Australian Government | National Statistical Service

Statistical Data Integration involving Commonwealth Data

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

Summary version

Applicant:	Department of Social Services
Auditor:	Protiviti
Date accredited:	5 October 2018

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

Secretariat

Phone (02) 6252 7198

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

As an accredited Integrating Authority (IA) the Department of Social Services (DSS) has the ability to provide integration services for joining data with internal and external sources for the benefit of evidence-based policy development. The integration of isolated external datasets with Departmental data will greatly expand the scope of analysis, allowing outcome-based reporting and better informed decision-making. DSS's ability to undertake these integrating projects will also satisfy increasing demand for the use of DSS data.

Formal accreditation as an Integrating Authority ensures that DSS' data practices conform to the highest possible standard: demonstrating best practice when it comes to data integration and ensuring the safety and security of data and personal information.

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 lined datasets can only access those parts of the datasets required for the analysis).

The Department of Social Services (DSS) practices separation of datasets based on Australian Bureau of Statistics (ABS) methodology, which is widely regarded as best practice for protecting data confidentiality. The separation function is outlined in corporate methodologies and linkage manuals published on the ABS' external website and will be applied to all DSS data linkage projects. (See: http://www.abs.gov.au/websitedbs/d3310114.nsf/home/statistical+data+integration)

In alignment with the ABS' separation principle, DSS will ensure the secure management of data used for statistical and research purposes. The adoption of the ABS data integration model through separation of functional roles guarantees secure access to datasets requiring linkage and secure data visibility. DSS understands it is of critical importance that personal information is protected and privacy is assured, and that unauthorised disclosure of confidential information does not occur while still making the most effective use of data.

The key linking roles are:

Assembler – staff performing assembling will only have access to unit record level data to merge pre-linked datasets for confidentiality purposes at the client level.

Linker – staff performing linking are only able to see a view of the data that contains the fields they need to do their linking (i.e. demographic/linking variables file), which will be provided to them by the Librarian. The datasets are linked and a common linking ID is created in each dataset.

Librarian – a staff member who has this role has access to run processes against the data such as creating datasets for 'Linkers' or 'Analysts'.

Analyst – staff performing analysis of linked data are only provided with access to the fields they need to do their analysis, which is again provided to them by the Librarian.

Please note:

- The Librarian, Assembler and Linker roles described above are internal DSS roles, undertaken by DSS staff.
- No individual can have access to more than one role at a time and no role allows the entire combined files to be viewed.
- A senior DSS officer (an Executive Level officer or above) is responsible for access controls managed by IT.
- All access to data files is logged and monitored.

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.*
DSS will conduct regular internal audits for all their integration projects through the Data Governance Committee (DGC) and Departmental regulatory programs. Regular independent external audits will also be carried out to ensure that DSS is compliant with the separation function and other data integration principles, and is meeting all legislative and procedural requirements as an Accredited Integrating Authority. DSS adheres to the Australian Commonwealth security frameworks such as the Protective Security Policy Framework (PSPF), upon which the Australian National Audit Office (ANAO) bases its compliance activities. DSS has a rolling program of internal audits: the Internal Audit Practice Charter. This Charter provides an operational framework for the conduct of Internal Audits in the Department of Social Service (DSS) and has been developed in accordance with the International Professional Practices Framework (IPPF, 2013) of the Institute of Internal Auditors (IIA) and the ANAO's better practice guidelines. The Charter is reviewed annually for approval by the Audit and Assurance Committee (AAC).
I(c) Do employees (including contractors) undergo police checks upon employment?
Yes. All DSS employees, including contractors, are required to undergo an entry level background and identity check prior to commencing employment with DSS. The Pre-Employment background and identity checks are required before staff and contactors are provided access to official information and resources including IT systems and DSS buildings and facilities. All advertisements for vacancies and selection documentation in the Department must include the Pre-Employment Check as a condition of employment. Contracts with outsourced providers must include a clause stipulating that any contractor employee accessing official information and resources must undergo a Pre-Employment Check before given access to official information and resources. Additional background checks may be identified for particular positions where additional risks have been identified or higher assurance of the position holder's integrity is required. These additional checks may be included in any conditions of employment when advertising the vacancy and in selection documentation, or in contracts with outsource providers. In addition, all people involved in the linkage process hold a security clearance relevant to each role (determined by a competent external vetting authority).
I(d) How is access to the agency's premises controlled? Provide details.
Access to all DSS premises and areas are restricted at all times to approved persons and are controlled by the use of electronic access control systems, sign-in registers and contract guards.

