaire** .............................................................................................................................................................. 16
4.1.3 Excel Tracker Help Button ................................................................. 17
4.1.4 Examples: “non-IDP”, “IDP” and “in Development” .......................... 18
4.1.5 Categorization Tools ........................................................................ 18
4.2 IDP Classification – Step 2 & Step 4 .................................................. 19
  4.2.1 Risk Survey Questionnaire ............................................................... 20
  4.2.2 IDPs with higher Risk ....................................................................... 21
4.3 IDP Classification – Step 2 & Step 4 .................................................. 23
4.4 Approval and Risk Management – Step 3 .......................................... 24
4.5 Focus on Responsibility of the IDP coordinator .................................. 25
4.6 Storage, Back-up and Versioning ........................................................ 26
5. Conclusion ............................................................................................. 27
  5.1 Summary ............................................................................................. 27
  5.2 Hints and Tips ..................................................................................... 27
  5.3 Useful Links ......................................................................................... 28
1. Purpose of the Document

The document details information about a training on “Individual Data Processing”.

Individual components of the training and subsequent explanation are well described in this Document.
2. Introduction

The purpose of this training is to give an understanding on

- How to identify an IDP by using the criteria that constitute and IDP,
- The individual steps needed to correctly classify an IDP as well as
- The compliant treatment of an IDP along legal requirements and under consideration of the internal framework

2.1 Learning Content
Chapter 2: Definition

2.2 What is “Individual Data Processing”?

What is ‘Individual Data Processing’?

‘Individual Data Processing’ is a defined term stemming from several regulations. It describes an activity which is

- undertaken by an individual End User
- in order to support them in an activity to process data,
- where no regular IT application is used,
- using e.g., formulas, functions, scripts, scripting languages and programming languages.

The most frequent Individual Data Processing (IDP) activities at DBG are undertaken in MS Excel and MS Access. Furthermore, there are about 20 programming languages to consider which are defined in the IDP Standard (e.g., Powershell, Java, Python and SQL).

Standard applications such as SAP, Jira, MS Word and MS PowerPoint are not defined as IDPs.
2.3 What is “Individual Data Processing”? - Definition

**Individual Data Processing**

as stated in the IDP Policy

IDP: Individual Data Processing consists of processing business relevant information by means of End User developed computations using formulas, functions, scripts, scripting languages and programming languages. Business relevant information is contextual to the importance of it being processed in the respective organisational units as part of their processes. End Users and their management are responsible for determining the relevance of this specific type of processing of information. Since IDP would otherwise take place outside of regular IT management processes, it requires adequate governance, control, and protection measures.

The following criteria characterise and support the identification of IDPs. An IDP must fulfill all of these criteria:

1. IDPs are neither developed, nor provided or maintained based on the standard processes for Regular Applications.
2. IDPs are based on the functionality of runtime environments or script languages listed in the appendix of the IDP Standard.
3. IDPs are used to change data and content as well as process data used as input for business processes.

IDPs have to meet the requirements specified in the IDP Standard according to their classification.

Regular Applications: Regular Applications are managed by the IT function. The development, maintenance and support follow established IT processes. Information about all regular applications is stored in a central register and the security criticality ratings.

Irregular Applications: Irregular Applications are indifferent from regular applications in terms of e.g., size or complexity, but are used exclusively through the business department employing such applications. Due to the lack of central IT process enforcement, security controls are often not implemented on process and technical level. The use of Irregular Applications within DBG is prohibited. Irregular applications existing at the time this policy becomes effective must (1) be reported to the IT Governance function or Senior Management immediately, and (2) either be transferred to regular applications or be deactivated.
2.4 Legal background of IDP – Management and Identification

What is the legal background and why does IDP need to be identified and managed?

The requirements further described in this IDP training can be derived from several regulations:

- MuRisk - minimum requirements for risk management.
- BAIT - Banking supervisory requirement for IT in Germany.
- CSSF - Financial Sector Supervisory Commission.
- MAS TRM - MAS Technology Risk Management Guidelines.

