Office of the Auditor General
Serving the Public Interest

Report 5: 2023-24 | 22 September 2023

INFORMATION SYSTEMS APPLICATION AUDIT

Triple Zero

Office of the Auditor General
Western Australia

Audit team:
Aloha Morrissey
Kamran Aslam
Michael Chumak
Svetla Alphonso
Fareed Bakhsh

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: Tapati Rinchumrus/shutterstock.com

WESTERN AUSTRALIAN AUDITOR GENERAL'S REPORT

Triple Zero

Report 5: 2023-24
22 September 2023

This page is intentionally left blank

THE PRESIDENT
LEGISLATIVE COUNCIL

THE SPEAKER
LEGISLATIVE ASSEMBLY

TRIPLE ZERO

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 computer aided dispatch call management system (Triple Zero). The system is used by the Western Australia Police Force, the Department of Fire and Emergency Services and Western Australia's ambulance services to respond to emergencies and life-threatening incidents in WA.

I wish to acknowledge the entities' staff for their cooperation with this audit.

CAROLINE SPENCER
AUDITOR GENERAL
22 September 2023

Contents

Auditor General's overview

The Triple Zero system is critical to the real-time deployment of emergency response resources to the Western Australian (WA) public. The system is used by the WA Police Force, the Department of Fire and Emergency Services (DFES) and WA's ambulance services.

Our audit looked at system use by the WA Police Force and DFES, and how the confidentiality, integrity and availability of the Triple Zero system and its information is safeguarded. We did not examine system use by WA's ambulance services.

We found that Triple Zero assists the WA Police Force and DFES to manage and respond to emergencies. It was pleasing to find that both entities had implemented sufficient controls to protect the integrity of Triple Zero and its information, including the use of data quality reviews to identify significant issues.

However, both entities lacked controls to detect unauthorised access to sensitive or personally identifiable information held in the system, such as reports on domestic violence incidents and other criminal incidents. This is a common issue that we continue to find through our information system audits. In addition, deficiencies in interagency governance arrangements, and recovery and support plans could hinder the availability of Triple Zero and entities' ability to respond to system outages effectively.

I recognise the work that WA Police Force has already completed in recent months to address some of the audit findings and note both entities' commitment to addressing the outstanding weaknesses.

Introduction

This audit assessed the computer aided dispatch call management system (Triple Zero). The system is used by the Western Australia Police Force (WA Police Force), the Department of Fire and Emergency Services (DFES) and Western Australia's (WA) ambulance services to respond to emergencies and life-threatening incidents in WA.

Our objective was to determine if the WA Police Force and DFES effectively manage the confidentiality, integrity and availability of the Triple Zero system and its information. The audit did not examine system use by WA's ambulance services.

Background

Triple Zero, a commercial off-the-shelf system, has been used by the WA Police Force since 2004 and DFES since 2017. Both entities, through an interagency Memorandum of Understanding (MoU), use Triple Zero to support statewide call-taking, real-time deployment of emergency response resources and management of incident records.

