



Australian
Competition &
Consumer
Commission

Submission for Executive Management Board

Meeting date	5 December 2016		
Meeting number	1617/12	Paper number	EMB1617/78
Title	For decision – Audit on the handling of confidential information for public registers – Implementation of recommendations		
Recommendation	The EMB agreed to the proposed steps for finalising the implementation of the auditors' recommendations on handling confidential information for public registers.		
Presented by	Sophie Ward (ext 1282) and Ron Neilan (ext 1368)		
EGM Sponsor	Tim Grimwade, EGM Legal and Economic Division		
Committee consideration and other consultation	Last considered on 26 April 2016 by the Executive Management Board Last considered on 25 November 2016 by the Audit Committee.		

1. Summary

- 1.1. Axiom Associates' May 2016 audit report on the ACCC and AER's handling of confidential information for public registers identified a number of risks for the organisation. A working group comprising representatives from various ACCC divisions and the AER has been established to consider the issues and develop ways to implement the auditors' recommendations.
- 1.2. This paper seeks EMB's support to finalise the working group's proposed steps for implementation.

2. Background

- 2.1. The *2015-2019 ACCC and AER Internal Audit Plan* includes an internal audit of public registers focusing on the handling of confidential information. The objective of the audit was to evaluate the efficiency, effectiveness and economy of public register confidential information handling systems, processes and procedures across the ACCC and AER.
- 2.2. Axiom Associates was commissioned to conduct the audit of ACCC/AER public registers, which it did over February and March 2016.
- 2.3. Divisional EGMs were provided a draft of the audit report on 1 April 2016 and asked to provide management response contributions by 11 April 2016. These responses were incorporated into the consolidated management response for each recommendation in the final report.
- 2.4. The final report was considered by EMB on 26 April 2016. EMB agreed to endorse the consolidated management response, and take ownership of remediation of the recommendations.

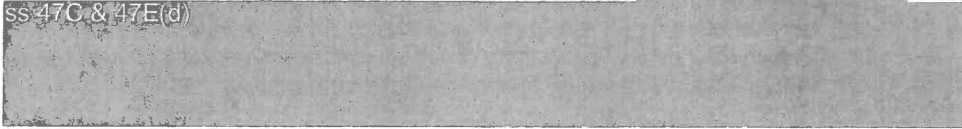
- 2.5. Axiom Associates provided its final report to the Audit Committee on 13 May 2016. A copy of the report is contained in the EMB paper presented on 26 April 2016. Management suggestions are included in Attachment D to that report and may be taken forward by the working group as part of the ongoing process to improve the organisation's handling of confidential information.

Auditors' recommendations

- 2.6. The report identified a number of potential risks to the organisation and made the following recommendations to address these issues.
- 2.7. Recommendation 1: that the ACCC and AER explicitly address the risk of confidential information being improperly released within each responsible division's risk mitigation strategy.
- 2.8. Recommendation 2: that the ACCC:
- implement a competencies-based approval and publication workflow for each public register
 - document the publication and approval process used to prepare and publish information on each public register and provide these documented procedures and control checklists to staff responsible for the process. The development of a standard template could be used by all divisions to drive key principles of:
 - approval of material for publication by at least three staff with appropriate competency and authority
 - restricted access to publish information
 - details of security setting protocols
 - implement induction and refresher training for staff involved in administering each public register on methods to prepare and publish information, including appropriate handling of confidential information.
- 2.9. Recommendation 3: that the ACCC and AER develop a standard mechanism (such as a working group or mailing list) to share improvements in the administration of public registers, particularly lessons learnt in relation to handling confidential information.
- 2.10. Recommendation 4: that the ACCC implement restricted system permissions for reclassification of documents and publication of information to appropriately authorised and skilled staff.

Implementation of auditors' recommendations

- 2.11. MARD is project managing the implementation of the recommendations, with Tim Grimwade as the EGM sponsor. In addition, following discussions at the Audit Committee, the implementation project will also include the ACCC's own review of its public registers to determine which registers no longer need to be maintained. This paper includes recommendations relating to both projects.
- 2.12. The Audit Committee was updated on this project on 25 November 2016. The submission to the Audit Committee, indicating progress in relation to each of the auditors' recommendations, is at **Attachment A**.

