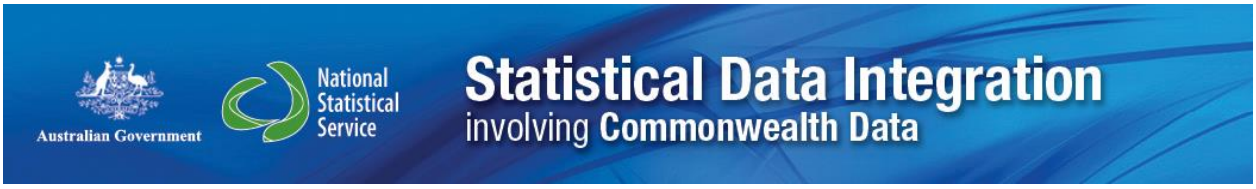

Application for accreditation as an Integrating Authority against the interim accreditation scheme

Summary version

Applicant:	Australian Institute of Family Studies (AIFS)
Auditor:	Deloitte Touche Tohmatsu
Date accredited:	11 November 2014

The summarised application can be found on the following pages of this file.
For further information about the application contact:

The Cross Portfolio Data Integration Secretariat

Phone (02) 6252 7198

Email: statistical.data.integration@nss.gov.au

Criterion I – Ability to ensure secure data management

Auditor rating against criterion I – compliant

I(a) How does your agency adhere to the separation principle? 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).

An important strategy used at AIFS to further limit access to sensitive data is to compartmentalise data processing roles during data integration using the separation principle. The internal separation principle is a practical way to limit access by compartmentalising data processing roles within the Data Management Integration Team (DMIT) (those who do the linking) and between the DMIT and researchers (those who do the analysing) to ensure that no person has access to the confidential details in the linked dataset during or after dataset linkage.

For all data integrations, a minimum of four DMIT members is required (this will increase by 1 person for each additional dataset that is to be integrated). Each dataset will be sent to only one team member. Access will be granted to only that person in accordance with AIFS' policy.

Members that initially receive the data (Person 1 & 2) will extract the identifying information and send only this information to the "linkage key creator" (Person 3). Person 3 will combine the identifying information from the separate datasets in order to create unique linkage IDs for all respondents in the data files. The identifying information and the linkage IDs will be returned to Person 1 and 2 and the linkage IDs will be added to the file.

Person 1 and 2 will remove the identifying information from their files and send only the linkage ID and the non-identifiable data items to Person 4 (the merger). The "merger" will merge the datasets together, confidentialise the data, assign new unique random IDs to the dataset and remove the linkage IDs. This means only Person 1 and 2 would be excluded from any analysis on the new combined dataset. Person 3 could be an analyst, but because the linkage IDs are removed and replaced by new IDs, Person 3 would not be able to identify any individual case.

In this way, access to identifying information is restricted to a specialised DMIT where delegated persons have access to perform the steps only relevant to their role. Researchers are only involved in the last step and therefore do not need, and cannot access, any personal identifying information. At no point in the process does an individual have access to the linked dataset with identifying variables. Persons 1 and 2 will similarly be excluded from all research or analysis with the linked de-identified dataset.

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 (and can demonstrate this to the auditor) the remaining questions under criterion I do not need to be answered so proceed to question IIa. Otherwise, please complete the following questions.

AIFS is required to adhere to the Australian Government Protective Security Policy Framework (PSPF), in accordance with guidelines published by the Attorney-General's Department.

Internal audits
The Institute also conducts an annual review of its Protective Security Policies and Procedures to assess compliance with the PSPF.

External audits
The Australian National Audit Office (ANAO) undertakes an annual statutory audit of AIFS' financial statements.

Structured risk assessment procedures

Prior to any project beginning at AIFS, a structured risk assessment is required for executive approval. Data Integration projects undertaken in the future will also require a risk assessment to be undertaken. The risk assessment will follow the risk assessment framework provided by the National Statistical Service. The AIFS Ethics Committee will assess proposed data integration projects to balance the benefits of a project with any risk to privacy. AIFS Ethics Committee clearance is required for all proposed research and data integration projects.

All data integration projects at AIFS will be assessed using the National Statistical Service (NSS) guidelines for assessing risk, which are structured into the following dimensions of risk:

Identification— Risk increases as the probability of an individual being identified through a combination of quasi-identifying and other variables on a dataset increases.

The risk of identification is a factor that must be taken into consideration in each of the remaining dimensions.

Sensitivity—Risk increases if datasets in the proposed integration project contain sensitive personal information such as details of religious belief, health, crime or any other sensitive information.

Amount of information about data provider—Risk increases if the project contains a large number of quasi-identifying variables and large numbers of other variables.

Challenges of appropriately confidentialising information — Risk decreases if publishing simple aggregated data with basic confidentialisation required.

Managerial complexity—Risk is increased when data sources are obtained from multiple agencies, organisations or jurisdictions, or where high numbers of staff are required for integration.

Duration of the project—Risk increases when a linked dataset is held, maintained or updated for long periods. Risks may be decreased if a project is short term and if the linked dataset is destroyed after analysis.

Data provider consent—Risk is decreased if consent has been obtained by data providers for use of their personal information for data integration.

