Guidance on Data Assurance Process and Risk Assessment of External Data Returns

# Background

Responsibility for oversight of a University framework for management and accountability of data quality of external data returns rests with the Data Assurance Group (DAG). DAG has developed a framework for managing and providing assurance on the quality of data included in statutory returns made by the University (mainly to the Office for Students, OfS, and the Higher Education Statistics Agency, HESA). The DAG data assurance toolkit comprises:

1. Guidance on Data Assurance Process and Risk Assessment of External Data Returns;
2. Data Returns Risk Assessment Template;
3. Data Returns Risk Register Template;
4. Data Returns Sign-Off Briefing Template.

This document (item 1 above) describes the data assurance process established and overseen by DAG and offers guidance on risk assessment and management in the context of external data returns.

# The Data Assurance Process

Data assurance is an important part of managing the activities of the University and in meeting the external reporting requirements which support accountability to funders and other stakeholders. The following chart shows the steps that form the data assurance process for external returns.

The Data Returns Risk Register Template needs to be completed for each statutory external data return and submitted for review by the DAG (step 2 above) prior to return compilation (step 3 above). This includes completion of the Data Returns Risk Assessment Template which feeds into the risk register.

The Data Returns Sign-off Briefing Template should be prepared for the officer/body signing off a return (often the VC – step 4 above). Sign-off briefings will need to be submitted to DAG for review only in case of a major change during the compilation process or a reportable event.

# Risk Management

Risk is inherent in any activity undertaken by an organisation. For commerce it is typically measured by using a cash focus. In Higher Education, with its wide range of activities it undertakes, risks are much wider than financial, often around reputation; these risks are typically more difficult to quantify than those that have a direct financial impact. This is particularly true for data, where outputs are produced after much processing of raw inputs. The perceived level of risk at Oxford is perhaps greater than at other HEIs due to the high profile of the University. A framework providing an objective view of risk can help maintain an appropriate focus on the range and depth of control needed to provide assurance over data produced by the University. This document specifically focuses on risk related to external data returns. More information about risk and the University’s risk management framework beyond data returns is available on the [University website](https://compliance.web.ox.ac.uk/risk-management#/).

Risk management is a methodology to provide a framework for assessing risk and reducing the effect of undesirable events. At a basic level, there are three stages:

1. assessing risk (gross risk);
2. managing risk (resulting in a net risk);
3. developing response plans on the net risk where appropriate.

## Two Types of Risk

When it comes to external data returns, we distinguish two types of risk associated with each return: A ‘data risk’ and a ‘financial/reputational impact risk’.

The ‘data risk’ is the risk that the data submitted in the return are incomplete or flawed. It has a number of dimensions including but not limited to the volume and quality of source data, knowledge and expertise around return preparation, and IT aspects of processing the return. Inaccurate data returns do not necessarily have severe consequences for the University.

Some (though not all) statutory data returns may have significant impacts if they are incomplete, materially wrong or failed to be submitted on time. Negative consequences of an inaccurate data return can be financial (e.g. affecting funding grants) or reputational (e.g. influencing performance indicators; being analysed in the media). We label the risk of such consequences the ‘financial/reputational impact risk’.

From a data assurance perspective, the ‘data risk’ is of particular interest to understand the risk that a certain return may be inaccurate. From a wider risk management perspective, a ‘financial/reputational impact risk’ is relevant in focusing scrutiny on those critical returns where the negative consequences of failure would be most severe. The ‘data risk’ drives the likelihood of a negative impact and the risk register and risk assessment templates cover both types of risk.

## Assessing Risk

The risk assessment process should be undertaken in advance of the start of the preparation of the return, ideally taking into account any guidance for the return and experience from previous years (including any annual reports or reviews such as the sign-off briefing).

Risk is typically assessed through gauging the likelihood of a negative outcome using a number scale multiplied by the impact (or consequence) of that outcome occurring.

The Data Returns Risk Assessment Template should be used in order to determine both the ‘financial/reputational impact risk’ as well as the ‘data risk’ (step 2 of the process outlined above). The template contains further advice on how to assess the appropriate levels of impact and likelihood. The result should then be referenced in the Data Returns Risk Register Template (step 2) which, alongside the Risk Assessment Template, will need to be reviewed by the Data Assurance Group (step 2) in advance of the return compilation (step 3).

## Managing Risk

Rehearsal of risk management practice is intended to ensure that risks (gross and net) are being assessed in an objective way, and to ensure that risk reduction activities are in keeping with the level of risk encountered. They should be proportionate and cost effective.

Activities designed to manage risk can be general (e.g. ensuring inputs are valid for the student records system, used for a number of specific purposes) or specific, addressing a specific problem. Management activities should be appropriate to the specific risk which is being addressed.

In risk management there are four generally accepted ways of managing risk. These are:

* **Avoid** – not undertaking the activity that incurs the risk. This is often not an option for the returns under consideration as they are mandatory and relate to being in the business of higher education.
* **Reduce** – to put into place actions that reduce the likelihood of the risk. Control processes that occur as part of the compilation of the return or independent challenge on the completed return are methods of reducing risk.
* **Transfer** – typically this is insurance for financial risks or outsourcing activity where there is insufficient expertise within the organisation.
* **Accept** – tolerate the risk, setting aside funds or capacity to manage a negative outcome. This may be necessary for net risk (i.e. after reduction strategies have been employed). Contingency can reduce the impact of a risk (e.g. insolvency in a commercial environment). For data returns this may be an audit by the OfS or some other body. Sometime these are periodic, other times reacting to a difference from expectation. This has an opportunity cost in terms of what the funds could otherwise be used for.

