



**Australian Competition & Consumer
Commission (ACCC)**

Australian Energy Regulator (AER)

**Internal Audit: Public Registers –
Handling Confidential Information**

Final Report - March 2016



Engagement History

Stage	Planned Timing	Actual
Engagement plan approved by	15 January 2016	15 January 2016
Entry interview	12 January 2016	12 January 2016
Fieldwork completed	14 February 2016	21 March 2016
Exit interview	22 February 2016	26 April 2016
Draft Report	29 February 2016	29 March 2016
Management comments received	14 March 2016	15 April 2016
Final report to management	14 March 2016	26 April 2016
Final report to Audit Committee	15 April 2016	13 May 2016

Table of Contents

1. EXECUTIVE SUMMARY	4
1.1 Background.....	4
1.2 Objective and Criteria.....	4
1.3 Summary of Findings and Recommendations.....	5
1.4 Overall Observations and Conclusion.....	6
2. INTERNAL AUDIT REPORT.....	7
2.1 Objective	7
2.2 Scope.....	7
2.3 Methodology	7
2.4 Audit Outcomes	9
2.5 Risk Ratings.....	10
2.6 Form of Assurance	11
3 DETAILED FINDINGS.....	12
Finding 1: Adequacy of risk mitigation strategies	12
Finding 2: Control Frameworks	14
Finding 3: Support systems and applications	22
ATTACHMENT A – RISK RATING	26
ATTACHMENT B – PUBLIC REGISTERS RISK ASSESSMENT	27
ATTACHMENT C – BREACH INCIDENT ANALYSIS.....	30
ATTACHMENT D – PUBLICATION STREAMS	32
ATTACHMENT E – MANAGEMENT SUGGESTIONS.....	33
ATTACHMENT F – STAKEHOLDERS CONSULTED.....	35
ATTACHMENT G – STATEMENT OF RESPONSIBILITY	37

1. Executive Summary

1.1 Background

The 2015–19 Australian Competition & Consumer Commission (ACCC) and Australian Energy Regulator (AER) Internal Audit Plan includes a performance audit of 'Public Registers' focusing on the handling of confidential information. Axiom was engaged to conduct this audit for the period February to March 2016.

The ACCC and AER are required to create and maintain public registers under the legislation they administer. They also maintain several voluntary public registers. There are 53 statutory and voluntary public registers (including the Freedom of Information (FOI) disclosure log). 36 of the 53 public registers have either current content and/or have been updated within the last two years. The information they contain can vary from a few sentences giving a decision only, through to a detailed comprehensive file. All registers are available on the ACCC and AER external facing website.

ACCC and AER staff rely on online publication systems to upload information and documents to relevant registers. Each branch and division with responsibility for maintaining registers follow slightly different processes to ensure that any confidential or redacted information is handled appropriately.

In the past 18 months, the ACCC has experienced several incidents where confidential or redacted information was inadvertently published to its registers. In some cases these publications contained sensitive commercial-in-confidence information. In all cases the information was promptly removed. Organisations or individuals that were able to be identified as having accessed the information were notified of its confidential nature and requested to discard the information.

Irrespective of remedial steps taken when a breach has occurred, a breach presents significant potential reputational consequences to the ACCC or AER. It could also give rise to significant financial damages being sought for loss or injury suffered. This has the potential to harm future information gathering processes and impact on the ACCC and AER's effectiveness as a regulator.

1.2 Objective and Criteria

The objective of this audit was to evaluate the efficiency, effectiveness and economy of public register confidential information handling systems, processes and procedures across the ACCC and AER.







The criteria assessed during the audit in order to meet the objective were:

- Public register confidentiality risks are adequately captured in divisional risk mitigation strategies.
- There are adequate and robust controls and effective document and confidential information-handling systems and processes in place.
- Public register confidentiality disclosures and information management requirements are adequately communicated to stakeholders.
- Critical decision points in public register processes, including approval of information for publication, are handled by staff with appropriate levels of knowledge and authority.

A copy of the scope and methodology is included within Section 2.

1.3 Summary of Findings and Recommendations

A summary of the issues identified during the course of this audit is outlined in the table below. The assessment of risk ratings in relation to each finding is addressed in section 2.5

F.1	Some divisions do not adequately capture and address the risk that confidential information could be inadvertently released on a public register within their risk mitigation strategies.	
F.2-1	A strong three-tier competency based approval process has been implemented for all AER public registers.	Positive
F.2-2	The ACCC FOI disclosure log is administered using a robust approval and publication workflow.	Positive
F.2-3	The absence of critical controls in some ACCC public register systems and processes increases the risk of confidential information 'leakage' during administration and publication stages. Control gaps identified include: <ul style="list-style-type: none"> • inadequate staff training in public register administration and management of confidential information • lack of procedural and process documentation to adequately support publication and approval processes, including to promote knowledge transfer and manage shared administration • non-competency-based and manual approval workflows. 	
F.2-4	There is currently no formal mechanism to enable sharing of lessons learnt and enhancements in public register administration across ACCC and AER to facilitate continuous improvement.	
F.3-1	Secure record-keeping systems (TRIM/DORIS) are used to electronically store public register materials.	Positive
F.3-2	Most public registers are administered across multiple service lines and without fit-for-purpose project management systems; none utilise system-based approval and preventative controls, as well as documented protocols to prevent unauthorised publication.	
F.3-3	There is no common workflow or automated publication process used throughout ACCC and AER.	
F.3-4	When information is redacted (unless a document is scanned or converted from TIF to PDF format) there is risk that confidential information may still be accessible to external parties.	

Audit Recommendations Summary

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

It is also recommended that ACCC and AER:

- explicitly address the risk of confidential information being improperly released within each responsible division's risk mitigation strategy
- 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.

In order to address the issues/risks highlighted in this audit, it is recommended that the ACCC & AER assign centralised responsibility to the remediation of findings raised in this report. Consideration should also be sought for ongoing monitoring and compliance activities.

1.4 Overall Observations and Conclusion

In our opinion the public register confidential information handling systems, processes and procedures used across the ACCC and AER are diverse in design and application. Only a few public register systems, processes and procedures incorporate critical controls, including those necessary to prevent breaches of confidentiality. Audit found AER's public register systems, processes and procedures in general, to be sufficiently robust. Overall, ACCC has an inadequate system of internal control to prevent confidential information breaches in most public register categories.

Four high level recommendations are made. A number of discretionary enhancements are outlined in the management suggestions in Attachment E to this report.

While management's response to our identified findings and application of relevant recommendations is likely to improve the controls and processes overseeing the administration of public registers by ACCC and AER, it is important for such actions to be considered in accordance with ACCC and AER's risk appetite and in the context of broader organisational issues and priorities.

2. Internal Audit Report

2.1 Objective

To evaluate the efficiency, effectiveness and economy of public register confidential information handling systems, processes and procedures across the ACCC and AER.

2.2 Scope

Review the adequacy and suitability of public register confidential information handling systems, processes and procedures, including document handling, document management, security settings, approval points, risk mitigation strategies and publication applications. In particular, to assess the:

- adequacy of document handling processes and document management systems e.g. DORIS/TRIM, TrackIT and CRM¹
- use of document security settings and the effectiveness of those settings
- effectiveness of approval points ahead of publication
- suitability of online publication applications and tools
- adequacy of other risk mitigation strategies to address staff handover, workload pressures and level of vigilance.

2.3 Methodology

The methodology required the following steps to be undertaken:

Governance and staff awareness

- a. Identified and obtained existing policy, procedures and process documentation relevant to the audit. Identified and confirmed relevant legislation, in particular the *Competition and Consumer Act 2010*;
- b. Understood and documented via stakeholder discussions the roles and responsibilities, relating to public register processes within ACCC;
- c. Understood and documented through discussions with stakeholders and review of relevant guidance, ACCC's approach to the management of public registers including the confidential information handling systems, processes and procedures.

