Report 9: 2024-25 | 21 March 2025

INFORMATION SYSTEMS APPLICATION AUDIT

Child Protection Case Management System – Assist

Office of the Auditor General
for Western Australia

Audit team:
Aloha Morrissey
Kamran Aslam
Paul Tilbrook
Ben Goodwin
Jason Bhawoo

National Relay Service TTY: 133 677
(to assist people with hearing and voice impairment)

We can deliver this report in an alternative format for those with visual impairment.

ISSN: 2200-1913 (print)
ISSN: 2200-1921 (online)

The Office of the Auditor General acknowledges the traditional custodians throughout Western Australia and their continuing connection to the land, waters and community. We pay our respects to all members of the Aboriginal communities and their cultures, and to Elders both past and present.

Image credit: shutterstock.com/ESB Professional

WESTERN AUSTRALIAN AUDITOR GENERAL'S REPORT

Child Protection Case Management System – Assist

Report 9: 2024-25
21 March 2025

This page is intentionally left blank

THE PRESIDENT
LEGISLATIVE COUNCIL

THE SPEAKER
LEGISLATIVE ASSEMBLY

CHILD PROTECTION CASE MANAGEMENT SYSTEM – ASSIST

This report has been prepared for submission to Parliament under the provisions of section 25 of the *Auditor General Act 2006*.

Information systems audits focus on the computer environments of entities to determine if these effectively support the confidentiality, integrity and availability of information they hold.

This audit assessed the Assist application, and related systems, used by the Department of Communities for its work supporting children and families.

I wish to acknowledge the entity’s staff for their cooperation with this audit.

Caroline Spencer
Auditor General
21 March 2025

Contents

Auditor General’s overview

Across Western Australia there are more than 5,000 children in the State’s care. Personal and sensitive information relating to their circumstances along with information about other children, family groups and carers is stored in Assist.

Assist is an application used by over 2,500 Department of Communities’ (Communities) staff to support some of the most vulnerable people in our society. In 2023-24, Communities received over 61,000 reports and identified 71,662 children of concern. With convenient access to personal and highly sensitive information comes the responsibility for Communities to appropriately manage and secure that information to maintain people’s safety and privacy. Reliance on information systems and technology more broadly means additional risks need to be managed that extend beyond the purely operational.

My Office’s audit of Assist found significant weaknesses that risk the confidentiality, integrity and availability of the system and vulnerable peoples’ information. Assist is a flawed system that does not appropriately support Communities to manage its interactions with children and families. I am pleased Communities now has plans to replace it. The State Government has provided initial funding to develop the project definition plan.

Until a new system is in place, planned to occur in 2028, Communities can and should take steps to better protect Assist and its information. This includes restricting children’s files to only staff supporting their care, only storing investigation reports in Assist or other approved recordkeeping systems and implementing more comprehensive logging and monitoring to detect inappropriate access to information.

The audit also raised concerns about the quality of information in Assist. Errors and gaps in information could delay or impede Communities’ support to children. Additionally, Communities needs to improve its business continuity plans to consider how it will continue to deliver services if Assist has an outage.

I acknowledge the dedicated work of Communities staff, including child protection, case and care workers, to support and improve the lives of vulnerable children and their families.

Executive summary

Introduction

In this audit we assessed the Assist application, and related systems, used by the Department of Communities (Communities) for its work supporting children and families.

