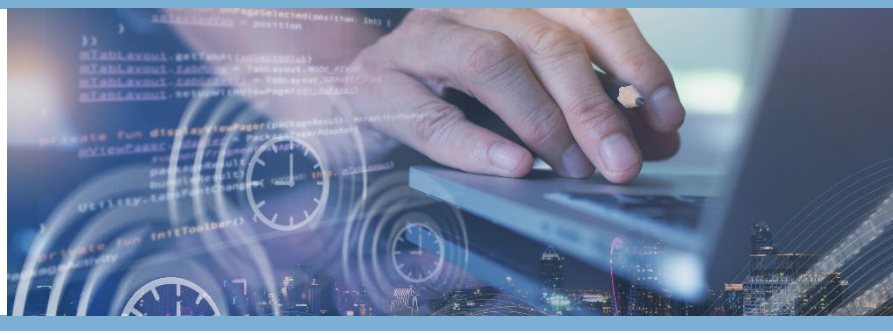
Western Australian
Auditor General's Report



Application Controls Audits 2021

Report 16: 2020-21
9 March 2021

Office of the Auditor General
Western Australia

Audit team:
Jordan Langford-Smith
Kamran Aslam
Paul Tilbrook
Fareed Bakhsh

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

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

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

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

WESTERN AUSTRALIAN AUDITOR GENERAL'S REPORT

Application Controls Audits 2021

Report 16: 2020-21
March 2021

THE PRESIDENT
LEGISLATIVE COUNCIL

THE SPEAKER
LEGISLATIVE ASSEMBLY

APPLICATION CONTROLS AUDITS 2021

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

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

I wish to acknowledge the entities' staff for their cooperation with these audits.

CAROLINE SPENCER
AUDITOR GENERAL
9 March 2021

Contents

Auditor General's overview

This report summarises the results of our audit of 4 entities' business applications during 2019-20. It contains important findings and recommendations to address common weaknesses that can potentially compromise sensitive and operational information held by entities.

The audit examined whether entities exercise effective controls to manage their applications and information. We identified control weaknesses across all 4 applications and reported 75 findings to the entities. Addressing these weaknesses is a key priority for these entities and it is pleasing to see that they have addressed, or are in the process of actively addressing, them.

Public sector entities rely on business applications to deliver a variety of important services to citizens. These applications range from custom built systems to off-the-shelf programs, hosted internally or in the cloud. Information processed by these applications can be used to enable key decisions and functions, including to support, enable or pay citizens, and it is therefore vital that the security and integrity of information is maintained.

Application controls need to be considered in conjunction with existing organisational processes and IT controls. A holistic approach towards governance, risk management and security is critical for secure and effective operations.

Public facing applications are prone to cyber threats. It is therefore essential to manage system vulnerabilities and other weaknesses that could expose entities to compromise. We found that all audited entities could improve their controls around user access, vulnerability management and situational awareness to address cyber risks.

Application controls audits

Introduction

Applications are software programs that facilitate an organisation's key business processes including finance, human resources, case management, licensing and billing. Applications also enable entities to perform important functions that are unique and essential to them. Applications may affect stakeholders, including the public, if the application and related processes are not managed appropriately.

Each year we review a selection of important applications that entities rely on to deliver services. We focus on the key controls that ensure data is complete, accurately captured, processed and maintained. Failings or weaknesses in these controls have the potential to affect other organisations and the public. Impacts range from delays in service and loss of information, to possible fraudulent activity and financial loss.

Audit focus and scope

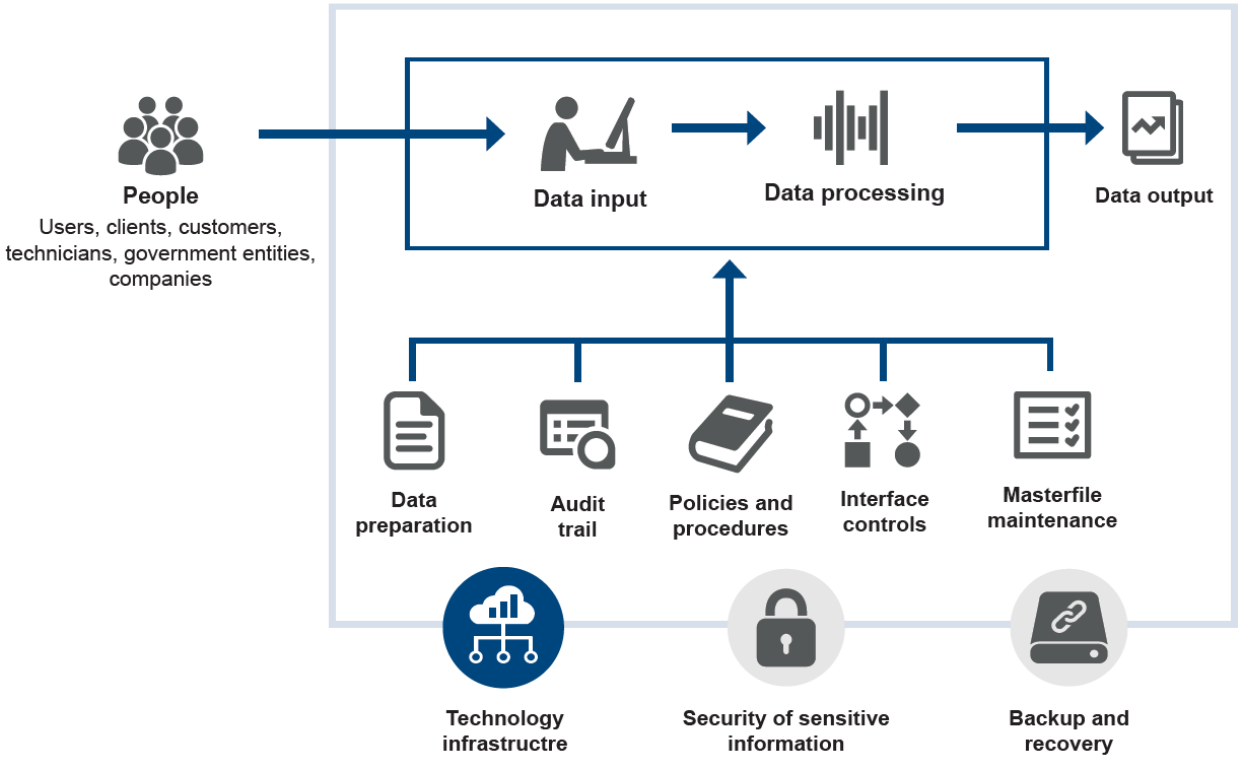
We reviewed the following key business applications:

1. **Teacher Registration System** – Department of Education, Teacher Registration Board of Western Australia
2. **Deliveries and Billing System** – Forest Products Commission
3. **Housing Management System (Habitat)** – Department of Communities
4. **Student Management System** – Department of Training and Workforce Development, North Metropolitan TAFE, South Regional TAFE.

Our audits focus on the systematic processing and handling of data in the following control categories:

1. **Policies and procedures** – are appropriate and support reliable processing of information
2. **Security of sensitive information** – controls exist to ensure integrity, confidentiality and availability of information at all times
3. **Data input** – information entered is accurate, complete and authorised
4. **Backup and recovery** – is appropriate and in place in the event of a disaster
5. **Data output** – online or hard copy reports are accurate and complete
6. **Data processing** – information is processed as intended, in an acceptable time
7. **Segregation of duties** – no staff perform, or can perform, incompatible duties
8. **Audit trail** – controls over transaction logs ensure history is accurate and complete
9. **Masterfile maintenance, interface controls, data preparation** – controls over data preparation, collection and processing of source documents ensure information is accurate, complete and timely before the data reaches the application.

We focus on people, process, technology and data in application audits. In consideration to these elements, we follow the data from input and processing through to storage and outputs.



Source: OAG

Figure 1: Key elements of focus for our application audits

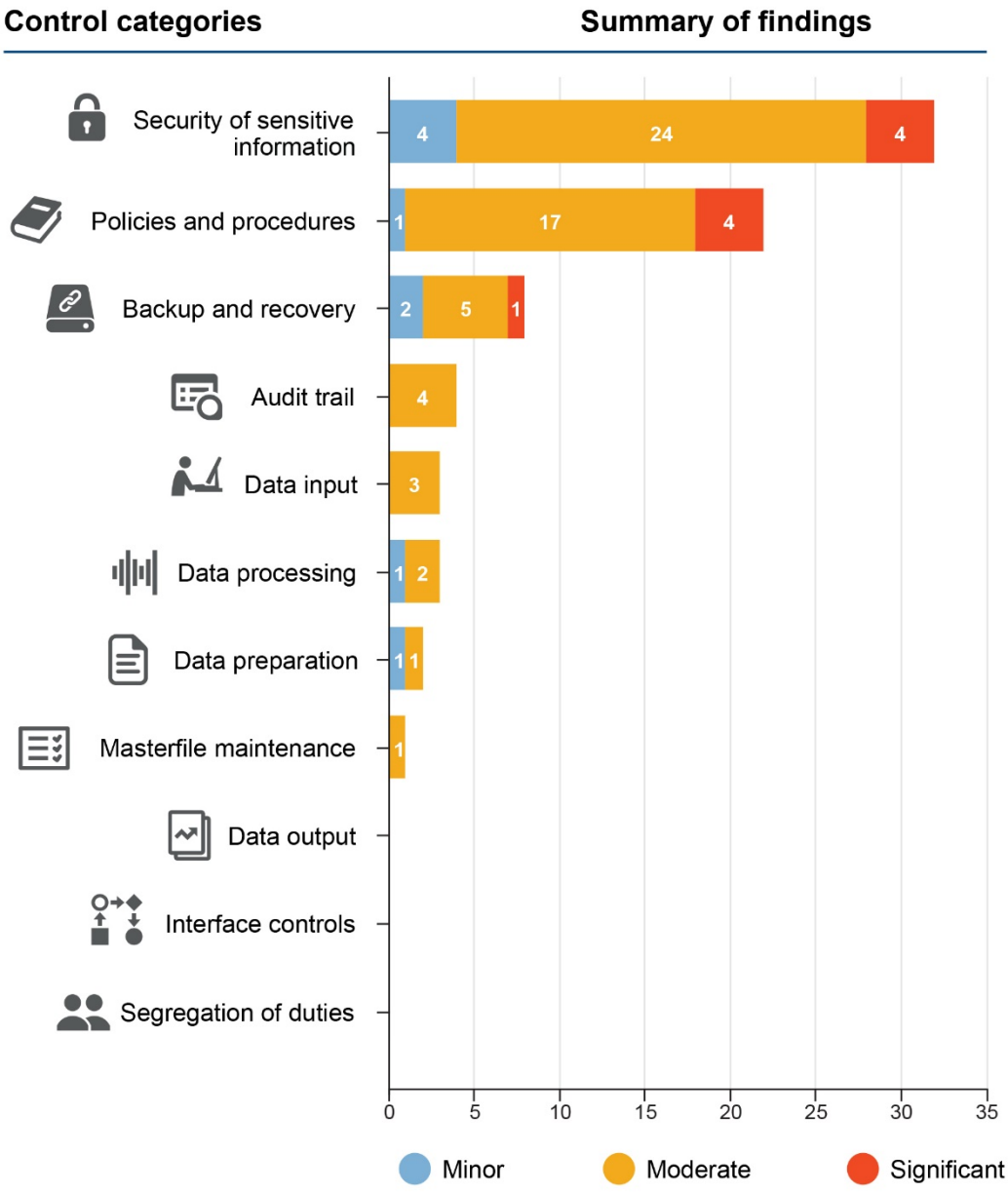
Our testing was performed during 2019-20 and is a point in time assessment. We reviewed a sample of key controls and processes to obtain reasonable assurance that the applications worked as intended and that information they contained and reports were reliable, accessible and secure. Our testing may highlight weaknesses in control design or implementation that increase the risk that an application's information may be susceptible to compromise. However, we do not design our tests to determine if information has been compromised.

