[P.P.4R

Government
of South Australia

Report

of the

Auditor-General

Supplementary Report

for the

year ended 30 June 2016

Tabled in the House of Assembly and ordered to be published, 20 October 2016

Second Session, Fifty-Third Parliament

RevenueSA Information Online system: October 2016

By authority: P. McMahon, Government Printer, South Australia

2016

General enquiries regarding this report should be directed to:

Auditor-General
Auditor-General's Department
Level 9
State Administration Centre
200 Victoria Square
Adelaide SA 5000

Website: www.audit.sa.gov.au

ISSN 0815-9157

Government of South Australia
Auditor-General's Department

Level 9
State Administration Centre
200 Victoria Square
Adelaide SA 5000
DX 56208
Victoria Square
Tel +618 8226 9640
Fax +618 8226 9688
ABN 53 327 061 410
audgensa@audit.sa.gov.au
www.audit.sa.gov.au

19 October 2016

The Hon R P Wortley MLC
President
Legislative Council
Parliament House
ADELAIDE SA 5000

The Hon M J Atkinson MP
Speaker
House of Assembly
Parliament House
ADELAIDE SA 5000

Dear President and Speaker

Report of the Auditor-General: Supplementary Report for the year ended 30 June 2016: RevenueSA Information Online system: October 2016

As required by the *Public Finance and Audit Act 1987*, I present to each of you my Supplementary Report for the year ended 30 June 2016 'RevenueSA Information Online system: October 2016'.

Content of the Report

Part A of the Auditor-General's Annual Report for the year ended 30 June 2016 referred to audit work that would be subject to Supplementary reporting to Parliament. In 2015-16 we reviewed the Department of Treasury and Finance's RevenueSA Information Online system to assess the effectiveness of IT processes and security controls. This Report outlines our findings and remediation recommendations, and the Department of Treasury and Finance's planned remediation responses.

Acknowledgements

The audit team for this Report was Andrew Corrigan, Brenton Borgman and Tyson Hancock.

I also express my appreciation for the cooperation and assistance provided by Department of Treasury and Finance staff during the audit.

Yours sincerely

Andrew Richardson
Auditor-General

Table of contents

RevenueSA Information Online system (RIO): October 2016

1 Executive summary 1
- 1.1 Introduction 1
- 1.2 Audit conclusion 1
- 1.3 Summary of key system improvements 2
- 1.4 Summary of key audit findings 2
- 1.5 Department response 4

2 Background 5
- 2.1 RevenueSA Information System to Enable Compliance implementation project 5
- 2.2 RIO system functionality 5
- 2.3 Previous IT audit findings on RIO information technology operational controls 7

3 Audit objective and scope 8
- 3.1 Objective 8
- 3.2 Audit scope 8

4 IT application controls 9
- 4.1 Introduction 9
- 4.2 Validation approach 10
- 4.3 Inadequate reconciliation controls with the general ledger 10
- 4.4 Insufficient controls to restrict access to create and modify land parcel data in RIO 12
- 4.5 Billing set information in RIO can be generated and amended without formal approval 12
- 4.6 Undetected changes to bank statements can be made 13
- 4.7 Insufficient data matching of land information data uploads to RIO 14

5 IT change management controls 15
- 5.1 Introduction 15
- 5.2 Validation approach 16
- 5.3 Inadequate change management processes existed 16
- 5.4 Insufficient security management of the test environment and personal testing data 17
- 5.5 Irregular implementation of RIO operating system, application and database patching 18

6 IT system monitoring and maintenance controls 20
- 6.1 Introduction 20
- 6.2 Validation approach 21
- 6.3 Inadequate supporting documentation 21
- 6.4 RIO system access can bypass application level controls 22
- 6.5 RIO system database audit logging is not activated 23
- 6.6 Lack of internal technical expertise 23

Table of contents

7 IT system security design controls 25

7.1 Introduction 26

7.2 Validation approach 26

7.3 Inadequate global systems change option and client settings 26

7.4 Inappropriate security access, including emergency access 27

7.5 Inadequate controls over default user access 29

7.6 Inappropriate access to production clients 29

7.7 Insufficient security restrictions and ongoing review of customised transaction code programs 30

7.8 Company codes settings may allow data to be incorrectly deleted 31

7.9 User master records were inconsistent and poorly managed 31

7.10 Inadequate management of SAP[1] roles within RIO 32

7.11 Inappropriate database configurations 33

8 IT user access management controls 34

8.1 Introduction 35

8.2 Validation approach 35

8.3 Inconsistent assignment of new user access 35

8.4 No process to manage segregation of duty conflicts 36

8.5 Insufficient user access reviews 37

8.6 Excessive use of a shared privileged database account 37

8.7 Inappropriate privileged user access on SAP production servers 38

Appendix 1 – Overview of RIO SAP modular based system 39

Appendix 2 – Glossary 40

[1] Systems, Applications and Products (SAP). The application software is from the German software company SAP SE, which develops enterprise software to manage business operations and customer relations.

1 Executive summary

1.1 Introduction

The Department of Treasury and Finance (DTF) is the lead agency for the collection of State taxes exceeding $3 billion[1] p.a. Principal revenue taxes include payroll, land, and the fixed property component of the Emergency Services levy (ESL). All of these taxes are subject to an Act or regulatory requirement.

DTF uses taxation revenue management systems to assist in the collection of these State taxes. One is the RevenueSA Information Online system (RIO). RIO has replaced components of RevenueSA's legacy taxation system, which operated for nearly 20 years. RIO was designed and built as part of the RevenueSA[2] Information System to Enable Compliance (RISTEC) project.

RIO was originally intended to be deployed via the RISTEC project in a series of releases. Release 1 focused on the base SAP system[3] and payroll tax. Release 2 incorporated land tax and the ESL. A proposed Release 3 was intended to add stamp duties and sundry taxes. Due to system problems, this release was dropped from the RISTEC project.

Throughout the life of the RISTEC project we have conducted a number of reviews, which have been communicated in previous Reports to Parliament. In particular, we reported that the project experienced several delays, ongoing costs increased and some expected benefits were lost through the ongoing use of legacy systems.

Releases 1 and 2 are now complete, but the collection of stamp duties and sundry taxes remains on RevenueSA's legacy taxation system. At this stage, no decision has been made about migrating these functions to an alternate revenue management system.

In 2015-16 we reviewed RIO to assess the effectiveness of IT processes and security controls. Given RIO's size and complexity, we engaged an external audit firm to assist our review.

This Report outlines our findings and remediation recommendations, and DTF's planned remediation responses.

1.2 Audit conclusion

Collecting State taxes is fundamental to the State's financial activities. It is essential that the systems used to manage the collection of taxes have satisfactory controls.

We assessed that the controls operating for RIO were insufficient for the system's purpose. Although we have been advised that a number of positive revised practices have recently been established across the RIO system environment, our review identified numerous IT control matters that need to be addressed. In particular, we identified deficiencies in application controls, change management, system monitoring and maintenance, system security design and user access management. Some of these control matters were originally identified in our 2012-13 review.

---

1 2016-17 State Budget Statement, chapter 3, page 36.

2 RevenueSA is a division of the Department of Treasury and Finance.

3 SAP is an acronym for Systems, Applications and Products. The application software is from the German software company SAP SE, which develops enterprise software to manage business operations and customer relations.

These RIO system control deficiencies could have a significant financial impact to the State by affecting revenues generated from specific taxes and levies. This risk arises where controls do not sufficiently address or detect risks of unauthorised, invalid or incorrect transactions or system changes. These control deficiencies can also impact the confidentiality, integrity and availability of the data on the system, which includes sensitive customer data.

Given the importance of this system to the State and the potential risks associated with these control deficiencies, prompt remediation of these matters is paramount. We note DTF's positive response to our findings and recommendations, and the interim remediation measures already applied will help address these risks.

1.3 Summary of key system improvements

RevenueSA advised that a number of positive revised practices have been established across the RIO system environment. They included remediating some control weaknesses identified in our 2012-13 review of RIO Release 1.[4]

Our review has not validated these advised improvements.

The significant developments/improvements advised by RevenueSA included:

- Release 2 ESL and land tax property functionality successfully implemented in July 2015
- successfully issuing over 650 000 ESL and land tax notices of assessment for 2015-16
- automation of approvals/delegations via rules and workflows within RIO
- establishing problem management processes for RIO for effective tracking and prioritisation of issues identified
- a disaster recovery process that considers business requirements to recover RIO within an agreed period
- ongoing remediation of identified defects in RIO operational functionality, in consultation with support service providers
- advancements in the proposed system patching upgrade strategy and implementation of an alternate testing environment as part of that upgrade
- further developments in operational production and application functional support, in consultation with system service providers.

1.4 Summary of key audit findings

Our 2015-16 review of RIO identified numerous control weaknesses. It also confirmed that a number of matters raised in our 2012-13 review continue to require management attention.

The following is a summary of key findings that require remediation.

[4] At the time of our 2012-13 review the implementation of Release 2 was still in progress.