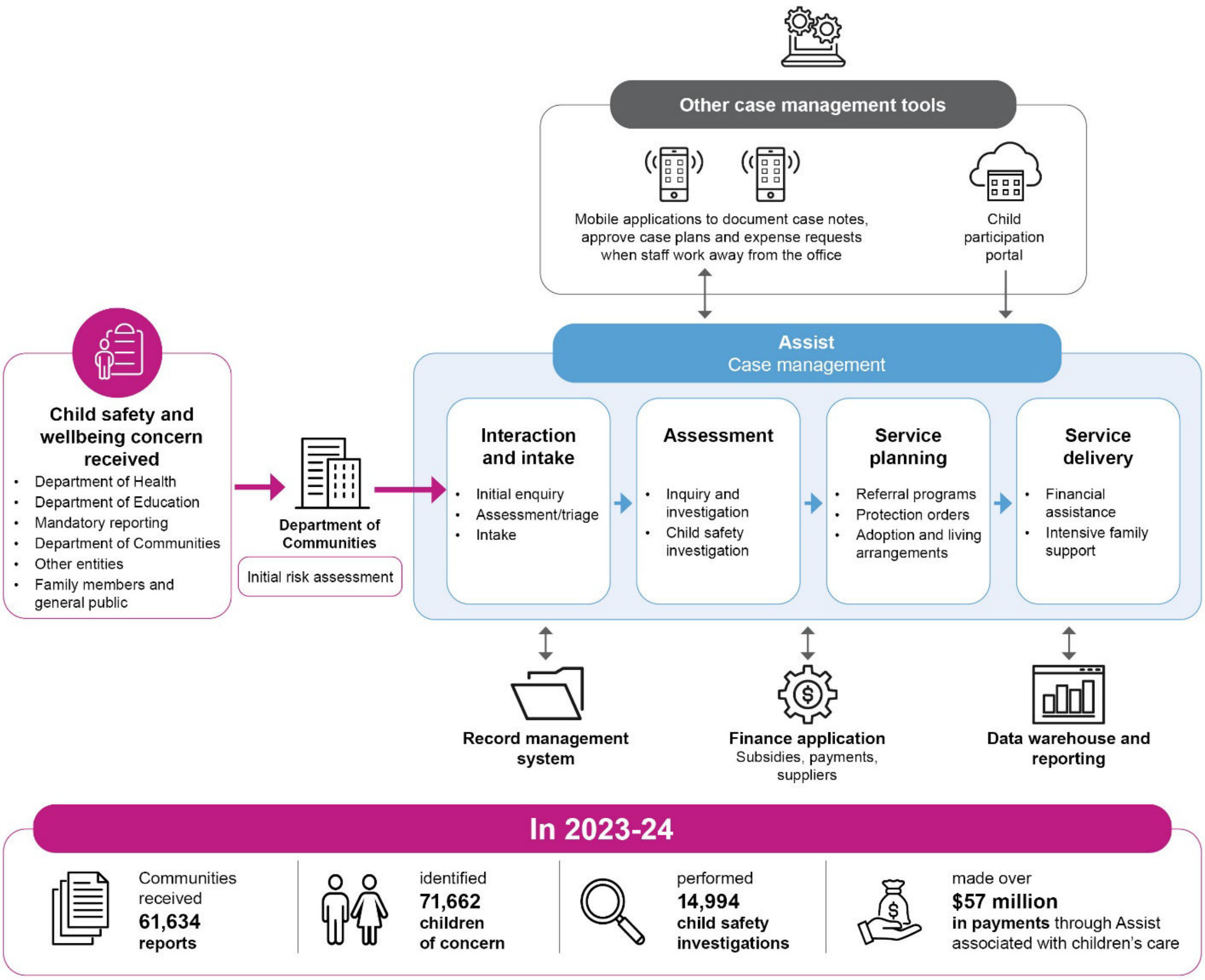
Our objective was to determine if Communities effectively manages the confidentiality, integrity and availability of Assist and its information.

Background

Assist is a highly customised, customer relationship management system used by over 2,500 staff including child protection, case and care workers across 37 metropolitan and regional offices. It supports their work to investigate, assess and monitor children at risk and provide family support and services to children in Communities' care (Figure 1).

Assist has been used since 2010 and stores the current and historic personally identifiable information of over 180,000 children, 218,000 family groups and 38,000 carers. It also contains reports of suspected or confirmed child abuse and the details of victims, witnesses and perpetrators.

Communities' staff and contracted vendors support and maintain the Assist application and its underlying infrastructure.