Audit Sampling and Analysis

- d. For a sample of recent public register records across registers identified during our planning as high risk, evaluated the efficiency, effectiveness and economy of confidential information handling systems, processes and procedures by:
 - reviewing current processes and procedures through staff interviews, document reviews and actual process reviews
 - conducting a gap analysis of current processes and procedures with best practice standards

¹ TrackIT is a reporting and communication information tool. It is an in-house reporting tool to provide ACCC staff with a means of recording and reporting actions they undertake on matters. Microsoft Dynamics CRM is also used in some business areas and is planned to be rolled out as a replacement for the ageing TrackIT system.

- assessing the level of consistency in processes and procedures across branches and divisions
- identifying any changes required to ensure the efficiency and effectiveness of confidential information handling systems, processes and procedures.

In performing step d. above, we have considered the following guidance:

- *ANAO Report No.53 2011–12 Performance Audit Records Management in the Australian Public Service*
- The Australian Privacy Principles (APPs) under the *Privacy Act 1988 (Cth) and Australian Privacy Principles Guidelines* issued by the Office of the Australian Information Commissioner

Reporting

- e. Consultation occurred with key stakeholders throughout the audit. Findings of the audit and proposed recommendations were discussed with the Governance & Support staff prior to the preparation of the draft and final reports.

Our methodology also considers the possible impact of the occurrence of fraud in all engagements.

Our preliminary assessment includes the identification of relevant fraud indicators and our field work was sensitive to these indicators. Where necessary we will identify and report fraud related issues to the ACCC. (Note: No fraud related issues were identified during the audit).

2.4 Audit Outcomes

A summary of the results of the audit against the in-scope areas is outlined in the table below:

Element	Audit assessment
<p>Adequacy and suitability of document handling processes and document management systems.</p>	<p><u>Positive Aspects</u></p> <p>Public register document handling and management processes are sufficiently robust for AER and FOI disclosure public registers. Stronger procedures have been implemented and systems are being enhanced to improve the control framework for managing merger and adjudication public registers.</p> <p>Secure record-keeping systems (TRIM/DORIS) are used to electronically store public register materials.</p> <p><u>Findings Summary</u></p> <p>There are instances where ACCC process controls could be strengthened and publication workflows streamlined and more consistently implemented to reduce risk. Improvements to reduce risk could include structured staff training in public register administration and handling of confidential information, documented processes and procedures for knowledge transfer as well as competency and system-based approval workflows.</p>
<p>Adequacy and suitability of risk mitigation strategies and associated controls including use and effectiveness of security settings, approval points and staff handover strategies.</p>	<p><u>Positive Aspects</u></p> <p>The approval workflow for public register documents is sufficiently robust for AER and FOI disclosure registers.</p> <p><u>Findings Summary</u></p> <p>The risk and management of confidential information breaches that may occur as a result of public register administration processes are not captured in all responsible division risk mitigation strategies.</p> <p>Protocols for applying security settings in relation to public register records are not documented and understood by all ACCC staff.</p> <p>There is significant reliance on the corporate knowledge of a select number of staff. There is limited reference to documented procedures for the administration of public registers and handling of confidential information. Documented procedures could support the improvement of knowledge transfer.</p> <p>The workflow approval process could be streamlined and more consistently implemented across the ACCC to reduce risk. Improvements to reduce risk could include competency and system-based approval workflows.</p>





Element	Audit assessment
<p>Adequacy and suitability of publication applications and tools.</p>	<p><u>Positive Aspects</u></p> <p>Development and roll-out of an enhanced and fully supported workflow, and content management applications, for administration of public registers is underway.</p> <p><u>Findings Summary</u></p> <p>There is no uniform publication process using approved systems employed by ACCC and AER. Some publication mechanisms do not utilise automated transfer of information to content management systems. Direct upload of information to website platforms reduces approval points and increases the risk of human error leading to breaches of confidential information.</p> <p>Protocols for managing document versions in TRIM are not documented and understood by all ACCC staff. This can lead to inappropriate updates to public registers.</p>

2.5 Risk Ratings

We have based our risk ratings on the ACCC ratings risk outlined in **Attachment A**.

Our assessment of risks for the findings raised also adhered to the methodology recommended in the Australian and New Zealand Risk Management Standard (AS/NZS ISO 31000:2009). This standard categorises organisational risks according to their consequence and likelihood.

Risk Rating legend:

	<p>Extreme Risk - This is a serious internal control or risk management issue that if not mitigated, may, with a high degree of certainty, lead to:</p> <ul style="list-style-type: none"> • Substantial financial losses, possibly in conjunction with other weaknesses in the control framework or the organisational entity or process being audited. • Serious violation of corporate strategies, policies, or values. • Significant or sustained reputation damage, such as negative publicity in national or international media, external enquiry • Significant or sustained adverse impact to staff safety.
	<p>High Risk - This is a serious internal control or risk management issue that if not mitigated, will likely lead to:</p> <ul style="list-style-type: none"> • Major financial losses, possibly in conjunction with other weaknesses in the control framework or the organisational entity or process being audited. • Violation of corporate strategies, policies, or values. • Serious reputation damage, such as negative publicity in national or international media. • Major adverse impact to staff safety.
	<p>Medium Risk- This is an internal control or risk management issue that could lead to:</p> <ul style="list-style-type: none"> • Financial losses. • Loss of controls within the organisational entity or process being audited. • Reputation damage, such as negative publicity in local or regional media. • Adverse impact to staff safety.
	<p>Low Risk - This is an internal control or risk management issue, the solution to which may lead to improvement in the quality and/or efficiency of the organisational entity or process being audited. Risks are limited.</p>

2.6 Form of Assurance

The engagement was performed as an audit as defined under Australian Standard on Assurance Engagements (ASAE) 3000 "Assurance Engagements Other than Audits or Reviews of Historical Financial Information". Our procedures were designed to provide reasonable assurance as defined by ASAE 3000, which recognises the fact that absolute assurance is rarely attainable due to such factors as the use of judgment in gathering and evaluating evidence and forming conclusions, the use of selective testing, the inherent limitations of internal control and because much of the evidence available to the auditor is persuasive rather than conclusive in nature.

We would like to take this opportunity to thank the ACCC and AER staff for their assistance during our audit.

Dom Susic
 Certified Information Systems Auditor (ISACA)
 Certified Practising Accountant (CPA)

Partner
 Axiom Associates

3 Detailed Findings

Finding 1: Adequacy of risk mitigation strategies

Background

The ACCC and AER administer 53 public registers (including the FOI disclosure log). There are 14 public registers that are administered voluntarily to provide transparency in the public interest. The remaining 39 are required to be administered under legislation. 10 of the 53 registers do not include any records or are not being actively maintained².