Control of access to the Department's premises is based on the Protective Security Management Framework (PSMF) (https://www.protectivesecurity.gov.au) which provides policy, guidance and better practice advice for governance, personnel, physical and information security. The Department's Protective Security Policy encompasses physical, personnel and information security and is accessible to all staff on DSS' Corporate Policy List.

Protective Security Management Framework – Protective Security Policy
DSS' approach to physical security is based on the approach that the external and internal environments of facilities can be designed and managed to create conditions that, together with specific physical security safeguards, will reduce the risk of violence to employees, protect against unauthorised access, detect attempted or actual unauthorised access and activate an effective response. DSS has a range of physical security principles, including a multi-layered security-in-depth approach and security impact assessments.

I(e) How is your agency's Internet gateway secured?

DSS secures its internet gateway in accordance with controls listed in the Information Security Manual to the PROTECTED level. There are a number of different aspects as to how this is designed including firewalls, micro segmentation and intrusion protection.

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. The Department's Protective Security Management Framework (PSMF) outlines policies and procedures including protective control of data, secure ICT access, and documented roles and responsibilities.

A focus on understanding, prioritising and managing security issues and risks is fundamental to effective security at all levels and in all circumstances. In order to ensure this focus is maintained, the DSS' PSMF is organised in a tiered, hierarchical structure.

Tier 1 – DSS Security Directive

The directive clearly articulates the Executive's expectations that protective security will be managed within DSS based on an agreed level of risk tolerance.

DSS' Security Directive is the keystone of the Protective Security Management Framework. It highlights the Executive's requirement for protective security to be a business enabler that allows the portfolio to work together securely in an environment of trust and confidence.

Tier 2 – Protective Security Policies

Tier 2 comprises:

a. personnel, information and physical security core policies; and
b. protective security governance arrangements.

This tier includes the 33 mandatory requirements against which DSS will need to report compliance annually to the Minister.

DSS' Protective Security Policies articulate the security requirements to maintain compliance with the Australian Government's Protective Security Policy Framework's core policy environments. It is the responsibility of all DSS employees to ensure that DSS ICT resources are properly secured and controlled and that the DSS ICT Security Policy is adhered to

DSS also has an Information Communication Technology (ICT) Security Policy Plan whose objective is to

enable DSS, partner agencies, clients and customers to achieve their business objectives and manage risks through the use of secure, trusted, resilient and sustainable ICT systems.

To achieve these objectives, system owners and authorised users will:

a. Awareness – be aware of the need for security of information systems and networks and what they can do to enhance security, through information security training, awareness and education;

b. Responsibility – be responsible for the security of information systems and networks;

c. Response – act in a timely and co-operative manner to apply information security to prevent, detect and respond to security incidents;

d. Conduct – demonstrate responsible behaviour in the use of DSS ICT systems and respect the legitimate interests of others;

e. Risk Management – understand risk management processes and make informed risk based decisions;

Security design and implementation – adopt positive security culture in applying a comprehensive approach to the management of information security, by adhering to the DSS Acceptable Use Policy and Procedures.

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.

Access restricted to endorsed applicants

As an Accredited Integrating Authority DSS will only provide integration services to agencies and organisations with a legitimate and approved need to join data to social security information, and only if it is of benefit to DSS. The requesting organisation/agency will be required to provide appropriately separated datasets to DSS that align with the functional separation principles. DSS will then link the dataset to be integrated with the data variables requested from the second source. DSS will only provide the integrated data back to the requesting agency/organisation at the 'analysis' dataset level (i.e. anonymised), which includes only the variables required by the analyst to do their analysis.