Summary

All 4 applications had control weaknesses. Most related to poor information security and policies and procedures. We also found weaknesses in controls aimed to ensure the applications function efficiently, effectively and remain available. We reported 75 findings across the 4 applications. Nine findings were rated as significant, 57 moderate and 9 minor.

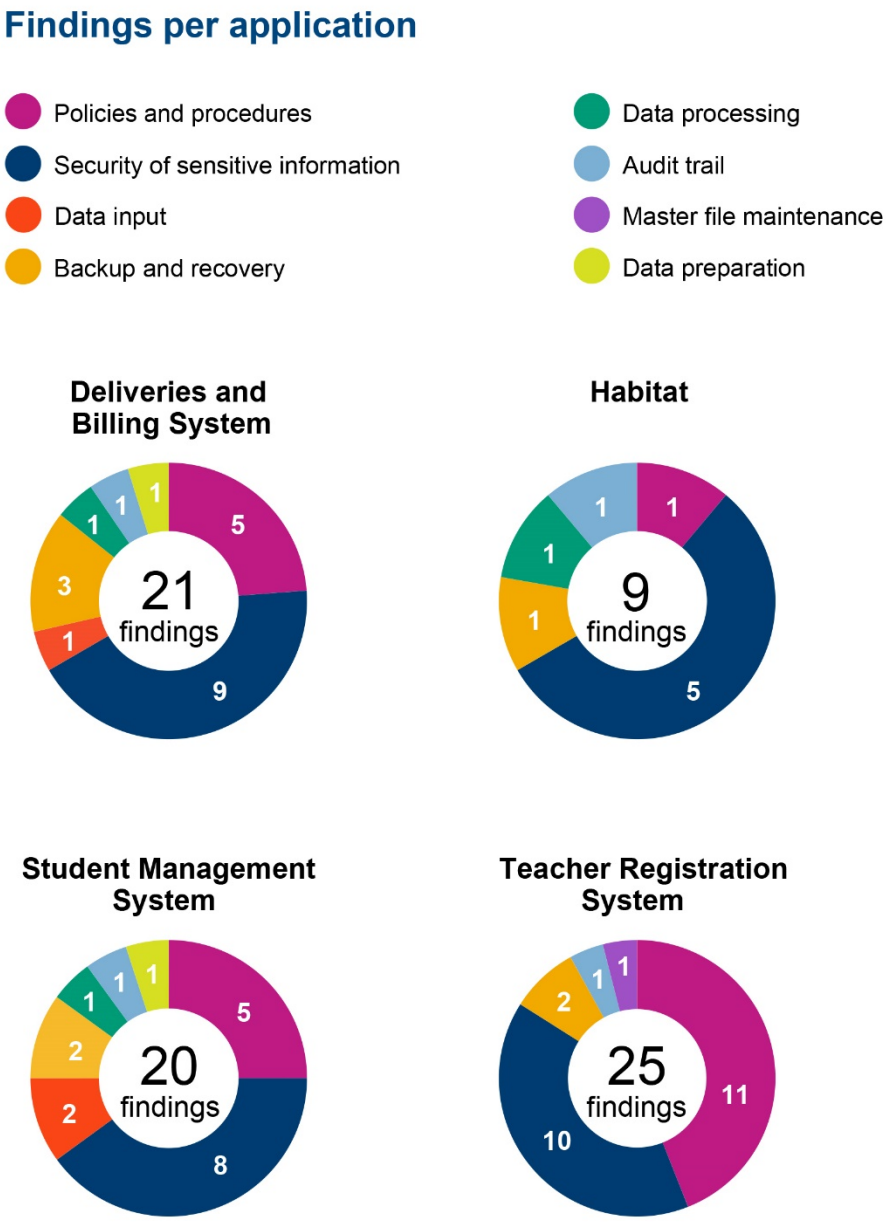
Most of the issues we found are relatively simple and inexpensive to fix. Figure 2 shows the findings for each of the control categories and Figure 3 shows the findings for each of the 4 applications reviewed.

Application audits



Source: OAG

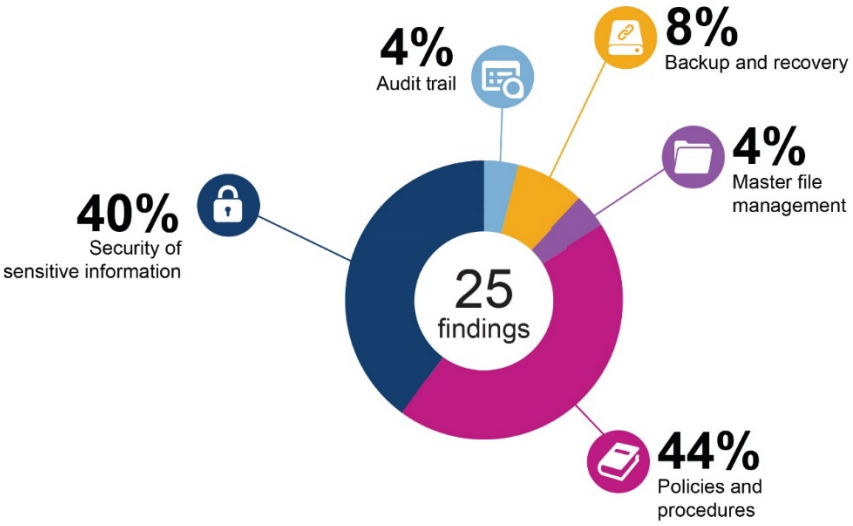
Figure 2: Findings per control category



Source: OAG

Figure 3: Findings per application

Teacher Registration System – The Teacher Registration Board of Western Australia

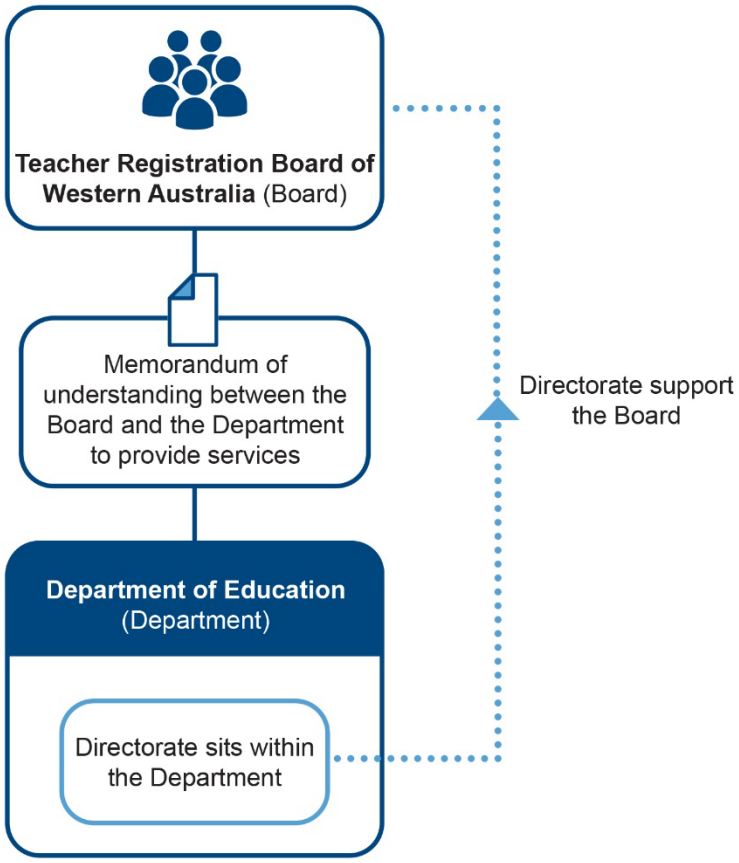


Source: OAG

Figure 4: Summary of audit findings for this application

Introduction

The Teacher Registration Board of Western Australia (Board) is a 7 member board responsible for the registration of teachers and the accreditation of initial teacher education programs in Western Australia. The Board relies on the Teacher Registration Directorate (Directorate) within the Department of Education (Department) for administrative support to deliver teacher registration services (Figure 5).



Source: OAG

Figure 5: Overview of the structure

The Directorate uses a suite of applications (System) to deliver services on behalf of the Board. The System processes approximately 13,000 new registrations per year, renews existing registrations and maintains the information of over 55,000 teachers. The information in the database is relied upon to determine whether a person has met the relevant requirements to practice as a teacher in Western Australia.

Our audit examined the effectiveness of the controls and governance processes for managing teachers' registration information in the System.

Conclusion

The System assists the Board to deliver teacher registration and related functions. However, the information systems and technology services do not adhere to the Department's IT governance and control frameworks as the Department has been slow to transition the Directorate, and its systems, into the Department's IT operations. Consequently, there are a number of significant weaknesses in the System which prevent the Board and the Department from efficiently managing public resources and effectively managing information security risks relating to sensitive teacher information. Basic governance and controls, including limiting access and segregation of duties for system changes, were not implemented.

There is also a risk that insufficient disaster recovery planning and ongoing System failures could result in an outage that impacts teacher registration services.

Background

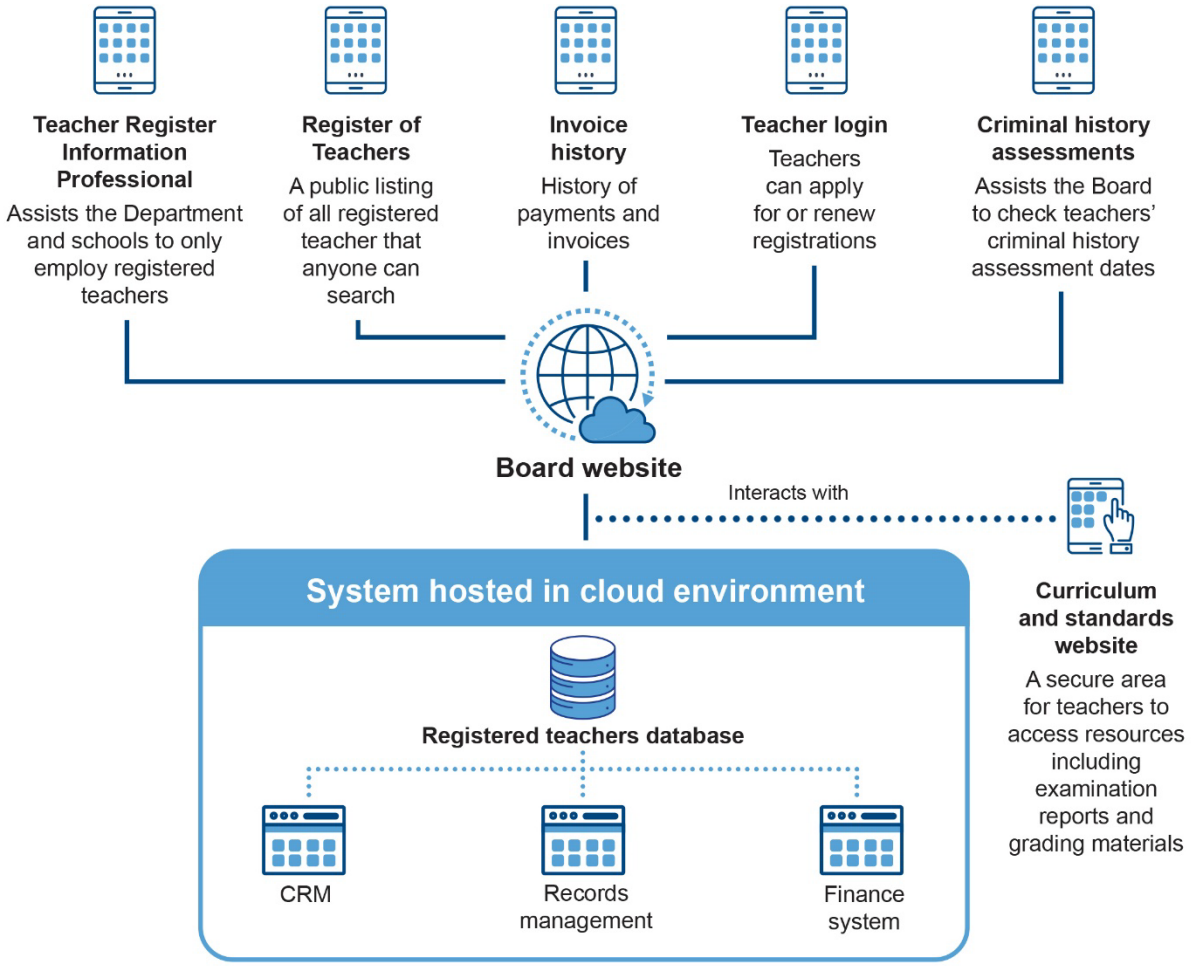
The Directorate was transferred from the Department of Education Services to the Department of Education following Machinery of Government changes in 2017. In June 2019, the Board and the Department signed a memorandum of understanding (MOU) to formalise the services the Department would provide.