Data access—The risks of disclosure are higher if access to identified or identifiable data is required for integration. Risks are also increased with the number of organisations requiring access to the data, the length of time the access is required or when international groups or agencies require access.

To further ensure that risk is being properly assessed at AIFS, the DMIT will undertake an annual audit of all data integration projects managed at AIFS to ensure that all processes and protocols are being followed and that risk is being appropriately assessed for every dataset. As part of compliance to the Protective Security Policy Framework, AIFS is required to have annual audits performed on data stores in AIFS possession.

I(c) Do employees (including contractors) undergo police checks upon employment?
Yes. Since AIFS first reported its PSPF compliance as at July 2013, all AIFS employees, contractors and temporary staff who require ongoing access to Australian Government information and resources must be: eligible to have access; have had their identity established; suitable to have access; and willing to comply with AIFS' policies, standards, protocols and guidelines that safeguard AIFS' resources (people, information and assets) from harm.
I(d) How is access to the agency's premises controlled? Provide details.
Access to AIFS offices is only possible through AIFS swipe cards. Visitors must sign in and out at reception, wear a visitor pass and be escorted by an authorised AIFS staff member at all times. Access to the "data lab" is restricted on a need to know and need to go basis, with unescorted access granted to ICT and DMIT staff only.
I(e) How is your agency's Internet gateway secured?
The Institute currently uses an in-house managed gateway which has had its configuration checked by an assessor from the Information Security Registered Assessors Program (IRAP) and undergone an IRAP penetration test. The gateway has been accredited by AIFS to the PROTECTED level.
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.
Yes, AIFS has an Information Security Policy that covers: Security Principles Legislative Requirements, Standards and Guidelines Roles and Responsibilities of System Owners and Information Owners and Employees Operational Responsibilities Need to Know Data Aggregation Disciplinary Actions

Further, AIFS has an ICT Security Policy that covers:

Acceptable Use
Third Party Access and Outsourcing
Asset Classification, Control and Handling
Personnel Security
Physical and Environmental Security
Communications and Operations Management
Access Control
System Development and Maintenance
Incident Management
Emergency Procedures
Business Continuity Management
Legal Compliance

Criterion II – IAs must demonstrate that information that is likely to enable identification of individuals or organisations is not disclosed to external users

Auditor rating against criterion II – compliant

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, IAs may also restrict access to endorsed applicants (similar to the restrictions placed on access to Confidentialised Unit Record Files by the ABS, 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 IA confidentialises data.

AIFS has seven protective protocols in place to ensure the identification of individuals or organisations in AIFS-administered datasets is not possible.

1. All unit record files are de-identified and confidentialised where appropriate.
2. Access to unconfidentialised and confidentialised unit record file data is granted by the Data Owner/ Custodian and only on a need-to-know basis.
3. Access to unit record file data is granted on a need-to-know basis and only granted by the Data Owner/ Custodian.
4. Access to unit record file data is only ever granted to users for purposes agreed to by the Ethics Committee.

5. Users of AIFS-administered datasets are subject to penalties for disclosure of any information on individuals and must sign the undertakings contained in the data access application form.
6. Data released from AIFS is released in a form that will make identification unlikely through confidentialisation and de-identification.
7. Output of researchers is regularly assessed to ensure that only aggregate data, which does not pose a risk of disclosure, is released.

The above risk managing steps ensure that:

- Access to unit record file data is restricted to a need-to-know basis.
- Unit record file data cannot be matched, in whole or part, with any other information or data for the purposes of attempting to identify individuals, and that no attempt to identify an individual can be made.
- The AIFS employee will not disclose or release the information to any other person or organisation, except as statistical information that does not identify an individual.
- The information is only used for statistical purposes relevant to the *Family Law Act 1975*, which authorises AIFS to conduct, encourage and coordinate research relevant to Australian families.
- The information will not be used as a basis for any legal, administrative or other action that could directly affect any particular individual or organisation as a result of their identification in a particular project.

Storage

The data will be encrypted and password protected using AES-256 bit encryption and compliant with the complexity as specified in the Password Policy. During the linking process the data will be only accessible to the appropriate DMIT member. After use the data will be confidentially destroyed.

Confidentialisation

Policies and protocols in place at AIFS ensure that appropriate confidentialisation procedures are followed at all times. Confidentialisation is a broad term used to describe the process of removing, aggregating or amending personal information that might enable direct or indirect identification in datasets. Data are risk assessed and evaluated for the potentiality of a privacy breach and de-identified and confidentialised prior to analysis and release.

Data confidentialisation can be categorised into two broad areas based on the type of data that is to be confidentialised: (1) micro-data confidentialisation; and (2) aggregate data confidentialisation. The techniques used to confidentialise micro-data and aggregate data are similar, however the way risks are assessed and data are amended are different.

Some possible methods include:

- aggregating geographic coverage;
- rounding;
- grouping or combining categories;
- top- (or bottom-) coding;
- imputing values from a model;
- suppressing fields or cells;
- suppressing variables; and
- time delay.

Micro-data confidentiality techniques are applied to data items within individual unit records that are identified as a risk to privacy before aggregation or analysis.