Data Access Protocols

DSS ensures the safe access to data through the implementation of the:

- Bilateral Management Arrangement (BMA) Management Information Protocol
- Protocol for Release of Social Security and Related Information (SSRI)
- Deeds of Licence and Deeds of Confidentiality.

The governance of operational processes is guided by the:

- Access to and use of data – (BMA) Management Information Protocol
- Release and sharing of information to third parties – Protocol for the Release of Social Security and Related Information (SSRI).

Data users are bound by formal requirements set out in relevant licence deeds and data manuals.

Appropriate confidentialisation of data

DSS has been making unit record level data available for statistical purposes in the form of Confidentialised Unit Record Files (CURFs) since 1998, mostly consisting of Income Support recipient data. The Household, Income and

Labour Dynamics in Australia (HILDA) unit record level survey data has been made available to selected analysts and research institutions under certain conditions for the past 15 years.

DSS enforces strict access controls to all Departmental data. The approval process for extraction and release of information is adhered to at all times which is consistent with Commonwealth's High Level Principles for Data Integration, Principle 5: *Statistical data integration must be used for statistical and research purposes only.*

Deeds of Licence and Deeds of Confidentiality are required for the release of Confidentialised Unit Record Files (CURFs) to data users. On 31st March 2011, the Secretary of DSS signed a 'Responsible Officer Undertaking Minute' to guarantee that DSS will abide by the conditions for use of CURFs. CURFs are released to data users upon receipt of a completed licence application and a signed Deed of Confidentiality.

CURFs are randomly generated to ensure there is no way to reverse engineer the confidentialisation of personal information or to re-identify the original record.

Current confidentialisation process

The current process for the Data Access and Integration Section has moved beyond the creation of CURFs. Current linkage projects undertaken within DSS involve a process of the Assembler attacking the dataset to try and determine whether distinct individuals can potentially be re-identified. The subsequent assessment is based on looking at all high-risk variables and applying an appropriate statistical treatment using appropriate methods to reduce the risk.

Further controls can also be put in place to assess the dataset and verify there is no likelihood of re-identifying individuals, for example checks by dataset curator, and data item access managed through project-specific Public Interest Certificates. Data is then stored in a secure file-safe environment (for e.g. SURE) or released in an aggregated format (e.g. Data.gov.au, Dataverse).

The Data Access and Integration Section is currently working with Data 61 to automate the 'Attacking' process. This R4 automated tool and process will be used for all data integration projects in the future.

Access to data via secure remote access facilities

The password-protected Remote Access Research Gateway was established by the Sax Institute at the request of the Department of Social Services. The Gateway enables accredited researchers to analyse data with direct identifiers removed using statistical programming languages in a Secure Unified Research Environment (SURE), supported by the Australian Institute of Health and Welfare (AIHW).

Accreditation as a user of the gateway requires sponsorship by a university or other institution to verify that the individual has the required skills to undertake the analysis and can be trusted to appropriately and ethically use the data. The researcher must also sign agreements that stipulate how the data is to be used, their responsibilities, and information about penalties for misusing information. Finally, accredited users are required to undertake training on the responsibilities of research principles, information security and statistical disclosure analysis and control.

The Gateway has been assessed as providing appropriately secure protection processes services through a Privacy Impact Assessment, an independent Information Security Risk Assessment and found compliant against relevant legislation including the *Privacy Act 1988* and social security and family assistance law.

Aggregated Data access

The same rules used for unit record level data around security and confidentiality also apply to aggregated data.

Review of data by appropriately skilled internal staff

DSS has a strict Quality Assurance (QA) and clearance process for all data released internally and externally. Data extracted and/or any reports developed are sent to the business data and policy areas for approval/clearance to release or publish the information.

