Office of the Auditor General
Serving the Public Interest

Report 4: 2023-24 | 13 September 2023

PERFORMANCE AUDIT

Staff Exit Controls for Government Trading Enterprises

Office of the Auditor General
Western Australia

Audit team:
Jason Beeley
Andrew Harris
Jeremy Bean
Nicholas Chin
Chris White

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: Prostock-studio/shutterstock.com

WESTERN AUSTRALIAN AUDITOR GENERAL'S REPORT

Staff Exit Controls for Government Trading Enterprises

Report 4: 2023-24
13 September 2023

This page is intentionally left blank

THE PRESIDENT
LEGISLATIVE COUNCIL

THE SPEAKER
LEGISLATIVE ASSEMBLY

STAFF EXIT CONTROLS FOR GOVERNMENT TRADING ENTERPRISES

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

Performance audits are an integral part of my Office's overall program of audit and assurance for Parliament. They seek to provide Parliament and the people of WA with assessments of the effectiveness and efficiency of public sector programs and activities, and identify opportunities for improved performance.

This audit assessed whether four government trading enterprises effectively and efficiently manage the exit of staff to minimise security, asset and financial risks.

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

CAROLINE SPENCER
AUDITOR GENERAL
13 September 2023

Contents

Auditor General’s overview

Entities need to ensure when a staff member leaves that premises and information are protected, and all public assets recovered. Ineffective controls increase the risk of security breaches and the loss of information, physical assets and public money. Issues with controls on staff exits are regularly identified in my Office's financial and information systems audits, and performance audits on this topic.

For this audit, my Office chose to look at government trading enterprises, in part to see if the different operating environment made a difference to both the risks and controls around staff exits. We found that risks and controls are similar and that although performance was generally better than other State sector entities we have examined, areas for improvement remain.

We found responsibility for staff exit controls is often shared across business units that may not routinely work together, so entities need good systems and policies to support effective coordination. Also that exit controls were not adapted to the different risks posed by high integrity positions and high risk exits. This is similar to what we found in our August 2021 audit of State government entities.

I recommend all public sector entities consider the findings, recommendations and better practice material in this and previous reports, and seek to apply them in their own operating context.

Executive summary

Introduction

This audit assessed whether four government trading enterprises (Electricity Generation and Retail Corporation (trading as Synergy), DevelopmentWA, Insurance Commission of WA and Pilbara Ports Authority) effectively and efficiently manage the exit of staff to minimise security, asset and financial risks.

Our office regularly conducts control health checks on entities to ensure the systems they use are effective and secure. Our 2021 Staff Exit Controls[1] audit on State government entities found that access to work premises and information technology (IT) systems was not consistently cancelled immediately, exit controls were not risk based and adjusted for high integrity positions, and termination type and salary overpayments or debts were not settled at the time. Our office's recent work in financial and information systems audit have consistently found similar issues.

Background

Government trading enterprises (GTEs) are owned by the State Government. While GTEs are public entities, they operate in a commercial business environment and in accordance with prudent commercial principles. The main purpose of a GTE is to increase financial and community benefit through the performance of its function.

A GTE's function is determined by its Establishing Act. Establishing GTEs in this way is intended to create a more accountable, commercial and competitive operating environment than that of typical government entities. Being at arm's length from Government, they have the autonomy to introduce private sector disciplines, incentives, sanctions and competition that are expected to secure operational efficiencies and ensure value for money service delivery.

GTEs provide services and supporting infrastructure to nearly every household and business in the State. To deliver these services, they manage critical infrastructure such as electricity substations and port facilities. GTEs provide their employees with a range of assets to carry out their duties, including computers, laptops, tablets, mobile phones, credit cards, vehicles and housing. Many also have access to commercially sensitive information on transactions between the State and private companies, and personal information on the public.

At the four audited entities, 1,186 people, including contractors, ceased employment in the 12-month period to February 2023.

[1] Office of the Auditor General, *Staff Exit Controls*, OAG website, 5 August 2021, accessed 13 September 2023.

Entity	Contractors	Employees	Total exits	Selected sample
Electricity Generation and Retail Corporation (Synergy)	737	193	930	30
DevelopmentWA	60	31	91	28
Insurance Commission of Western Australia (ICWA)	7	58	65	28
Pilbara Ports Authority (Pilbara Ports)	35	65	100	27
Total	**839**	**347**	**1,186**	**113**

Source: OAG using audited entity information

Table 1: Number of terminations at the audited entities

A staff member may cease employment with an entity for a range of reasons including through resignation, retirement, dismissal, end of contract or permanent transfer to another public sector entity. When a staff member ceases employment with the entity, the entity should:

- cancel access to the information systems, premises and confidential information immediately
- deactivate all security access passes and keys
- collect all entity issued property
- recoup all financial debts from the exiting employee
- offer exit interviews.