Aggregate data refers to micro-data that has been aggregated. Aggregate data are usually displayed in the form of tables, graphs and maps. Confidentiality techniques for aggregate data are applied to cells in a table that are identified as a risk to privacy after aggregation.

The two primary methods used in the Institute to confidentialise data are (1) data perturbation; and (2) data reduction methods.

Data perturbation

Data perturbation methods for unit record file data involve a purposeful falsification of certain data items that are deemed potentially identifiable (i.e., pose a risk of privacy disclosure). Examples of data perturbation used on datasets at AIFS include:

- perturbation of certain geographic levels (i.e., postcode for school areas in LSAC data);
- transformations of certain variables (e.g., postcodes are given an indicator so that all children selected in the same postcode can be identified but the postcode can not be known);
- transformation of a respondent's date of birth to a monthly variable.

Data reduction

Data reduction refers to methods that control or limit the amount of detail available in the data without compromising the overall usefulness of the information available for research.

Some examples of data reduction that can be used at AIFS include:

- the removal of specific personal identifiers (e.g., date of birth, name, address);
- the removal of qualitative data, (i.e., names, address, etc.). This needs to be reviewed on a variable-by-variable basis as well as a case-by-case basis;
- top coding extreme values to less extreme values. Top coded variables include income and payment related data items, housing-related data items and health-related data items such as body measurements;
- collapsing certain categories (e.g., occupation codes at the 2-digit level).

Access restriction

Restricting access to datasets at AIFS is a core method used to minimise the risk of a privacy disclosure. All persons involved with an integration project and subsequent analyses are required to make signed undertakings so that they are aware of their responsibilities.

Access to integrated data is restricted in the following manner:

- Access to all/any data is only granted on a need-to-know basis, justified in the Data Transfer Deed.
- Access to de-identified and confidentialised unit record file data is granted by a centralised body (Data Owners/Data Custodians).
- Access to any unconfidentialised unit record file data is only granted if this is explicitly stated in the methodology that is given clearance by the AIFS Ethics Committee.
- All data are used only for the purposes for which they were collected (i.e., research) unless specified otherwise by the AIFS Ethics Committee.
- Dataset linkage for high risk projects is processed through the separation principle with a minimum of four persons involved.
- All persons involved in dataset linking are required to make signed undertakings relevant to their role for each new project.

All persons involved in integration projects are informed of AIFS/Commonwealth Integration Authority linkage principles, which guide all data integration processes. All AIFS officers are required to make signed undertakings relative to their role in the integration process and to follow the data protocols.

Criminal penalties apply if confidential information is disclosed in contravention of the *Privacy Act 1988*. Penalties include a maximum penalty of $370,000 for individuals.

Criterion III – Availability of appropriate skills

Auditor rating against criterion III – compliant

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.

AIFS has a history of over 30 years of conducting high quality research design, collection, storage and dissemination to the Australian Government. AIFS has been instrumental in informing policy and has experience in managing large longitudinal linkage data such as LSAC, *Growing up in Australia*: The Longitudinal Study of Australian Children (LSAC).

Expertise in linkage and merging functions
AIFS has completed several data linkages across a number of projects. AIFS was responsible for developing the procedure required to successfully link the data in a confidential manner. AIFS then provided this linked data, along with survey data to data users.

AIFS ability to confidentially link datasets is demonstrated through the merging of National Childcare Accreditation Council, Medicare Australia, the Australian Bureau of Statistics and the National Assessment Program—Literacy and Numeracy (NAPLAN) data into the main LSAC data file. To ensure that none of the organisations involved in the linking process were able to see all data in its entirety, the separation principle involving multiple agencies was used. AIFS did not possess identifiable information about the participants, i.e., names, addresses, school names, etc. Identifiable data about our participants is kept by our fieldwork collection agencies, who require this information to track and conduct interviews across time with participants.

A method used by AIFS to perform data linkage and a method that has been implemented using LSAC (above) as an example, consists of the following steps:

1. AIFS contacts the organisation we required data from informing them of what is required, what consent was obtained, etc.
2. The fieldwork collection agency sends the organisation a list of consenting participants containing all necessary variables required to complete the matching process (including name, surname, school name, etc.). Each record in this file is given a dummy ID.
3. The organisation completes the matching and supplies AIFS with only the dummy ID with the variables added by the organisation. No identifiable information is supplied to AIFS (i.e. The organisation is required to remove identifiable information before sending the file to AIFS).
4. The fieldwork collection agency supply's AIFS a concordance file listing the real ID and the dummy ID for all of AIFS respondents.
5. AIFS used the concordance file supplied by the fieldwork collection agency to convert the dummy IDs to the real ID's on the data file supplied by the organisation.
6. The data file sent by the organisation is confidentialised and merged with the survey data.

Expertise in privacy
Following the changes to the Privacy Act, AIFS has conducted Institute-wide privacy training to ensure staff are aware of their privacy obligations and what constitutes good practice. The training provided a description of the requirements of the *Privacy Act 1988*, with a particular focus on the implications of the amendments introduced as part of the *Privacy Amendment (Enhancing Privacy Protection) Act 2012*.
AIFS has the capacity to undertake a Privacy Impact Assessment where necessary.

