Shire of Dardanup

APPENDICES
(Part 1)

AUDIT & RISK COMMITTEE MEETING

To Be Held

Wednesday, 14th September 2022
Commencing at 2.00pm

At

Shire of Dardanup
ADMINISTRATION CENTRE EATON
1 Council Drive - EATON

This document is available in alternative formats such as:
~ Large Print
~ Electronic Format [disk or emailed]
Upon request.

RISK ASSESSMENT TOOL

OVERALL RISK EVENT: Western Australian Auditor General – Schedule of Reports

RISK THEME PROFILE:

3 - Failure to Fulfil Compliance Requirements (Statutory, Regulatory)

RISK ASSESSMENT CONTEXT: Strategic

CONSEQUENCE CATEGORY	RISK EVENT	PRIOR TO TREATMENT OR CONTROL			RISK ACTION PLAN (Treatment or controls proposed)	AFTER TREATEMENT OR CONTROL		
		CONSEQUENCE	LIKELIHOOD	INHERENT RISK RATING		CONSEQUENCE	LIKELIHOOD	RESIDUAL RISK RATING
HEALTH	No risk event identified for this category.	Not Required - No Risk Identified	N/A	N/A	Not required.	Not required.	Not required.	Not required.
FINANCIAL IMPACT	No risk event identified for this category.	Not Required - No Risk Identified	N/A	N/A	Not required.	Not required.	Not required.	Not required.
SERVICE INTERRUPTION	No risk event identified for this category.	Not Required - No Risk Identified	N/A	N/A	Not required.	Not required.	Not required.	Not required.
LEGAL AND COMPLIANCE	Not considering the risks, controls and recommendations arising from the Auditor General's report could have an impact on Council not meeting its compliance requirements.	Moderate (3)	Rare (1)	Low (1 - 4)	Not required.	Not required.	Not required.	Not required.
REPUTATIONAL	Council's reputation could be seen in a negative light for not adhering to its requirement to fulfil duties and functions that are prescribed in legislation.	Moderate (3)	Unlikely (2)	Moderate (5 - 11)	Not required.	Not required.	Not required.	Not required.
ENVIRONMENT	No risk event identified for this category.	Not Required - No Risk Identified	N/A	N/A	Not required.	Not required.	Not required.	Not required.

(Appendix AAR: 8.1B)

Western Australian
Auditor General's Report

2022 Transparency Report: Major Projects

Office of the Auditor General
Western Australia

Audit team:
Aloha Morrissey
Colin Campbell
Daniel Franks
Wendi Zeng
Chiara Galbraith

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

2022 Transparency Report: Major Projects

Report 17: 2021-22
June 2022

This page is intentionally left blank

THE PRESIDENT
LEGISLATIVE COUNCIL

THE SPEAKER
LEGISLATIVE ASSEMBLY

2022 TRANSPARENCY REPORT: MAJOR PROJECTS

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

The objective of this review is to provide transparency to Parliament and the community around the cost and time performance of 17 major State government projects.

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

CAROLINE SPENCER
AUDITOR GENERAL
17 June 2022

Contents

Auditor General's overview

Funding for major projects is listed in the annual State Budget papers for each State government entity under their Asset Investment Program. The combined value of the State's Asset Investment Program totals $7 billion in 2021-22. This includes funding for roads, hospitals, schools, prisons and other government infrastructure for the people and economy of Western Australia (WA). However, Parliament and the public cannot easily access detailed or consolidated information on the cost and time performance of these projects.

This second report by my Office provides a snapshot look at 17 selected major projects, including impacts on project costs and delivery timeframes from ongoing material and labour supply shortages due in part to the COVID-19 pandemic responses. We found there has been an 11% budget increase across the 17 projects since their original approval, from $5.11 billion to $5.67 billion. Of the 14 active projects, 7 have had their completion dates extended by a year or more, with 1 project's completion date extended by 2.5 years. Twelve of the 14 active projects have had their cost and/or time budgets increased since original approval.

Many projects are now competing with a boom in WA's building and construction sector, driven by stimulus measures, supply chain disruption and a tight labour market. We note the Government has responded to these market pressures by smoothing its pipeline of works through delayed commencement of some projects, particularly in the Transport portfolio. It is important the State Government considers predictable events, such as stimulus measures and the impact of closed borders on labour supply, when planning the delivery of its Asset Investment Program to avoid overstimulating industry.

In 2020, my Office published our first *Transparency Report: Major Projects*[1] to help address the lack of transparency in major project reporting. In that report I said it would be a simple matter for Government to regularly report publicly on the status of projects to improve transparency to both Parliament and the public. This reporting would satisfy parliamentary and public interest, promote accountability, and build community trust and confidence around the management of the State's significant investment of public money in major public assets. I note that the Department of Finance regularly reports to Government on the status of major projects and I have recommended this form the basis of regular public reporting. It is my intention to continue to periodically report and track a selection of major projects until Government fills the gap.

This year, my team reviewed the high-level financial and governance controls for all selected projects and performed a detailed controls review for 5 of the projects. Sound governance and financial oversight help support project delivery to achieve planned outcomes on time and on budget.

I thank the staff at each of the entities for their cooperation and assistance in completing this work and strongly encourage entities to publicly report on the cost and time progress of major projects on a regular basis.

[1] Western Australian Auditor General's Report, *Transparency Report: Major Projects*, Report 6: 2020-21, 29 October 2020.

Executive summary

Introduction

The objective of this review is to provide transparency to Parliament and the community around the cost and time performance of 17 major State government projects in various stages of planning, procurement and delivery. We also included a high-level review of the financial and governance controls for all selected projects and a detailed review of control implementation for 5 projects.

For the purposes of our review, we have defined major projects as either a single project or program of works that costs $10 million or more.

Project summary sheets provide a summary, overall status and our assessment for each selected project. Interactive versions of the project summary sheets are available on our website.

Background

Despite the significant investment in Western Australia (WA) of public money in major projects, Parliament and the public cannot easily access information on their progress. Our previous *Transparency Report: Major Projects* in 2020 highlighted the need for greater transparency in this area of significant public and parliamentary interest.

Similarly, the incoming WA Government's 2018 *Special Inquiry into Government Programs and Projects* commented that Government had 'defaulted to confidentiality around major projects rather than transparency' and recommended Government 'provide information about major projects in an accessible and transparent way to the public'.

The Major Projects Expenditure Review Sub-Committee was established following a Cabinet decision in June 2021. Its responsibilities include monitoring the delivery of the State's Asset Investment Program through the review of regular reports on major projects and programs. The sub-committee meets about every 6 weeks.

The Infrastructure Delivery Unit (IDU), within the Department of Finance, has been asked by the sub-committee to submit progress reports on the status of 21 significant building and infrastructure projects, and the State's entire Asset Investment Program.

Our 2020 report covered 15 major projects managed by 8 State government entities. This report covers 17 projects managed by 10 State government entities. Ten projects are still underway from our first report, 2 have been completed, 1 is no longer funded and 4 new projects have been added.

Conclusion

In compiling this transparency report, nothing has come to our attention to indicate that, in all material respects, information provided in the project summary sheets within this report is not accurate and reliable.

Nine of the 14 active projects are on-track against their current approved cost and time budgets. Two other projects are at risk of exceeding their approved cost budgets and 3 are at risk of not being delivered on time.

Over-stimulated markets and the COVID-19 pandemic responses have caused materials and labour supply shortages, contributing to increased cost and time budgets for many projects. Across all 17 projects there has been an 11% increase in project budgets since original approval, from $5.11 billion to $5.67 billion.

Twelve of the 14 active projects have had their cost and/or time budgets increased since original approval. Cost and time risks, if realised, have a flow on impact requiring reprioritisation of projects across the State's future Asset Investment Program.

Of the 2 completed projects, both were delivered within approved cost and time budgets, albeit 1 was delivered about a year later than originally planned (Project 2 - Greenough Regional Prison).

All projects had adequate high-level financial and governance controls, including monitoring and internal reporting processes. We did not identify any significant issues for the 5 projects included in our detailed controls review. All entities were able to provide reasonable and substantiated explanations of cost and time variations when requested.

Findings

Table 1 provides a summary of the 17 selected projects and our assessment of their status against their current approved cost budgets (inclusive of operating and capital expenditure) and completion dates. Current approved budgets are those approved by Cabinet, completion dates are those approved by the project steering committees and reported to Cabinet.

Table 1 also shows those projects that have had an increase to their original approved cost budgets and completion dates approved.

Project name		Project phase				Status at mid-June 2022		
		Planning	Procurement	Delivery	Complete	Cost	Time	OAG assessment
1*	Casuarina Prison Expansion - Stage 2			●			⏰	
2*	Greenough Regional Prison - Female Unit Upgrade				●		⏰	
3*	Geraldton Health Campus Redevelopment		●			$		
4	Joondalup Health Campus Development - Stage 2			●		$	⏰	
5*	John Forrest Secondary College Redevelopment			●				
6*^	Bob Hawke College - Stage 2			●			⏰	
7	Metronet - Forrestfield-Airport Link			●			⏰	
8^	Metronet - Morley Ellenbrook Line			●				
9	Queen Victoria Street - Swan River Crossing			●		$	⏰	
10	Tonkin Highway Gap - Collier Road to Stanton Road			●		$		
11	Tonkin Highway Grade Separation - Hale, Welshpool, Kelvin Roads	●					⏰	
12	Tonkin Highway Stage 3 Extension - Thomas Road to South Western Highway	●				$	⏰	
13	Fuel Jetty Rottnest Island				●	$		
14	Main Jetty Rottnest Island			●		$	⏰	
15	South Thomson Bay Development Rottnest Island (Barge Landing and Cargo Facilities)					Did not proceed		
16^	Common Ground - East Perth		●			$	⏰	
17^	Common Ground - Mandurah	●				$		

Source: OAG

** managed by the Department of Finance*

^ new project selected for this report

$ *funding increase approved*

⏰ *extension to completion date approved*

Table 1: OAG status assessment of selected major projects at mid-June 2022

Table 2 is the risk matrix we used to assess cost and time status of projects and to form our overall assessment. In some cases, potential risks have been identified by entities or the OAG in the cost or time commentaries of our Project Summary Sheets that have yet to impact on cost or time status.

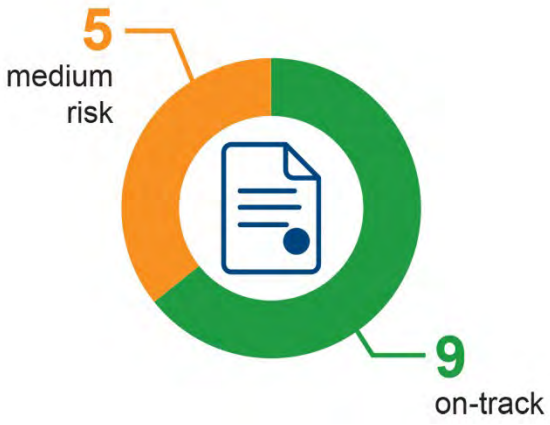
	Significant	Medium	On-track	Not applicable
Cost	Actual or forecast cost more than 10% over current approved budget	Actual or forecast cost between 5 to 10% over current approved budget	Actual or forecast cost less than 5% over current approved budget	
Time	Actual or forecast delivery more than 6 months over current approved time	Actual or forecast delivery between 3 to 6 months over current approved time	Actual or forecast delivery less than 3 months over current approved time	
OAG assessment	Both cost and time at significant risk	Either cost or time at significant or medium risk	No cost or time risk evident at report date	

Source: OAG

Table 2: Risk matrix used to assess project status

Overall assessment

We assessed 9 of the 14 active projects as being on-track to meet their current approved cost and time budgets (Figure 1). We note however that 12 of these projects have had their cost and/or time budgets increased to accommodate scope changes, material and labour shortages, price increases and scheduling challenges (Figure 2). Five have had both their cost and time budgets increased. A further 3 projects have received more funding and 4 have had their completion dates extended. Only 2 of the 14 active projects have not had their cost or time budgets increased since original approval.



Source: OAG using entity information

Figure 1: OAG overall assessment of project status at mid-June 2022

Source: OAG using entity information

Figure 2: Projects with approved increases to original approved cost and/or time budgets

We found there has been an 11% increase across all project budgets since their original approval, from $5.11 billion to $5.67 billion. Seven of the 14 active projects have had their completion dates extended by a year or more, with 1 project's completion date extended by 2.5 years.

The 5 projects we assessed as being at medium risk have identified cost and time risks that have either already been realised, as with the delay to completion of the **Metronet – Forrestfield-Airport Link**, or are yet to have changes to their cost and time budget approved. Two of these projects are at significant risk of exceeding their approved cost budgets, and 3 are at significant risk of not being delivered on time.

We note that the cost and time risks identified in our 2020 report were realised for 4 projects:

- **Greenough Regional Prison – Female Unit Upgrade** – finished about a year later than originally approved, albeit within the revised approved timeframe
- **Geraldton Health Campus Redevelopment** – the project budget has increased and the delivery schedule is to be determined based on the outcome of the procurement process. It will not meet its target completion date of August 2024.
- **Main Jetty Rottnest Island** – the budget has increased by over $6 million and the current completion date has been extended by a year from the original approved date
- **South Thomson Bay Development Rottnest Island** – with an original budget allocation of $10 million, the project did not proceed once a business case was developed and assessed.

Casuarina Prison Expansion – Stage 2 and **Metronet – Forrestfield-Airport Link** were both previously reported as being within their approved cost and time. **Metronet – Forrestfield-Airport Link** has not been able to meet revised deadlines, and the **Casuarina** project is now facing cost risks due to construction industry pressures.

Three projects are in the planning phase

Three projects are at various stages of planning.

The Common Ground - Mandurah project is providing accommodation and support services for people suffering from chronic homelessness. The project plans to submit a Project Definition Plan (PDP) to Cabinet before 30 June 2022. The current budget is $28.1 million, which has increased by around $18 million from the original approved budget of $10 million. The estimated completion date is October 2024. The project team is expecting to submit a request for further funding to accommodate expected cost pressures. The PDP will inform future project cost and delivery schedules.

Two **Tonkin Highway projects** (Grade Separation and Stage 3 Extension) have had their start and completion dates deferred to smooth the State's pipeline of works and ease construction industry pressures:

- **Tonkin Highway Grade Separation** has an approved budget of $366 million. Estimated expenditure to 30 June 2022 is $17.05 million, which exceeds the budgeted expenditure of $9.84 million by around $7 million.
- **Tonkin Highway Stage 3 Extension** has an approved budget of $755 million which has increased by $250 million from the original budget of $505 million. The budget increase is due in part to scope changes and construction industry pressures.

Two projects are in the procurement phase

Two projects in the procurement phase have had their original budgets increased and both expect further cost increases due to construction industry pressures:

- **Common Ground – East Perth** has an approved budget of $45.4 million, which has increased by around $20 million from the original budget of $25 million. The increased budget was due mainly to scope changes, but with some recognition of construction industry cost pressures. The expected completion date is September 2024. The tender for construction closed in May 2022 with assessment to be completed by end of June 2022.
- **Geraldton Health Campus Redevelopment** went to tender in September 2021. However, bids came in well above the original approved $73 million budget as a result of materials and labour supply shortages and associated cost increase. As a result, the procurement process was put on hold while approval was sought for additional funds. A revised budget of $122.66 million was approved by the Expenditure Review Committee of Cabinet and revised options for procurement approaches are being assessed. The outcomes of the revised procurement will determine future timeframes for the project.

Nine projects are in the delivery phase

Five projects in delivery are on-track to be completed on time and within approved cost budgets:

- **Bob Hawke College – Stage 2** is expected to be completed on time and within its $52.9 million approved budget. The project was originally scheduled for completion by October 2022 but had its approved completion date extended to January 2023 due to construction industry pressures.
- **John Forrest Secondary College Redevelopment** is at mid-stage of delivery. The project is expected to be completed in September 2023 and within its $50 million approved budget. Estimated expenditure to 30 June 2022 is about $9 million above the $23.36 million budgeted.
- **Main Jetty Rottnest Island** is at mid-stage of delivery. It is within its revised approved budget of $12.9 million. The budget increased from the original $5.65 million due to expanded scope requirements identified during planning. However, the project team is aware the upcoming procurement for the final packages of work may identify further cost risks. The project is due for completion in December 2023.
- **Metronet – Morley Ellenbrook Line** is still in the early stages of delivery with a budget of $1.1 billion and completion due by December 2024.
- **Joondalup Health Campus Development** is at mid-stage of delivery. It is within its approved budget of $256.7 million and on schedule with expected practical completion date in early 2025.

One project in delivery is on time but faces a cost risk:

- **Tonkin Highway Gap – Collier Road to Stanton Road** is at mid-stage of delivery. The project faces cost risks with estimated expenditure to 30 June 2022 of $314.36 million, about $138.5 million above the $175.85 million budgeted. The project's revised approved budget of $520 million, increased from the original $290 million. The budget increase was for Main Roads to deliver the Morley Ellenbrook rail enabling works along the Tonkin Gap corridor. Cost escalation is also expected due to construction industry pressures. The project is due for completion by June 2023.

Two projects in delivery are within their cost budgets but face time risks:

- **Metronet – Forrestfield-Airport Link** is due for completion in mid-2022, about 6 months later than the current approved completion date and nearly 2 years later than originally planned. COVID-19 has impacted recent supply of specialist equipment and resources required for commissioning. At the time of reporting, completion is imminent. The project is within its approved budget of $1.86 billion.
- **Queen Victoria Street – Swan River Crossing** is in the early stages of delivery. Extra time on stakeholder consultation during planning delayed the start date with construction now expected to commence in late 2022, about a year later than originally planned. Completion is now expected in late 2025 or early 2026, about 2 years later than originally planned. The project is within its revised approved budget of $280 million, which has increased by $50 million from $230 million. The budget increase relates to scope changes following stakeholder consultation. Budgeted and actual/estimated expenditure to 30 June 2022 are on-track at $35.58 million and $35.38 million respectively.

One project is facing a cost risk. **Casuarina Prison Expansion – Stage 2** is at mid-stage of delivery. It is expected to require a budget increase due to construction industry pressures. The completion date has been deferred by about 6 months from the end of 2023 to mid-2024.

Two projects are complete, and one did not proceed

Since our last report in October 2020, 2 projects have been completed (**Greenough Regional Prison – Female Unit Upgrade** and **Fuel Jetty Rottnest Island**). Both were completed within revised and approved budgets, albeit Greenough Regional Prison was delivered about a year later than originally planned. A further project did not proceed past the Business Case (**South Thomson Bay Development Rottnest Island** (Barge and Cargo Landing Redevelopment)) with funds approved to be transferred to the **Main Jetty Rottnest Island project**.

Cost increases and resource shortages have impacted many projects

Twelve of the 14 active projects have had their cost and/or time budgets increased since original approval. Five projects have had both their time and cost impacted, and 7 have had either their cost or time impacted.

It is difficult to accurately assess the impacts that COVID-19 has had on project budgets and time schedules. We reported in 2020 that the Government had fast-tracked a number of the projects we selected for review to help off-set the expected negative economic impacts of COVID-19. This resulted in increased demand for labour and materials at the same time as border restrictions and world-wide supply issues reduced supply. COVID-19 infection and isolation requirements have also significantly impacted labour supply for projects. However, a number of projects have also been impacted by scope changes as they progressed from planning into procurement and delivery phases.

Project financial and governance controls were adequate

Our high-level review of the financial and governance controls, including regular monitoring and internal reporting of project status, confirmed they were generally adequate for all projects. We reviewed the adequacy of control design in the following areas:

- documented and functioning governance frameworks including relevant project management and steering committees and project reporting and approvals processes
- management of conflicts of interest including gifts registers

- records management processes and systems for key project documentation
- project and financial management systems appropriate to the risk and complexity of the projects being managed
- authorisation of payments and segregation of duties in accordance with *Treasurer's Instruction 304 Authorisation of Payments*
- independent processes to confirm quality, quantity and cost reports for projects prior to authorisation of payments.