The Digital Security Policy[2] issued by the WA Office of Digital Government provides a checklist of controls that all entities responsible for public assets should apply. It includes making clear the enduring requirement for staff to maintain the security of information after they leave employment with a government entity, and that entities should ensure that all IT assets are returned when the person's employment ends. Entities need to assess the security implications and other risks posed by all staff who leave their employment, regardless of the reason.

In each of our sampled entities, the staff exit management process is a shared responsibility between multiple business units (Figure 1). Good staff exit management requires all business units to work together to ensure actions are completed promptly. Failure to provide an effective staff exit management process exposes the entity to risks of security breach and asset or financial loss.

[2] Office of the Government Chief Information Officer, *Whole-of-Government Digital Security Policy*, Office of the GCIO, Perth, 2017.

Source: OAG using audited entity process maps and information

Note: The business unit names and configurations may vary at different entities.

Figure 1: Five key business units generally involved in the staff exit management process

This report includes a better practice guide, adapted from the Australian Government Protective Security Policy Framework[3] to assist entities to strengthen their staff exit controls (Appendix 1).

Conclusion

The GTEs we audited have been generally effective and efficient in managing their staff exits. They could demonstrate that assets had been returned, access to information systems had been cancelled and overpayments had been managed. However, there are areas where all four GTEs can improve to further reduce risk.

Physical and information security risks were not always minimised. Entities were not consistently managing the return of assets on the day of termination. Only one entity routinely minimised the information security risk through the consistent cancellation of access to information systems within 24 hours of the exit date.

[3] Department of Home Affairs, *Protective Security Policy Framework*, protectivesecurity.gov.au, n.d., accessed 8 August 2023.

Staff exit controls in entities are not risk based to take account of high integrity positions and the circumstances in which staff leave. Staff leaving high integrity positions with, for example, access to sensitive or commercial-in-confidence information and critical infrastructure are not subject to risk assessment and adjusted exit controls.

The use of exit interviews and surveys varied among the sampled entities, with some limiting them based on employment status or length of service. This meant that contractors were often excluded from this feedback mechanism. Not seeking feedback from exiting staff misses an opportunity for identifying areas of improvement in business operations.

Findings

Entities do not always remove access and collect assets in a timely manner when staff exit

Delays in access cancellation risks unauthorised access to information systems and premises

DevelopmentWA performed better than the other three entities as all exiting staff's access to information systems and premises was removed when it was no longer required. For the other entities we audited, we found 74 users whose access was removed within 24 hours of the exit date but in 11 instances across the three entities, it took between two and 112 days after the exit date to remove access to information systems and premises (Table 2). While we did not identify any inappropriate access to systems, these delays increase the risk and can compromise the integrity and confidentiality of the information held on the entities' systems.

At ICWA, in a sample of 28, we found five instances where user access was not removed within 24 hours of the exit date. In one case, internal audit found access to information systems had not been removed 112 days after the exit date. The entity advised that this was the result of an IT issue and has since changed its internal processes.

At Pilbara Ports, access to systems was not cancelled the day after the exit date in three out of 27 instances. Although the access cancellations were less than three days after exit, the small delay still posed a risk of unauthorised access to confidential information. Pilbara Ports advised us that employees have confidentiality obligations that survive their employment contract.

In addition to the three instances where access to information systems was not cancelled within 24 hours, we found another two instances where access to premises was not removed within 24 hours of the exit date. Pilbara Ports advised us that access to the site is monitored on a 24/7 basis.

Pilbara Ports advised that, for two of the cases, notification to remove access to systems was received late on a Friday and could only be completed the next business day, which was a Monday. In one of these cases, physical access to premises was also not cancelled until the Monday, allowing free access for the former staff member over the weekend. We did not identify any inappropriate access over the weekend for these two cases however the delay increased the risk of unauthorised access and weakened controls over inappropriate use.

Entity	Number of instances	Minimum number of days	Maximum number of days
ICWA	5	3	112
Pilbara Ports	5	2	6
Synergy	1	41	41

Source: OAG using audited entity information

Table 2: Number of instances and days to cancel access to information systems and premises after the exit date

Not all entities were effectively managing the return of assets on the last day of employment

We found instances at Pilbara Ports and Synergy where asset management systems showed assets not returned on the day of exit. Assets included laptops, tablets, mobile

phones and credit cards. Out of a sample of 30 staff exits at Synergy, nine individuals (30%) had a total of 12 instances where asset management systems showed late return of assets. We found similar process gaps at Pilbara Ports where eight out of 27 sampled staff exits (30%) had a total of nine instances where asset management systems showed late return of assets (Table 3). Pilbara Ports advised us that while the asset management systems recorded the late return, the assets were held in their custody and posed no risk.