The Department provides services to the Board including human resources and personnel for secretariat support, infrastructure, financial services and information systems and technology support.

The System

The System is a combination of internally developed and commercial software applications. It is hosted on public cloud infrastructure and is developed and maintained by Department staff and contracted suppliers.

The Directorate heavily customised a customer relationship management system (CRM) to provide online tools to manage teacher registrations, fees and records through integration with other business systems (Figure 6).



Source: OAG based on information from the Department

Figure 6: Simplified overview of the System

Key findings

IT services are not aligned with the Department's IT governance processes

The Department has been slow to transition the IT services provided to the Board into its IT operations. As a result, the Directorate has continued to operate independently, and the IT services it provides to the Board did not follow or were not subject to the Department's IT governance processes.

The Board relies on the Department to provide support staff, services and facilities to perform its functions. The Department's priorities may not necessarily align to the Board's needs which could impact on teachers' registration functions. It took 2 years for the Board and the Department to formalise the MOU. Prior to this, the Board did not have any other mechanism to hold the Department accountable for the services it should provide.

Although the Directorate and the Department developed a plan for IT support and resource management, they have been slow to implement this plan. For example, the Directorate spent approximately $240,000 between July 2019 and February 2020 on contracted services that the Department could provide. Failure to implement the agreed plan has resulted in avoidable expenditure and exposes the Board to the risk of not achieving its business objectives.

There is also a conflict of interest risk as the same contractor proposed and undertook projects. The Directorate spent approximately $500,000 in 6 months with this contractor. The Department advised us that they were recruiting permanent staff to resolve this conflict and ensure they achieve value for money.

IT governance, security and risk management are poor

The Board has not sought, and the Department has failed to provide it with, appropriate corporate direction and governance for the System. We found:

- **No IT strategy** – there is no long-term IT strategic plan nor a short-term plan to guide System investments and operations. Without this, IT resources and processes may not align with the Board's business strategies and priorities.
- **Limited oversight** – there is no governance committee to oversee and direct System technology investment and priorities. Additionally, management processes are not in place in the areas of:
    - risk management
    - change management
    - project management
    - incident and problem management
    - cloud management
    - continuity management.

    Governance and management controls are essential to ensure that key information system controls operate as intended. Weak governance increases the risk that the business objectives will not be achieved.
- **A lack of information security management** – there are no policies and procedures to manage information security for the System. While the Department has information security policies, these were not applied to the System largely because it operates on a

separate network to the Department. The lack of policies and procedures leaves the confidentiality, integrity and availability of the System, and any information it holds at risk of compromise.

- **Poorly managed cloud resources[1] create risk and inefficiency** – there are no polices to manage security risks associated with the cloud environment. Consequently, the Board does not know if these risks are managed effectively. We identified the following issues:
    - Roles and responsibilities for managing the cloud environment have not been defined. There were 33 subscription owners that can manage and have full access to the cloud resources. As this is the highest level of access, the vendor recommends a maximum of 3 owners to reduce the risk of a potential System breach.
    - There is no process to manage cloud resources and associated costs. Neither the Board nor the Department had reviewed if existing resources are necessary and associated costs are reasonable.
    - There were a large number of resources (119) allocated to data centres outside Australia, including Southeast Asia and the United States. Any data or information processed and held by a resource is subject to the laws of the country where the data centre is located. The Department had not assessed if those laws met their information security and privacy needs to protect information from deliberate or unintentional disclosure, which is recommended by the cloud provider.

  The Department has policies and procedures to manage its cloud environment which should be used for the System and could be easily applied to manage risks.

- **The overall approach to risk management is ad-hoc and unstructured** – System risks are not managed in line with the Department's risk management policy. Without adequate information risk management processes, threats may not be identified, treated and monitored.

- **Lack of appropriate project governance** – the Department's project governance framework has not been applied to manage IT projects. There was no business case to support the decision to use the chosen website management software for the System. In addition, the electronic forms project for the System was delivered 8 months late. Without project governance, it may be difficult to ensure that projects are delivered on time and do not exceed budget.

Software development has not always considered security

We found that the Department's security processes were not applied during System development. This introduced security vulnerabilities that need to be managed. We found that:

- **There is insufficient documentation supporting the design of the System** – secure software development rules and guidelines have not been developed for the System. In addition, there was a lack of:
    - documentation on the design and flow of data between System applications and processes

[1] Cloud resources include applications, servers, databases and other IT infrastructure

- an up-to-date diagram that details the cloud and network architecture including key security components.

Future System development or replacement projects could be adversely affected by a lack of System knowledge if key staff leave.

- **Lack of controls to maintain versions and changes to the source code** – changes to the System are not controlled in line with the Department's change management policy. System changes and approvals are only recorded in emails and not in an appropriate change management tool.

  A history of changes made to the System's underlying source code is not retained. Additionally, new functions are deployed to the production environment without appropriate testing and production environments are not monitored or periodically reviewed to ensure no unauthorised changes have been made. These weaknesses could compromise the availability and integrity of the System.

- **No segregation of duties** – we found that the same individual develops and implements changes between test and production environments without any oversight. The risk of inappropriate changes being made and going undetected is significantly increased as a result of this inadequate change control.

- **Unauthorised access to the source code** – we also identified that a terminated staff member, who was involved in the System development, still had access to the System source code. This occurred because the Department did not promptly remove access to the source code repository when the staff member departed.

Without appropriate software development processes, security vulnerabilities can be introduced into production. These vulnerabilities could be exploited by malicious attackers to gain unauthorised access to teachers' information. Access and changes to code need to be well managed to protect the security, performance and stability of the System.

Websites for online services had security weaknesses

We found security weaknesses in websites used to manage teachers' information. In particular:

- **Access controls can be bypassed** – the teachers criminal history assessments website allows the Department to check teachers' registration status and criminal history assessment dates. The password for the website could be found in the HTML code by anyone visiting the website. Further, we were able to bypass authentication processes and accessed restricted parts of the website. These weaknesses could compromise teachers' personal information.

- **Teachers' invoice payment histories could be accessed without a password** – teachers' payment histories, including current account balances and invoice details, could be accessed by anyone without authentication. We were informed that unauthenticated access should have been decommissioned but this was not the case at the time of our audit. Sensitive information should be closely guarded from unauthorised access as it could be used for malicious purposes.

- **Teachers' details are not verified before granting access to the curriculum website** – the online registration process did not verify teachers' details and allowed anyone to access the secure areas without being a registered teacher or even applying for registration. This website contains grading materials for teachers which could impact the Department's reputation if they were made available to everyone.

When online services are not secure, there is an increased risk of unauthorised access or disclosure of sensitive information. This may adversely impact teachers and damage the Board and Department's reputation.

Weak security controls place sensitive records at risk of inappropriate access and misuse

The System stores teachers' personal and sensitive information and evidence related to misconduct investigations. We found the following issues:

- **Sensitive information is not stored appropriately** – copies of sensitive information (e.g. 100-point identity documents and credit card details) used for teacher registration or misconduct investigations are stored indefinitely outside the System in less secure emails and network storage. While these documents are imported into the records management system they are not removed from emails and shared storage. Personal identifiable information is extremely valuable to malicious attackers and requires an appropriate level of classification and protection.

- **Personal identity information is not redacted in work instructions and communications** – guidance material used by the Directorate's staff contain teachers' identity information. In addition, monthly reports emailed to other business units outlining the number of registrations received and approved contain unnecessary personal information for over 55,000 registered teachers. Teachers' personal and sensitive information may be compromised if this information is deliberately or inadvertently sent to an unauthorised recipient.

- **Weak database controls could expose information** – the Directorate does not perform periodic reviews of user access rights. There were 32 accounts that have full access to the CRM production database which included people who did not require this access such as testers. We also found over 70 users who can directly access teachers' information from the database without going through the System. Additionally, the CRM, finance and records management databases are running on unsupported operating systems which could negatively impact security and operational support.

  Without appropriate database security controls that limit access to information on a need-to-know basis, teachers' sensitive information is at higher risk of unauthorised access and disclosure.

- **Live production data is used in test environments** – data is not appropriately de-identified when copied into test environments, which are often not as secure as production environments. Using identifiable information in test environments increases the risk of unauthorised access or disclosure of teachers' information.

- **Inadequate cloud security controls to protect teachers' information** – appropriate security controls are not in place to limit network traffic and communications from untrusted networks. We found that:

  - a web application firewall is not implemented
  - firewall rules do not appropriately restrict traffic
  - internet-facing virtual machines, virtual networks, key vaults[2], and storage accounts[3] are not appropriately secured

[2] Stores secrets such as passwords and certificates in the cloud.

[3] Contains all data objects including files, disks and tables.

- over 30 servers do not have anti-malware protection installed
- alerts have not been configured to notify staff when security has been compromised
- appropriate encryption controls to secure data in transit and at rest are not in place
- an independent security review of the cloud environment has not been performed to verify that security controls will detect and prevent malicious attacks.

Without appropriate security controls and processes to manage the cloud environment, there is an increased risk that the System and its information may be compromised and the Department may not be aware, limiting its ability to respond effectively.

- **Overall access management could be improved** – the process to manage the identity and privileges of staff and third party contractors requires improvement. We found:
  - There is no regular review of network user access to ensure it is appropriate and removed promptly when staff leave. In addition, the Department's human resources information is not used to identify terminated staff whose access should be removed. Consequently, we identified a terminated staff member who still had access to the network and System. We did not find any instances that this user accessed the network or the System after leaving the Department.
  - Twelve of 18 staff with the highest level of network privileges do not have a separate unprivileged account. Staff use their privileged account for day-to-day access including email and web browsing which increases the risk of compromise. It is good practice to only use privileged accounts for those tasks that require it.
  - Over 480 of 1310 accounts do not use multifactor authentication. This includes 40 staff and contractor privileged accounts that have full access to the cloud environment. We identified a former employee that still had access to cloud resources via a personal email account. We also found that any enabled account can invite other external users to access and modify the cloud infrastructure. This increases the risk that the System and the information it holds may be compromised.
  - The Teacher Login and Teacher Register Information Professional websites do not outline terms and conditions for use. This makes it difficult to hold people accountable for unauthorised System use.