In addition, from a risk management perspective an adequate handling of IDP is required in order to:

- reduce the risk of a so called ‘Shadow IT’ (i.e. IT that is not approved or controlled by IT),
- appropriately protect critical information in IDPs by proper identification, assessment, approval and reporting, and
- migrate IDP with an information classification ‘Critical’ into a regular IT application.
3. Roles, Responsibilities and Process Overview

3.1 Relevant Stakeholders

3.1.1 CISO

- Defines the IDP framework of Deutsche Börse Group, and
- ensures its adherence to the regulation and its operational effectiveness.
3.1.2 IDP Master Coordinator

**IDP Master Coordinator**
- Supports the IDP coordinator and ensures the set up of additional sample checks,
- establishes guidelines for documenting control activities and provides an archive / storage area,
- increases awareness by providing mandatory trainings,
- verifies decommission plans for critical IDPs, and
- reports on status of IDP compliance.

3.1.3 IDP Coordinator

**IDP Coordinator**
- Role is not mandatory - in case no IDP Coordinator is named, the Process Owner takes over this task.
- Coordinates the IDP process in his area of responsibility / Legal Entity, and
- carries out controls, as defined in the IDP Control Catalogue, to ensure compliance to IDP regulation.

3.1.4 IDP Process Owner

**IDP Process Owner**
- Must be Level 5 or above,
- regularly reviews IDP within his area of responsibility,
- for IDP files with ‘Major’ and ‘Critical’ information classification*: approves the IDP (delegation possible), and
- in case no IDP Coordinator is named, the IDP Process Owner takes over those tasks (see next slide).
### 3.1.5 IDP Developer

**IDP Developer**

- Develops, categorizes, classifies, maintains the IDP and the IDP inventors.
- For IDP files with ‘Major’ and ‘Critical’ classification*: initiates the approval process and provides mandatory IDP documentation.
- For IDP files with ‘Critical’ classification ensures that a plan to migrate the IDP to a regular IT application is created (decommission plan).
- Re-classifies the IDP upon periodic trigger (Risk Survey User).
- Re-categories Non-IDP upon periodic trigger (Saving User).

* For all IDPs with higher risk regarding confidentiality a limited documentation should be provided.

### 3.1.6 IDP Tester

**IDP Tester**

- For IDP files with ‘Major’ and ‘Critical’ information classification*: prepares the test documentation and executes the test cases for the IDP as part of an acceptance test and a release cycle.
- IDP tester and End User can be the same person.

* For all IDPs with higher risk regarding confidentiality a limited documentation should be provided.
3.1.7 IDP Business Support

**IDP Business Support**

- Consults and provides services on IDP tools, and
- provides services to all IDP Coordinators or Process Owners, where no IDP Coordinator is appointed.

3.1.8 IDP Information Owner

**IDP Information Owner**

For IDP files with “Major” and “Critical” information classification*: manages the risks identified as a result of the Risk Assessment.

* For all IDPs with a higher risk regarding the information security objective confidentiality a limited documentation should be provided.

3.2 IDP Lifecycle

What does the typical lifecycle of an IDP look like?

Click on the individual steps for more information.

IDP Inventory – IDV Suite
The Inventory contains all meta data of files categorized in ‘IDP'V, ‘Non-IDP', files ‘In Development' and ‘unassessed'.
3.2.1 File Creation and Categorization

**End User / IDP Developer**

**Identification**

When creating and saving a file which contains formula or codes the End User is requested automatically to answer a first set of questions after 24h which will then lead to a categorisation of files into

- Non-IDP,
- IDP or
- In Development.

**IDP**

All files classified as IDP will move on to the next step where the Risk Survey is performed.
IDP Developer

Classification
When categorised as IDP, the IDP Developer is requested automatically to answer a Risk Survey in order to determine the overall protection requirement:

- Negligible
- Minor
- Major
- Critical

‘Major’ and ‘Critical’
IDPs require further steps (documentation, Risk Assessment, approval etc.)