Entity	Laptop	Mobile device	Credit card
Synergy	9 (max 14 days)	2 (max 6 days)	1 (max 2 days)
Pilbara Ports	6 (max 7 days)	2 (max 5 days)	1 (max 5 days)

Source: OAG using audited entity information

Table 3: Number of instances where asset management systems showed assets not returned on the day of exit

Synergy, ICWA and Pilbara Ports could identify the dates assets were returned. During the audit, DevelopmentWA advised that their systems had limitations that would not allow the return dates to be entered but it has since advised of a process change to address this. Without any records of assets returned, entities cannot identify when the assets were collected and if there are any gaps in the staff exit management process. All four entities could demonstrate that assets issued to staff were ultimately returned.

While employees are commonly provided with computers, tablets, mobile phones and credit cards, in some cases, employees are provided with vehicles and houses. Synergy employees working onsite have access to vehicles while some Pilbara Ports employees are provided with housing. Physical return of such items does not always complete the process. For example, a vehicle was left at a Synergy worksite on an employee's last day, but it took 162 days for Synergy to reassign the vehicle to another employee by completing the internal transfer documents. This could have created liability issues between the driver and the insurance company if the vehicle had been involved in a crash during that time.

A failure to return assets and remove user access to information systems within 24 hours of the exit date exposes an entity to the risk of inappropriate access and financial loss.

Entities do not consistently monitor the staff exit process to ensure that it is effective

Entities do not monitor exits so they do not know if their policies are being complied with

Termination checklists are used at three of the entities (ICWA, DevelopmentWA and Pilbara Ports) while the fourth (Synergy) used an automated termination workflow for this purpose. We found incomplete termination checklists and actions outstanding at ICWA and Pilbara Ports. The inaccuracy of checklists makes effective review more difficult and risks missing steps in the exit process.

In 12 out of 27 instances (44%) at Pilbara Ports, IT termination checklists were not dated to identify when they were completed while two out of the 12 instances incorrectly showed assets not returned. Furthermore, human resources (HR) termination checklists for two contractors were not completed and signed by a delegated authority. However, Pilbara Ports advised that termination checklists are only used as a guide to assist staff during the staff exit process and should not be relied on as a control document.

At ICWA, we found that termination checklists were often incomplete. For example, we found three instances where leave audits were carried out but not marked on the termination

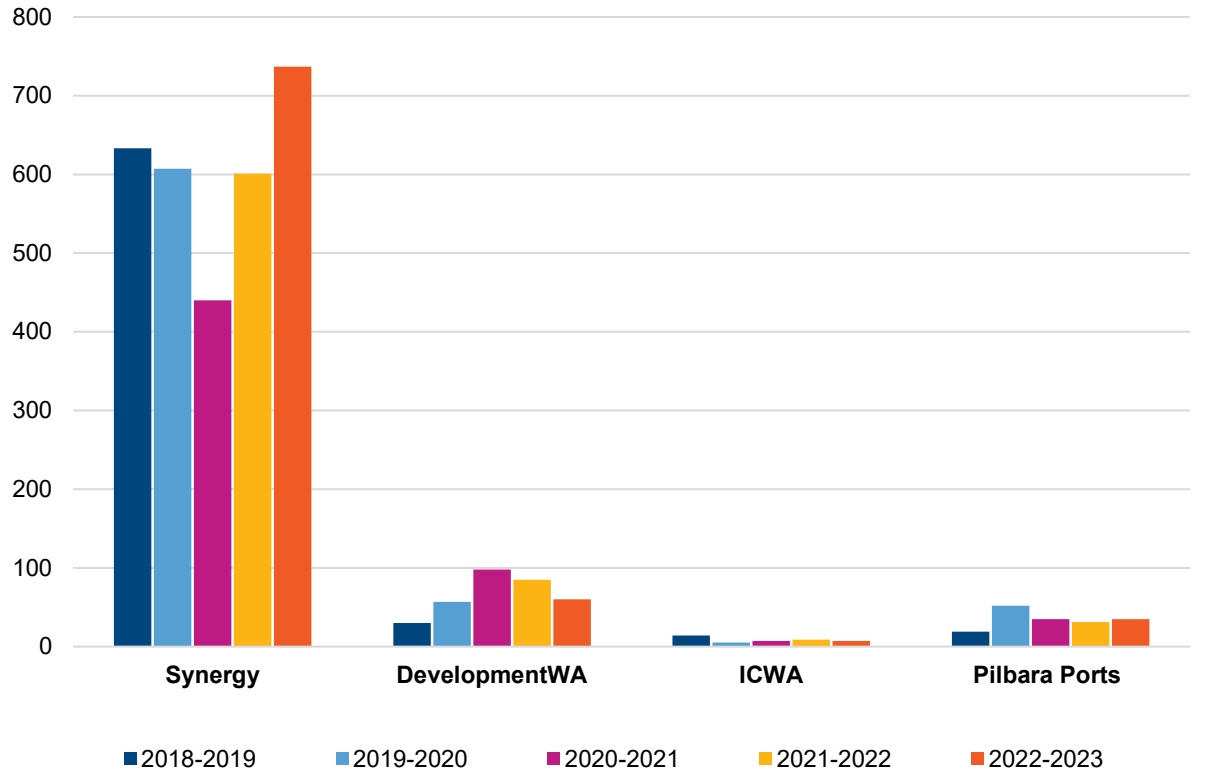
checklist when staff transferred to another public sector entity. Failure to use control documents such as checklists increases the risk of steps in the staff exit process being omitted. In the cited example, the risk is to the financial liability for accrued leave, which can represent a sizeable financial liability for an employer. It is important that balances are accurately paid out or transferred to other public entities.

