Australian Government

Department of Veterans' Affairs

Internal Audit Services

FINAL Report

Review of Privacy Policy and Freedom of Information - 2011-12 #29

Planned	Feb 2012
Fieldwork Commenced	Apr 2012
Fieldwork Completed	May 2012
Draft Report	Jun 2012
Final Report	Jun 2012

This report was produced by staff provided by KPMG under a contract for the provision of internal audit services.

INHERENT LIMITATIONS

This report has been prepared as outlined in the Scope Section of this report. The services provided in connection with the engagement comprise an advisory engagement which is not subject to assurance or other standards issued by the Australian Auditing and Assurance Standards Board and, consequently, no opinions or conclusions intended to convey assurance, as defined by that standard, will be expressed.

Due to the inherent limitations of any internal control structure, it is possible that fraud, error or non-compliance with laws and regulations may occur and not be detected. Further, the internal control structure, within which the control procedures that have been subject to the procedures we performed operate, has not been reviewed in its entirety and, therefore, no opinion or view is expressed as to its effectiveness of the greater internal control structure. The procedures performed were not designed to detect all weaknesses in control procedures as they are not performed continuously throughout the period and the tests performed on the control procedures are on a sample basis. Any projection of the evaluation of control procedures to future periods is subject to the risk that the procedures may become inadequate because of changes in conditions, or that the degree of compliance with them may deteriorate.

No warranty of completeness, accuracy or reliability is given in relation to the statements and representations made by, and the information and documentation provided by, DVA management and personnel consulted as part of the process.

KPMG have indicated within this report the sources of the information provided. We have not sought to independently verify those sources unless otherwise noted within the report.

KPMG is under no obligation in any circumstance to update this report, in either oral or written form, for events occurring after the report has been issued in final form.

The findings in this report have been formed on the above basis.

THIRD PARTY RELIANCE

This internal audit report has been prepared at the request of the Audit Committee or its delegate in connection with our engagement to perform internal audit services as detailed in the internal audit plan. Other than our responsibility to the Secretary and Management of the Department of Veterans' Affairs, neither KPMG nor any member or employee of KPMG undertakes responsibility arising in any way from reliance placed by a third party on this internal audit report. Any reliance placed is that party's sole responsibility.

This report may be provided to the Australian National Audit Office, as the external auditor of the Department, for its own use. If the Australian National Audit Office intends to rely on internal audit work it can only do so in the context of the professional requirement placed on it by the provisions of Australian Auditing Standard ASA 610 (*Considering the Work of Internal Audit*).

We believe that the statements made in this report are accurate, but no warranty of accuracy or reliability is given in relation to information and documentation provided by Departmental Management and personnel.

LIMITATION OF LIABILITY

KPMG's liability in relation to these Services is limited under an Institute of Chartered Accountants in Australia Scheme approved under the relevant Australian States and Territories professional standards legislation, including, where applicable, the Treasury Legislation Amendment (Professional Standards) Act 2004 (Cth).

TABLE OF CONTENTS

1 Executive Summary

1.1 Background, Scope and Objectives

The *Freedom of Information Act 1982* (FOI Act) allows the Australian public to access documents from Australian Government agencies and its authorities such as the Department of Veterans' Affairs (DVA). It provides a general right of access, which is limited by the exemptions and exceptions identified in the FOI Act.

The *Privacy Act 1988* (Privacy Act) provides protection of personal information in the federal public sector and in the private sector.

The objective of this Internal Audit was to assess whether FOI and Privacy policies and procedures are effective in assisting the Department in meeting the legislative requirements of the FOI Act and Privacy Act.

This internal audit considered the policies and procedures covering FOI activity within the Department with reference to the FOI Act and considered the mechanisms in place for ensuring compliance with the Privacy Act.

Internal Audit did not assess whether the decision to release or withhold information following a FOI request was appropriate or correct.

This internal audit was conducted in accordance with the *International Standards for the Professional Practice of Internal Auditing.*

1.2 Significant matters arising (CR1[1], CR2)

There were no CR1 issues raised during this internal audit.

This internal audit detected no non-compliance issues in relation to the FMA Act.

CR2 Finding	Implementation Timeframe
There is a requirement for greater assurance that all DVA staff are aware of their responsibilities under the Privacy Act.	December 2012
There is no Departmental policy to adequately outline procedures for administering requests for information under s59 SRCA and s331 MRCA.	December 2012

1.3 Summary of other issues (CR3, BIR)

The following issues were also identified during this internal audit:

- Aspects of FOI administration that were not in accordance with the FOI Act and/or ANAO better practice.
- The FOI database provides limited functionality and is impacting on the ability of DVA staff to accurately report to the OAIC in accordance with the FOI Act.

1.4 Number and categorisation of observations

CR1	CR2	CR3	BIR
-	2	1	1

[1] Classification of audit findings is explained at Section Appendix D.

1.5 Assessment

Based on our scope and methodologies, our internal audit found that generally, DVA has effective procedures for the administration of requests for information under the FOI Act. In addition, staff responsible for processing requests for information under the FOI Act have demonstrated a good level of understanding of the FOI Act and client correspondence on files tested was to a high standard. Our internal audit identified some instances where FOI requests were not completed within the statutory timeframes prescribed by the FOI Act. In addition, Internal Audit identified two instances where charges were imposed for the release of information although statutory timeframes were not met.

There is scope to improve the accuracy of reporting on FOI Act administration through enhancing the legacy database. Internal Audit has suggested that the database should be corrected to enhance the accuracy of information reported in respect of the timeframes taken to process FOI requests.

DVA has established procedures for the routine release of personal and/or sensitive information. Although there is a high level of understanding of the Privacy Act among the Advising and Public Law staff, Internal Audit considers that measures should be taken to enhance general Departmental staff awareness of the obligations and requirements under the Privacy Act.

Internal Audit was informed that DVA does not have a policy for the administration of requests for information under s59 of the SRCA and s331 of the MRCA. This creates a potential exposure for the Department as there are no legislated or endorsed timeframes, protocols or protection mechanisms specific to the administration of these requests. In the absence of a relevant policy, staff have been following the FOI Guidelines and where relevant, guidelines published by Comcare in administering these requests.

Internal Audit also notes that DVA has consolidated its FOI processing function to a National FOI Processing Unit, based in Sydney, in addition to the Advising and Public Law team in Canberra. This followed a recommendation contained in 2007-08 Internal Audit #01 Review of Privacy and Freedom of Information.