Source: OAG based on Communities information

Figure 1: Overview of the Assist application

Conclusion

Communities does not effectively manage the confidentiality, integrity and availability of Assist and the important information it holds. Furthermore, the complex legacy application does not support Communities to efficiently manage its interactions with children and families. Communities has acknowledged this and received initial funding to develop a project plan to replace Assist.

Access to confidential information in Assist is not effectively controlled. Child protection, case and care workers' access is not restricted to only those cases to which they are assigned, there is inadequate logging and monitoring of access, and Communities does not obfuscate[1] information accessible to third-party vendors in non-production environments. In addition, due to the lack of collaboration features in Assist, some documents are being stored outside of the application resulting in unnecessary copies of sensitive information. These issues increase the risk of inappropriate access, modification and disclosure of information which could impact vulnerable children, family members, carers, witnesses and staff.

The quality of information stored in Assist is poor. Legacy data migration issues, a lack of controls to verify data changes and a difficult to use interface have contributed to data integrity issues, including errors and gaps in important information. If staff cannot easily find reliable information in Assist, it may affect their ability to provide timely and appropriate support to children and families.

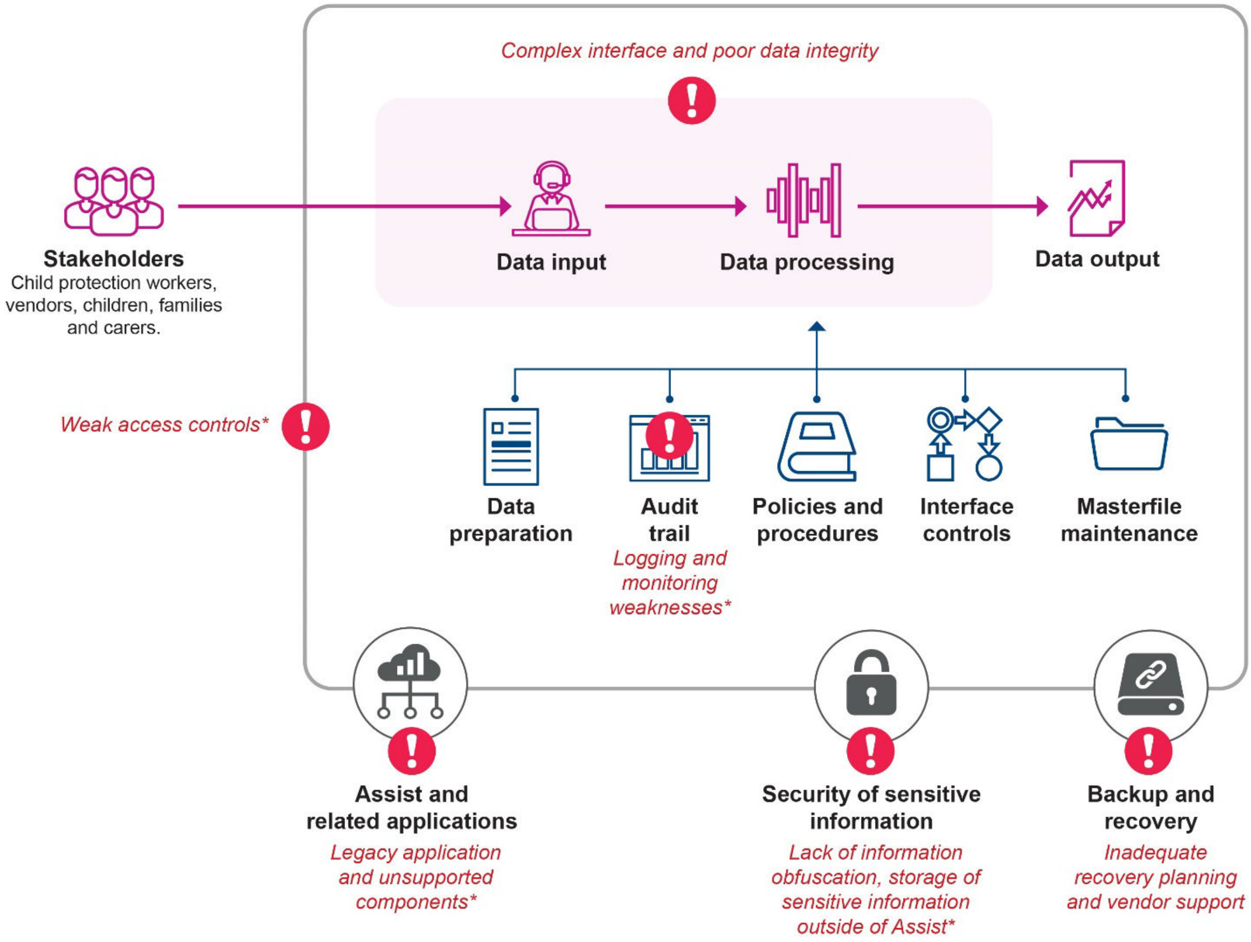
Communities needs to do more to ensure the availability of Assist following an outage. Although it has business continuity plans for its various offices, the plans do not clearly define how the offices will continue to deliver services if Assist is not available for an extended period. In addition, Communities has not tested its Assist disaster recovery plan and its contract with the application support vendor only provides best-efforts[2] out-of-hours support. Communities may not be able to recover Assist in line with business expectations following an outage, impacting the delivery of services.