Rather than manual termination checklists, Synergy uses an automated termination workflow to guide the staff exit process. We found nine instances where the termination workflow was initiated after the staff member had exited. For seven of these the average delay was under two days but one took 12 days and another 41 days. In the latter case, a contractor managed by an agency company had been on long term leave prior to their resignation and Synergy had not been aware that the contractor had effectively exited. It removed the contractor's access to information systems on the day it was informed.

At Synergy, contractor exit processes are managed by contractors' line managers rather than by HR staff with specialist expertise and centralised oversight. This practice and a lack of regular monitoring and communication between business units and agency companies creates a level of risk in the exit process. The risk is compounded by contractors exiting before the contract termination date while access is maintained for the length of the contract by default.

Of the entities we audited, Synergy relies most heavily on contractors (Figure 2) but we found the same issue affected all the entities. All contractor accounts are created with an expiry date, this is known as the contract end date. However, if the contracted services are no longer required, the contractor can exit prior to the contract end date. This leaves a gap between the exit date and the contract end date where the contractor still has access to the entity's information system. While our procedures found no evidence of inappropriate access after the exit date, this gap presents a risk to entities.

To address these concerns, it is vital that entities monitor the exit process closely to identify systemic and individual problems. This could be achieved by ensuring termination checklists and workflows are followed and verified by responsible parties when staff exit, whether they are employees or contractors. Failure to do so significantly undermines their effectiveness.



Source: OAG using audited entity information

Figure 2: Number of contractor terminations at the audited entities

Exit interviews are not consistently used in the exit process to identify areas of improvement

Across all four entities, only 59% (38 out of 64) of exiting employees we sampled were offered the opportunity to complete a staff exit interview. With the inclusion of contractors, this decreases to 34% (38 out of 113). Offering staff exit surveys to contractors could offer valuable insight as they provide an external view of the entities' current processes.

All four entities offer staff exit surveys as part of their staff exit process but they are limited either to employees only or employees and contractors engaged for longer than three months. Apart from DevelopmentWA, the entities in our sample did not offer the opportunity for contractors to complete either an interview or a survey. In our samples, 43% (49 out of 113) of staff exits we tested were employed as contractors.

At DevelopmentWA, 50% (6 of 12) of exited employees completed staff exit interviews in person with a staff member from HR.

Pilbara Ports offers exit surveys to all employees, which are completed online and provided by a third-party supplier. Exit surveys can also be completed face to face with a member of the HR team. Participation is voluntary and nine of 19 (47%) in our sample, did not complete an exit survey.

At ICWA, five out of 23 employees were offered a staff exit interview. Only employees with more than 12 months of service were offered this opportunity. The entity advised that this process has changed and risk-based decisions are now made to determine if exit interviews are offered to exiting employees.

Synergy was the only audited entity where none of the samples completed an exit survey. However, the entity could provide survey results completed by other exited employees within the audit period. The entity advised that the completion of exit surveys is optional.