- 2.13. In response to recommendation 1, Tim Grimwade advised EGMs by email on 23 June 2016 and 17 August 2016 of the need to consider ^{ss 47C & 47E(d)} 
- 2.14. The working group, comprising representatives from various divisions of the ACCC and the AER, was established in response to recommendation 3. In addition to the group email address (Public Registers Review Group) and VCU meetings which are held as needed, an intranet page will be created to share information and lessons learned on the handling of confidential information for public registers.
- 2.15. In response to recommendation 2, the working group has considered what was currently in place across the organisation, and developed and documented a number of processes relating to public registers for use across the organisation. Note that this recommendation applies only to the ACCC, and not to the AER. In consultation with the working group, we have developed a template for reviewing and approving documents for publication to the public registers (**Attachment C**), a checklist for use in the approval and publication process (**Attachment D**), and general guidelines for training staff involved in the creation, review, approval or publication of public register documents (**Attachment E**). These proposals are the principal measures by which the ACCC may reduce some of the risks identified in the audit report.
- 2.16. While the scope of the audit was restricted to public registers, members of the working group noted that there may be benefits in extending some of these processes to non-public register material published on the ACCC or AER websites.
- 2.17. Recognising the differences between the various public registers, the guidelines and processes have been designed to include a degree of flexibility. This should enable divisions to tailor the systems according to the needs of their own divisions and public registers, while still meeting the recommendations of the auditors. The proposals are also dependent on the capabilities of the IT systems available. In particular, the checklist at Attachment D should become part of the approval system where the system allows it.
- 2.18. In response to recommendation 4, it is proposed that restrictions on reclassifying documents be achieved through policy and procedures. As the ACCC transitions to new IT systems, it may be possible to implement this recommendation through IT based controls. The working group will continue to monitor this possibility.

2.19. ^{ss 47C & 47E(d)} 

2.20. 

3. Recommendation

- 3.1. Divisions with responsibility for a public register should address in their divisional plans the risks of disclosing confidential information on the public register, and

confirm this has been done by providing the Doris link to the business plan (or amended business plan) to Ron Neilan on behalf of the working group.

- 3.2. Divisions with responsibility for a public register should tailor and adopt the proposed approval and publication process, according to the requirements of their public registers. Responsibility: each EGM.
- 3.3. L&D should be asked to assist with development of an online module on handling confidential information and public registers. Responsibility: each Doug Cross, GM People and Culture Branch.
- 3.4. Divisions should ensure the relevant staff undertake training on the handling of confidential information and public registers. This training should be based on the guidance provided, but can be tailored by divisions as they consider most appropriate for their staff and their public register functions. One option is to have staff complete an on-line learning module. Responsibility: each EGM.
- 3.5. Support for an intranet page to be developed to share information and lessons learned on the handling of confidential information for public registers. Divisions should identify to the working group the person responsible for managing each public register in their division so they can be identified as a contact person on the intranet page when established. Responsibility: each EGM.
- 3.6. Support by EGMs for the continued participation of their nominees in the working group to continue meeting to share improvements in the administration of public registers, particularly lessons learnt in relation to handling confidential information.
- 3.7. Following consultation by the working group, divisions should confirm which of their public registers can be retired without the need for legislative change by 31 March 2017 with a plan of steps needed to retire them by June 30 2017. Responsibility: each EGM.

4. Attachments

- A Audit Committee – Action Sheet
- B Business plan example
- C Approval and publication workflow
- D Checklist
- E Training principles

Action Sheet - Public Registers - Handling of Confidential Information Performance Audit

Area audit: ACCC and AER

Report date: November 2016

Date of audit: March 2016

Audit recommendation	Management comments	Resp. officer	Estimated completion date	Risk rating	Status as at November 2016
<p>Recommendation 1:</p> <p>It is recommended that ACCC and AER explicitly address the risk of confidential information being improperly released within each responsible division's risk mitigation strategy.</p>	Agreed	Executive Management Board (EMB) via EGMs to implement in next divisional business plan reviews.	March 2017 (revised from July/August 2016) - timing subject to the completion date of divisional plans	[REDACTED]	EGM commitment to incorporate in business plans when they are finalised: <u>D16/141627</u> .