The audit identified the inherent risk attached to each of the public registers in the context of the following factors:

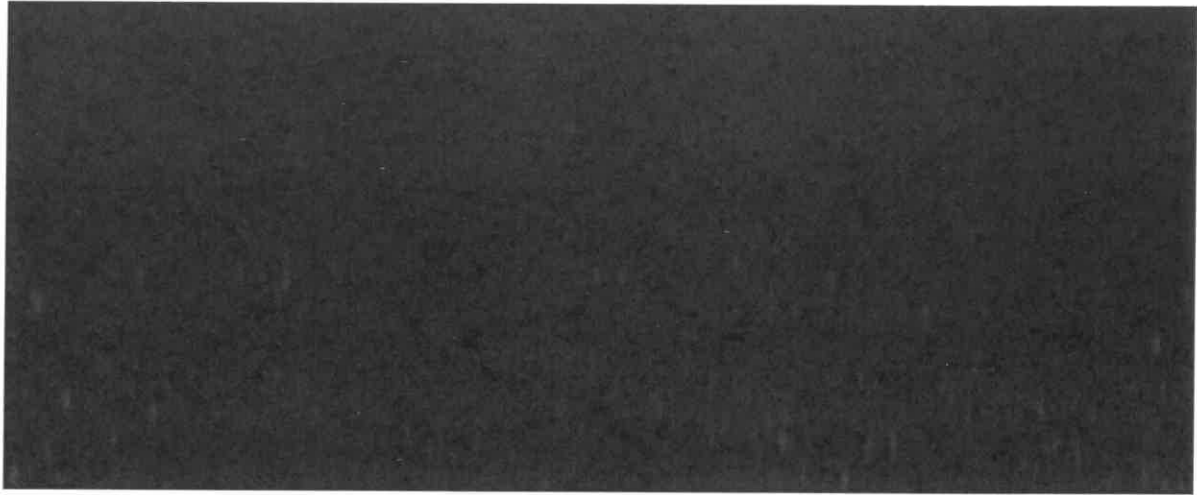
- sensitivity of information managed in relation to the public register (potential confidentiality issues)
- requirement for redaction or modification of information prior to publication
- frequency with which the public register is updated
- whether clearly understood and documented approval and publication workflows exist in relation to the public register.

Risk attached to each public register was based on stakeholder interviews and information received from business areas.

These factors were also weighted in accordance with perceived impact on risk. For example, the more frequent the requirement for information to be redacted or otherwise modified the higher the perceived risk and the higher the weighting score. The final risk rating for each of the registers is outlined in Attachment B.

Observation

² This occurs where, for example, the legislation is changed and the public register is no longer required to be updated or there have been no instances where publication on a statutory register has been required.



Findings

F.1	
-----	--

Implication



#	Recommendation	Management Response	Responsible Officer and Timing
R.1	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.	Agreed.	Executive Management Board via Executive General Managers to implement in next divisional business plan reviews.

Finding 2: Control Frameworks

Background

The ACCC and AER administer a large number of public register publication processes and systems with a number of varied control frameworks. There are 3 separate publication streams employed (refer to Attachment D). Local variations in document handling and publication and approval workflows exist between public register processes.

In the past 18 months, the ACCC has experienced several incidents where confidential or redacted information was inadvertently published to its registers (refer to Attachment C). In some cases these publications contained sensitive commercial-in-confidence information. In all cases the information was promptly removed, and all organisations or individuals that were able to be identified as having accessed the information were notified of its confidential nature and asked to destroy it.

However, irrespective of remedial steps taken when a breach has occurred, a breach presents significant potential reputational consequences to the ACCC or AER. It could also give rise to significant financial damages being sought for loss or injury suffered. This has the potential to harm future information gathering processes and impact on the ACCC and AER's effectiveness as a regulator.

Observation

Audit reviewed the incidents where confidential or redacted information was inadvertently published to ACCC registers (there are no records of any instances in relation to AER public registers). Based on discussions with business area stakeholders, audit identified a probable cause in relation to each incident. Audit's analysis is outlined in Attachment C.

Audit also reviewed the existence of key controls to ensure proper management of public registers and handling of confidential information. This included examining the adequacy of critical internal controls as follows:

- Secure record-keeping in approved systems. (A)

- Approval of documents and redacted information by appropriately competent and authorised staff. (B)
- Controls to prevent information changes and publication by other staff. (C)
- Adequate formal training for all staff involved in administration of registers. (D)
- Sufficient and appropriate documented procedures and processes and document protocols (including security settings) for accessible reference by staff (must be current). (E)
- Appropriate positioning and timing of approval and review points. (F)
- Confirmation of the confidential nature of information with external applicant/subject entity. (G)
- Log of process tasks and involved personnel. (H)

Key controls were identified with reference to interviews with key stakeholders responsible for administering a sample of public registers (including registers assessed as high risk – refer Attachment B) and examination of a sample of public register records and available guidance.

The following table summarises the existence of the aforementioned controls in relation to sampled public registers by category.

Sampled public register category	(A)	(B)	(C)	(D)	(E)	(F)	(G)	(H)
AER retail and networks								
ACCC:								
Mergers								
Adjudication								
Price Notifications								
Telecommunications								
Enforcement								
FOI disclosure log								

- ✓ controls exist for all public registers sampled in category
- ✗ controls absent from one or more public registers in category
- R reservation – refer explanation below

AER public registers

Four active public registers are maintained by AER:

- Register of Network Exemptions
- Register of Retail Exemptions
- Register of Retail Authorisations
- Register of Retailers (RoLRs).



Mergers public registers

There are five merger public registers.



The Informal merger clearances register is a voluntary register which is used in place of the statutory formal merger clearance register as this is more economic for applicants³. Non-statutory Guidelines are provided on the website outlining how the register is used. The merger record type in TRIM/DORIS is restricted to a select group of merger staff and documents are given an in-confidence security setting when they are not for publication. Other staff outside of mergers do not have access to merger records.

In mergers a director and a GM must approve each document for publication. [REDACTED]

Adjudication public registers

There are four public registers on which ACCC authorisations and notifications are published. [REDACTED]

Access to Services and Price Notification public registers

Information was received from business areas on all five Access to services public registers and the Price notification public register. This was used to assess the inherent risk of each of these registers (refer Attachment B). [REDACTED]

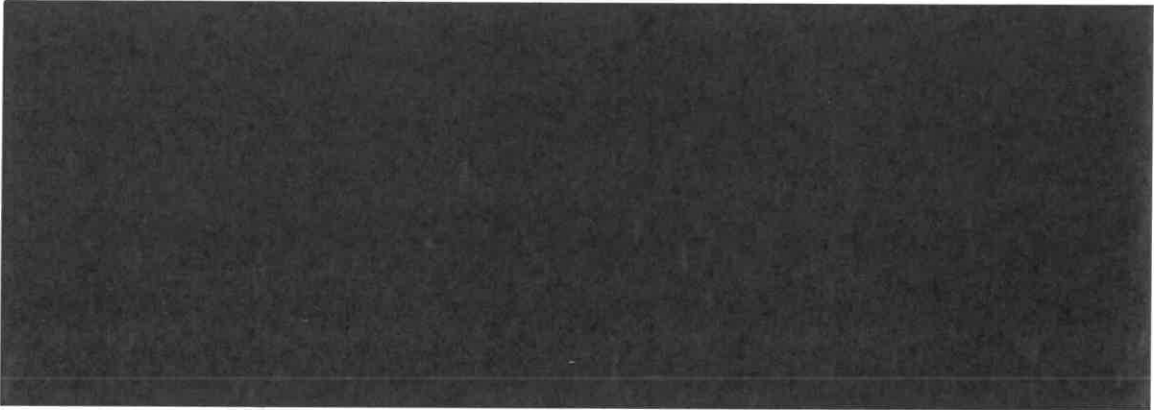
³ The informal merger register comprises the following records:

- 1) description of transaction and timeline for publication of ACCC decision
- 2) Market enquiries letter
- 3) Statement of Issues
- 4) Any associated undertaking (court enforceable document).

⁴ Approximately [REDACTED] ACCC staff.

⁵ Refer Attachment D for further information.

The Price notification public register includes proposals for pricing increases in relation to monopoly market participants in accordance with the *Competition and Consumer Act 2010* (CCA) as well as interim and final decisions of the ACCC assessing these price rises⁶. Documents are received in hardcopy as well as softcopy from market participants and include requests for identified information to remain confidential (these documents are saved in DORIS/TRIM). Proposals need to be received in the correct format.