Information from exit interviews and surveys can help entities to assess strengths and vulnerabilities, and focus workforce management strategies to drive talent attraction and retention. Consequently, restricting the opportunity for feedback to only employees presents a missed opportunity for the entity's business improvement.

Gaps in policies and procedures lead to inconsistencies in the staff exit process

Policies and procedures are not always complete, leaving parts of the process unclear to staff and they are not formally reviewed or approved

The policy and procedure documents we reviewed in all four entities have some gaps and do not provide complete guidance of the staff exit management process. For example, none of the policies or procedures state that cancellation of access to information systems should be completed within the best practice timeframe of 24 hours of the exit date. DevelopmentWA has since updated its processes to include this requirement. We also found that nearly half (13 out of 29) of the documents did not have a review or approval date. Policies and procedures that are not reviewed regularly may not reflect any recent changes in operations or environment.

Pilbara Ports has a dedicated team that manages housing and vehicles, but procedure documents were still being developed at the time of the audit to guide the team in the staff exit process. The management of housing can be more complex than assets such as laptops and mobile phones as there are regulations around vacating the property and recovering debts from staff. While there have been no issues to date with the return of housing or vehicles, a lack of documented procedures could increase the risk of disputes and associated costs, and inefficient use of assets.

Only ICWA had documented procedures to guide the collection of overpayments for staff. While only one of the four entities recorded an overpayment, lack of documentation to guide the recovery process means that staff are not aware of the process and regulations around collecting outstanding debt, potentially delaying recovery of the funds. ICWA recorded an overpayment of less than $10,000 following an early change to a leave agreement. As of 17 July 2023, the overpayment is still outstanding and has been referred to an external debt collection agency that has organised a repayment plan.

All GTEs have an obligation under the *Financial Management Act 2006* to account for public money. Failure to collect all outstanding debt or make repayment arrangements before staff leave increases the risk of financial loss. Entities can minimise this risk of financial loss by reviewing the final termination payment and ensuring all financial assets are returned on the last day of employment. Entities also need to make payment arrangements that comply with section 17D of the *Minimum Conditions of Employment Act 1993* which does not allow employers to withhold money from employees without their consent.

Policy and procedure documents help guide and direct entity staff. They provide a structure for consistency and ensure compliance with regulations and standards. Having incomplete policy and procedure documents makes it hard for entities to align practice with their strategic values and comply with regulations and standards.

Risk assessments are not used systematically to manage differing levels of risk posed by staff leaving high integrity positions

Although all four entities have procedures in place to manage the staff exit process, entities are not formally assessing and documenting the risks created by the circumstances of their exit or their access to sensitive information or critical infrastructure. However, we found that all entities removed access to premises and information systems within 24 hours of the exit date when staff had been terminated for disciplinary or other adverse reasons.

We found one entity completed a risk assessment for a high integrity role. Actions were taken to limit the entity's exposure to risk, such as removal of access and review of the final termination payment, but these did not fully align with all the risks identified. Access to premises was not removed or limited when it was no longer necessary for the employee to attend the premises. We found that this was the only risk assessment conducted in our sample and was not routine.

Risks are most effectively identified and managed with a systematic approach to assessing them. Risk assessments assist entities to identify security implications and tailor approaches to minimise risks to information, assets and finances. An understanding of the risks and having documented procedures to mitigate them allows adjustments of controls to be made in the staff exit process to match the circumstances. For example, controls may need to be adjusted to manage risks or security concerns of staff:

- who are in high integrity positions
- who have access to confidential information
- whose employment contract is terminated due to adverse reasons
- who are subject to a code of conduct investigation.

Recommendations

1. All entities should:
   a. review policies and procedures for employee terminations
   b. review staff exits periodically to ensure compliance with policies and procedures.

   Implementation timeframe: February 2024

   Synergy response:

   Supported.

   DevelopmentWA response:

   Supported.

   ICWA response:

   Supported.

   Pilbara Ports response:

   Supported.

2. To better manage risks posed by different positions and circumstance of exit, all entities should:
   a. evaluate risk posed by different positions and termination types
   b. develop and document procedures to manage the risks effectively and efficiently
   c. communicate the process to key staff in the relevant business functions or areas.

   Implementation timeframe: January 2024

   Synergy response:

   Supported.

   DevelopmentWA response:

   Supported.

   ICWA response:

   Supported.

   Pilbara Ports response:

   Supported.

3. To minimise the risk of property and information loss entities should:
   a. ensure access to IT systems is removed or disabled within 24 hours of the exit date
   b. ensure all assets are returned on the day of exit
   c. clearly record when the return of assets occurred.

   Implementation timeframe: December 2023

Synergy response:

Supported.