3.2.2 IDP Initial / Classification / Risk Survey
3.2.3 IDP Approval, Test and Risk Assessment

**IDP Process Owner / Tester / Developer**

‘Major’ and ‘Critical’

IDPs classified as ‘Major’ or ‘Critical’ are considered to bear a higher risk (‘higher risk IDP’) and therefore require further steps:

- A complete set of mandatory documentation to be provided by the IDP Developer and / or Tester.
- A Risk Assessment and the approval by the IDP Process Owner (or delegate).

3.2.4 IDP Periodic confirmation / Re-classification / Approval

**IDP End User**

**Re-classification / Confirmation**

When using an IDP file, the End User is automatically requested to confirm or re-classify the file after a defined period.

**Approval**

‘Major’ and ‘Critical’ IDPs have to be confirmed annually.
3.2.5 Controls; Review

**IDP Coordinator / Process Owner**

**Controls**
The IDP Coordinator contacts the Process Owner for

- the verification of categorization and classification of the IDP file,
- the control of approvals and mandatory documentation,
- the verification of existence of replacement plans,
- the annual confirmation of the IDP category and
- IDP files that are classified as ‘In development’, as they must not have this status for more than 180 days.

**Review**
The IDP Process Owner needs to review all active files on a yearly basis.
4. Chapter 4: Classification Process (and related tasks)

4.1 First Things First - Step 1

First things first – what needs to be done at step 1

Do you create formulas in Excel / Access or any other coding? No? Then you most probably will not be the one who creates an IDP.

The file you create will most probably be a ‘Non-IDP’ file.
4.1.1 Is my file an IDP file?

<table>
<thead>
<tr>
<th>Is my file an IDP file?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Will my file be saved again within the next 24 hours?</td>
</tr>
<tr>
<td>Yes</td>
</tr>
<tr>
<td>Which category is my file?</td>
</tr>
<tr>
<td>IDP file</td>
</tr>
<tr>
<td>MS Excel/Access questionnaire</td>
</tr>
<tr>
<td>Non-IDP file</td>
</tr>
<tr>
<td>Result:</td>
</tr>
<tr>
<td>IDPs are used to modify and process data and contents that are used as input for business processes and</td>
</tr>
<tr>
<td>IDPs are neither developed, deployed or maintained according to the standard procedure for regular applications</td>
</tr>
<tr>
<td>Furthermore, IDPs are based on the functionality of the runtime environment (Excel/Access) or scripting languages listed in the IDP Standard.</td>
</tr>
</tbody>
</table>

4.1.2 MS Excel Questionnaire

File: MiscOuts_DBAG/TEST.xlsx

Please select if this file is an IDP or not.
If the file fulfills the criteria of an IDP, select - Yes (IDP).
If not select - No (Non-IDP).
If the file is not yet finalized (e.g. adding code or formulas), select - Development.
In development files are not to be used in daily work activities and should not remain in this status longer than 180 days.

IDP DEFINITION: PLEASE CLICK ON THE QUESTIONMARK!

In case the business purpose this file is being used for has to be provided. Also please specify in detail the main driver(s) for the risk that affect the classification (state those facts that make the assessment comprehensible to third parties).
4.1.3 Excel Tracker Help Button

![ExcelTracker V4.0 FPSa (Build: 139-DLL) - Note](image)

**IDP:** Individual Data Processing consists of processing business relevant information by means of End User developed computations using formulas, functions, scripts, scripting languages, and programming languages. Business relevant information is contextual to the importance of it being processed in the respective organizational units as part of their processes.

An IDP must fulfill all of these criteria:

1. IDPs are neither developed, provided or maintained based on the standard processes for Regular Applications.
2. IDPs are based on the functionality of runtime environments (Excel/Access) or script languages (e.g., Python, SQL, PowerShell) listed in the appendix of the IDP Standard.
3. IDPs are used to change data and content, process data used as input for business processes.