IT application control findings

- Data transferred into RIO is not appropriately matched and validated.
- Excessive user account access exists, which allows the creation, modification and deletion of key data without review.
- The detailed reconciliation process had limited supporting documentation, was heavily reliant on a key accounting staff member, and at the time of our review was nine months behind schedule.

IT change management control findings

- Inadequacies exist in change management processes.
- There is insufficient protection of sensitive data, and inadequate audit logging and controls over user test accounts within the testing environment.
- RIO operating system, SAP application and database security patches have not been regularly applied.

IT system monitoring and maintenance control findings

- Procedural, user and system documentation needs updating.
- Audit logging is not enabled at the database level.
- Inadequate technical expertise at the agency level has resulted in a high reliance on external service providers.

IT system security design control findings

- Insufficient formal processes exist to manage critical security access controls or activities within the SAP production environment.
- Excessive access exists through the continuing use of generic accounts, unregulated user and role administration functions, and the ability to update key master data tables.
- Default user accounts are insufficiently configured and user master records are inconsistent and poorly managed.

IT user access management control findings

- Methods used to assign access differ between business access and SAP Basis access.
- No segregation of duties process currently exists.
- No review of segregation of duties and privileged access occurs.
- No documented procedures define the roles and responsibilities for performing a user access review.

- The SAP Basis team has super user access rights through shared service accounts that access the RIO system database.

- Unnecessary user accounts exist on the servers that host RIO.

Sections 4 to 8 detail our review findings and associated recommendations.

We were advised that although many of these control deficiencies were previously known, RevenueSA resources have been focused on addressing other key activities. In particular, finalising implementation of RIO's in-scope functionality, readying the system for its annual invoicing cycle and preparing to upgrade the application's software to maintain support warranty provisions have been priorities. We acknowledge these were important activities. This has, however, been to the detriment of strengthening RIO system controls.

1.5 Department response

DTF has positively responded to all findings and recommendations raised in this Report.

We note that in most cases, DTF is unable to fully address our recommendations until a code freeze[5] applied to the system (as part of an upgrade project) is completed. DTF has advised that, once the code freeze ends, appropriate changes will be scheduled, with many recommendations addressed by the end of December 2016. In the interim, some preliminary control measures have been applied to partially mitigate some risks.

DTF's responses are contained in sections 4 to 8.

[5] A code freeze is when program changes to the system are suspended at a point in time. This is usually performed to help preserve system stability and/or reduce unintended performance issues.

2 Background

2.1 RISTEC implementation project

RevenueSA advised that revenue collected through payroll and land tax and the fixed property component of the ESL represented approximately 19% of total general government sector revenue generated in 2015-16. This revenue was previously collected through a legacy taxation system that had been in place for nearly 20 years. Given the importance of this revenue collection process it was deemed critical to replace the legacy taxation system.

The RISTEC project to implement the replacement taxation system commenced in July 2002, with Cabinet approving an initial budget of $22.6 million. The purpose was to develop a system, referred to as RIO, that could effectively and efficiently collect taxes, levies and duties owed to South Australia.

Following the procurement process, in May 2008, Cabinet approved a budget for the RISTEC project of $45.5 million covering both capital and operating costs.

Implementation was intended to be deployed in a series of releases. Release 1 focused on the base SAP system and payroll tax. Release 2 incorporated land tax and the ESL, and a proposed Release 3 was intended to add stamp duties and sundry taxes.

A number of scope changes, problems and delays occurred throughout the project, which resulted in amendments to the required budget. Key scope changes included:

- the implementation of the ESL into Release 2, which was not part of the initial project cost
- $2.4 million for new government initiatives, which was also not part of the initial project cost
- the removal of Release 3 (stamp duties and sundry taxes).

As a result, in July 2012, Cabinet was informed that the revised estimated cost of the project was $48.8 million.

In 2015 the project was closed. DTF advised that the final project cost was $55.8 million.[6]

2.2 RIO system functionality

RIO processes taxation transactions for payroll and land tax and the fixed property component of the ESL. To assist in this process, DTF is provided with data from other government agencies and employers.

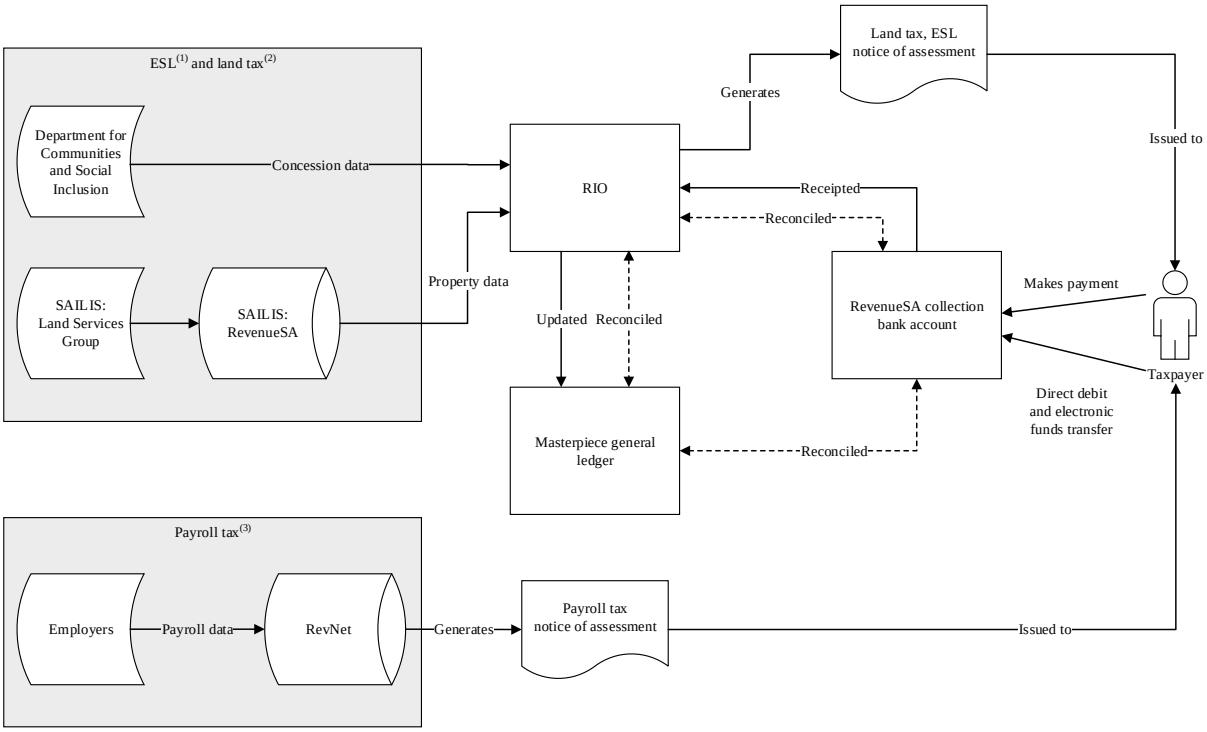
Most access to RIO is through the RevNet[7] website portal (external users) or through a SAP portal for internal office and support staff. For further details specific to the RIO SAP modular based system refer to Appendix 1.

---

[6] The cost of implementing a solution for stamp duties and sundry taxes will need to be factored into any future project.

[7] RevNet is an internet based system that is intended to provide an easy, flexible and more effective way for clients to do business with RevenueSA.

The following diagram shows the process and generation of tax and levy revenue.



The data input process for each tax and levy is as follows:

(1)(2) ESL and land tax: Data is provided from the South Australian Integrated Land Information System (SAILIS), managed by the Land Services Group within the Department of Planning, Transport and Infrastructure (DPTI). This data confirms the land valuations associated with parcels of land. In addition, concession information is provided by systems within the Department for Communities and Social Inclusion.

(3) Payroll tax: Employers provide details of the wages they pay throughout the year through the RevNet website managed by DTF. This web portal transfers the payroll information into RIO.

The calculation process for each tax and levy is as follows:

(1) The ESL is a levy on all land to help fund emergency services across South Australia. The levy is calculated in accordance with the ownership and capital value of land on 1 July each year.

(2) Land tax is applied against the land ownership and site value (not capital value). It is calculated by applying a progressive rate structure to the total taxable site value of all land owned (by an owner or a group of owners). The tax is calculated as at 30 June of each year to determine the land tax for the next financial year.

By applying the respective tax rate against the value of a parcel of land, DTF generates invoices for both the ESL and land tax, which are sent to each property owner. Each invoice is adjusted for any specific tax exemptions, remissions or concessions.

(3) Payroll tax is calculated on wages paid or payable when an employer's (or group of employers') total Australian wages paid exceeds the South Australian threshold (currently $600 000). This tax is collected and administered in accordance with the *Payroll Tax Act 2009*. Employers provide details of the wages they pay throughout the year and submit their payroll tax where applicable. An annual return and reconciliation at year end confirms the total wages that are subject to payroll tax.

