Western Australian
Auditor General's Report

Staff Exit Controls

Report 3: 2021-22
5 August 2021

Office of the Auditor General
Western Australia

Audit team:
Jason Beeley
Issihaka Toure
Joel Mendelson
Rachael Wilkins

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.

WESTERN AUSTRALIAN AUDITOR GENERAL'S REPORT

Staff Exit Controls

Report 3: 2021-22
August 2021

THE PRESIDENT
LEGISLATIVE COUNCIL

THE SPEAKER
LEGISLATIVE ASSEMBLY

STAFF EXIT CONTROLS

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 if the Department of Planning, Lands and Heritage; the Department of Finance and the Department of Local Government, Sport and Cultural Industries 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
5 August 2021

Contents

Auditor General's overview

Entities need to have controls in place to make sure that when a member of staff leaves their job their access to buildings and information systems is cancelled and all assets that have been issued to them are returned. If these controls are absent or ineffective, entities increase the risk of unauthorised access to buildings and information, and the risk of losing sensitive information and public assets and money.

My financial and information systems audits in previous years have raised concerns over former employees having systems access after they leave an entity, and the failure to complete staff exit checklists. This report, based on a more in-depth review of 3 state entities, confirms those findings and identifies issues around asset return and physical access. It again highlights how critical effective exit controls are.

Having effective controls is not, however, straightforward. One of the reasons that entities can struggle with staff exit controls is that they are a shared responsibility across areas of entity operations that may not always work closely together. The controls also need to operate across multiple systems that may not be linked. To deliver prompt action there needs to be a shared understanding of the risks, and good coordination between the different divisions within the entity.

The risks and challenges identified in my report are not confined to the 3 entities we audited. I urge all state and local government entities to look at the findings and recommendations from this report, and draw on the better practice guidance provided in Appendix 1, to ensure that they have effective staff exit controls in place.

Introduction

This audit assessed if the Department of Planning, Lands and Heritage; the Department of Finance and the Department of Local Government, Sport and Cultural Industries effectively and efficiently manage the exit of staff to minimise security, asset and financial risks.

Our 2015 audit on *Controls Over Employee Termination* found that entities were not following their approved staff exit requirements. More recent financial and information systems audits from this office have also highlighted similar issues. This audit builds on this work.

Background

In December 2020, there were over 148,500 people employed in the Western Australian State sector to deliver a diverse range of government services and programs. Public sector employees (including contractors and consultants) generally have access to confidential information and use a range of public resources to carry out their daily duties. These include credit cards, cars, computers, mobile phones, laptops and tablets.

At the 3 audited entities, 957 people including third party contractors ceased their employment in the 18 month period to December 2020 (Table 1).

Entity	Employees	Contractors	Total exits	Selected sample
Department of Finance (DoF)	180	50	230	26
Department of Local Government, Sport and Cultural Industries (DLGSC)	429	36	465	30
Department of Planning, Lands and Heritage (DPLH)	148	114	262	27
Total	**757**	**200**	**957**	**83**

Source: OAG using audited entity information

Table 1: Number of staff exits at the audited entities

When staff leave an entity through dismissal, resignation, retirement, end of contract or permanent transfer to another public sector entity, entities should:

- immediately cancel access to information systems, premises and confidential information
- revoke all physical controls such as ID cards, security access passes (fobs or cards) and keys
- collect all entity owned property
- issue a reminder of the individual's ongoing obligations not to disclose entity information
- offer exit interviews.

Entities should also assess the relative security implications and other risks posed by staff members who leave voluntarily or are terminated for misconduct or other adverse reasons (Appendix 1: Staff exit better practice guidance).