If the file does not fulfill all criteria, the file, by definition, is not an IDP (Non-IDP).

The difference to Regular Applications is:

Regular Applications (e.g., SAP, JIRA) are managed by the IT. The development, maintenance and support of Regular Applications follow established IT processes and do not need to be included in the IDP inventory.

Examples where the assessment of the file will not be automatically triggered:

1. A generated list out of a master system
   - e.g., a monthly budget report exported from SAP (AFO)
   - e.g., a staff overview (ZPORQ)
2. A simple list without any calculations or graphs
   - e.g., birthday lists or vacation overviews
   - e.g., office / home office attendance lists
3. A simple data table with [auto-filter] activated
   - e.g., provider lists with spend data
4.1.4 Examples: “non-IDP”, “IDP” and “in Development”

Examples for ‘non-IDP’, ‘IDP’ and ‘in Development’

- **Non-IDP**: No codes, formulas etc.°
  - Examples:
    - Single export e.g. from SAP
    - Document test results
    - Customer templates
  - No further tasks to be conducted

- **IDP**: This file does fulfill the criteria of IDP
  - Examples:
    - An Excel-file to process business data
    - A script-file to read business data out of a data-base and transform / process the data
  - A Risk Survey required - performing an initial protection requirement analysis as well as corresponding further tasks

- **In Development**: As long as the status is set to ‘In Development’ it is not allowed to use the file in daily work activities
  - Examples:
    - An Excel-file to process business data where the formulas are currently being developed
    - A script-file to read business data out of a data-base and transform / process the data which is currently being tested
  - No Risk Survey required until the file is ready to be used

° for further information on functionality of runtime environments, script languages see appendix of the IDP Standard

4.1.5 Categorization Tools

**Tools for categorization of IDP, non-IDP and in development files**

- IDPs based on other technology than Access or Excel for example Python are defined in the IDP Standard and must be identified with the help of the FileTracker.
- The identification leads to a registration in the IDP inventory.
- The FileTracker is an application with an interface on the IDV-Suite.
Tools for categorization of IDP, non-IDP and in development files

- Unless otherwise defined, the IDP Developer must manually identify and actively add the IDP to the IDP inventory via the FileTracker (Registration).
- In a second step the file must then be classified.
- You can download the FileTracker from the Software Centre which loads the icon onto your desktop.
- The FileTracker is also available in the AppLauncher (Citrix environment).

4.2 IDP Classification – Step 2 & Step 4

Step 2 – IDP classification - first to dos when initially classifying a file (step 2) and periodically re-confirming or re-classifying (step 4)

When the file was categorized as IDP, the Risk Survey needs to be answered in order to determine the overall protection requirement.

These are the 4 information security objectives:
- Confidentiality,
- Integrity,
- Authenticity and
- Availability.

to consider for the overall protection requirement. They can be rated:
- Negligible,
- Minor,
- Major or
- Critical.
Step 2 – IDP classification - first to dos when initially classifying a file (step 2) and periodically re-confirming or re-classifying (step 4)

Please use the help icons and question marks for an explanation and breakdown of the individual questions.

‘Major’ and ‘Critical’ IDPs require further steps (specific Documentation, Risk Assessment, Approval etc.).

4.2.1 Risk Survey Questionnaire

The risk survey questionnaire at a closer look

The IDP Developer is guided through the questionnaire to determine the protection needs and thereby the criticality of the IDP.

The overall criticality has four pre-defined classification levels based on the potential impact on the business and the protection requirements / information criticality. They are ‘Negligible’, ‘Minor’, ‘Major’ and ‘Critical’.

The answers are evaluated using the IDP Information Classification decision tree which is detailed in the IRM Guideline.

The decisions are based on the Information Security objectives:

- Confidentiality: Enabling authorized access to information and associated assets when required.
- Integrity: Guaranteeing the accuracy and completeness of information and protection methods.
- Availability: Enabling access to information when required.
- Authenticity: Ensuring genuineness and reliability of information.

