**TERMS OF REFERENCE FOR INTERIM ACCREDITATION AUDITS OF INTEGRATING AUTHORITIES**

1. **Background**
	1. In October 2010, Commonwealth Portfolio Secretaries endorsed a set of [governance and institutional arrangements](http://www.nss.gov.au/nss/home.nsf/NSS/00FB7E20E1D56B96CA2577F20016C3DB?opendocument) for the safe and effective use of Commonwealth data in data integration projects for statistical and research purposes. The governance and institutional arrangements aim to ensure that data integration involving Commonwealth data is done safely (e.g. the personal information of people and business is kept confidential) and effectively (e.g. as much existing data is used for statistical and research purposes that benefits the public, as possible). These arrangements require that authorised integrating authorities are accredited to undertake ‘high risk’ projects. For information about how data custodians determine the project risk rating please see the document “[Commonwealth data integration projects – how to determine risk leve](http://www.nss.gov.au/nss/home.NSF/pages/Data%2Bintegration%2Bprojects%2B%E2%80%93%2Bhow%2Bto%2Bdetermine%2Bthe%2Brisk%2Blevel?opendocument)l” on the National Statistical Service website.
	2. The interim accreditation process for integrating authorities requires an independent **audit** as one of the steps. The steps in the interim accreditation process are: self-assessment; audit; decision; and publication of list of accredited agencies.
	3. A Cross Portfolio Data Integration Oversight Board, chaired by the Australian Statistician, has been established with membership of three Portfolio Secretaries: Health; Human Services; and Social Services.
	4. A Secretariat (the Cross Portfolio Data Integration Secretariat), housed in the Australian Bureau of Statistics, is coordinating the interim accreditation process.
	5. There are eight criteria integrating authorities must meet to gain interim accreditation:
2. ability to ensure secure data management;
3. Integrating authorities must demonstrate that information that is likely to enable identification of individuals or organisations is not disclosed to external users;
4. availability of appropriate skills;
5. appropriate technical capability;
6. lack of conflict of interest;
7. culture and values that ensure protection of confidential information and support the use of data as a strategic resource;
8. transparency of operation; and
9. appropriate governance and administrative framework.

See Appendix 2 for full details of what each criterion means.

1. **Purpose**
	1. The audit services required are compliance audits as part of an interim integrating authorities accreditation process. The interim accreditation process is outlined in Appendix1.
	2. The objective of the audit is to provide assurance to the Cross Portfolio Data Integration Oversight Board that the applying integrating authority meets the interim accreditation criteria.
	3. Prior to the audit integrating authorities apply for interim accreditation by preparing a self-assessment report explaining how they meet the criteria for interim accreditation. The function of the audit is to ensure the integrating authority’s self-assessment report is substantiated by the evidence supplied and satisfies the eight criteria requirements.
2. **Integrating authority responsibilities**
	1. The integrating authority is responsible for the costs of the audit.
	2. All integrating authorities applying for interim accreditation are obligated to engage a qualified auditor for the provision of auditing services as part of the interim accreditation process and in accordance with its internal procurement procedures.
	3. Each integrating authority seeking an audit will assign a representative who will be the single point of contact, for all matters. The integrating authority will ensure that this person provides continuity of service for the duration of the audit.
	4. The integrating authority should ensure access to all facilities, documentation and staff appropriate to the scope of the audit outlined within their self-assessment submission.
3. **Auditor responsibilities**
	1. It is expected that the auditor will work in cooperation with the Australian National Audit Office (ANAO) and its nominated external audit service provider, and other relevant representatives as required. The audit will be carried out in accordance with the ANAO auditing standards.
	2. The audit approach is a matter for professional judgment of the auditor. However, to ensure consistency across audits and integrating authorities, the Secretariat would normally expect the audit approach to include the steps outlined below.
4. Planning: Prior to the start of audit work the **auditor** will be required to inform the Secretariat of work being undertaken. If an integrating authority can demonstrate that a **suitable program of audits** has been done recently (in the two years prior to the application), these audits can be used to reduce the scope of the integrating authority interim accreditation audit. Prior to the commencement of the audit, copies of any previous relevant audit reports must be obtained by the auditor.
5. Fieldwork: For this compliance audit most criteria may be sufficiently assessed through sighting of documentation, discussion and observation rather than detailed testing. However non-compliant criterion may require more detailed testing to provide quality assurance. The auditor may undertake an audit visit to the integrating authority’s organisation to personally assess compliance. Relevant evidence includes:
	* internal and external audit program relevant to the criteria;
	* governance, legislation and policy documentation;
	* documented procedures to assess whether they are consistent with requirements;
	* relevant training;
	* facilities;
	* organisational expertise through evidence of relevant staff and project experience; and
	* public communications including publications and website material.
6. Draft Report: A copy of the draft report should be submitted to the integrating authority and the Secretariat.
7. Provision of integrating authority management comments: The auditor will amend the report as appropriate to include comments from the integrating authority.
8. Final Report: The final report will be submitted to the integrating authority and to the Cross Portfolio Data Integration Oversight Board via the Secretariat email. The auditor should provide a comprehensive report. The report information should include:
	* an executive summary including introduction, audit objectives, scope, methodology; summary conclusion;
	* compliance summary\* for each criteria;
	* audit findings and recommendations;
	* a list of the key documents examined, integrating authority representatives participating in the audit and audit team members and hours utilised.