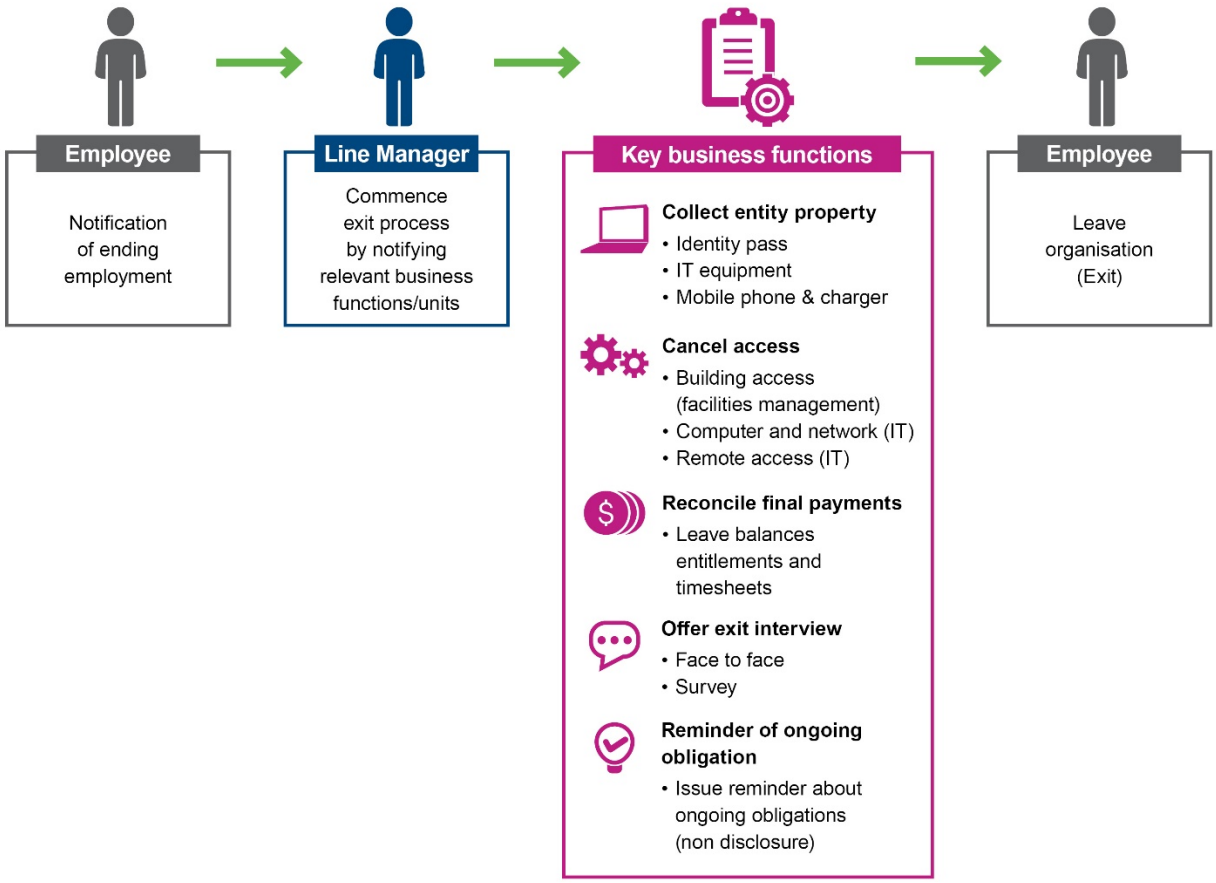
The Commonwealth Government established the *Protective Security Policy Framework* to assist Commonwealth entities to protect people, information and assets. It underpins the Commonwealth Government's security policy and aims to ensure the secure delivery of government business. The framework is not mandatory for state and territory government

entities, but is considered better practice. It supports entities to implement policies across security governance and its principles reflect key aspects of minimising security risks that can come with staff exits:

- information security – maintaining the confidentiality, integrity and availability of all official information
- physical security – providing a safe and secure physical environment for people, information and assets
- personnel security – ensuring continued protection of resources after staff leave the entity.

The *Digital Security Policy* issued by the WA Office of Digital Government provides a checklist of controls that entities should apply. It includes making clear the enduring requirement on 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.

At our sampled entities the staff exit process is a shared responsibility across multiple business areas and positions (Figure 1). Consequently, good staff exit processes require areas to work together to ensure responsibilities are actioned effectively and promptly. Failure to do this presents significant risks to the entity of a security breach, asset or financial loss.



Source: OAG using entity and Australian Public Service Commission information

Figure 1: Staff exit process

Conclusion

To varying degrees, the entities were not effectively or efficiently managing the exit of staff to minimise security, asset and financial risks. Although the Department of Finance managed its staff exits better than the other 2 entities, none of the 3 entities consistently met all the key criteria of an effective and efficient staff exit management process.

Physical and information security risks were not minimised because access to entity premises was not consistently cancelled immediately, or in some cases at all, when staff left. The cancellation of IT access at all 3 entities was also not timely.

Entities were not effectively or efficiently managing asset returns or recovery of salary overpayments. Two entities could not demonstrate that all assets were returned or accounted for when staff left because they did not keep adequate records of what assets were provided and what was returned. Not all salary overpayments or debt owed by exiting staff were settled at the time of leaving and in some cases, entities had no arrangements to recover the money. Across the 3 entities, 20 staff that had left still owed around $53,500.

The exit controls at the entities were not risk based to take account of high integrity positions and the circumstances in which staff leave. At all entities there were missed opportunities for identifying areas of improvement because they were not consistently offering or conducting exit interviews. Exit interviews or surveys can help entities assess organisational strengths and vulnerabilities with the aim to improve staff attraction, retention and performance.

Findings

Access to work premises and IT systems were not cancelled immediately when staff left

At all 3 entities access to premises and IT systems were not cancelled within 24 hours of staff leaving or, in some cases, at all. This means that government entities that are entrusted with significant resources and highly sensitive and confidential information, are not minimising the risk of:

- information and physical assets being made inoperable, lost or used without appropriate authorisation
- damage to the building
- compromised personal security.