Each dataset/report is QA'd by the team that extracts the data in the first instance then sent to other teams within the section. Data is cross-checked against source data and published information. The data/report is then sent to the business area(s) for clearance to release or publish the information.

All clearances are in writing and start at the Director level (EL2 and above). Caveats and metadata are checked and verified by both the QA process and business areas. Once approval has been received, the data is released with the business area(s) included in all correspondence.

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.

Expertise

DSS has been at the forefront of collecting and analysing information relating to the wellbeing of Australians for many years. The core business of the Department is to collect, process, analyse and disseminate statistical information to support evidence-based policy decisions. This experience has enabled DSS to develop the infrastructure and expertise required to enable the Department to undertake high-risk data integration projects. This includes hiring and retaining specialists in statistical methodology and analysis, technology support officers, legal and policy advisors, and subject matter experts.

All staff in the Department with access or roles related to data/information management and integration have extensive training and expertise in information management principles, data quality and clearance processes. The specialist areas within DSS support the functional areas undertaking statistical operations, including data integration, and are outlined in the DSS ICT Security Policy.

DSS has built its data integration expertise through projects such as linking Welfare and LSAC data (Longitudinal Study of Australian Children), the Census and Social Security and Related Information dataset linkage, the Multi-Agency Data Integration Project and the Data Integration Partnership for Australia. DSS has skills and experience in implementing the separation principles, improving its information technology and data security, risk management, and data governance.

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

Documentation

DSS has many forms of documentation on data linkage which supports the basis for ongoing data integration projects. DSS is working to develop procedural manuals and training documentation tailored to operational staff. Some documents and training are developed according to the needs and scope of the project. DSS' supporting documentation is published on the Department's internal website and includes:

- ICT – Acceptable User Policy and Procedures
- ICT Security All IT Policies
- SSRI Protocol
- Bilateral Management Arrangements
- Data Terminology Catalogue
- MADIP Evaluation Report 1
- MADIP Evaluation Report 2
- MADIP Evaluation Report 3

The following governance and other strategic documents are stored internally including:

- Data Governance Committee Forward Work Program 2016-17
- Department of Social Services Data Access Policy Principles
- Data Access Policy
- Data Confidentialisation Policy
- Data Embargo Policy
- Data Stewardship Policy
- DSS Information Management Strategy 2014-17
- Building Data and Systems Capability (ADP) Strategic Plan 2014-2017
- DSS Metadata Management Strategy
- Data Release Schedule
- DSS Data Quality Principles
- DSS Strategic Plan for Data Management
- DSS Steps in Managing Data Quality
- DSS Data Management Action Plan
- DSS Data Management Implementation Plan
- DSS Data Quality Assurance Guide
- DSS Data Quality Management Strategy
- DSS Data Quality Risk and Issue Register

Training

The Data Access and Integration Section has a Departmental Centre for Data Capability and Education, develops and delivers a suite of modules relating to foundations of data management and data quality management. As DSS increases its data integration work, there will be a regular training session run for data experts reiterating linkage methodologies and principles, as well as providing practical opportunities for upskilling. These modules are supported by the Department's strategic policy guidelines on data integration, data quality, data access, data tools, data stewards and related governance. The DSS Centre for Data Capability and Education provided the coordination and delivery of four all day Data Resource training courses as part of the Advanced Social Policy Modules. Delivery of eight half-day customised Data Foundation enabling training courses to business areas across the department and presentations of DINGO, DOMINO, data.gov.au and the national map were provided to business teams, communities of practice and committees to assist with better understanding of the Departmental tools enabling business to have improved access evidence and information to support policy development.

Other relevant training provided includes; Security Awareness; Induction; and social policy data. Multiple training formats are available such as on-the-job, webinars and mentoring.

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.