DevelopmentWA response:

Supported.

ICWA response:

Supported.

Pilbara Ports response:

Supported.

4. All entities should consider:
   a. offering interviews to all exiting staff
   b. offering surveys to contractors.

Implementation timeframe: December 2023

Synergy response:

Supported.

DevelopmentWA response:

Supported.

ICWA response:

Supported.

Pilbara Ports response:

Supported.

The full response to each recommendation from the four entities is at Appendix 2.

Response from Electricity Generation and Retail Corporation (trading as Synergy)

Synergy thanks the OAG for the review and welcomes the findings and recommendations contained in the report. It is pleasing that the report acknowledges that staff exit processes are generally effective and efficient. Synergy is fully committed to implementing recommendations that will strengthen controls over the exit process and will ensure these are completed within the relevant timeframes.

Response from DevelopmentWA

DevelopmentWA recognises the significant importance of an effective staff exit process and implementation of controls to minimise security, asset and financial risks. As such DevelopmentWA values the Auditor General's assessment, particularly highlighting the positive outcomes achieved through its staff exit procedures.

In response to the audit's findings, DevelopmentWA is committed to implementing the recommendations to enhance its staff exit procedures and policies. Notably, DevelopmentWA's practice of revoking information systems and facility access for departing personnel once it becomes unnecessary has been acknowledged.

DevelopmentWA values the efficient execution of its current exit interview procedure and the subsequent utilisation of the feedback to proactively guide improvements in employee recruitment and retention strategies. The organisation remains dedicated to refining its processes and ensuring a seamless and beneficial transition for its staff members.

Response from Insurance Commission of Western Australia

The Insurance Commission acknowledges the findings of this performance audit. The Insurance Commission considers that implementation of the findings will further reduce the risks associated with employees and independent contractors who exit the organisation.

Improvements have been made to our processes since the audit and we are currently testing an automated separation application to enhance our processes and provide improved guidance to employees and managers on the exit process.

Response from Pilbara Ports Authority

Pilbara Ports Authority (PPA) thanks the Office of the Auditor General (OAG) for its thoroughness and consideration of all elements of practice associated with staff exit controls. The discussions what constitutes better practice and the place of guides (versus requirements) within PPA and the OAG was of particular interest, and provoked consideration of changes that will benefit PPA’s exit controls.

Audit focus and scope

The audit assessed whether four entities (Electricity Generation and Retail Corporation (trading as Synergy), DevelopmentWA, Insurance Commission of WA and Pilbara Ports Authority) effectively and efficiently manage the exit of staff from their organisations to minimise security, asset and financial risks. Our key questions were:

- Do entities have appropriate policies and procedures to effectively manage staff exits?
- Do entities comply with policies and procedures?

The audit covered the period 1 March 2022 to 28 February 2023.

In conducting the audit, we:

- reviewed policies and procedures and records for staff exits at the entities
- reviewed OAG financial audit and information systems audit management letters from 2020-21 to 2021-22 financial year
- interviewed key staff responsible for staff exits at the four entities (facilities management, finance, HR, payroll and IT services)
- selected a sample of 30 staff from Synergy, 28 from DevelopmentWA, 28 from ICWA and 27 from Pilbara Ports Authority (including contractors) that had left between 1 March 2022 and 28 February 2023. For each we sought evidence that:
    - termination checklists had been completed before or on the staff exit date and signed by the relevant authority
    - building access cards had been de-activated and/or keys had been collected prior to staff leaving
    - assets issued to staff (computers, tablets, mobile phones, vehicles, housing) were returned
    - credit cards were returned and cancelled, with no transactions occurring after this date
    - access to the entity's IT systems was revoked within 24 hours of their departure
    - an exit interview was offered or conducted
    - final payments reviewed and money owed to the entity was identified and paid at the time of leaving
    - risks posed by departing staff and circumstances of their exit were assessed.

We did not assess termination decisions and whether they complied with the relevant legislation.

This was an independent performance audit, conducted under section 18 of the *Auditor General Act 2006*, in accordance with Australian Standard on Assurance Engagements ASAE 3500 *Performance Engagements*. We complied with the independence and other ethical requirements related to assurance engagements. Performance audits focus primarily on the effective management and operations of entity programs and activities. The approximate cost of undertaking the audit and reporting was $277,000.

