WESTERN AUSTRALIA

CCC | Corruption and Crime Commission

Review of the Office of the Auditor General's response to misconduct risks with access to confidential information

24 June 2021

ISBN: 978-0-6488863-6-5

This report and further information about the Commission can be found on the Commission website at www.ccc.wa.gov.au.

Corruption and Crime Commission

Postal Address	PO Box 330 Northbridge Post Shop WA 6865	**Email**	info@ccc.wa.gov.au
		Website	www.ccc.wa.gov.au
Telephone	(08) 9215 4888 1800 809 000 (toll free for callers outside the Perth metropolitan area)	**Twitter**	@CCCWestAus
		Office Hours	8.30 am to 5.00 pm, Monday to Friday
Facsimile	(08) 9215 4884		

Special Needs Services

If you have a speech or hearing difficulty, contact the Commission via the National Relay Service (NRS) on 133 677 for assistance or visit the NRS website, www.relayservice.com.au. NRS is an Australia-wide telephone service available at no additional charge. The Commission's toll-free number is 1800 809 000.

If your preferred language is a language other than English, contact the Translating and Interpreting Service (TIS) for assistance on 13 14 50. TIS provides a free, national, 24 hours a day, seven days a week telephone interpreting service. TIS also provide on-site interpreters for face-to-face interviews by contacting 1300 655 082.

TABLE OF CONTENTS

Introduction 1
The Commission's report 1
The Office of the Auditor General's response 2
The Commission's review 3
Conclusion 3

THIS PAGE HAS INTENTIONALLY BEEN LEFT BLANK

Introduction

[1] On 23 April 2020, the Commission reported[1] to Parliament on serious misconduct and corruption risks within the Office of the Auditor General (OAG).

[2] The risks related to access to confidential information.

[3] During the Commission's investigation, it had become evident that the OAG policies and instructions governing access to, and storage of, confidential information did not work.

[4] The Commission recommended the OAG review its procedures to ensure that following an audit, data is only retained in a secure location.

[5] This report reviews the response of the OAG to the recommendation in that report.

The Commission's report

[6] The 2020 Commission report detailed how two auditors regularly accessed sensitive and confidential information within OAG systems that were not properly protected.

[7] Both auditors had unrestricted access to confidential information, which would normally be restricted to employees who required access to that information for their work.[2]

[8] The Commission's investigation also made a startling discovery of sensitive audit data that had been stored and improperly retained on an OAG laptop computer.

[9] The sensitive audit data was a spreadsheet which contained the names and addresses of every serving police officer in Western Australia. Unbeknown to the OAG, this information had remained on the laptop years after completion of the audit. While there was no evidence the police data was shared, the Commission identified the serious misconduct risks and the immediate need for this to be addressed by the OAG.

[10] In response to the Commission's 2020 report, the OAG informed the Commission that immediate actions had been taken to tighten access to confidential information.[3] Specifically, the security control issues within

[1] Corruption and Crime Commission, *Report into misconduct risks with access to confidential information in the Office of the Auditor General,* August 2020.
[2] Clarifications enclosed in letter from the Auditor General to the Acting Commissioner, 8 April 2020, p 2.
[3] Ibid, p 3.

the TRIM record management system had been rectified and policies reviewed to ensure instructions to auditors on managing audit data were clear.

[11] The Commission recommended that the OAG review its procedures to ensure that following an audit, data is retained only in a secure location.

[12] The Commission further suggested that policies, procedures and instructions are not enough. There must be periodically reviewed technological security built into the system.

The Office of the Auditor General's response

[13] In April 2021, the Commission commenced a review[4] of the OAG response to the Commission's 2020 recommendation.

[14] The OAG provided the Commission with a comprehensive and transparent response during the review process. The Commission commends the agency for its approach and continued commitment to reducing serious misconduct risks around data management.

[15] The OAG informed the Commission[5] that OAG laptops are encrypted, can only be accessed by an authorised user and any audit information saved on an OAG laptop, is retained in a secure location.

[16] The OAG stated that a number of initiatives have been implemented to improve the storage and handling of, and staff behaviours related to data management. Specifically, the OAG has:

- Updated policies and procedures to require the storing of audit data in OAG secure audit data software only.
- Provided information sessions and regular reminders to staff on the data storage requirements throughout an audit.
- De-activated all IronKey (encrypted USB devices) and restricted their use to exceptional circumstances, requiring Deputy Auditor General approval.
- Commenced use of a secure online file transfer system for sensitive information transferred between client entities and the OAG.
- Conducted regular checks to ensure audit information has been deleted in accordance with policy requirements.

[4] *Corruption Crime and Misconduct Act 2003* s 41.
[5] Letter from the Auditor General to the Acting Commissioner, 16 April 2021.

[17] The OAG stated that while many processes and controls are automated, they have been on an 'accelerated technology transformation and information security journey'[6] and that continued improvements will remain a focus given the cyber landscape in which they operate.[7]

The Commission's review

[18] The OAG took immediate action to address system deficits identified in the Commission's 2020 Report. The OAG continues to take steps to improve its overall data management.

[19] The Commission appreciates that while the inherent risks associated with the storage of audit information on an OAG laptop or IronKey USB cannot be eliminated, the actions taken by OAG evidence an approach of minimising risk and maximising misconduct detection.

[20] The use of IronKey USB storage is now authorised, registered and audited by the OAG. Regular IT checks are performed on randomly selected laptops and there are many automated controls and monitoring within IT systems.

[21] OAG requirements for data management are clearly articulated in policy and procedure. Team Leaders and Directors are responsible for managing staff compliance within an audit.

[22] The implementation of monitoring controls and policy compliance measures demonstrates the OAG's commitment to reduce and manage risk.

Conclusion

[23] While the Commission's 2020 report directly involved the OAG, the report was also a reminder to the wider public sector of the risks associated with confidential data management.

[24] The Commission made a call for action and recommended all public authorities evaluate their data management risks and where necessary, take action to mitigate them. It is not clear how the broader public sector has responded.

[25] However, the actions taken by the OAG in response to the Commission's 2020 report has resulted in improvements to OAG procedures and increased staff awareness.

[6] Letter from the Deputy Auditor General to the Acting Commissioner, 3 June 2021.
[7] Letter from the Auditor General to the Acting Commissioner, 16 April 2021.

[26] The OAG recognition 'that people are our greatest strength but also can be our weakest link',[8] illustrates the importance of monitoring staff compliance with policy and procedures.

[27] The Commission continues to emphasise the importance of securing private information. The access to and the use of private information should remain for legitimate work related purposes and no other.

[28] **The Commission considers this recommendation to be complete.**

[8] Letter from the Deputy Auditor General to the Acting Commissioner, 3 June 2021.