  These weaknesses significantly increase the risk of inappropriate and unauthorised access to the System and the information it holds.
- **Inadequate vulnerability management** – system vulnerabilities and software updates are not well managed. Our vulnerability scans identified over 1,300 critical and over 2,000 high severity vulnerabilities on 7 servers and 32 workstations. Our scans also identified that the email system uses insecure protocols that could allow an attacker to intercept and read messages. These vulnerabilities are due to unsupported systems, missing patches and inadequate security configurations. They pose a risk to the System as they can be exploited by internal or external attackers to compromise the System and its information.
- **Lack of network segregation and unauthorised devices** – there is insufficient separation of key business systems and supporting infrastructure within the network. If critical systems reside on the same network as all other network users and computers,

there is a greater potential for harm as a breach would be more difficult to contain. Segregating business systems can act as an additional layer of protection.

In addition, there are inadequate controls in place to prevent or detect the use of unauthorised devices on the Directorate's network. Any unapproved device connected to the network can be used to collect information from the network and attack internal systems. This risk is elevated due to a lack of network segregation.

- **Inadequate logging and monitoring** – the existing network and System logging and monitoring process is not effective as:
    - the network is not configured to log key security events (for example, file access and/or changes, use of privileges and configuration changes). For the events that are logged, they are not protected against unauthorised access and changes
    - database logging and auditing is not in place to monitor and record changes in the CRM and records management databases.

  Without effective logging and proactive monitoring of security events and changes, unauthorised access or malicious activity may not be detected and evidence to support any forensic or internal investigations may not be available. As a result, individuals cannot be held accountable for their actions.

System failures have occurred and remain an ongoing risk

There is no business continuity and associated disaster recovery plan for the System. These are needed to ensure the ongoing delivery and timely restoration of critical business processes and systems following a major incident.

The System has many points of single failure. The failure of any 1 application could result in a total failure of the System and loss of services to teachers, schools and the Department. During our audit, we observed a failure that caused an outage to the whole System. A staff member had to be recalled from leave to resolve this incident.

In addition, the Directorate may not be able to maintain the integrity and availability of teachers' information as it does not have a backup policy for applications and information. We identified the following issues:

- **No long-term backups** – the data backup policy is inadequate as the System is configured for daily backups, which are only kept for 60 days. Quarterly, biannual or yearly backups are not maintained. If an unidentified error or data loss occurred more than 60 days ago, all backups would have the same issue and data could not be recovered.
- **Monitoring of backups is ineffective** – we found that a System component had not been backed up for 5 months due to an error, and the Directorate was unaware that this had occurred.
- **Backups are not regularly tested** – backup arrangements for systems and services are not tested to ensure they can be relied upon in the event of a disaster and meet the business expectations.
- **Incidents and problems are not managed appropriately** – there is no IT incident and problem management process to address identified issues in the System. The Department has not transitioned the Directorate to its incident management system.

Without appropriate incident management procedures, any incidents with the System may not be addressed, causing loss of services. In addition, the lack of business continuity procedures could delay recovery of the System following a major disruption.

Recommendations

1. The Board should implement appropriate arrangements to monitor the services delivered by the Department.

   Response: Agreed

   Implementation timeframe: by April 2021

2. The Department should:

   a. apply its process for managing cloud security, risks, cost management and data sovereignty to the System

      Response: Agreed

      Implementation timeframe: by July 2021

   b. develop business continuity, disaster recovery and adequate data backup plans to ensure the integrity and availability of the System and its information

      Response: Agreed

      Implementation timeframe: by July 2021

   c. implement services agreed under the MOU with the Board

      Response: Agreed

      Implementation timeframe: by April 2021

   d. implement its plan for resource management for the Board

      Response: Agreed

      Implementation timeframe: by April 2021

   e. apply its software development framework to ensure that information security is an integral part of the System lifecycle. This includes ensuring that design documentation is available for System support

      Response: Agreed

      Implementation timeframe: by July 2021

   f. review websites to address security weaknesses that could compromise teachers' information

      Response: Agreed

      Implementation timeframe: by April 2021

g. review the practice of storing sensitive information relating to teacher registration or misconduct investigations in emails and network shares and ensure it is protected and managed in-line with the Board's expectations

Response: Agreed

Implementation timeframe: by November 2021

h. improve its user access processes to control privileges and ensure only current and valid users have access to the Board network, applications and databases

Response: Agreed

Implementation timeframe: by April 2021

i. review and enhance technical vulnerability management processes for the System to ensure that key systems and information are protected from internal and external security threats.

Response: Agreed

Implementation timeframe: by April 2021

Combined response from the Teacher Registration Board of Western Australia and the Department of Education

Since receipt of the management letter from the Office of the Auditor General (OAG) in July 2020, the Department of Education and the Teacher Registration Board of Western Australia (TRBWA) have worked collaboratively to resolve the 25 audit findings to improve the controls associated with the processing and handling of data in the Teacher Register Information System. To date:

- 18 of 25 findings have been addressed:
- 5 of 25 findings are more than 60% completed
- 2 of 25 are at least 50% completed.

The decision to align support of the TRBWA to the Department as a result of the 2017 Machinery of Government changes has helped realise economies of scale. In particular, the TRBWA is now supported by the shared services of the Department of Education, including information systems and technology, corporate governance and assurance, human resources and finance, addressing several of the concerns raised in the audit.

In addition to the significant progress made in addressing the findings since the management letter was issued, at the time the audit was proposed in 2019, there was already an acknowledged need to replace the Customer Relationship Management (CRM) system that houses the key teacher registration database. A project to complete that replacement is well underway and will be completed in 2021.

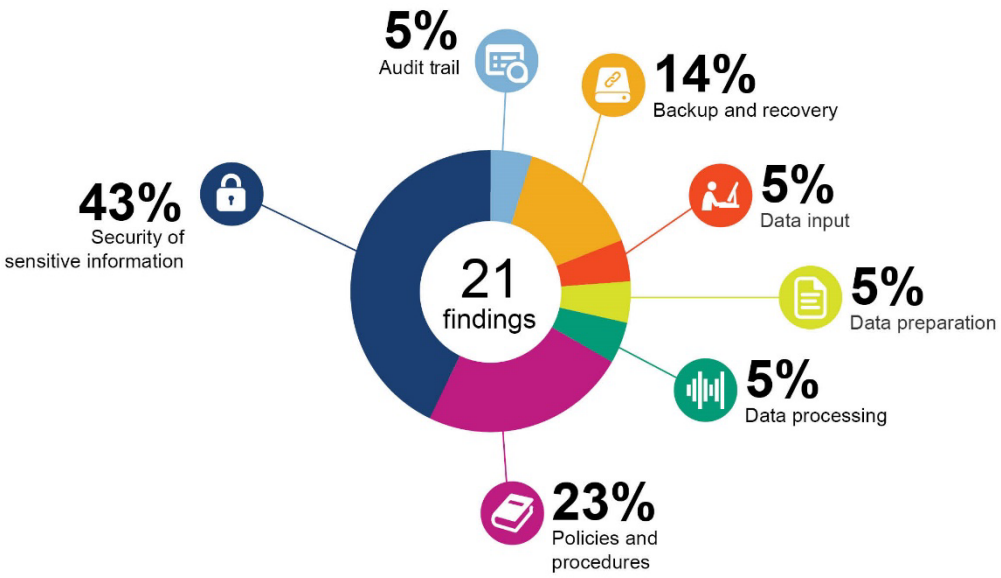
This has been coupled with progress against an implementation plan responding to the audit findings. Notably, this has included alignment with the Department's IT governance processes, an improved approach to IT governance, security and risk management, better consideration of security issues with respect to software development, security weaknesses associated with websites for online services being addressed and improved security controls. In particular, since the audit, the TRBWA has adopted, or is now included in, the Department's:

- ITIL services management platform (Service Management, Incident, Problem, Change etc.)
- Vulnerability and Patch Management processes
- Project Management Model
- Backup Approach, including periodic testing
- Office 365 Email platform
- Security model, including the Security Operations Centre service
- Cloud Management Processes
- Database Management Approach, including access control and logging
- Access to TRB production databases, systems or applications was reviewed/removed where applicable, a process agreed for granting access and a scheduled review every three months.

Website issues were fixed immediately once draft recommendations were provided. A partial penetration test of a key website was also successfully conducted. Development of design and software documentation framework has commenced.

The Department of Education and the TRBWA welcomes the recommendations from the applications control audit by the OAG. The integrity, confidentiality and controls of the TRBWA remain a high priority and the audit conducted by the OAG assisted the TRBWA and the Department in increasing compliance and governance. The resolution of the remaining recommendations continues to be prioritised.

Deliveries and Billing System – Forest Products Commission



Source: OAG

Figure 7: Summary of audit findings for this application

Introduction

The Forest Products Commission (Commission) is a statutory authority governed by the *Forest Product Act 2000* (Act) and the Forest Management Regulations 1993 (Regulations). The Commission is responsible for harvesting timber products from the State's native forests and plantations and selling it to customers. In 2019-20, the Commission recorded $122 million of sales from timber products. It uses its Deliveries and Billing System (DAB) to process information for revenue and payment purposes.

Conclusion

The DAB enables the Commission to generate revenue and payment information from the harvest and sale of timber products. However, inadequate practices for verifying this information and monitoring compliance with the Regulations, increase the risk of revenue loss or fraud.

Security weaknesses in the DAB database and the Commission's network may expose the Commission to malicious attacks and unauthorised access. In addition, weaknesses in controls, including the review of information entered into the DAB and monitoring of compliance with the Regulations, creates risks of incorrect revenue or payments and non-compliance.