Finally, Internal Audit notes that the Attorney General announced new privacy reforms that were introduced into the Australian Parliament on 23 May 2012. The implementation of these reforms will provide an opportunity to remind and inform DVA staff of their responsibilities under the Privacy Act and for relevant policies and procedures to be updated.

To assist the Department in making the necessary improvements we have included an Action Plan at Section 2.

1.6 Sign off

Exempt Material

Partner, KPMG

Exempt Material

Carolyn Spiers
Principal Legal Adviser

Other Stakeholders

Exempt Material

Jennifer Collins
Deputy Commissioner, NSW/ACT

2 Action Plan

Control weaknesses and other opportunities for improvement identified during this internal audit are set out below. Each includes an indication of whether line management agree that a weakness exists and their proposed action in response.

2.1 The requirement for greater assurance that all DVA staff are aware of their responsibilities under the Privacy Act (CR2)

What we found

Internal Audit considers that current procedures are not sufficient to ensure that all staff maintain an adequate awareness of their obligations under the Privacy Act. As such, current procedures do not provide sufficient assurance that the Department is meeting the legislative requirements of the Privacy Act. This view is supported by our review of the Complaints and Feedback Management System, which indicated that there have been 28 privacy related complaints since July 2011.

Internal Audit has identified that DVA induction training and related materials do not make reference to the Privacy Act.

The Privacy Site located on the DVA intranet contains out of date information and missing links. Internal Audit acknowledges that the Advising and Public Law team are aware of this and have assigned responsibility for updating the site to the DVA Privacy Officer.

On 2 May 2012 the Attorney General announced new reforms to the Privacy Act. Advising and Public Law team staff appeared well informed of the reforms. DVA Advising and Public Law team staff advised that some of the content on the Privacy Site will be updated when the reforms take effect.

What is expected

All staff should be made aware of their responsibilities under the Privacy Act upon commencement of employment at DVA. There should be mechanisms in place to ensure that staff maintain an appropriate level of awareness of the Privacy Act.

Why this happened

The absence of Privacy Act requirements in induction materials appears to be an oversight.

Implication

Some DVA staff members may be unaware of their obligations under the Privacy Act when dealing with clients and client information.

Suggested action

The *Welcome to DVA - What You Need to Know* booklet and other induction materials should be updated to specifically outline staff responsibilities under the Privacy Act and should direct staff to current information, policies and guidance within the Department to enhance continued compliance with the Privacy Act.

In addition, DVA should facilitate an enhanced culture of compliance with the Privacy Act and should take additional measures to continuously inform and remind staff of their obligations under the Privacy Act. Staff should be reminded of the need to report all suspected privacy breaches to support the continual improvement of procedures and reduce the likelihood of future breaches.

The following suggestions are provided for management consideration:

- The development and provision of an online training module that addresses the requirements of the Privacy Act (the effectiveness of such a module would be enhanced if the module required mandatory completion and assessment at periodic intervals).
- Staff should be informed of all material changes to FOI and Privacy Laws in a timely manner.
- Periodic reminders of appropriate use and disclosure of personal information, including appropriate circulation of personal information within the Department.

Management Response		Agree
	Intended Action #1	Legal Services & Assurance is working on improvements to the privacy material over the coming months. It is expected that all new material will be in place over the next 3-6 months.
	Responsibility	Principal Legal Adviser
	Complexity Factors[2]	None identified
	Timeframe	December 2012

2.2 There is no Departmental policy to adequately outline procedures for administering requests for information under s59 SRCA and s331 MRCA (CR2)

What we found

DVA does not have an endorsed policy for administering requests for information under s59 SRCA and s331 MRCA.

The National FOI Processing team administers routine s59 SRCA and s331 MRCA requests. Certain s59 SRCA and s331 MRCA requests, such as those that are contentious or are made by or on behalf of a high profile client, are administered by the Advising and Public Law team.

In the absence of a relevant policy, staff have been following the FOI Guidelines and, where relevant, Comcare Guidelines and associated case law in administering these requests.

Comcare releases information under s59 SRCA and has developed guidelines in respect of the release of this information. There are no external guidelines specifically relevant to the release of information under s331 MRCA.

What is expected

It is expected that DVA has an endorsed policy for administering requests for information under s59 SRCA and s331 MRCA that is clear and defensible.

Why this happened

In 2004 when MRCA took effect, the responsibility for administering requests for information under s59 SRCA and s331 MRCA was given to the National FOI Processing team and the Advising and Public Law team. These teams were administering requests for information on behalf of the Department under other mechanisms, such as FOI. The development of a policy has not yet occurred.

Implication

This creates a potential exposure for the Department as there are no legislated or endorsed timeframes, protocols or protection mechanisms specific to the administration of these requests.

Suggested action

A policy should be developed and endorsed for the administration of requests for information under s59 SRCA and s331 MRCA.

---

2 Complexity factors are explained at Section D.2.

Management Response	Agree
Intended Action #2	s59 SRCA and 331 MRCA policy are to be developed as part of a suite of work outlined in Section 2.1 in the next 3 - 6 months.
Responsibility	Principal Legal Adviser in consultation with the First Assistant Secretary, Rehabilitation and Support.
Complexity factors	None identified
Timeframe	December 2012

2.3 Aspects of FOI administration that were not in accordance with the FOI Act and/or ANAO better practice (CR3)

What we found

During FOI file testing, Internal Audit identified the following breaches of the FOI Act in the administration of FOI requests tested. Specifically:

- There were five identified instances where the statutory timeframe was not adhered to. Of these, there were two instances where charges were imposed. This is a breach of Regulation 5 of the FOI Act, which states:

  There is no charge for providing access to an applicant's personal information or for providing access outside the statutory processing period unless the Information Commissioner has extended that period[3].

- There were two instances where requests were not acknowledged within 14 days.

What is expected

Statutory timeframes prescribed under the FOI Act for acknowledgement of FOI requests and for providing a decision on FOI requests should be met. Where the timeframe is not met, charges must not be imposed.

Why this happened

This appears to be an oversight. Internal Audit was advised that the National FOI Processing Team experiences delays in receiving internal notification that payment for FOI charges has been received and receipted within DVA. These delays can impact the ability to provide documents requested under the FOI Act within the statutory timeframe.

Implication

DVA may be in breach of the FOI Act.

Suggested action

DVA should determine whether it is appropriate to repay charges to applicants whose FOI requests were not administered within the statutory timeframes.