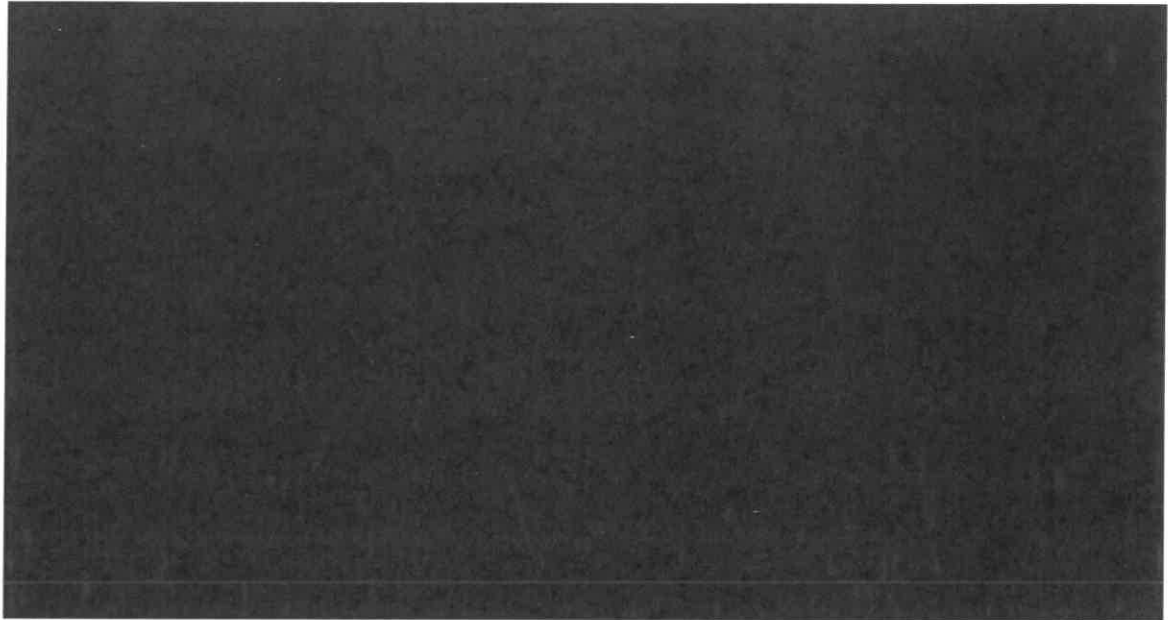


Telecommunications

Information was received from business areas on all 15 telecommunications public registers. This was used to assess the inherent risk of each of these registers (refer Attachment B).

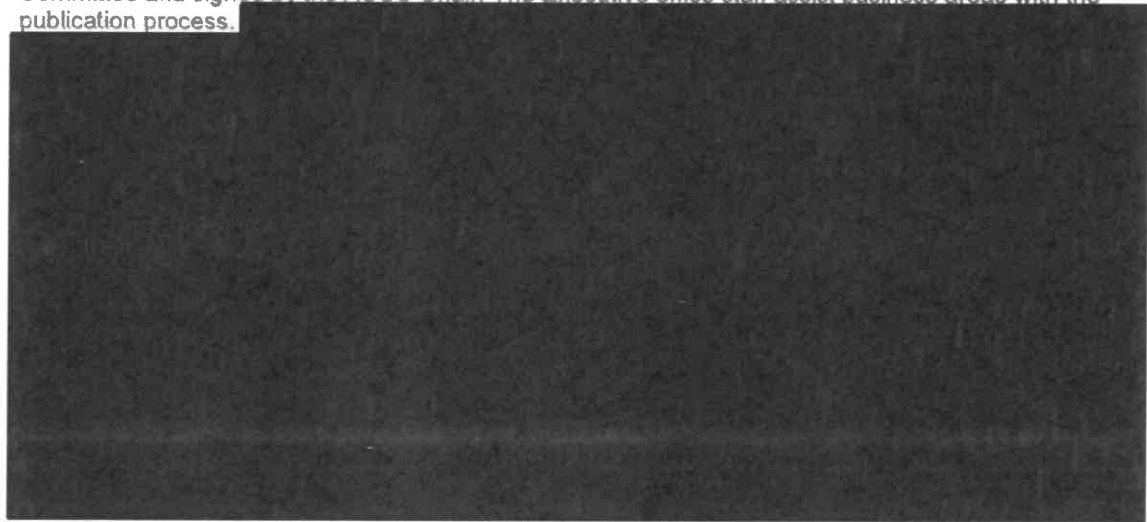


⁶ Typically price rise proposals are received from these entities (such as Australia Post and Air Services Australia) at least once every two years.



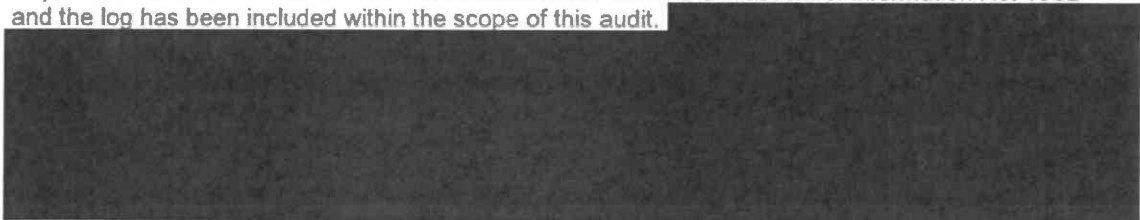
Enforcement

There are seven enforcement public registers. These comprise paid notices (infringement notices or rarely published public warning notices⁷) as well as undertakings approved by the Enforcement Committee and signed by the ACCC Chair. The Executive office staff assist business areas with the publication process.

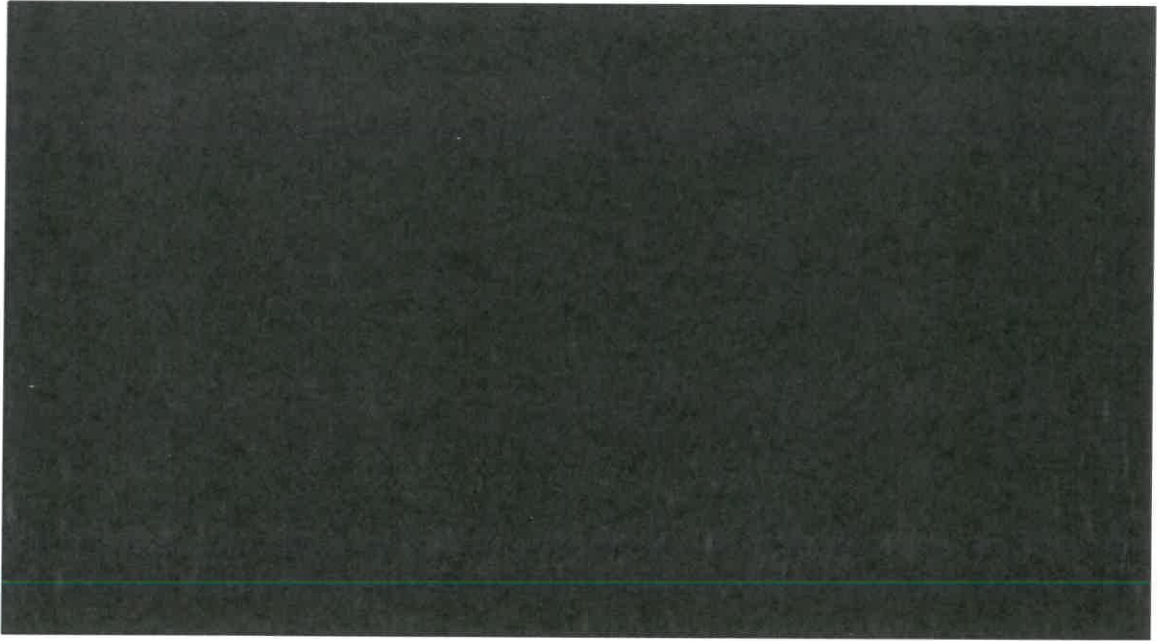


FOI disclosure log

The FOI disclosure log is not referred to as a 'register' in the legislation, however disclosures are required to be made available in certain circumstances under the *Freedom of Information Act 1982*⁸ and the log has been included within the scope of this audit.