The classification must be performed separately for each security objective and must always depict the estimated maximum impact for each security objective, which could occur in case of any possible breach.
The risk survey questionnaire at a closer look

The classification scheme follows the Group Risk Classification scheme and consists of
- types of impact to be considered and
- specific criteria for each classification level for the different types of impact.

<table>
<thead>
<tr>
<th>Type of Impact</th>
<th>Critical</th>
<th>Major</th>
<th>Minor</th>
<th>Negligible</th>
</tr>
</thead>
<tbody>
<tr>
<td>Financial impact</td>
<td>EUR</td>
<td>EUR</td>
<td>EUR</td>
<td>EUR</td>
</tr>
<tr>
<td>Non-financial impact</td>
<td>EUR</td>
<td>EUR</td>
<td>EUR</td>
<td>EUR</td>
</tr>
<tr>
<td>Regulatory impact</td>
<td>EUR</td>
<td>EUR</td>
<td>EUR</td>
<td>EUR</td>
</tr>
<tr>
<td>Reputation impact</td>
<td>EUR</td>
<td>EUR</td>
<td>EUR</td>
<td>EUR</td>
</tr>
</tbody>
</table>

4.2.2 IDPs with higher Risk

IDPs with higher risk (‘Major’ and ‘Critical’)

For IDPs with higher risk (‘Major’ and ‘Critical’) the following documentation is mandatory and needs to be in place before approval through the IDP Process Owner or his delegate.

- Business Requirements and Business Acceptance Criteria,
- Test Cases and Test Execution Documentation,
- User Guide / Training Material,
- Technical Documentation,
- Access Concept and
- Recovery Procedures.
IDPs with higher risk (‘Major’ and ‘Critical’)

Exception! For IDPs with higher risk (‘Major’ / ‘Critical’) due to information security objective ‘Confidentiality’, a reduced documentation set must be provided.

Additionally, it is mandatory to provide the information in which Legal Entities the IDP is being used (to be included under Additional Information within the IDP Tracker documentation). The overview below shows which documentation is mandatory for what kind of protection requirement/information criticality.

<table>
<thead>
<tr>
<th>Documentation</th>
<th>Negligible</th>
<th>Minor</th>
<th>Major*</th>
<th>Critical*</th>
</tr>
</thead>
<tbody>
<tr>
<td>Business Purpose</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>Business Requirements</td>
<td>no</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>Test Cases</td>
<td>no</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>User Guide / Training Material</td>
<td>no</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>Technical Documentation</td>
<td>no</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>Access Concept</td>
<td>no</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>Recovery Procedure</td>
<td>no</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>Risk Assessment</td>
<td>no</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
</tr>
</tbody>
</table>

* For IDPs classified as major or critical due to confidentiality reasons, an Access Concept must be available as a minimum requirement. The information in which Legal Entities the IDP is being used must also be included.

The Business purpose should provide a short, high-level description for what business process / purpose the file is needed for, e.g., overview sales revenue, calculation tools. This is required for all files.

When the risk survey is completed if you have a ‘Major’ or ‘Critical’ file you must add the relevant documentation.

Then initiate the approval process. Inform IDP Process Owner / delegate of required approval.
4.3 IDP Classification – Step 2 & Step 4

Step 2 – IDP classification - first to dos when initially classifying a file (step 2) and periodically re-confirming or re-classifying (step 4)

After a defined period of time, the ExcelTracker triggers a request to confirm or re-classify the IDP. In addition, a IDP can be re-classified at any period in time needed.

With the relevant file opened, choose ExcelTracker from the ribbon bar and select Risk Survey.