Expertise in confidentiality
As previously specified, confidentiality is a fundamental principle and an essential requirement for all projects conducted by AIFS. Our respondents are our most important resource and they need to feel assured that their identity will remain confidential. This is achieved in a number of ways, primarily with de-identification and confidentialisation.

Most of the surveys conducted by AIFS have the data de-identified by the data collection agency prior to it being received by AIFS. All data that are not de-identified prior to AIFS receiving it is de-identified soon after receiving it and before any analysis is conducted. The de-identification of data ensures that the risk of a respondent being identified (by a data user) is considerably reduced.

Even after the dataset is de-identified, the combination of a number of variables (especially unique responses) can lead to the possibility of identification of respondents. For this reason the confidentialisation process is performed in addition to the de-identification process, in order to better protect the privacy of respondents.

The two primary methods used in the Institute to confidentialise data are (1) data perturbation; and (2) data reduction methods.

Ability to provide useful metadata to data users
AIFS provides metadata and documentation for most if not all datasets that are processed within the agency. An example of metadata that is provided to data users can be best illustrated by reviewing the data dictionary that has been created and is provided along with the *Growing Up in Australia*: Longitudinal Study of Australian Children (LSAC) data.

The data dictionary provides metadata for every variable contained in the LSAC datasets. Metadata is available for all variables including questionnaire position, topic, question, variable labels, response code frames, informant, etc. Providing metadata to data users is extremely helpful to them in navigating large complex datasets and a necessity especially if these complex datasets are publically released.

Appreciation of data quality issues
Data quality issues are always prevalent for numerous reasons when conducting surveys and/or linking data. Data quality issues occur because of respondent error, interviewing coding error, or data entry error, matching processes, instrument error, etc.
AIFS provides thorough and varied documentation to users and the general public through numerous publications. Publications are provided alongside the release of datasets, and are available online.

III(b) What documentation and training is available to ensure staff have the appropriate skills and knowledge required in high risk data integration projects?

AIFS has been performing data integrations for several years and has a wealth of knowledge and experience in being able to link numerous datasets together and disseminate these datasets publicly in a confidential manner. This is best illustrated in the *Growing Up in Australia*: Longitudinal Study of Australian Children project (LSAC) as previously discussed. The cleaning and processing document for the LSAC project describes the procedures undertaken for previous data integrations.

The AIFS DMIT keeps abreast of developments with respect to best practice by attending conferences and workshops and provide knowledge and understanding about data integration processes to other agencies and partners. The sharing of knowledge and the ability to adapt to a changing environment ensures that team members are well versed in this area.

AIFS provides its staff with training about security, privacy and confidentiality, all of which are cornerstones for undertaking any data integration project. The training provided is illustrated in this application.

AIFS has also prepared a Data Integration document detailing the policies, procedures and protocols that need to be adhered to, in order to successfully complete a Data Integration Project. This legacy document will enable Data Integration procedures to be applied consistently across time. The Data Integration document is also dynamic. To ensure that AIFS remains abreast of linking methods and can complete linking projects to the highest possible standard, the procedures document will be updated to incorporate emerging trends and best practice. Before working on any linking project DMIT staff will go through a training process, which involves a simulated linking procedure. Staff must successfully understand and complete this task before they can be involved in any linking projects.

AIFS provides an active learning and development program to its staff with a focus on supporting relevant statistical, analytical and writing skills.

Criterion IV – Appropriate technical capability

Auditor rating against criterion IV – compliant

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.

AIFS is able to be custodians of large and complex files associated with data integration projects.

Hardware infrastructure at AIFS

Storage: The Institute uses an Enterprise SAN for data storage. All data is backed up to a Virtual Tape Library (VTL) on disk and tape, and tape backups are encrypted with an ASD approved encryption algorithm. Tapes are stored off-site with a commercial data storage company.

Data-lab: The AIFS data centre is environmentally controlled and monitored.

Computer type

The Institute uses energy-efficient multicore server hardware with redundant power and RAID. All hardware is on a 24/7 4-hour on-site response. The desktop environment is energy efficient hardware with next business day on-site response.

All hardware is maintained on a day-to-day basis by the Institute's on site specialist ICT Team.

Software infrastructure at AIFS

All systems undergo certification and accreditation in accordance with the Institute's accreditation process based on best practice as defined in the Information Security Manual, with all internal clients and servers accredited to the PROTECTED level.

All access to Institute data is controlled on a need-to-know basis and all access to data (including datasets) on the Institute's file server is logged. These logs are duplicated and stored on the central enterprise level logging solution.

The Institute's Gateway has undergone an external IRAP audit and has been accredited to the PROTECTED level.

ICT security

AIFS uses best practice technology, procedures and policies to protect its ICT infrastructure. A layered system of security is in place with different techniques used at different levels.

In accordance with the Protective Security Policy Framework (PSPF):

- A defence in-depth approach is used in all system design.
- Passwords are changed regularly.
- Accounts are locked out after multiple failed attempts.
- ASD guidelines are used for patching operating systems, networking equipment and servers.
- Application software updates are tested and applied as soon as practical after release.
- Access to the data-lab is controlled and is restricted to ICT staff.
- The network is protected by a state-of-the-art firewall to protect against external intrusion.
- Anti-virus software is constantly updated.
- Regular backups are taken, including rotation of encrypted backups to a secure off-site storage facility.