⁷
⁸

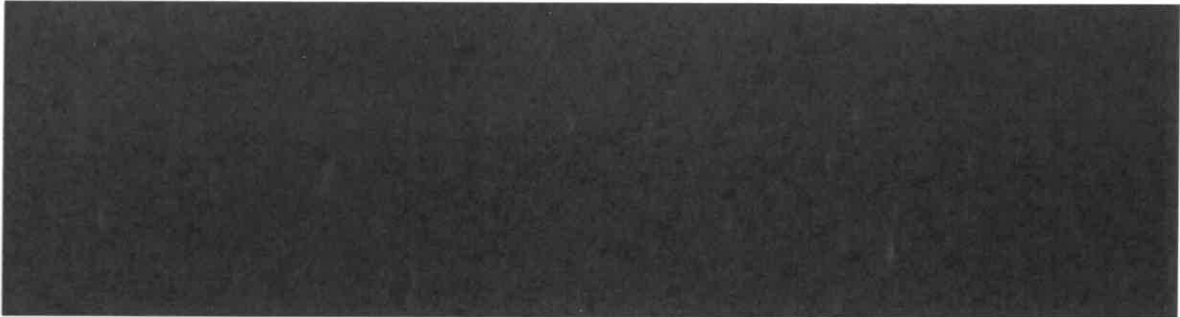


Findings

F.2-1	
F.2-2	
F.2-3	
F.2-4	

Implication





#	Recommendation	Management Response	Responsible Officer and Timing
R.2	<p>Audit recommends that ACCC:</p> <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> ○ 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. 	<p>Agreed.</p> <p>The Executive Management Board will maintain oversight of a project to be set up to implement the remaining recommendations.</p>	<p>Executive Management Board</p>
R.3	<p>Audit recommends that ACCC and AER:</p>	<p>Agreed.</p>	<p>Executive Management Board</p>

#	Recommendation	Management Response	Responsible Officer and Timing
	<ul style="list-style-type: none"> 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. 	To be considered as part of the project.	

Finding 3: Support systems and applications

Background

There are nine active categories of public registers (listed in the table below). Each ACCC and AER public register under these categories is administered using one of three system publication 'streams' (outlined at Attachment D). Publication mechanisms fall into one of the following streams:

-
-
-

Work is currently underway by the Application Development team to transition business areas to common supported applications (instead of unsupported legacy applications):

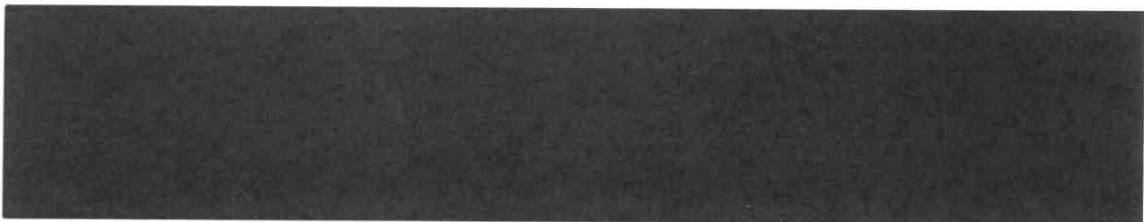
- CRM instead of TrackIT project management system; and
- Drupal instead of Sytadel for website content management.

This work is almost complete for product recalls⁹ and will then be rolled out for use in updating mergers and adjudication, followed by enforcement public registers.

Observation

⁹ Product recalls published on the website are numbered in the thousands. They are not a formal or statutory register.

¹⁰ Such as in the case of ICT relying on the contact(s) who send an email with documents for publication being appropriately authorised and competent to request publication of the information.



Primary public register materials are all saved down to the DORIS/TRIM record-keeping system¹¹.

The system supported publication processes for each public register / category are outlined in the table below.

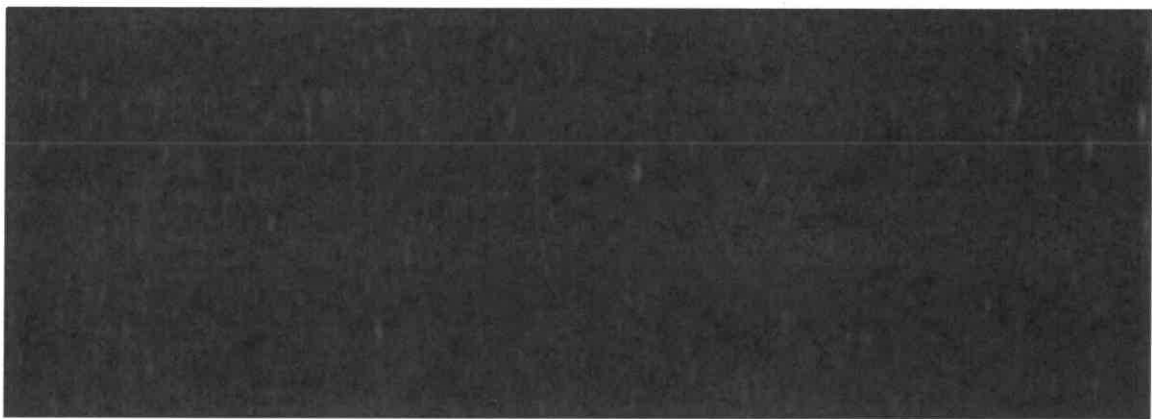


Register category	Specific	Publication process	Notes
Mergers	Merger clearances and authorisations	<ul style="list-style-type: none"> • ACCC-Integrated (refer Attachment D) 	[Redacted]
	Supplementary registers e.g. Statement of Issues Register	<ul style="list-style-type: none"> • ACCC-Standard (refer Attachment D) 	
Adjudication	Authorisations and notifications	<ul style="list-style-type: none"> • ACCC-Integrated (refer Attachment D) 	
Price notifications, Access to Services, International Shipping Investigations, Telecommunications and Enforcement (and associated consultation documents)	N/A	<ul style="list-style-type: none"> • ACCC-Standard (refer Attachment D) 	
FOI disclosure log	FOI disclosures deemed appropriate for public register	<ul style="list-style-type: none"> • ACCC-Standard (refer Attachment D) 	
AER	Retail and Network disclosures	<ul style="list-style-type: none"> • AER (refer Attachment D) 	

¹¹ A key element of sound public administration and accountability is adequate recording or documentation of the business of government. To achieve this, agencies need to develop records management frameworks and systems designed to ensure that records are appropriately managed. (ANAO Report No.53 2011–12 Performance Audit Records Management in the Australian Public Service, pg 13)

Register category	Specific	Publication process	Notes

Prior to publication, confidential information is redacted through different means and using varying applications across ACCC and AER. It is important to meet legislative and confidential information policy requirements under which systems which manage information operate so that records can be proven to be genuine, are accurate, can be trusted and are secure from unauthorised access, alteration and deletion¹².



