



Guidance for the Verification of Data Transition Processes

1. Exporting Data

1.1 Before

Execute a full system backup, and ideally a “disk image”. If possible, generate a complete dataset audit and write it to an audit file. Such functionality might be provided by standard Report tools available within the System. Also consider creating screenshots of critical sections of the data structure, such as collapsed high-level folders.

	date	comments
<i>system backup</i>		
<i>audit files</i>		
<i>screenshots</i>		

1.2 During

Monitor the export process for System-specific status reports and/or error messages, which might be displayed on screen, written to log files or sent as emails to nominated persons.

	date	comments
<i>status reports</i>		
<i>error messages</i>		

1.3 After

If possible, generate an audit of the exported dataset and write it to file. Compare the relevant physical dataset audits (or System reports) from BEFORE & AFTER – and look for discrepancies. Consider automating this process using known [utilities](#) or bespoke scripting (programming) in a language like [Perl](#).

If the exported dataset format is XML, check it at least for [Well-formedness](#) and ideally also for [Validity](#) if an accompanying XSD schema file is available. A variety of [tools](#) are available which can perform these [functions](#).

Consider manual spot-checks of the exported dataset (or its or audit file) against the original dataset in situ. If the original System is unavailable, spot-checks might still be possible via the [screenshots](#) of the original.

	date	comments
<i>audit files</i>		
<i>audit file comparison</i>		
<i>well-formed XML</i>		
<i>valid XML</i>		
<i>screenshot checks</i>		

Guidance for the Verification of Data Transition Processes

2. Data Conversion or Transformation

2.1 Before

Perform a full data backup. Generate a physical dataset audit and write full [File System directory](#) listings (eg. filenames, [extensions](#), byte counts, [timestamps](#)) to an audit file.

If the original dataset format is XML, check it at least for [Well-formedness](#) and ideally also for [Validity](#) if an accompanying XSD schema file is available. A variety of [tools](#) are available which can perform these [functions](#).

	date	comments
<i>data backup</i>		
<i>audit files</i>		
<i>well-formed XML</i>		
<i>valid XML</i>		

2.2 During

Monitor the conversion process for process-specific status reports and/or error messages, which might be displayed on screen, written to log files or sent as emails to nominated persons.

	date	comments
<i>status reports</i>		
<i>error messages</i>		

2.3 After

If possible, generate a new dataset audit and write it to an audit file. Compare relevant physical dataset audits from BEFORE & AFTER – and look for discrepancies. Consider automating this process using known [utilities](#) or bespoke scripting (programming) in a language like [Perl](#).

If the transformed dataset format is XML, check it at least for [Well-formedness](#) and ideally also for [Validity](#) if an accompanying XSD schema file is available. A variety of [tools](#) are available which can perform these [functions](#).

	date	comments
<i>audit files</i>		
<i>audit file comparison</i>		
<i>well-formed XML</i>		
<i>valid XML</i>		

Guidance for the Verification of Data Transition Processes

3. Copying and Transferring Data

3.1 Before

Generate a physical dataset audit and write full [File System directory](#) listings (eg. filenames, [extensions](#), byte counts, [timestamps](#)) to an audit file.

If the original dataset format is XML, check it at least for [Well-formedness](#) and ideally also for [Validity](#) if an accompanying XSD schema file is available. A variety of [tools](#) are available which can perform these [functions](#).

	date	comments
<i>audit files</i>		
<i>well-formed XML</i>		
<i>valid XML</i>		

3.2 During

Monitor the copy/transfer process for System-specific status reports and/or error messages, which might be displayed on screen, written to log files or sent as emails to nominated persons.

	date	comments
<i>status reports</i>		
<i>error messages</i>		

3.3 After

If possible, generate a new dataset audit and write it to an audit file. Compare relevant physical dataset audits from BEFORE & AFTER – and look for discrepancies. Consider automating this process using known [utilities](#) or bespoke scripting (programming) in a language like [Perl](#).

If the copied dataset format is XML, check it at least for [Well-formedness](#) and ideally also for [Validity](#) if an accompanying XSD schema file is available. A variety of [tools](#) are available which can perform these [functions](#).

	date	comments
<i>audit files</i>		
<i>audit file comparison</i>		
<i>well-formed XML</i>		
<i>valid XML</i>		

Guidance for the Verification of Data Transition Processes

4. Importing Data

4.1 Before

Generate a physical dataset audit and write full [File System directory](#) listings (eg. filenames, [extensions](#), byte counts, [timestamps](#)) to an audit file.

If the import dataset format is XML, check it at least for [Well-formedness](#) and ideally also for [Validity](#) if an accompanying XSD schema file is available. A variety of [tools](#) are available which can perform these [functions](#).

	date	comments
<i>audit files</i>		
<i>well-formed XML</i>		
<i>valid XML</i>		

4.2 During

Monitor the import process for System-specific status reports and/or error messages, which might be displayed on screen, written to log files or sent as emails to nominated persons.

	date	comments
<i>status reports</i>		
<i>error messages</i>		

4.3 After

If possible, generate a complete dataset audit and write it to an audit file. Such functionality might be provided by standard Report tools available within the recipient System.

Consider manual spot-checks of the imported dataset (or its or audit file / System report) against the import dataset (or its or audit file).

Even consider spot-checking the dataset within the recipient System against the [screenshots](#) of the original System.

	date	comments
<i>audit files</i>		
<i>audit file comparison</i>		
<i>screenshot checks</i>		