*\*Compliance Summary -* The report should provide a table that summarises the compliance rating using the compliance rating scale in Table 1 below.

**Table 1**

|  |  |  |
| --- | --- | --- |
| Name  | Rating  | Description  |
| COMPLIANT  | 3 | Compliant - no further action required  |
| PARTIALLY COMPLIANT  | 2  | Improvements are required in order to meet criteria requirements |
| NON-COMPLIANT  | 1 | Does not meet criteria requirements  |

**APPENDIX 1 - Proposed process for interim accreditation of integrating authorities with the capacity to do high-risk data integration projects**

The process for interim accreditation of integrating authorities involves:

1. *Self-assessment*. Integrating authorities apply for interim accreditation by preparing a self-assessment report explaining how they meet the criteria for interim accreditation. The assessment must be signed off by the agency head or the application will not be considered.
2. *Audit*. An independent third party audits the integrating authority’s self-assessment against the criteria, in line with the ANAO Auditing Standards. If an integrating authority can demonstrate that a suitable program of audits has been done recently (in the two years prior to the application), these audits can be used to reduce the scope of the integrating authority interim accreditation audit. The Secretariat will manage the audit process on a fully cost-recovered basis.
3. *Decision.* The Cross Portfolio Data Integration Oversight Board will make the final decision on interim accreditation, based on the self-assessment and results of the audit. Once a decision is made, a full report explaining the compliant and non-compliant criteria, with recommendations for what needs to change, will be supplied to the applicant.
4. *Publication of list of accredited agencies*. The Secretariat will publish a list of accredited integrating authorities on the web, together with a summarised version of the integrating authority’s application and a summary of the audit report.

**APPENDIX 2 - Interim accreditation criteria for integrating authorities wishing to be endorsed as capable of doing high risk data integration projects**

There are eight criteria that integrating authorities must meet to gain interim accreditation:

1. ability to ensure secure data management;
2. integrating authorities must demonstrate that information that is likely to enable identification of individuals or organisations is not disclosed to external users;
3. availability of appropriate skills;
4. appropriate technical capability;
5. lack of conflict of interest;
6. culture and values that ensure protection of confidential information and support the use of data as a strategic resource;
7. transparency of operation; and
8. appropriate governance and administrative framework.

***i) Ability to ensure secure data management***

Integrating authorities seeking interim accreditation must demonstrate that they have secure data management systems in place to protect data both during and after integration, including systems for the safe exchange of sensitive data across agencies. This may include secure management of metadata or software programs to protect intellectual property, as negotiated with the data custodian(s). Agencies who demonstrate they meet Australian Government standards for security practices as set out in the [***Australian Government Protective Security Policy Framework***](http://www.ag.gov.au/pspf) would automatically be rated suitable on this criterion, provided that they can also demonstrate that they adhere to the separation principle and that they have an ongoing program of audits to ensure the continued security of the data. Agencies who cannot meet all the requirements in the Framework would need to comply with particular aspects, including control of access to the agency’s premises and police checks for staff.

***ii)***  ***Integrating authorities must demonstrate that information that is likely to enable identification of individuals or organisations is not disclosed to external users***

Integrating authorities seeking interim accreditation must be able to demonstrate that information that is likely to enable identification of individuals or organisations is not disclosed to external users. Removal of identifying information will not be sufficient. Integrating authorities must ensure that information is only released in a way that is not likely to enable identification, either directly or indirectly, of individuals or organisations. Examples of different ways this criterion can be met include:

* use of formal confidentiality algorithms; and/or
* use of statistical disclosure control techniques such as cell suppression and perturbation; and/or
* providing access to data that are not likely to enable identification of individuals or organisations via on-site data laboratories; and/or
* providing access to data that are not likely to enable identification of individuals or organisations via secure remote access facilities; and/or
* manual review of data by staff with appropriate skills prior to any data release.

As an additional protective measure, integrating authorities may restrict access to data that are not likely to enable identification of individuals or organisations to approved applicants.