Recommendation 2:

Audit recommends that ACCC:

- implement a competencies-based approval and publication workflow for each public register
- implement induction and refresher training for staff involved in administering each public register on methods to prepare and publish information, including appropriate handling of confidential information.
- document the publication and approval process used to prepare and publish information on each public register and provide these documented procedures and control checklists to staff responsible for the process. The development of a standard template could be used by all divisions to drive key principles of:
 - approval of material for publication by at least three staff with appropriate competency and

Agreed.

EMB

December 2016

Completed

Standard ACCC competencies-based approval and publication workflow developed and documented at D16/148171.

Standard training principles developed and documented at D16/149040.

Standard control checklist created at D16/148189.

These documents will be submitted in a paper to the

authority

- o restricted access to publish information
- o details of security setting protocols.

EMB to consider endorsing adoption and implementation by divisions.

Recommendation 3:

Audit recommends that ACCC and AER:

develop a standard mechanism (such as a working group or mailing list) to share improvements in the administration of public registers, particularly lessons learnt in relation to handling confidential information.



July/August for establishment of working group

EMB

Agreed.
To be considered as part of the project.

Completed

Email distribution group established. Group has met to discuss its role and implementation of the audit recommendations.

On completion of all recommendations, an intranet page will also be set up to facilitate sharing of information on the administration of public registers.

Recommendation 4:

Audit recommends that ACCC implement restricted system permissions for reclassification of documents and publication of information to appropriately authorised and skilled staff.



Following the establishment of the training program.

EMB

Agreed.
To be considered as part of the project.

Completed

This recommendation is achieved through the implementation of recommendations 2 and 3.

Note: The review of public registers is a separate project which did not form part of the auditors' recommendation but the COO has requested that it be considered as part of this project. A number of public registers have been identified as potentially suitable to be archived or deleted.

5. Risk Description	Impact of risk happening	Consequence Rating	Likelihood Rating	Risk Level
Confidentiality Breach	Unable to adequately perform functions Loss of confidence in the ACCC	SS 47C & 47E(d)		
Risk Sources	Current controls and adequacy of controls Fully adequate = A Moderately adequate = M Inadequate = I	Person Responsible	By When	Person Monitoring
Complex information management requirements due to complexity of IT architecture increases potential for human error	Processes and systems have some safeguards built-in. On the job training about procedure Most ACCC generated content is initially created from template text and is subject to review and approval..	Office Manager	Ongoing	GM C&S
Staff error and confidential information released in a public document or on the internet	Established workflows and protocols for publishing material on public register	Office Manager	Ongoing	GM C&S
Confidential information release via court submission or correspondence to a third-party error	Legal unit oversight of all litigation and key sensitive correspondence GM and EGMs sign off on all confidential information Ongoing training for all staff	EGM, GMs and Office Manager	Ongoing	EGM

Attachment B - Business Plan example

5. Risk Description	Impact of risk happening	Consequence Rating	Likelihood Rating	Risk Level
Confidentiality Breach	Unable to adequately perform functions Loss of confidence in the ACCC	SS 47C & 47E(d)		
Risk Sources	Current controls and adequacy of controls Fully adequate = A Moderately adequate = M Inadequate = I	Person Responsible	By When	Person Monitoring
Other unauthorised use or release of confidential information	Induction training Conflict of interest checks Conditional provision of information to non-MARD staff	EGM, GMs and Office Manager	Ongoing	EGM

ACCC publication and approval framework

Step 1: preparation

Ensure confidential information is clearly identified. Where possible, apply an ACCC/AER wide approach to identifying confidential information.

Distinguish confidential versions from publication version. Where possible, apply an ACCC/AER wide approach for distinguishing versions.

Where possible, apply system based controls to prevent non-public register documents being published.