Findings

F.3-1	
F.3-2	
F.3-3	
F.3-4	

Implication



¹² ANAO Report No.53 2011–12 Performance Audit Records Management in the Australian Public Service.

#	Recommendation	Management Response	Responsible Officer and Timing
R.4	Audit recommends that ACCC implement restricted system permissions for reclassification of documents and publication of information to appropriately authorised and skilled staff.	Agreed. To be considered as part of the project.	Executive Management Board

Attachment A – Risk Rating



Risk Assessment Criteria

Frequency	1	2	3	4	5
A Almost Certain	L	M	H	E	E
B Likely	L	M	H	H	E
C Possible	L	M	M	H	H
D Unlikely	L	L	M	M	H
E Rare	L	L	L	M	M

Frequency is defined as follows:
A Almost Certain: Occurred in the past or circumstances are such that it is certain to happen.
B Likely: Has occurred in the last 10 years or has occurred frequently in the past.
C Possible: Has occurred in the past or circumstances are such that it is likely to happen in the next 10 years.
D Unlikely: Has never occurred in ACCC or has occurred infrequently in the past.
E Rare: Has never occurred in ACCC or has occurred very infrequently in the past.

Likelihood	Consequence				
	1	2	3	4	5
High	Minor	Moderate	Major	Catastrophic	Catastrophic
Medium	Minor	Moderate	Major	Catastrophic	Catastrophic
Low	Minor	Moderate	Major	Catastrophic	Catastrophic

Risk Rating legend:

E	Extreme Risk
H	High Risk
M	Medium Risk
L	Low Risk

Attachment B – Public Registers Risk Assessment

ACCC & AER Public Registers

No.	Register type	Register title	Authority	Assessed Risk*
1	Mergers register	Informal merger clearances	Voluntary	[Redacted]
2		Formal merger clearances	Statutory	
3		Public competition assessments	Voluntary	
4		Statement of issues	Voluntary	
5		Merger authorisations register	Statutory	
6	Authorisation and notification register	Authorisations register	Statutory	
7		Exclusive dealing notifications register	Statutory	
8		Collective bargaining notifications register	Statutory	
9		Private disclosure of pricing information notification register	Statutory	
10	Price Notification Register	Register of price notifications given to ACCC under Division 4 of Part VIIA (prices surveillance) of the CCA (mainly s44Q etc)	Statutory	
11	Access to Services Register	Section 44Q(a) Decisions of the Minister that a State or Territory access regime for access to a service is an effective access regime	Statutory	
12		Section 44Q(aa) Decisions of the Minister to extend the period in force of a decision on the effectiveness of an access regime	Statutory	
13		Section 44Q(b) Declarations (including those no longer in force)	Statutory	
14		Section 44Q(c) Decisions of the Commission to approve a tender process as a competitive tender process	Statutory	
15		Section 44Q(d) Decisions of the Commission to revoke a decision to approve a tender process as a competitive tender process	Statutory	

* Risk analysis based on sensitivity of information received in relation to public register, requirement for redaction of confidential information/modification of documents, frequency that register is updated and whether there are documented approval and publication workflows in place that are clearly understood. This analysis is prior to consideration of the control framework for each public register.

No.	Register type	Register title	Authority	Assessed Risk*
16	Telecommunications Registers	Access undertakings register	Statutory	
17		Competition notices register	Statutory	
18		Declared services register	Statutory	
19		Register of Access determinations	Statutory	
20		Final and interim access determinations	Statutory	
21		Ministerial pricing determinations register	Statutory	
22		Telecommunications access codes register	Statutory	
23		Published arbitration determinations	Voluntary	
24		Exemption orders register	Statutory	
25		Tariff information register	Voluntary	
26		Tariff filing directors register	Statutory	
27		Access agreement register	Statutory	
28		Register of Binding Rules of Conduct	Statutory	
29		Register of NBN access agreement statements	Statutory	
30		Register of Layer 2 Bitstream Access Agreement Statements	Statutory	
31	Investigations register (international liner cargo shipping Part X of the CCA)	Register of references given to the Commission by the Minister under ss 10.47(1), 10.50(1), 10.57(1) and 10.63(1)	Statutory	
32		Register of particulars of decisions to hold investigations made by the Commission under ss 10.48(2), 10.28(2A) and 10.58(2)	Statutory	
33	AER Register	Register of Network Exemptions	Voluntary	
34		Register of Retail Exemptions	Statutory	
35		Register of Retail Authorisations	Statutory	
36		Register of retailers (RoLRs)	Statutory	
37	Enforcement register	Register of infringement notices	Voluntary	
38		Infringement notices (Water Act 2007 s156)	Voluntary	
39		General undertakings	Voluntary	
40		Section 93AA undertakings (ASIC Act 1989 and ASIC Act 2001)	Voluntary	
41		Section 163 undertakings (Water Act 2007)	Voluntary	
42		Section 87B undertakings	Voluntary	
43		Public warning notice register	Voluntary	

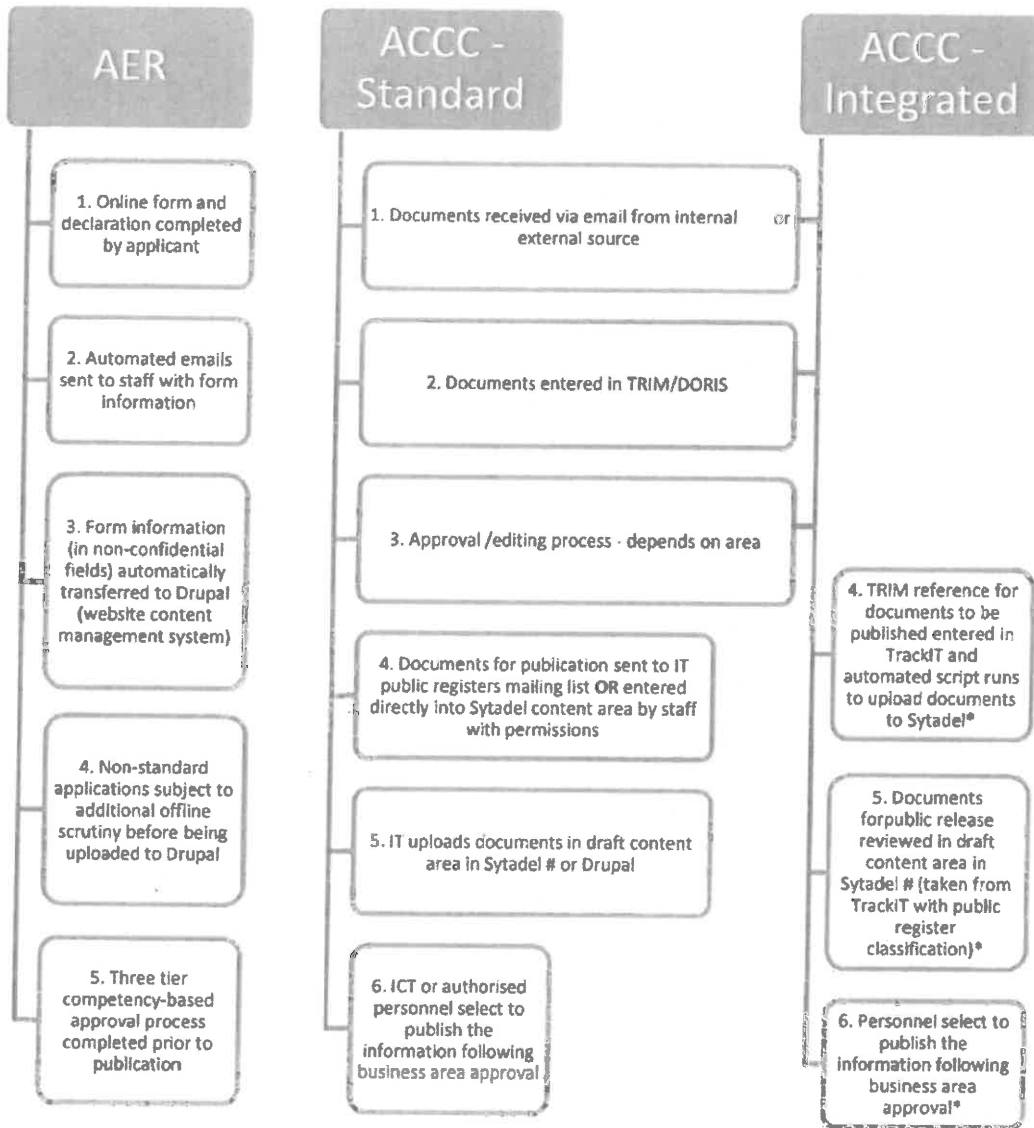
No.	Register type	Register title	Authority	Assessed Risk
44	Freedom of Information	FOI disclosure log	Statutory	
45	Archived registers - Enforcement	GST Compliance Register	Voluntary	
46	Archived registers - Consumer Product Safety	Product safety conference register (section 65 of the TPA)	Statutory	
47	AER Access to Services Register	Section 44ZZL Determinations	Statutory	
48		Section 44ZZC(1) Access undertakings and access codes accepted by the Commission (including those no longer in operation)	Statutory	
49		Section 44ZZC(2) Variations of access undertakings and access codes	Statutory	
50		Section 44ZZC(3) Extensions of operating period of an access undertaking or an access code	Statutory	
51		National Electricity Market Access Code	Statutory	
52		Section 44ZW(3) Decisions of the Commission not to register a contract	Statutory	
53		Section 44ZW(1)(a) Registration of Contract	Statutory	