Appendix 1: Better Practice Guide

Key requirements	
Assess and mitigate risks posed by exiting staff	Entities should assess the security implication and other risks posed by the exiting staff member. Exiting staff can include those leaving voluntarily or terminated for misconduct or other adverse reasons. Below is a checklist of actions to be considered in a risk assessment: • assigning a risk level by considering the reason for leaving (resignation, retirement, termination for corruption or misconduct) • reducing level of access to IT systems • limiting access to entity premises • monitoring accrued leave balance to reduce overpayments • identifying assigned assets (vehicles, mobile phones, laptops etc.) and assess need for immediate collection • removing access to confidential or secret information • consider position within the entity and level of delegated authority over staff • existing financial delegations and purchasing card limit • existing conflicts with staff.
Collect all entity owned property	Entities should maintain an updated register of all assets issued to staff when they start and during their employment with the entity. Using information on the register ensures that all entity owned property is returned when staff leave. These include but not limited to: • identification badges and name tags • office, cabinet and safe keys • access security passes and swipe cards • computer and other IT equipment - laptops, tablets, storage devices, headsets, mouse and keyboards • mobile phone and charger • vehicle keys, fuel cards and logbooks • cab charges. Where access security passes and keys are not returned entities should take immediate action to cancel access cards, reprogram or change locks.

Key requirements	
Cancel all access to premises and IT systems	Entities should ensure that exiting staff have their access to entity premises and information systems withdrawn or cancelled immediately when staff leave. These include but not limited to: • building (including carpark) access • computer login and network access • changing passwords or access to shared or high privileged accounts • email address • voicemail • remote access • corporate memberships • customer accounts with external organisations. Where physical exit date and formal termination date differ, risks should be mitigated by removing access on the physical exit date.
Issue reminder of ongoing obligations	Entities should ensure that all exiting staff especially those with access to sensitive or classified information are advised and acknowledge their obligation not to disclose entity information. This helps safeguard entity assets and limit potential for the integrity, availability and confidentiality of sensitive information to be compromised.
Offer exit interview	Entities should offer staff exiting the option of an exit interview. This can be in form of a structured discussion or survey to gauge their perception of working in the entity. Entities should also collate the data, report internally and where relevant act on the findings. Information from exit interviews can help entities assess organisational strengths and vulnerabilities and target workforce management strategies to drive attraction, retention and performance.
Prevent overpayments and recover debt owed	Entities should ensure that they meet their responsibility to recover overpayments and rectify underpayments, while considering the needs and special circumstances of employees. Timely review of payroll information will reduce the likelihood of errors. Overpayments can also be prevented by checking employee leave balances before approval and avoiding late changes to booked leave or working arrangements where possible. Where overpayments occur entities need to make timely payment arrangements in line with section 17D of the *Minimum Conditions of Employment Act 1993*.
Regularly monitor and review staff exit processes	Entities should periodically review staff exits to ensure that they comply with: • entity policies and procedures • better practice.

Source: OAG, using policies from the Australian Government Protective Security Policy Framework[4]

[4] Department of Home Affairs, *Protective Security Policy Framework*, protectivesecurity.gov.au, n.d., accessed 8 August 2023.

Appendix 2: Specific responses to recommendations from audited entities

1. All entities should:
    a. review policies and procedures for employee terminations
    b. review staff exits periodically to ensure compliance with policies and procedures.

    Synergy response:

    a. Synergy reviews and updates all policies and procedures on a regular basis. Revisions made to exit procedures as a result of this audit will be incorporated into the relevant policies and procedures within the prescribed timeframe.

    b. Additional system workflows are being considered to centralise oversight over exit processes and allow for additional monitoring by HR. In addition, review of the staff exit process is within the scope of the Synergy internal audit programme and is subject to periodic review.

    DevelopmentWA response:

    Accepted. DevelopmentWA is committed to reviewing policies and procedures as significant HR policies and procedures are updated annually. This recommendation is accepted and a review of the policies and procedures will be undertaken within the recommended implementation timeframe proposed, namely February 2024. DevelopmentWA is also committed to periodically reviewing staff exits in line with the policies and procedures.

    ICWA response:

    Agreed. The Insurance Commission has commenced a review of all policies and procedures for employee terminations. Policies will clearly specify that access to IT systems is to be removed or disabled within 24 hours of exit date. Staff exits will be periodically reviewed by the Head of Human Resources to ensure compliance with policies and procedures.

    Pilbara Ports response:

    a. In line with PPA's Quality Management System, reviews of controlled documents are undertaken as part of a continuous improvement cycle. Where the OAG have identified improvements that can be made, PPA will review policies and procedures.

    b. PPA has processes to ensure employee and contractor exits are completed in accordance with PPA controlled documents. The OAG has made recommendations to improve interactions between PPA's controlled forms and checklists designed to assist employees carry out their duties that will be implemented.