Select "...need to be renewed" and go ahead with the classification.
4.4 Approval and Risk Management – Step 3

Step 3 – approval and risk management - focus on responsibility of the IDP Process Owner (or Delegate)

- Once an IDP has been classified as ‘Major’ or ‘Critical’, the approval process needs to be initiated by the IDP Developer via the ExcelTracker.
- The Risk Assessment needs to be completed before the approval can be finalized.
- The approval must be provided by the Process Owner or their Delegate.
- The Process Owner must be Head of Section (Level 5) or above.
- Once approved, the IDP can be used in daily work activities.
- In case the criticality of the file has changed, e.g., because formulas have been changed and the so called ‘Check Sum’ (auto-calculated value based on the complexity of the file), the approval of the file will be automatically revoked and the approval needs to be renewed.
- In case the ‘Major’ or ‘Critical’ IDP was not changed within 365 days, the Process Owner needs to re-approve the IDP.
- In addition, the IDP Process Owner needs to review all active* files on an annual basis.

* Files which have not been used since dated for more than 3 months are considered not to be active.
4.5 Focus on Responsibility of the IDP Coordinator

Focus on responsibility of the IDP Coordinator

- The IDP Coordinator is responsible for coordinating the IDP Process within his Legal Entity respective area of responsibility.
- He facilitates that tools which are provided by IDP Business Support are used for identifying, classifying and assessing IDPs as well as taking inventory of the IDP files.
- He may be made responsible for carrying out controls to ensure compliance with the IDP Framework, therefore a Board Mandate is needed. If made responsible for controls, the following controls according to the IDP Control Catalogue need to be conducted:
  - Verification of categorization and classification,
  - control of approvals and required documentation,
  - verification of existence of decommission plan and
  - annual Confirmation.
- In addition, the IDP Coordinator collects the confirmation of the annual review from the Process Owner.
- He also supports the IDP Process Owner in fulfilling the control activities.
4.6 Storage, Back-up and Versioning

**Storage, back-up and versioning**

- In general, IDPs must be stored on company-controlled networks e.g. OneDrive or Sharepoint.
- IDPs must not be stored on your private drive (N: drive).
- If an IDP is stored locally a daily back-up must be undertaken.
- Versioning must be applied to IDPs.
- Not used files / temporary files shall be deleted respecting document retention periods.
5. Conclusion

5.1 Summary

Summary

While the purpose behind the laws and regulations on Individual Data Processing is easy to understand, the details can sometimes be confusing.

Keep in mind the following basic principles:

- Files containing formulas or codes are most probably an IDP file. They need to be classified and require further treatment if the information criticality is rated 'Major' and 'Critical'.
- Files in 'development' may only be used with test data and not in the day-to-day business.
- In case difficulties occur within the classification, the respective Process Owner (line manager) can be contacted for support.
- When using an IDP, a re-confirmation or respectively a re-evaluation is triggered periodically.
- 'Major' and 'Critical' IDPs need to be approved and the usage is only allowed after the approval. In addition, they require further documentation and management.
- All active files require an annual review by the Process Owner.

Always remember to follow the policies and procedures of Deutsche Börse Group and do not hesitate to contact IDP Business Support or the Master IDP Coordinator team for guidance.

5.2 Hints and Tips

Hints and tips

- If reclassifying a file, please make sure to access the file using the complete path and file name.
- You are not required to have Negligible or Minor classified files approved.
- The file does not move if the user moves / leaves the organisation. The file remains in the organisational unit where it was surveyed / saved.
- The responsibility for the file is with the IDP Process Owner.
- Consider if additional copies of IDP files are really needed before creating copies.
- Consider if sending the IDP file by email is required, send a SharePoint link instead.
- The list of programming / scripting languages to consider and include is available in the IDP Standard.
- Do not forget that an IDP outside of Excel or Access has to be identified using the FileTracker app.
- Regular housekeeping will keep IDPs manageable.
- Do not store the IDP file locally and remember to back-up the file daily.
5.3 Useful Links

IDP Standard
Information Security Framework and Governance Intranet
IRM Guideline
IDP Guideline
IDP Guideline Appendix