Each tax and levy is raised through either paper based or electronic transactions. Once received the revenue is reconciled to RevenueSA's bank account and then further reconciled between RIO and DTF's Masterpiece general ledger.

2.3 Previous IT audit findings on RIO information technology operational controls

In 2012-13 we reviewed the IT controls for Release 1 of RIO, the payroll tax module. At that time, Release 2 functionality had not been implemented.

Despite finding some positive control arrangements in place at that time, our 2012-13 review highlighted a number of concerns, including:

- operational support teams needed access functions segregated
- application log monitoring and system reporting needed to improve
- operating system logging needed to be strengthened
- reliance on Fujitsu technical expertise
- control deficiencies within RevNet
- SAP security patching was reactive not proactive
- controls over generic administrator accounts needed further tightening
- no internal security assessment of RIO had been performed or was planned
- some procedure and system documentation was incomplete or outdated
- weak SAP password configuration controls existed.

We noted that any control breakdowns experienced as a result of these deficiencies could have a significant financial impact to the SA Government and taxpayers. We therefore recommended prompt remediation.

3 Audit objective and scope

3.1 Objective

The objective of our 2015-16 review was to follow up issues previously identified in our 2012-13 operational controls review. We also assessed RIO's operational IT security controls (application and general), and system business and exception rules within RevenueSA.

3.2 Audit scope

Our review involved selected testing of:

- IT application controls for specific business processes, including revenue and general ledger audit cycles
- IT general controls and other information security aspects. This included change management, user access management, password configuration, selected application controls, backup and disaster recovery, problem and incident management, patch management and operating system and database security. Where applicable, this testing also validated any remediation of the issues raised in our 2012-13 review
- the system business and exception rules.

This review did not assess the effectiveness of RevenueSA's financial controls, which are reviewed annually through the audit of DTF and reported on in Part B of the Annual Report of the Auditor-General for the year ended 30 June 2016.

4 IT application controls

Summary of key findings

Our 2016 review of application controls identified significant deficiencies that need to be corrected/remediated.

Application control deficiencies identified included:

- data transferred into RIO from DPTI SAILIS is not appropriately reconciled and validated and may be incomplete or inaccurate
- user account access within RIO gives some users the ability to:
  - create and modify land parcel data used to generate SA Government revenue
  - delete bank statement data without activity logging or periodic review
  - generate and amend billing sets[8] without review or formal approval
- the current reconciliation process is heavily reliant on key accounting staff, with limited formal documentation to support established processes
- the detailed reconciliation process for the financials was nine months behind schedule at the time of our review, which increases the potential for misstatement within the general ledger.

Summary of key recommendations

Remediation of these control deficiencies is needed to ensure that revenue generated through specific taxes and levies in RIO is accurately raised and safeguarded. This can occur by:

- establishing reports and processes to confirm the completeness and accuracy of data uploaded into RIO
- reviewing the adequacy of system access segregation and alignment with job roles and business functions/rules. This includes revoking a user's ability to both manually create and modify billing sets, land parcels and bank statement data
- establishing formal monitoring controls that help to detect unauthorised changes
- ensuring that the formal reconciliation process is documented and performed promptly.

4.1 Introduction

Our review of RIO assessed the adequacy of the established IT application controls applied to the system. IT application controls incorporate controls over data input, data processing and data output.

Data input controls seek to confirm the accuracy of data entered into a computer application through computerised validation, data audit logging and error handling procedures. Input controls should also ensure that data entered into the application is authorised and suitably approved.

[8] Billing sets are groups of customers that are billed at the same time.

Data processing controls seek to ensure processing is complete and accurate through batch or real-time processing. They should check that no data is inadvertently added, lost or altered during general processing. They should also identify instances of unusual or unauthorised activity, errors encountered, and where corrective action is required through exception reporting.

Data output controls seek to ensure sufficient segregation of duties and the integrity and correctness of any output data processed.

If sufficiently applied within RIO, these IT application controls ensure the complete and accurate generation, receipt and processing of certain government taxes and levies. If not sufficiently applied, however, the SA Government may lose revenue through inaccurate revenue invoices being generated, receipted and processed into RevenueSA's general ledger.

4.2 Validation approach

To test IT application controls within RIO, we interviewed key staff and examined key application policies and procedures. We also assessed the access privileges relevant to the application controls within RIO. This included testing certain system input, processing and output procedures relative to key business rules, and exception reports that support key monitoring controls.

Our assessment of the IT application controls focused on:

- the appropriateness of segregation of duties between the receipting, banking, invoicing, debtor follow-up and general ledger functions
- the appropriateness of restrictions on access to key system functions and charts of accounts
- the appropriateness of generated invoices raised and their formal approval
- confirming that changes to tax/levy data are valid and approved
- confirming that data transferred between the tax/levy revenue system, general ledger and bank is complete, accurate, regularly reviewed and cleared (where applicable)
- confirming that cash account balances are regularly reconciled and independently reviewed.

The following sections summarise the findings from our IT application control testing.

4.3 Inadequate reconciliation controls with the general ledger

Recommendations

DTF should:

- ensure reconciliation controls are documented and are being performed promptly to detect incomplete journal extracts. The reconciliation should be performed between RIO and the Masterpiece[9] general ledger. Key transaction mapping rules and filters should also be taken into account

[9] Masterpiece is an accounts payable system used throughout most SA Government agencies.

- perform an overarching reconciliation between the Masterpiece general ledger and the subledger
- investigate opportunities to automate reconciliation activities
- perform additional testing over mapping rules.

Findings

Cash transactions are extracted daily into the Masterpiece general ledger using a series of mapping tables. The mapping tables define the specific combination rules to allocate transactions to the Masterpiece general ledger. Where a transaction is not correctly mapped, it could be excluded from the data extract, and could remain undetected until a manual reconciliation between the extract and cash transactions is performed.

A reconciliation is performed between RIO and the Masterpiece general ledger to ensure the completeness and accuracy of the general ledger interfaces. Although this is a sound process for ensuring that all the data is accounted for, there were some limitations noted at the time of our review. In particular:

- the reconciliation process was manually performed and reliant on a senior accounts officer, with limited supporting documentation available. Under this arrangement there was significant reliance on the senior account officer's knowledge and understanding of the process, increasing the risk of process failure
- at the time of the review, the detailed reconciliation process was nine months behind and therefore could not be used as a control for ensuring that data transfers were completed and correct
- there was no overall reconciliation being performed between RIO and the Masterpiece general ledger.

These reconciliation deficiencies could lead to incomplete journal transfers and misstatements in the general ledger not being detected.

Department response

Monthly reconciliations are ongoing, however RevenueSA agrees that further consideration and investigation is warranted to refine this process going forward.

A review of financial reconciliation processes will occur during the code freeze (depending on the upgrade project currently in progress, likely to be completed in December 2016). It is intended that this review will involve external expertise in SAP financials and reporting where possible to explore standard SAP capabilities in this area. Any system changes associated with a revised reconciliation methodology will be considered and implemented after completion of the upgrade project as a matter of priority.

Short-term changes to remove some reconciliation effort have also been implemented since our review.

4.4 Insufficient controls to restrict access to create and modify land parcel data in RIO

Recommendations

DTF should:

- revoke all access/ability to manually create land parcels in RIO
- review the security framework to ensure that all assigned access is in line with each user's job role and RevenueSA's business functions
- review and update the business rules to align with the current practices.

Findings

Creating land parcels in RIO is based on a daily file containing land data from DPTI. This file is automatically uploaded into RIO to prevent manual handling of the data transfer.

Our review noted that user access is not being updated to reflect this automated business rule. Over 30 users currently have unnecessary access to create and modify land parcel data. This access is not aligned with the defined business rules.

Excessive user access to manually modify land parcel data increases the risk of invalid land tax and ESL transactions being processed.

Department response

The ability to amend land parcel data is essential to day-to-day business activities. Field level access restrictions are implemented to restrict amendments of higher risk fields to the Property Data Manager security role only.

The ability for authorised tax officers to manually create a land parcel in RIO was a base requirement of business. Access restrictions were contained within the system to allow the creation of a land parcel to the Property Data Manager security role only. This access is to be reviewed as part of an overarching security review to be undertaken after the code freeze (depending on the upgrade project currently in progress, likely to be completed in December 2016). Changes to security access can then be implemented. This will include any alignment of related business rules.

4.5 Billing set information in RIO can be generated and amended without formal approval

Recommendations

DTF should:

- review all composite roles in RIO to ensure that a property data management role is not assigned
- restrict the ability of the property data management role to edit billing set information on exception.

Findings

Our review of the user access rules indicated that a property data management role within RIO has access to manually trigger the generation of mass billing as well as to edit generated billing sets. The updates include changing the billing business name or date.

At the time of our review, around 30 people had been indirectly assigned this role. The risk associated with changes to billing sets is increased as the process for generating billing sets in RIO is not subject to review and approval outside of the annual mass billing process.

Access to generate and modify billing sets without requiring a review or approval process increases the risk of fraudulent or erroneous modification of billing sets.