[1] Obfuscation disguises sensitive data and is a common method to protect information in development and testing environments. For example, real names are replaced with randomly generated names to hide the identity.

[2] Support/assistance that is provided outside defined service level commitments.

Findings

Our audit of Assist and its related systems found weaknesses across six of the 12 application audit control categories (Figure 2).



Weaknesses identified

Source: OAG

These weaknesses are discussed under the confidentiality of information finding.

Figure 2: Key weaknesses identified in Assist controls

Confidential child protection information is at an elevated risk of inappropriate access and disclosure

Communities does not effectively control access to confidential child and family information, including information related to legal matters. Vulnerable children, family members, witnesses, carers and staff may be put at risk of harm if information is inappropriately accessed and disclosed.

- **Access to information is not effectively restricted –** Over 2,500 staff have access to all records in Assist and can view and modify information such as personal details and case and investigation records. Although staff undergo screening, their access is not restricted to only those cases to which they are assigned or have a valid reason to access. Communities told us this open access is needed to efficiently assign cases and that it would be administratively burdensome to lock it down. However, Communities has not formally documented this decision including consideration of the risks and benefits of its approach. It is better practice to restrict access to information on a need-to-know and least privilege basis. Communities' open access approach increases the likelihood of information in Assist being inappropriately accessed, modified and disclosed. It would also be difficult to identify who was responsible for the access or modifications as logging and monitoring are not fully effective (see below).

- **Access to an internet accessible portal containing sensitive information was not appropriately restricted –** Communities has not established an access authorisation and review process. Users including the portal vendor, Communities' staff and other individuals involved in care planning could request and receive access from the portal vendor without Communities' authorisation. In addition, multifactor authentication was not required. The portal contains sensitive information and is used by Communities to enable children to participate in planning their own care. Without access authorisation and review processes, sensitive child information may be inappropriately accessed or modified.
- **Sensitive information is inappropriately stored and communicated** – we found sensitive documents stored outside of Assist, creating unnecessary copies and significantly increasing the likelihood of unintentional or malicious disclosure.

  Draft child safety investigation[3] reports are stored on staff computers and network folders and shared internally using email. Communities developed this process because Assist does not have functionality for multiple staff to collaborate on reports. Better practice would be for Communities to use its records management system to draft, review and finalise reports which would improve security and prevent unnecessary copies of sensitive information.
- **Information in non-production environments is not obfuscated –** personally identifiable and sensitive information in Assist and its related systems is regularly copied to non-production environments without obfuscation. These non-production environments are used by third-party vendors and Communities' staff for testing purposes. This information is more vulnerable to unauthorised access as non-production environments are not secured to the same standards as production systems. The vendor advised us that Assist support staff undergo background screening.
- **Application and database logging and monitoring needs improvement –** Information about children and families can be accessed either directly through the databases or through the Assist application. While a limited number of individuals had direct access to Assist databases, Communities did not log or monitor this access to identify inappropriate access or record modification.