Staff who receive and receipt payment in respect of FOI requests should be reminded of the need to inform the National FOI Processing Team of payment receipt in a timely manner, to enable FOI requests to be processed within the statutory timeframes.

---

3 Guidelines issued by the Australian Information Commissioner under s 93A of the Freedom of Information Act 1982, Section4, Page 3.

Management Response		Agree
	Intended Action #3	FOI staff will be reminded of new rules. All staff involved with FOI processing will be reminded of new rules via a Business Line to be issue mid June.
	Responsibility	Principal Legal Adviser
	Complexity Factors	None identified
	Timeframe	July 2012

2.4 The FOI database provides limited functionality and is impacting on the ability of DVA staff to accurately report to the OAIC in accordance with the FOI Act (BIR)

What we found

The National FOI Processing team in Sydney operates a Microsoft Access database in respect of separate state locations. Staff have experienced a number of inefficiencies in the operation of the database.

Of particular concern is the inability for staff to "stop the clock" when entitled to under the FOI Act. As an example, when an applicant is advised of the intention to impose charges for the release of information, the applicant has 30 days to accept and pay, or dispute the charges. As such, DVA is entitled "stop the clock" and hold the processing of the application until the applicant pays the applicable fee, disputes the fee or withdraws the request. Figures for reporting to the OAIC and for inclusion in the DVA Annual Report are obtained from the database.

This was reflected in our testing, Internal Audit observed instances where DVA has adhered to the statutory FOI processing timeframes, however, figures reported indicate that DVA is in breach of statutory FOI processing times.

Internal Audit is aware that a business case for a new Freedom of Information Claim System was submitted on 28 April 2010.

What is expected

DVA should provide accurate figures, including timeframes, to the OAIC in respect of the administration of requests for information under the FOI Act.

Why this happened

Prior to the formation of the National FOI Processing team, DVA operated FOI processing teams across multiple states, each operating a separate database. The National FOI Processing team still operates a separate database for each state. Database functionality has not been enhanced since the consolidation.

Implication

The FOI databases cause inefficiencies in the processing of FOI requests and potential inaccuracies in reporting to the OAIC and in DVA's Annual Report.

Suggested action

Internal Audit supports an initiative to enhance the functionality of the FOI database.

A record should be maintained to correctly record instances where DVA is entitled to "stop the clock" in respect of FOI applications for which charges are considered.

Management should if possible, correct the database to allow for the stopping of the clock or consider implementing an additional register. A reconciliation between the register and the FOI database(s) may need to be performed to ensure that accurate figures that reflect DVA's level of adherence to statutory timeframes are provided to the Advising and Public Law team in Canberra. Please note that this would require the creation of additional steps and controls.

Management Response		Agree
	Intended Action #4.1	A business case to reform the FOI databases was submitted for consideration in the 2012 – 2013 draft capital management plan. It was not funded. The proposal will be resubmitted for consideration again in 2013 -2014.
	Responsibility	Deputy Commissioner, NSW/ACT
	Complexity factors	Securing Required Funding
	Timeframe	2014
Management Response		Agree
	Intended Action #4.2	The FOI register is to be amended to include additional functionality as recommended. Work on this initiative will be subject to examining the changes required to the system and how they can be best achieved in the Department's existing upgrade /improvements to its ICT systems. In the absence of an automatic upgrade, DVA will implement a manual work around. Timeframe: examine systems requirements, costing for changes, any alternative approaches and finalise strategy to implement this recommendation by end August 2012.
	Responsibility	Principal Legal Adviser
	Complexity factors	None identified
	Timeframe	August 2012

Appendix A Background and Scope

A.1 Background

The 2011-12 Audit Program includes an Internal Audit to assess whether FOI and Privacy policies and procedures are effective in assisting the Department to meet legislative requirements. The timing of this Internal Audit allows for DVA's approach to the IPS requirements to be reviewed and is supported by the ANAO's view that all organisations should consider using internal audit to periodically review the administration of FOI requests.[4]

Freedom Of Information

The *Freedom of Information Act 1982* (FOI Act) came into effect on 1 December 1982. It allows the Australian public to access documents from Australian Government agencies and its authorities such as the Department of Veterans' Affairs (DVA). Freedom of Information (FOI) is a general right of access, which is limited by the exemptions and exceptions identified in the FOI Act. Substantial changes were made to the FOI Act in 2010 as part of wide-ranging open government reforms, which established the Office of the Australian Information Commissioner (OAIC). Part 2 of the FOI Act established an Information Publication Scheme (IPS) which came into effect on 1 May 2011. The IPS requires agencies to take a proactive approach in publishing information so that greater openness and transparency in government is established.

DVA received 4955 FOI requests in the 2010-11 financial year.[5]

Privacy

The *Privacy Act 1988* (Privacy Act) came into effect on 1 January 1989. It is the principal piece of legislation providing protection of personal information in the federal public sector and in the private sector. On 1 November 2010 the Office of the Privacy Commissioner was integrated into the OAIC. The Privacy Act contains 11 Information Privacy Principles (IPPs). These apply generally to Australian Government agencies, including DVA, and establishes standards for handling personal information.

In addition, the Privacy Act contains 10 National Privacy Principles (NPPs) which some private sector organisations need to comply with in relation to personal information they hold. All health service providers in the private sector need to comply with these principles.

These principles deal with all stages of the processing of personal information, including setting out standards for the collection, use, disclosure and quality, and security of personal information. For the individuals concerned, the principles also create requirements of access to, and correction of, such information.

During the 2010-11 financial year the OAIC was notified of three incidents that resulted in privacy breaches.[6]

---

4 Source: ANAO Report No.57 2003-04 Administration of Freedom of Information Requests, page 74

5 Source: DVA 2010-11 Annual Report, page 48

6 Source: DVA 2010-11 Annual Report, page 48

Department of Veterans' Affairs

Within DVA the release of information is managed across two business areas: Legal Services and Assurance (LSA), reporting to the Principal Legal Adviser and the National FOI Processing Unit, reporting to the NSW/ACT Deputy Commissioner. LSA has overall responsibility for the policy, practices, delivery of training relating to FOI and Privacy functions, liaison with the OAIC, adherence to the Information Publication Scheme (IPS) and management of complex or vexatious applicants.

The National FOI Processing Unit processes applications and reports statistical information on processing timeframes. Requests for information under section 59 of the SRCA and Section 331 of the MRCA are also processed by the National FOI Processing Unit.