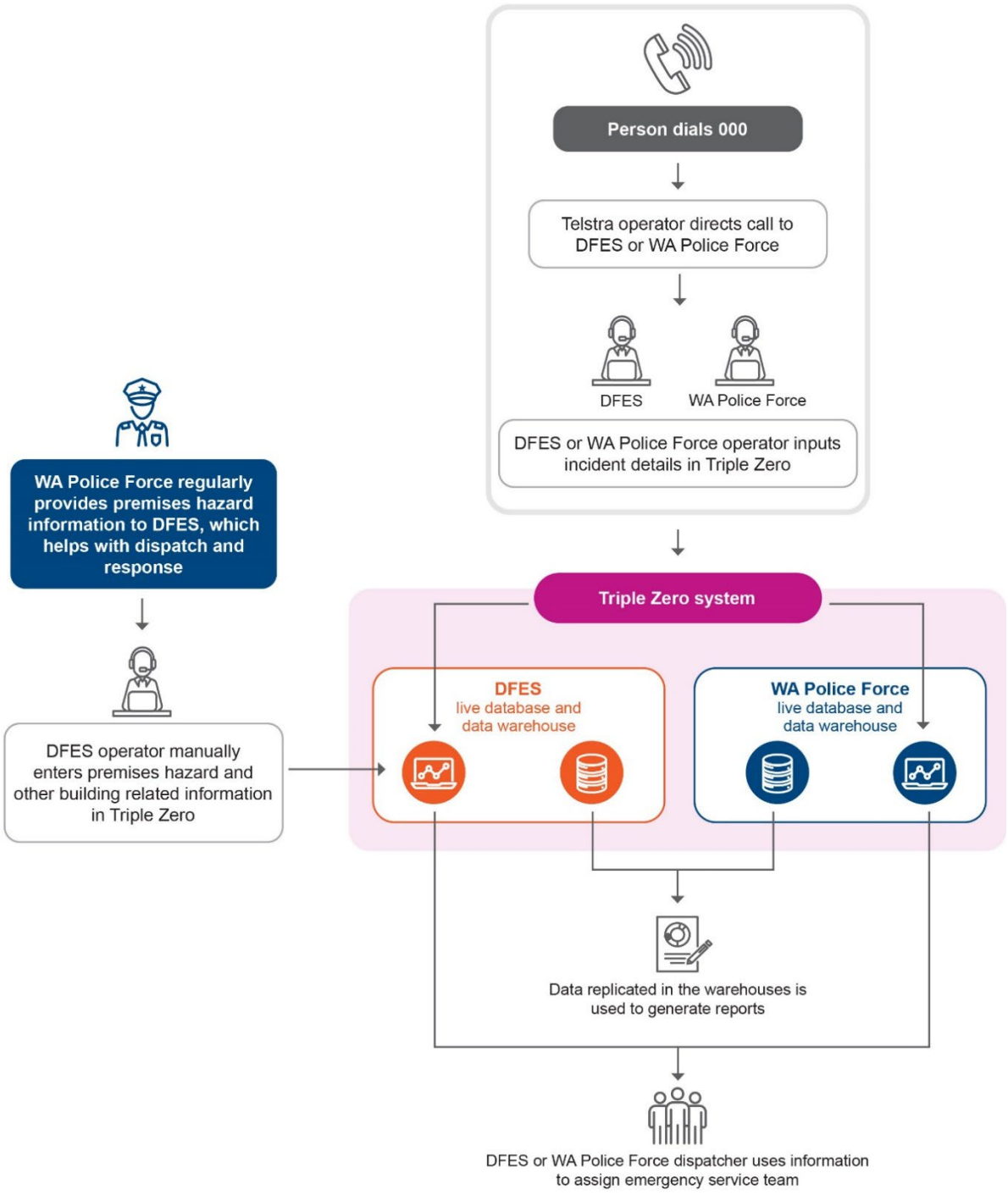
When a person dials 000, a Telstra operator transfers them to the relevant emergency service (police, fire or ambulance). The emergency service then speaks directly to the caller and records information in Triple Zero including personal and sensitive information such as people's names, addresses and details of possible domestic violence and other criminal incidents.

The WA Police Force and DFES also provide other information, which is stored in the system to support emergency response efforts. This includes premises hazard information and plans for buildings protected with Direct Brigade Alarms[1] and significant premises such as government, medical and industrial buildings.

All Triple Zero information is stored in separate WA Police Force and DFES live databases. The databases are replicated to data warehouses, which the entities use to develop reports, such as the number of daily incidents and incident response times (Figure 1). Entities' staff access Triple Zero through workstations and mobile devices (phones and tablets).

The WA Police Force is the lead entity responsible for hosting the Triple Zero infrastructure, managing the data centres and servers, and contract management with the vendor who developed the system. Both the WA Police Force and DFES have contracts with the vendor for ongoing support such as backups and keeping the system up-to-date and secure. However, WA Police Force is the first point of escalation for DFES to resolve technical problems.

[1] DFES maintains a fire alarm monitoring network for all buildings that require direct links to a fire brigade.



Source: OAG

Figure 1: Key elements of the Triple Zero business process[2]

[2] The audit did not examine Triple Zero use by WA's ambulance services.