Our more detailed review for 5 projects[2] involved testing a small number of transactions or activities to confirm the above controls had been implemented as required. The testing did not identify any significant issues in control implementation.

[2] Casuarina Prison Expansion – Stage 2; Geraldton Health Campus Redevelopment; Queen Victoria Street – Swan River Crossing; Common Ground – East Perth and Common Ground – Mandurah.

Recommendation

Similar to the recommendation in our 2020 report, the Department of Finance should work to improve transparency through regular reporting to Parliament and the public on the cost, time and status of major projects.

Response from the Department of Finance

The Department of Finance (Finance) welcomes the Auditor General's transparency report on major projects and is pleased the performance [review] acknowledges the improved governance arrangements that have been implemented across the public sector to guide the planning and delivery of the State's Asset Investment Program, including the recent establishment of the Major Projects Expenditure Review Sub-Committee.

Given the ongoing impacts of COVID-19 on the Western Australian economy and the current challenges within the building and construction industry, the Government's priority continues to be the delivery of critical infrastructure projects. A suite of industry support measures were announced as part of the 2022-23 State Budget in recognition of these issues and to support a vibrant and sustainable industry.

Furthermore, there are a number of existing mechanisms that provide a level of transparency over the Government's major projects, which the Auditor General's major projects report complements. In particular, the Budget papers, Standing Committee on Estimates and Financial Operations, Public Accounts Committee, agencies' annual reports and proposed updates to information published on the Pipeline of Work, all work together to provide a level of transparent reporting on the Government's major projects.

Accordingly, while Finance supports the intent of the recommendation, it is not well placed to progress the matter, noting many of the issues cited in Finance's previous response are yet to be resolved and will take considerable time and effort to work through, in close consultation with key stakeholders. Finance's current focus remains on project delivery and industry support measures, which have consequential impacts on small and local business, as well as the broader community.

Response from the Department of Treasury

Treasury supports transparent reporting on the status of the State's major projects. To this effect, Treasury welcomes the Auditor General's report and is pleased that it acknowledges improvements that have been implemented across the public sector, such as establishment of the Major Projects Expenditure Review Sub-committee (MPERSC) and Infrastructure Delivery Unit (IDU) in the Department of Finance.

Whilst supportive of the intent of the performance [review's] recommendation, Treasury believes existing major project reporting governance has been strengthened by the recently established MPERSC and the ongoing reporting function of the IDU.

In addition, scrutiny of major projects is achieved through:

- the annual Budget papers
- the Standing Committee on Estimates and Financial Operations
- the Public Accounts Committee
- agencies' annual reports and other public communications on major projects.

Further major project reporting is likely to result in duplication of these existing functions, and would require considerable resourcing if a $10 million project cost threshold was to be applied (major projects are generally defined as those with an estimated total cost of $100 million and above).

Treasury values the independent assurance provided by the Auditor General in relation to the cost, time and status of major projects, and would welcome the continuation of its existing program of transparency audits which are reported directly to Parliament.

Focus and scope

The objective of this transparency review was to provide information to Parliament and the public around the cost and time performance of a selection of major projects. The key questions we asked were:

- What is the current status of costs and timing (at mid-June 2022) for each project against approved funding?
- Can entities provide a reasonable and substantiated explanation where there are significant variations in costs and timing?

We reviewed 17 projects at 10 State government entities. For the 5 projects managed on behalf of entities by the Department of Finance, we obtained and compared financial data from both entities.

We conducted a high-level review of the design of financial and governance controls for all projects and a detailed review of the implementation of those controls for 5 projects. Our detailed review involved testing a small number of transactions or activities to confirm controls had been implemented as required.

During the review we:

- interviewed staff at the 10 entities
- reviewed relevant project documents and reports
- reviewed financial and governance controls for each project
- assessed the reliability of information provided
- confirmed the validity of reasons for project variances.

This was a limited assurance direct engagement, conducted under section 18 of the *Auditor General Act 2006*, in accordance with the Standard on Assurance Engagements ASAE 3500 *Performance Engagements* issued by the Australian Auditing and Assurance Standards Board. We complied with the independence and other ethical requirements relating to assurance engagements. This review varies in nature, timing, and extent from an audit. As such, the level of assurance provided in this report is substantially lower than for an audit.

The approximate cost of undertaking this review and reporting was $182,000.

Project summary sheets

The project summary sheets are available for interactive viewing on our website.

Project 1

Casuarina Prison Expansion - Stage 2

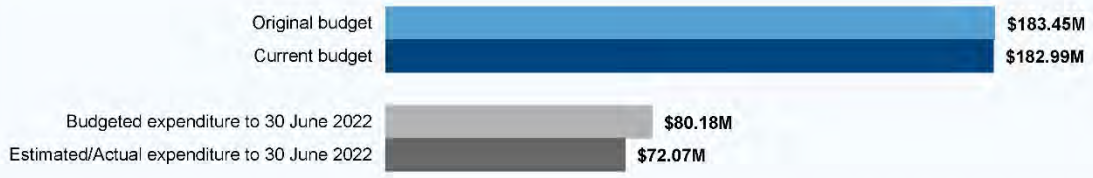
Entity Department of Justice

Phase Delivery

OAG's assessment

The project is in the mid-stages of delivery. It faces a cost risk.

Cost



The project is currently within budget, however recent planning estimates a budget increase is needed to deliver the full scope of works to allow for COVID-19 and other impacts on labour and material costs. A cost escalation request will be submitted to Treasury in June 2022.

Construction delays have impacted the project cashflow with expenditure around $8 million less than budgeted to 30 June 2022.

Time

The project was planned to be delivered within expedited timeframes. However, the approved completion date has recently been extended by 6 months from December 2023 to mid-2024 to allow completion of critical works required to commence the next phase of works.

Construction is split into 2 tranches. Tranche 1 construction works are tracking several months behind the original program due to COVID-19 related delays and prison operational requirements. Earliest delivery of Tranche 1 is expected in mid to late-2022.

Project summary

In April 2019, the WA State Government announced plans for a further expansion of 344 beds at Casuarina Prison. Following submission of the business case, in July 2019 the Expenditure Review Committee of Cabinet approved the project with a capital budget of $183.45 million.

The project includes upgrades to the prison's existing infrastructure and facilities including the provision of beds and specialist 'precincts' for high needs prisoners such as those who are disabled, infirm or elderly; who are currently not well catered for across the custodial estate. The expansion will also include assisted care, mental health and high security facilities. With a focus on design flexibility and future proofing, the aim is for the asset to remain suitable for managing changing cohorts over the next 50 plus years and to reduce lifecycle and maintenance costs. When complete, the prison's capacity will be up to 1,790 general purpose beds and 141 special purpose beds, making it one of the largest prisons in WA.

The project will see building taking place at the Prison continuously through to at least 2023.

Project status

The project is running behind on key milestones. A builder is contracted to deliver the Tranche 1 New Buildings. The tender for the Tranche 1 Refurbishment has been advertised and the Tranche 2 design documents are being developed by the lead consultant.

Response from the entity

We confirm the cost and time information and associated commentary present an accurate reflection of the status of the project as at June 2022. We agree with the OAG's assessment of the project status.

Project 2

Greenough Regional Prison - Female Unit Upgrade

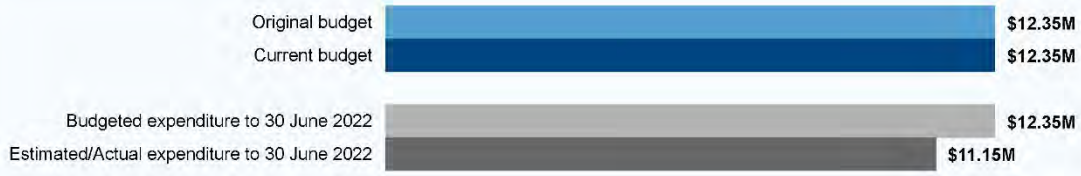
Entity Department of Justice

Phase Complete

OAG's assessment

The project was completed within the original approved budget and the revised approved timeframe, albeit about a year later than originally planned. Delays occurred in the planning phase and also during final construction.

Cost



The project was completed within the original approved budget.

Time

The project was completed about a year later than originally planned but within the revised approved timeframe. Delays occurred in planning due to extended consultation with stakeholders to agree the project scope. Further delays occurred during the final stages of construction due to COVID-19 and other impacts on material supply chains and contractor availability.

Project summary

In July 2018, a riot at Greenough Regional Prison resulted in significant damage to the facility, particularly the women's precinct. In July 2019, the State Government approved $12.3 million to address safety, security and separation concerns for the women's precinct, specifically:

- improved precinct perimeter fencing with visual separation on all prison facing sides and an energised fence
- improved CCTV quality and coverage including a conversion from analogue to digital and additional coverage including internal wing cameras
- additional support infrastructure to limit the need for women to leave the precinct including access to employment/constructive activity, medical consulting space and delivery of education and programs
- re-orientation of recreational facilities to provide better separation from other units and the oval
- improved access and egress with the installation of a secure egress point into the management fence to facilitate planned evacuations.

Project status

Complete.

Response from the entity

We confirm the cost and time information and associated commentary present an accurate reflection of the status of the project as at June 2022. We agree with the OAG's assessment of the project status.

Project 3

Geraldton Health Campus Redevelopment

Entity WA Country Health Service

Phase Procurement

OAG's assessment

The project is in the procurement phase. The project has had to manage both cost and time risks. The project will not meet its completion date of August 2024 and revised timeframes will not be known until the procurement process is complete.

Cost

The May 2022 State Budget provided additional funds of around $50 million to the original budget of $73.34 million, to cover cost increases and enable the project to proceed. This resulted in a current budget of $122.66 million.

Time

Before going back to market to procure a contractor to deliver the approved scope the project had been waiting for additional funding to cover increased costs. Revised delivery timeframes will not be known until the subsequent procurement strategy and process are finalised.

Project summary

The Government approved $73.34 million for the Geraldton Health Campus redevelopment project in the 2018 Budget.

The redevelopment is intended to strengthen quality health care in the mid-west and improve access to mental health services. The scope of works includes:

- a new emergency department (ED) including a 12-bed short-stay unit, inclusive of 3 mental health short-stay beds
- integrated mental health services, including a 12-bed (4 high dependency/8 low dependency) inpatient unit with co-located mental health community treatment team
- a new 8-bed critical care unit comprising 4-bed intensive care unit (ICU)/4-bed high dependency unit to be built in the old ED space
- essential engineering service upgrades.

The new ED and integrated mental health service was initially due for completion by late 2022 and the refurbishment of the old ED into a new critical care unit was to be completed in late 2023.

Project status

Delays to the original approved completion date have arisen due to an unfavourable tender result, changing market conditions and pending confirmation of additional funding from Government. Following consideration of these issues, and further market research and advice from the Department of Finance, additional funding was approved by Government and announced by the Minister for Health on 4 May 2022.

Response from the entity

We confirm the cost and time information and associated commentary present an accurate reflection of the status of the project as at June 2022. We agree with the OAG's assessment of the project status.

Project 4

Joondalup Health Campus Development - Stage 2 (JHCD2)

Entity Department of Health - North Metropolitan Health Service

Phase Delivery

OAG's assessment

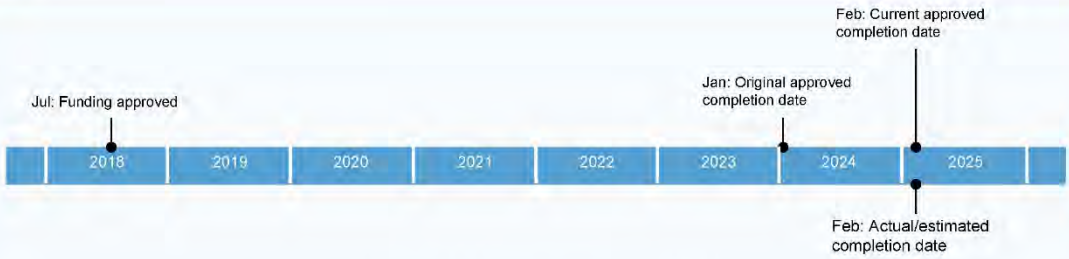
The project is in the mid-stages of delivery. It is within budget and expected to be completed on schedule in early 2025, although with an increased budget and a year later than originally intended due to scope changes approved as part of Project Definition Planning.

Cost

The Commonwealth Government and the State executed the Project Agreement for the Western Australian Hospital Infrastructure Package in 2018-19, providing $158 million for this project. The Project Definition Plan submitted as part of the 2019-20 Mid-Year Review included additional project scope to meet service demand. An additional investment of $98.7 million was approved by the State Government, resulting in a total project budget of $256.7 million.

Estimated expenditure to 30 June 2022 is about $1.5m more than budgeted. The increased expenditure reflects the progress of works on site which are ahead of schedule.

Time



The project is progressing and expected to be completed on schedule in early 2025.

- Emergency Department and Staff Car Park expansion works were completed in November 2021.
- Partial demolition of the Joondalup Health Campus Community Health Building was completed on 16 November 2021.
- Construction of the new 102 bed Mental Health Unit commenced on 17 November 2021.
- Public Car Park construction works commenced on 26 November 2021.
- Phase 1 works for the Central Energy Plant Upgrades commenced on 2 November 2021.
- The planned construction completion date was revised to February 2025 following acceptance of the Early Contractor Involvement (ECI) proposal which included a contracted works completion date of 13 February 2025.

Project summary

The JHCD2 project is a major redevelopment of the existing Joondalup Health Campus with the construction of:

- a new 102 bed Mental Health Unit (consisting of 30 additional beds, 25 shelled bed spaces to meet future demand with life safety and main service provision for future fit out and 47 replacement beds)
- 12 new emergency department (ED) beds (comprising 10 bays and 2 isolation rooms)
- 1 specialised Behavioural Assessment Urgent Care Clinic (BAUCC) located within the expanded ED
- refurbishments to the Emergency Assessment Unit (EAU) located within the expanded ED
- a new 112-bed Public Ward block (30-bed medical/surgical inpatient ward, 16-bed Cardiac Care Unit (6 additional and 10 relocated), 66 shelled beds to meet future demand, physiotherapy, administration and shelled space)
- 1 new Theatre
- 1 new Cardiac Catheterisation Laboratory (Cath Lab) and relocation of the existing Cath Lab
- refurbished Discharge Lounge
- increased parking bays for staff and public
- upgraded staff facilities (staff rooms, change rooms and training areas)
- upgrades to associated services (including Central Energy Plant, Sterilising Department, Biomedical Engineering and Stores).

Project status

The project is progressing on schedule and within the approved budget.

Response from the entity

We confirm the cost and time information and associated commentary present an accurate reflection of the status of the project as at June 2022. We agree with the OAG's assessment of the project status.

Project 5

John Forrest Secondary College Redevelopment

Entity Department of Education

Phase Delivery

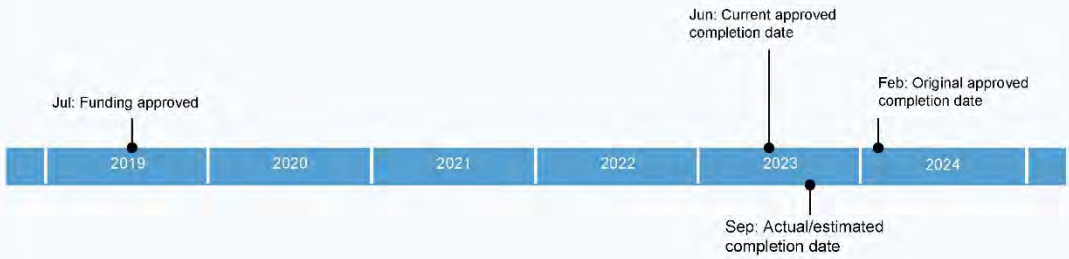
OAG's assessment

The project is in the mid-stages of delivery. It is slightly behind schedule due to materials and labour shortages but on track for completion within approved cost and time budgets.

Cost

The project is within its approved budget of $50 million.
Estimated expenditure to 30 June 2022 is about $9m more than budgeted. This increased expenditure reflects progress of significant new works on site, refurbishment and demolition on the existing school site, and increased material and labour costs. However, completion is still expected within the $50m approved budget.

Time



The project is currently 8-12 weeks behind schedule, but early project handover is still expected in September 2023, within the original timeframe of January 2024.

Project summary

On 13 September 2017, the State Government announced funding for a $50 million major rebuild at John Forrest Secondary College which forms part of a commitment to upgrade secondary schools across the State. Funds were made available in the 2019-20 State Budget. The redevelopment will see the college modernise and expand its permanent student accommodation.

The design will deliver high quality, highly functional and sustainable educational facilities including new technology and arts learning areas along with administration, sports hall and science labs. Some refurbishments to existing classrooms may also be included.

The project will increase the permanent student accommodation on the site to 1,300 students to meet current demand and increase the quality of the school's infrastructure.

Project status

The project has experienced challenges and slight delays due to material and labour supply shortage and working on an occupied site.

Response from the entity

We confirm the cost and time information and associated commentary present an accurate reflection of the status of the project as at June 2022. We agree with the OAG's assessment of the project status.

Project 6

Bob Hawke College - Stage 2

Entity Department of Education

Phase Delivery

OAG's assessment

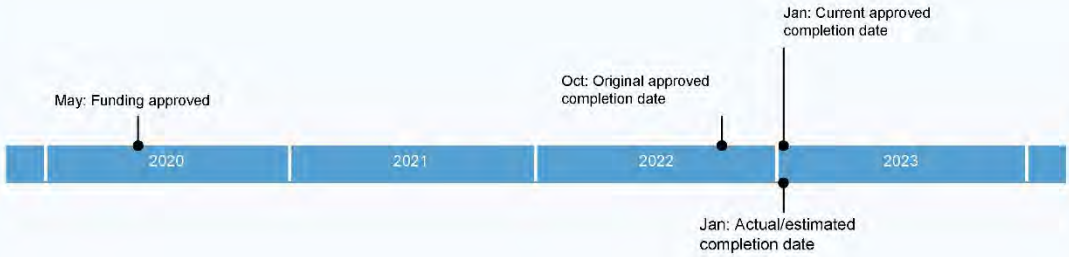
The project is in the mid-stages of delivery, it has experienced some delays but is on time for completion in January 2023 and within budget.

Cost

The project is within its approved budget.

Expenditure to 30 June 2022 is about $4m less than budgeted as a result of delayed progress.

Time



The handover date has been extended slightly to January 2023 to account for delays caused by materials and labour shortages.

Project summary

The project is for the second stage of Bob Hawke College and is due to open in 2023. Stage 1 of the college opened in January 2020, catering for 1,000 students. Stage 2 will accommodate a further 1,000 students and include additional general classrooms, a performing arts centre, visual arts, music and media studios. The Stage 2 site addresses Subiaco Road and is adjacent to the Stage 1 development on the former Kitchener Park, Subiaco.

Project status

The project is on time and budget but experiencing some challenges.

Response from the entity

We confirm the cost and time information and associated commentary present an accurate reflection of the status of the project as at June 2022. We agree with the OAG's assessment of the project status.

Project 7

Metronet - Forrestfield-Airport Link

Entity Public Transport Authority

Phase Delivery

OAG's assessment

The project is in the final stages of delivery. The project will be completed within the approved budget but around 6 months later than the approved completion date and nearly 2 years after the original planned completion.