A.2 Objective

The objective of this Internal Audit was to assess whether FOI and Privacy policies and procedures are effective in assisting the Department in meeting the legislative requirements of the FOI Act and Privacy Act.

A.3 Scope

This internal audit considered the policies and procedures covering FOI activity within the Department with reference to the FOI Act. It also considered the mechanisms in place for ensuring compliance with the Privacy Act.

In conducting this piece of work we:

- Held discussions with key Departmental staff to determine the processes in place to manage the release of information;
- Held discussions with staff and reviewed relevant documentation to gain an understanding of the business processes created by DVA to implement the IPS;
- Reviewed policies and procedures covering FOI and Privacy; and
- Performed sample testing to assess adherence to policies and procedures focusing specifically on FOI transactions, DVA's IPS and personal records.

This internal audit did not consider IT related browsing of client/staff/supplier records as this was addressed in 2010-11 #20 Internet and Client Records Monitor. However, it did identify and consider the controls in place to prevent unauthorised access to such records. A separate internal audit in 2010-11, #23 Review of Protection of Information already considered the storage and maintenance of personal and otherwise sensitive information, hardcopy client pension, medical, advocacy and HR files, policy, commercial and personal information.

Internal Audit did not assess whether the decision to release or withhold information following a FOI request was appropriate or correct.

This internal audit took account of the ANAO Report No. 57 *Administration of Freedom of Information Requests 2003-04* as well as findings from the following relevant Internal Audits:

- 2007-08 #01 Review of Privacy and Freedom of Information; and
- 2009-10 #20 Client Registration, Proof of Identify Process & Client Management.

This review involved a visit to the Sydney office.

This internal audit was conducted in accordance with the *International Standards for the Professional Practice of Internal Auditing*.

Appendix B Detailed Report

This section details the work performed in response to the key risks and review objectives identified in the agreed assignment plan. A summary of weaknesses and opportunities for improvement can be found in the Observations and Action Plan at page 4. Details of testing conducted may be found at page 21.

B.1 Process Description

B.1.1 Administration of FOI requests

DVA receives requests for access to information under the FOI Act by post, facsimile, in person at DVA offices, via email and via inter-agency transfer.

Generally, requests for access to information under the FOI Act (FOI requests) are administered by the National FOI Processing Unit in Sydney. Requests from high profile clients, journalists, Members of Parliament and requests that are considered to be highly sensitive or contentious are administered by the Advising and Public Law Team and/or the Principal Legal Adviser.

The DVA website contains a Factsheet FIP01 *Access to Information about You* that explains the right of access to personal information and how to obtain access. The website also contains D8601 *FOI Application for Access to Documents*.

General FOI process

Upon receipt, requests reviewed to determine whether they are valid. Valid requests are logged in the FOI Register in respect of requests administered by the Advising and Public Law Team and the FOI Database in respect of requests administered by the National FOI Processing Unit. Where a request is invalid or the scope of the request is not clear, the applicant is contacted and is given an opportunity to refine or amend their request. Applicants are provided with, FOI factsheets that are available on DVA's website are provided. In determining whether a request is valid, the team apply the FOI Guidelines provided by the OAIC.

In processing FOI requests, the documents or information requested are considered and relevant business areas within DVA are consulted to determine the extent of information available and the method and timeframes by which it can be retrieved. Where appropriate, the application of charges is considered and determined. Charges are not imposed for access to a client's personal information. Upon notification of the imposition of charges, applicants have 30 days to accept the charge and pay any applicable deposit or dispute the charge. If the applicant does not respond within 30 days, the FOI request is considered to be withdrawn.

In accordance with section 15(5)(a) of the FOI Act, DVA attempts to acknowledge all FOI requests within 14 days of receipt. If an extension of time is required to complete a FOI request, DVA staff will generally request an extension from the applicant and will advise the OAIC of the extension. DVA staff may also apply directly to the OAIC for an extension of time.

Unless an extension applies, DVA staff aim to meet the statutory timeframe of 30 days from receipt of a FOI request unless charges apply for providing a decision on whether a FOI request will be allowed, rejected or partially allowed. The applicant will generally be provided with a schedule outlining the documents provided as well as any documents within the scope of the request that were not provided, with reasons for exempting or editing the documents.

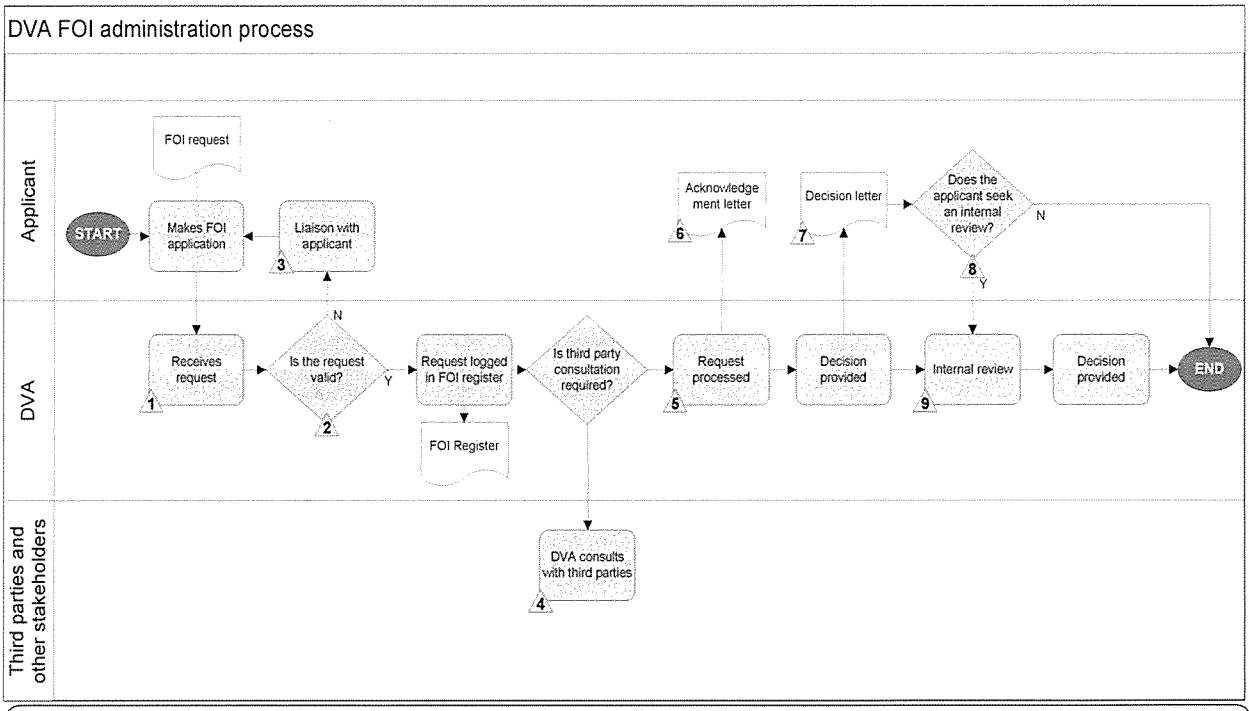
All National FOI Processing Unit and Advising and Public Law Team staff are delegated to make a decision on whether to accept, partially accept or reject a FOI

request. Where required, the Departmental Medical Officer will be consulted to determine if the release of information is considered to be detrimental to the mental or physical wellbeing of the client. In this case, DVA will only release the information through the client's doctor or psychologist, and only with the consent of the client.