  The Assist application does log access and changes to key information but Communities has a limited understanding of this capability and has not appropriately configured logging and monitoring to provide visibility of user activity across Assist and related systems. For example, Communities can see who has accessed a child's record but has limited visibility of what specific information was viewed and modified. Logging and monitoring of both the Assist application and database would enable Communities to detect any inappropriate access or modification to sensitive child and family information.

Data integrity issues undermine the quality of Assist information

Various legacy data migration issues, a lack of controls to verify data changes and a difficult to use interface have affected the quality of Assist data. Errors and gaps in important

[3] A child safety investigation determines if a child has experienced or is likely to experience harm or abuse, and what protection is required.

information mean staff cannot always easily find and rely on the information in Assist to deliver timely and appropriate support to vulnerable children and families.

- **Duplicate records cause inefficiencies and can mean important information is missed –** Assist contains duplicate individual and family records, the result of legacy data migration issues. Staff told us of the difficulties they encounter when trying to understand the details of a case when information is spread across multiple entries and records. To save time, staff often create new records, further compounding the issue. Communities has not fixed this since Assist was implemented in 2010. Instead, it removes duplicates on an ad-hoc basis as they are identified. We examined Assist related service desk tickets created between August 2023 and February 2024 and found that twenty-four percent (123 of 514) related to duplicate records.

  Duplicate records impact the quality and reliability of information extracted for reporting and oversight purposes, which may result in an inaccurate understanding of cases and workloads, and impact decision-making.

- **Lack of controls leave key performance targets[4] open to manipulation –** Communities has not implemented controls to prevent changes to child safety investigation start and end dates in Assist, nor does it require reasons for changes to be documented or verified. We reviewed 12 investigations and found one had its start date backdated, resulting in an internal target to start the investigation within 24-hours being met. Without controls to ensure the integrity of underlying system records, Communities could not confirm if child safety investigations were backdated for appropriate reasons.

- **Some child locations are not accurate in Assist –** Assist does not automatically deactivate or end-date an old address when a new address of the same type (e.g. home) is added. While an address can be flagged as the primary address, we found instances where more than one address was flagged as the primary address. As a result, it can be difficult for staff to find the correct address of children. This increases the risk of delays in locating a child and may risk the safety of children and staff if they are sent to the wrong address.

  Additionally, some child protection teams use spreadsheets outside of Assist to record the location of children in group homes. Communities staff informed us this is due to difficulties in storing group homes addresses in Assist. This means, other business units cannot rely on Assist to quickly ascertain the accurate location of children.

Case study 1: Four days to obtain children's location

In early 2024, it took a business unit in Communities four days to determine the location of 12 children as the information was not in Assist but stored in a separate spreadsheet. The location was needed for an independent assessor to visit children in Communities' care.

- **Difficult to use interface –** Staff told us about their concerns when entering information into Assist including unclear field titles and a lack of online guidance on what to enter and in what sequence. We sighted instances where data entry screens cleared and needed re-entry if the entry sequence was incorrect. To address this lack of guidance, senior staff we spoke with have developed their own guides for data entry.

  In addition, some of the navigation screens (such as child protection orders and period of care) only display a child's unique identifier making it slower for staff to find

[4] Communities has set targets to start priority 1 child safety investigations within 24 hours and priority 2 within five calendar days. It also has a target to complete all investigations within 30 days. These targets are inputs into the audited *Improved safety key effectiveness indicator* and *Child protection assessment and investigation key efficiency indicator*. The identified weaknesses in Assist's data integrity resulted in a qualification on these key performance indicators in the 2023-24 audit.

information for the relevant child. We also found the navigation menu incorrectly shows child safety investigations as open when they are not. These difficulties with navigating the interface have contributed to inefficiencies, reduced user engagement and led to workarounds.