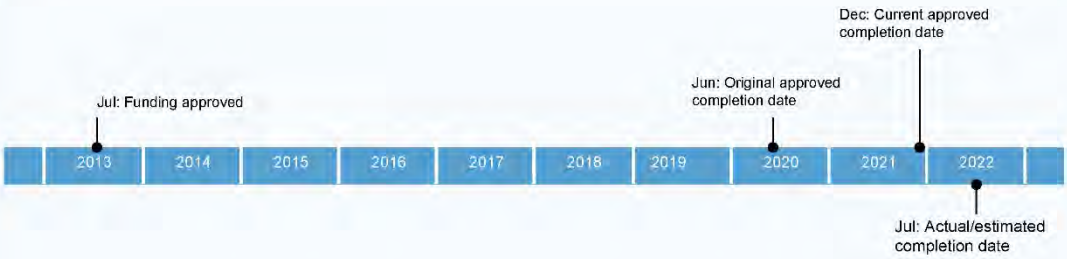
Cost

Funding of $2,015 million was originally approved for the Airport Rail project in the 2013-14 Budget under the Department of Transport. The project was transferred to the Public Transport Authority in the 2014-15 Budget and funding increased to $2,021 million. This was reduced to $1,861 million in the 2017-18 Budget with $60 million for rail cars transferred to the Future Urban Railcar Procurement Program and a further $100 million returned to Treasury.

At 30 June 2022 expenditure was lower than expected due to:

- ongoing delays in construction / commissioning works of the new Airport Line
- deferral of funding to manage defect liability period and project closeout activities which will commence after entry into service, practical completion and revenue services commence.

Time



The project completion date is about 2 years later than originally expected. Recently there has been delays to the supply of some specialist equipment and resources, and track laying progress was slower than expected which had a direct impact on the tunnel fit out activities.

Project summary

Forrestfield-Airport Link is a $1.861 billion State Government project to extend Perth's rail service, with 3 new train stations – Redcliffe, Airport Central and High Wycombe. The rail link will connect with the existing Midland Line near Bayswater Station and will run to High Wycombe through underground tunnels ensuring minimal impact on the existing land and road network. The design, construct and maintenance contract was awarded in April 2016. The first operational trains are expected to run before the end of July 2022.

Project status

At the time of reporting, the physical infrastructure had been completed including the 3 stations, 12 cross passages, 3 egress shafts and the tunnel fully fitted out with the required rail systems (track, overheads, signalling and communications).

Final commissioning, operational readiness checks and driver training are ongoing in anticipation that services will commence shortly.

Response from the entity

We confirm the cost and time information and associated commentary present an accurate reflection of the status of the project as at June 2022. We agree with the OAG's assessment of the project status.

Project 8

Metronet - Morley Ellenbrook Line

Entity Metronet

Phase Delivery

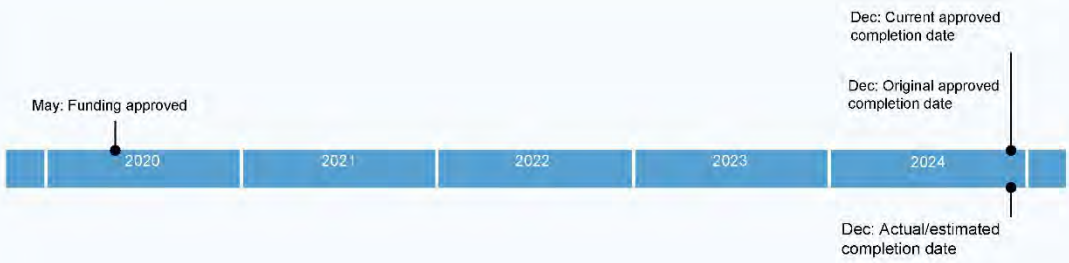
OAG's assessment

The project is in the early stages of delivery, on time and within budget.

Cost

The current budget remains unchanged from the original budget. The estimated/actual expenditure to 30 June 2022 is about $2.44 million more than the budgeted expenditure for the same period.

Time



Practical completion is still expected in July 2024 with entry into passenger service in December 2024. These dates are unchanged from the original approved completion dates.

Project summary

The Morley-Ellenbrook Line starts at Bayswater Station on the Midland Line, travels in the median of the Tonkin Highway exiting shortly after Marshall Road and travelling through Bennett Springs until it reaches Drumpellier Drive. The alignment then continues along the western side of Drumpellier Drive and ends in Ellenbrook, south of The Parkway.

The project includes:

- constructing 21.3km of new dual-track passenger railway from the Midland Line near Bayswater to Ellenbrook
- building 5 new stations at Morley, Noranda, Malaga, Whiteman Park and Ellenbrook complete with station infrastructure including parking, bus interchanges (excluding Noranda which will have on-street bus connections), cycling facilities, passenger amenities and standard station systems to cater for an estimated total of 18,070 daily boardings in 2031
- constructing 2 elevated rail structures, road bridges, one rail waterway bridge and one rail underpass
- constructing 3 new intersections and 3 new roads for station access
- constructing 2 rail pedestrian underpasses at Ellenbrook Christian College and Whiteman Park Station and 1 road pedestrian underpass at Benara Road, Morley
- constructing shared path connections in proximity to the stations to connect to existing pedestrian and cyclist networks.

Project status

Following contract award in October 2020, the project primarily focused on design throughout 2021 and into early 2022. Contractor mobilisation to site commenced in January 2022, with completion of site compounds at Ellenbrook, Whiteman Park, Bennett Springs and Malaga. Development approvals have been obtained for the majority of stations, with clearing, earthworks and other site preparation activities ongoing since early 2022, focusing on the 3 northern-most stations at Ellenbrook, Whiteman Park and Malaga.

Response from the entity

We confirm the cost and time information and associated commentary present an accurate reflection of the status of the project as at June 2022. We agree with the OAG's assessment of the project status.

Project 9

Queen Victoria Street - Swan River Crossing

Entity Main Roads WA

Phase Delivery

OAG's assessment

The project is in the delivery phase. The project is on time and budget, albeit due for completion 2 years later than originally approved and costing $50 million more.

Cost

An additional $50 million of funding was approved in the 2022-23 Federal and State Budgets for the impacts of cost escalation in the construction industry as well as approved changes to the alignment of the Bridge following stakeholder engagement.

Time

An alliance contract was awarded in January 2021. In response to a request from key stakeholders, additional planning and development work was undertaken to consider the feasibility of alternative configurations for the southern intersection at Queen Victoria Street / Canning Highway. This combined with efforts to find a more cost-effective solution delayed the commencement of construction and culminated in support of a new intersection design.

Construction is expected to start in late 2022 with completion due by late 2025 or early 2026.

Project summary

This project is fundamentally about replacing the aging Fremantle Traffic Bridge which will need to be closed due to its age, condition and continued deterioration. Replacing this bridge will continue to provide 2 road connections across the Swan River at Fremantle: the Stirling Bridge, which is the freight route for heavy vehicles servicing the Port; and the replacement road bridge, which will be used by light vehicles only and as a diversion route for freight when an incident occurs on the Stirling Bridge which requires lane closures.

The project is also about addressing the significant capacity constraints on the Fremantle Rail Bridge, which limit rail freight to access the Port to very limited times, which in turn places a 'cap' on the number of trains which can operate and the amount of freight which can be moved by rail.

The key outcomes to be provided by the project are:

- supporting the productivity of the Port by enabling the continued growth in container trade without adverse congestion impacts
- providing effective connectivity for rail freight, other traffic and pedestrians and cyclists across the Swan River
- addressing the navigational safety risks associated with the Fremantle Traffic Bridge
- providing river crossings which are achievable and sustainable, by aligning with stakeholders' requirements and minimising whole of life costs
- providing network resilience when disruptions to the flow of freight occur from incidents which close lanes on the Stirling Bridge.

Project status

Concept design development is underway for the changed intersection design.

Response from the entity

We confirm the cost and time information and associated commentary present an accurate reflection of the status of the project as at June 2022. We agree with the OAG's assessment of the project status.

Project 10

Tonkin Highway Gap - Collier Road to Stanton Road

Entity Main Roads WA

Phase Delivery

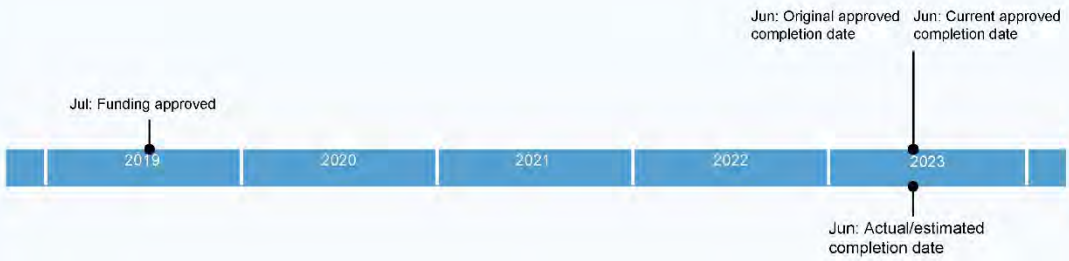
OAG's assessment

The project is in the mid-stages of delivery. The project faces some cost risks due to price increases.

Cost

The current budget is $230m higher than the original budget as the Expenditure Review Committee of Cabinet agreed in 2020-21 for the project to also deliver the Morley Ellenbrook rail enabling works along the Tonkin Gap corridor.
In 2021-22, expenditure of $138.5m above the $175.85m budgeted, was advanced in accordance with the delivery timeline opportunity, however the overall estimated expenditure for the project remains within the total project budget. Cost escalation mitigation measures have also been put in place to address any potential cost risks.

Time



Project is on-track for completion by 30 June 2023.

Project summary

The Tonkin Highway 'Gap' is approximately 8 kilometres east of Perth, between Great Eastern Highway and Collier Road. This section of Tonkin Highway forms part of a vital freight and commuter access route.

Traffic often exceeds design capacity at this location resulting in congestion and safety issues, limiting traffic flow benefits from recent and planned investments in other sections of the Tonkin Highway.

The project comprises:

- construction of collector - distributor roads between Guildford Road and Great Eastern Highway
- duplication (and/or widening) of existing bridges over Railway Parade, Guildford Road and Dunstone Road
- modifications to Great Eastern Highway interchange (including tie-ins to Stanton Road), reconfiguration or widening of existing Redcliffe Bridge and construction of new Redcliffe Bridge south / west of the existing bridge
- construction of new footbridge over Railway Parade and Guildford Road
- Principal Shared Path connectivity to and along Tonkin Highway
- safety barriers, noise walls, full street lighting and Intelligent Transportation Systems to ramps and mainline construction of an additional bridge north of the existing structure to enable future 4 all-lane-running capacity
- rail-enabling works for the METRONET Morley-Ellenbrook Line along Tonkin Highway, including underpasses and dive structures, to enable trains to enter and travel along the median of Tonkin Highway then exit in Malaga. Road and bus bridges will be built at Broun Avenue to provide access to the future Morley Station.

Project status

The project is just over 50% complete and has been tracking against agreed milestones.

Response from the entity

We confirm the cost and time information and associated commentary present an accurate reflection of the status of the project as at June 2022. We agree with the OAG's assessment of the project status.

Project 11

Tonkin Highway Grade Separation - Hale, Welshpool, Kelvin Roads

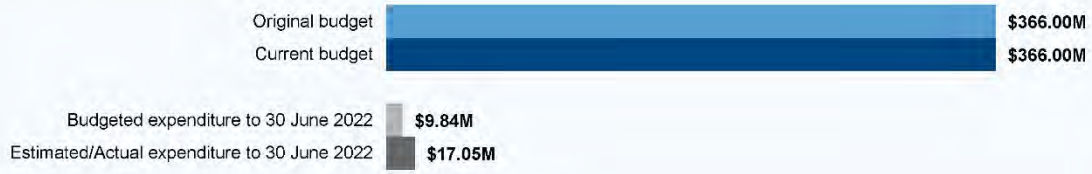
Entity Main Roads WA

Phase Planning

OAG's assessment

The project is in the planning phase. Its start date has been deferred and the completion date extended by 2.5 years to smooth the State's pipeline of work and ease industry pressures.

Cost



Estimated expenditure to 30 June 2022 exceeds what was budgeted by $7.21 million as a result of advanced project development activities, including land acquisition, geotechnical investigations and environmental compliance requirements budgeted in 2022-23 across the Tonkin Grade Separations Project. The project remains within its approved budget.

Time

Main Roads was originally working towards a start date of January 2022 and a finish date of June 2024. Following detailed consultation with industry, the State Government's infrastructure program was reviewed with a view to smoothing the pipeline of work to ease workforce pressures across the economy and create a long-term sustainable pipeline. As a result, project procurement has been delayed until June 2023 and the completion date extended to late 2026.

Project summary

The Tonkin Highway (South of Roe Highway) Project seeks to reduce congestion, improve safety and cater to growing demand in Perth's eastern suburbs. Three grade separations on Tonkin Highway at the intersections of Hale Road, Welshpool Road and Tonkin Highway will provide significant benefits to north-south commuters and freight traffic around the Perth Airport Industrial Hub.

The project scope includes:

- Tonkin Highway grade separated (elevated) at Hale Road ('Half Diamond' interchange with north-facing ramps), Welshpool Road ('Diamond' interchange) and Kelvin Road ('Diamond' interchange)
- widening Tonkin Highway to a 6 lane dual carriageway over a 6.2km section from south of Roe Highway to 1.1km south of Kelvin Road
- Principal Shared Path on eastern side of the Tonkin Highway for the full length with lighting, grade separation at interchanges and connections to side roads
- Intelligent Transport Systems, lighting of Tonkin Highway and road safety barriers where required.

Project status

All project development activities have been completed for the Hale Road and Welshpool Road interchanges and associated highway widening ready for procurement. Land acquisition, and environmental approvals are progressing and due for completion by December 2022.
Project development is being finalised for Kelvin Road and due for completion in June 2022. Environmental submissions are being finalised with approvals scheduled for early 2023.

Response from the entity

We confirm the cost and time information and associated commentary present an accurate reflection of the status of the project as at June 2022. We agree with the OAG's assessment of the project status.

Project 12

Tonkin Highway Stage 3 Extension - Thomas Road to South Western Highway

Entity Main Roads WA

Phase Planning

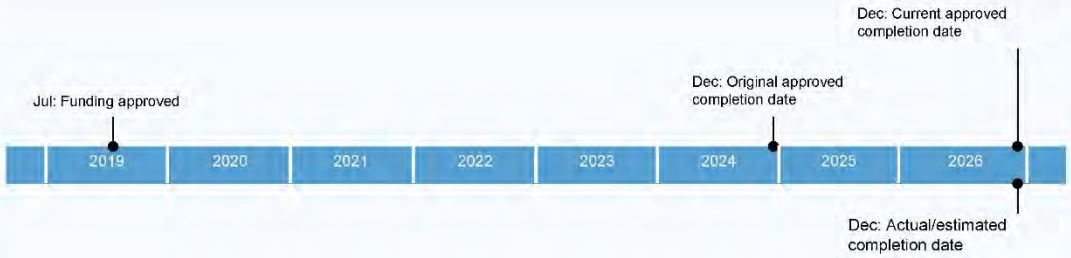
OAG's assessment

The project is in the planning phase. Its start date has been deferred and the completion extended by 2 years to smooth the State's pipeline of work and ease industry pressures.

Cost

The original funding of $505 million was announced by the Commonwealth Government in April 2019 and included in the 2019-20 Budget Papers. In March 2022, the Australian Government announced an additional $200 million for the project which has an 80%/20% funding share with the State Government funding $50 million. Funding was increased to include a grade-separated interchange at Bishop Road and cover cost increases from projects competing for limited labour, equipment and material supplies.

Time



Main Roads was originally working towards a start date of late 2022 and a finish date of June 2024. However, as a result of the State Government's consultation with the WA civil construction industry the WA transport infrastructure delivery program has been smoothed to develop a sustainable pipeline of work for coming years. As a result, project procurement has been delayed until mid-2023 and the finish date extended to late 2026.

Project summary

The Tonkin Highway Extension Stage 3 – Thomas Road to South Western Highway is expected to relieve traffic in the quickly expanding Byford and Armadale townsites in Perth's south eastern suburbs. The Project is imperative to support growth of nationally significant industry in the region and the expected residential growth fuelled in part by new employment opportunities in the region.

The project is planned to construct the 14km 4 lane extension of Tonkin Highway from Thomas Road to South Western Highway south of Mundijong Road. The scope includes:

- 4 lanes road extension (2 lanes each direction) from Thomas Rd to South Western Highway with provision to widen to 6 lanes in the future
- upgraded intersection at Thomas Road
- new intersections at Orton Road, Mundijong Road and South Western Highway
- new grade separated interchange over the freight railway and Bishop Road
- bridges over the existing freight rail line, Perth to Bunbury passenger rail line, Wright Road and Shanley Road
- shared path along the eastern side of Tonkin Highway, with planned connections to local path networks
- equine, pedestrian and cyclist underpasses under Tonkin Highway at Abernethy Road and near Gossage Road.

Project status

Project development activities are progressing with community consultation for the equine underpasses and network connectivity strategy taking place. Environmental approvals have been obtained, with heritage approvals and geotechnical investigations progressing. The land acquisition process has started. The freight railway realignment planning activities will continue as a separate project and will not be delivered by this contract.

Response from the entity

We confirm the cost and time information and associated commentary present an accurate reflection of the status of the project as at June 2022. We agree with the OAG's assessment of the project status.

Project 13

Fuel Jetty Rottnest Island

Entity Department of Biodiversity, Conservation and Attractions - Rottnest Island Authority (RIA)

Phase Complete

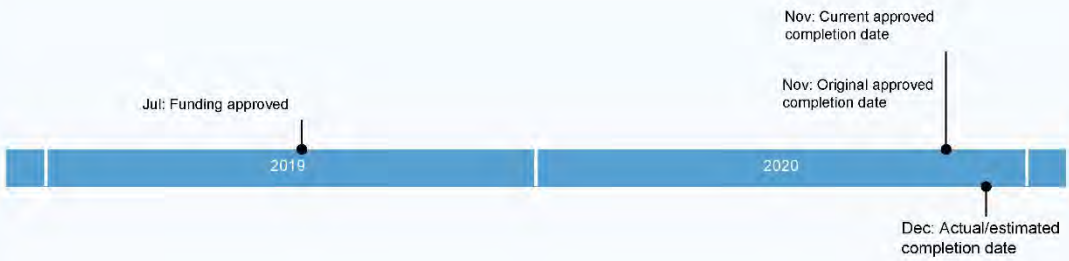
OAG's assessment

The project was completed on time and on budget.

Cost

The original budget was $0.5 million. This was increased to $3 million following a condition and structural assessment which changed the scope of the project from minor works to complete replacement. The project was completed within the approved $3 million budget.

Time



The project was completed on 4 December 2020, within 4 days of the approved practical completion date.

Project summary

The Fuel Jetty in Thomson Bay on Rottnest Island is a critical piece of infrastructure for small recreational and commercial vessels on the island. The jetty was approaching the end of its design life. The project involved demolishing the existing jetty and rebuilding it with upgrades.

Project status

Complete.

Response from the entity

We confirm the cost and time information and associated commentary present an accurate reflection of the status of the project as at June 2022. We agree with the OAG's assessment of the project status.

Project 14

Main Jetty Rottnest Island

Entity Department of Biodiversity, Conservation and Attractions - Rottnest Island Authority (RIA)

Phase Delivery

OAG's assessment

The project is in the mid-stages of delivery and is on track to meet the revised cost and time budgets, however some cost risks remain. It is due for completion by December 2023.

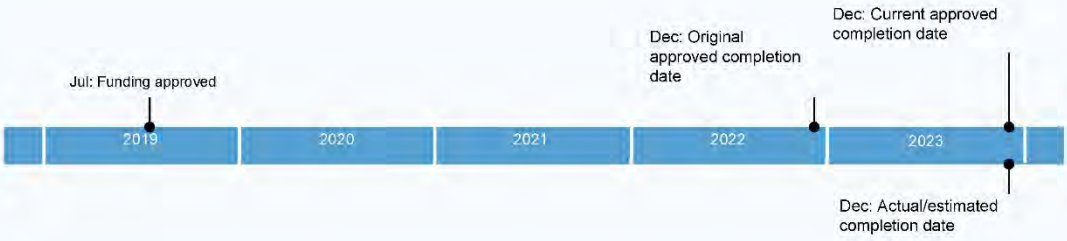
Cost

The budget has increased by over $6 million from $5.65 million to $12.90 million to cover significant cost escalations for the reconstruction of the Berth 4 and 5 concrete deck area since the original budget allocation.