If the applicant is not satisfied with DVA's decision, then the applicant may apply for an internal review of the decision. All internal reviews are referred to the Advising and Public Law Team and are generally conducted by the Director, Advising and Public Law or Senior Legal Adviser, provided that they were not involved in the preparation or review of the request response to conduct the internal review. Where it is not possible to appoint a member within the team, the Principal Legal Officer or an interstate Senior Legal Adviser or Senior Lawyer will be appointed to conduct the review.

If DVA does not provide a decision within the statutory or extended deadline, then the FOI request is deemed to be refused. In this case, the applicant has a right to an internal review of the decision.

Figure 1 - DVA FOI administration process



Notes:
1 FOI requests are generally administered by the National FOI Processing Unit. Requests from high profile clients, staff members, journalists, Members of Parliament and highly sensitive or contentious requests are administered by the Advising and Public Law Team.
2. The FOI Guidelines provided by the OAIC are used to determine whether a request is valid.
3. Should a request be invalid, the client will be contacted to refine/update/correct the request. To assist the applicant, FOI factsheets available on the DVA website are provided to the applicant.
4. Where information subject to a FOI request contains information in relation to a third party, the third party will be consulted to obtain their views and any objections.
5. After the scope has been defined, the relevant business areas within DVA are consulted where necessary to locate the required information. Charges are considered. If charges are to be applied, the applicant will be notified. The applicant then has 30 days to agree to the charges. Should the applicant not respond within the 30 day timeframe, the request will be withdrawn. Search and retrieval involves locating documentation with the assistance of relevant areas in DVA to satisfy the scope of the request.
6. Upon receiving a request, DVA must within 14 calendar days notify the applicant that the request has been received.
7. Unless an extension has been agreed, DVA has 30 calendar days to respond to the applicant. The request for information will either be allowed, partially allowed or rejected. All charges paid by the applicant will be disclosed.
8. If the applicant is not satisfied with DVA's decision, the applicant may apply for an internal review of the decision.
9. The internal review is carried out by a staff member that is independent of the initial request i.e. the staff member was not involved with the initial request. At this stage, if the applicant is not satisfied with the internal review decision, they may request a review with the OAIC.

Quality control and peer review

The Senior FOI Officer in the National FOI Processing team periodically checks:

- The case list that the team are processing compared to the applicable database;
- Adherence to statutory timeframes; and
- Spot checks of documentation for quality control.

In addition certain FOI requests are referred to the Senior FOI Officer and the Manager, Sydney VAN and National FOI Processing Team for processing and review. All new National FOI Processing Team staff are assigned a buddy and have all of their work peer-reviewed until they are considered proficient. Generally, the peer review process continues for a few weeks.

Advising and Public Law Team staff have their responses to FOI requests reviewed by another team member.

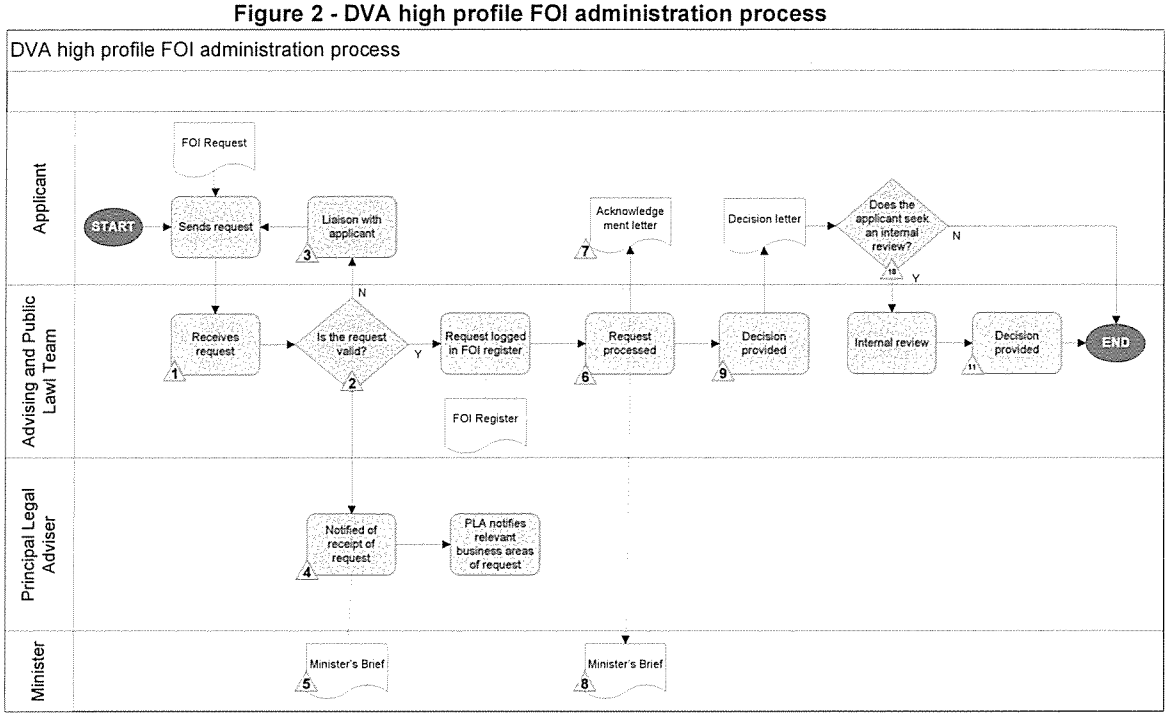
Highly sensitive FOI requests

Requests from high profile clients, journalists, Members of Parliament and requests that are considered to be highly sensitive or contentious are administered by the Advising and Public Law Team and/or the Principal Legal Adviser. The Principal Legal Adviser will determine any additional notification requirements to interested parties, including the Minister and relevant First Assistant Secretary, Assistant Secretary and DVA Media Unit.