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?

All access to Institute data is controlled on a need-to-know basis and all access to data (including datasets) on the Institute's file server is logged. These logs are duplicated and stored on the central enterprise level logging solution.

IV(c) What IT support is in place for staff?

An on-site specialist ICT Team supports AIFS with extensive experience in supporting large international and national research projects. The team provide end-to-end service, including a help desk. The team's expertise includes: database and application development; web application design and development; data analysis; survey support, development and customisation; infrastructure design and management; and the management of sensitive information. There are also several people employed at AIFS who are highly qualified and experienced in database administration, management and data analysis..

Criterion V – Lack of conflict of interest

Auditor rating against criterion V – compliant

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.

No. The Australian Institute of Family Studies (AIFS) operates under the provisions of the *Family Law Act 1975*, which establishes AIFS to conduct, promote, encourage and co-ordinate research relevant to Australian families,

through the Director. AIFS has been set up solely for research purposes and has no regulatory or compliance purpose. In addition to the functions under subsection 114B(2) of the *Family Law Act*, in the *National Gambling Reform Act, 2012*, the function of AIFS, through the Director, are also to undertake or commission research into gambling, as the Australian Gambling Research Centre, which is within AIFS.

Further to this, the AIFS Advisory Council, with members appointed by the responsible Minister, provides specialist advice to the Director in relation to the strategic and research directions of the Institute. This ensures the Institute follows its intended function.
.

Criterion VI – Culture and values that ensure protection of confidential information and support the use of data as a strategic resource

Auditor rating against criterion VI – compliant

VI(a) How is an appropriate culture and values embedded in the agency's corporate plan/mission statement/policies etc?

As Government employees, AIFS employees are bound by the *Public Service Act 1999* that establishes the Code of Conduct and values to which all Government employees must conform. The culture and values of AIFS are re-enforced in the staff induction process and maintained through policies and procedures, training and corporate directions. AIFS policies and procedures further support the APS values and codes. For example, security and privacy policies emphasise confidentiality and integrity; finance policies allow accountability and transparency; human resources procedures reflect fairness and respect; and the Ethics Committee ensures processes to protect research participants and uphold AIFS' reputation.

Staff training on these policies and procedures is conducted regularly and serve as a reminder of values and obligations. Finally, values are further endorsed through the performance and development management system, through monthly staff-wide meetings and Director's updates and through promotional material such as posters throughout the building.

Regarding corporate direction, AIFS' mission and planned outcome is:
"to increase understanding of factors affecting how Australian families function by conducting research and communicating findings to policy-makers, service providers and the broader community".

This aligns with the APS Values and Code of Conduct and is published publicly.

Further, AIFS' strategic goals focus on the areas of informing, researching, disseminating and communicating, and performance monitoring. Specifically, the goals for 2012—2015 are:

1. Undertaking high-quality impartial research relating to the wellbeing of families in Australia.

2. Sharing the information and transferring our knowledge

3. Valuing and developing our relationships

4. Managing our organisation

AIFS' Research Directions are aligned with the Strategic Directions and are expected to have value for:

- responding to the needs of governments and community sector organisations through its capacity to conduct timely, balanced and accurate analysis of existing datasets, and responding to requests for submissions, advice, and analysis of issues and data

A culture of risk awareness is enhanced through risk assessments, which are required for every potential integration project. Each potential project must be approved through executive approval and ethics clearance processes.

Regarding induction, since AIFS first reported its PSPF compliance as at July 2013, it is a condition of engagement that all AIFS staff sign a commitment to uphold the Australian Public Service Values and Code of Conduct in the presence of a witness. Further, employees are required by law to adhere to the APS Values, Employment Principles, and Code of Conduct.

Since AIFS first reported its PSPF compliance as at July 2013, it is a further condition of engagement that all AIFS staff sign an acknowledgement of Section 70 of the *Commonwealth Crimes Act 1914* in front of a witness.

Further, since AIFS first reported its PSPF compliance as at July 2013, it is a condition of engagement that all AIFS staff sign an acknowledgment of the Institute's policies, procedures and guidelines relating to ICT, Security and Records Management in the presence of a witness and indicate a willingness to comply with the policies, procedures and guides.

Further, staff are required to adhere to the *Privacy Act 1988,* which outlines appropriate collection, use, disclosure and storage of personal information. As previously mentioned, penalties apply if confidential information is disclosed in contravention to the *Privacy Act 1988*.

Finally, for every data integration project conducted at AIFS, signed undertakings are required for all members of the DMIT. This ensures that the DMIT, researchers and data custodians are fully aware of their roles and responsibilities during the integration process and are reminded of them each time they integrate data.

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?

As in VI(a), staff sign documents that state they will comply with Section 70 of the *Commonwealth Crimes Act 1914* regarding the disclosure of information and with AIFS' Security and Records Management policies, procedures and guides. Staff are required to participate in training that addresses key points of the policies. Staff are required to further educate themselves on the Security and Records Management Policy documents, which are available on the Institute's Intranet. Staff are informed through email of any changes to the Security and Records Management Policies and are required to educate themselves with respect to any changes to these documents.