The approved budget was also increased in the recent May 2022 Budget as a result of $800,000 for the South Thomson Bay Development (Barge and Cargo Landings) project being reallocated to this project. The estimated expenditure of $2.4 million is lower than the $4 million budgeted. This reflects a revised cashflow following award of the main construction tender.

Cost risks remain with tenders still required to complete fire hydrants and sheet and fender pile works.

Time



The project is on track for completion by December 2023.

The T-jetty upgrade and anode replacement on the sheet pile wall (Berths 1,2 and 3) were completed this financial year. The tender for the reconstruction of the Berth 4 and 5 concrete deck area has been awarded and will be completed in November 2022. The completion of the fire main and hydrants depends on the tender prices received for the sheet pile refurbishment (Berths 1,2 and 3) and the anchor pile upgrade (Berths 1 and 2).

Project summary

The Main Jetty and associated barge and cargo landing facilities are situated in Thomson Bay on Rottnest Island. The jetty provides primary access to and from the Island by ferry for people, luggage and bikes. The barge and cargo landing facilities provide access for a range of commercial supplies and larger cargo.

The Main Jetty has 5 ferry berths. Berths 1, 2 and 3 extend out from the shore on the south side and are protected by a rock wall on the north side of the jetty. Berths 4 (south side) and 5 (north side) were built in the 1970s as an extension of the original jetty and are near the end of their serviceable life. A T-jetty on the north side about halfway along the jetty is available for recreational vessels.

A study commissioned by the Rottnest Island Authority found the concrete deck and piles for berths 4 and 5 need replacing and a wave screen needs to be built to protect berth 4 during northerly winds. The sheet and fender piles for berths 1-3 also need refurbishment and fire hydrants need to be installed along the jetty. The barge landing and cargo facilities need reconstruction.

Project status

The project is on track for completion by December 2023.

Response from the entity

We confirm the cost and time information and associated commentary present an accurate reflection of the status of the project as at June 2022. We agree with the OAG's assessment of the project status.

Project 15

South Thomson Bay Development Rottnest Island (Barge Landing and Cargo Facilities)

Entity Department of Biodiversity, Conservation and Attractions - Rottnest Island Authority (RIA)

Phase Did not proceed

OAG's assessment

The project is no longer supported and funding for upgrade of the barge and cargo facilities has been transferred to the Main Jetty project.

Cost

N/A

Time

N/A

Project summary

The business case was not supported. Funding of $800,000 has been reallocated to the Main Jetty project so the upgrades can proceed.

Project status

The project is no longer funded.

Response from the entity

We confirm the cost and time information and associated commentary present an accurate reflection of the status of the project as at June 2022. We agree with the OAG's assessment of the project status.

Project 16

Common Ground - East Perth

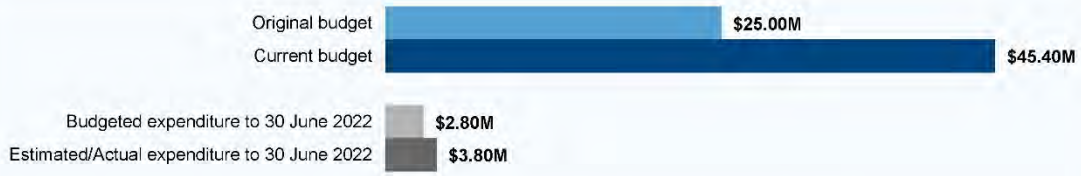
Entity Department of Communities

Phase Procurement

OAG's assessment

The project is in the procurement phase. It faces cost risks due to construction industry pressures. However, $8.5 million, not included in the approved budget, has been provisionally approved to cover cost escalations.

Cost

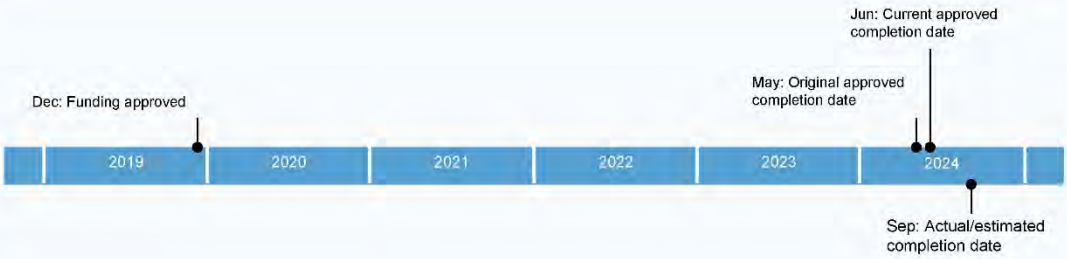


The original project budget has been increased by around $20 million from $25 million to $45 million.

The budget increase from the original announcement in 2019 was due to the State Government's approval of the Business Case, which increased the capacity of Common Ground East Perth to 112 units in response to the growing number of people sleeping rough in Perth.

Due to the ongoing impact of the COVID-19 pandemic on the construction industry, and as part of the 2022-23 State Budget process, $8.5 million is provisionally approved to cover cost escalations.

Time



The practical completion date was revised to June 2024 based on the Project Definition Plan, which refined the project schedule and procurement method.

Due to impacts from COVID-19 on the current construction market, the current estimated practical completion date is September 2024. Common Ground East Perth will become operational by December 2024.

Project summary

Common Ground is a model of homelessness services and housing provision, providing permanent accommodation to people who have experienced chronic homelessness, affordable housing to low-income earners, and on-site, wrap around services to individuals who need them.

The purpose-built East Perth Common Ground facility will be located on the corner of Hill and Wellington Streets and will comprise 112 self-contained apartments along with communal areas, on-site support services and commercial space.

Project status

In October 2021, an Expression of Interest for the construction head contractor was advertised and shortlisted respondents were notified in January 2022.

In January 2022, the project architect achieved 100% design development.

In March 2022, the restricted Request for Tender for the head construction contractor was published. The tender closed in May with the evaluation of responses underway and anticipated for finalisation in June 2022.

Response from the entity

We confirm the cost and time information and associated commentary present an accurate reflection of the status of the project as at June 2022. We agree with the OAG's assessment of the project status.

Project 17

Common Ground - Mandurah

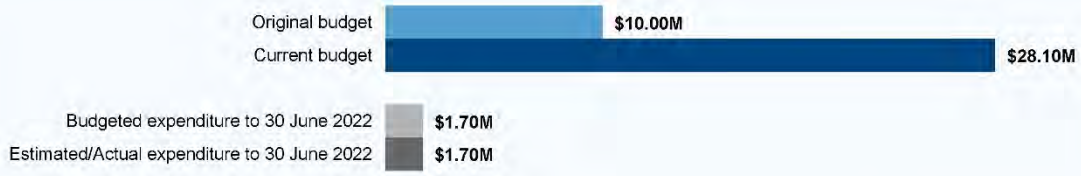
Entity Department of Communities

Phase Planning

OAG's assessment

The project is in the planning phase. It is within its approved cost budget but has identified potential cost risks due to increased prices for materials and labour. The project definition plan (PDP) estimates a practical completion date of October 2024, 5 months later than the practical completion date outlined in the Business Case.

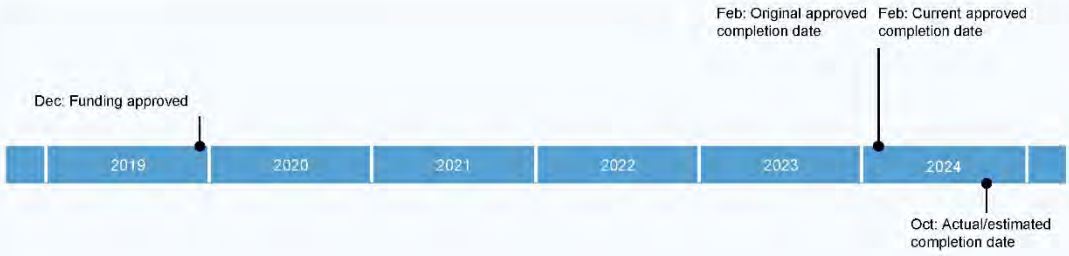
Cost



The original project budget has been increased by around $18 million from $10 million to $28.1 million. The budget increase was due to the State Government's approval of the Business Case, which increased the capacity of Common Ground Mandurah to 50 units in response to the growing number of people sleeping rough in Mandurah.

Based on finalised concept designs and cost escalations due to labour and material shortages from COVID-19, costs may be higher than previously approved. A revised budget will be finalised upon approval of the PDP.

Time



The PDP has refined the project schedule and procurement method and outlines a practical completion of October 2024. The revised practical completion date is also due to additional time required for Mandurah site negotiations and acquisition.

Project summary

Common Ground is a model of homelessness services and housing provision, providing permanent accommodation to people who have experienced chronic homelessness, affordable housing to low-income earners, and on-site, wrap around services to individuals who need them.

Mandurah Common Ground will be located at 81-87A Allnutt Street, Mandurah. The purpose-built facility will deliver up to 50 self-contained apartments with communal areas, on-site support services and commercial space.

Project status

The project is currently at the preliminary design and PDP approval phase. As part of the PDP process the project budget is being refined through independent cost estimates, and finalisation of the concept design. The PDP will be reported back to the Expenditure Review Committee to seek approval and release of the final capital budget in June 2022.

Response from the entity

We confirm the cost and time information and associated commentary present an accurate reflection of the status of the project as at June 2022. We agree with the OAG's assessment of the project status.

This page is intentionally left blank

Auditor General's 2021-22 reports

Number	Title	Date tabled
16	Staff Rostering in Corrective Services	18 May 2022
15	COVID-19 Contact Tracing System – Application Audit	18 May 2022
14	Audit Results Report – Annual 2020-21 Financial Audits of State Government Entities Part 2: COVID-19 Impact	9 May 2022
13	Information Systems Audit Report 2022 – State Government Entities	31 March 2022
12	Viable Cycling in the Perth Area	9 December 2021
11	Forensic Audit Report – Establishment Phase	8 December 2021
10	Audit Results Report – Annual 2020-21 Financial Audits of State Government Entities	24 November 2021
9	Cyber Security in Local Government	24 November 2021
8	WA's COVID-19 Vaccine Roll-out	18 November 2021
7	Water Corporation: Management of Water Pipes – Follow-Up	17 November 2021
6	Roll-out of State COVID-19 Stimulus Initiatives: July 2020 – March 2021	20 October 2021
5	Local Government COVID-19 Financial Hardship Support	15 October 2021
4	Public Building Maintenance	24 August 2021
3	Staff Exit Controls	5 August 2021
2	SafeWA – Application Audit	2 August 2021
1	Opinion on Ministerial Notification – FPC Arbitration Outcome	29 July 2021

Office of the Auditor General
Serving the Public Interest

Office of the Auditor General
Western Australia

7th Floor Albert Facey House
469 Wellington Street, Perth

Perth BC, PO Box 8489
PERTH WA 6849

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

@OAG_WA

Office of the Auditor General for
Western Australia

(Appendix AAR: 8.1C)

Western Australian
Auditor General's Report

Forensic Audit – Construction Training Fund

Office of the Auditor General
Western Australia

Audit team:
Carl Huxtable
Forensic Audit team

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

Forensic Audit – Construction Training Fund

Report 19: 2021-22
June 2022

This page is intentionally left blank

THE PRESIDENT
LEGISLATIVE COUNCIL

THE SPEAKER
LEGISLATIVE ASSEMBLY

FORENSIC AUDIT – CONSTRUCTION TRAINING FUND

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

Forensic audits seek to identify vulnerabilities to, and indicators of, significant fraud in State government entities. Their purpose is to improve resilience to fraud across the WA public sector.

This audit focused on identifying key risks to payment fraud in targeted areas of the finance and payroll systems of the Construction Training Fund.

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

CAROLINE SPENCER
AUDITOR GENERAL
22 June 2022

Contents

Auditor General's overview

The Construction Training Fund (CTF) collected $45 million last year in levies from residential, commercial and civil engineering projects valued at more than $20,000. Levies are intended to be returned to the building and construction industry to subsidise training for apprentices, trainees and mid-career retraining and upskilling.

The building and construction industry in Western Australia is experiencing boom conditions, but is under some stress, as evidenced by the collapse of a number of high profile builders. The utility of the CTF could not be more important at this time, noting further support from the fund was announced in the 2022-23 State Budget for the development of Western Australia's construction industry workforce.

This forensic audit was initiated in response to a number of risks identified during our financial audits, which resulted in audit findings and a qualified controls opinion in 2020-21, and through referrals and other risk indicators over a number of years. This audit set out to identify key risks in targeted areas of payment fraud within the CTF's finance and payroll systems.

Until recent times, and similar to some other (self-funded) public entities, the CTF has not sufficiently demonstrated a sound understanding of its obligations to operate within the public sector governance framework.

Through our forensic audit work, which goes deeper in particular areas than an annual financial audit can do, we found serious deficiencies in systems, processes and controls, which exposes the CTF to significant fraud risk. More concerningly, the CTF is unable to examine whether fraud vulnerabilities have been exploited in some areas in the past due to a lack of records.

Conditions for fraud in CTF have certainly existed in recent years, driven by environmental and administrative red flags, including:

- new systems integration
- senior management and board member turnover
- inactive fraud controls
- poor record keeping
- poor configuration and use of financial management systems
- poor conflict management
- a growing cash balance over the last 3 years (in excess of $40 million at 30 June 2021, representing a $10 million increase from 2020)
- the impact of COVID (new grants, subsidies and revised WA procurement thresholds).

The CTF has taken some intensive steps over recent years to uplift its resilience through implementing new systems and key controls, using third party data for validation purposes and creating a conflict of interest register. I am encouraged by these and other recent determined tangible efforts by both past and present chief executive officers, however there is much more to be done. The Board, Chief Executive and Minister must maintain keen oversight so that momentum in the pace of necessary control improvements continues, and adequately addresses identified shortcomings to raise CTF's financial governance to a level acceptable for a public entity.

Introduction

Targeted, risk based forensic audits identify vulnerabilities to, and potential indicators of, significant fraud to improve resilience to fraud and corruption across the Western Australian (WA) public sector.

Public sector entities (entities), together with their audit and risk committees and boards, are responsible for establishing governance arrangements and financial management controls with multiple lines of defence against fraud. This includes building strong integrity frameworks and effective fraud prevention, identification and response capabilities. Ineffective identification and management of fraud risk by entities exposes them to financial loss, compliance costs and staff turnover as well as eroding public confidence that funds are appropriately directed to essential services.

Selecting an entity for a forensic audit does not mean we suspect fraud or corruption is occurring. Our audits are targeted where there are a number of flags to indicate that significant fraud risks exist and we do not have confidence they are being well managed. Our intent is, preferably, to identify vulnerabilities that can be eliminated before fraud has occurred.

This forensic audit into the Building and Construction Industry Training Board was initiated in response to a number of risks identified during our financial audits, which resulted in a qualified controls opinion in 2020-21, and through referrals and other risk indicators over a number of years. The objective of the audit was to identify key risks to payment fraud in targeted areas of the finance and payroll systems. This was not a review of the entire fraud control system, nor did it examine all of the entity's activities.

This is our first forensic audit report following our introductory *Forensic Audit Report - Establishment Phase.*[1]

Background

The Building and Construction Industry Training Board (the Board) is a statutory authority whose purpose is to create a skilled and sustainable workforce for the WA building and construction industry. It is managed by industry representatives and an independent chairperson with members appointed by the Minister for Education and Training.

The Board oversees an account called the Building and Construction Industry Training Fund (BCITF). The Board, its staff and its oversight of the BCITF are branded as the Construction Training Fund (CTF).

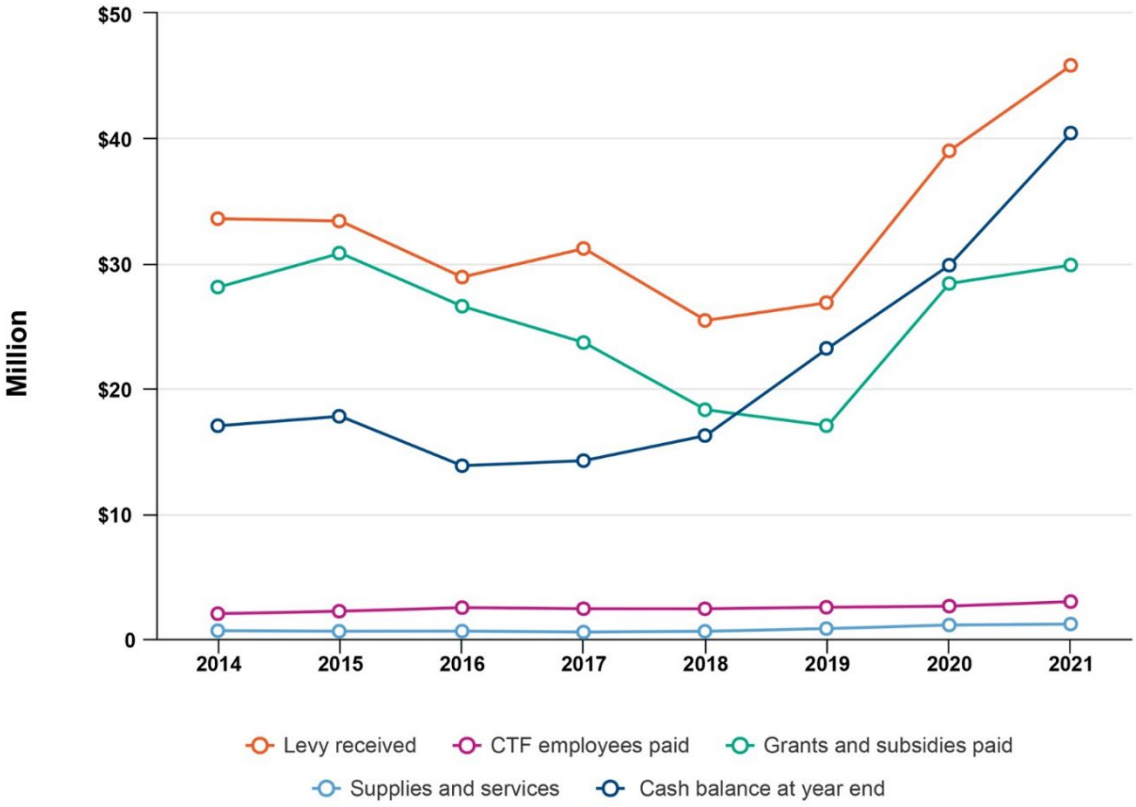
Under the *Building and Construction Training Fund and Levy Collection Act 1990* (CTF Act), the CTF collects a training levy on all building and construction projects in WA valued at more than $20,000. Collected levies are intended to be used to subsidise the training of a diverse, job-ready workforce and educate the next generation about the variety of roles and opportunities on offer in the building and construction industry. Most of the levies collected are paid to:

- several thousand different construction related businesses across the State employing apprentices working towards relevant qualifications
- registered training organisations through grants and subsidy payments.

This has included special COVID payments to support the industry locally.

[1] Western Australian Auditor General's Report, *Forensic Audit Report - Establishment Phase*, Report 11: 2021-22, 8 December 2021.

The extension of the levy to the resource sector in October 2018 and an increase in construction activity have significantly raised the amount collected. Figure 1 illustrates the increase in the levies received and payments made for the financial years ended 30 June 2014 to 2021.



Source: OAG using information from CTF annual reports

Figure 1: The CTF's cash balance at year end, levy received and expenditures paid

Since March 2020, there have been substantial personnel movements, including a new Board Chair, a new Chief Executive and Corporate Services team, and turnover in half of the Board's membership.