Two of the entities could not demonstrate that all security access passes were returned or deactivated immediately or, in some cases, at all

We tested a sample of 57 people that had left the DPLH and DLGSC. The entities lacked adequate information to show that access passes had been returned or deactivated when 41 out of 57 (72%) staff left.

For 19 out of our sample of 27 people (70%) who left DPLH there was insufficient evidence to confirm that access passes were returned or disabled. The entity advised us that they had not previously tracked when passes were reallocated, deactivated or cancelled but a new process had been implemented in May 2021 in response to our audit.

At DLGSC, similar issues were evident. For 22 out of 30 (73%) people, there was insufficient evidence to verify that access passes were returned or disabled when staff left.

We were advised by staff at both entities that there was a disincentive to cancel or deactivate passes because they incurred a $12 fee for any changes to the status of passes from the private operator that managed the building.

At DoF all access passes were cancelled or deactivated after staff left the entity. However, for 5 out of 26 (19%) the cancellation of passes was not timely. For 4 people it took between 6 and 44 days. In another case it took 116 days to cancel the card after the person had left. The entity advised that this case related to a secondment arrangement where the former employee continued undertaking work on behalf of the entity following the end of their secondment.

Failure to reclaim, deactivate or cancel security passes when staff leave increases security risk to assets, information and people through unauthorised physical access.

DLGSC and DPLH could not account for all active security passes with 24/7 access to key floors

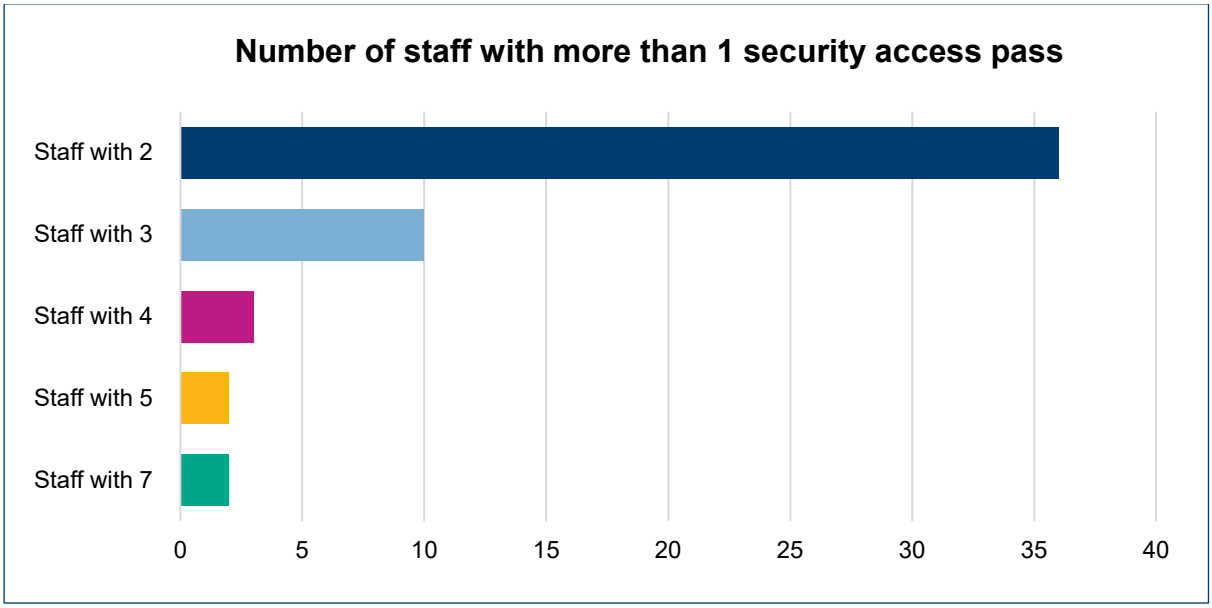
Our review of records of all access passes issued by DLGSC at 1 of its premises showed that there were 320 unallocated but active security access passes with 24 hour access to all floors of the building. This contravened the entity's own access control procedures. On 4 June 2021, the entity advised that an audit of all security access passes had been completed and all unauthorised or unallocated passes had been deactivated.

The DPLH and its contracted building access control firm did an audit in 2019 and found 205 active passes where cardholders could not be identified. At the time of this audit we found that for 164 passes there was insufficient evidence to demonstrate that these had been

deactivated or the cardholders identified. This increased the risk of these passes being used to access the premises without authorisation or knowledge of the entity.

DLGSC had current staff with multiple security passes even though it is prohibited under their policy

We found 17 staff still employed by the entity who each held between 3 and 7 active access passes to the same premises. An additional 36 people had 2 active passes each (Figure 2). Under the entity's *Key control guideline*, the keeping of spare keys and activated access passes is prohibited.



Source: OAG analysis using the DLGSC information

Figure 2: Number of current staff at DLGSC with more than 1 security access card

All entities cancelled exiting staff's IT system access, but not always immediately

Cancellation of exiting staff's IT system access at all 3 entities was not timely. It took between 2 and 161 days to deactivate or withdraw access to information systems after staff left the entity. This increases the risk of unauthorised access and can compromise the confidentiality, integrity and availability of the entities' information.