Department response

The ability to modify billing sets is required to ensure that the number of notices of assessment (which reflect pending tax liability) issued in each billing set is manageable in terms of taxpayers' contact (eg phone calls/correspondence received from taxpayers).

The ability to modify billing sets does not enable a taxpayer to be excluded from receiving a notice of assessment.

A review/approval process will be implemented by the end of June 2017 in time for next year's billing and invoicing.

4.6 Undetected changes to bank statements can be made

Recommendations

DTF should:

- restrict user access to prevent bank statement data from being modified
- establish appropriate monitoring controls to detect unauthorised changes to bank statements.

Findings

Bank statement data is uploaded to RIO to enable bank reconciliations to be performed. We found that the Revenue Accounting team is able to delete line items from the uploaded bank statement data within RIO. Changes made by either the Revenue Accounting or Functional Support teams are not logged or monitored.

The ability to make undetected changes to bank statement data increases the risk of reconciling items being inappropriately deleted.

Department response

Security access for Revenue Accounting staff will be removed and any manual processing of bank statements will only be done by the Functional Support team under the segregation of duties process. This will be actioned immediately.

A security review will also be conducted to ensure roles are appropriate for current business processes and responsibilities. This review is to be undertaken during the code freeze (depending on the upgrade project currently in progress, likely to be completed in December 2016). Once the code freeze ends, changes to security access can be scheduled. This will include any alignment of related business rules.

4.7 Insufficient data matching of land information data uploads to RIO

Recommendation

DTF should implement data matching reports to confirm that data uploaded into RIO from DPTI's SAILIS application is complete and accurate.

Finding

Data received from the daily DPTI SAILIS application file is reconstructed into a file that can be uploaded to RIO. There is no data matching performed between the data received electronically from DPTI and the data processed into RIO.

Lack of data matching increases the risk of interface errors (or file transfer errors) not being detected. This could potentially lead to incorrect invoicing and notices of assessment (which reflect pending tax liability).

Department response

To ensure successful provision, transformation and processing of SAILIS data uploads, a data matching reconciliation has been implemented. This matching occurs across three databases:

- DPTI database (source of SAILIS data)
- DTF Internal SAILIS Composite database (transforms DPTI data to data prepared for processing in RIO)
- RIO database (processes transformed DPTI data).

Data matching is currently undertaken on selected data fields that directly impact liability calculation.

This reconciliation will occur at critical times over the property tax lifecycle to minimise data discrepancies in preparing to issue notices of assessment. It is also envisaged that the data matching process will include all fields received from DPTI in a financial year.

Significant test effort has focused on ensuring that rules triggered upon processing of transactions received via the SAILIS data upload were correct.

5 IT change management controls

Summary of key findings

Our review of change management controls identified that an established business process existed for reviewing change logs in the revenue module. Despite this, a number of areas associated with the change and release management process had weaknesses including:

- inadequate processes for verifying approved changes
- excessive opportunity to make unauthorised changes direct into the production environment
- insufficient protection of sensitive data during Quality Assurance (QA) testing
- lack of audit logging within the QA environment
- failure to establish formal user test accounts within the RIO test environment. This creates the potential for testers to have full user access to displayed end user menu options and sensitive data within the test environment
- a series of operating system SAP application and database security patches that have not been applied.

Summary of key recommendations

Remediation of these control deficiencies is required to ensure that RIO change management processes do not affect the integrity of its day-to-day operations.

This can occur by:

- establishing a formal change process that restricts direct changes into the production environment
- considering extending the existing security management plan to cover data management in the QA environment
- providing an audit trail of user activity during testing
- ensuring system patches are applied promptly.

5.1 Introduction

RevenueSA had applied a software code freeze of certain aspects of RIO between 2012 and 2016. This was to stabilise the system while each system module was developed and put into production.

At the time of our review, RevenueSA was attempting to apply many of the required software code changes, such as overdue system patches, that were not applied during the software code freeze.

Using effective IT change management controls is important when applying system changes to RIO. Types of system changes include application, hardware, software, network and environmental changes.

IT change management seeks to ensure that all changes to the RIO environment are assessed, approved, implemented and monitored in a controlled, standardised way to preserve the integrity of underlying programs and data. All changes should be tracked through a change management system.

Implementation of any changes should also occur through a controlled and clearly segregated approach. This will help to ensure that sufficient testing and approval has occurred before the changes are migrated into the RIO production[10] environment.

Failure to implement effective IT change management could impact the integrity of RIO's day-to-day operations, increase incidents of system failure, and increase the potential for revenue miscalculation and reporting within the underlying financial system.

5.2 Validation approach

To test RIO change management, we interviewed key staff, examined key change management policies and procedures and reviewed the RIO system change register. We also assessed the segregation of the RIO environments and user access relating to a defined range of RIO system changes.

Our assessment of change management and patch management focused on whether:

- changes were appropriately documented to minimise the likelihood of disruption, unauthorised alteration and data error within the RIO production environment
- the change management system provided for the analysis, implementation and follow-up for all changes raised. Also only authorised changes were migrated to the production environment once satisfactorily tested and documented
- the integrity of the patch management and upgrade strategy was adequate to safeguard and avoid potential risk or loss of data or revenue
- system changes to the production environment had undergone sufficient user acceptance testing and met all documented requirements before being implemented.

The following sections summarise the findings from our IT change management control testing.

5.3 Inadequate change management processes existed

Recommendations

DTF should:

- restrict transport[11] update access to designated personnel with the defined job function for the release of changes into production (eg SAP Basis team or change release team)
- implement a formal process to ensure that only approved changes are released into the production environment by comparing system updates to authorised system changes. This can be achieved by extracting system updates via defined tables and comparing the list of updates to approved changes after every release cycle

[10] A production environment is where an organisation's day-to-day operational programs are run in real-time rather than as part of a test or development scenario.

[11] Transport is a package within the RIO SAP system that is used to transfer data, and provide enhancements or new developments of existing business functions from development to production.

- enforce a fixed dialogue window for transporting changes into the production environment as part of a sound change management process.

Findings

We found the following shortcomings in the RIO change management process:

- direct transport update access was available to many users in the production environment, increasing the risk of unauthorised transports of changes into RIO
- there was no process to verify that only approved changes were released into the production environment
- transport updates were not always applied through specified and approved dialogue windows.

Inadequate change management controls increase the risk of undetected and/or unauthorised changes in production, which could result in reduced system integrity. Additionally, not adhering to approved change management scheduling timeslot could negatively impact other business processes.

Department response

A daily and monthly documented transport reconciliation process has been applied to the production environment. This was introduced to decrease the risk of undetected and/or unauthorised RIO changes and to ensure only authorised changes have been applied in the approved timeslot.

The following change management controls will be introduced to reduce the risk of undetected and/or unauthorised changes in the RIO production environment:

- On completion of an internal user access review project, established managed roles will be assigned to new user access requests, with tracking controls permanently activated.
- A direct table update reconciliation process will be established to be run both daily and monthly. This will ensure only authorised direct table updates have been applied to the production environment, within each update's authorised change window.

These changes will be undertaken after the successful completion of the SAP upgrade, expected to be December 2016.

5.4 Insufficient security management of the test environment and personal testing data

Recommendations

DTF should consider extending the RIO system security management plan to cover data management in the SAP QA environment. This plan should include:

- appropriate identification of critical and personal data that needs to be scrambled[12] in the QA environment

[12] Data scrambling involves making data unintelligible or removing sensitive data.

- the use of dummy data for testing and other verification purposes where appropriate.

DTF should also consider establishing a set of generic user accounts to be used during user acceptance testing. Where testing includes access to sensitive data, DTF should capture details of the tester and the session time being used to provide an audit trail of user activity. This may discourage the inappropriate use of sensitive data during testing.

Findings

Production environment data and functionality is replicated into the QA environment. We noted that this replication process does not scramble sensitive data (such as concession details). We also noted that audit logging is not enabled in the QA environment.

RISTEC project users were required to perform user acceptance testing on behalf of end users. As part of that process, the end user's password was reset in the test environment and provided to the testers. Testers then have full access to the user's menu items and sensitive data in the RIO test environment.

Inappropriate access to sensitive production data in the QA environment increases the risk of unauthorised users being able to view and extract sensitive information that could be used for unauthorised access to RIO.

Department response

DTF staff are bound by the *Public Sector Act 2009* and the Code of Ethics for the South Australian Public Sector in relation to the disclosure of public information within and outside their employment. Any breach of the Code of Ethics is subject to disciplinary provisions. In addition, RevenueSA staff are bound by the *Taxation Administration Act 1996* which prohibits the disclosure of any information obtained under or in relation to the administration of a taxation law (other than for a prescribed purpose).

Regarding scrambling data in the RIO test systems, DTF acknowledges the potential for access to sensitive data. However, this needs to be balanced against the need to ensure the testing of software changes or defect corrections is robust and will not compromise the integrity of the notice of assessment against the taxpayer when the solution is deployed into production. DTF will consider if an acceptable approach can be designed that both ensures adequate testing but also limits user access to confidential taxpayer information.