The CTF has also experienced major changes to its corporate operations in recent years, including:

- a new financial management system in 2019
- a new client management system in 2018
- a new payroll system in 2019
- integration of information obtained from the WA Apprentice Management System maintained by Department of Training and Workforce Development in 2020.

These system changes and increased volume of transactions have affected the CTF's risks and its capacity to manage them.

The government announced 'a $14.3 million investment in the 2022-23 State Budget to support the development of Western Australia's construction industry workforce and provide financial support to apprentices and trainees'.[2] This will likely increase the volume of transactions and associated risks.

[2] Government of Western Australia, *State Budget's $14.3 million boost to build construction careers*, media statement, 13 May 2022.

Conclusion

Until recent times, the Construction Training Fund (CTF) has not sufficiently demonstrated a sound understanding of its obligations to operate within the public sector governance framework.

Our in-depth forensic audit found that the CTF's disorganised financial management exposes it to an alarming level of fraud vulnerability.

From the forensic audit procedures we conducted, using data analytics to examine the last several years of many (but not all) types of financial transactions, we identified numerous shortcomings in process and controls, and significant instances of non-compliance with procurement and record keeping obligations.

While we can never provide absolute assurance that there has not been financial wrongdoing, we are confident that the multiple concerning findings in this case represent a level of incompetence or lack of care, rather than corruption. However, all the pre-conditions were in place for fraudulent activity to occur undetected.

Identified issues represent non-compliance with public sector procurement requirements and record keeping obligations under the *State Records Act 2000,* with inappropriate loss or destruction of payroll records upon system changeover in 2019.

While not within the scope of this audit, we noted that the CTF's process for assessing the eligibility of the thousands of claims for apprenticeship-related grants and subsidies was labour-intensive and relied heavily on the manual review and diligence of the claims team. The CTF should undertake data analytics and spot checks to verify the accuracy and legitimacy of such payments.

We acknowledge the extensive corporate reform since 2020, which continued apace during the audit. Under its new leadership, the CTF has already made changes to improve compliance and its control environment, but we have identified further urgent work needed to be undertaken to lift its systems of governance to an acceptable level and have made recommendations in this regard. This will take ongoing sustained effort and time. We have provided further in-depth findings and analysis to the CTF to assist in this endeavour.

Findings

Finance system control weakness: inability to verify changes to information stored in the CTF finance system or supplier master file

We found that the CTF had not activated the audit logging function on its new finance system since implementation in March 2019.

An audit log provides an essential date and time stamped sequential history of changes to accounting records in the finance system. This log allows reviewers to detect if staff have changed information in their finance system and investigate the appropriateness of those changes.

Our data matching identified 8 payments (totalling $196,814) that were paid to incorrect bank accounts between January 2020 and June 2021. Due to an absence of audit logs, we were unable to verify who entered the account numbers and when.

Three of the payments (totalling $178,451) had already been identified by the recipients and rectified with the CTF prior to our audit commencing, suggesting incompetence and sloppiness in financial administration and not collusion for nefarious purposes.

We provided the details of the remaining 5 payments (totalling $18,362) to the CTF for investigation. Four were made to bank accounts that were not known to the CTF. We were unable to conclude if these payments were the result of fraud or error due to a chaotic control environment in the finance system.

In addition to inactive audit logs, the CTF has not maintained adequate supporting documents for changes made to the supplier master file.[3]

We identified 148 suppliers with different bank details (BSB and account numbers) between the payments list and supplier master file. Of these, 83 were due to clerical errors, 34 appeared to be legitimate bank account changes and we were unable to verify the remaining 31 due to an absence of supporting documentation.

The lack of audit logs and the inability to monitor changes increases the risk that fraudulent or erroneous payments will go undetected. Of more concern is that post-transaction audits or investigations are obstructed by lack of evidence of who, when and why changes were made.

Finance system control weakness: insufficient controls to prevent duplication and detect fraudulent supplier payments

Between March 2019 and June 2021, 3% of transactions (1,441) recorded in the CTF's financial management system did not include an invoice number. Invoice numbers are essential to identify the correct record for payment as without them there is a risk of incorrect (including duplicate) or fraudulent payments going undetected.

We identified apparent duplications in the supplier master file, such as:

- 1 supplier created 19 times

[3] The central, comprehensive file that holds information about suppliers.

- 157 suppliers with 58 common addresses
- 522 suppliers with 168 common email addresses
- 271 suppliers with 127 common contact numbers.

These findings are concerning as duplication of suppliers increases the risk of incorrect or fraudulent payments going undetected.

We found the current supplier master file does not have mandatory fields such as Australian Business Number (ABN), addresses and emails to uniquely identify the supplier (see Table 1). We also found the CTF's current process of creating a new supplier does not require an independent verification of the supplier banking information such as bank correspondence evidencing the business name and account number. Inadequate supplier due diligence increases the risk of fraudulent payments being made to false entities.

Total vendors	Without ABN	Without address	Without email	Without contact number
5,539	35%[4] (1,967)	42% (2,308)	3% (191)	26% (1,443)

Source: OAG using information from the CTF current supplier master file

Table 1: Summary of supplier master file for key identifiers

While not within the scope of this audit, we noted that the CTF's process for assessing the eligibility of the thousands of claims for apprenticeship-related grants and subsidies was labour-intensive and relied heavily on the manual review and diligence of the claims team. The CTF should undertake data analytics to verify the accuracy and legitimacy of such payments.

We analysed the CTF's apprenticeship-related grants and subsidies against the apprenticeship data provided by Department of Training and Workforce Development and found:

- 4 instances where group training organisations were incorrectly paid as the apprentices were no longer active during the period[5]
- 8 instances ($21,000 in total) where the CTF had paid the employers more than the COVID support bonus.

Poor assessment of fraud risk

The CTF does not perform a fraud risk assessment, which is an essential process in managing fraud risk.

A fraud risk assessment involves:

- identifying fraud risks specific to an entity
- analysing those fraud risks, considering resources, consequences, likelihood and control effectiveness
- evaluating the outcomes of the analysis against the entity's overall risk appetite
- treating those risks by implementing controls to reduce opportunities for exploitation.

[4] Only 1% of the supplier master file in previous finance system contained ABNs.

[5] Our data request did not include information to quantify these overpayments.

A fraud risk assessment would highlight the CTF's exposure to fraud vulnerabilities in its core business. Regular fraud risk assessments, a fundamental element of risk management, would highlight new and emerging risks. Exposure to fraud vulnerabilities from an increase in the number of transactions, total funds collected and changes in processes, systems and key personnel could be analysed, evaluated and treated.

Effectively understanding fraud risks would allow the CTF to implement essential controls such as audit logs and data retention when implementing new finance and payroll systems.

Poor management of conflicts of interest

The CTF's current *Conflicts of Interest (COI) Policy* was published in December 2020. We were not provided with any evidence of a policy or register prior to this date. The policy states that it applies to all employees engaged to work for the CTF, including direct employees, secondees and contractors.

Board members, who are omitted from this policy, are industry representatives appointed by the Minister for Education and Training. Consequently, their appointment creates a perceived, and potential for an actual, conflict of interest on different matters that come before the Board.

The CTF Act requires Board members to disclose, and record in minutes of the Board, direct or indirect interests in proposals before the Board and exclude themselves from any deliberation or decision on them. Interests are also disclosed via annual reports.

Better practice may be achieved through the addition of a standing board member declaration in the central conflict of interest register with a management plan consistent for each board member.

We also found that historical conflicts are removed when the conflict no longer exists. This prevents validation of declarations and the ability to confirm whether appropriate mitigation programs were implemented. A permanent record of all declarations made should be maintained.

We analysed the CTF's employees and suppliers using relationship mapping to identify potentially undisclosed relationships amongst them and identified 32 relationships for further examination. These included:

- declared relationships (declared verbally, in meeting minutes and by disclosure in annual reports however some of these were not recorded in the conflict of interest register)
- relationships inadvertently created by poor financial administration in the CTF
- distant professional relationships between employees and suppliers which did not raise concerns in this instance.

We reviewed transactions related to the 32 relationships identified, the majority of which appear reasonable. Due to the poor financial administration at the CTF, we were unable to form an opinion as to reasonableness of transactions relating to a handful of these relationships. All relationships have been provided to the CTF management for review.

While not within the scope of this audit, we found some payments were payroll to casual staff, board fees and settlement of an employee's final entitlements. The CTF should investigate if these payments had complied with the Australian Tax Office's pay as you go withholding requirements and rectify accordingly if required.

Evidence of non-compliance with Western Australian Procurement Rules

We found that the CTF did not maintain a contracts register. Maintaining a comprehensive contracts register is essential for contract management and accountability. It also enables entities to meet their financial reporting obligations while providing better transparency for procurement oversight.

Treasurer's Instruction (TI) 820 Register of Contracts, which came into effect in September 2016, required entities to maintain a contracts register that records key contract information. The TI was replaced by the Department of Finance's Western Australian Procurement Rules Procurement Direction 2021/02 Rule F5 Establish and Maintain a Contracts Register.

The CTF did not use purchase orders in its procurement process. Purchase orders detail the intended purchase of goods or services from external suppliers and should be approved by a delegated staff member. The use of purchase orders is not mandated but is an important fraud risk control and budget management tool.

The CTF's procurement procedures are consistent with the minimum competitive requirements set out in the Procurement Direction 2021/02 Rule C4 Procurement Method. However, the CTF was unable to provide records demonstrating compliance with their procedures for all but 1 of the 23 suppliers' engagements we examined. Inadequate record keeping impacted our ability to make informed decisions on the legitimacy of the CTF's procurement activities.

We also found that the CTF has not purchased from the mandatory common use arrangements (CUA) for booking domestic air travel and purchasing card services. These CUAs are in place for entities to deliver savings through pre-negotiated pricing and efficiencies like easy ordering and risk mitigation strategies.[6] State government entities must purchase from mandatory CUAs unless specifically exempt.[7]

A culture of non-compliance and the absence of a contracts register, purchase orders and procurement records reduces transparency and increases fraud risk.

Evidence of non-compliance with *State Records Act 2000* requirements

In August 2019, the CTF changed to a new payroll system but the existing payroll data was not transferred to the new system. The CTF advised it could not provide this legacy data as it no longer exists.

Also, during our verification procedures of non-payroll transactions, we found that the CTF was unable to provide standard payments verification records, such as supplier invoices and receipts in 90 of 235 transactions selected for review.

These examples show non-compliance with the State Records Office's minimum retention requirements under the *General Disposal Authority for State Government Information*.[8] Inadequate record keeping impacted our ability to make informed decisions on the accuracy and legitimacy of payments and increases the CTF's vulnerability to the risk of fraud.

[6] Western Australian Government, 4 May 2022, Department of Finance, viewed 9 June 2022, <https://www.wa.gov.au/government/cuas/common-use-arrangements-cuas>.

[7] Western Australian Government, 23 August 2021, Department of Finance, viewed 9 June 2022, <https://www.wa.gov.au/government/multi-step-guides/western-australian-procurement-rules/section-c-procurement-planning>.

[8] Western Australian Government, 7 June 2022, State Records Office of Western Australia, viewed 9 June 2022, <https://www.wa.gov.au/government/document-collections/retention-and-disposal-of-state-records#general-disposal-authority-for-state-government-information>.

Recommendations

1. The CTF should:

    a. in the context of its risk management framework:

        i) implement regular and detailed assessment of fraud risks to identify current and emerging risks, particularly when significant changes to its operations are foreseeable such as with new government policy announcements or market conditions

        ii) urgently implement fit for purpose fraud risk treatment controls to the standard expected of the WA public sector including, for example[9]:

            (1) ensure vendor information in its system is an exact match to public records such as the Australian Business Register

            (2) ensure all information required to be included in a tax invoice is recorded in the system

            (3) ensure correct cost codes are used in respect of payments

            (4) create a system check to flag instances where third party data does not match the entity's data

            (5) enable all available system-based audit logging[10] functions and monitor relevant logs for inappropriate entries

            (6) commence regular data analysis to provide additional oversight of payments

        iii) ensure records are properly maintained for key payment and supplier management processes

    b. in respect of procurement:

        i) use mandatory common use agreement suppliers and maintain a contracts register

    c. in respect of record keeping:

        i) ensure records are maintained

        ii) ensure a conflict of interest register is maintained that includes:

            (1) board members

            (2) a permanent record of all declarations made

        iii) consider the implications of possible breaches of the *State Records Act 2000* and Western Australian Procurement Rules. The CTF should also report actual breaches to the relevant entities.

[9] This is not indicative of all controls that should be implemented, only examples based on vulnerabilities we have identified in this limited scope examination of the CTF.

[10] An audit logging function provides an essential date- and time-stamped sequential history of changes to accounting records in the finance system.

Construction Training Fund response to recommendations:

Management accepts all recommendations.

Within the context of the CTF's risk management framework, the CTF has established a strategic risk management framework within the CTF's strategic plan that was implemented in 2021. In April 2022 an operational risk review was performed, with treatment plans currently being finalised.

Several system and manual fraud treatment controls have been implemented to mitigate the risk of fraud; however, management acknowledge further improvement is required with continued reform of the CTF. The enhancement of the CTF's grant management and financial management information systems are a key fraud risk treatment strategy for the CTF.

In respect to procurement, the CTF has begun the process of transitioning all relevant contracts to mandatory Common Use Arrangements, with a contract register now implemented.

In respect of recording keeping a review of all record keeping systems, policies, practices, and staff training is underway with an expected completion date of 31 December 2022.

Implementation timeframe: 31 December 2022

Response from the Construction Training Fund

The Construction Training Fund (CTF) acknowledges the Summary of Findings reflects the historic governance and the financial management practices of the agency. Management wish to thank the Office of the Auditor General for their expertise, professionalism, and rigour in conducting their review. Whilst no fraudulent activity was detected during the review, management recognise that within the CTF, an environment existed that if a fraudulent act was perpetrated it would have been problematic to prevent or detect.

During the review period the Minister appointed a new Board Chair, a new Chief Executive Officer was recruited and at the end of the review period a new Chief Finance Officer was recruited. Prior to the Office of the Auditor Generals Forensic review, the Board, under its new Chair and newly established Audit, Risk and Performance Committee, and the Chief Executive Officer instigated several internal audits through an external provider, to assess the effectiveness of the CTF's governance and processes, which has allowed organisational reform to begin before the commencement of this review.

In relation to the finance system controls, the CTF established and recruited a dedicated IT Systems Manager and engaged an external ICT firm to perform an examination of the grant management system and financial management system which were poorly implemented in 2018 and 2019 respectively. The examination has concluded, with findings and recommendations delivered to the Board and management in March 2022. Management have begun the process of securing the funding approvals for commencement of the procurement process to undertake the recommended significant re-implementation of these critical systems.

Due to the size of the agency and the increasing workload, critical financial functions and their oversight were inadequately segregated and managed. Historically, the control environment was designed to effectively manage the workload within a small team with a high volume of work rather than having fraud prevention and detection as its central feature.

The CTF implemented a new structure on 1 July 2021 and management continue to review and update the structure to ensure appropriate resources, processes, and control effectiveness is in line with the CTF's risks. The CTF currently has 30 employees, managing a budgeted total cost of services of $52 million in 2022-23. To further support the governance practices, the CTF has implemented a project management framework to improve governance and accountability and procurement in new initiatives and is increasing engagement with relevant government agencies such as the Department of Finance to improve compliance in government procurement processes.

A conflict-of-interest policy was approved in December 2020 and the CTF continues to improve employee awareness of perceived and actual conflicts of interest and the actions required to declare the interest and excuse themselves from any related decision-making process. A conflict-of-interest register is now in place. The conflict-of-interest policy and forms are provided to all employees, Board members and Committee members and are provided in the induction pack for new employees and Board members. Accountable and ethical decision-making training is delivered to all employees and Board and Committee members annually. A standing agenda item has been included on all Board and Committee meetings for declaration of interests and contact with lobbyists.

Management acknowledges its inability to locate and produce sufficient historical records of its procurement processes to substantiate compliance with mandated WA Government procurement practices. A contract register has been established, procurement processes and policies published with ongoing training of employees who have been delegated

procurement responsibilities by the Board. Significant work has been undertaken to improve record keeping practices across the organisation.

Audit focus and scope

Our audit focused on identifying key risks to payment fraud in the finance and payroll systems of the CTF. We pieced together extracts of historical data across 8 current and legacy business systems for testing.

We designed insider fraud detection tests using extensive data analytics and interrogated the anomalies. This was not a review of the CTF's entire fraud control system nor did it examine all of the CTF's activities, such as the allocation of grants or receipt of levies. This examination was limited in scope to focus on potential:

- ghost employee payments
- fraudulent supplier payments
- awarding of work to employee related suppliers
- fraudulent payment of grants and subsidies[11]
- manipulation of bank transfers.

Forensic testing methods included but were not limited to:

- Benford's Law[12]
- procurement and payment profiling
- supplier analysis
- searching for undisclosed relationships between employees and suppliers
- matching of apprentice information.

Our capacity to undertake all desired test procedures was affected by availability, completeness and reliability of data obtained from the CTF and external sources. Further, our audit period for payroll was limited to the period from August 2019 to 30 June 2021 as we were unable to obtain any prior payroll data from the legacy payroll system. In order to avoid compromising the systems and information at the CTF, we have not identified specific systems or individuals[13] in this report. We provided the CTF the details of our test procedures to address vulnerabilities identified.

This was an independent forensic audit, conducted under section 18 of the *Auditor General Act 2006*. The approximate cost of undertaking the audit and reporting was $403,000.

[11] We examined payment data only and not the grant or subsidy approval process.

[12] Benford's Law is a statistical measure extensively used in detecting potential fraudulent transactions.

[13] Any individual where a reasonable suspicion of misconduct arises is reported pursuant to the *Corruption, Crime and Misconduct Act 2003*.

This page is intentionally left blank

Auditor General's 2021-22 reports

Number	Title	Date tabled
18	Opinion on Ministerial Notification – FPC Sawmill Volumes	20 June 2022
17	2022 Transparency Report: Major Projects	17 June 2022
16	Staff Rostering in Corrective Services	18 May 2022
15	COVID-19 Contact Tracing System – Application Audit	18 May 2022
14	Audit Results Report – Annual 2020-21 Financial Audits of State Government Entities Part 2: COVID-19 Impact	9 May 2022
13	Information Systems Audit Report 2022 – State Government Entities	31 March 2022
12	Viable Cycling in the Perth Area	9 December 2021
11	Forensic Audit Report – Establishment Phase	8 December 2021
10	Audit Results Report – Annual 2020-21 Financial Audits of State Government Entities	24 November 2021
9	Cyber Security in Local Government	24 November 2021
8	WA's COVID-19 Vaccine Roll-out	18 November 2021
7	Water Corporation: Management of Water Pipes – Follow-Up	17 November 2021
6	Roll-out of State COVID-19 Stimulus Initiatives: July 2020 – March 2021	20 October 2021
5	Local Government COVID-19 Financial Hardship Support	15 October 2021
4	Public Building Maintenance	24 August 2021
3	Staff Exit Controls	5 August 2021
2	SafeWA – Application Audit	2 August 2021
1	Opinion on Ministerial Notification – FPC Arbitration Outcome	29 July 2021

Office of the Auditor General
Serving the Public Interest

Office of the Auditor General
Western Australia

7th Floor Albert Facey House
469 Wellington Street, Perth

Perth BC, PO Box 8489
PERTH WA 6849

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

@OAG_WA

Office of the Auditor General for
Western Australia

(Appendix AAR: 8.1D)

Western Australian
Auditor General's Report

Fraud Risk Management – Better Practice Guide

Report 20: 2021-22

22 June 2022

Office of the Auditor General
Western Australia

Report team:
Carl Huxtable
Chiara Galbraith

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

Fraud Risk Management – Better Practice Guide

Report 20: 2021-22
June 2022

This page is intentionally left blank

THE PRESIDENT
LEGISLATIVE COUNCIL

THE SPEAKER
LEGISLATIVE ASSEMBLY

FRAUD RISK MANAGEMENT – BETTER PRACTICE GUIDE

This report has been prepared for submission to Parliament under the provisions of section 23(2) and 24(1) of the *Auditor General Act 2006*.