At DoF, it took between 6 and 161 days to cancel access to IT systems after the last day of employment. The entity advised that the case that took 161 days related to a secondment arrangement where the former employee continued undertaking work on behalf of the entity. Without that case it took the entity on average 7 days to cancel IT systems access. For 10 (38%) of the people in our sample, there was insufficient information to determine when their access was cancelled. DoF's security management framework notes that IT access for terminated staff is to be disabled on the last day of employment. In some cases, this may mean people continue to have access while clearing their remaining leave when they should have no need to access systems. This increases the risk of unauthorised access and weakens controls over inappropriate use. The entity advised that employees have genuine need to access systems such as HR self-service, email and other web systems while they remain formally employed.

DPLH confirmed that they did not routinely record specific dates when IT access is cancelled. Based on system log information where it was available, late cancellations ranged between 1 and 124 days after the individual had left. For 10 of our sample, there was no information to determine when access was cancelled.

At DLGSC there was insufficient information to determine when access to IT systems was cancelled for all 30 people in our sample. System logs showing the dates of when this occurred were not recorded. In the absence of this information, we checked whether any of the individuals had accessed the IT systems and found that 29 did not access the system after they left. One person had accessed the system 4 days after their exit date.

Concerns over ongoing systems access at the audited entities has been consistently raised in our financial and information systems audits for the last 6 years (2013-14 to 2019-2020).

None of the entities systematically remind all exiting staff of their obligation not to disclose information or access systems upon exit

At both DLGSC and DoF there was no evidence that 56 people in our sample had been reminded of their obligation not to disclose confidential information when they left.

At DPLH only 2 people out of 27 had been reminded of and acknowledged their obligation not to disclose confidential entity information or make any unauthorised disclosure after leaving. For the other 25 in our sample we found no evidence that this had occurred. The entity's policy requires employees not to disclose confidential entity information or make unauthorised disclosures after leaving.

All 3 entities have access to information that is not in the public domain and can be highly sensitive and confidential. The entities have obligations to manage how and when the information is released. Failure to remind exiting staff of their obligations not to disclose entity information increases the risk of its misuse.

Entities were not effectively managing asset returns or recovering salary overpayments prior to staff exit

Entities could not demonstrate that all assets were returned because they did not keep accurate records of what was provided to staff

None of the audited entities had a complete and easily accessible record of all assets, including ergonomic and IT equipment, provided to staff at the start and throughout their employment. Without sound information on assets that are issued to staff, entities cannot verify with certainty that all entity owned assets are returned when staff leave.

At DPLH, we could not verify whether all IT assets had been returned because there were insufficient records of what was issued to the 27 people in our sample:

- 15 staff had left with no evidence of laptop return or what was issued
- the entity advised that 6 people were not issued with IT equipment
- 6 had some information of laptop return.

The entity advised that the system overrides the history of ownership when the asset is re-issued and are confident that no assets had been taken from the entity when staff left.

Mobile phones were also inconsistently captured on the entity's asset management system or register of attractive assets. Without evidence of what mobile phones were issued, their return could not be verified. Only 2 of the 27 people in our sample at DPLH were known to have had a phone issued. Information provided at the time of the audit showed that only 1 had been returned.

At DLGSC records of only 6 exited staff in our sample of 30 had some evidence that laptops had been returned or re-issued. We were advised that historical information for the majority of laptops in our sample was not available. In the absence of this information or any other records we could not determine whether these were returned.

We note that at DPLH and DLGSC, accessories such as computer mouses, chargers and laptop bags are not captured increasing the risk that these are not returned when staff leave.

While employees are generally provided with computers and mobile phones for work, some positions are responsible for other valuable items. For example, at DLGSC camp managers have custody of items such as kayaks, canoes, electric bikes and portable radios. Entities should ensure that such items are adequately accounted for when staff leave. None of the individuals in our sample had such items.

DoF demonstrated that 19 of 26 staff in our selected sample returned their IT equipment. However, 7 did not have adequate documentation of asset return. The entity attributed this to previously having 2 different asset management processes. They advised that since February 2021, the administration of all hardware assets and mobile equipment was centralised within the Procurement and Asset team.

Lack of sound information increases the risk of asset loss. This may also increase the risk of sensitive information being compromised especially if access to systems is not terminated.

All entities identify overpayments to exiting staff but do not always implement strategies to recoup the payments in a timely manner

In some cases, staff may receive a salary overpayment, such as where salary is continued to be paid when staff are on leave but they have no leave entitlements. We found that in a number of cases the overpayments were not repaid before the person left the entity and that repayment plans were not always in place.