5.5 Irregular implementation of RIO operating system, application and database patching

Recommendation

DTF should ensure that system patches[13] are promptly applied for operating systems, application and databases.

Finding

During RIO's development and following implementation of Release 2 there was a freeze on patching its operating system, SAP application and databases.

[13] A software patch is a piece of software that is designed to fix defects or vulnerabilities, or provide updates to an information system.

We found a number of operating system, SAP application and database security patches that were not applied. We were advised that a project was underway to upgrade the patching software for the RIO operating system, SAP application and database servers, with an estimated completion date of October 2016.

The lack of up-to-date software system patching increases the risk of security attacks, application loss and loss of vendor's system warranty and support.

This finding was previously raised in our 2012-13 review.

Department response

DTF undertakes patching of all servers (including those supporting RIO) monthly, where the latest server security patches are applied.

RevenueSA acknowledges that as a result of the SAP upgrade project a code freeze was imposed on the RIO production environment, and the SAP and database server software patching is not at the level it would otherwise be. The SAP upgrade project is scheduled for completion in December 2016.

Once the SAP upgrade project is completed and implementation takes place, the underlying server database and the SAP software will be patched to the highest level.

After this exercise, RevenueSA will ensure a regular patching strategy (half yearly or yearly as approved by the affected stakeholders) for SAP software and the underlying server database is implemented.

6 IT system monitoring and maintenance controls

Summary of key findings

Our review of IT system monitoring and maintenance controls across the RIO environment identified the following control weaknesses:

- incomplete, out of date or inadequate procedural, user and system documentation including password policies
- lack of audit logging at the database level
- inadequate technical expertise at the agency level that has resulted in a high reliance on external service providers.

Summary of key recommendations

Remediation of these control deficiencies is required to ensure RIO's original specifications and desired security parameters are maintained. Inadequate monitoring and maintenance controls could result in excessive system downtime, loss of taxation revenue and fraudulent and/or malicious activity going undetected.

Remediation can occur by:

- establishing appropriate user and technical documentation, including password policies
- enabling audit logs to detect unusual activity within the RIO environment and database
- continuing to progress the transition of system technical knowledge from the external service provider to internal support staff.

6.1 Introduction

IT system monitoring relates to ongoing monitoring of system processes, system access, system performance and data configuration. Effective monitoring should cover all activity within the individual application, operating system, database and associated network(s).

At the application level, database tables should be monitored, and system logs should record the level of data collected, data sensitivity and user accessibility within the respective IT environment.

Weaknesses in audit logging and monitoring of the IT environment increase the risk that inappropriate or unauthorised activities could go undetected by management.

Where inappropriate activities have occurred, management may not be able to trace the origins of the event if there are incomplete or missing audit trails. This could be even more difficult if generic user access accounts are used, which further restrict the identification of individual users.

IT system maintenance within RIO can be categorised into three classes – corrective, adaptive and perfective.

Corrective maintenance involves removing any highlighted program errors that arise because of faulty design or wrong assumptions.

Adaptive maintenance involves program functions being changed to provide access to information needed by the user. This could become necessary due to changes in procedures, objectives, goals, system controls and/or security needs.

Perfective maintenance means adding new programs or modifying existing programs to enhance the performance of the information system. This may occur as a result of a change to user needs within or outside of the organisation.

Weaknesses in managing IT system maintenance across RIO could result in:

- the inability to identify and restrict changes to the system and associated security programs
- failure to address risks promptly
- an impact on system security and operational performance.

This increases the risk of RIO not performing in accordance with its original specifications and desired security parameters. It could also result in excessive system downtime, loss of taxation revenue and fraudulent and/or malicious activity going undetected.

6.2 Validation approach

To test IT system monitoring and maintenance controls within RIO, we interviewed key staff and examined key technical design and support documentation. We also assessed the adequacy of the design and implementation controls over system configuration, logging and reporting, and general support technical expertise.

Our assessment of IT system monitoring and maintenance focused on whether:

- adequate application, operating system and database general security controls existed to prevent unauthorised use
- RIO is being monitored and security events are being recorded in system audit logs
- adequate security skills and documentation are maintained to manage the environment efficiently and effectively.

The following sections summarise the findings from our IT system monitoring and maintenance control testing.

6.3 Inadequate supporting documentation

Recommendation

Appropriate user and technical documentation should be established.

Finding

There are a significant number of procedural, user and system documents that are incomplete or outdated.

Some examples we noted were the RIO SAP Security Configuration (last updated August 2015), SAP Security Framework (last updated March 2011) and the RIO interface diagram (last updated February 2008).

We also noted that documented business rules did not reflect recent changes to business processes and functionality.

Inadequate systems documentation could result in:

- business processes being performed inconsistently resulting in errors and inefficiencies
- poor decision-making relating to change management
- changes to the system being inaccurately assessed for impact or delays in restoring systems (and dependencies) in the event of a system issue.

This finding was previously raised in our 2012-13 review.

Department response

A review of functional and technical supporting documentation was done prior to Release 2 user acceptance testing to ensure baseline functionality was known. All functional supporting documentation is in need of review and updating. This will commence once the SAP upgrade project is complete. From this point, ongoing updates of documentation will occur when required (eg system modification due to upgrades, new business requirements being implemented).

6.4 RIO system access can bypass application level controls

Recommendations

DTF should

- enforce policies to ensure that users are not provided with direct login passwords to RIO's underlying SAP system
- remove access to direct login within SAP, other than for disaster recovery requirements.

Findings

Discussion with management indicated that users generally log in to RIO with a single sign-on though a SAP portal (refer Appendix 1). If the user is not able to log in successfully via this portal, the user's direct RIO system login password is reset and provided to the user. RIO's password policies are not as strong as those enforced by the portal control.

Accessing RIO using a direct login overrides application level security, increasing the risk of undetected and unauthorised activities in RIO. This could result in data integrity issues or fraudulent activity.

Department response

It has been necessary for DTF to assign passwords directly due to the use of an unsupported browser. The SAP upgrade will enable a supported web browser to be used and will mean that it will no longer be necessary to assign passwords directly.

6.5 RIO system database audit logging is not activated

Recommendations

DTF should consider enabling and monitoring audit logs to detect unusual activity within the RIO system database. Some events to be considered include:

- account logon (success/failure)
- changes to key application and database tables and functions
- modification and creation of critical tables such as supplier and customer masterfiles
- updates and deletions to database security tables
- access permissions for creations and updates.

While we recognise that database logging can sometimes adversely affect performance, there are still control benefits to be achieved through focused and regular reviews. This auditing can be tailored to significant areas attached to the business application.

Finding

Audit logging has not been enabled for the RIO system database.

Lack of audit logging reduces the ability to investigate or monitor activities performed directly within the database.

Department response

The Technical team has received advice on how to activate database level auditing and this will be applied to the RIO production database. This is expected to be completed by the end of December 2016.

6.6 Lack of internal technical expertise

Recommendation

DTF should continue to transfer system technical knowledge from the RIO system external service provider (Fujitsu) to DTF's internal support staff.

Finding

DTF is reliant on Fujitsu's technical expertise. This reduces its ability to monitor and ensure that the technical support provided by Fujitsu meets DTF's security requirements and policies.

A transition plan has been established with system upgrade and intermediate support activities expected to be finalised by December 2016. This forms part of the current extended support arrangement with Fujitsu.

Failure to adequately transfer technical expertise to DTF could place increased reliance on the service provider for ongoing support and technical assistance.

This risk was previously raised in our 2012-13 review.

Department response

Fujitsu is continuing the skills transfer to internal staff covering aspects relating to system access, data table management and system security.

7 IT system security design controls

Summary of key findings

Our review of IT system security design controls across the RIO environment identified the following weaknesses:

- insufficient formal processes to manage emergency access or activities performed in the production environment
- excessive access to sensitive system functions through the continuing use of generic accounts, unregulated user and role administration functions, and the ability to update key tables
- inadequate execution and managing of programs and batch job schedules, excessive access to the ABAP dictionary,[14] and the ability to execute external computer operating system commands and alter company codes, with insufficient security access controls
- default user accounts were insufficiently configured and were either inappropriately enabled or had not been created
- user master records were inconsistent and poorly managed through a lack of user account validity end-dates, user accounts not being assigned to user groups and procedures used to create users not being consistently applied.

Summary of key recommendations

Remediation of these control deficiencies is required to ensure that the system security design controls assigned within the RIO environment are consistent with key configuration settings, commands and system parameters.

This can occur by:

- ensuring that changes to users, roles assigned and user master records are only made by the Central User Administration (CUA)[15] and consistently applied
- removing all generic user accounts
- updating existing user management procedures and extending the RIO security structure to incorporate appropriate customised roles for system users
- developing emergency roles for each system module and ensuring all standard roles are removed from the production environment
- identifying different types of users and creating user groups for each category of user, while ensuring that all users and respective roles have valid end-dates and are regularly reviewed for appropriateness
- restricting access to security administration areas, master data tables, specific key transactions, executable external computer operating system commands and customised programs
- ensuring that all default user accounts are locked and passwords restricted.