Better practice checklists regularly feature in my Office's performance audit reports as a means of providing guidance to help the Western Australian public sector perform efficiently and effectively. This is the third comprehensive stand-alone better practice guide we have produced.

CAROLINE SPENCER
AUDITOR GENERAL
22 June 2022

Contents

Auditor General's overview

Fraud and corruption are ever present and growing threats to businesses, including the Western Australian public sector. As well as loss of funds, fraud and corruption can result in loss of confidence in government institutions. The community needs to have faith that the public sector is serving them well for democracy to work.

The social contract between taxpayer and Government is threatened when public money is misappropriated or other wrongdoing occurs. It strikes at the core of trust, accountability and transparency in Government.

Good governance is important to protect our power, water, justice and transport infrastructure, as well as our health, education and regulatory systems from ineffectiveness, inefficiency and of course failure to deliver what people need when they need it.

It is therefore critical that all levels of the Western Australian (WA) public sector commit to good governance to safeguard public assets from fraudulent or corrupt activity. To do this, every WA public sector entity must understand, in detail, the risks that occur generally within the public sector environment and the specific risks relevant to the activities they undertake.

A common motivator for most people who join the public sector is a desire to do a good job. To assist with this we develop and share guidance on better practice. The purpose of this Better Practice guide is to raise the standard of fraud and corruption control across the WA public sector. Parts 1 and 2 of this guide are aimed at decision makers, highlighting the importance of a fraud and corruption risk management program and the current state of fraud control in the WA public sector. Part 3 is aimed at guiding those responsible for developing and implementing an entity's fraud risk management program.

The guide follows the establishment of our Forensic Audit team as set out in my report of December 2021, its purpose being to uplift fraud resilience within the WA public sector. As has always been the case, public sector entities are responsible for the prevention and detection of fraud and corruption. This guide is intended to empower entities to do more to discharge their governance responsibilities by better controlling their risks of fraud and corruption.

We encourage entities to use this guide along with the tools and other available resources to manage the risk of fraud against their entity. While fraud risks cannot be eliminated, a robust and well-resourced fraud risk management program can minimise the likelihood and consequences of fraud events.

We thank the Commonwealth Fraud Prevention Centre for their generous support in helping develop this guide as well as McGrathNicol Advisory for their guidance. We also extend our appreciation to the State entities that provided valuable feedback on the draft guide.

Part 1: Introduction

1.1 About this guide

This Better Practice Guide aims to help Western Australian (WA) public sector entities to manage their fraud and corruption risks. It outlines why fraud and corruption risk management is important (Part 2) and provides practical guidance on the process of developing a fraud and corruption risk management program (Part 3).

The guide refers to a range of tools which are included in the appendices and available on our website (www.audit.wa.gov.au). The online tools will be updated as required.

1.2 Who should use this guide

This guide is intended for use by WA public sector entities (entities) and may be applicable to other organisations.

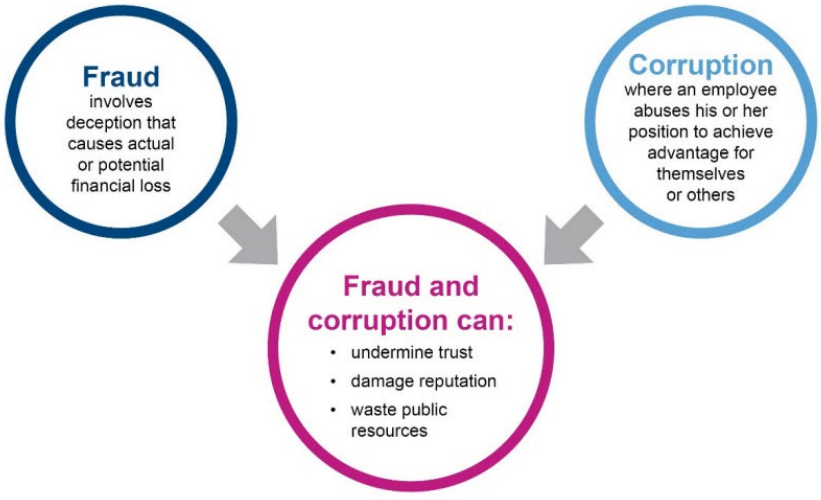
Parts 1 and 2 are intended for directors general, chief executive officers, managers and other key decision makers. Part 1 outlines the high-level principles entities should apply to fraud and corruption risk management and Part 2 highlights the importance of entities implementing an effective fraud and corruption risk management program.

Part 3 is for those tasked with fraud risk management within an entity. It aims to step them through the process of developing, executing and monitoring an entity's fraud and corruption risk management program.

Ultimately, preventing and detecting fraud and corruption is the responsibility of every person in the WA public sector, and as such, this guide may be relevant for all public sector employees.

1.3 What is fraud and corruption

Fraud and corruption involve a benefit being obtained through dishonesty and/or an abuse of position to the detriment of another person or entity (Figure 1). They can pose a risk to an entity's finances, reputation, and service delivery. More seriously, they go to the heart of trust and confidence in Government. In this guide, we use the term fraud to include corruption.



Source: OAG using information from the Victorian Auditor General's Office – *Fraud and Corruption Control* report, March 2018

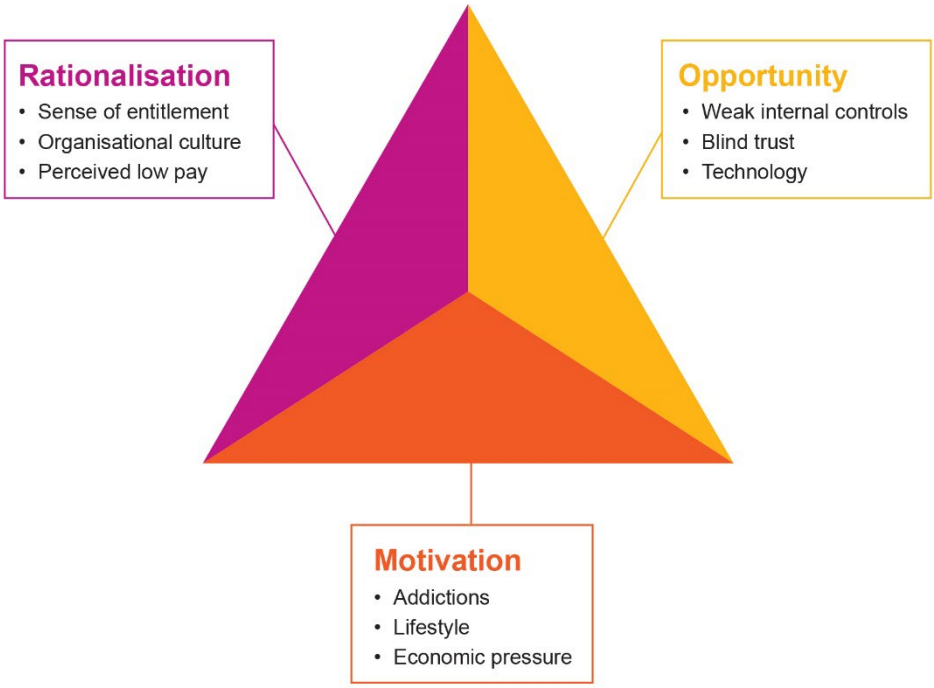
Figure 1: Definitions of fraud and corruption

Not all fraud can be prevented – every organisation, public or private, is vulnerable. A robust and rigorous fraud control system, with appropriate prevention and detection processes, can reduce the risk of fraud occurring and minimise losses.

To effectively fight fraud an entity must first acknowledge that fraud occurs and then seek to understand how and why it occurs. The fraud triangle (Figure 2) outlines 3 key elements that are generally present when fraud has occurred in an entity:

- **Opportunity** – a vulnerability within systems or processes is identified and exploited.
- **Motivation** – also referred to as pressure, is the reason someone commits fraud.
- **Rationalisation** – how someone justifies their fraudulent behaviour to themselves.

With the right mix of motivation, opportunity and rationalisation even the most trusted employee can be tempted to commit a fraudulent act.



Source: OAG adapted from Other People's Money[1]

Figure 2: The fraud triangle

A fraudster's personal motivation and the ability to rationalise their behaviour is largely beyond an entity's control although, entities will benefit from being alert to and aware of behavioural red flags in respect of their staff and suppliers. The most effective way for an entity to manage its risk of fraud is by controlling the opportunity – implementing or enhancing controls aimed at preventing fraud or detecting it quickly if it does occur.

1.4 Fraud control principles

To build a robust and effective fraud risk management program requires 10 essential principles. Each of the following principles link to 1 or more stages of a better practice fraud risk management program as set out in this guide.

[1] *Other People's Money: A Study in the Social Psychology of Embezzlement*, Dr Donald Cressey, Free Press 1953.

Strong leadership	An entity's leadership must model a commitment to fraud control, establishing a strong 'tone at the top' culture to demonstrate their personal commitment to operating with integrity and encouraging a 'finding fraud is good' mindset.
Recognise fraud as a business risk	Entities must acknowledge they are vulnerable to fraud. Fraud should be viewed and treated in the same way as an entity's other enterprise risks.
Adequate control resourcing	Entities should invest in appropriate levels of fraud control resourcing including specialist information system security management personnel.
Clear accountability for fraud control	Entities should establish clear personal accountabilities for fraud control at the governance, executive management and management levels.
Implement and maintain an effective fraud control system	An effective fraud control system (FCS) can reduce the opportunity for fraud. It needs to align with better practice guidance, be fully implemented, monitored and updated periodically.
Periodic assessment of fraud risks	Fraud risk assessments should be carried out periodically or whenever a significant change that affects the entity occurs.
Effective awareness raising program across the entity	To ensure employees recognise red flags for fraud, entities should establish an effective awareness program.
Open channels to report suspicions of fraud	To encourage whistle-blowers to come forward entities should support: • active reporting of fraud through accessible anonymised reporting channels • ensure that the entire workforce is aware of organisational expectations for reporting detected or suspected cases of fraud • ensure they have robust whistle-blower protection policies and procedure that includes assurance that victimisation of those who, in good faith, make such reports will not be tolerated.
Implement a fraud detection program	An effective fraud detection program that includes detection measures such as data analytics and post-transactional review are important.
Consistent response to fraud incidents	Rapid and robust response to suspected fraud events with effective investigation procedures will drive decisive action and result in better outcomes for detected fraud incidents. A strong and consistent response to all fraud events will send a strong message to the workforce that the entity will not tolerate fraud, no matter how minor.

Source: OAG

Table 1: Foundation principles for fraud control

1.5 Acknowledgements

We would like to express our appreciation to the entities and their employees who contributed to the development of this guide.

We also acknowledge and express our appreciation to the Commonwealth Fraud Prevention Centre (CFPC) and Standards Australia, who willingly shared their original intellectual property in the development of this guide, and McGrathNicol Advisory, who were engaged to provide technical expertise.

Part 2: Why develop a fraud risk management program

2.1 Overview

In this part of the guide, we outline why entities should develop a fit for purpose fraud risk management program. In summary:

- there are WA government requirements to implement integrity measures to protect the financial and reputational position of entities
- the financial, reputational and human impact on an entity and its employees when fraud occurs can be significant
- entities' fraud control maturity is not meeting best practice.

Fraud risk management has a critical role in preventing and promptly detecting fraud to minimise loss, retain trust in entities and protect employees.

2.2 Public sector requirements

Entities are required to consider their risks and implement protections.

Treasurer's Instruction (TI) 825 requires all WA State government entities to develop and implement a risk management program. The TIs state, where possible, entities' policies and procedures should be consistent with Australian Standards including:

- AS ISO 31000:2018 – *Risk management - Guidelines* (risk standard)
- AS 8001:2021 – *Fraud and corruption control* (fraud control standard).

Similarly, Regulation 17 of the Local Government (Audit) Regulations 1996 requires local government CEOs to review their entity's systems and procedures, including for risk management, to ensure they are effective and appropriate for the entity's needs.

In addition to these requirements, the Public Sector Commission encourages all entities to commit to implementing its *Integrity Strategy for WA Public Authorities 2020-2023.* This strategy includes the *Integrity Snapshot Tool* which enables entities to self-assess their current integrity position and help identify areas for improvement.

This guide is intended to aid all entities in the application of the above Australian Standards and is not a replication of them. Entities should obtain a copy of the above from Standards Australia or from an authorised distributor to ensure a full and proper understanding of the content and their compliance with them.[2]

2.3 Impact of fraud in the WA public sector

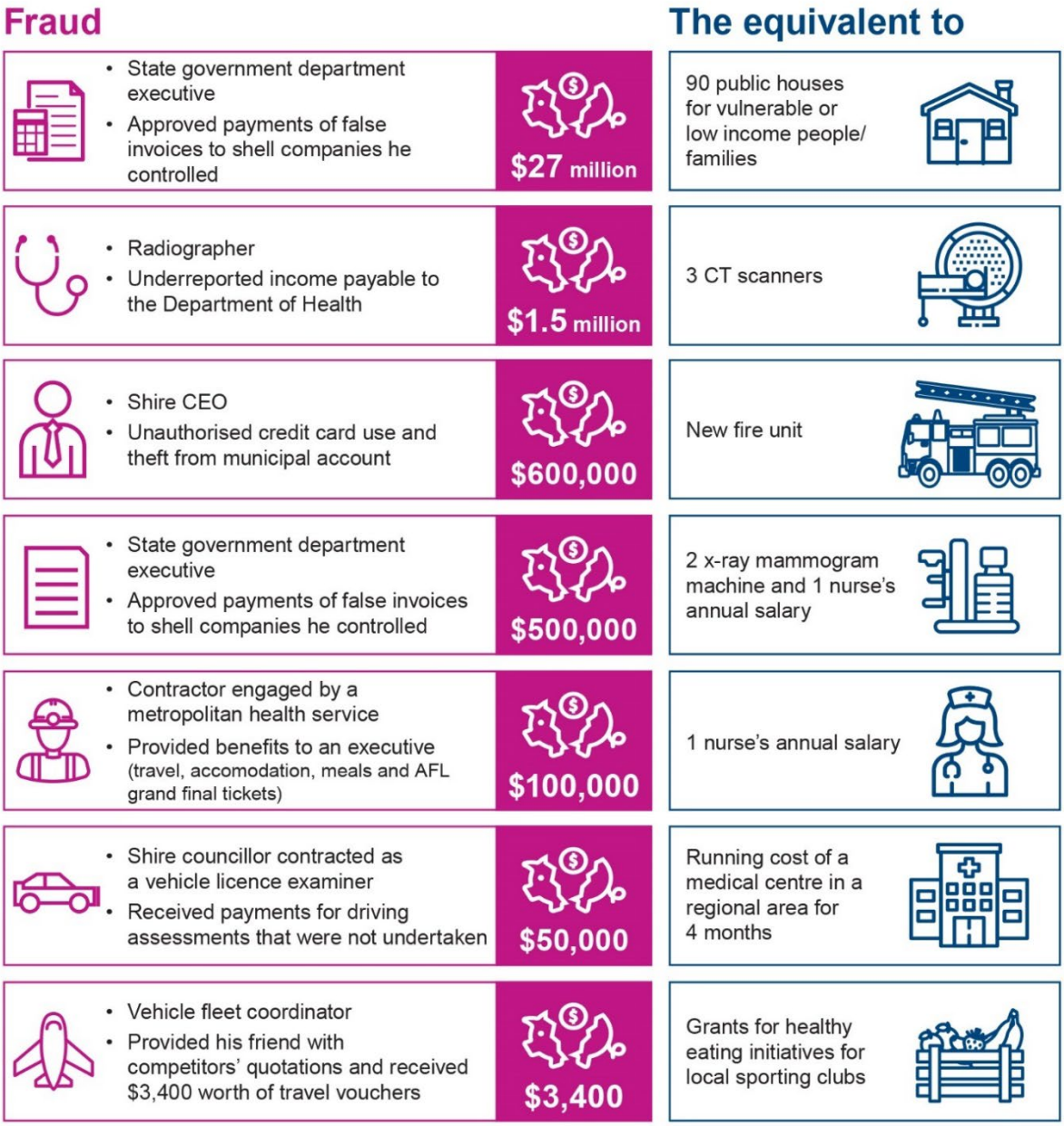
The Association of Certified Fraud Examiners Report to the Nations 2022, estimated that fraud losses in businesses, government and not-for-profits are approximately 5% of their

[2] Reproduced by Office of the Auditor General (WA) with the permission of Standards Australia Limited under licence CLF0622OAGWA.

annual turnover.[3] If this estimate is an accurate reflection of actual fraud losses within the WA public sector, the impact on the people of WA, and the services to them, is considerable.

Fraud within the WA public sector is typical of instances in other jurisdictions and sectors where investigations regularly find deficiencies within entities' controls. These deficiencies may have been identified earlier if the entities had a robust and rigorous fraud risk management program in place.

The following is a short summary of some detected fraud events within the WA public sector in the last 15 years and the practical impact on service delivery. These incidents demonstrate that the WA public sector remains vulnerable to fraud by members of its own workforce as well as external fraudsters.



Source: OAG

Figure 3: Examples of known fraud in the WA public sector

[3] Association of Certified Fraud Examiners, *Occupational Fraud 2022: A Report to the Nations.*

The impact of fraud goes beyond financial and service delivery losses and includes:

- **Human impact**: Those who rely on government services (such as the elderly, the vulnerable, the sick and the disadvantaged) are often the ones most harmed by fraud, increasing the disadvantage, vulnerability and inequality they suffer.
- **Reputational impact**: When it is handled poorly, fraud can result in an erosion of trust in government and industries, and lead to a loss of international and economic reputation. This is particularly true when fraud is facilitated by corruption.
- **Industry impact**: Fraud can result in distorted markets where fraudsters obtain a competitive advantage and drive out legitimate businesses, affecting services delivered by businesses and exposing other sectors to further instances of fraud.
- **Environmental impact**: Fraud can lead to immediate and long-term environmental damage through pollution and damaged ecosystems and biodiversity. It can also result in significant clean-up costs.[4]
- **Organisational impact**: The impact of fraud on employees can be significant. It can lead to low morale, mistrust, inefficient additional oversight and ultimately staff leaving due to the entity's damaged reputation. It can also result in reduced efficiency and effectiveness of the entity's activities.

2.4 Status of fraud control maturity across the sector

In 2021, we conducted a high-level review of State government entities' fraud risk management. As reported in our *Forensics Audit Report – Establishment Phase*, we found many entities fell well short of better practice. We reported similar results in our 2013 report, *Fraud Prevention and Detection in the Public Sector,* and in our 2019 report, *Fraud Prevention in Local Government*. Significant work is required across the public sector to raise the standard of fraud risk management to a satisfactory level.

As part of our 2021 review we asked: "Has the entity completed an assessment of its fraud and corruption risks?" Set out at Table 2 is an analysis of the findings of that review.

Responses			
Assessment completed	**Assessment in progress**	**Assessment not completed**	**Total**
71	12	11	92

Source: OAG

Table 2: Number of entities who have completed an assessment of their fraud and corruption risks

We selected a sample of 12 entities for more detailed analysis. This further analysis highlighted several key themes as set out in Table 3 below:

Theme	Summary	Why it matters
Lack of a risk framework	Some entities did not have an overall risk framework that could be applied in the context of fraud risk.	An overall risk framework ensures consistency in approach to all the entity's identified risks.

[4] Commonwealth Fraud Prevention Centre, *The total impacts of fraud* (accessed 17 May 2022).