Attachment C – Breach Incident Analysis

Date	Breach	Description	Probable cause / How addressed
May 2015	Redacted confidential information viewable with copy and paste of content	Redacted confidential information in a re-authorisation application (PDF document) readable if copy and pasted to a Word document	<ul style="list-style-type: none"> • Formatting of redacted information in PDF document did not prevent viewing of information. • Addressed by changing formatting process for redacted document (conversion from PDF to TIF back to PDF)
June 2014	ACCC internal document upload including confidential information	<ul style="list-style-type: none"> • Internal document considering proposed acquisition by one company of another company's assets published on merger public register • Removed after approx. 3 hrs and known persons who accessed the document advised document destroyed 	<ul style="list-style-type: none"> • Two documents open at the same time / incorrect naming of document • Permitted desktop upload of document without second competency-based check to enact publication • Addressed through removal of direct document upload (link to approved document is used instead following ACCC-Integrated process – refer Attachment D)
Various	Incorrect document changes published	Incidents have occurred where documents (in TRIM) have been approved for upload to the website, however an unauthorised change to the same document version just before the automated script runs to transmit the information to the website management system is not picked up in draft review and is inadvertently published (and is later retracted).	<ul style="list-style-type: none"> • Protocols for document and version control are not clearly specified • Local changes have been made to address this issue, however these are dependent on staff vigilance
Unspecified	Un-redacted document published	Mergers published the pre-redacted version of a Market enquiries letter inclusive of confidential information rather than the redacted version.	<ul style="list-style-type: none"> • Not checked properly despite review by Director and final approval by GM. Director was new to the branch. • Feedback provided to staff to improve process.
Unspecified	Unintended document content viewable on publication	A letter to treasury (used as a template) was viewable instead of a Market Enquiries Letter when published.	<ul style="list-style-type: none"> • Using a historical document as a template can result in the original document content being

Date	Breach	Description	Probable cause / How addressed
			<p>viewable when the document is published.</p> <ul style="list-style-type: none"> • Staff have been advised to use clean templates.
Various	Confidential information emailed to unauthorised external party	Emails sent to incorrect external recipients.	<ul style="list-style-type: none"> • Emails sent to external stakeholders incorrectly due to the auto-complete email address function. • Staff have been required to turn off the auto-complete email function.