2. To better manage risks posed by different positions and circumstance of exit, all entities should:
    a. evaluate risk posed by different positions and termination types
    b. develop and document procedures to manage the risks effectively and efficiently
    c. communicate the process to key staff in the relevant business functions or areas.

    Synergy response:

    The risks associated with different position types/circumstances are considered informally by Synergy and reflected in the exit process. Synergy will formalise this

process and ensure it is documented, incorporated into policies & procedures, and communicated to relevant stakeholders.

DevelopmentWA response:

Accepted. DevelopmentWA agrees with the recommendation and proposed time frame. For staff exiting for disciplinary reasons and for those where risks are identified, DevelopmentWA proactively manages exit procedure restricting access, as relevant, during the process. It is accepted to better manage risks posed by different positions and circumstance of exit through:

a. identification of positions and termination types that pose significant risk; and

b. develop and document procedures to manage the risks and communicate those to relevant staff in the relevant business units.

ICWA response:

Agreed. The Insurance Commission acknowledges the risk involved with separations will vary on a case by case basis. The Insurance Commission will update its procedures to reflect the management of the risks posed by different positions and termination types. The updated procedure will communicated to managers and supervisors.

Pilbara Ports response:

a. PPA considers risks associated with each termination in the context of the employee. Where a termination is required because of poor behaviour, or there is a potential risk associated with information breaches, PPA acts proportionately. Documentation of risk considerations will be added to PPA's termination checklist.

b. PPA has procedures in place that identify risks associated with disciplinary investigations and requires that physical and electronic access is removed, and PPA equipment returned as appropriate whilst an investigation takes place. As per R2(a) above, the termination checklist will be updated to document these elements.

c. Agreed.

3. To minimise the risk of property and information loss entities should:

   a. ensure access to IT systems is removed or disabled within 24 hours of the exit date

   b. ensure all assets are returned on the day of exit

   c. clearly record when the return of assets occurred.

Synergy response:

Synergy generally has effective controls in place regarding the termination of employees. Consideration is being given to additional system workflow steps that will enforce completion of the exit process by managers (including extending the workflow process to contractors). Enhanced reporting will also provide HR greater visibility where exit processes remain outstanding. Controls will also be established to initiate exit processes for contractors who leave Synergy prior to their originally agreed date.

DevelopmentWA response:

As evidenced by this audit, the practices recommended are already integrated into our existing procedures at DevelopmentWA. The prompt revocation of access and the retrieval of assets within 24 hours are actions we consistently undertake. Additionally, we have recently introduced and operationalised an asset return reporting process, providing a transparent and traceable history of asset returns.

ICWA response:

Agreed. The Insurance Commission will review its processes governing the removal or disabling of network access to ensure action is completed within 24 hours of separation date. Managers/Supervisors will be reminded of the importance of ensuring that all assets are returned on the employee or independent contractors last day. This will be enhanced by the planned use of automated workflow for separations including scheduled email notifications. Dates assets are returned will continue to be recorded in the Ascender HR System.

Pilbara Ports response:

a. Agreed.

b. PPA provides housing and vehicles to some employees, in remote locations. PPA makes arrangements for assets to be returned. However, this may not coincide with the day of exit. The return of assets post termination is monitored closely and PPA has never lost any asset through this process.

c. Based on the report findings, PPA fully meets this recommendation, and it is agreed this will continue.

4. All entities should consider:

   a. offering interviews to all exiting staff

   b. offering surveys to contractors.

Synergy response:

Synergy already offers exit interviews to employees and analyses the feedback provided. Synergy will consider extending exit interviews/surveys to selected contractor positions and incorporating this step into the system workflow.

DevelopmentWA response:

Following our current policy and established procedure, we extend exit surveys/interviews to all departing employees and contractors who have been with us for more than three months, when relevant. Consequently, we consider this recommendation to already be an integral part of our process. At DevelopmentWA, we actively leverage the insights and trends gathered from these surveys and interviews to drive enhancements within the workplace.

ICWA response:

Agreed. The Insurance Commission will promote the benefits to managers/supervisors on offering exit interviews to all employees who cease employment. The Insurance Commission does not engage a large number of independent contractors and will consider offering exit surveys within that context.

Pilbara Ports response:

a. PPA offers staff exit surveys to all employees voluntarily exiting the business. Which is undertaken by an independent 3rd party, unless the employee prefers an internal interview.

b. As noted in the report, PPA is not highly reliant on contractors and plans with the contracted entities for feedback. It is not intended to offer individual exit surveys to contractors.

Auditor General's 2023-24 reports

Number	Title	Date tabled
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