Face-to-face security awareness training is mandatory. Staff who have completed this are identified and recorded and those who have not are approached to arrange a session that they can attend. Training addresses key aspects of the Protective Security Policy Framework (PSPF).

Face-to-face privacy awareness training is currently being undertaken across AIFS. Staff who have completed this are recorded and those who have not are requested to participate in the next available session. Training provides a description of the requirements of the *Privacy Act 1988*, with a particular focus on the implications of the amendments to the Act, in the *Privacy Amendment (Enhancing Privacy Protection) Act 2012*.

As part of the induction process staff are required to undergo face-to-face records management training.

VI(c) Do staff sign undertakings related to secrecy and fidelity?

Yes. As in I(c)**,** since AIFS first reported its PSPF compliance as at July 2013, all staff requiring access to the Institute's information must be determined to be eligible. Since AIFS first reported its PSPF compliance as at July 2013, all persons requiring access to official information and resources require an Entry Level Check prior to being granted access.

All temporary staff, contractors and visitors that haven't completed an Entry Level Check and require access to AIFS ICT infrastructure will be escorted by personnel that have completed this process.
AIFS will ensure that all staff members who work on data integration will have, at a minimum, an Entry Level Check before they commence any work on data integration.

VI(d) What mechanisms are in place to engage with stakeholders to maximise the usefulness of the data holdings?

AIFS has a number of mechanisms in place, both technical and procedural, to assist stakeholders in maximising the usefulness of data. AIFS provides data user support i.e., responding to queries, documentation (e.g., Data Dictionary – this contains metadata about all variables in the dataset, labelled questionnaires, etc.) and data user workshops. AIFS keeps up-to-date with emerging trends and liaises with stakeholders about research questions their data might be able to answer.

Public availability
AIFS publish all output reports on the AIFS website where possible in an accessible manner so that the general public can benefit from the information gained through research. For an example of this see the annual statistical reports and discussion papers from the LSAC project. Making data and reports publicly available maximises the use of existing data and the resources that have been used to clean, link, analyse and record the results of studies.

Linking datasets
Through the linking of datasets, AIFS make use of the resources already used and the impact on participants by combining existing datasets. This reduces any potentially wasteful overlap of studies. For example, it was much more effective to link existing, current and accurate Medicare data to the LSAC study, rather than to endeavour to collect this health information anew from each participant. The more data sources that are linked to the main dataset, the more powerful and informative it becomes.
The resulting linked dataset is easier to use because many sources of information are held centrally in the one location. It can also be used more broadly as many researchers across different fields of study can use the one resource.

Consultation
In order to ensure the most useful and relevant information is being collected, AIFS conducts various consultations with stakeholders. AIFS works in conjunction with other agencies and regularly assesses whether these stakeholders' needs are being met through meetings, reports, emails and timelines.

Projects at AIFS also rely heavily on the input of advisory committees. Members are experts in their field, come from a variety of research disciplines and advise on content, method and length of studies. For example, LSAC has the Consortium Advisory Group (CAG), comprised of leading researchers at research institutions and universities throughout Australia, to ensure comprehensive coverage of influences on child development.

Finally, data users are consulted on the content of studies to ensure its usefulness to their research needs. AIFS also communicates with data users to ascertain what aspects of data are most/least used, how data are used (e.g., what types of analysis are run), how often the data are used and the reasons users provide for accessing data. This information can be used to make the data more informative.

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?

AIFS has several procedures in place to facilitate a culture that ensures the protection of confidential information and that data is used as a strategic resource. For example the process used in LSAC is outlined in the LSAC Data Management Issues paper.

The following outlines a strategy that will be further developed to guide data confidentialisation and access.

The Data Manager will be responsible for:

- facilitating access to the datasets;
- monitoring adherence to security requirements;
- contributing to a registry of users and completed research papers;
- signing the contracts and licenses governing the release of both the confidentialised and unconfidentialised datasets;
- providing technical assistance to users of both datasets, as well as developing the metadata.

Managing access to datasets

AIFS protective protocol six states that data released from AIFS is released in a form that will make identification unlikely through confidentialisation and de-identification.

All requests to use the datasets must be made in writing to AIFS using the appropriate form on the AIFS website. A request needs to include:

- the name of the organisation requesting the data;
- a description of the proposed project or general research purpose;
- the names and qualifications of researchers requiring access to the data under the project; and
- the project methodology and timeframe (necessary only if a specific project is proposed).

Access to datasets will be further assessed by the Data Manager, that:

- the applicant is able to meet the control measures; and
- the release is consistent with the purposes for which the data was collected and that there are no impediments to the data being used in this way.

Users must notify the Data Manager if there is any change in their place of employment (including retirement) or in their research topic, as such changes may impact on their access status.

Access to data will be made on a case-by-case basis and will always be dependant on a deed of confidentiality being signed by the user.

Additionally, parties granted a deed contract would be required to take all reasonable steps that may be reasonably required, to keep the confidential information, including all documents and all other things recording, containing, setting out or referring to any confidential information, under effective control of the licensee.

Users may be classified into various user groups based on the degree of risk associated with their access. This classification system will in turn dictate which datasets the user will have access to, and by which means (i.e., type of contract):

- moderately confidentialised data—e.g., postcode and date of birth removed and some top coding on variables such as income and age; or
- unconfidentialised—data will be aggregated or deleted.