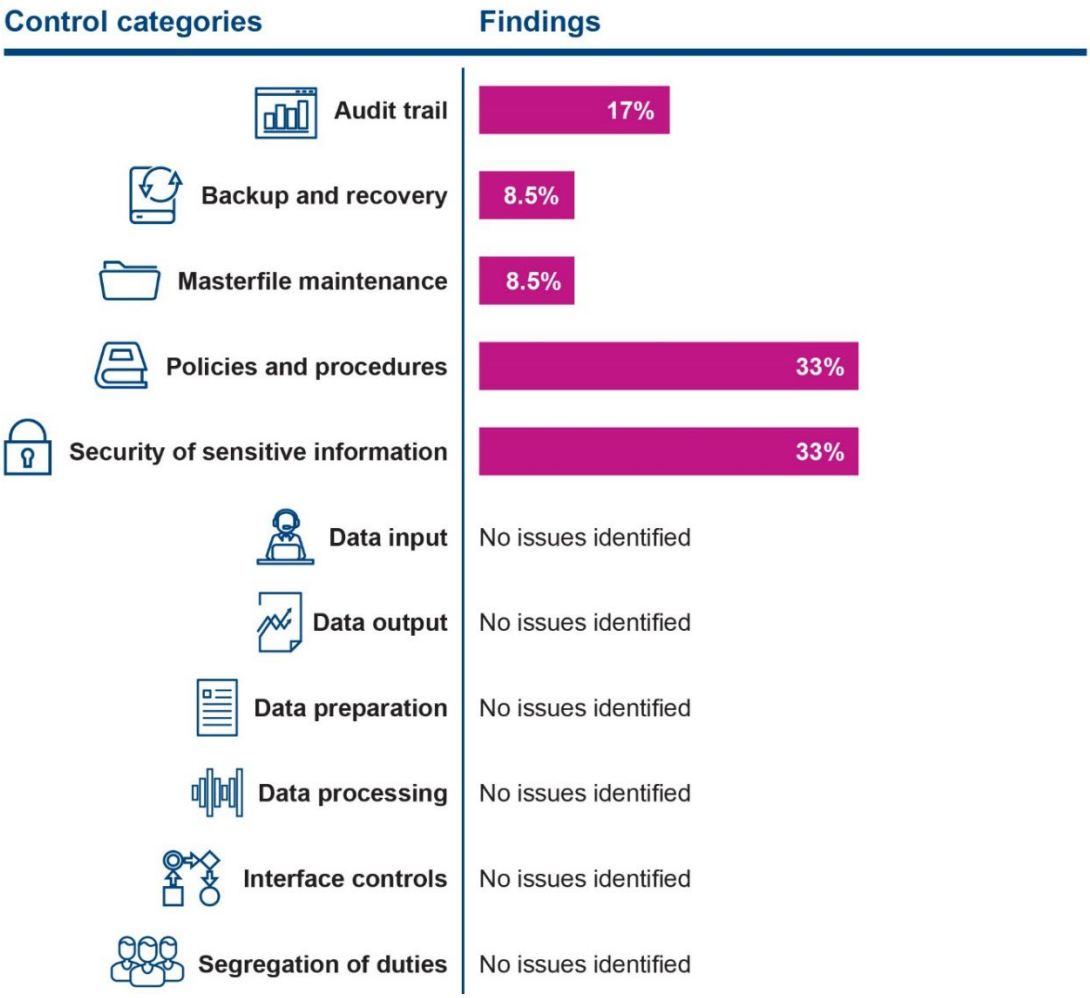
Conclusion

The Triple Zero system is essential to the WA Police Force's and DFES' response to emergencies. Sufficient controls were in place to protect the integrity of data, however both entities need to improve their controls to protect the confidentiality of personal and sensitive information and maintain the availability of the system.

We found there were insufficient access controls that could result in unauthorised access to sensitive information. At DFES, inadequate staff screening processes further exacerbate the potential for inappropriate access. A lack of system activity logs and monitoring means inappropriate access will go unnoticed.

The WA Police Force has not promptly addressed known vulnerabilities which could result in degraded services. Additionally DFES and the WA Police Force do not have effective governance arrangements and adequate recovery and support plans, which will hinder their ability to continue operations and respond to outages effectively.