The Department:

- Uses analytical systems including SAS servers and Enterprise Guide to support the use of large and/or complex files.
- Secures its IT infrastructure in accordance with the Information Security Manual.
- Uses data centres and equipment certified in accordance with the Protective Security Policy Framework and Security Construction and Equipment Committee (SCEC).
- Currently holds and protects significant amounts of individuals' data including but not limited to commercially sensitive information, medical data and data considered sensitive under the Privacy Act.
- Operates its environment using a segmented architecture based on data classification and risk profile. This allows the Department to deploy different security controls to different sets of data and usage profiles including but not limited to public access, UNCLASSIFIED and PROTECTED data.
- Actively restricts administrative privileges to systems and data on a need-to-know basis.
- Routinely scans its environment for missing patches, configuration issues and vulnerabilities.
- Actively monitors for risks through the environment with real-time monitoring using data correlation and machine learning to search for anomalous activities.
- Attempts to remediate identified risks within 48 hours. Where this cannot be done due to operational requirements, risks are addressed using alternative controls

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?

The Department records user activity in accordance with the requirements of the Information Security Manual control. This includes but is not limited to the following:

- A secure centralised logging facility
- Events are logged/captured in real time or near real time
- Events are analysed in real time
- Typically the following events are logged depending on the capabilities of the individual systems and where sensitive data has been identified:
  - all privileged operations
  - successful and failed elevation of privileges
  - security related system alerts and failures
  - user and group additions, deletions and modification to permissions
  - unauthorised access attempts to critical systems and files
  - logons
  - failed logon attempts
  - logoffs
  - DNS logs
  - web logs

Tracking of all activity is undertaken at the database, operating system and web application levels

IV(c) What IT support is in place for staff?
DSS is extensively supported by the Information Management & Technology Group (IMTG) through many channels of communication. The Department has an IT Service Helpdesk (contactable via phone and on the Intranet (StaffNET), which is operational between the hours of 7am and 8pm ESDT), and a Front Door area that responds to requests for new IT services or any enhancements to an existing IT service need. Requests are logged with the IMTG Front Door through IT Services Online. The IMTG gateway is further supported by a range of infrastructure and network specialists, database administrators, data managers and an IT Operations area containing highly skilled SAS Administrators who assist in resolution of issues.

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.
Yes. DSS has a compliance monitoring and a regulatory function and has a long history of data matching exercises for the purposes of program evaluations, monitoring and compliance under other arrangements and agreements that are out of scope of the Integrating Authority arrangements. Responsibilities for program monitoring, evaluation and review are clearly defined and are kept separate from data integration activity. DSS will conduct regular internal audits for all their integration projects through the Data Governance Committee (DGC) and Departmental regulatory programs. Regular independent external audits will also be carried out to ensure that DSS is compliant with the separation function and other data integration principles, and is meeting all legislative and procedural requirements as an Accredited Integrating Authority. The Data Access and Integration Section will work closely with B ranches across DSS to ensure that the Department aligns with any framework that exists for linking of data. It is vital that the integration of datasets always follows best practice while taking into account various pieces of legislation both within the Department and more broadly across other agencies and organisations. Finally, the Investigations; Enterprise Compliance and Feedback; and Fraud Analytics Sections within DSS also have dedicated compliance monitoring and regulatory functions which are separate to the data integration projects undertaken within the Department.

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.?

The Department's values are outlined in the *Department of Social Services Corporate Plan 2017-18*, along with DSS' vision and mission statements.

DSS values reflect those of the broader Australian Public Service (APS Values and Code of Conduct) and are central to the way we work with Ministers, colleagues, stakeholders and the public. This includes being impartial, committed to service, accountable, respectful, and ethical.

Ethical behaviour includes the values of honesty, integrity, transparency, diligence, fairness, trust, respect and consistency. It identifies and avoids conflicts of interest and improper use of our position or role as APS and DSS staff members.

Other behaviours that DSS staff are expected to understand and exhibit are how to manage official information, follow departmental and legislative guidance about making public comments, exercise a duty of care when providing information and advice, follow the relevant standards when dealing with lobbyists, ministerial staff and government Ministers.

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?