[14] ABAP dictionary is a central repository for data definitions in the RIO SAP system. It creates and manages a description of all data used in the system. The aim is to assist in preserving integrity, consistency, security and sensitivity of data.

[15] CUA is a SAP system that enables a user to perform user maintenance for all the connected systems from one central system.

7.1 Introduction

A well designed and secure IT system should maintain the confidentiality, integrity and availability of system data. If a system is poorly designed and has security flaws or vulnerabilities, this may increase the potential for the system to be breached or compromised, with consequences to the confidentiality, integrity and availability of data.

Given the importance of RIO to the SA Government as a key revenue system, it is critical that its security design is comprehensive and well maintained, with supporting administration policies and procedures. This includes securing RIO interfaces with various external systems, including the Masterpiece general ledger and the DPTI SAILIS application.

In addition, RIO's security design should ensure configuration settings, system commands, system parameters, data, master records and user access controls are appropriately restricted and defined.

Weaknesses in RIO system security design controls may result in the system being compromised which could lead to inappropriate modification of system settings, programs, data and master records.

7.2 Validation approach

To test RIO's system security design, we interviewed key staff and examined key technical design policies and procedures. We also assessed the configuration of selected security controls within the RIO technical infrastructure.

Assessment of the IT system security design focused on the:

- adequacy of security administration procedures within the system
- appropriateness of data controls to prevent errors, loss, unauthorised modification and misuse
- security procedures around the change/management of defined configuration settings and system commands
- system parameters set to confirm the appropriateness of values and the mapping to authorised objects and classes.

The following sections summarise the findings from our IT system security design testing.

7.3 Inadequate global systems change option and client settings

Recommendation

DTF should consider moving their CUA client into the Solution Management (SOLMAN)[16] system. It should also ensure that all changes to user and role master records are made centrally in one CUA client and distributed to child (Production) systems with no option to maintain master records locally.

[16] SOLMAN is an integrated end-to-end platform intended to assist users in adopting new developments, managing the application lifecycle and running SAP solutions.

Finding

SAP CUA is used to maintain user master records. Changes made in the CUA are distributed to the other SAP system modules (child systems).

Our review of the configuration settings of the CUA system in SAP found that user and role records can be updated across multiple system modules as well as child systems within RIO without appropriate security constraints.

Allowing for unrestricted user access changes in child systems increases the risk of breaking the security design within RIO. It also means that inappropriate access may not be easily detected.

Department response

DTF is determining a solution in consultation with their implementation partner, Fujitsu, and the Auditor-General's Department. This solution will attempt to provide the necessary security controls to address the highlighted risks, without unnecessarily compromising system performance.

This solution will be developed in conjunction with an appropriate risk assessment and testing before implementation occurs.

DTF will keep the Auditor-General updated on the implementation progress.

7.4 Inappropriate security access, including emergency access

Recommendations

DTF should review the security approach to users' access permissions to ensure that job functions are appropriately assigned.

At a minimum DTF should consider:

- restricting security administration access to the SAP security team. Access for user management and role authorisation should also incorporate an emergency role to be assigned during a critical incident and with appropriate approvals
- restricting access to master data tables to a small user group. Additional restriction should be implemented to ensure that access to change direct tables in the production environment is restricted
- ensuring that access to specific key transactions is restricted and not assigned to any user in the production environment. Access to these transactions should be transferred to emergency roles, which can be assigned only during a critical incident with appropriate approval
- developing emergency roles for each SAP module within RIO. As these roles will have access to sensitive data and functionality they should be subject to appropriately documented approval and regular review

- conducting periodic user access reviews to confirm the appropriateness and validity of assigned privileges
- restricting user access to execute external computer operating system commands from within SAP
- removing SAP administrator generic accounts from users and create appropriately customised roles.

Findings

During testing, we noted that access to sensitive SAP functions was not restricted to the SAP security team. A number of technical and functional RIO system users had access to sensitive functions (direct and indirect). This increased the risk of data integrity being compromised, fraudulent activity or application failure.

Examples of access assigned to sensitive functions and their associated risks include access to:

- SAP administrator generic accounts (34 users). These profiles provide users with super user access and the ability to bypass all security controls. This risk was previously raised in our 2012-13 review
- perform user and role administration functions (41 users). These functions can enable the creation of false user accounts or the assignment of access privileges to conduct untraceable fraudulent activity in the system
- update tables (74 users). This function can allow unauthorised access to intentionally or unintentionally update master data in RIO
- execute and manage programs (41 users) and batch job schedules (231 users). These functions could enable users to bypass RIO security controls and increase the risk of inappropriate and unauthorised access
- the ABAP dictionary (41 users). This function allows each user to modify the data structures, which increases the risk of reduced data integrity and possible system loss
- execute external computer OS commands (48 users). If maliciously used this could potentially lead to application loss or external attacks to the system.

In addition, there was no formal process in place to manage emergency access within the SAP system. Under the current arrangements we noted that when emergency access was requested the user was provided the SAP administrator generic accounts profile. As previously mentioned, these profiles provide users with a very high level of access and the ability to bypass all security controls.

Department response

A security review is required to ensure roles are appropriate for current business processes and responsibilities.

This review is to be undertaken during the code freeze (depending on the upgrade project currently in progress, likely to be completed by December 2016). Once the code freeze ends, changes to security access will be scheduled. This will include any alignment of related business rules.

The process for replacing administrator profiles with customised roles is in progress. This review will be completed during the code freeze, with implementation scheduled once the code freeze ends.

7.5 Inadequate controls over default user access

Recommendations

DTF should:

- ensure that all default user accounts are locked and their default passwords are changed
- create and lock all the default users that are missing in SAP, and change their passwords
- ensure that access to default user passwords is restricted to the security team for access in emergency situations.

Findings

When SAP was implemented for RIO, default user accounts were created in the database, with default passwords. In order to protect SAP modules within RIO from external attacks, the implementation process for SAP includes creation of user accounts with the same name in the application layer. The passwords of these default users are changed in the SAP modules within the RIO system/application and the user account is locked.

Testing of the implementation showed that in some cases default user accounts in the application layer were either unlocked or had not yet been appropriately created.

Active default user accounts increase the risk of inappropriate access to RIO. Additionally, if the default user does not exist in RIO, there is an increased risk that users could potentially bypass the RIO system security control.

Department response

A review of standard users will be conducted and users that are not active will be locked. This will be repeated periodically. The initial review is expected to be completed by the end of December 2016.

7.6 Inappropriate access to production clients

Recommendations

DTF should ensure that production clients[17] are closed by default to avoid accidental or

[17] A production client is used to set up and confirm specific function and object capabilities within the SAP production environment.

deliberate deletion of transaction data. Where there is a requirement to open a client for maintenance purposes, DTF should consider implementing processes that enforce:

- monitoring of user activities performed on the client
- leaving production clients open for a maximum predetermined limited period.

Findings

Production clients in SAP should be closed to avoid accidental or deliberate deletion of transactions. Our review of the production client settings indicated that a production client was open.

Requests to open production clients are lodged through a service request. The SAP security team opens the requested production client once appropriate approval has been received. However, there is no process for monitoring the activities performed on the open client.

Opening production clients in SAP for prolonged periods increases the risk of intentional or unintentional deletion of transactions in RIO. Further, the lack of monitoring of activities performed in RIO increases the risk of undetected unauthorised deletion of transactions.

Department response

These jobs will be reviewed by the RIO Operations Support team to ensure correct client monitoring.

Additionally, a process will be implemented to log access attempts and activity within the open clients. This is similar to the procedure to request administrator access within RevenueSA. This will include a proper request procedure with approval and any activity will be closely monitored.

Both actions are expected to be completed by the end of December 2016.

7.7 Insufficient security restrictions and ongoing review of customised transaction code programs

Recommendations

DTF should review the security over custom programs ensuring that:

- all custom programs have been restricted to appropriate authorisation objects[18] to ensure a second level authorisation check has occurred at the role level (ie only an authorised user with an appropriate authorisation object would be granted access to execute programs)
- a development standard is implemented in SAP that requires all custom programs and transaction codes to be assigned to authorisation objects and classes
- appropriate table access restrictions have been applied based on risk.

[18] Authorisation objects are groups of authorisation fields that control a particular activity.

Findings

Testing indicated that a number of custom programs and transaction codes (over 20 codes/ programs) in the RIO production environment were not mapped to authorisation objects or classes, resulting in unrestricted access to the custom programs.

Additionally, there were no security restrictions on table access to prevent users from executing critical reports.

When authorisation objects are not mapped to transactions, SAP allows the free execution of the transaction, with no restriction on the level of data the user is allowed to view. This may expose sensitive data and programs.

Department response

DTF provided a technical response to address these findings, with an expected completion date of December 2016.