DVA has a procedural document titled Updated FOI Processes and Clearances for High Profile/Media Requests that outlines the timing and content of briefing material to the Minister and the DVA Media Unit.

The Minister and other relevant stakeholders are provided with an initial brief upon receipt of high profile FOI requests. In addition to initial briefing of the content of high profile FOI requests, the Minister and DVA Media Unit are provided with a final brief and talking points in the event of media enquiries, four days prior to the release of information in response to an FOI request.

Figure 2 - DVA high profile FOI administration process



Notes:
1 FOI requests from high profile clients, staff members, journalists, Members of Parliament and highly sensitive or contentious requests are administered by the Advising and Public Law Team
2 The FOI Guidelines provided by the OAIC are used to determine whether a request is valid
3 Should a request be invalid, the client will be contacted to refine/update/correct the request. To assist the applicant, FOI factsheets available on the DVA website are provided to the applicant
4 The Principal Legal Adviser is notified of FOI requests that are considered to be high profile or highly sensitive. The Principal Legal Adviser notifies other areas within DVA as appropriate. Generally, this includes the DVA Media Unit.
5 The Minister is provided with a Brief advising of the nature of the FOI request.
6 After the scope has been defined, the relevant business areas within DVA are consulted where necessary to locate the required information. Charges are considered. If charges are to be applied, the applicant will be notified. The applicant then has 30 days to agree to the charges. Should the applicant not respond within the 30 day timeframe, the request will be withdrawn. Search and retrieval involves locating documentation with the assistance of relevant areas in DVA to satisfy the scope of the request.
7 Upon receiving a request, DVA must within 14 calendar days notify the applicant that the request has been received.
8 The Minister is provided with a second Brief and relevant talking points four days before information is to be released.
9 Unless an extension has been agreed, DVA has 30 calendar days to respond to the applicant. The request for information will either be allowed, partially allowed or rejected. All charges paid by the applicant will be disclosed
10 If the applicant is not satisfied with DVA's decision, the applicant may apply for an internal review of the decision.
11 The internal review is carried out by a staff member that is independent of the initial request i.e. the staff member was not involved with the initial request. At this stage, if the applicant is not satisfied with the internal review decision, they may request a review with the OAIC.

FOI third party consultation process

Where information subject to a FOI request contains information in relation to a third party, the Advising and Public Law Team consult with the relevant third party to obtain consent seek their views and any objections on the release of information. In addition, the Department of Prime Minister and Cabinet is consulted where it is suspected that their approval will be required to release information.

Generally, this relates to personal information, business information, Commonwealth or State Government issues, International issues (infrequent) and documents connected with the Department of Prime Minister and Cabinet.

The Advising and Public Law Team uses an inter-agency flowchart in guiding consultation between agencies.

B.1.2 Administration of s59 SRCA and s331 MRCA requests

Section 59 of the SRCA and section 331 of the MRCA allow for the release of information held by DVA in relation to a person's claim.

Generally, requests for access to information under section 59 of the SRCA and section 331 of the MRCA are administered by the National FOI Processing Unit in Sydney. Requests in relation to high profile clients and requests that are considered to be highly sensitive or contentious are administered by the Advising and Public Law Team and/or the Principal Legal Adviser.

As DVA does not have a policy in respect of the administration of requests for information under section 59 of the SRCA and section 331 of the MRCA, these requests are administered in accordance with the FOI guidelines and where relevant, guidelines issued by Comcare in relation to the release of information under section 59 of the SRCA. Where a request includes information that relates to a *Veterans Entitlements Act 1986* (the VEA Act) component, the VEA component will be administered as a FOI request under the FOI Act.

Due to the volume of the SRCA and MRCA files, applicants who have been granted access to the requested information are invited to inspect the files at their nearest DVA office. Files that are to be made available for inspection are reviewed to ensure that only relevant information is able to be inspected. Inspections are generally by conducted by veteran advocates and are supervised by a DVA staff member.

There are no charges imposed for the release of information under section 59 of the SRCA and section 331 of the MRCA.

B.1.3 Other types of release of information from DVA

Generally, information that is released is released via specified protocol with established procedures, such as the release of information under subpoena or FOI.

The National FOI Processing Unit and Advising and Public Law Team administer requests for information outside of the FOI process, including:

- Emails requesting veteran's contact details (from veteran's and ex service organisations)
- Subpoenas
- Comcare requests for veteran claim information
- VEA, SRCA and MRCA determination information and claim forms
- Police requests
- Requests for death certificates

DVA has established procedures for the initial proof and subsequent authentication of identity, relationship status and Power of Attorney status.

B.1.4 Privacy

The Advising and Public Law Team, which includes the DVA Privacy Officer, provides policy and legal advice on privacy matters. Privacy queries are generally directed to the DVA Privacy Inbox and the guidelines issued by the Information Commissioner are referred to in providing advice on privacy matters.

In relation to the potential use of information by contracted providers, projects and Memoranda of Understanding are reviewed by the Advising and Public Law Team while contracts are subject to review by the Contracts Advisory Unit.

The DVA Privacy Officer conducts privacy training as requested by business areas. Training for all call centre and Veterans' Access Network (VAN) staff outlines DVA requirements for the proof of identification procedures and subsequent authentication of identification procedures in respect of Veterans, their Power of Attorney and Veterans' family members.

DVA relies on the following mechanisms to ensure adherence to the IPPs:

- Obtaining consent for the use and disclosure of personal information upfront, through notices on forms that are used for the collection of personal information.
- Content provided on the DVA Privacy Site.
- Initial Departmental proof of identification procedures and subsequent authentication of identification procedures in respect of Veterans, their Power of Attorney and Veterans' family members.
- Departmental procedures for confirming veteran consent for FOI and MRCA requests made on their behalf.
- DVA provides the information required under IPP 5 to the OAIC via a Proxy Information Digest.
- DVA quarterly income testing reminders in respect of Veterans' obligations to provide DVA with current information supports DVA in ensuring that personal information held by DVA is accurate.
- The provision of information from allied health providers and data matching with other Government Departments supports DVA in ensuring that personal information held by DVA is accurate.
- Communication protocols, electronic and email usage policies assist staff in understanding their obligations in relation to the use and disclosure of personal information.
- The requirement that the DVA Ethics Committee must approve the use of personal information in relation to medical use.