Findings



Source: OAG

Figure 2: Percentage of OAG audit findings in Triple Zero system by control category

Weak access controls increase the risk of unauthorised access to sensitive and personal information

WA Police Force do not monitor access to information in the data warehouse

Most WA Police Force staff can access information in the Triple Zero data warehouse through reports, but this access and activity are not appropriately logged and monitored, unlike the live database which is restricted and monitored. As a result, unauthorised or inappropriate access to sensitive or personally identifiable information, such as reports on incidents involving domestic violence or high-profile individuals, may go unnoticed.

DFES' use of generic accounts and shared passwords undermine accountability

DFES staff use a generic workstation account and a shared password to access Triple Zero. As such, DFES is unable to identify who accesses sensitive or personal information and if the access is authorised and appropriate. Although the Triple Zero vendor captures access logs to the live database and the data warehouse, monitoring of these will not help identify unauthorised or inappropriate access due to the use of generic accounts.

Case study 1: Disclosure of sensitive data on social media

DFES suffered a data breach in November 2021 where sensitive information about a Triple Zero incident was shared on social media. DFES could not identify who was responsible for the unauthorised disclosure due to the use of the generic account.

Dedicated privileged accounts are not used for system maintenance

The WA Police Force has granted administrator privileges for Triple Zero maintenance to a number of day-to-day use accounts. Privileged accounts provide immense levels of access and if compromised can be used by malicious actors to compromise the confidentiality, integrity and availability of Triple Zero. It is better practice to separate accounts with administrator privileges from day-to-day accounts.

Further, the WA Police Force does not require all users to have a strong password that complies with its information security guidelines. However, multi-factor authentication is in place, which reduces the risk of breaches from compromised passwords.

Inadequate DFES employee screening processes increase the risk of internal threats

DFES staff are only required to have a basic national police clearance, which may not be adequate for staff accessing sensitive Triple Zero information. For example, information on high-profile individuals, buildings access codes and plans, and premises hazard information. Inadequate screening increases the likelihood of inappropriate access.

Some known vulnerabilities have not been addressed to protect Triple Zero from cyber threats

The WA Police Force performed a penetration test of Triple Zero during a system upgrade in late 2020 and promptly addressed the critical weaknesses. These tests are an effective mechanism to identify and help address system vulnerabilities.

However, the WA Police Force's 2023 vulnerability reports indicate a number of other critical weaknesses that could affect Triple Zero and other IT infrastructure. While patches for these weaknesses have been available for several years, the WA Police Force has not applied them. In addition, its Triple Zero database runs on a system no longer supported by the vendor. Unsupported legacy systems are generally costly to maintain and no longer receive security updates to address vulnerabilities. If these are not addressed, Triple Zero is more susceptible to potential threat actors who may want to exploit these vulnerabilities to compromise the confidentiality, integrity and availability of the system and its information.

The WA Police Force told us a regular process to address weaknesses and upgrade Triple Zero servers to vendor-supported versions has now been implemented.

Ineffective governance could impact availability

The Triple Zero disaster recovery plan is inadequate

The draft Triple Zero disaster recovery plan (DRP) does not establish clear targets to minimise downtime and data loss during an adverse event. In July 2022, the WA Police Force conducted a Triple Zero DRP test for the first time in three years. It identified several issues including a lack of effective interagency communication and outdated documentation. These issues remain unresolved.

If an effective and up-to-date DRP is not in place, this could intensify the negative impact of a Triple Zero outage and any arising data loss incidents.

Outdated interagency cooperation documents could lead to service disruptions

Various steering committees provide governance over Triple Zero operations, contract and interagency cooperation, but terms of reference for these committees have remained in draft since 2018. Further, the MoU between DFES and the WA Police Force for the use of the Triple Zero has not been updated since 2018. Out-of-date documents increase the risk of service degradation due to ineffective governance.

DFES's internal incident management, call escalation for system troubleshooting and change management policies are in draft and unapproved. We acknowledge that in November 2022, DFES engaged a third party to review its incident data quality which did not identify any significant problems.

Case study 2: Consequences of ineffective interagency governance on Triple Zero

The WA Police Force conducts ongoing changes to infrastructure that supports Triple Zero without notifying DFES. This has led to multiple outages at DFES. If DFES is not aware of important changes, it cannot adjust its infrastructure to account for changes, resulting in Triple Zero downtime.

The lack of effective interagency governance, coordination and communication can significantly disrupt Triple Zero, delaying the delivery of emergency services to the WA community.