Theme	Summary	Why it matters
Entity size not an indicator of quality	Several larger entities provided insufficient details to show they had undertaken a fraud risk assessment. This suggests that inadequate resourcing is not the sole cause of poor fraud risk assessments being conducted.	The public sector collectively provides a diverse range of services and entities should apply a fit for purpose approach to their fraud risk assessment.
Lack of collaboration	Our analysis suggested a lack of collaboration with risk and process owners in the identification and analysis of the entity's fraud risks.	Collaboration is important because different employees bring different perspectives and experience.
No fraud risk register	Many entities did not have a fraud risk register, despite this being a requirement of their fraud control program.	Entities cannot efficiently monitor and review fraud risks if they have not been documented. The appropriate way to document an entity's fraud risks is in a fraud risk register.
Failure to assess fraud risk	It was clear from our analysis that a significant proportion of entities had not assessed their fraud risks. In many cases entities mistook a fraud control framework for a fraud risk assessment.	Entities must ensure they have a sound understanding of fraud risks that could impact their organisation – this can only be done by implementing a comprehensive process to identify, analyse and evaluate specific fraud risks that could impact the entity.
Data analytics not targeted	Entities had not identified and assessed relevant fraud risks prior to undertaking data analytics to identify fraudulent transactions.	Data analytics is a useful tool for the prevention and detection of fraud, but it requires discipline for it to be efficient and effective. Entities risk implementing inefficient and costly data analytics that are not effective for fraud risks specific to their entity.
Excessive generalisation	Fraud risks that were identified were excessively general rather than being linked to specific processes.	Entities must properly identify and define their vulnerabilities to enable implementation of effective controls.
Risk register limited to strategic risks	Fraud had been identified as an overall strategic risk; however, we saw little evidence that specific fraud risks were identified for individual business units or that a comprehensive fraud risk assessment had been undertaken across all parts of the organisation.	

Source: OAG

Table 3: Themes identified from survey of entities' fraud control maturity

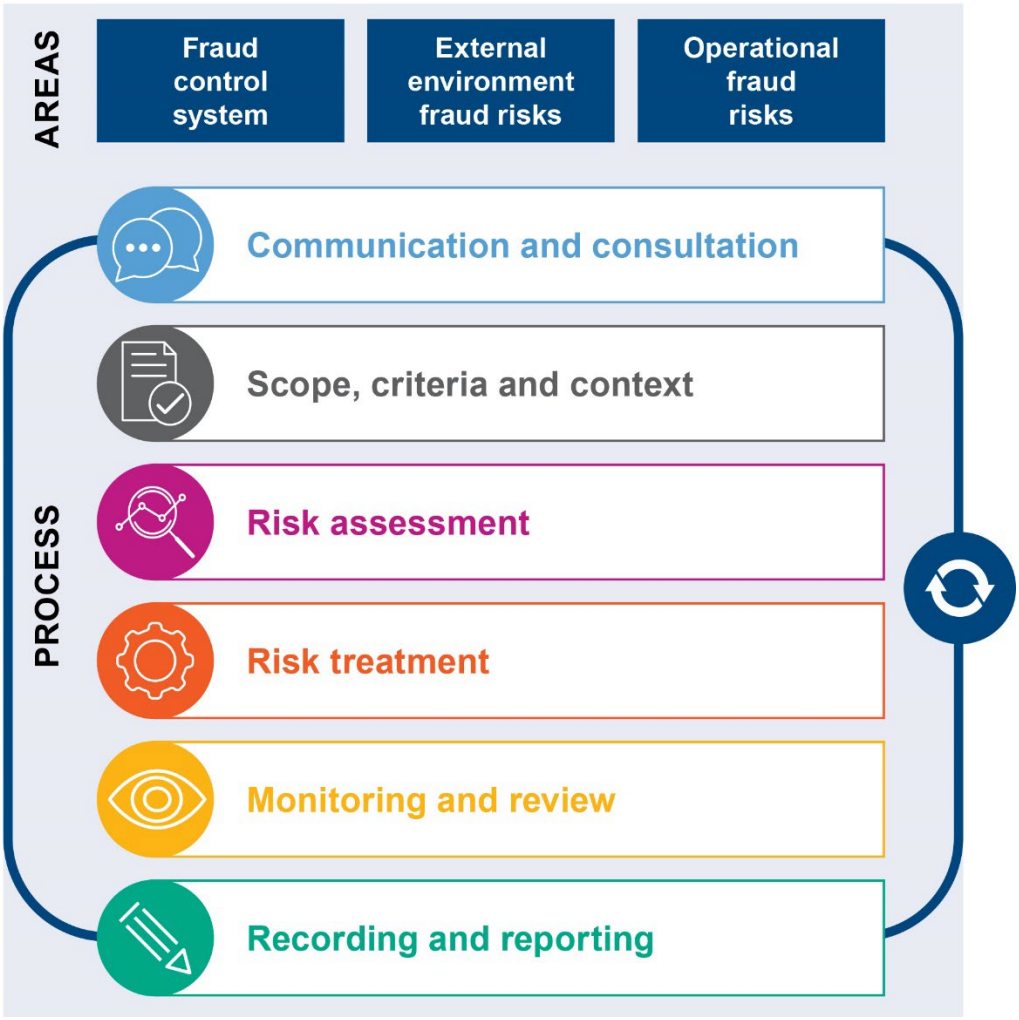
Part 3: How to develop a fraud risk management program

3.1 Overview

To effectively manage fraud risks, entities should develop and implement a robust and effective fraud risk management program. The program should be tailored to an entity's objectives, environment and risk profile and cover:

- the 3 areas where fraud vulnerabilities can be found (based on AS 8001:2021 – *Fraud and corruption control*) – section 3.2
- the 6-stage process to manage risks (based on AS ISO 31000:2018 *Risk management – Guidelines)* – section 3.3.

The diagram below is a simple illustration of the fraud risk management program.



Source: OAG based on AS 8001:2021 and AS ISO 31000:2018

Figure 4: Risk management process including 3 areas of fraud risks to consider

3.2 Where to look for fraud vulnerabilities

In accordance with AS 8001:2021, effective management of fraud risk requires a comprehensive examination of an entity's overall fraud control system (FCS), external threats and operational (or internal) activities.

Our survey of State government entities found that most entities who had taken steps to manage their risk of fraud only considered 1 of the 3 vulnerability areas and none provided evidence that they had considered all 3.

The following is a brief overview of the 3 areas of fraud vulnerability. Whilst we have focused the fraud risk management process that follows at 3.3 on operational risks, it can be applied to the other 2 areas of fraud vulnerability.

A fraud control system is the tools and techniques used to mitigate an entity's fraud risks. When considering fraud risks, analysing the existing control environment is important to assess how closely it aligns to better practice.

AS 8001:2021 – *Fraud and corruption Control* Clause 2.10 identifies 4 elements for an FCS: foundation, prevention, detection and response, examples of these are included in the table below:

FCS elements	Overview
Foundation	Adequate resourcing to implement a multi-faceted approach to managing fraud risks. Examples include specialist resourcing, awareness training, risk management, information security management systems.
Prevention	Prevention controls are the most common and cost-effective way to mitigate fraud. Examples include an integrity framework, internal controls, workforce screening, physical security.
Detection	Detection controls can help to identify when fraud has occurred but are not as cost-effective as preventative measures. Examples include post-transactional review, data analytics, whistle-blower management.
Response	Response controls can assist the entity to respond to a fraud incident after it has occurred and are the least cost-effective, however can significantly reduce the impact of present and future frauds. Examples include investigation, disciplinary procedures, crisis management, recovery.

Source: OAG based on AS 8001:2021 – *Fraud and corruption control* Clause 2.10

Table 4: Elements of a fraud control system

Entities may not have formally documented their FCS, but it is likely they have several existing controls.

Designing and implementing a robust fraud risk management program will inevitably strengthen an entity's FCS. It is for this reason it is recommended an entity assess their FCS against better practice prior to undertaking the fraud risk management process.

The fraud control standard (Clause 2.10) sets out an approach to developing and implementing an entity's FCS and a structure for documenting it. Appendix 3 is a tool for entities to benchmark their current FCS maturity against the fraud control standard.

Updating the fraud control system documents throughout the fraud risk management process assists entities to monitor their increased maturity.

External threats come from outside an entity and are largely beyond their control. The fraud control standard recommends entities consider the 6 external factors that can impact an organisation, known as the PESTLE model. The model is explained in the table below and a complete tool is provided in Appendix 4:

PESTLE factor	**Overview**
Political	To identify the political situation of the country, State or local government area in which the entity operates, including the stability and leadership of the government, whether there is a budget deficit or surplus, lobbying interests and local, regional, national or international political pressure.
Economic	To determine the economic factors that could have an impact on the entity including interest rates, inflation, unemployment rates, foreign exchange rates and monetary or fiscal policies.
Social	To identify the expectations of society by analysing factors such as consumer demographics, significant world events, integrity issues, cultural, ethnic and religious factors, and consumer opinions.
Technological	To identify how technology, including technological advancements, social media platforms and the role of the internet more broadly, is affecting or could affect the entity.
Legal	To identify how specific legislation, including industry specific regulations, and case law are affecting or could affect the entity's future operations.
Environmental	To identify how national and international environmental issues are affecting or could affect the entity.

Source: OAG based on AS 8001:2021 – *Fraud and corruption control,* Clause 2.9

Table 5: External factors that can impact an entity

Operational fraud risks are the fraud risks associated with an entity's day-to-day operations. There will be risks that are common to all entities (e.g. procurement, payroll, asset management) and those that are entity specific (e.g. property development, grant administration, major projects). Operational risks will also include changes in function or activity (e.g. new government initiative, creation of a relief fund in response to a natural disaster). The following section, Fraud risk management process, is focused on managing your operational fraud risks and discusses this in more detail. We also provide further tools in the appendix to assist with better managing them.

3.3 Fraud risk management process

In this section we have mapped out the 6 stages in the risk management process as summarised in Figure 4 above. It is not a linear process; each stage will connect to others at different times throughout the risk management cycle.

We describe the stages and introduce several tools which can be used to assist in developing an effective fraud risk management program. The complete tools are included in the appendices and are available on our website. These tools are not an exhaustive list, there are many tools available (free and for a fee) and entities should determine which ones best suit their needs.

Communication and consultation

To effectively identify fraud risks within an entity's processes and systems, it is essential that the people who best know and run or control the business processes and business area are adequately engaged throughout the fraud risk management process. Entities should also consider if subject matter experts need to be engaged, such as information system security specialists.

Communication and consultation are intended:

"…to assist stakeholders in understanding risk, the basis on which decisions are made and the reasons why particular actions are required."[5]

Employees can feel challenged when asked to respond to questions or contribute to discussions about fraud risks – they may feel that considering this issue with them or in their presence is, in effect, calling their integrity into question. Those tasked with the fraud risk management program should keep the people they need engaged and at ease throughout the process to ensure the best outcome.

Communication and consultation	Better practice
Promote awareness and understanding of fraud risks	• Implement multimodal training programs specific to fraud risks – "What is a fraud risk" • Effectively communicate to employees that the objective is to protect the integrity of the entity and employees
Bring different expertise together throughout the process using effective mechanisms	• Engage different levels of expertise and experience to bring various perspectives • Use a variety of communication methods such as emails, workshops, one-on-one interviews and surveys to obtain a wide range of feedback and opinions
Build a sense of inclusiveness and ownership for process owners (e.g. one-on-one interviews, focus groups)	• Use fraud risk workshops to obtain "buy in" from process operators and owners • Invite all relevant employees, regardless of seniority, to attend a workshop
Obtain sufficient knowledge from relevant stakeholders of business processes to facilitate fraud oversight and decision making	• Facilitate fraud risk workshops to discuss and map business processes and internal controls • Ask attendees to consider "what could go wrong?" in processes they engage with or manage • Identify areas of fraud risk in a process map that requires internal controls
Engage with relevant stakeholders to obtain feedback and information to support decision-making	• Structure emails and/or surveys that focus on fraud risks for specific processes • Adopt appropriate modes of communication

Source: OAG

Table 6: Better practice examples of the communication and consultation stage

[5] AS ISO 31000:2018 *Risk management - Guidelines* Clause 6.2.

One way to enhance communication is by meeting one-on-one to facilitate a better understanding of relevant risk and control issues.

To help with communication and consultation, entities should prepare a communication plan that outlines the intended methods, people and timelines for consultation. This also forms the basis of reporting to any oversight committees on the progress of projects in the fraud risk management program. Examples of methods of communication and consultation are provided in Appendix 5.1.

Scope, context, and criteria

Establishing the scope, context and criteria for the fraud risk assessment is done using the communication and consultation processes outlined above. They will differ for each entity and will be determined by the size and complexity of the process being assessed.

"…Scope, context and criteria involve defining the scope of the process and understanding the external and internal context."[6]

Case study 1: Example of scope, context and criteria for a risk assessment of selected parts of the Procure to Pay process

Factor	Procure to Pay

Scope	• The specific parts of the Procure to Pay process to be assessed are: supplier selection, onboarding vendors, purchase validation (business case, receipt of goods/services) and release of payment.
	• We will engage with the finance business unit and operational staff responsible for purchase orders and validation of receipt of goods/service.
	• The entity's risk assessment policy dated 31 January 2020 will be applied in conjunction with the approved fraud risk assessment program dated 30 June 2021.
	• As the entity's procurement staff are across the State, we will need to engage in a number of online meetings with potential site visits.
	• Timeline:
	  ○ engagement with procurement staff by 30 June 2022
	  ○ identification of risks by 31 October 2022
	  ○ completion of risk register and mapping of risks by 31 December 2022
	  ○ first review to Internal Audit and Risk Committee (IARC) by 28 February 2023
	  ○ second review to IARC by 30 April 2023
	  ○ submission to Board for approval by 31 May 2023.

[6] AS ISO 31000:2018 *Risk management - Guidelines* Clause 6.3.

Context	Internal factors include: • the strategic objectives of the entity are: community focused delivery of services, sound business practices and quality services. A list of the specific goods, services or works to be procured are provided in Annexure A • the existing employee level in the Procure to Pay process is sufficient, however, their experience is inadequate. No training has been delivered in identifying indicators of potential fraud • there is no assessment of fraud controls within vendors • the entity has policies and processes in respect of independence for supplier selection panels and purchase validation. External factors include: • increasing fraud trends targeting procurement and finance teams (i.e. business email compromise ‑ fake emails impersonating an internal senior person or a vendor) • recent known scams in the public domain that have been uncovered.
Criteria	• The below risk criteria are taken from the entity's risk assessment policy dated 31 January 2020. • The entity rates likelihood risk on a scale from extremely unlikely to almost certain. Within the Procure to Pay process, rare is conceivable but unlikely, unlikely is conceivable and has occurred in the past but unlikely in the next year. • The entity rates consequence risk on a scale from negligible to catastrophic across the following loss factors: financial, reputational, legal, service delivery. • Within the Procure to Pay process, negligible has no negative consequence, low disrupts internal non-management process and has no external financial loss, moderate requires corrective action by senior management, potential disciplinary action and minor financial impact etc.

Entities will need to develop a scope, context and criteria for all activities and processes they perform. The CFPC's *Fraud Risk Assessment Leading Practice Guide* provides a strategic profiling tool in support of its recommendation that entities responsible for multiple activities and processes prioritise the areas of the entity that are at higher risk for fraud.

Scope, context and criteria	Better practice
Define the scope of the activity being assessed for fraud risk including objectives and decisions to be made prior to commencing any fraud risk assessment	• Clearly document the scope and objective of the process that is being assessed for fraud risks • Circulate a document that sets out the scope to all employee participating in the fraud risk assessment • Break down complex processes into manageable scopes

Scope, context and criteria	Better practice
Establish the context of the fraud risk activity	• Understand the external environment • Understand the internal operating environment • Reflect the specific environment of the activity to which the fraud risk management process is to be applied
Align the fraud criteria with an overarching risk management framework used to assess all business risks for consistency	• Review the entity's existing risk management framework prior to commencing to ensure up-to-date and fit-for-purpose • Align consequence and likelihood criteria and the risk rating matrix with existing framework
The fraud risk assessment criteria should reflect the organisation's values, objectives and resources and be consistent with policies and statements about risk management	• Review the entity's existing risk management policy to understand the entity's risk appetite

Source: OAG

Table 7: Better practice examples of the scope, context and criteria stage

Appendix 5.2 provides a guide on how you could outline your scope, context and criteria.

Risk assessment

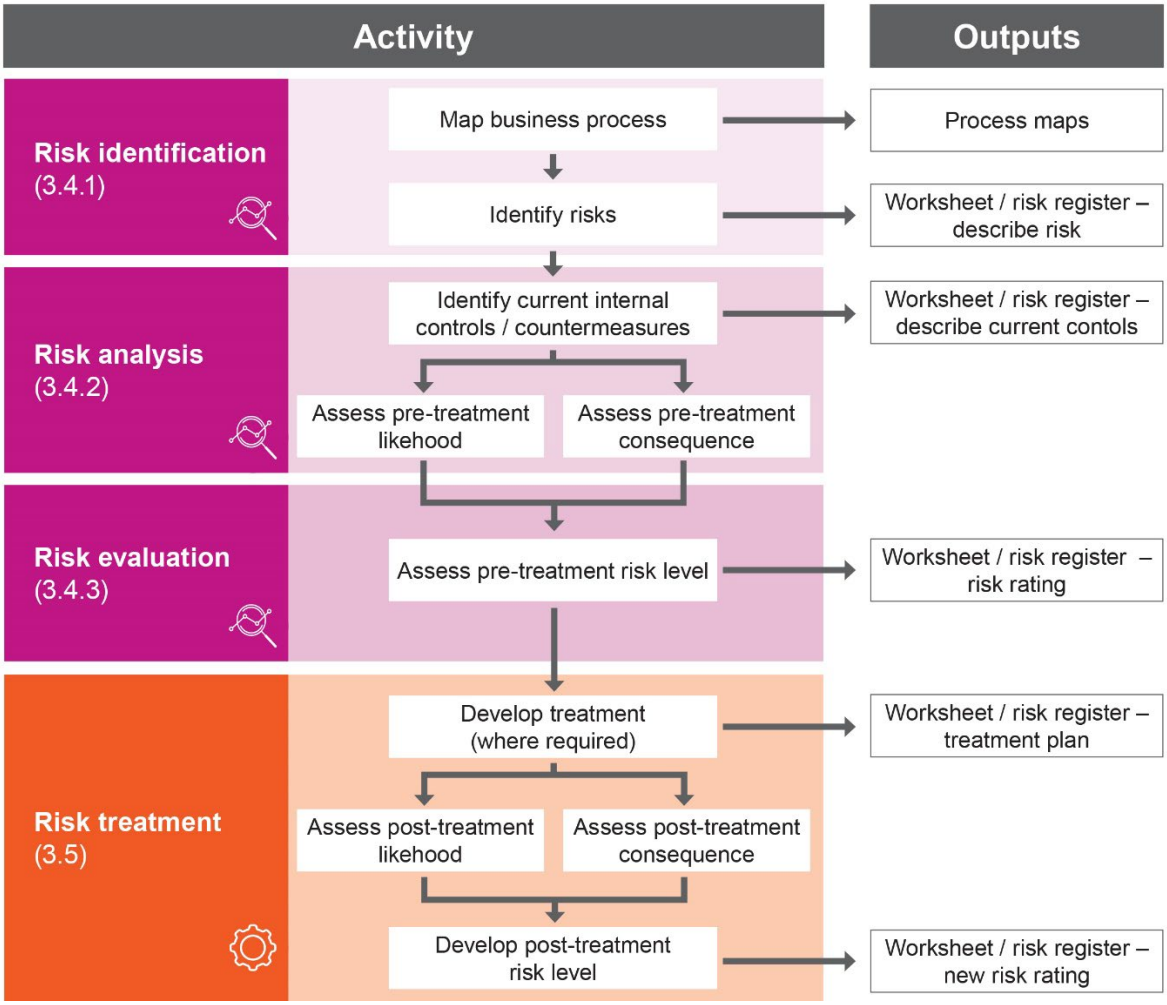
Once the scope, context and criteria are established, entities need to assess their fraud risks.