B.1.5 Information Publication Scheme

In accordance with Part 2 of the FOI Act, DVA must establish an Information Publication Scheme (IPS). From 1 May 2011, agencies have been required to publish a disclosure log on the agency's website, which lists information that has been released on response to the FOI access request.

DVA has policy of updating the disclosure log with required requests every second Friday. Personal information released under the FOI Act is not required to be published on the disclosure log.

The FOI, IPS and disclosure log pages link to each other on the DVA website. Internal Audit notes that this is in accordance with the Guidance for Agency Websites issued, in March 2011 by the OAIC, pursuant to Section 93A of the FOI Act, prior to the implementation of the FOI reforms in May 2011.

B.2 Internal Audit Methodology

The risks considered in the conduct of this internal audit and our methodology for assessing how DVA is managing the risks is outlined below.

B.2.1 Conformance Risks

Risk	Security, Privacy, Records Management
What we did to assess how DVA is managing the risk	Internal Audit held discussions with staff and assessed the adequacy of procedures in place to meet the requirements of the Privacy Act. We performed sample testing of requests for access to information under the FOI Act as well as s59 SRCA and s331 MRCA to assess whether these procedures are undertaken in practice. In conducting our testing, we reviewed a sample of relevant contracts with third party providers to determine whether the contracts adequately outlined the need for third party providers to adhere to the Information Privacy Principles. Internal Audit reviewed the privacy and FOI complaints recorded on the DVA Complaints and Feedback Management System for the period July 2011 to May 2012. Internal Audit notes that that IT related browsing of client/staff/supplier records was addressed in 2010-11 #20 Internet and Client Records Monitor. In addition, the storage and maintenance of personal and otherwise sensitive information, hardcopy client pension, medical, advocacy and HR files, policy, commercial and personal information were addressed in 2010-11 #23 Review of Protection of Information.
Our results and observations	DVA induction training and related materials do not make reference to the Privacy Act. The Privacy Site located in the DVA intranet contains out of date information and missing links. However, Internal Audit acknowledges that the Advising and Public Law team are aware of this and have assigned responsibility for updating the site to the DVA Privacy Officer. Our sample testing of requests for access to information under s59 SRCA and s331 MRCA identified one instance where documentation requested could not be located as it was lost.
Reference	*Section 2.1 on page 4.*

Risk	Documentation
What we did to assess how DVA is managing the risk	Internal Audit reviewed the Department's documented policies and procedures for the protection of privacy, adherence to the Information Privacy Principles and the administration of FOI requests. We assessed whether the policies and procedures are adequately documented to ensure compliance with relevant legislation.
Our results and observations	Staff in the Advising and Public Law team predominantly rely on the Guidelines Issued by the Information Commissioner under s93 of the FOI Act in administering the FOI Act. In addition, DVA has a policy document that is used in high profile and media FOI requests. The document outlines the steps that must be taken in addition to the FOI Guidelines, and prescribes the manner in which the Minister is to be briefed on these requests. The National FOI processing team in Sydney has a procedural guide titled "Processing of Freedom of Information Requests" which outlines Departmental procedures for receiving and administering requests. This procedural guide also prescribes the procedures that must be followed in proving and authenticating a person's identity, relationship with a person and Power of Attorney status. DVA does not have an endorsed policy for administering requests for information under s59 SRCA and s331 MRCA. In the absence of a relevant policy, staff have been following the FOI Guidelines and where relevant, Comcare Guidelines and associated case law in administering these requests.
Reference	*Section 2.3 on page 6*

Risk	Auditability, Authorisation/Accountability
What we did to assess how DVA is managing the risk	We held discussions with staff to determine the procedures in place for authorising the release of information. We reviewed the Department's documented policies and procedures for the administration of FOI requests and adherence to the Privacy Act. We performed sample testing of requests for access to information under the FOI Act as well as s59 SRCA and s331 MRCA to ensure that requests were authorised and an appropriate audit trail existed.
Our results and observations	The National FOI Processing Team and the Advising and Public Law Team have a well established division of responsibilities for the administration of requests for information. In conducting sample testing, Internal Audit observed opportunities for minor improvements to the standard of documentation and content of FOI file-notes on the files tested by Internal Audit, to enhance the auditability of FOI administration. These improvements include the need to withdrawn requests are identified in the database as withdrawn, and not closed. Internal Audit discussed the suggested improvements with staff from the National FOI Processing Team. Procedures for release of information – Advising and Public Law Team provide advice to DVA on staff on the appropriate use and disclosure of personal or otherwise sensitive information. In addition, DVA has an established Ethics Committee that must provide approval for the release of personal information for certain purposes.
Reference	*Section 2.2 on page 5*

Risk	Legal and Regulatory Compliance
What we did to assess how DVA is managing the risk	Internal Audit held discussions with staff and reviewed documented policies and procedures for the administration of FOI requests and adherence to the Privacy Act asses whether they are adequately documented to ensure compliance with the FOI Act and Privacy Act. We performed sample testing of requests for access to information under the FOI Act as well as s59 SRCA and s331 MRCA to assess whether FOI requests for information are administered in accordance with the FOI Act.
Our results and observations	During FOI file testing, Internal Audit identified the following breaches of the FOI Act in the administration of FOI requests tested; ▪ There were five identified instances where the statutory timeframe was not adhered to. Of these, there were two instances where charges were imposed, although the statutory timeframes (after taking into account the ability to stop the clock) were not met. This is a breach of Regulation 5 of the FOI Act, which states: *There is no charge for providing access to an applicant's personal information or for providing access outside the statutory processing period unless the Information Commissioner has extended that period*[7]. ▪ There were two instances where requests were not acknowledged within 14 days. DVA does not have an endorsed policy for administering requests for information under s59 SRCA and s331 MRCA. The National FOI Processing team administers routine s59 SRCA and s331 MRCA requests. Certain s59 SRCA and s331 MRCA requests, such as those that are contentious or are made by or on behalf of a high profile client, are administered by the Advising and Public Law team. In the absence of a relevant policy, staff have been following the FOI Guidelines and where relevant, Comcare Guidelines and associated case law in administering these requests. Comcare releases information under s59 SRCA and has developed guidelines in respect of the release of this information. There are no external guidelines specifically relevant to the release of information under s331 MRCA.
Reference	*Section 2.2 on page 5* *Section 2.3 on page 6*

7 Guidelines issued by the Australian Information Commissioner under s 93A of the Freedom of Information Act 1982, Section4, Page 3.