Vendor service and support plan is out-of-date

While the WA Police Force has established an escrow[3] agreement with the system vendor, it has not finalised service support specifications since 2016. It has also not reviewed the services management plan with the vendor since 2017. This plan defines all service and support operations for Triple Zero. As a result, support specification and the services management plan may no longer be fit for purpose and lead to inadequate support arrangements.

Governance roles and responsibilities could be improved

The MoU between the WA Police Force and DFES has documented roles and responsibilities. The WA Police has a Triple Zero system custodian who is also responsible for overseeing other key applications. As a result, compliance with security policies and standards, internal and interagency service level agreements, and licensing requirements may not be prioritised. Without effective governance, there is an increased risk Triple Zero will not align with business objectives.

[3] A software escrow helps protect all parties involved in a software license by having a neutral third party (escrow agent) hold source code, data and documentation.

Recommendations

DFES and the WA Police Force should:

1. revise and finalise the Memorandum of Understanding and Triple Zero governance documents to align with business objectives.

   Implementation timeframe: three to six months

   WA Police Force response:

   The WA Police Force will work to revise the Memorandum of Understanding (MoU) and Triple Zero (also known as Premier 1 Computer Aided Dispatch or P1CAD) governance documents. Consultation with DFES will be undertaken to agree on what revisions are required and how the MoU should be worded.

   Implementation timeframe: December 2023

   DFES response:

   Agree. DFES will work with WA Police Force to implement this recommendation.

2. improve access management controls to ensure access to sensitive Triple Zero information is monitored and can be tracked to individuals.

   Implementation timeframe: 12 months

   WA Police Force response:

   All WA Police Force user access direct to P1CAD can be traced to individual accounts. There is a known issue where some reports that contain some P1CAD data can be accessed without appropriate logging or monitoring. This issue is being investigated and will be addressed.

   Implementation timeframe: June 2024

   DFES response:

   Agree. DFES has already increased technical controls where possible, and has plans in place to further reduce technical controls in outstanding cases, with these cases being remediated by non-technical management processes and protocols in the interim of full remediation.

DFES should:

3. review its employee screening processes for staff with access to sensitive information and implement higher screening processes where appropriate.

   Implementation timeframe: December 2023

   Entity response:

   Agree. DFES is reviewing the employee screening protocols and will implement higher screening protocols where it is deemed appropriate.

The WA Police Force should:

4. continue to undertake security assessments and promptly identify, assess and address known vulnerabilities.

   Implementation timeframe: Ongoing

Entity response:

The WA Police Force has addressed all known vulnerabilities of the P1CAD application. This work was completed in June 2023.

The WA Police Force has taken significant steps in the past year to improve Cyber Security and vulnerability management of policing applications. Vulnerability Management meetings are held monthly to identify new cyber security threats and vulnerabilities and put in place plans to treat those vulnerabilities. As Cyber Security threats are ever evolving, this is an ongoing process that requires ongoing vigilance and effort.

5. improve its governance and oversight of Triple Zero's support, maintenance and recovery activities.

Implementation timeframe: six months

Entity response:

The WA Police Force has a system custodian for P1CAD who is responsible for ensuring compliance with security policies and standards, internal and interagency service level agreements, and licensing requirements. However, they also have this responsibility for other core policing applications. The WA Police Force are reviewing the workload of the role to determine whether a dedicated system custodian for P1CAD is required.

6. review and finalise its Triple Zero disaster recovery plan and other important vendor service plans.

Implementation timeframe: 12 months

Entity response:

The WA Police Force has a contemporary, but draft, P1CAD disaster recovery plan, which has been updated to address deficiencies identified in the latest disaster recovery test. Work to complete and endorse the disaster recovery plan amongst appropriate business and vendor stakeholders is ongoing.

Response from the Western Australia Police Force

Triple Zero (Computer Aided Dispatch) is a core policing application, critical to the day-to-day operations of the WA Police Force. The WA Police Force takes the recommendations of the Office of the Auditor General very seriously and work to address the recommendations has and will continue to be undertaken as a priority.

The WA Police Force has made significant efforts over the past year to address many of the recommendations of the Triple Zero Application Audit. Work to address the outstanding recommendations noted in this audit is continuing and will be completed over the coming year.