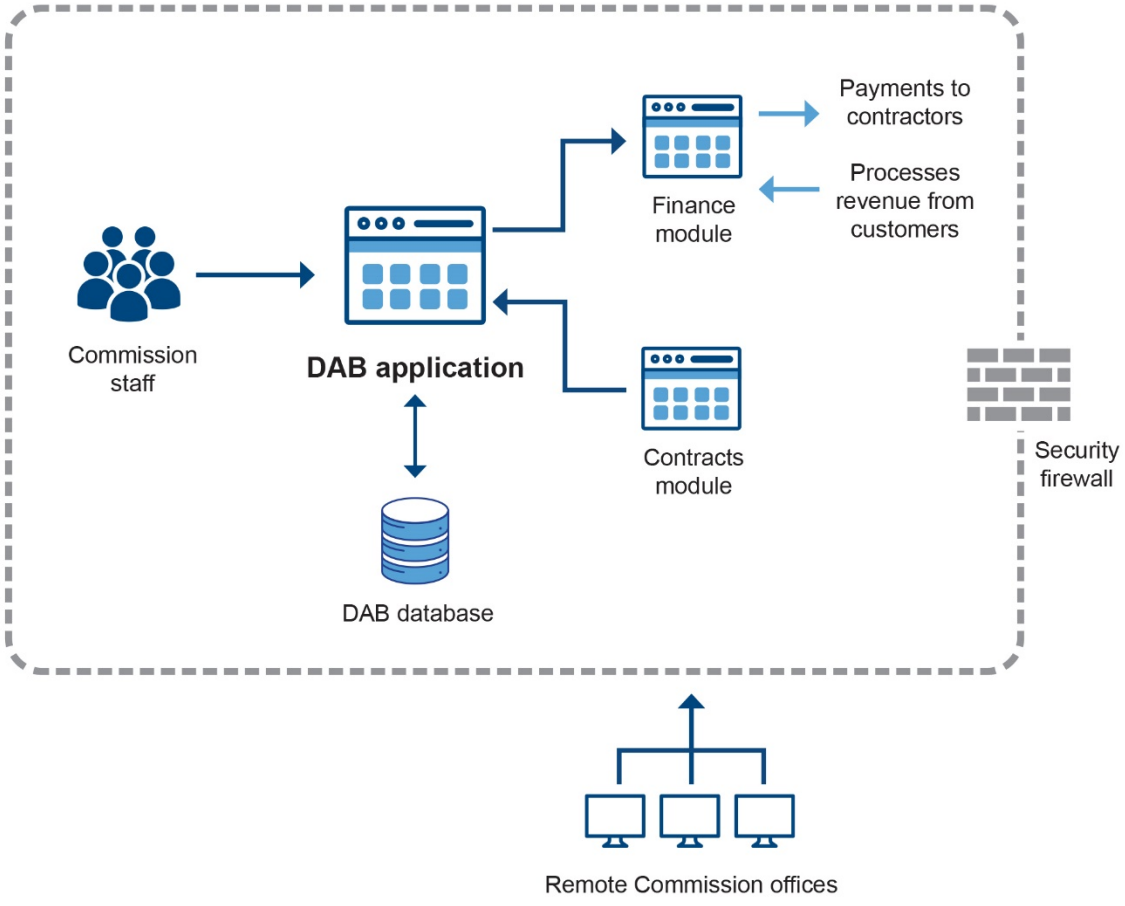
The 2019 DAB implementation project encountered delays and cost overruns, and the Commission could not demonstrate that an effective project governance framework was in place. While the Commission had a lot of project delivery templates, they were not used due to a lack of policy.

Background

In August 2016, the Commission started a project to replace its former logging operations system. It purchased an additional module for an existing business system to meet the Commission's needs. The module, referred to as the DAB, went live in July 2019. The DAB consists of an application and a database which holds all of the information. Both reside within the Commission's network.

The Commission uses paper-based delivery notes to collect harvest and haulage information from contractors and customers, which is entered into the DAB. As shown in Figure 8, the DAB uses rates from the contracts module to generate billing information. The finance module then processes customer invoices (revenue) and payments to contractors who harvest and haul timber products (expenses).

Since going live in July 2019, up to September 2019, the DAB has processed over 6,000 delivery notes.



Source: OAG using information from the Commission

Figure 8: The DAB consists of an application and a database, hosted internally within the Commission's network

Key findings

Lack of controls over reported timber volumes elevate the risk of fraud

The Commission did not validate or reconcile timber volumes reported by 2 customers (private firms) who organise their own harvest and haulage of timber products from

Department of Water and Environmental Regulation lands. For these sales, the Commission solely relies on information provided by the customers about the volume of harvested products. In addition, the volumes of harvested products are not recorded in the DAB. The total revenue received by the State in 2019-20 from these customers was around $640,000. The absence of controls to verify the reported volumes increases the risk of fraud or errors that could lead to loss of revenue or non-compliance.

The Commission acknowledges the risk and has agreed to revise its sale process.

Inadequate controls threaten the integrity and confidentiality of data

The Commission does not adequately manage key information entered, processed and stored in the DAB that generates invoices and payments. We found:

- **Lack of independent review of data entry** – we identified over 240 instances where the same staff member entered and reviewed delivery note information in the DAB. Independent review is important to detect and correct errors. Inaccurate or incomplete information in the DAB increases the risk of incorrect invoices to customers and payments to contractors. Despite this weakness, we did not find any instances in our small sample where data entry was incorrect.
- **Insecure access to data files** – the DAB relies on various system files to generate invoices and payments. These files are stored on a shared network folder outside the DAB, without adequate controls. All staff connected to the network have full access to view, modify or delete these files. Unauthorised modification of these files could compromise the integrity and availability of the DAB. Since the Commission does not record access and changes made to these files, it may not know when unauthorised changes are made or who was responsible for the changes.
- **Database security is weak** – a number of security weaknesses expose the DAB database to security threats and may compromise the confidentiality, availability and integrity of information.
    - The Commission is using an unsupported version of the DAB database which no longer receives security updates from the vendor. This means the database is not protected from security threats.
    - The DAB database is not segregated to restrict and protect information from unauthorised access. All users accessing the Commission network can directly connect to the database. Good practice suggests that only users and systems that need access to a database should have it.
    - Multiple staff share 1 highly privileged account to administer the database and its password has not changed for an extended period. Using a shared account limits the accountability of actions performed by staff. In addition, it is important to change the password for shared privileged accounts as they are often targeted by malicious actors.
    - There is no encryption of sensitive information such as names, account information and contract rates. This exposes sensitive information to unauthorised access and misuse.
    - All database accounts had privileges allowing them to run privileged system tasks. If the database is breached, this level of access may help an attacker gain control of the DAB database server.
- **Ineffective user access management for the network and application** – the Commission does not have appropriate controls to manage user access to its network

and the DAB. We identified the following weaknesses which may allow unauthorised access to the Commission's IT systems and information:

- Staff identity is not appropriately verified before resetting passwords. It is important to verify the identity of individuals requesting password changes as malicious attackers use social engineering techniques to trick operators to provide passwords.
- IT staff with highly privileged accounts do not have a separate, unprivileged account, for day-to-day access. Using high privileged accounts for day-to-day activities like email and web browsing increases the risk of compromise. It is good practice to only use privileged accounts for those tasks that require it.
- The Commission's monthly review of user access is not effective. We identified the account of 1 terminated employee that was not disabled and was later used to access the network. Once we informed the Commission, it disabled the account but could not determine the reason for this access. In addition, we found unused enabled accounts for 2 users that have never accessed the network, and 5 accounts that have not accessed the network in over 6 months. Unused accounts could be misused to gain unauthorised access.

- **Event logging and monitoring** – logging and auditing is not in place to monitor and record system changes in the DAB database. This means that the Commission will not be able to detect and investigate unauthorised changes and security breaches. The primary network server is also not configured to log key security events including file access and changes, use of privileges and configuration changes. As a result, any unauthorised changes or access to the systems may go undetected.

  While the DAB application and network firewall generate event logs, these are not reviewed nor secured to protect against unauthorised access or changes, increasing the risk that they could be altered. Security information and event management systems can assist with efficient analysis of security events.

- **Shared production environment** – the DAB training, development and test databases are installed on the same server as the production database. Configuration changes to the other environments could compromise the availability of the DAB.

Network security and technical vulnerabilities are not well managed, leaving the DAB exposed to malicious attacks

The Commission has controls in place to manage core infrastructure. However, we found the management and configuration of these controls ineffective. The following issues were identified:

- **Firewall management** – the Commission's network is managed through a central firewall. It is a single point of failure as there is no secondary firewall to switch over to in event of failure. Its failure would compromise the availability of the network and systems.

  The Commission does not periodically review the firewall rules to ensure they reflect changes to the network over time and address security threats. Regular review would allow weaknesses due to inappropriate configuration to be identified and addressed.

  We also found that all firewall administrators use a shared generic account to make changes to the firewall and rules. This reduces individual accountability for unauthorised or unintentional changes to the firewall.

- **Unauthorised devices** – unapproved equipment can connect to the network without any restriction. There are no controls to prevent and detect these connections, allowing

them to reach key IT assets, systems and information undetected. As a result, there is a potential for malicious attacks from inside the network to the Commission's systems and information.

- **Technical vulnerabilities** – we found the Commission's vulnerability management process is not effective and does not apply to workstations (for example, desktops and laptops) that are exposed to threats through email and internet use. We conducted scans on 6 workstations and key servers supporting the DAB, and identified 66 critical and over 150 high severity vulnerabilities, some dating back to 2014. These vulnerabilities, which can be avoided by regularly patching and configuring systems appropriately, could be exploited to gain unauthorised access to the system and disrupt business operations. The Commission has agreed to address these vulnerabilities.

  In addition, we found that server software updates are applied to fix vulnerabilities without testing, which could impact the availability of systems.

- **Lack of testing for external attack risks** – the controls which detect and prevent external network attacks have never been tested to check if they are adequate and operating effectively. Failure to regularly perform these tests may result in undetected vulnerabilities, which could be exploited by malicious attackers to gain unauthorised access to systems or information.

Inadequate controls could result in regulatory non-compliance

The Regulations place a number of obligations on the Commission, contractors and customers. We found the Commission's controls for recording and reconciling harvest and haulage data are not implemented as required by the Regulations. In particular:

- The Commission collects harvest and haulage information using delivery notes which are issued by the Commission to customers and contractors in Delivery Books. The Regulations require that unused Delivery Books be returned 12 months after issue. We found over 560 issued Delivery Books had not been returned after 12 months, 19 books were issued over 9 years ago.
- The Commission checked the accuracy of delivery notes at a lower rate than the minimum thresholds established by the Regulations (5%). We found that the Commission only checked 4% for August 2019 and 3.75% for September 2019.
- Customers must return original delivery notes to the Commission within 3 days of receiving product as per the Regulations. Delivery notes are stamped by the Commission when received but these dates are not recorded in DAB. This makes it difficult for the Commission to monitor if they were returned within 3 days.

Failure to perform these important controls increases the risk of inaccurate, incomplete or fraudulent delivery notes being provided to the Commission. This may result in a loss of revenue to the State and non-compliance with the Regulations.

Ineffective project governance

The Commission does not have a project governance framework to inform its staff of requirements for project delivery. This contributed to the following deficiencies in the DAB implementation project:

- **Lack of project documentation** – the project commenced without an approved project initiation document defining the scope, resourcing and budget. It was approved 3 months after the project started.
- **Delayed implementation** – we reviewed the draft DAB project closure report which states that the project was planned to be completed in 2017. However, it did not go live

until 2019 and was overspent by approximately $720,000. This time delay was mainly due to another dependent project being late.