Improvements are needed to ensure Assist remains available and can be recovered after an incident

Communities may not be able to effectively deliver services for children during an Assist outage, as key information on how to deliver services when Assist is unavailable does not exist or has not been maintained and tested.

- **Business continuity plans have not been finalised or tested –** Communities has multiple business continuity plans for its metropolitan and regional offices. We reviewed four and found each of them lacked details on how Communities would deliver child protection services during an Assist outage. Additionally, three of the four plans were either in draft, not updated or not tested. Appropriate planning and testing help staff understand how to continue to deliver services and reduce the likelihood of a prolonged outage and disruption to services.
- **Disaster recovery has not been tested –** Communities has disaster recovery procedures and environment[5] for the Assist application. However, these procedures have not been tested to verify their effectiveness. Assist is a complex system with recovery dependent on multiple vendors. Testing would provide confidence that procedures are fit for purpose to recover Assist in line with business expectations and needs.
- **Assist is a legacy application with some of its components not fully supported by software vendors –** While a contracted application support vendor provides support and maintenance services for Assist, we found several of Assist's underlying software components no longer receive new patches/fixes or receive limited support, increasing the likelihood of technical vulnerabilities. Additionally, we found instances of Assist being temporarily unavailable due to updates (operating system and/or supporting software) causing incompatible Assist software components to fail. Communities plans to replace Assist by 2028 and has received initial[6] funding of $4.5 million. Replacement by 2028 depends on a full understanding of the complexity of existing processes and systems and is subject to further funding.
- **Out-of-hours incident risks need better management –** the Assist application support vendor is only contracted to provide best-efforts support for incidents outside of business hours. This increases the likelihood of an extended outage to Assist, which Communities has not factored into its business continuity planning, and creates a risk that staff operating in a 24/7 environment may not be able to access important information when required.

[5] A backup site and IT infrastructure used to recover systems when the primary system and infrastructure is unavailable due to an incident.

[6] Funding to develop a business case and a project definition plan. These document the scope, cost, schedule and risks to a project.

Recommendations

1. To protect the confidentiality of Assist information, Communities should:

    a. review its current practices to ensure sensitive information is only stored in its approved recordkeeping systems

    Implementation timeframe: 30 June 2025

    Entity response: Accepted

    Communities is reviewing its current practices to ensure sensitive information is stored in secure locations and its record keeping systems of Assist and Objective.

    b. review, document and update user access permissions to ensure information is accessible on a need-to-know basis as required by staff roles

    Implementation timeframe: 30 June 2025

    Entity response: Accepted

    Communities staff engaged in statutory roles must undergo and pass screening to have access to sensitive information. Communities' professional workforce cohort that has access to system information are well versed in managing sensitive information appropriately. Communities is reviewing its Assist access matrix and will update permissions where appropriate to continue to support access on a need-to-know basis as required by staff roles and to support current workforce practice.

    Staff are also well versed in initiating restrictions for sensitive cases to combat conflict of interest issues. Communities will review and update guidance on initiating restrictions for sensitive cases and where appropriate enhance and recommunicate to ensure a consistent application of workforce practice.

    c. fully understand and utilise Assist and related systems' logging and monitoring capabilities to detect inappropriate access and modifications.

    Implementation timeframe: 30 June 2025

    Entity response: Accepted

    Communities will assess the current logging and monitoring capabilities of Assist and examine the feasibility of defining further key events to be audited and implemented.

2. To ensure the integrity of Assist information, Communities should:

    a. continue to identify and address duplicate information in Assist

    Implementation timeframe: 31 December 2025

    Entity response: Accepted

    Communities will continue to take active measures in addressing and minimising duplicate information within Assist through workforce education to ensure consistent practice and where feasible technology enhancements to identify and merge duplicates where appropriate.

b. implement controls to prevent modification of data without appropriate reasons.

Implementation timeframe: 31 December 2025

Entity response: Accepted

Communities will review Assist functionality and process and undertake required changes where feasible to ensure data integrity.