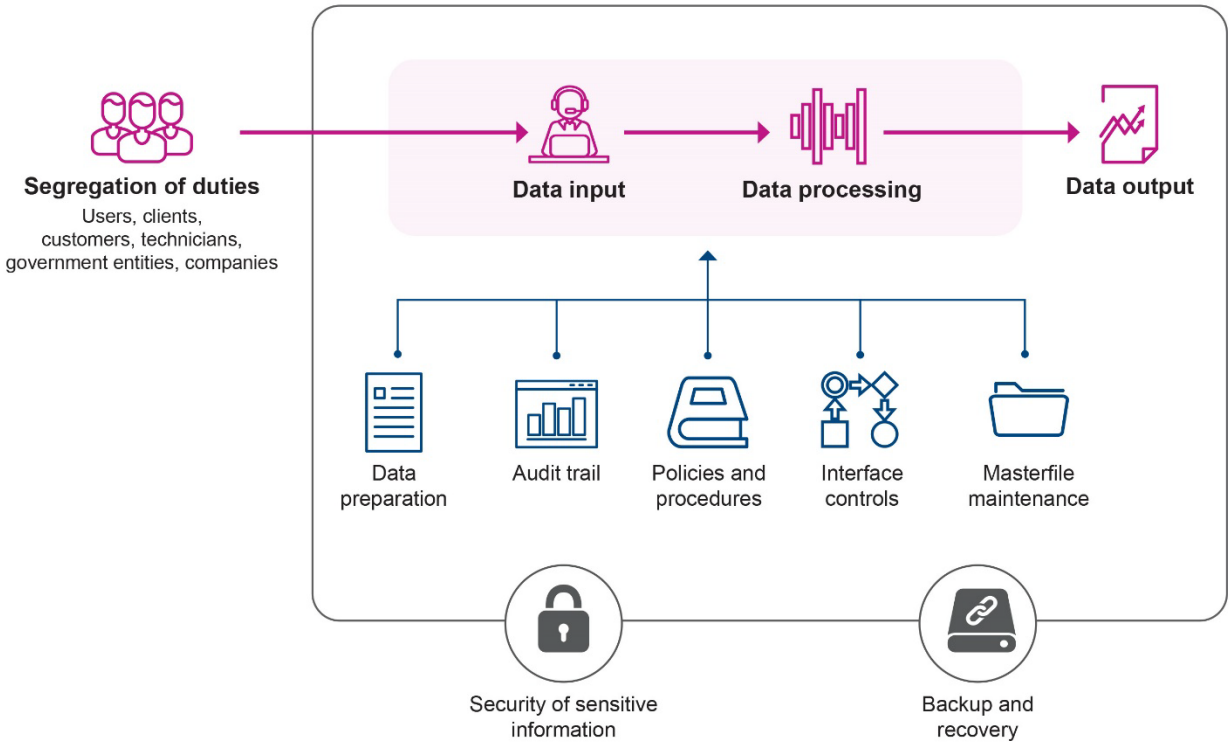
Response from the Department of Fire and Emergency Services

DFES notes the improvements and recommendations and has already begun making improvements regarding the recommendations. Some of the technical and procedural improvements will require longer timeframes for implementation based on a number of factors, so DFES will implement interim mitigation protocols where required to mitigate possible near-term risks.

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 important service delivery) and other 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.

Our application controls audits focus on people, process, technology and data. In considering these elements, we follow data from input and processing through to storage, handling and outputs.



Source: OAG

Figure 3: Key elements of focus in our application audits

We review key 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, service delivery delays and disruptions, and 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.

We reviewed a sample of key controls and processes to obtain reasonable assurance that Triple Zero worked as intended. Our testing was performed between August 2022 and May 2023 and is a point in time assessment.

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 $105,000.

This page is intentionally left blank

Auditor General's 2023-24 reports

Number	Title	Date tabled
5	Triple Zero	22 September 2023
4	Staff Exit Controls for Government Trading Enterprises	13 September 2023
3	Financial Audit Results – Local Government 2021-22	23 August 2023
2	Electricity Generation and Retail Corporation (Synergy)	9 August 2023
1	Requisitioning of COVID-19 Hotels	9 August 2023

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