At 31 December 2020:

- At DoF 6 staff had left who had not fully repaid overpayments, leaving a total of $19,680 still owing. Two of the staff still owed a total of $3,735 but did not have a payment plan.
- At DPLH 13 staff had left with outstanding overpayments totalling $19,308. Six of them (accounting for $17,835) had repayment plans in place, but 7 ($1,473) did not. The DPLH's policy requires that any outstanding debt is settled before staff leave the entity.
- At DLGSC 3 staff who had received overpayments had left. Two had made full repayments but 1 person had $14,542 outstanding debt with no arrangements for repayment at the time the information was provided to us. The entity advised that they are in the process of undertaking a full audit and quality assurance check on the reported overpayment. Following this, DLGSC will commence the recoup and recovery of overpayment.

Causes of overpayments at all 3 entities included:

- late notification of termination
- incorrect higher duties allowance
- late notice of unpaid leave
- error on payment of leave entitlements.

All State government entities 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 need to make payment arrangements whilst still complying with section 17D of the *Minimum Conditions of Employment Act 1993* that does not allow employers to withhold money from employees without their consent.

In a few cases procedures requiring a second person to check the accuracy of payments calculations to exiting staff were not followed

At DPLH records of human resources' calculations of final payments were available for the staff who had exited. However, for 5 in our sample of 27 they had not been checked by a second person. One was a fixed term contract employee and the other 4 were secondments. At DLGSC 3 cases in our sample of 30 were not reviewed by a second person. These were all before the entity established a formal quality assurance function in October 2019.

Failure to cross check calculations increases the risk of over or under payments due to calculation errors.

Controls for managing staff exits were not adjusted for risks posed by position and termination type

Entities do not evaluate risk posed by individual positions or the reason people leave

Although all 3 entities have procedures in place to manage staff exits, none assessed or evaluated risks posed by individual positions and the circumstance in which people left. Risk assessments can help entities identify security implications and use different approaches to adequately minimise risks to information and assets.

Not all positions and circumstances by which people leave an entity are the same. So, an entity's understanding of the risks and having sound processes is vital to allow for prompt adjustment of controls when needed. For example, controls may need to be adjusted to manage risks or security concerns for staff:

- whose employment or contract is terminated for adverse reasons
- who are subject to a code of conduct investigation, whether completed or not
- who have outstanding security issues, including any risks or issues identified through a risk assessment
- in positions of increased trust and access e.g. IT and senior positions.

Risks of information loss and other adverse impacts to the entity are increased when staff have access to sensitive or classified information or administrative rights to the entity's information systems.

Communication between business areas responsible for managing staff exits could be improved

At all entities, communication between the different functions, to verify that relevant tasks had been completed, could be improved to enhance timeliness and effectiveness of the staff exit process. Although managers are responsible for initiating the exit process, several business areas are involved and have different responsibilities for parts of the process. Consequently, clear and prompt communication is vital to ensure that risks are adequately mitigated. This is critical when, for instance, staff with access to privileged information are terminated for adverse reasons.

The relevant business functions included payroll, IT services/ help desk and facilities management.

The majority of exit checklists or forms used to ensure all staff exit requirements are met were not completed on time

Entities use an employee exit checklist or form as the main control to help relevant staff make sure that all steps are followed when an employee is terminated. However, none of the entities completed these promptly.

At DPLH, checklists for 20 out of 27 exited staff (74%) were completed after the individual had left the entity. On average it took 90 days after the person had left to finalise the checklist. In 1 instance it took 268 days for an exit form to be completed after the staff member had left. The DLPH's policy requires managers and employees to complete the forms and all the relevant responsibilities as soon as practicable.

Exit forms at DPLH were not completed for 4 contractors employed under a common use agreement (CUA). We were advised that the process of completing termination checklists for CUA contractors at the entity commenced in June 2020. This was evident for the 2 CUA contractors in our sample who had an exit form completed after that date.

At DLGSC we found no evidence that checklists had been completed for 21 of the 30 people (70%) in our sample. For 4 people we were advised that this was not necessary as 3 were still employed as casual and 1 was still working for the DLGSC but had moved roles. Nine (30%) people in our sample had completed checklists. Of these 2 had been completed late, 19 and 91 days after the termination date.

None of the contractors at DLGSC had a completed checklist on file. The entity requires that the employee checklist is actioned as soon as the employee has provided notice of termination or a decision has been made not to renew a contract.

At DoF just over half (14 of 26) of our sample had exit forms/checklists completed late. On average it took 23 days after the person left to finalise the checklist. For 9 people we could not determine when checklists were completed because the entity's system does not maintain an audit trail of the logs/records when the electronic service tickets are closed. For 1 person it took 169 days to complete their checklist.

Long timeframes to complete checklists increase access and security risks to the entity's IT system, information, property and premises, and over/under payments of staff. A checklist or form generally includes the requirement to return all entity property from the exiting employee and removal of physical and system access. Consequently, it is vital that these are completed and verified by all responsible parties in a timely way when staff leave.

Failure to complete termination checklists in a timely manner or at all has been consistently raised with the audited entities in our financial and information systems audits since at least 2015-16.