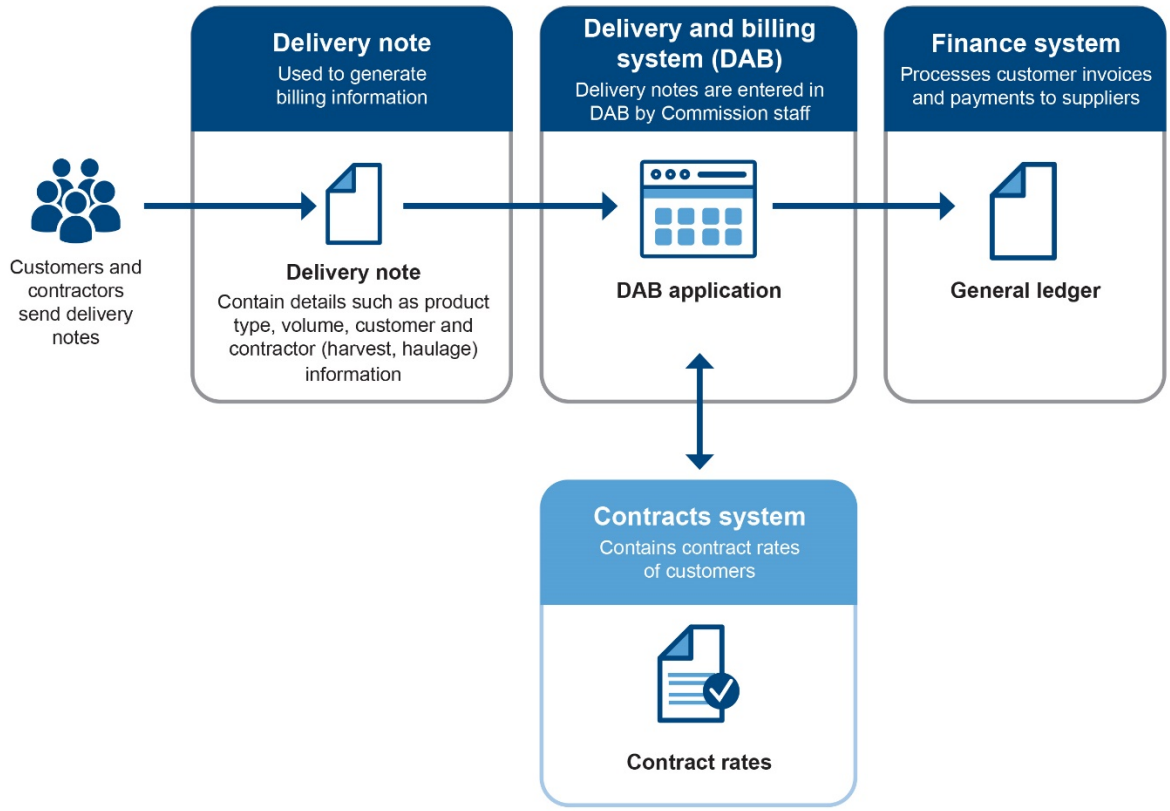
- **Inadequate risk management** – the project risks were not recorded in the governance management system as required by the Commission's risk management procedure. The Commission could not demonstrate if the DAB project risks were reported to senior management through other processes. It is therefore not evident that senior management had sufficient visibility of these risks during the DAB implementation project.
- **Unclear system ownership –** the Commission has not defined a business owner for the DAB. A business owner has the accountability and resources to ensure the system is meeting business needs and is functioning appropriately. Without clear business ownership, the system may not meet business requirements.

  A key role of the system owner is to prioritise and approve changes to the system. We found instances where changes to the system were implemented without an assessment as to whether they were needed. We also found changes where the same individual developed and implemented the change into the production environment without approval. Without change control and assessment, the Commission's resources may be spent on unnecessary features that introduce risks and weaknesses.
- **Lack of technical documentation** – the Commission purchased and configured the DAB as a module to add to an existing business system. However, the Commission did not document changes it made to the DAB configuration. As a result, the ICT team relies on outdated design documentation and may not be able to provide system support or resolve system problems as they arise.

Manual intervention during the billing run undermines transparency and accountability

The DAB processes paper-based delivery notes and sends billing information to the finance system to generate customer invoices and payments to contractors (Figure 9). The Commission conducts a weekly billing run. It runs multiple validation checks to make sure delivery note data is as per the contract and the price is accurate. In cases of error, Commission staff manually correct contract rates and haulage information to resolve issues.

However, the Commission does not record actions taken to correct delivery notes and contract rates. Without appropriate controls to capture these corrective actions, the Commission may not be able to determine who made the changes and why. This impacts the integrity of its harvest, haulage, revenue and payment information.



Source: OAG using information from the Commission

Figure 9: Simplified overview of billing process

Recommendations

The Commission should:

1. establish processes to verify the accuracy of customer reported information on harvest
2. protect databases by only granting privileges to those who need it to perform business functions. In addition, the Commission should restrict the use of shared generic accounts, place databases behind network or application firewalls and protect sensitive information through encryption
3. test and implement vendor security updates in a timely manner to address vulnerabilities
4. perform ongoing reviews of network security to protect systems from internal and external security threats
5. enhance the user access management process to ensure only current and valid users have access to the network and systems
6. improve practices to ensure delivery notes are returned and checked as prescribed by the Regulations
7. clearly define and assign ownership for effective governance of the DAB
8. ensure up to date design documentation is available for the IT support team to effectively provide support and updates for the DAB
9. implement adequate processes to record all actions to correct delivery notes and contract rates.

Commission response for all 9 recommendations: Agreed

Implementation timeframe for all 9 recommendations: by April 2021

Response from the Forest Products Commission

The Forest Products Commission (FPC) accepts the outcomes and the timeframes for implementation of the audit findings.

Regarding the security of ICT systems, the FPC has undertaken the following initiatives since the audit was completed:

- Expedited network consolidation and strengthening via GovNext.
- Implemented an Information Security Management System compliant with the whole-of-Government Digital Security Policy.
- Developed an ICT Project Management framework to improve project lifecycle controls.
- Implemented technological changes to address the SECC top 5 controls (patching and vulnerability management, privileged user access management, multi factor authentication, user application hardening and password management).

The above changes have been facilitated through the appointment of a dedicated ICT Security Manager. This position has responsibility for identifying and implementing initiatives to enhance existing security controls and for monitoring and managing any new security risks as they emerge.

Further to improvements in the security of its systems, the FPC has strengthened all aspects of its Deliveries and Billing System. We have ensured consistency of information and process by aligning the responsibilities for DAB with the FPC Contracts Branch. Furthermore, we have developed an Electronic Delivery Note system (EDN) to replace the paper-based process and made the regulatory changes necessary to support the mandatory use of EDN from 1 January 2021. The use of real time information as part of the EDN process will substantially improve governance processes and provide robust and verifiable audit trails of any changes to delivery information.

Housing Management System (Habitat) – Department of Communities

Source: OAG

Figure 10: Summary of audit findings for this application

Introduction

The Housing Authority (Authority) is part of the Department of Communities. It uses the Housing Management System (Habitat) to manage most aspects of public housing across Western Australia (WA) including rental applications and property maintenance. The system stores confidential information including income, asset and bank details of prospective and current tenants. A third party vendor provides the system and its maintenance under a contractual arrangement.

Conclusion

Habitat adequately processes rental accommodation applications, property allocations and work orders issued for housing maintenance. A sound contract and service level agreement is in place between the Authority and the vendor to facilitate the ongoing service delivery and performance monitoring.

However, manual processes and inadequate system security controls could compromise the integrity of information, increase the risk of incorrect or inappropriate property allocations and put sensitive information at risk. The Authority has not performed a risk assessment to identify threats to the system and ensure adequate controls are in place.

The Authority does not have a disaster recovery plan, which means in the event of an incident or disruption, Habitat may be unavailable for extended periods.

Background

The Authority

The Authority is a major provider of public housing in WA. It has more than 25 offices and 650 staff across the state that process rental applications and manage tenancy matters using

Habitat for more than 39,000 properties. This includes housing for remote communities, non-government organisations and over 5,000 properties that house government employees.

People can apply for housing either in-person or by posting completed application forms to the Authority. The Authority staff enter these applications into Habitat for processing and eligibility checks. Applicants are placed on the public housing waiting list in Habitat if they meet the criteria.

Habitat

Habitat consists of a front end application used by Authority staff and a database which stores all the information entered through the application. Habitat information can be accessed and modified either through the application or directly from the database. Habitat also interfaces with Centrelink's system to verify applicants' income details. It generates many reports to assist with property management including weekly waiting lists, debt summary and property inspection schedules.

Key findings

Lack of risk assessments and oversight of controls may leave Habitat exposed to security risks

The Authority had not assessed the information security risks for Habitat. A risk assessment would allow senior management to understand if appropriate controls are in place to protect the sensitive information it holds. This risk assessment is especially important for the Authority as some controls are managed under contract by a third party.

In addition, the Authority had not implemented adequate processes that provide oversight of Habitat controls. Without regular testing of controls, the Authority may not identify control weaknesses that could impact the Habitat system, processes and information.

Manual processes are inefficient and could compromise the integrity of information

There are a number of manual processes for managing public housing information within Habitat.

For example, we identified that:

- Managers could offer a public housing property to an applicant outside the normal waitlist process. Our review of 8 such instances showed that this usually occurred due to urgent transfers caused by medical or domestic violence issues. These decisions are electronically stored in a different system instead of Habitat. This makes reconciliation between Habitat data and approval decisions difficult and time consuming.
- While Habitat shortlisted eligible applicants based on their needs and the time of application, the Authority's staff copied this information into a spreadsheet to manually shortlist applicants. Manually shortlisting applicants outside Habitat increases the risk of errors or that staff could allocate properties incorrectly or fraudulently.
- Team leaders do not receive any alerts when account adjustments or invoices are created by officers for approval. Instead, the team leaders manually monitor and search for items pending their approval such as an unauthorised account adjustment or an invoice. Automated workflows within the system, which notify officers when they need to approve an item, will help to streamline the authorisation processes.

- To reduce the risk of errors and fraud, the Authority does not allow property services officers to create work orders with emergency and urgent priorities. Instead a different division raises maintenance work orders. However, the system does not enforce or validate this rule and does not alert officers if they allocate an incorrect job priority. This may result in additional costs if a job priority is allocated incorrectly.

Reducing the extent of manual processing and better aligning of business workflows within Habitat will help to strengthen the integrity of Habitat information. It will also improve transparency and reduce the risk of incorrect or fraudulent property allocations.

Sensitive data was at risk of exposure due to insufficient database and application security controls

The Habitat database stores sensitive information of tenants including bank account, income and asset details. Habitat security controls were not effective in protecting the confidentiality and integrity of the information it stored. Some of the weaknesses were:

- **Weak passwords** – we identified 178 database user accounts with easy to guess passwords and 1,195 accounts where the password had not been changed for 5 years. These include accounts with high privileges, which are often targeted during malicious attacks. Easy to guess passwords are inconsistent with good practice and increase the likelihood of unauthorised access. In addition, none of these passwords met the requirements for complexity and aging included in the Authority's policies.

- **Shared use of a generic account** – the Authority's IT staff used and shared a highly privileged account to administer the Habitat database, rather than each using their own uniquely identifiable accounts with appropriate privileges. In addition, the password for the shared account was easy to guess and was not changed in line with the Authority's policy. As a result, staff moving within, or leaving, the Authority could retain access to the database, increasing the risk of unauthorised access to and disclosure of people's sensitive information.

- **Inappropriate privileged access** – the database had inappropriately assigned privileges to all user accounts allowing them to run privileged database functions. This allowed users to access and make changes to sensitive information.

  The application layer also had no formalised process to manage privileged. We identified a large number (73) of user accounts with high level privileges and full access to Habitat. When combined, these issues increase the risk of unauthorised, unintentional or deliberate modifications to Habitat and its information, without being detected.

- **Sensitive information was not protected –** the Habitat database was not designed to encrypt sensitive information including bank account, income and asset details of people who have applied for, or have been allocated, public housing. Also, the Authority replicated confidential information without masking into the test and development environments which usually do not have same security controls as the production environment. This increases the risk of sensitive personal information being misused.

The Authority would not know if inappropriate or unauthorised changes to Habitat information were made

We identified over 5,000 accounts with direct access to the database. The database does not have logging and auditing processes in place to record and monitor key information changes. This is concerning as the Authority will not know if information has been accessed or modified.

In addition, while changes made to records through the Habitat application are captured, the Authority does not regularly review these to identify inappropriate access or changes. As a result, changes to Habitat information and any suspicious access would go unnoticed.

There is no disaster recovery plan for Habitat

The Authority did not have a documented IT disaster recovery plan for Habitat unlike other systems. This is a key document that provides details of procedures to be followed to recover systems in the event of an incident or disruption. It also confirms the roles and responsibilities between the Authority and the contracted vendor for remediation action. An extended outage of Habitat could compromise the delivery of key services and potentially damage the reputation of the Authority.