Training in requirements for protecting personal information

All employees of DSS are required to undergo the Protective Security training on a regular basis. This consists of an online training course on how to manage information, secure data and manage the release of Commonwealth information. Each employee is assessed and is required to attain a 'pass' achievement. The internal 'Learning Hub' provides regular training opportunities and staff are encouraged to attend courses on (for example) APS Values and Principles and the APS Induction courses for new employees. These courses cover staff responsibilities pertaining to security and expectations relating to the handling of Departmental and Commonwealth information.

As the Department relies heavily on ICT to deliver its services, all staff must actively manage the security risks associated with electronic data transmission, aggregation and storage. Extensive training is conducted for all employees on how to manage responsibilities within each individual's roles and teams. Staff are also encouraged to attend training in skills specific to their role (e.g. technical IT training).

On-the-job training is an essential part of the role each staff member performs in the Data Access and Integration Section. Due to the sensitive nature of the work that is conducted in the Section it is imperative that each person is aware of the legislation that governs the work that is performed and has the appropriate security measures in place to perform tasks such as data linkage and confidentialisation.

Policies regarding breaches of security or confidentiality

Relevant Officers (Band 1) will ensure that staff responsible for working with data are familiarised with policies and procedures through which the Department protects the confidentiality of its data. These include:

- (Draft) Data Protection and Breach Policy
- Data Breach Response Plan
- Data Access Policy
- Data Confidentialisation Policy

- Data Stewardship Policy, and
- Internal Privacy Policy.

Staff will be able to access this information via the departmental portal for Data Information and Governance (DINGO) via StaffNET.

Potential breaches of security or confidentiality are managed in DSS through the Data Protection and Breach Policy and the Data Breach Response Plan.

In response to the Notifiable Data Breaches Scheme, which took effect on 22 February 2018, the Legal Services Branch developed the Data Breach Response Plan (the Plan) which includes procedures for taking action in the event of a serious breach of personal information, so that DSS can respond in a timely and coordinated way. The aim of the plan is to clearly establish who in DSS is responsible for managing the Departmental response to data breaches, and to provide staff with a practical tool to investigate, rectify damage, assess the risk of serious harm and notify where required.

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

Yes. All DSS staff members sign a Declaration of Confidentiality upon commencing employment or on reassignment or promotion from an external agency. This ensures they are aware of their privacy, confidentiality and secrecy obligations under Commonwealth law. For example under Section 204 of the Social Security (Administration) Act, if a person intentionally makes a record of, discloses to any person, or otherwise makes use of information, where they were not authorised or required by law to do so and where they know the information is protected information, then the person is guilty of an offence.

All service providers contracted or funded by DSS who deal with personal information belonging to the Department also sign a Deed of Confidentiality. The deed ensures that service providers are aware of their obligations in regards to privacy, confidentiality and secrecy obligations under Commonwealth law.

DSS employees, including contractors requiring access to security classified resources must obtain a security clearance assessed externally by an approved vetting organisation.

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

The Department is committed to optimising the use and reuse of public data and collaborating with private and research sectors to extend the value of public data for the benefit of the Australian public. In doing so, DSS undertakes a range of activities to engage with stakeholders to maximise the usefulness of its data holdings. This includes participating in a wide range of data linkage work that provides benefits to Government, researchers and the Australian public.

DSS publishes a wide range of data on Data.gov.au, the central repository of government data, to facilitate public access and promote more efficient data sharing and analysis.

The Department has engaged extensively with stakeholders during the development of the Multi-Agency Data Integration Project and Remote Access Research Gateway project, including universities, research organisations, individual researchers and numerous Government agencies.

DSS staff have also conducted Australia-wide presentations and workshops on the PIA research data set released onto the ABS' TableBuilder platform in late 2017.

DSS has multiple business areas that have expert Data Stewards and data programmers who provide regular advice, support and clearance for datasets from multiple sources. These experts liaise with staff in all areas of the Department and are called upon to discuss or conduct regular presentations around sensitivity of data and the business rules that govern the strict criteria for release of DSS client level information.