7.8 Company codes settings may allow data to be incorrectly deleted

Recommendation

DTF should ensure that all company codes are set to productive mode[19] within the SAP system.

Finding

If the company codes are not set to productive mode within SAP, the standard deletion programs can be used and executed. This can lead to unintentional deletion of production data.

Our review of the SAP modules of RIO found that not all company codes were changed from test mode to productive mode following the system implementation.

If company codes are not set to productive this increases the risk of production data being deleted.

Department response

This recommendation is expected to be adopted and completed by the end of December 2016.

7.9 User master records were inconsistent and poorly managed

Recommendations

DTF should review user master records to:

[19] Productive mode allows users to transfer/load old asset master records and values into the subledger as required.

- identify all users who do not have validity end dates and implement processes to maintain them based on user access requirement. For example, contractors should have a validity end date that aligns to their contract end date

- identify different types of users that exist in the system and create user groups for each category of user. This would simplify the process for mass user group updates.

DTF should update existing user management processes and configure SAP to ensure that user master records are only updated in the CUA.

Findings

Our review of RIO's user master records identified that these records are inconsistent and poorly managed. Some of the weaknesses identified included:

- lack of user accounts validity end dates – many critical and end users did not have validity end dates (eg they are left blank) which increased the risk of inappropriate user access

- users accounts are not assigned to user groups – appropriate classification of user accounts in SAP is achieved by assigning the accounts to user groups. Classification of user accounts provides auditing clarity and enables the system to better manage users access by their classification

- users are created outside of the CUA – many users are directly created in child systems and not in the CUA, resulting in inconsistencies in user access across the SAP modules within RIO and misalignment with RIO's security model.

Inadequate controls over user master data potentially increase the risk of inappropriate or obsolete user access.

Department response

The transfer of security skills from Fujitsu to DTF will allow internal support staff to improve the integrity of the user master records. Specifically, adherence to validity dates and address data will need to be remediated.

Existing user management processes will be updated and SAP will be configured to ensure that user master records are only updated in the CUA. This activity is expected to be actioned once the SAP upgrade is successfully completed (expected in December 2016).

7.10 Inadequate management of SAP roles within RIO

Recommendations

DTF should:

- remove all standard roles from users in the production environment

- extend the RIO security structure to incorporate appropriate customised roles for system users.

In addition, security roles should not be updated directly in the RIO production system. Role changes should be made through a formal change management process.

Findings

Our review of SAP roles in RIO indicated that an excessive number of standard SAP roles are assigned to system and technical support team members. This increases the risk of unauthorised access being given to many users.

We also noted that at least 10 roles had been directly updated in the production system, which is not in accordance with the security and transport management process.

Assigning standard SAP roles to users increases the risk of a user being given inappropriate access. Direct updates of security roles in the production system are a breach of the security process and could increase the possibility of unauthorised changes to user access.

Department response

A security review will be conducted to ensure roles are appropriate for current business processes and responsibilities. This review is to be undertaken during the code freeze (depending on the upgrade project currently in progress, likely to be completed in December 2016). Once the code freeze ends, changes to security access can be scheduled. This will include a review of SAP standard roles currently assigned to users.

7.11 Inappropriate database configurations

Recommendation

DTF should strengthen RIO database security controls.

Finding

Some values assigned to RIO's database key configuration parameters increased the database's vulnerability to inappropriate access. In addition, some of these inappropriate configuration parameters could result in potential trojans,[20] viruses or denial of service attacks.[21]

Department response

An internal review of these settings is currently being conducted and they will be applied to the RIO database in line with SAP standards after the successful completion of the SAP upgrade, likely to be completed in December 2016.

[20] A trojan is a program that appears harmless, but is in fact malicious.

[21] A denial of service attack is where an attacker attempts to prevent legitimate users from accessing information or services.

8 IT user access management controls

Summary of key findings

Our review of IT user access management controls across the RIO environment identified the following weaknesses:

- methods used to assign access within RIO differed between business access and SAP Basis access[22]
- no segregation of duties process currently exists to address conflicting access permissions within the SAP modules of RIO
- while user access reviews occur regularly, the review of segregation of duties and privilege access is not performed
- no documented procedures define the roles and responsibilities for performing a user access review
- the SAP Basis team has access to the RIO database through the use of shared service account access which has been assigned super user access rights
- unnecessary user accounts exist within the local administration level access on the servers hosting RIO.

Summary of key recommendations

Remediation of these control deficiencies is required to ensure that the user access management controls assigned within the RIO environment are consistently applied to preserve confidentiality and integrity of the IT system and associated data.

This can occur by:

- implementing a consistent method of applying position and role based security for all RIO system users
- establishing formal segregation of duties for business and technical support
- defining a procedure and associated roles and responsibilities for periodic user access reviews that include functional and technical privileged access
- ensuring user access is periodically reviewed to identify potential conflicts that may require resolution at the user role and profile level
- ensuring shared accounts are not used to perform administrative tasks, including access to system infrastructure
- ensuring local accounts with administrative privileges are limited and locked, with associated passwords regularly changed.

[22] SAP Basis is a foundational part of SAP systems and consists of client/server architecture and configuration, a relational database management system, graphical user interface, a development environment, data dictionary and user and system administration and monitoring tools. It forms part of the system administration function for creating users, assigning roles, installing software, configuring parameters, integrating connectivity, monitoring system performance and initiating change management.

8.1 Introduction

User access management relates to the process of managing system access to both applications and data. This will include the approval, change and deletion of individual access as well as the periodical review of the alignment of staff roles and responsibilities.

User access management controls should also include the review of the appropriateness of super users, or users who have wide-ranging and heightened authorisation or privileges within the application and IT system.

User access management's primary objective is to maintain the confidentiality and integrity of ICT systems and associated data.

Weaknesses in user access management controls may result in inappropriate and excessive privileges assigned to system and data access, which could affect the completeness and accuracy of transactions.

8.2 Validation approach

To test IT user access management for RIO, we interviewed key staff and examined key user access design policies and procedures. We also assessed user access configuration within RIO's SAP application, database and operating system servers.

We evaluated the controls implemented by management to ensure access to systems and data is suitably restricted to only authorised users who require the access for legitimate business purposes.

Our assessment of the IT user access management focused on:

- procedures that restrict, control and appropriately authorise user access. This included the creation, modification and deletion of user access and also the appropriateness of segregation of duties requirements
- assessing password policies that safeguard information against unauthorised use.

The following sections summarise the findings from our user access management control testing.

8.3 Inconsistent assignment of new user access

Recommendation

DTF should implement a consistent method to apply position and role-based security for all RIO system users.

Finding

There are two different methods used to assign access within the RIO SAP modular based system. Business user access is based on position and role, while SAP Basis access is established on individual user permissions. These different approaches to user access management increase the complexity and effort required to monitor and maintain security permissions.

Using different methods to manage access within the SAP modules increases complexity, and increase the risk of assigning inappropriate access to users. This could also result in the integrity, availability, and confidentiality of financial data being compromised.

Department response

A security review is required to ensure roles are appropriate for current business processes and responsibilities. This review is to be undertaken during the code freeze (depending on the upgrade project currently in progress, likely to be completed by December 2016). Once the code freeze ends, changes to security access can be scheduled. This will include adopting a consistent approach to assignment of user access.

8.4 No process to manage segregation of duty conflicts

Recommendations

DTF should define business and technology support responsibilities for managing the segregation of duties whereby:

- a process should be established to manage segregation of duties risk
- a full assessment of segregation of duties controls should be undertaken
- potential segregation of duties conflicts should be reviewed and addressed to ensure that appropriate mitigating controls or changes to access are implemented
- periodical (eg six-monthly) reviews of user access (user level, role level, profile level) should be performed to identify conflicts that require resolution.

Findings

There is no process to manage segregation of duties risk. Segregation of duties system rules have not been established to identify the potential conflicting access permissions within RIO.

In our sample testing we identified conflicts with users having the ability to:

- manually make changes to payments as well as maintaining posting periods in the SAP general ledger
- perform bank reconciliations as well as make changes to bank payments
- create a business partner, generate invoices and change invoices.

If conflicting access is assigned to a user, there is an increased risk of malicious activity by users within the system, including inappropriate use and fraud.

This finding was previously raised in our 2012-13 review.

Department response

A security review is required to ensure roles are appropriate for current business processes and responsibilities. This review is to be undertaken during the code freeze (depending on the upgrade project currently in progress, likely to be completed by December 2016). Once the code freeze ends, changes to security access can be scheduled.

Once this review is complete and has been implemented, RevenueSA will consider segregation of duties based security processes including evaluation of risks and feasibility. Using SAP programs to perform and report on segregation of duties violations will be considered, however external assistance with expertise in SAP security processes will need to be engaged.

8.5 Insufficient user access reviews

Recommendation

DTF should define a procedure and associated roles and responsibilities for periodic user access reviews, including functional and technical access, which highlights where potential segregation of duties conflicts exist.

