



MANAGEMENT ARCHITECTURE ASSESSMENT INFRASTRUCTURE

# Case study



Government of **Western Australia**  
Department of **Health**

**A Security Review of its Data Linkage Systems ensures the Department of Health's Data Linkage Branch can optimise its approach to Information Security.**

## THE CLIENT

Although data linkage has been used for health and medical research in Western Australia since the 1970s, the WA Data Linkage System (WADLS) was formally established in 1995 as a collaboration between the WA Department of Health, University of Western Australia, Telethon Kids Institute (then the Telethon Institute for Child Health Research) and Curtin University.

The Data Linkage Branch (DLB) manages the WADLS, which entails the creation and maintenance of linkages within and between a wide range of Health and other datasets. These linkages use rigorous, internationally accepted privacy preserving protocols, probabilistic matching, clerical review and quality control mechanisms to create a robust and complex system of links between

otherwise disparate pieces of individual information.

## THE BUSINESS CHALLENGE

DLB required a Security Review of their existing data linkage systems, including associated protocols and practices, incorporating the WA Data Linkage System (WADLS) and identified Department of Health Data Collections.

This Security Review would help determine the current security posture across each component and process plus assist in identifying areas where further security measures could be implemented and enhanced.

## THE SOLUTION

Asterisk Information Security was selected to perform a Security Review of Data Linkage Systems.

For this particular engagement, Asterisk utilised industry standards and guidelines including ISO/IEC 27002:2013, ASD Strategies to Mitigate Cyber Security Incidents, and SANS Critical Security Controls for Effective Cyber Defense.



MANAGEMENT



ARCHITECTURE



ASSESSMENT



INFRASTRUCTURE

Asterisk proposed a range of activities that would provide visibility of the current state of information security including:

- \* Identification of compliance obligations
- \* Threat modelling activities
- \* Analysis of WADLS
- \* Presentation of findings

The findings gathered from these activities were presented in a report, detailing the overall security status of all items assessed.

The report highlighted improvements to enhance the overall security applied to Data Linkage Systems, as well as feature observations based on the evaluation findings themselves.

Additionally, a detailed threat model was provided, including a diagrammatical representation and categorised list of identified threats which could target the Data Linkage Systems and associated components.

The report also included a prioritised list of recommendations aligned with an appropriate risk assessment methodology to improve and address areas of concern.

“The information collected and cited during the workshops was critical in understanding the WADLS architecture

and determining the current security posture across each component and process,” said Greg Roberts, Director, Consulting and Infrastructure Services Manager at Asterisk Information Security. “The analysis of WADLS resulted in the identification of areas where further security measures could be implemented and enhanced.”

#### THE BENEFITS

Implementing the recommendations presented in the report will help mature the Information Security posture within the Data Linkage Branch through the optimisation of existing processes. It is expected that optimising the approach to Information Security will result in the adoption of new technologies and alignment of processes to protecting key information assets.

“The consultants from Asterisk were a pleasure to work with,” said Tom Eitelhuber, Manager Data Linkage Systems at DLB. “The entire process was well coordinated, with each phase being clearly explained and very collaborative in nature. With the final report and recommendations, we have a clear pathway ahead to further solidify DLB’s security measures.”

#### WE ARE ALL ABOUT INFORMATION SECURITY

Asterisk Information Security is a specialist consultancy providing actionable advice and solutions to enhance information security and reduce business risk.

The team at Asterisk has been involved in the information security industry for over 18 years. Our clients range from SME to large enterprises across a variety of sectors including government, mining and resources, critical infrastructure, finance, retail, healthcare and not-for-profit.



For further information on how Asterisk can improve your information security, please contact **1800 651 420**

✉ [contact@asteriskinfosec.com.au](mailto:contact@asteriskinfosec.com.au)  [@asteriskinfosec](https://twitter.com/asteriskinfosec)  [linkedin.com/company/asterisk-information-security](https://www.linkedin.com/company/asterisk-information-security)