The following mechanisms are in place to engage with stakeholders to maximise the usefulness of data holdings:

- Direct marketing by meeting with requestors
- Identifying suitable data and engaging to publish
- Visiting state offices
- Working groups
- Presentations and speaking to stakeholders on a range of information relating to data and reporting (e.g. the PIA research data set on TableBuilder)
- Meeting with key stakeholders around security, infrastructure required for integration of datasets, and other datasets that rely on accessibility from individual users' desktops.
- Cross-agency collaboration on Open Data initiatives
- Whole-of-Department engagement via StaffNET (internal intranet)
- Working collaboratively with Data Stewards
- Media engagement
- Media releases
- Website announcements on data and policy initiatives
- Making data available to the public (e.g. the ACLD-SSRI data linkage project with the ABS).

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?

DSS actively supports the Australian Government Public Data Policy Statement (Attachment A) and other initiatives to improve access to public data, while protecting the privacy and confidentiality of individuals.

DSS recognises the importance of a trusted, transparent and balanced approach to sharing public data where the privacy and confidentiality of individuals are priorities. In this context, DSS is committed to collaborating with research and private sectors to extend the value of public sector data for the benefit of Australians.

The approach to protecting privacy varies depending on how access is provided. For example, the Remote Access Research Gateway Data Access Project involves de-identifying unit record level data, providing access in a secure enclave, and undertaking a Privacy Impact Assessment (PIA) and an Independent Security Risk Assessment. Other methods that will provide access involve de-identifying then aggregating data (TableBuilder Data Access Project), and perturbing data using mathematical algorithms (Synthetic Data Project).

DSS publishes aggregated data to the Data.gov.au website. This website is designed as a central repository for Government data to provide a single point of access to Government information. DSS data has been very popular with over approximately 40,230 views and 9,616 downloads, making it one of the most popular data agencies. No significant sensitivities have been identified during this time.

Criterion VII – Transparency of operation

Auditor rating against criterion VII – compliant

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

DSS has a destruction strategy where names and addresses will only be retained while they hold significant value. Consistent with the Australian Privacy Principles, the case for retention will be periodically reviewed and data will be destroyed if there is not a compelling case for retention.

DSS' data retention and disposal practices are outlined in the DSS Records Management Policy. This policy operates within the framework of National Archive requirements (NAA Act) for data retention and management and the Privacy Act 1988, APP 11 on the security of personal information.

DSS' approach to data retention and data disposal aligns with the retention policies on the National Statistical Services website.

Upon being created, all records will receive an authorised disposal authority. This will ensure compliance with standards, as standard-compliant records cannot be disposed of without a valid and authorised retention and disposition authority. DSS will implement the NAA-approved AFDA Express retention schedule as well as implementing specific DSS records authorities. These will be implemented at the transaction level of the Department's Business Classification Scheme (BCS). All Departmental records will be subject to appropriate retention and disposal schedules. These schedules allow for records to be kept for as long as they are required and then disposed.

DSS contract arrangements and business processes will address requirements for security, privacy, access, storage, management, retention and disposal to ensure our digital information is protected for the long term.

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

Yes, data governance arrangements for Data Integration projects more generally – is outlined on the external website under 'Policies and Legislation' (https://www.dss.gov.au/policies-legislation/data-integration).

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

DSS will publish a register of data integration projects in scope of the Commonwealth Arrangements. This will include developing a website dedicated to information relating to projects and ongoing work undertaken by the Department and other agencies who have requested integrating services from DSS. The website will be for both internal and external users (enforcing the strict privacy access protocols) and will also provide a front door contact point specifically for providing advice and information relating to all areas of the Department's integrating expertise. The website will also link to the DSS internal intranet (StaffNET), providing consistency of access to customers both internally and externally. These online services will ensure staff and customers have access to the relevant protocols, registers/schedules, documentation required for security, and linking procedures and methodologies developed by DSS.