Vulnerability management process could be further improved

Habitat servers were included in the Authority's monthly vulnerability scans but the scans did not successfully work for over 6 months due to incorrect configurations. This means some vulnerabilities were undetected.

We conducted vulnerability scans on key Habitat servers including the database and application servers across the development, test and production environments. Our scans identified that the servers running Habitat were not patched with software updates released by the vendor to address over 20 critical and 180 high severity security and performance issues. The critical vulnerabilities were published a number of years ago with some going back 15 years. Over 15 vulnerabilities also had known exploits which could be used by attackers to compromise and potentially gain unauthorised access to Habitat and its information. A lack of robust processes to identify, assess and address known vulnerabilities increases the risk that information and systems are not protected against potential threats.

Recommendations

By April 2021, the Authority should:

1. undertake a risk assessment to identify and treat risks associated with information security in Habitat and related business processes
2. review manual processes and implement automated workflows to improve efficiency and transparency
3. implement appropriate access controls to protect Habitat from unauthorised access and misuse through:
    a. better authentication for all accounts including administrator accounts
    b. limiting the number of accounts with high privileged access
    c. a risk assessment which determines appropriate controls, including encrypting sensitive information in storage. The assessment should also include non-production environments
4. implement an effective framework for logging and monitoring key events that impact Habitat and its information
5. develop, regularly review and test an IT disaster recovery plan
6. review and enhance patching process and apply software updates recommended by vendors in a timely manner.

Authority response to all 6 recommendations: Agreed

Implementation timeframe for all 6 recommendations: by April 2021

Response from the Housing Authority

The Department of Communities accepts the Office of the Auditor General's recommendations and immediately implemented a program of work in conjunction with the third party provider of Habitat to address audit findings once they were identified.

Among the findings was that sensitive data was at risk of exposure due to insufficient database and application security controls. As a matter of priority, the Department remediated these technical vulnerabilities. Processes are now in place to ensure the ongoing review of database and application security controls to protect the confidentiality, integrity and availability of Habitat data in the future.

Substantial progress has also been made in addressing the other recommendations arising from the application controls audit to improve the security and resilience of Habitat and the Department remains committed to completing this remediation work in accordance with the proposed time frames.

Student Management System – Department of Training and Workforce Development

Source: OAG

Figure 11: Summary of audit findings for this application

Introduction

The Student Management System (System) is used by Western Australian TAFE colleges to manage all aspects of the student experience from registration and enrolment through to graduation. The Department of Training and Workforce Development (Department) provides the System to TAFE colleges and manages changes and improvements. The System stores sensitive personally identifiable student information, bank account details and tax file numbers.

As part of the audit we reviewed the Department's controls to manage the System. We primarily focused on student registration and enrolment. We also included 2 System users, North Metropolitan TAFE and South Regional TAFE, to inform our audit findings.

Conclusion

The System enables TAFE colleges to manage student administration and experiences. However, we identified a number of opportunities to improve the overall governance of the System and help the Department and TAFE colleges better realise the intended benefits of the System.

The audit found that sensitive student information was at risk due to inadequate monitoring of user activity and poor user access management. The confidentiality of this information could be strengthened through improved database security and the de-identification of sensitive data in test and development environments.

There is also a risk that the System may not be recovered quickly in the event of a disruption because the Department has not fully tested its disaster recovery plan and the System software required for vendor support is out-of-date.

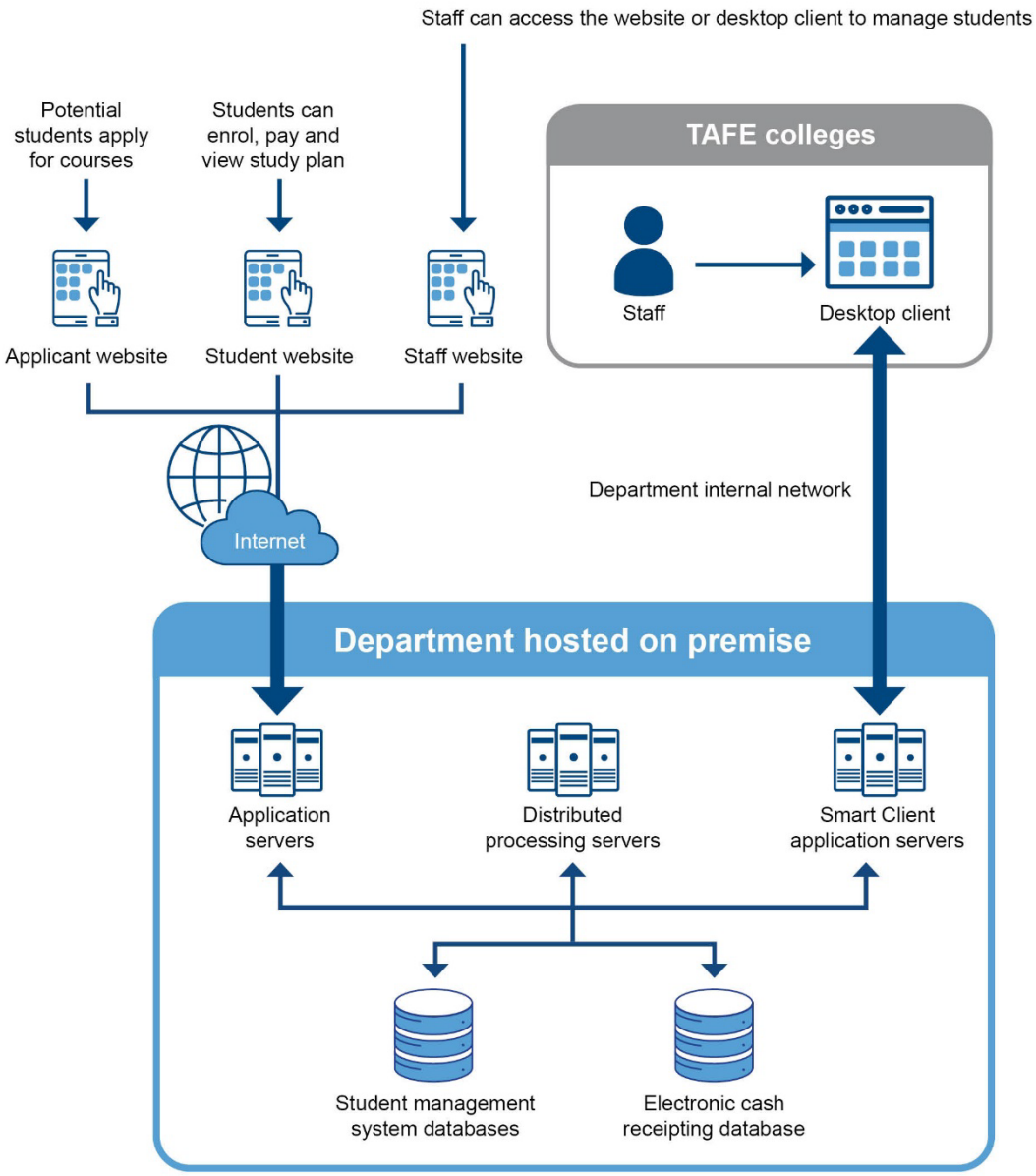
In addition, manual entry of data from other related systems into the System compromises efficiency and data integrity.

Background

The State's vocational education and training sector consists of the Department and 5 independent TAFE colleges. In 2019, TAFE colleges collected over $66 million in student fees and the System was used by almost 4,300 staff providing educational services to over 77,000 students.

Where possible, the Department and TAFE colleges work together to provide cost effective solutions for the entire sector. One example is the Department providing the System as a whole-of-sector student management system to replace the aging Unified Enrolments and Assessment and Results Interface. The System deployment commenced with North Metropolitan TAFE in January 2018, the regional TAFE colleges in June 2018 and remaining in January 2019. All TAFE colleges were using the System by June 2019.

The System provides a modern web-based experience which links to external applications, such as the timetabling system. The System resides in the Department's network and consists of an application and databases which hold all of the information (Figure 12). A third party vendor provides maintenance and System support.



Source: OAG using information from the Department

Figure 12: Student management system overview

Key findings

Inadequate controls mean unauthorised access or data changes may not be detected

The System has good logging and auditing capability, but it is not fully used. The Department, North Metropolitan TAFE and South Regional TAFE did not monitor user activity, nor had they developed policies and procedures to guide what they should monitor. In addition, neither TAFE college had the ability to review audit logs.

Analysis of audit logs could identify inappropriate access to information and changes to records, such as fees or grades. Without appropriate logging and monitoring being defined and configured, the Department and TAFE colleges may not detect unauthorised access or malicious activity.

Better application governance will help the System achieve its intended benefits

We found weak governance processes prevent the Department and TAFE colleges from realising the intended benefits of the System. These benefits include an integrated scalable solution, greater operational efficiencies, meeting strategic priorities, gaining competitive advantage and lower life-cycle costs. We found the following weaknesses:

- **Application governance is not fully established** – the Department has not fully established a governance body to oversee changes to the System and facilitate feedback from TAFE colleges on important issues. Although the Department had plans to establish a governance body, its membership had not been decided at the time of our audit. It is important that this body is established so that expected benefits of implementing the System are realised and system improvements align to TAFE college needs.
- **Inadequate contract management** – the Department has a contract management plan to manage the application vendor's performance, however we found the Department does not manage the contract according to the plan. In particular, the vendor has not met its 6 monthly performance reporting requirements and the Department has not followed this up. We also found that the contract review meetings were held annually rather than 6 monthly as required by the plan. Inadequate contract management increases the risk that the Department will not receive contracted services or be aware of any vendor delivery issues.
- **Service levels are not defined** – the Department has not established a service level agreement (SLA) with the TAFE colleges for services it delivers to support the System. Without defined responsibilities and key performance indicators documented in a SLA, there is greater uncertainty about the services being provided and responsibility for them. This may lead to local workarounds that result in inconsistent practices across TAFE colleges.

Sensitive data is at risk of exposure due to inadequate controls

The System processes and stores student information including bank account details, tax file numbers and personal information such as race and disability. The Department's security controls do not protect the confidentiality and integrity of this information. In particular, we found:

- **Sensitive information is not protected in the database** – we tested the controls for the North Metropolitan and South Regional TAFE databases. We identified the same issues, which are likely to exist for other TAFE databases. The issues are:
    - The databases are not fully encrypted to protect all sensitive information. Bank account details and tax file numbers are encrypted in the database.
    - The databases are not appropriately segregated from users and other systems. We reviewed the Department's firewall and found that all staff in the Department's head office had direct access to the database servers.
    - Access to databases is not appropriately restricted and reviewed. We identified over 80 individuals with 'read' access to both System databases. The Department has since confirmed that the majority of these individuals do not require access.

  These weaknesses compromise the confidentiality, integrity and availability of sensitive information stored in the databases.
- **Data is not de-identified** – the Department regularly copies production System data to test and training databases. We found that personally identifiable and sensitive

information is not appropriately de-identified when the data is copied from production to training and test environments. Having a much wider group of people with access to this information in a less secure test environment increases the risk of information exposure. We found that the Department's security policy requires the de-identification of data when copied between environments, but this does not occur in practice.

- **User access management could be improved** – the Department does not have documented procedures to request, authorise and review privileged accounts within the System. These privileged accounts have the ability to change the System configuration, master data, batch jobs and reports. It is critical that these privileges are managed appropriately to reduce the risk of unauthorised or unintentional modifications to the System.