Registry of users

Data users will be required to provide AIFS with details of any work utilising the datasets (including advance copies of any papers produced). AIFS will maintain a registry of users and their work (completed and in-progress).

This registry and copies of research findings (including work in progress) may be published on the data management website and in the AIFS annual report.

Clearance of research papers

Non-Commonwealth Government researchers using the unconfidentialised datasets will be required to clear papers for publication with AIFS to ensure the privacy of the survey respondents has been maintained. All researchers using the moderately confidentialised datasets will be asked to provide AIFS with an advance copy of any research to be published.

User support

With the datasets supplied to users, the following documentation will be provided in the form of a user manual, which would include:

- description of the conduct of the survey;
- details of weighting and imputation procedures;
- questionnaires;
- variable listing outlining variable names, labels, response categories;
- details of derived variables;
- structure of the datasets; and
- examples of use of the datasets.

User training

In conjunction with the public release of the datasets, user training sessions will be offered by AIFS to further develop the information provided in the user manual and to allow users to dynamically interact with the DMIT.

Criterion VII – Transparency of operation

Auditor rating against criterion VII – compliant

VII(a) Are data retention and data disposal statements publicly available? Provide details.

AIFS policies and procedures that apply to records management also apply to the management of data.
As a Commonwealth Agency, AIFS adheres to Section 24 of the *Archives Act 1983* in relation to the lawful destruction of Commonwealth records. Tools that AIFS uses to dispose of its records are:

- a records authority;
- a Normal Administrative Practice (NAP).

The data management website will provide a statement that AIFS complies with *Archives Act 1983*. The website will also provide links to the Act and relevant National Archives websites, which specify the data retention and disposal requirement that AIFS must abide by.

VII(b) Are details of governance arrangements publicly available? Provide details.

Details about the Institute's governance arrangements are currently publicly available here:

http://www.aifs.gov.au/institute/pubs/annualreports/ar13/ar13d.html

http://www.aifs.gov.au/institute/aifs/corpgovernance/index.html

Information will also be made available on the data management section of the AIFS website.

VII(c) Where are details of data integration projects published?

These will be made available on the data management section of the AIFS website. This will include a list of past, present and future projects, where relevant, which can be sorted by various variables of interest, such as name, number of participants, etc.

AIFS' communications plan stipulates that information about projects be made publicly available.

Any future linking projects involving Commonwealth data will also be provided on the National Statistical Service project register.

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.

AIFS currently provides information about existing projects, for example the LSAC webpage. These pages inform users of:

Specific information about the datasets to be linked, for example data dictionaries, sample size, retention rates, and the questionnaires/measures and methods used in the study.

Request for data, links to data user responsibilities and obligations and more information.

Details on privacy protection and protocols, freedom of information statements, and the complaints procedure.

Research publications (e.g., statistical reports, discussion papers, technical reports and data user guides).

Details of linking procedures are made publicly available in technical papers, for example here:

http://www.growingupinaustralia.gov.au/pubs/technical/tp8/02.html

Examples of these types of web pages are publicly available here:

http://www.growingupinaustralia.gov.au/common/privacy.html

A data management website will expand on the type of information that already exists to include more information on linking requests, details of linking projects and the linking procedure and data retention and disposal statements. Select parts of a Data Integration Procedure document will be made publically available on the data management website.

Criterion VIII – Existence of an appropriate governance and institutional framework

Auditor rating against criterion VIII – compliant

VIII(a) What are the institutional and project-specific governance arrangements for data integration? (Provide attachment or link to where published.)

AIFS is committed to protecting the privacy of all data that it has custodianship of through effective and structured data management processes. Data integration processes provide an explicit link between risk assessments, data management processes, Ethics Committee recommendations and privacy legislation, to ensure the highest level of security for data during the integration process.

AIFS has five levels of governance, ensuring data integration occurs as described in the Institute's policies and procedures.

1. Over-arching AIFS governance and executive management arrangements outlined in the management and accountability section of the annual report, which is publicly available here:

http://www.aifs.gov.au/institute/pubs/annualreports/ar13/ar13d.html

In addition to this, the Institute has transitioned to the new Australian Government Protective Security Policy Framework (PSPF), in accordance with guidelines published by the Attorney-General's Department.

The PSPF stipulates as a mandatory requirement that AIFS is to implement an audit, review and reporting process to assess the Institute's protective security performance in ensuring the confidentiality, integrity and availability of essential resources. The audit process must include:

- internal audit and reporting—self-assessment with an annual report to the Minister;
- the Australian National Audit Office (ANAO) audits of protective security; and
- the Attorney-General's Department annual review of protective security.

To ensure AIFS complies with the PSPF mandatory requirement (Gov. 7), security audit and reporting includes:

- an annual security assessment against the PSPF mandatory requirements; and
- a report on AIFS' overall compliance with the mandatory requirements to the Minister.

The security audit report also includes:

- a declaration of compliance by the Director; and
- details any of non-compliance, including details on measures taken to lessen identified risks.