Due to the nature and immediacy of a child safety investigations (CSI) Communities will commence investigation activities, inclusive of safety planning as its priority of response. The current Assist Application functionality makes recording time consuming and requires dedicated time post the initial response to ensure the correct information is transferred from recorded notes and documents stored in Objective [Communities' record keeping system]. Communities will review the existing functionality of the Assist Application and if feasible add in the capacity to record the reasons for change in start dates to ensure auditing and governance processes are enhanced.

3. To ensure the availability of Assist and its information, Communities should:

a. develop appropriate business continuity plans to clearly define how Communities will deliver child protection services when there is an Assist outage

Implementation timeframe: 30 June 2025

Entity response: Accepted

Communities will ensure processes are put in place to regularly test its business continuity plans (BCPs) to ensure continuance of service delivery is attainable and sustainable in the event of an extended outage of the Assist Application.

b. regularly test business continuity and disaster recovery plans

Implementation timeframe: 31 December 2025

Entity response: Accepted

Communities will conduct appropriate regular tests to verify the effectiveness of its existing Assist Disaster Recovery Process (DRP) and procedures to ensure that the existing plan is fit for purpose and delivers the intended result of recovery in line with business expectations.

c. update vendor contracts to include after-hours support where required by business needs.

Implementation timeframe: 31 December 2025

Entity response: Accepted

Communities will review existing vendor after hours support arrangements and amend to suit business response times where appropriate and feasible.

Response from the Department of Communities

The Department of Communities (Communities) acknowledges and accepts the recommendations included in Communities Assist report from the Auditor General.

Communities extends its thanks to the Office of the Auditor General (OAG) for its review and provision of recommendations in relation to the Assist Application. As identified in the report, the Assist Application is a legacy system that is due for replacement. A business case to undertake this work was submitted and funding appropriated to provision a detailed Project Definition Document (PDP). The PDP has now been finalised.

In relation to the summarised recommendations Communities has initiated actions where appropriate to enhance its existing processes and procedures, and information management and controls for system access.

Communities is committed to addressing the findings identified and will continue to pursue maturing our capabilities in cybersecurity and audit controls and information governance, management and privacy awareness.

Audit focus and scope

Each year we review a selection of important software programs (applications) that public sector entities rely on to facilitate their key business processes. Applications help entities perform important routine functions (such as finance, human resources, case management, licensing, billing and service delivery) and those functions that are unique and essential to them. If applications and their related processes are not managed appropriately, stakeholders including the public, may be affected.

We review key application controls that ensure information is complete, accurately captured, processed and maintained. Failures or weaknesses in these controls can result in loss or inappropriate use or disclosure of information and service delivery delays and disruptions. They also increase the risk of fraud and financial loss.

Our tests may highlight weaknesses in control design or implementation that increase the risk that an application's process or information may be susceptible to compromise. While our tests are not designed to identify if information has been compromised, we may become aware of instances during an audit.

This was an independent audit, conducted under section 18 of the *Auditor General Act 2006*, and in accordance with Australian Auditing and Assurance Standards. The approximate cost of undertaking the audit and reporting was $195,000.

Auditor General’s 2024-25 reports

Number	Title	Date tabled
9	Child Protection Case Management System – Assist	21 March 2025
8	Universities and TAFEs 2023 – Financial Audit Results	5 December 2024
7	WA Student Assistance Payment – Controls Review	27 November 2024
6	Provision of Additional Information to the Standing Committee on Estimates and Financial Operations – Opinions on Ministerial Notifications	22 November 2024
5	Implementation of the Aboriginal Procurement Policy	21 November 2024
4	Quality and Utilisation of Emergency Department Data	20 November 2024
3	Management of State Agreements	30 October 2024
2	Legislative Reform Priorities and Timeframes – Opinion on Ministerial Notification	19 August 2024
1	Supplier Master Files – Better Practice Guide	1 August 2024

Office of the Auditor General
for Western Australia

7th Floor Albert Facey House
469 Wellington Street, Perth

T: 08 6557 7500
E: info@audit.wa.gov.au

www.audit.wa.gov.au

@OAG_WA

Office of the Auditor General
for Western Australia