Entities were not consistently offering or conducting exit interviews to identify problems and areas for improvement

Only 1 of the 27 DPLH staff exits we looked at was offered an exit interview. Although the entity's policy requires that staff leaving are invited to participate in a voluntary exit interview, we were advised that these were not generally conducted. In the 1 instance where this had occurred, it was to manage a dispute regarding roles and responsibilities that arose during a secondment and not standard practice. The entity advised it has now introduced an exit survey for all employees leaving the entity to fill in.

At DLGSC only 5 staff of the 30 that we sampled had been asked to complete an exit survey. One declined, 2 accepted the offer and for the remaining 2 individuals there was no information on whether they declined or completed the survey.

Information from exit interviews and surveys can help entities to assess organisational strengths and vulnerabilities, and target workforce management strategies to drive talent attraction, retention and performance. Consequently, failure to consistently offer or conduct exit interviews presents a missed opportunity for the entity's business improvement.

Only DoF collates information from exit survey responses and reports key themes to its corporate executive on an annual basis

DoF offers exit surveys to staff but for 12 of 26 people (46%) in our sample, the entity did not offer an exit survey. We note that participation in the exit interview process is voluntary. However, failure to encourage departing staff to participate means that there are missed opportunities to improve management strategies to drive talent attraction, retention and performance.

DoF was the only audited entity that collated and reported the results of its exit surveys to management annually.

Case study 1: Use of exit interviews for business improvement

DoF gathers data from staff exit surveys to inform and identify issues relating to its staff retention strategies. In 2018, the entity identified that staff were leaving due to lack of career advancement and challenge. Using this insight, the entity introduced the Aspiring Leaders Pilot Program targeting level 3 to 6 staff as a retention strategy and development opportunity.

The entity's 2019 Exit Survey report was deferred due to the COVID-19 emergency in 2020 and was to be incorporated into the 2020 Exit Survey report which was in development at the time of the audit.

Recommendations

1. To minimise the risk of unauthorised access to premises when staff leave, DPLH and DLGSC should:

    a. maintain an accurate register of all access passes including returns, cancellation/deactivation

    b. conduct regular audits of all active passes held by staff

    c. immediately ensure that all unclaimed, duplicate or lost access passes are cancelled/ deactivated

    d. ensure all access passes are returned when staff leave.

    DPLH response: Accepted

    Implementation timeframe: by October 2021

    DLGSC response: Accepted

    Implementation timeframe: by October 2021

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

    a. ensure access to IT systems is removed or disabled immediately when staff leave

    b. clearly record when the removal of IT system access occurred

    c. maintain a register of all assets issued to staff at commencement, during employment and what is returned at exit

    d. ensure all assets are returned when staff leave

    e. maintain an audit trail of asset ownership.

    DPLH response: Accepted

    Implementation timeframe: by October 2021

    DLGSC response: Accepted

    Implementation timeframe: by October 2021

    DoF response: Accepted

    Implementation timeframe: by October 2021

3. To minimise the risk of financial loss from overpayments entities should ensure that overpayments are identified and repayment arrangements are determined before staff leave.

    DPLH response: Accepted

    Implementation timeframe: by October 2021

    DLGSC response: Accepted

    Implementation timeframe: by October 2021

    DoF response: Accepted

    Implementation timeframe: by October 2021

4. 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.

   DPLH response: Accepted

   Implementation timeframe: by January 2022

   DLGSC response: Accepted

   Implementation timeframe: by January 2022

   DoF response: Partially accepted

   Implementation timeframe: by January 2022

5. To improve communication between business functions responsible for staff exits all entities should ensure:

   a. each business area knows its roles and responsibilities in relation to exiting staff and the action they need to perform

   b. there is good communication and coordination around staff exits at the right time.

   DPLH response: Accepted

   Implementation timeframe: by October 2021

   DLGSC response: Accepted

   Implementation timeframe: by October 2021

   DoF response: Accepted

   Implementation timeframe: by October 2021

6. All entities should:

   a. offer interviews to all staff leaving

   b. collate, analyse and internally report exit interview themes/results.

   DPLH response: Accepted

   Implementation timeframe: by October 2021

   DLGSC response: Accepted

   Implementation timeframe: by October 2021

   DoF response: Accepted

   Implementation timeframe: by October 2021

Response from Department of Finance

The Department of Finance (Finance) acknowledges the findings of this audit and will implement recommendations where they will strengthen its staff exit processes. Finance is pleased with the Auditor General observation of the strengths in its staff exit processes, including the exit interview process. Finance actively uses the exit interview process to improve staff attraction and retention.

Appendix 2 includes Finance's specific responses to recommendations.

Response from Department of Local Government, Sport and Cultural Industries

The Department of Local Government Sport and Cultural Industries (DLGSC) are committed to minimising the risks associated with staff exiting the department. We welcome the findings to review and enhance our processes. DLGSC are pleased to report that we have made steady progress in the 18 months since the audit sample and continue to make improvements.

Appendix 2 includes DLGSC's full response.