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.
In 2015 the DINGO online portal was developed as an easy-to-use centralised source for data and data-related information. DINGO is now used as the corporate repository for data information and governance within the Department, is accessed directly from the front page of STAFFnet, and is available to all staff internally. It contains data governance policies and strategies; a whole-of-Department data listing; data rules; 'how to'-type documents; a Data Stewards page; and key contacts information. DSS is now in the process of establishing a DINGO Extranet Portal to allow other Government departments to publish and consume Social Services data and foster interdepartmental data exchange, creating a much more collaborative and self-service data environment within Government. Access controls via SharePoint permissions can be applied at various levels.

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.)

DSS' data integration governance will be managed utilising existing governance structures. The Data Policy and Governance Section is responsible for Secretariat support for the Data Governance Committee, the Data and Projects Sub-committee and the Data Stewardship Community of Practice.

The Data Governance Committee (DGC) reports to the Policy and Regulatory Reform Committee. The DGC oversees and provides strategic guidance on data policies, systems, activities and projects—including data-related investments. The committee aims to promote a common data vision driven by business priorities, and to ensure that all data-related activities and projects reflect business needs, outcomes and objectives.

The Policy and Regulatory Reform Committee provides governance of the Department's policy and regulatory reform activities. The committee is responsible for the strategic, cross-cutting and outcome policy strategies and positions for the Department, and ensures that DSS' policy activities and advice take account of regulatory views and deregulation opportunities.

The Data and Projects Sub-committee oversees data improvement projects. It promotes bids for future data-related activities and projects that reflect strategic business needs, outcomes and objectives.

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

DSS has a number of ways for handling complaints. Complaints relating to data integration projects will be managed through a tiered approach. The Integration team in the Data Access and Integration Section will have a centralised email box and a dedicated phone number that will be publicised, enabling customers to send through requests for new integrated projects; request advice regarding the integration of data; access governance information (e.g. guidelines, publications, protocols and security etc.); and raise issues, problem solving and complaints.

Any complaints that are made will be managed by the Team Leader and filtered through to the Section Director. Depending on the nature of the complaint the Director will either respond personally to the customer or filter the complaint through to the Branch Manager for a formal response.

DSS also has a Feedback Coordination team that has a formal process published on the Corporate Policies webpage for handling of all complaints received about DSS programmes and DSS funded service providers. The team has a Complaints Management Policy whereby:

- If a call is received from a member of the public who wishes to raise a complaint, staff are to inform the caller to contact the DSS Complaints line (see phone number below).
- All complaints should be scanned and emailed to the complaints inbox, or if this is not possible, complaints can be posted to the DSS Feedback and Coordination team.

Complaints about Government policy, legislation or reviews over eligibility for a benefit or entitlement are not handled by the DSS Feedback and Coordination team. If a caller has a concern about a policy or piece of legislation

administered by DSS, they can write to the Minister or their concerns can be forwarded to the relevant program area for consideration when next that policy or legislation is reviewed.
Ph: 1800 634 035 | **Email:** complaints@dss.gov.au

Other feedback, complaints, suggestions and enquiry mechanisms include:

Commonwealth Ombudsman

The Department may receive requests from the Commonwealth Ombudsman's Office in regards to a complaint about an action or decision made by the Department or about a service provider funded by DSS.

When an Ombudsman request is received, it is forwarded to the relevant line area for response. The Ombudsman has strict guidelines for agencies to follow and all responses will be reviewed by DSS Feedback and Coordination before being submitted to the Ombudsman.

Queries on the process can be made via email at ombudsmancomplaints@dss.gov.au

Dashboard Reports - DSS Feedback and Complaints

In 2011 DSS implemented protective security governance guidelines for reporting incidents and conducting security investigations: GovGuide Conducting Security Investigations. These guidelines implement the PSPF governance requirements relating to incident reporting and investigative procedures and adhere to the implementation guidance provided in the AS/NZS ISO/IEC 27002:2006 – Code of Practice Standard.