B.2.2 Performance risk

Risk	Efficiency
What we did to assess how DVA is managing the risk	Internal Audit held discussions with staff and observed procedures in place for administering requests for information under the FOI Act, s59 SRCA and s331 MRCA.
Our results and observations	The National FOI Processing team was established in 2009 as a result of consolidating state-based FOI processing teams. This consolidation has allowed for greater consistencies and efficiencies in the administration of requests for information under the FOI Act, s59 SRCA and s331 MRCA. The National FOI Processing team in Sydney operates a separate Microsoft Access database for each state locations, as well as a database for the administration of requests for information under s59 SRCA and s331 MRCA. Staff have experienced a number of inefficiencies in the operation of the database. Internal Audit has observed that the databases do not allow for generation of reports for an extended period (generally, issues and reduced functionality is observed when an attempt is made to generate a report for a period greater than six months). In addition, the database does not allow for staff to "stop the clock" to allow for an applicant to consider the imposition of charges, as allowed for under the FOI Act. As the database does not allow for the manipulation of request timeframes, there are instances where figures reported do not accurately reflect whether statutory timeframes are adhered to.
Reference	*Section 2.4 on page 7*

Appendix C Details of Testing

A range of formal tests were undertaken during this internal audit. The table describes the basis and results of testing undertaken.

Item Tested	Purpose of Test	Population[8]	Number tested	Basis of Sample	Result
FOI requests processed by the National FOI Processing team	To ensure that a sample of FOI requests have been processed in line with FOI legislation and guidelines.	4479	21	Manual random sample of FOI requests across each state for the period May 2011 to May 2012.	There were two instances where charges were imposed and the statutory timeframe was not met. There was one instance where documents requested could not be located.
FOI requests processed by the Advising and Public Law team	To ensure that a sample of FOI requests have been processed in line with FOI legislation and guidelines.	109	14	Manual sample of FOI requests including requests from journalists and requests from individuals for the period May 2011 to May 2012.	There were two instances where the applicant was not acknowledged within 14 days. There were three instances where the statutory timeframe was not met. In all instances, the over-run was low (generally, a few days).
Contracts with third party service providers	To ensure that DVA-contracted third party service providers are required to adhere to the relevant Privacy Act requirements and where relevant, the National Privacy Principles.	Not defined.	8	Selection of contracts for provision of services by various types of service providers across a range of business areas within DVA.	All contracts reviewed contained clauses requiring adherence to the Privacy Act.
Section 59 SRCA and section 59 MRCA requests	To review the process for administering requests for information under s59 SRCA and s331 MRCA. As there is no specific policy (refer Action Plan Item 3.5), IA did not make an assessment of the administration of these requests based on the files reviewed.				

[8] The total number of the specified item that is relevant to the scope of the review.

Appendix D Reference

D.1 Classification of Internal Audit Observations

Assigning a category to an internal audit finding is one of professional judgement. There are various factors that will be considered when an internal auditor assigns a category classification.

The purpose of assigning a classification to a finding is to communicate the importance of that finding with the audit committee, management and staff of the Department. This communication plays an important part in interpreting the internal auditor's opinion with respect to what priority a finding and its associated recommendation should be given.

In the table below are a number of the factors an internal auditor considers when assigning category classifications. It is important to note that an internal auditor will assign a category classification with the best interests of the 'organisation as a whole' in mind.

Factors considered when categorising findings	CR1 Observation	CR2 Observation	CR3 Observation
Priority of attention required (Who)	Branch Head and above	Branch Head and below	Director
Priority of attention required (Timeliness of action required)	Immediate commencement of corrective action	As soon as practical within the next 3 – 6 months.	When resources permit at the discretion of the organisation.
Likelihood or impact of the uncontrolled risk	Catastrophic/Major The likelihood/impact of the uncontrolled business or financial risk may threaten either the operation of the Department or the effective function of a critical/significant project and/or have a severe impact on the Department's reputation and credibility.	Moderate/Minor The likelihood/impact of the uncontrolled business or financial risk would threaten the efficiency or effectiveness of an aspect of operations.	Insignificant The likelihood/ impact of the uncontrolled business or financial risk could be dealt with by routine operations.
Suitability of the policies and/or procedures	No policies and/or procedures exist. Policies and/or procedures are not considered appropriate to manage a significant risk or function of the organisation.	No policies and/or procedures exist. Policies and/or procedures are not considered appropriate to manage a core business risk or routine function.	Policies and/or procedures are appropriate but out of date (the effect is not considered of serious consequence).

Factors considered when categorising findings	CR1 Observation	CR2 Observation	CR3 Observation
Compliance with documented procedures and policies	Policies and/or procedures are not being complied with.	Policies and/or procedures are not being complied with consistently (frequency and quality). Documentation does not reflect proper compliance with procedures and policies	Infrequent instances of non-compliance with policies and procedures were identified.
Breach of delegations (Financial and non-financial)	Any one of the following individually or in combination. Dollar values: Large Frequency of breaches: Regular Documentation to support exercise of delegation: Does not exist What/how: Breach of delegation exercised by Branch Head and/or above	Any one of the following individually or in combination: Dollar values: Medium Frequency of breaches: Periodic Documentation to support exercise of delegation: Not adequate What/how: Breach of delegation by middle management	Any one of the following individually or in combination: Dollar values: Small Frequency of breaches: Isolated Documentation to support exercise of delegation: Could be improved What/how: Breach of delegation reflecting ignorance
Fraud	All fraud or corrupt conduct identified is reported as CR1	N/A	N/A

BIR Business Improvement Recommendation - Arises where the internal auditor considers that the recommendation, if implemented, would result in a benefit accruing to the organisation (for example, through more efficient and/or cost effective processes, a reduction of expenditure or an increase in revenue.

D.2 Complexity Assessment

Corrective actions vary considerably in complexity and the complexity of an agreed action influences the timeframe for its implementation. Notwithstanding the need to take prompt corrective action, some aspects of a permanent solution to a CR1/CR2 observation may require more time than the nominal 3-6 months associated with this level of severity.

Factors that affect complexity include:

- Changes to legislation or regulation
- Significant changes to computer systems
- Cooperation/coordination of multiple business areas
- Requirement for new funding
- Dependency upon another agency

Management responses contain an assessment of the complexity provided by the relevant area.