  In addition, the Department and TAFE colleges do not regularly review System user accounts. This includes accounts that have not been used for a long time (dormant accounts) and the privileges (profiles and roles) that have been assigned to users. Dormant accounts could be used to gain unauthorised access to the System. In addition, if privileges assigned to a user are not regularly reviewed, they can accumulate over time as the individual's role changes. This may lead to unauthorised access to information within the System.

- **Multi-factor authentication is not used** – TAFE staff and students access the System over the internet through the staff and student websites. Multi-factor authentication, where a user has to provide 2 or more pieces of information prior to access being allowed, is not used. Multi-factor authentication reduces the risk of unauthorised access.

- **Weak local passwords** – the System has two ways that it can authenticate user access. The primary method is called 'same sign on' where users enter their username/password, which is authenticated against the Department's active directory. The second method called, 'local authentication', bypasses the active directory. This is where a user enters their username/password, which is verified against a password stored in the System, and can be different from their network password.

  We found that the System does not enforce password requirements for local authentication. In particular:

  - the password configuration does not comply with the Department's policy around password complexity and not reusing passwords
  - the password blacklist is not configured properly. Consequently, we were able to change passwords to well-known blacklisted passwords.

  We found over 30 staff accounts at North Metropolitan and South Regional TAFE that were using local authentication. In addition, students use local authentication during the registration period.

- **Data files are not appropriately restricted** – the System accesses data stored in an external network location called 'Server Folder'. Access/privileges to this external network location are managed within the System rather than the operating system, which is subject to stricter controls. We found that everyone with 'Server Folder' view function had full access privileges to create, read and delete all files and folders. This level of access increases the risk of unauthorised access or modification of information.

- **Weak website configuration** – our review of the System website identified some security weaknesses which increase the risk of unauthorised access or unintentional disclosure of information. We found:

  - the website discloses technical information which may be used by an attacker to identify vulnerabilities in the site

- unused components of the website are enabled, increasing the attack surface which could be exploited by attackers
- the website does not outline terms and conditions for System use, increasing potential for inappropriate access and use of systems.

Students can use the website to pay fees, update personal details, enrol and monitor progress. Staff use the website to manage all aspects of the student experience. If sensitive information is disclosed, it may lead to reputational damage for the TAFEs and adversely affect students.

The Department may not be able to recover the System quickly in the event of a failure

Whilst the Department has a disaster recovery plan for the system, it has not fully tested it by performing a cutover test which involves fully testing recovery systems. The System consists of multiple integrated applications and complex high availability infrastructure. Cutover testing is important in a high availability arrangement to confirm that the environment operates as expected and accurate data is available in the event of a failure.

Further, there is a risk that Department may not be able to fix the System in a timely manner in the event of an incident. This is because the Department has not updated the supporting technologies (operating systems and databases) to meet vendor support requirements. The vendor may require the Department to first upgrade to the supported versions prior to attempting to fix an issue.

The Department has not developed job-scheduling documentation to describe the sequence, timing, dependencies, expected results and error processing steps of scheduled background processing within the System. Without this documentation, the Department will not know if the jobs are executing correctly. As a result, incident resolution could take longer than expected.

A prolonged outage of the System would impact TAFE college operations, especially at critical times such as student enrolment, and affect the student experience. This may result in reputational damage.

Manual process are inefficient and increase the risk of errors

The Department and TAFE colleges perform a substantial amount of manual processing to collate and verify information in the System. We observed data being manually entered into the System, despite existing in other systems. This reduces efficiency and increases the risk of data errors. For example:

- Courses and units are created in the System by importing data from a Commonwealth Government website. After the data is imported, the Department staff manually enter additional information such as course codes and nominal hours. However, as this information already exists in other Department systems, the process could be improved.
- Apprenticeship information is imported into the System from the West Australian Apprenticeship Management System. However, TAFE staff manually enter employer information despite this being available in the Apprenticeship Management System. The Department informed us that manual creation of the employer record is intentional.

We also found that TAFE staff spend a significant amount of time following up with students to obtain information required for Commonwealth and State government performance management and reporting. The System does not enforce this information being recorded during student registration, admission and enrolment. We were informed that TAFE colleges have established this practice to streamline the student entry process.

North Metropolitan and South Regional TAFEs do not conduct adequate reviews of resource fees entered into the System. At both TAFE colleges we found instances where incorrect resource fees were charged to students, requiring the TAFEs to reimburse the student or absorb a financial loss. While the TAFE colleges manually check fees, this may not occur until after enrolment and incorrect fees have been charged to students. Better practice would be to review the accuracy of the fees prior to making the unit available for enrolment.

ICT changes to the System could be better managed

Changes to the System configuration, batch jobs and reports do not follow the Department's change management procedure for review, testing and authorisation. For example, we found changes where the same individual developed and implemented the change into the production environment. Formal change management is an important control where segregation between development and implementation of changes cannot be achieved. If changes are not independently reviewed, tested and authorised there is an increased risk that they may fail, which could affect the availability of the System and impact TAFE operations.

Recommendations

1. The Department should:

   a. in conjunction with the TAFE colleges conduct a risk assessment of the System and implement effective logging and monitoring

      Department response: Agreed

      Implementation timeframe: by April 2021

      The Department of Training and Workforce Development (DTWD) has updated the configuration and new audit trails have been implemented for result processing and financial transaction changes. DTWD will continue to work with the TAFE colleges to expand on the use of audit trails.

   b. establish appropriate governance and vendor management processes

      Department response: Agreed

      Implementation timeframe: by April 2021

      DTWD established a Project Steering Committee during the implementation of the SMS and have since established an ICT Governance Framework as well as an ICT Steering Committee. DTWD have also put practices in place to ensure that contracts are managed in line with the contract management plan. The development of a Service Level Agreement is in progress and is expected to be completed by 31 March 2021.

   c. protect sensitive information in test environments as per its policies. This should include a review of the firewall configuration to limit direct access to the database, and encryption of sensitive information

      Department response: Agreed

      Implementation timeframe: by April 2021

      DTWD has taken appropriate steps to minimise the risk of exposure of sensitive information. As identified in the Summary of Findings, encryption is currently applied to bank account details and tax file numbers and further review will be undertaken to determine the practicality of further encryption. Access to databases has been restricted, student information has been de-identified in the test and training environments and access to server folders has been limited.

   d. regularly test disaster recovery plans and maintain currency of supporting technologies

      Department response: Agreed

      Implementation timeframe: by April 2021

      DTWD tested its Disaster Recovery Plan for the Student Management System (SMS) in March 2020 and the next review of the plan is scheduled for December 2020. DTWD has also updated unsupported platforms to be in line with the vendor's list of supported platforms.

   e. implement effective user access management practices including, where appropriate, multifactor authentication

      Department response: Agreed

Implementation timeframe: by April 2021

TAFE colleges and DTWD have determined that multifactor authentication (MFA) will not be implemented for students due to the potential impact on the business and on students, having regard to existing controls already established. This decision aligns with the guidelines provided by the Office of Digital Government, which recognises the unique circumstances of students (particularly minors) and the practicality of implementing MFA. DTWD is exploring the possibility of MFA being implemented for staff utilising remote access. In addition to this, privileged user access approval has been updated, while increased password complexity will be implemented by 31 December 2020.

f. review manual processes, and where appropriate, implement automated workflows

Department response: Agreed

Implementation timeframe: by April 2021

DTWD is currently investigating the possibility of automated processes for the identified areas of improvement. Ongoing reviews of manual processes will be undertaken to identify where manual processing can be reduced and efficiencies can be gained.

g. ensure System changes are appropriately reviewed, tested and authorised

Department response: Agreed

Implementation timeframe: by April 2021

DTWD has reviewed existing ICT change management processes and all SMS functions are now subject to the change management procedures.

2. North Metropolitan and South Regional TAFE should:

a. in conjunction with the Department, conduct a risk assessment of the System and implement effective logging and monitoring

b. implement effective user access management practices including privileged and dormant accounts

c. implement appropriate data entry reviews to ensure the accuracy of resource fees entered into the System.

North Metropolitan TAFE response to all 3 recommendations: Agreed

South Regional TAFE response to all 3 recommendations: Agreed

Implementation timeframe for all 3 recommendations: by April 2021

Response from the Department of Training and Workforce Development

The Department of Training and Workforce Development (DTWD) acknowledge the findings of the Student Management System (SMS) audit. It should be noted that the audit commenced over 12 months ago and the majority of the findings have since been actioned. Further work is being conducted to address the remaining findings.

DTWD considers it has taken appropriate steps to minimise the risk of exposure of sensitive information and has suitable controls in place to manage this risk. DTWD successfully tested its Disaster Recovery Plan for SMS in March 2020.

Response from North Metropolitan TAFE

In response to the audit findings North Metropolitan TAFE has updated the process for user access to ensure all access reviews are stored in the record management system and are signed off/dated when the access review has been completed. All changes and approvals to user access are recorded in the service management system. User accounts are reviewed on a monthly basis, utilising the information from Human Resources monthly reports which lists changes in staff employment statuses e.g. commencements, higher duties, terminations, and changes in contract expiry which will affect access. Additionally a quarterly review has been implemented to review user accounts to ensure users have the most appropriate user profile assigned for their employment position. NMT is working with DTWD to increase access to a higher level of audit trails and to review an increase the number of audit logs that are available.

The College has undertaken a review to ensure appropriate reports are available to administration staff working within the limitations of the SMS system. A training and refresher program has been instituted to ensure administration staff are trained and aware of the importance of data accuracy. In addition to these measures, the SSS team will do a quarterly review via a random sample of (>100) student enrolments to ensure processes are being followed correctly and to further identify where training needs are required.

Response from South Regional TAFE

1. South Regional TAFE will work with DTWD to develop policies and procedure for guidance with regard to logging and monitoring. In conjunction with DTWD the college will define and implement logging and monitoring processes to provide adequate controls for oversight of unauthorised access or data changes.

2. South Regional TAFE has implemented centralized user access management. User access is reviewed on a regular basis to remove dormant accounts and levels of access are determined and approved by appropriate line management.

3. South Regional TAFE has implemented a resource review system to ensure data entry errors are identified prior to the unit being available for enrolment.

Auditor General's 2021-22 reports

Number	Title	Date tabled
15	Opinions on Ministerial Notifications – Tax and Funding Information Relating to Racing and Wagering Western Australia	26 February 2021
14	Opinion on Ministerial Notification – Hotel Perth Campaign Reports	24 February 2021
13	Opinion on Ministerial Notification – Release of Schedule of Stumpage Rates	24 February 2021
12	Grants Administration	28 January 2021
11	COVID-19 Relief Fund	21 December 2020
10	COVID-19: Status of WA Public Testing Systems	9 December 2020
9	Western Australian Registry System – Application Controls Audit	26 November 2020
8	Regulating Minor Pollutants	26 November 2020
7	Audit Results Report – Annual 2019-20 Financial Audits of State Government Entities	11 November 2020
6	Transparency Report: Major Projects	29 October 2020
5	Transparency Report: Current Status of WA Health's COVID-19 Response Preparedness	24 September 2020
4	Managing the Impact of Plant and Animal Pests: Follow-up	31 August 2020
3	Waste Management – Service Delivery	20 August 2020
2	Opinion on Ministerial Notification – Agriculture Digital Connectivity Report	30 July 2020
1	Working with Children Checks – Managing Compliance	15 July 2020

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
F: 08 6557 7600
E: info@audit.wa.gov.au
W: www.audit.wa.gov.au

@OAG_WA

Office of the Auditor General for
Western Australia