External reporting

AIFS reports annually to Government and/or stakeholders regarding the Institute's protective security effectiveness in achieving the Government's mandatory security requirements. Increasingly, AIFS will be required to provide evidence of protective security performance to Government and/or stakeholders, including performance in areas such as personnel security, information security, physical security, business continuity, and work health and safety.

The Director ensures a copy of the annual security audit report on compliance is sent to the following:

- the Secretary, Attorney-General's Department, and
- the Australian Government Auditor-General.

AIFS also advises the following of any non-compliance with mandatory requirements:

- the Director, Australian Signals Directorate for matters relating to the Australian Government Information Security Manual (ISM);
- the Director-General, Australian Security Intelligence Organisation for matters relating to national security; and
- the heads of any agencies whose people, information or assets may be affected by the non-compliance.

Australian National Audit Office

ANAO audits the protective security arrangements within Australian Government agencies in accordance with the *Auditor-General Act 1997.* ANAO uses the mandatory protective security standards as a benchmark of security standards when auditing security practices. These audits aim to, among other things, enhance the management of protective security within agencies, and provide assurance that public sector organisations are meeting their security obligations.

The Attorney-General's Department will report annually on the protective security status using Government agencies' annual compliance reports, and ANAO audits of protective security.

2. Risk Assessment and Audit Committee (RAAC)

RAAC reviews internal controls and performance management systems and investigates issues such as budgets, audits, risk and fraud control. RAAC meets three to four times a year, is chaired by an external member and reports to the Director.

3. AIFS Ethical oversight

AIFS has an ethics committee that assesses proposed data integration projects to balance the benefits of a project with any risk to privacy. AIFS Ethics Committee clearance is required for all proposed research and data integration projects.

AIFS Ethics Committee meets to assess all proposed data integration projects after an initial risk assessment has been undertaken through the AIFS DMIT. Each data integration project must have research merit and integrity, and

have appropriately identified risks of privacy disclosure.

4. AIFS Internal Data Management oversight

AIFS subscribes to the set of principles, governance and institutional arrangements outlined by the Commonwealth Secretaries Board for all data integration projects. These principles and data management protocols provide assurances that the privacy of data providers will be protected by ensuring that strong and consistent governance, methods, policies and protocols are followed for the integration of Commonwealth data for statistical and research purposes. To facilitate full compliance with Commonwealth protocols, AIFS has a specialised DMIT to oversee these processes. AIFS DMIT is responsible for a variety of data policies and protocols to minimise the potentiality of privacy disclosure including:

- access limitation;
- data integration using the separation principle; and
- data management practices and project reporting.

5. AIFS internal project specific oversight

Risk management, records management, security and privacy procedures are applied to the project throughout the life of the project until the project is complete, after which disposal procedures are applied to the closure of the project.

VIII(b) What framework is in place to conduct investigations and handle complaints?

The AIFS Ethics Committee is registered with the National Health and Medical Research Council (NHMRC) with members appointed for a three-year term. AIFS Ethics Committee meets regularly to ensure that the ethical standards outlined in the National Statement on Ethical Conduct in Research Involving Humans, and elaborated in the Institute's Ethics Protocols, are fulfilled in all research and data integration projects undertaken by the Institute. The AIFS Ethics Committee also considers any complaints or problems that may have arisen regarding ethical issues in Institute research and are an important point of reference for data privacy protocols when integrating data.

Anyone who has a concern or complaint is asked to contact the AIFS Ethics Committee Secretariat in the first instance. The Ethics Committee Secretariat ensures the concern is handled by someone not connected with the research project and facilitates a resolution to the concern in an impartial manner. The complainant is also advised that they can put in a formal complaint to the Commonwealth Ombudsman or Consumer Affairs Victoria.

Finally, the Office of the Australian Information Commissioner (OAIC) also has the power to conduct investigations in relation to privacy matters under the Privacy Act.

Appendix A: Glossary of Terms

Confidentialisation
Data or information that has been purposefully modified to protect the privacy and confidentiality of the data provider. Unconfidentialised data is data that has been de-identified, but has not had other confidentialisation techniques applied (such as top/bottom coding).

Data custodian
The agency responsible for managing the use, administration, disclosure and protection of data used in a statistical data integration project.

Data integration
The full range of management and governance practices around data linkage including: acquisition of the data, project approvals, integration concepts, and privacy breach minimisation.

Data linking
The process involved in linking two or more datasets.

Data Management Integration Team
The team at AIFS that specialises in data management and integration. All integration projects will be undertaken by that AIFS DMIT.

Data provider
Individuals, households, families, businesses or institutions that have provided the authorised statistical agency private information for research purposes.

Identifiable data
Indicates where the identity of a specific individual can reasonably be ascertained (e.g., name, image, date of birth or address).

Accredited integrating authority
Commonwealth agencies authorised to undertake high risk data integration projects involving Commonwealth data for statistical and research purposes.

Principle of separation
The separation principle means that no one individual can see the identifying or demographic information, used to identify which records relate to the same person or organisation (e.g. name, address, date of birth), in conjunction with the analysis data (e.g. clinical information, benefit information, company profits) in a linked dataset during or after dataset linkage.

Top/Bottom coding
The process of data perturbation where the most extreme data values are made less extreme. A type of confidentialisation that can be used for both micro-data confidentialisation and aggregate data confidentialisation.