***iii) Availability of appropriate skills***

An integrating authority seeking interim accreditation will need to have a high level of relevant skills to undertake high risk data integration projects or be able to show how they can gain these skills (e.g. secondment provisions, training). Relevant skills include:

* expertise in linkage and merging functions
* expertise in privacy (for example, the ability to conduct a [Privacy Impact Assessment](http://www.privacy.gov.au/materials/types/download/9509/6590))
* expertise in confidentiality
* information management skills
* ability to provide useful metadata to data users
* appreciation of data quality issues to allow the integrating authority to provide advice to stakeholders.

This may be evident in the experience of staff undertaking the integration projects and in the provision of training and documentation to support the integration projects.

***iv) Appropriate technical capability***

To obtain interim accreditation an integrating authority must have the necessary technical expertise and infrastructure, including secure hardware and software systems and system support, to undertake high risk data integration projects. Two factors that the integrating authority’s technical infrastructure will need to handle are the size of an integrated dataset (use of administrative data can result in very large files) and its complexity (e.g. maintaining a link that may be longitudinal or cross-sectional). The expertise and infrastructure required also extends to data access arrangements to maximise the public benefit of data integration.

***v) Lack of conflict of interest***

The Commonwealth Statistical Integration Principles state that statistical data integration must be used for statistical and research purposes only. Agencies with a regulatory function or with responsibility for compliance monitoring must demonstrate how they will address a potential conflict of interest if linked datasets could help them with these non-statistical purposes. Possible ways an agency may demonstrate a lack of conflict of interest include the use of some legally enforceable obligation, policies, and separation principles (e.g. restricting access so that staff with regulatory/compliance roles cannot access data which would enable list matching).

***vi) Culture and values that ensure protection of confidential information and support the use of data as a strategic resource***

Integrating authorities seeking interim accreditation will need to demonstrate a consistently high standard of behaviour by all employees, commensurate with an agency statement equivalent to the APS Code of Conduct. Security needs to be part of the agency’s culture. Staff working on data integration also need to value data as a strategic resource. Examples of how this standard may be demonstrated include:

* a culture of protecting identifiable information
* adequate training on security/privacy/confidentiality matters
* appropriate mechanisms to consult with stakeholders (data custodians, data users and the public).

***vii) Transparency of operation***

To maintain public trust, use of government data, particularly in data integration projects for statistical and research purposes, must be open and transparent. Integrating authorities seeking interim accreditation will need to demonstrate the transparency of their operations, including the ability to apply sanctions. This may be evidenced by:

* their legislation and policies, particularly in relation to their implementation of Gov2.0 recommendations which focus on increased openness in government
* mechanisms to consult with and inform the public and key stakeholders about projects that are underway (e.g. via publications, presentations at conferences, focus groups)
* publishing relevant material on the web e.g. data retention statements.

***viii) Appropriate governance and administrative framework***

An integrating authority must have frameworks in place for management of cost recovery (if applicable), conducting investigations and handling of complaints. An integrating authority must also demonstrate that they have appropriate institutional and project governance in place. Examples include Chief Executive Instructions and a Control Framework.

**APPENDIX 3: Signing page and template for applicants to complete**

Applicants wishing to apply for interim accreditation to undertake data integration projects involving Commonwealth data will need to complete the following template. They will need to attach additional supporting information (e.g. copies of relevant policies and procedures, a copy of the corporate plan, evidence of compliance with the Australian Government Protective Security Policy Framework) to help the Oversight Board and auditor make an assessment.

When making a decision about whether or not to apply for interim accreditation, integrating authorities will need to consider whether they are likely to have the authorisation required for projects they are contemplating. This will involve discussing obligations and requirements with the data custodian(s).

**Applications must be signed off by the agency head[[1]](#footnote-1) or they will not be considered.**

**Contact officer details**

|  |
| --- |
| **This assessment has been completed by:****Name:****Organisation:****Contact telephone:****Signature:****Date:** |

**Sign-off by agency head1**

I have undertaken sufficient review and investigation to ensure in my opinion that the answers and information provided are accurate, and that my organisation has the necessary values, skills and infrastructure to ensure data integration involving Commonwealth data for high risk statistical and/or research projects is carried out in a safe and effective way.