Response from Department of Planning Lands and Heritage

The Department welcomes the findings and recommendations contained within this performance audit. A number of improvement activities were underway at the time of the audit and the Department is confident that it can achieve all the recommended actions in line with the timeframes committed. Whilst the Department did not previously maintain an audit history of ICT asset and access card allocations, the Department has undertaken audits to verify all assets and access cards have been accounted for.

Appendix 2 includes the Department's specific responses to recommendations.

Audit focus and scope

The audit assessed whether the Department of Planning, Lands and Heritage, the Department of Finance and the Department of Local Government, Sports and Cultural Industries effectively and efficiently manage the exit of staff to minimise security, asset and financial risks. Our key questions were:

a) Do entities minimise the risk of financial, information and asset loss by effectively implementing staff exit controls?

b) Do entities conduct and consider exit interviews as part of the staff exit process?

The audit covered the period 1 July 2019 to 31 December 2020.

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 2013-14 to 2019-20
- interviewed key staff at the 3 entities responsible for staff exits (facilities management, human resources, payroll and information technology services)
- selected a sample of 30 staff from DLGSC, 27 from DPLH and 26 from DoF (including consultants and third-party contractors) that had left between 1 July 2019 to 31 December 2020. For each we sought evidence for whether:
    - termination checklists had been completed before or on the staff exit date and signed by the relevant authority
    - building security access passes had been de-activated and/or keys had been collected prior to staff leaving
    - assets issued to staff (computers, mobile phones, vehicles) were returned
    - credit cards were returned and cancelled, with no transactions occurring after this date
    - access to the entity's IT systems was revoked prior to their departure
    - an exit interview was offered or conducted
    - exiting staff were reminded and acknowledged their obligation not to disclose sensitive information
    - final payments were 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 and controls modified accordingly.

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 $258,000.

Appendix 1: Better practice guidance

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. So, an assessment should include: • reason for leaving (resignation, retirement, transfer to another entity and termination for corruption or misconduct) • level of access to key IT systems and entity premises • access to confidential or secret information • position within the entity and level of delegated authority • financial delegations and purchasing card limit • assigned assets (vehicles, mobile phones, laptops etc.).
Collect all entity owned property	Entities should maintain an up-to-date register of all assets and property issued to staff from 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 are not limited to: • identification badges and name tags • office, cabinet and safe keys • access security passes, swipe cards • computer and other IT equipment - laptop, iPad, storage devices, wireless mouse and keyboards • mobile phone and charger • vehicles, keys, fuel cards and logbooks • cab charges. Where access passes and keys are not returned entities should take immediate action to cancel access passes, reprogram or change locks.
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. This includes: • building (including carpark) access • computer login and network access • access to third party systems that they only have as a result of their employment • email address • voicemail • remote access • corporate memberships.
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*.

Key requirements	
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 even after they leave. This helps safeguard entity resources and limit potential for the integrity, availability and confidentiality of sensitive information to be compromised.
Offer exit interview	Entities should offer exiting staff the option of an exit interview. This can be 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.
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 the Australian Public Service Commission Information[1] and Australian Government, Protective Security Policy Framework[2]

[1] Australian Public Service Commission- Example employee exit checklist https://legacy.apsc.gov.au/checklistexample-employee-exit-checklist

[2] The Protective Security Policy Framework https://www.protectivesecurity.gov.au/

Appendix 2: Responses from audited entities

Department of Local Government, Sport and Cultural Industries

The Department of Local Government Sport and Cultural Industries (DLGSC) are committed to minimising the risks associated with staff exiting the department. We welcome the findings to review and enhance our processes. DLGSC are pleased to report that we have made steady progress in the 18 months since the audit sample and continue to make improvements.

We have already implemented, or commenced implementing processes to address Recommendations 1, 2, 3.

An asset register has been implemented to ensure the allocation, movement and return of all access passes are recorded and auditable. The register is regularly reviewed.
A digital solution is planned to provide greater security and auditability of the process.

The Digital and Technology Service Desk solution has been upgraded to enable the recording and tracking of IT systems access.

To strengthen and improve procedures and rates of recovery of overpayments, Payroll are reviewing and updating DLGSC overpayment processes and undertaking an audit of the current register of overpayments.

More broadly, key business functions are working together to implement an automated offboarding solution, clearly documented processes and communication strategies. The approach will improve on progress already made against Recommendations 1,2 and 3 also address Recommendations 4,5 and 6.

The offboarding solution will provide further security, transparency and the ability to produce information more efficiently for reporting purposes and further audits.

We are committed to implementing the solution by the October 2021 timeframe.

Specific responses to recommendations from DPLH and DoF

1. To minimise the risk of unauthorised access to premises when staff leave, DPLH and DLGSC should:

    a. maintain an accurate register of all access passes including returns, cancellation/deactivation

    b. conduct regular audits of all active passes held by staff

    c. immediately ensure that all unclaimed, duplicate or lost access passes are cancelled/ deactivated

    d. ensure all access passes are returned when staff leave.