Attachment D – Publication Streams

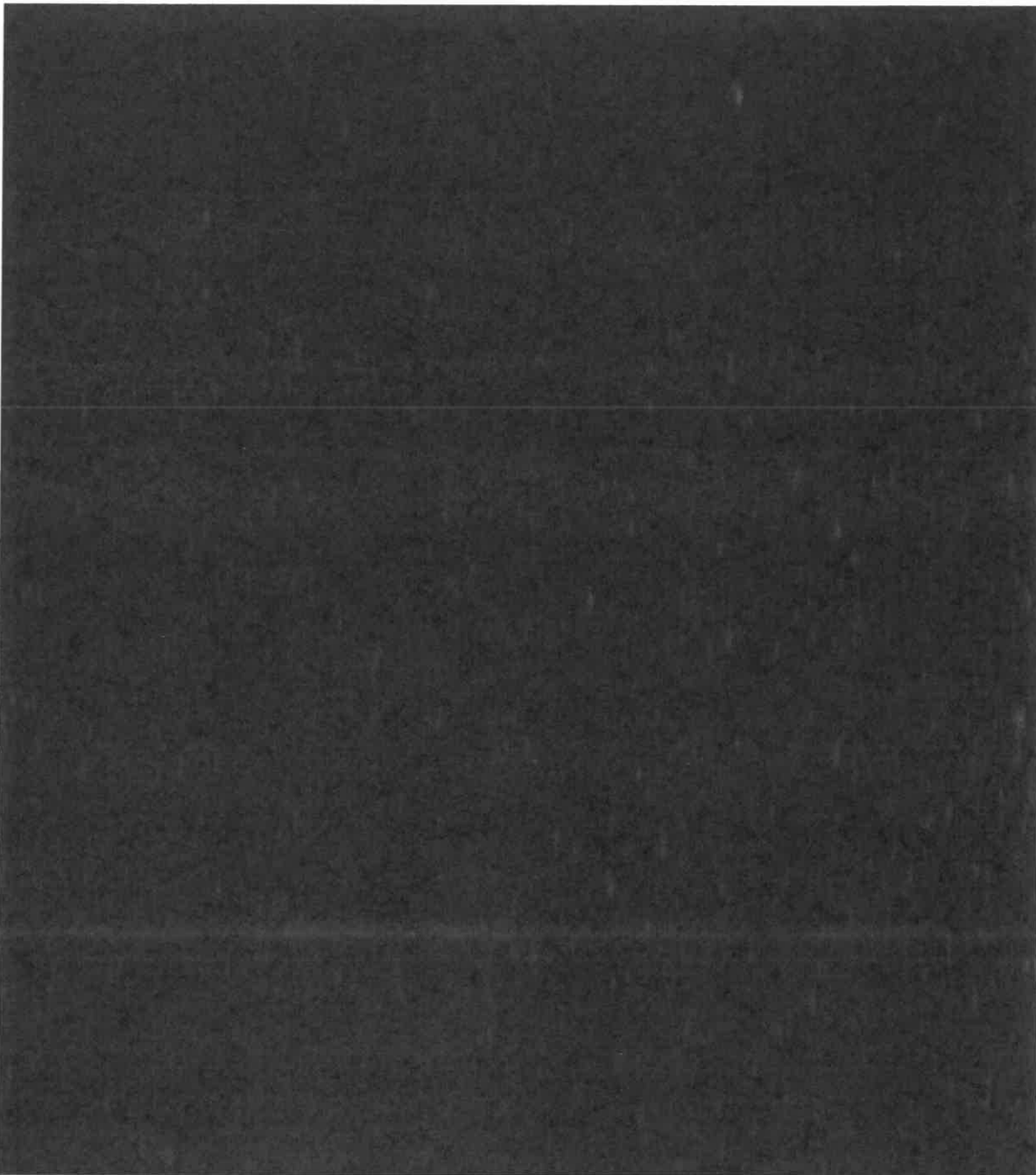


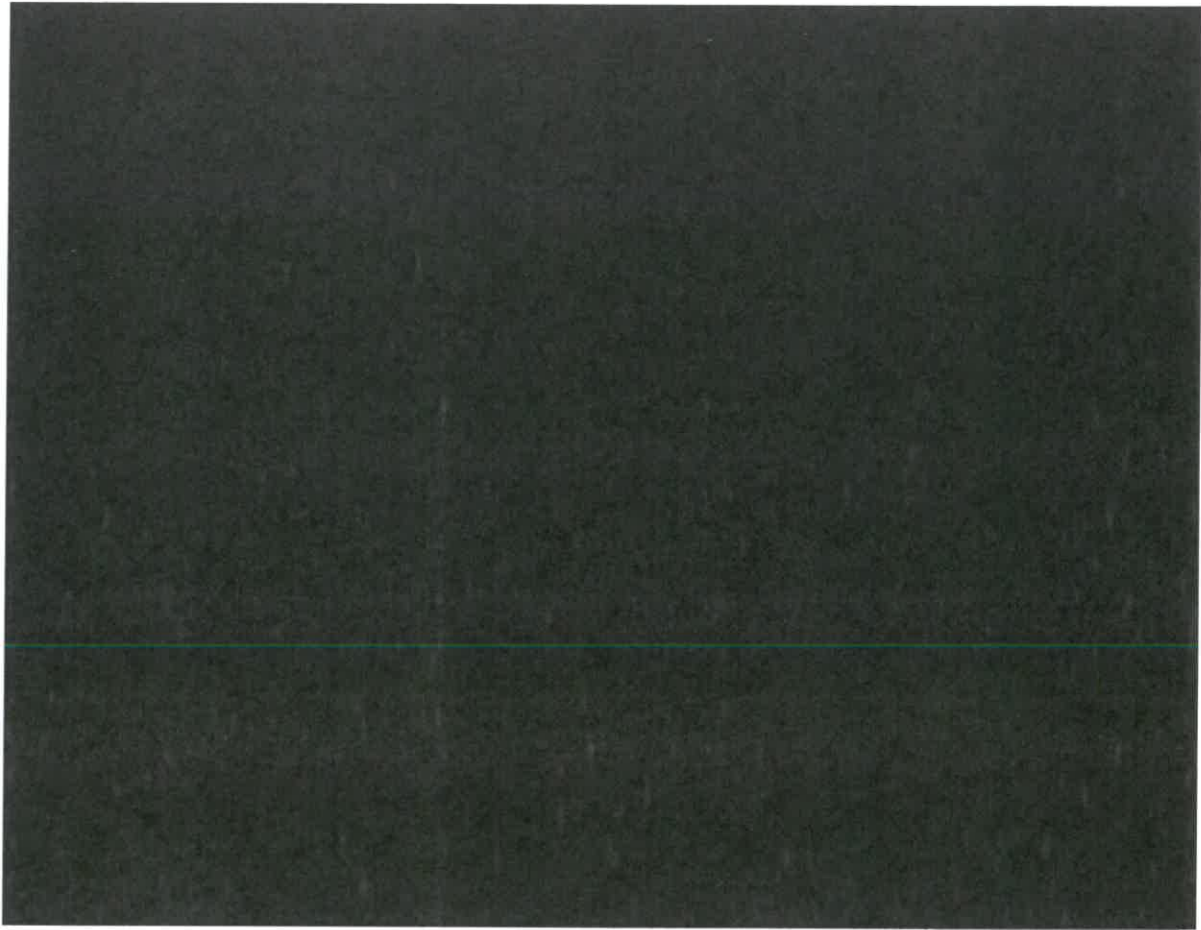
* Only records with a security setting of 'public register' or 'PR' in TrackIT (via TRIM number) can be published on the Sytadel content management system. All staff have access permissions to declassify records and publish documents

Document changes are presented in html code

Attachment E – Management Suggestions

Management suggestions represent a 'Business Process Improvement' opportunity. The suggestions may result in efficiencies and/or enhanced effectiveness of public register administration processes.





Attachment F – Stakeholders Consulted

Name	Position
Rhys Benny	Director, Corporate Operations and Governance
Christian Hadlington	Assistant Director – Governance, Internal Audit and Risk
Viraya Vannasy	Corporate Secretariat Officer, Governance & Support
Julia Kulakowski-Rupert	Assistant Director – Governance, Internal Audit and Risk
Ron Neilan	Office Manager, Merger & Authorisation Review
Peter Conlon	Director IT Governance
Richard Shanahan	Business Analyst and Knowledge Management Coordinator
Nathan Mollison	Senior Applications Administrator, Application Management
Lachlan Dolling	Business Analyst, IT Governance
Paul Dunn	Director and Regulatory Advisor, AER
Trinas Pitsakos	AER Web Manager
Nicholas Heys	Deputy General Manager, Enforcement Division
Tania Gratton	Assistant Director, Enforcement Coordination
Kayla Potter	Executive Assistant to the Chairman, Executive Office
Francesco Naismith	Assistant Director, Executive Office
Simon Haslock	Assistant Director, Regulatory Reform and Performance
Jessica Wicks	Assistant Director, Regulatory Strategy, Digital Economy & Coordination, Infrastructure Regulation Division
Heather Thomas	Principal Lawyer, Corporate Law
Seema Gosain	Project Officer, Corporate Law (previously Merger & Authorisation Review)
Belinda Blanch	Project Officer, Competition Law Implementation Program (previously Adjudication)
Cherish Cherian	Director, Application Management
Nathan Ter Bogt	Application Management Contractor
Joshua Davies	A/g Director Mobiles and Consumer Engagement

Name	Position
Elsbeth Philpott	Assistant Director, Transmission
Damian Bye	Assistant Director, Market Evolution & Access
Matthew Robertson	Assistant Director, Prices Oversight & Communication

Attachment G – Statement of Responsibility

We take responsibility for this report, which is prepared on the basis of the limitations set out below.

The engagement has been performed as an audit as defined under Australian Standard on Assurance Engagements (ASAE) 3000 "Assurance Engagements Other than Audit or Reviews of Historical Financial Information".

Our procedures were designed to provide reasonable assurance as defined by ASAE 3000, which recognises the fact that absolute assurance is rarely attainable due to such factors as the use of judgment in gathering and evaluating evidence and forming conclusions, the use of selective testing, the inherent limitations of internal controls and because much of the evidence available to the auditor is persuasive rather than conclusive in nature.

Further, the internal control structure of client has not been reviewed and no view is expressed as to its effectiveness.

The matters raised in this report are only those which came to our attention during the course of performing our procedures and are not necessarily a comprehensive statement of all the weaknesses that exist or improvements that might be made. We cannot, in practice, examine every activity and procedure, nor can we be a substitute for management's responsibility to maintain adequate controls over all levels of operations and their responsibility to prevent and detect irregularities, including fraud. Accordingly, management should not rely on our report to identify all weaknesses that may exist in the systems and procedures under examination, or potential instances of non-compliance that may exist.

This report has been prepared solely for your use and should not be quoted in whole or in part without our prior written consent. No responsibility to any third party is accepted as the report has not been prepared, and is not intended, for any other purpose.