**Signature: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Name** (block letters)**: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Email this form to the data integration secretariat, email:** **statistical.data.integration@nss.gov.au**

|  |
| --- |
| **Criterion I – Ability to ensure secure data management**  |
| I(a) How does your agency adhere to the separation of identifying and content data? Provide details of how only that information, from datasets to be linked, that is required to perform specific tasks is made available to those people performing the tasks. Specifically: * linking separation (where those people performing the linking of the datasets can only access those parts of the datasets to be linked that are required to complete the linkage)
* analysis separation (where those people performing analysis of the linked datasets can only access those parts of the datasets required for the analysis).
 |
| I(b) How does your agency’s audit program (internal and external) ensure the continued security of data?  |
| ***NOTE: If your agency complies with the*** [***Australian Government Protective Security Policy Framework***](http://www.ag.gov.au/pspf) ***(and can demonstrate this to the auditor) the remaining questions under criterion 1 do not need to be answered. Go to question IIa. Otherwise, please complete the following questions.*** |
| I(c)Do employees (including contractors) undergo police checks upon employment? |
| I(d) How is access to your agency’s premises controlled? |
| I(e) How is your agency’s Internet gateway secured? |
| I(f) Does your agency have an Information Security Policy and procedural plan (including protective control of data, secure ICT access and documented procedures)? Please specify key elements of your Information Security protocols. |
| **Criterion II – Integrating authorities must demonstrate that information that is likely to enable identification of individuals or organisations is not disclosed to external users**  |
| II(a) How will safe data access be provided? Please provide details of the proposed method. For example:* providing access to data that are not likely to enable identification of individuals or organisations via on site data laboratories
* providing access to data that are not likely to enable identification of individuals or organisations via secure remote access facilities
* review of data by appropriately skilled internal staff to ensure data is appropriately confidentialised before release
* provision of only confidentialised files to users (e.g. using formal algorithms to apply confidentiality)
* other - specify.

As an extra protection, in addition to one of the methods above, integrating authorities may also restrict access to endorsed applicants (similar to the [restrictions placed on access to Confidentialised Unit Record Files by the ABS](http://www.abs.gov.au/websitedbs/D3310114.nsf/home/CURF%3A%2BApplying%2Bfor%2BCURF%2BMicrodata), for example).***NOTE: Any of these options is acceptable provided the applicant can demonstrate safe practices. The application will need to include details of how the*** ***integrating authority confidentialises data.*** |
| **Criterion III – Availability of appropriate skills** |
| III(a) What expertise and experience does the agency have to undertake high risk data integration projects? If your agency does not have this expertise or experience, what strategies are in place to acquire the necessary expertise to undertake a high risk integration project?***NOTE: Relevant skills to consider include: expertise in linkage and merging functions; expertise in privacy; expertise in confidentiality; information management skills; ability to provide useful metadata to data users; and appreciation of data quality issues.*** |
| III(b) What documentation and training is available to ensure staff have the appropriate skills and knowledge required in high risk data integration projects? |

|  |
| --- |
| **Criterion IV – Appropriate technical capability** |
| IV(a) Does your agency have secure IT infrastructure, including hardware and software systems, and the capacity to support the potentially large and/or complex files associated with high risk data integration projects? Give a brief evidentiary statement. |
| IV(b) How does the system track access and changes to data to allow audits by date and user identification? Does the system 'footprint' inspection of records and provide an audit trail?  |
| IV(c) What IT support is in place for staff? |
| **Criterion V – Lack of conflict of interest** |
| V(a) Does the agency have a compliance monitoring or regulatory function? If yes, describe how this function will be separated from integration projects undertaken for statistical and research purposes to avoid this conflict of interest. |
| **Criterion VI – Culture and values that ensure protection of confidential information and support the use of data as a strategic resource** |
| VI(a) How is an appropriate culture and values embedded in the agency’s corporate plan/mission statement/policies etc?  |
| VI(b) How have staff been trained in requirements for protecting personal information and how are they made aware of policies regarding breaches of security or confidentiality?  |
| VI(c) Do staff sign undertakings related to secrecy and fidelity? |
| VI(d) What mechanisms are in place to engage with stakeholders to maximise the usefulness of the data holdings?  |
| VI(e) How does your agency provide for valuable use of the data, i.e. how does it maximise the value of data for users by providing them with access to as much data as possible while still protecting confidentiality? |
| **Criterion VII – Transparency of operation** |
| VII(a) Are data retention and data disposal statements publicly available? Provide details. |
| VII(b) Are details of governance arrangements publicly available? Provide details. |
| VII(c) Where are details of data integration projects published? |
| VII(d) What other relevant material is published? Examples include data protocols such as microdata access protocols, confidentiality protocols, protocols for linking and protecting privacy; and data integration manuals. |
| **Criterion VIII – Existence of an appropriate governance and administrative framework** |
| VIII(a) What are the institutional and project-specific governance arrangements for data integration? (Provide attachment or link to where published.)  |
| VIII(b) What framework is in place to conduct investigations and handle complaints for data integration projects? |

1. The ‘agency head’ is the person legally accountable for the activities of the organisation, and those of its staff and affiliates. In the case of a government department, this will be the Secretary of the department. For the private sector, it will be the CEO, Company Secretary or Managing Director. For a university, it will be the Vice-Chancellor, Pro Vice-Chancellor, Deputy Vice-Chancellor or University Registrar. [↑](#footnote-ref-1)