Should this be the chosen option then a response plan is typically required. The level of detail and timetable for remedial action in the plan should be in line with the net risk. (This might look like: low risk requires monitoring only; medium risk indicates implementation of action in time for next return; high risk requires the cause of the assessment to be addressed prior to commencement of the preparation of the next return).

Risk management should be a useful tool but care needs to be taken that it does not begin to dominate the process of compiling a return. Deadlines for data returns in the sector are pretty strict and it can be better to accept, rather than attempt to eliminate, a risk if the action identified will delay the return unduly, as such a delay may in itself constitute a risk. Also, the lower the ‘financial/reputational impact risk’ of a return, the higher a ‘data risk’ may be acceptable.

In the context of data returns, most actions will be categorised as reduction of likelihood. The range and number of methods used to reduce the gross risk can be adjusted in line with the assessment: the higher the gross risk, the more risk controls should be applied.

The list below outlines some key areas of mitigating actions available to reduce the ‘data risk’. This corresponds to Section C.II of the Data Returns Risk Register which requires details on risk controls in place, proportionate to the identified gross data risk.

|  |
| --- |
| **Skills, Knowledge and Experience** (corresponds to item 10 on the risk register template) |
| The skills, knowledge and experience required to successfully complete an external data return vary depending on the level of gross risk of the return, driven by risk assessments for the various dimensions determining the gross risk (see Data Returns Risk Assessment Template). A return with a medium ‘data risk’ may still require significant levels of expertise to guarantee completion. Some risks, e.g. around IT infrastructure, may be transferred/outsourced but the person responsible for completion of the return will still need to ensure the required expertise is maintained.Appropriate staffing levels and expertise are key to mitigating risks. The higher the level of gross data risk, the more important are the skills, knowledge and experience of the staff responsible for the return. In particular, single-points-of-failure need to be avoided for returns requiring high levels of expertise. |
| **Procedural Guidelines** (corresponds to item 11 on the risk register template) |
| All guidelines should be followed with a critical eye, noting any changes in the requirements of the return and a review of the accuracy of the previous year’s outcomes. This might include the recommendations from internal or external audit.With increasing levels of gross data risk, guidance and their regular review will need to become more detailed to manage risks appropriately. This will be particularly relevant for those dimensions of the Data Returns Risk Assessment Template with the highest risk. |
| **Process to ensure Completeness and Accuracy** (corresponds to item 12 on the risk register template) |
| Depending on the level of risk, (some of) the following processes can be incorporated to ensure completeness and accuracy of the data returned:* Reasonableness checks: Outcomes of compilation are in line with expectations, e.g. previous return adjusted for known changes in activity, e.g. significant expansion of particular course types
* Drawn from a central data source (e.g. student records or finance system) with its own built-in checks)
* Exception reports:
	+ Missing data lines (e.g. student) or duplication (perhaps with difference identifiers)
	+ Missing data items (e.g. year abroad information)
	+ Non valid data (e.g. part time student with 1 FTE)
* Sample checks:
	+ Random selection of data lines compared with another data source; could be small
	+ Periodic review of data manipulation processes, e.g. those that combine data from more than one source; the frequency of the review might depend on the criticality of the process to the compilation of the return, but not expecting that every process will be reviewed in detail each year.
* Review by external body, e.g. funding or research council, of processes used for compilation

All checks should be reviewed to ensure that they are addressing, as intended, the risk to which they relate. |
| **Cross-checks with Other Returns** (corresponds to item 13 on the risk register template) |
| * Low gross data risk: High-level review against previous returns
* Medium gross data risk: Comparison against previous return in more depth and high level review against other returns where possible
* High gross data risk: Comparison against previous return and other returns in greater depth where possible
 |
| **Review, Challenge and Authorisation Process** (corresponds to item 14 on the risk register template) |
| The higher the level of gross data risk, the more robust and independent should the review and challenge be.* For returns with a low gross data risk, a ‘light-touch’ version of the risk register may be completed for review by the DAG where not all sections are compulsory (see Data Returns Risk Register Template); independent challenge of the return can be kept at a low level (e.g. by a person senior to the compiler with an understanding of the purpose and aims of the return).
* Medium gross data risk: Review by a person senior to the compiler with an understanding of the purpose and aims of the return, prior to submission. This should be someone who has not been involved in the compilation. Completion of a data risk register and submission to DAG.
* Returns with a high gross data risk will need to ensure more robust processes to review and challenge the return (e.g. through an oversight group or challenge provided by someone outside the section where the return was compiled). This is particularly true for returns where not only the gross data risk is high but where also the ‘financial/reputational impact risk’ is medium/high. For those returns with the highest ‘financial/reputational impact risk’, a member of the DAG will provide external challenge.
* There may be external requirements for Committee and/or Accountable Officer (VC) sign-off before or after submission.
 |

Where such controls have been undertaken they should be recorded, and an outline included in the risk register as well as the sign-off briefing.

In order to assess the net risk, the activity should be re-scored (using the Risk Assessment Template), taking into account the control and review processes that will have occurred in the intervening period. The net risk is then recorded in Section C.III of the Risk Register Template.

## Response Plans

Due to the time constraints on compiling a statutory external return, it may be necessary to accept the risk of potentially material inaccuracies in data (data risk), depending on the consequences this might have for the University (negative impact risk). Where such inaccuracies are significant they may prompt an audit by the relevant external body even if there are no further negative financial or reputational consequences. Errors may also be regarded as requiring improvement for internal management information reasons. In these cases it may be helpful to produce an outline plan of action for improvement for future returns (to some extent, this is captured in box 17 of the Data Returns Risk Register Template, prompting consideration of future improvements).