Finding

Our discussions with management indicated that a review of business user access is conducted quarterly by the RIO functional support team. We noted that segregation of duties and privileged access (including support user access) are not currently being reviewed.

There is no documented procedure that defines the roles and responsibilities for performing a user access review in RIO.

The absence of a periodic user access review process for SAP support users could potentially result in an increase of accounts with privileged user access or terminated users maintaining critical support authorisation access. This could result in increased vulnerability and external security attacks against RIO.

Department response

A security review is required to ensure roles are appropriate for current business processes and responsibilities. This review is to be undertaken during the code freeze period (depending on the upgrade project currently in progress, likely to be completed by December 2016). Once the code freeze ends, changes to security access can be scheduled. This will include formalisation of existing procedures to undertake user access reviews and frequency of these reviews.

8.6 Excessive use of a shared privileged database account

Recommendation

Individual user access accounts should only be used to perform administrative tasks on the RIO system database.

All database account users should be required to authenticate via the Active Directory[23] login.

Finding

Our discussions with management indicated that the SAP Basis team has access to the RIO system database using the shared service account. We also noted that the service account used to access the RIO system database has super user access.

[23] Active directory is a centralised information system within the Microsoft Windows Server environment. It is used to manage network user authentication, data security and distributed resources and enables interoperation with other directories.

Using a shared service account to access the RIO system database increases the risk of undetected misuse of data, which could potentially result in data integrity issues or loss of the application. This risk is further compounded by the lack of audit logging onto the RIO system database level.

Department response

A security review is required to ensure roles are appropriate for current business processes and responsibilities. This review is to be undertaken during the code freeze period (depending on the upgrade project currently in progress, likely to be completed by December 2016). Once the code freeze ends, changes to security access can be scheduled. This will include any alignment of related business rules.

8.7 Inappropriate privileged user access on SAP production servers

Recommendations

DTF should:

- implement a process for periodically reviewing user accounts on privileged accounts on the network as well as on local servers
- lock the local administrator account on all servers hosting RIO. If the default account is required, DTF should change the password regularly
- ensure that local accounts with administrative privileged are limited.

Findings

Discussions with management indicated that there is an unnecessary user account with local administrator level access on the servers hosting RIO.

There are currently no formal privileged access reviews being performed over the RIO system servers within the SAP environment.

A default administration account is a potential target for security attacks and, if accessed, could result in unauthorised access and a possible compromise of the integrity of the data.

Department response

The RIO Operations Support team will conduct a review of privileged user access to SAP production servers immediately. This review will also incorporate agreed SAP standards and action to mitigate risk of inappropriate access will be undertaken as a priority. This will be followed up by regular reviews.

Appendix 1 – Overview of RIO SAP modular based system

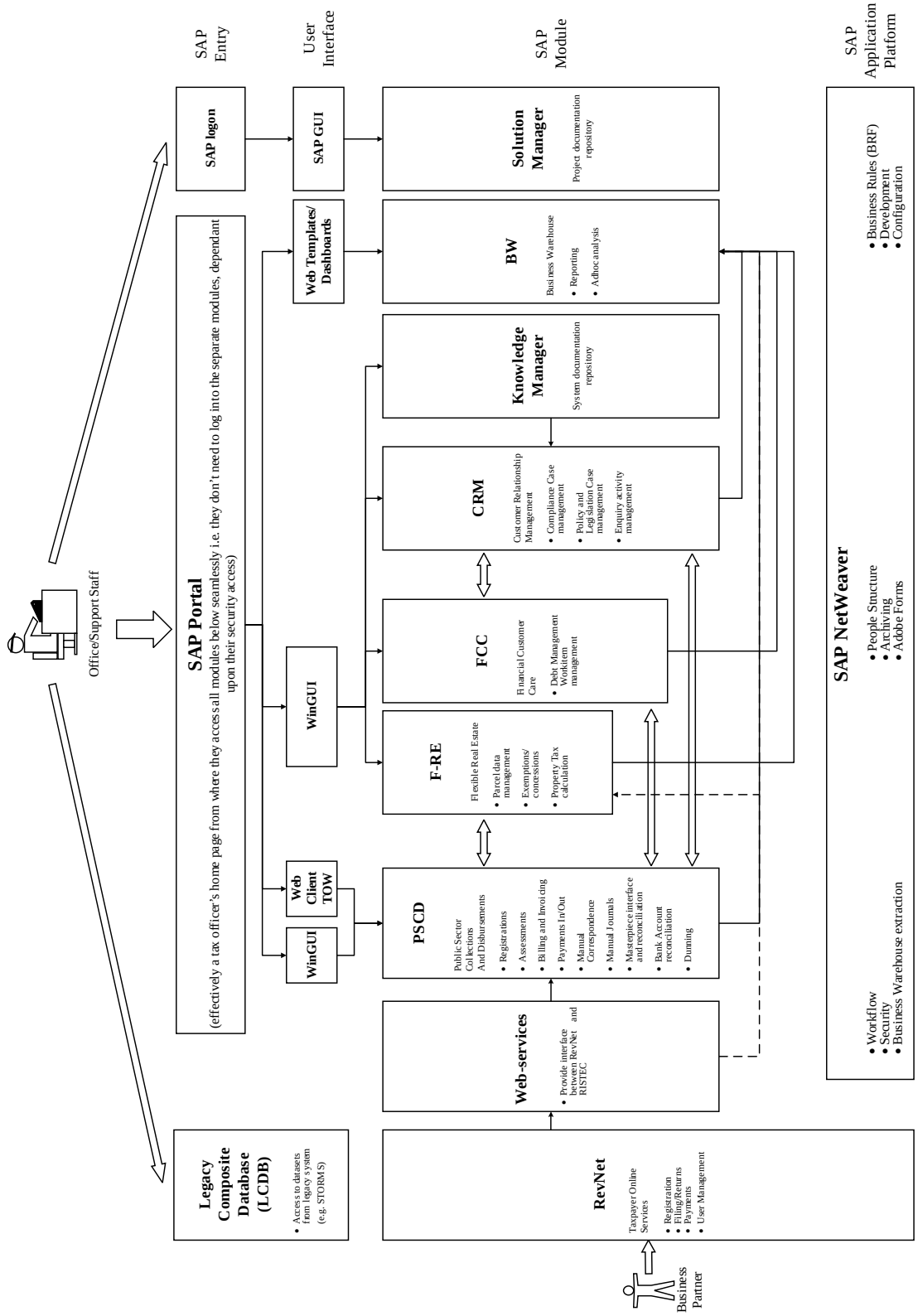


Diagram provided by DTF representatives on 24 November 2015.

Appendix 2 – Glossary

Term	Description
ABAP dictionary	is a central repository for data definitions in the RIO SAP system. It creates and manages a description of all data used in the system. The aim is to assist in preserving integrity, consistency, security and sensitivity of data.
Active directory	is a centralised information system within the Microsoft Windows Server environment. It is used to manage network user authentication, data security and distributed resources and enables interoperation with other directories.
Authorisation objects	are groups of authorisation fields that control a particular activity.
Billing sets	are groups of customers that are billed at the same time.
Central user administration (CUA)	is a SAP system that enables a user to perform user maintenance for all the connected systems from one central system.
Code freeze	is when program changes to the system are suspended at a point in time. This is usually performed to help preserve system stability and/or reduce unintended performance issues.
Data scrambling	involves making data unintelligible or removing sensitive data.
Denial of service attack	is where an attacker attempts to prevent legitimate users from accessing information or services.
Masterpiece	is an accounts payable system used throughout most SA Government agencies.
Production client	is used to set up and confirm specific function and object capabilities within the SAP production environment.
Production environment	is where an organisation's day-to-day operational programs are run in real-time rather than as part of a test or development scenario.
Productive mode	allows users to transfer/load old asset master records and values into the subledger as required.
RevNet	is an internet based system that is intended to provide an easy, flexible and more effective way for clients to do business with RevenueSA.
RIO	is the RevenueSA Information Online system.
RISTEC	is the RevenueSA Information System to Enable Compliance.
SAILIS	is the South Australian Integrated Land Information System
SAP	is an acronym for Systems, Applications and Products. The application software is from the German software company SAP SE, which develops enterprise software to manage business operations and customer relations.

Term	Description
SAP Basis	is a foundational part of SAP systems and consists of client/server architecture and configuration, a relational database management system, graphical user interface, a development environment, data dictionary and user and system administration and monitoring tools. It forms part of the system administration function for creating users, assigning roles, installing software, configuring parameters, integrating connectivity, monitoring system performance and initiating change management.
Software patch	is a piece of software that is designed to fix defects or vulnerabilities, or provide updates to an information system.
SOLMAN	is an integrated end-to-end platform intended to assist users in adopting new developments, managing the application lifecycle and running SAP solutions.
Transport	is a package within the RIO SAP system that is used to transfer data, and provide enhancements or new developments of existing business functions from development to production.
Trojan	is a program that appears harmless, but is in fact malicious.