    DPLH response: Agree with the identified recommendations and the proposed timeframes.

    Work has commenced on the identified recommendations and plans are in place to formalise the processes:

    a. In May 2021 an access card management process was implemented which included the introduction and maintenance of a comprehensive tracking sheet to

manage all access card activity including new card issues, re-assigned cards, or cancellations (due to loss or damage, returns (dated)) and the responsible officer.

b. An audit of all access cards was completed in June 2021 including a reconciliation between the contracted building access control and internal records. Annual audits of cards will be carried out at the end of each financial year.

c. Access cards that are unaccounted for have been cancelled and the access card management processes have been updated to ensure unclaimed, duplicate or lost passes are cancelled and deactivated as soon as they are identified.

d. Where cessation forms have been completed for a departing officer, the returned access card identity number will be recorded on the form. The tracking sheets developed will record this action as described in a) above.

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

   a. ensure access to IT systems is removed or disabled immediately when staff leave

   b. clearly record when the removal of IT system access occurred

   c. maintain a register of all assets issued to staff at commencement, during employment and what is returned at exit

   d. ensure all assets are returned when staff leave

   e. maintain an audit trail of asset ownership.

DPLH response: Agree with the identified recommendations and the proposed timeframes.

Work has commenced on the identified recommendations and plans are in place to formalise the process to:

a. Automate the off-boarding task to ensure access to IT systems is removed or disabled immediately when staff or contractors leave.

b. The recording of the actual effective time of removing IT systems access.

c. Tracking of the assets lifecycle to manage assets issued to staff at commencement, during employment and what is returned at exit.

d. The tracking of the assets lifecycle will ensure the reconciliation of assets as they are returned when staff leave. Whilst the Department was unable to show a history of allocation for each individual asset, the Department can confirm that all assets are accounted for an no assets have been lost.

e. The asset lifecycle will enable an audit trail of asset ownership.

DoF response: Finance acknowledges the recommendation and will implement changes to strengthen processes to minimise the risk of property or information loss.

3. To minimise the risk of financial loss from over payments entities should

   a. ensure that overpayments are identified and repayment arrangements are determined before staff leave.

DPLH response: Agree with the identified recommendation and the proposed timeframe.

The Department will review its staff termination and overpayment processes to ensure overpayments are identified and repayment arrangements are determined before staff leave.

Reporting on overpayments to the corporate executive was introduced in March 2021, with these reports to be presented to the corporate executive on a regular basis.

DoF response: Finance acknowledges the recommendation and will seek to ensure overpayments are identified prior to cessation of employment and repayment plans are put in place.

4. 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.

DPLH response: Agree with the identified recommendations and the proposed timeframes.

The Department will review its cessation process to:

a. Identify positions and termination types that pose significant risks.

b. Develop and document procedures to manage the risk.

Communicate the procedures to key staff and include the procedures in the Department's Management Training Module.

DoF response: Finance acknowledges the risk involved in staff exits will vary depending on the circumstance. For staff exiting for disciplinary reasons, Finance proactively restricts access through the disciplinary process.

Finance considers its existing staff exit processes apply sufficient risk mitigation for all positions including high trust positions.

5. To improve communication between business functions responsible for staff exits all entities should ensure:

   a. each business area knows its roles and responsibilities in relation to exiting staff and the action they need to perform

   b. there is good communication and coordination around staff exits at the right time.

DPLH response: Agree with the identified recommendations and the proposed timeframes.

The Department's cessation form already generates notifications to the relevant line manager as each business function completes its allocated tasks.

Work on the identified recommendations has occurred and processes are being implemented to ensure:

a. Each business area knows its roles and responsibilities in relation to exiting staff and the action they need to perform, and

b. There is good communication and coordination around staff exits at the right time.

DoF response: The recommendation is acknowledged and Finance will remind business areas involved in the exit process of their responsibilities to ensure effective and timely exiting of staff.

6. All entities should:

   a. offer interviews to all staff leaving

   b. collate, analyse and internally report exit interview themes/results.

DPLH response: Agree with the identified recommendations and the proposed timeframes.

a. Exit interviews were introduced for all departing staff as standard practice in April 2021.

b. Analyse of exit interview data will be undertaken and included in the Business and Corporate Services' report to Corporate Executive on a quarterly basis from FY 2021-22.

DoF response: The recommendation is noted and Finance will explore options to maximise the offer of exit surveys for departing employees to assist its annual exit survey report findings.

Auditor General's 2021-22 reports

Number	Title	Date tabled
2	SafeWA – Application Audit	2 August 2021
1	Opinion on Ministerial Notification – FPC Arbitration Outcome	29 July 2021

Office of the Auditor General
Serving the Public Interest

Office of the Auditor General
Western Australia

7th Floor Albert Facey House
469 Wellington Street, Perth

Perth BC, PO Box 8489
PERTH WA 6849

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

@OAG_WA

Office of the Auditor General for
Western Australia