Step 2: initial review

The initial review is to be by a person who is familiar with the content, aware of the risks of publishing confidential information, and who has completed the appropriate training.

The initial reviewer checks the proposed public register content contains no confidential information.

Where possible, the initial review should be conducted and captured in the content publication system.

The initial reviewer forwards the public register content for a second review.



Step 3: second review

The second review is to be by a person who is familiar with the content, aware of the risks of publishing confidential information, and who has completed the appropriate training.

The second reviewer checks the proposed public register content contains no confidential information. If appropriate, external parties should be consulted about any information in the content that may raise confidentiality issues following established protocols.

Where possible, the second review should be conducted and captured in the content publication system.

The second reviewer forwards the public register content for approval.



Step 4: approval

Approval is to be by a person who is aware of the risks of publishing confidential information and who has completed the appropriate training.

The approver checks the proposed public register content contains no confidential information. The approver should question any information included in the content that they have concerns about.

Where possible, approvals should be conducted and captured in the content publication system.

The approver authorises publication.



Step 5: publication

The ability to publish is restricted to staff who have had appropriate training in the approval and publication process.

Check all relevant approval processes have been completed before publishing.

Publish and immediately advise the reviewers (or other nominated person) that the content is live and ready to be checked. Where possible, this process should be automated.



Step 6: post-publication check

Check the document immediately after publication on the live site.

Action any breach immediately and in accordance with prescribed processes.

Advise SES officer of any breach as soon as possible.

Public register review and approvals - standard template

The auditors recommend the development of a standard template to drive the key principles stated above being:

- Approval of material for publication by at least three staff with appropriate competency and authority
- Restricted access to publish information
- Details of security setting protocols

As an example of what this may entail, below is a short template (based on one used in Mergers) when reviewing and approving content the informal merger reviews public register. This form may be suitable to adopt and develop / enhance conceptually for all areas.

Please confirm the following:

Initial reviewer: [name]	Second reviewer: [name]	Approver: [name]
<input type="checkbox"/> All new content has been reviewed	<input type="checkbox"/> All new content has been reviewed	<input type="checkbox"/> All new content has been reviewed
<input type="checkbox"/> All new documents have been opened and reviewed (all PDF, Word and HTML versions)	<input type="checkbox"/> All new documents have been opened and reviewed (all PDF, Word and HTML versions)	<input type="checkbox"/> All new documents have been opened and reviewed (all PDF, Word and HTML versions)
<input type="checkbox"/> None of the information to be published is confidential	<input type="checkbox"/> None of the information to be published is confidential	<input type="checkbox"/> None of the information to be published is confidential
<input type="checkbox"/> Approved for publication	<input type="checkbox"/> Approved for publication	<input type="checkbox"/> Approved for publication

ACCC training principles for public registers and handling confidential information

Different training is appropriate depending on the level of competency required. Some staff members will need to undertake more than one level of training.

Training for all staff - *may be involved in steps 1, 2 or 6*

- All ACCC/AER staff should receive training on handling confidential information, the risks associated with disclosing confidential information, and the use of public registers.
- If possible, this training should form part of the induction process, with a requirement for refresher training at appropriate intervals.
- If possible, this training should be conducted online. Online training would be more flexible, less resource intensive and would automatically create a log of who has received training and when.

Training for reviewers and approvers - *may be involved in steps 2, 3 or 4*

- Staff who are authorised to conduct a second or subsequent review must have additional training.
- Additional training must include:
 - Handling of confidential information
 - Risks of publishing confidential information
 - Steps required to conduct a thorough review
 - Recording the review
 - Public register review, approval and publication process
- This training should occur at least once a year or as required.
- This training may need to be specific to a particular public register or division, but resources should be shared where possible.

Training for publishers - *may be involved in step 5*

- Staff who are authorised to publish to the public register must have additional training.
- Additional training must include:
 - How to publish to the public register
 - Public register review and approval process
 - Post-publication process
- This training should occur at least once a year or as required.
- This training may need to be specific to a particular public register or division, but resources should be shared where possible.