If an entity has a detailed risk assessment approach, then it is logical and likely more efficient to apply that for fraud risks as well.

AS ISO 31000:2018 *Risk Management - Guidelines* sets out 3 sub-phases in the risk assessment stage:

- risk identification
- risk analysis
- risk evaluation.

The assessment stage is followed by treatment. An overview of the risk assessment and treatment stages is set out below.



Source: OAG based on AS ISO 31000:2018 *Risk Management - Guidelines* Clause 6.4 and 6.5

Figure 5: Risk assessment and treatment stages overview

Identifying risks

Think like a fraudster. Discover what you don't know.

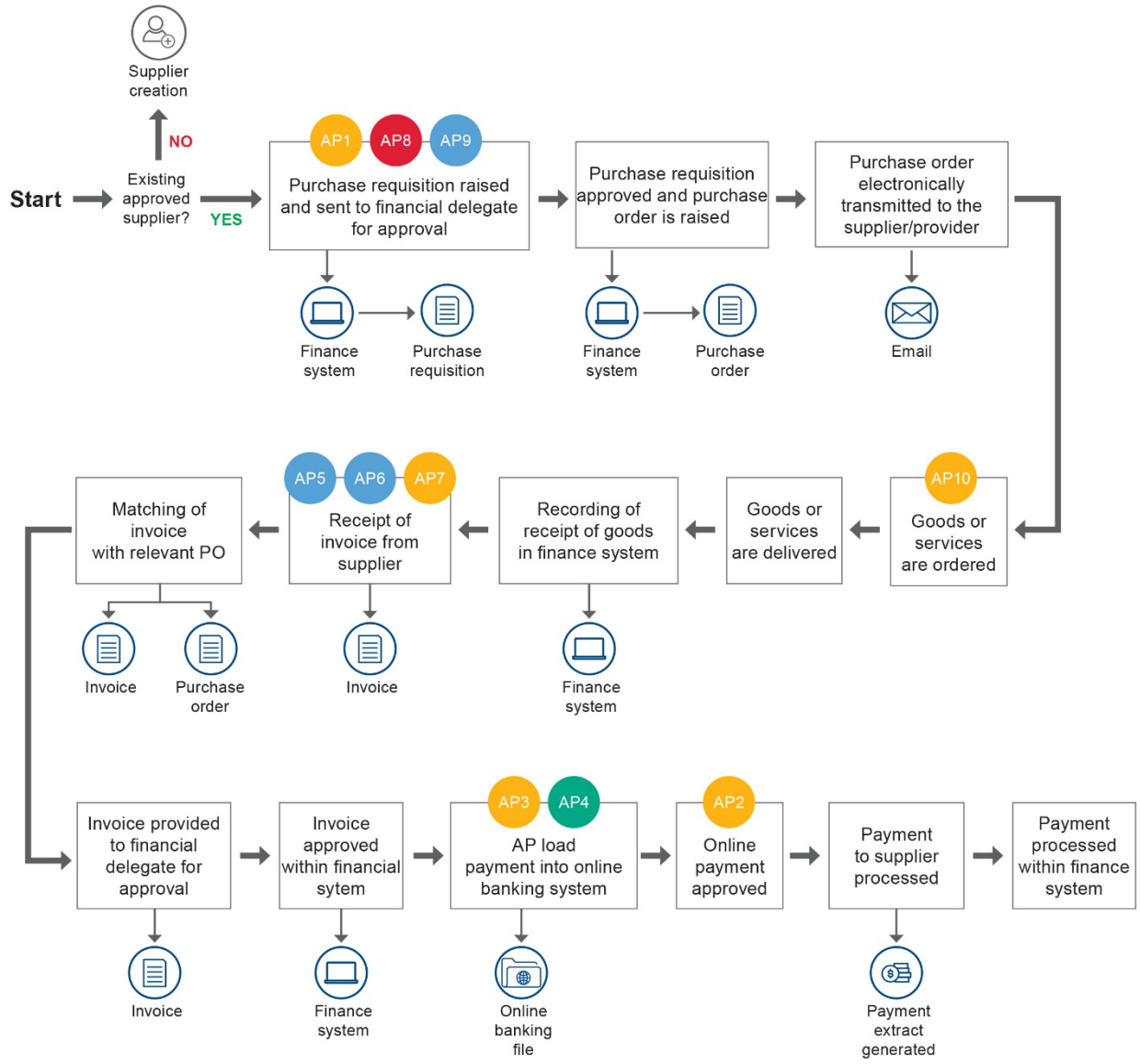
Risk identification involves:

"… finding, recognising and describing risks that might help or prevent an organisation achieve its objectives."[7]

It is important to avoid the temptation to be defensive and dismiss risks before they have been properly analysed and evaluated.

Identifying fraud risks should be viewed as a creative process. Brainstorm the various fraud schemes that have and could be committed within or against the entity. An effective way to identify fraud risks is to map the process that is being assessed and identify vulnerabilities within the process. Below is an example of an accounts payable process map, sometimes referred to as a flow chart. The coloured circles represent identified fraud risks in the accounts payable (AP) process.

[7] AS ISO 31000:2018 *Risk management - Guidelines* Clause 6.4.2.



Source: OAG

Figure 6: Accounts payable process map

A fraud risk assessment should consider common methods used by fraudsters and look for vulnerabilities within the entity's processes and activities. This will involve challenging assumptions about, and existing processes within, an entity to identify gaps and thinking of creative ways to circumvent internal controls.

Common frauds are a good place to start but entities should not stop there. Risk identification needs to be realistic but at the same time entities should remember that even the most far-fetched fraud scheme can occur when the right balance of motivation, rationalisation and opportunity are present. Asking hypothetical questions about how fraud could be perpetrated in a structured and controlled way will put the fraud risk assessment process on the right path.

Finally, a good fraud description will allow you to understand ways to prevent or detect the fraud. One way to identify and describe your fraud risks is to consider who did what and what the result was, also described below as the Actor, Action, Outcome method[8]:

[8] Commonwealth Fraud Prevention Centre, *Fraud Risk Assessment – Leading Practice Guide.*

- actor – accounts payable (AP) officer
- action – submits and processes fictitious invoice
- outcome – payment of invoice results in money going to AP officer's bank account.

Fraud risks that have been identified should be adequately documented on a fraud risk worksheet. Fraud risk worksheets can function as an aid to the risk assessment but also as a fraud risk register and an implementation worksheet.

Appendix 5.3 includes:

- an example of a fraud risk worksheet
- risk assessment and treatment process overview
- key questions you could ask when trying to identify fraud risks
- the CFPC's Actor, Action, Outcome method of describing fraud risks
- an example diagrammatic presentation of assessed fraud risks
- a short summary of fraud risks that are commonly found in the public sector environment. The summary is not intended to be an exhaustive list. The examples in section 2.3 would also be useful in this exercise.

Analysing fraud risks

Once the potential fraud risks within the business unit or process have been identified the next step is to analyse the risks.

Risk analysis is:

"… a detailed consideration of uncertainties, resources, consequences, likelihood, events, scenarios, controls and their effectiveness."[9]

Fraud risk analysis requires input from employees within the business unit(s) being assessed and any additional subject matter experts who can add value to the process.

An analysis of each risk includes considering:

- **the likelihood** of the risk occurring
- **the consequence** for the entity if it did occur
- **resourcing constraints** impacting controls
- **the effectiveness of existing controls** intended to mitigate the risks.

The entity should use its established risk analysis matrix to analyse the likelihood, consequences, and strength of existing controls to assign a risk rating to each fraud risk. It is critical that every business unit within an entity use the same risk analysis matrix to allow for a proper comparison of risks across the entity.

Figure 7 below is an example of a risk assessment matrix that shows the likelihood combined with the consequences risks results:

[9] AS ISO 31000:2018 *Risk management - Guidelines* Clause 6.4.3.

Likelihood	Consequence				
	Negligible	Low	Moderate	Major	Extreme
Almost Certain	Medium	High	Very High	Very High	Very High
Likely	Medium	High	High	Very High	Very High
Possible	Low	Medium	High	High	Very High
Unlikely	Low	Low	Medium	High	High
Rare	Low	Low	Low	Medium	Medium

Source: OAG

Figure 7: Example of a risk assessment matrix

Sometimes an entity undertaking a fraud risk assessment can overestimate the effectiveness of internal controls. One technique to fully assess their effectiveness is to conduct a walk-through of the relevant process or activity and determine if the controls are currently operating effectively. Applying a sceptical approach to the controls and adopting the mindset of a determined fraudster can help to assess if a control can be overridden or avoided. Internal audit resources can also be helpful in this assessment.

Risk analysis	Better practice
Consider uncertainties, risk sources, consequences, likelihood, events, scenarios, controls and their effectiveness	• Detailed documentation of the analysis including reasoning for decisions for example if a risk is determined to be HIGH for consequence document why and what inputs were used
Events can have multiple causes and consequences and affect multiple objectives	• Deep dive analysis to identify all causes, both internally, externally and potential consequences
Scrutiny of existing controls	• Sufficiently analyse and test existing controls including walk-throughs and penetration testing • Consider engaging specialists to identify gaps in existing system controls

Source: OAG

Table 8: Better practice examples of the risk analysis stage

Evaluating fraud risks

Once an entity's fraud risks have been analysed, they need to be evaluated against the entity's risk appetite and tolerance. This should be defined in the entity's risk management policy and framework. The evaluation is used to determine if further action is required to reduce identified residual risks to an acceptable level.

Entities' risk appetites and tolerances vary and depend on factors such as the circumstances of a particular program, the cost-benefit of implementing controls to reduce the risk of fraud, resources or other constraints and reputational risk. Risk tolerance is not static and should be determined on a case-by-case basis for each risk identified.

The purpose of risk evaluation is to:

"… support decisions. Risk evaluation involves comparing the results of the risk analysis with the established risk criteria to determine where additional action is required." [10]

It is important that the evaluation of fraud risks involves detailed input from the process and risk owners and includes senior employees who can consider the cost of countering fraud against the entity's risk tolerance. The evaluation considers the residual fraud risk and should conclude with one of the following outcomes[11]:

- avoid the risk
- accept the risk
- remove the risk source
- change the likelihood
- change the consequences
- share the risk
- retain the risk.

These conclusions, and links to any supporting documentation, should be included in the fraud risk assessment worksheet.

Risk evaluation	Better practice
Evaluate results from risk assessment	• Comparing the results of the risk analysis with the established risk criteria to determine if and where additional action is required
Record and communicate evaluation results	• Risk evaluation outcomes are recorded, communicated and then validated at appropriate levels of the organisation

Source: OAG

Table 9: Better practice examples of the risk evaluation stage

Risk treatment

After finalising the risk assessment, the risk treatment process is undertaken. An entity's evaluation of the risks and its risk appetite will determine if the residual risk is at an acceptable level or if treatment is required. Risk treatments can include enhancing existing controls, implementing new controls, or avoiding the risk altogether by no longer undertaking the activity, program or service.

An entity needs to consider how to mitigate the residual fraud risks that remain above the entity's tolerance level. The objective of treating the fraud risk is to reduce the residual risk identified in the assessment to an acceptable level.

[10] AS ISO 31000:2018 *Risk management - Guidelines* Clause 6.4.4.

[11] AS ISO 31000:2018 *Risk management - Guidelines* Section 6.5.2.

The aim of risk treatment is to:

".. select and implement options for addressing risk."[12]

An overview of the risk treatment process has been set out in Figure 5.

Some treatments may enhance existing controls or introduce new controls. Fraud controls are specific measures, processes or functions that are intended to prevent or detect fraud events or to enable the entity to respond to them. These would be suitable to address the following outcomes:

- accept the risk
- change the consequence
- change the likelihood
- change both the consequence and likelihood
- share the risk
- retain the risk.

Subject to the entity's risk appetite and tolerance, not every risk will require the development and implementation of treatments.

Risk treatment	Better practice
Determine appropriate risk treatments	• Select risk treatment options with the entity's objectives, risk criteria and available resources • Balance the potential benefits against cost, effort or disadvantage of implementation
Document implementation plan	• Document the treatment plan outlining the responsibilities, resources and other relevant implementation information in the fraud risk worksheet
Risks that do not have a treatment option	• If no treatment options are available or if treatment options do not sufficiently modify the fraud risk, the risk is recorded and kept under ongoing review
Remaining risk is documented	• Inform decision makers and other stakeholders of the nature and extent of the remaining risk after treatment • Document the remaining risk and subject to monitoring, review and, where appropriate, further treatment
Consider beyond economic consequences	• Justification for risk treatment is broader than solely economic consequences and considers the entity's obligations, voluntary commitments and stakeholder views

Source: OAG

Table 10: Better practice examples of the risk treatment stage

[12] AS ISO 31000:2018 *Risk management - Guidelines* Clause 6.5.

A useful way to examine your controls is to ensure they are specific, measurable, achievable, relevant and timed (SMART). This model and examples of internal controls that may be applied with a view to change the consequence, likelihood or both are provided at Appendix 5.4.

Monitoring and review

Entities should actively monitor the implementation of fraud risk treatments, because until the new or improved controls are in place, the fraud risk will remain above this tolerance level. Fraud risk owners will be responsible for ensuring the controls are implemented in a timely manner and remain effective. When a new or improved control has been implemented the entity should review the control in practice over time to ensure it continues to be effective.

Further, it is essential that entities have a program to continuously monitor and review their fraud risks. Sometimes only small changes to a business process or function can alter the inherent fraud risk rating, result in the emergence of new fraud risks, or impact the effectiveness of existing controls.

Monitoring and review is:

"… to assure and improve the quality and effectiveness of process design implementation and outcomes."[13]

Monitoring and review	Better practice
Monitoring and review takes place during all elements of fraud risk management program	• Monitoring and review includes planning, gathering and analysing information, recording results and providing feedback
Monitoring and review progress is reported	• Results of monitoring and review are incorporated throughout the entity's performance management, measurement, and reporting activities

Source: OAG

Table 11: Better practice examples of the monitoring and review stage

Recording and reporting

As noted earlier, fraud risks identified through a fraud risk assessment can be integrated into the entity's broader enterprise risk register. Whether entities combine all risks into a single source risk register or maintain a separate fraud risk register, they must be documented and reported. Entities should report to appropriate oversight committees and management including any audit committees which are responsible for overseeing the entity risk management and internal controls.

Risk management process and its outcomes should be:

"… documented and reported through appropriate mechanisms."[14]

[13] AS ISO 31000:2018 *Risk management - Guidelines* Clause 6.6.

[14] AS ISO 31000:2018 *Risk management - Guidelines* Clause 6.7.

The fraud risk assessment worksheet details several key processes and outcomes that should be documented including the methodology for the risk assessment, the results and the response.

Recording and reporting	Better practice
Detailed recording of fraud risk assessment process	• Worksheets include adequate information that demonstrates reason for decisions made and actions taken
Ongoing monitoring and periodic review of the fraud risk management process and its outcomes is planned, and responsibilities clearly defined	• Updates provided to senior management and those charged with governance on progress • Monitoring through audit committee • Documented responsibilities for undertaking fraud risk management are outlined in the entities' FCS

Source: OAG

Table 12: Better practice examples of the recording and reporting stage

Conclusion

Fraud is a pervasive and growing issue within Australia. Fraud can be initiated by employees or close associates of an entity and, increasingly, by parties with no apparent connection to the entity. It can also involve collusion between internal and external parties.

Historically, the approach of many Australian entities to fraud risk management has been wholly reactive. Entities that embrace adequate and proportionate approaches to managing fraud risks will increase their chance of reducing fraud events.

We encourage entities to use this guide along with the tools and any other available resources when applying AS ISO 31000:2018 – *Risk management - Guidelines* and AS 8001:2021 – *Fraud and corruption control* to manage the risk of fraud against their entity. While fraud risks cannot be eliminated, a robust and well-resourced fraud risk management program can minimise the likelihood and consequences of fraud events.

Appendix 1: Glossary

Term	Definition
Better practice guide (BPG)	A fraud risk assessment better practice guide (this report).
Bribery	Offering, promising, giving, accepting or soliciting of an undue advantage of any value (either financial or non-financial) directly or indirectly, and irrespective of location(s), in violation of applicable law, as an inducement or reward for a person acting or refraining from acting in relation to the performance of that person's duties.
Cloud computing	The practice of using a network of remote servers hosted on the internet to store, manage, and process data, rather than a local server or a personal computer.
Close associate	A person with a close connection with the organisation other than an employee (e.g. director, consultant, contractor).
Collusive tendering	The act of multiple tenderers for a particular contract colluding in preparation of their bids – also often referred to as bid rigging.
Conflict of interest	A situation in which a person is in a position to derive personal benefit from actions or decisions made in their official capacity.
Corruption	Dishonest activity in which a person associated with an entity (e.g. director, executive or employee) acts contrary to the interests of the entity and abuses their position of trust in order to achieve personal advantage or advantage for another person or entity.
Cryptocurrency	A digital currency in which transactions are verified and records maintained by a decentralised system using cryptography, rather than by a centralised authority.
Data theft	Also known as information theft. The illegal transfer or storage of personal, confidential, or financial information.
Enterprise risk	Risks arising from the general operation of an entity that can impact on the entity's ability to meet its objectives (refer also definition of 'risk' below).
FCS	Fraud Control System - a framework for controlling the risk of fraud against or by an entity.
Fraud	Dishonest activity causing actual or potential gain or loss to any person or entity including theft of moneys or other property by persons internal and/or external to the entity and/or where deception is used at the time, immediately before or immediately following the activity.
Identity fraud	Also known as identity theft or crime. It involves someone using another individual's personal information without consent, often to obtain a benefit.
Internal control	Internal control is a process, effected by an entity's board of directors, management and other personnel, designed to provide reasonable assurance that information is reliable, accurate and timely.
Malware	Malicious software intentionally designed to cause disruption to a computer, server, client, or computer network, leak private information, gain unauthorised access to information or systems, deprive user's access to information or which unknowingly interferes with the user's computer security and privacy.

Term	Definition
Nepotism and/or Cronyism	Where the appointee is inadequately qualified to perform the role to which he or she has been appointed. The appointment of friends and associates to positions of authority, without proper regard to their qualifications.
OAG	The Office of the Auditor General.
PESTLE model	Consideration of 6 external environmental factors that can impact an entity, namely the political, economic, social, technological, legal and environmental factors.
Phishing and/or Spear-phishing	Cyber-intrusion. Theft of intellectual property or other confidential information through unauthorised systems access.
Ransomware	Form of malware designed to encrypt files on a device, rendering any files and the systems that rely on them unusable.
Risk	The effect of uncertainty on objectives. An effect is a deviation from the expected. It can be positive, negative or both, and can address, create or result in opportunities and threats.
Risk appetite	The level of overall risk an entity is prepared to accept in pursuing its objectives.
Risk tolerance	The level of risk an entity is prepared to accept in relation to specific aspects of its operation – the practical application of the concept of 'risk appetite' to specific risk categories (relevantly to the subject of this guide, this can include application of an entity's risk appetite to the concept of fraud risk).
Social engineering	A broad range of malicious activities accomplished through human interactions (e.g. psychological manipulation of people into performing actions or divulging confidential information).

Appendix 2: References

Reference
Association of Certified Fraud Examiners, 2022.
Association of Certified Fraud Examiners, *Occupational Fraud 2022: A Report to the Nations*, 2022.
Australian Cyber Security Centre Australian Cyber Security Centre analysis, 2022.
Commonwealth Fraud Prevention Centre, *Fraud Risk Assessment Leading Practice Guide,* 2022.
Cressy, D., *Other People's Money: A Study in the Social Psychology of Embezzlement,* Free Press, 1953.
Department of Justice, *Corporations Act 2001,* 2001.
Department of Justice, *Western Australia Corruption, Crime and Misconduct Act 2003*, 2022.
Department of Justice, *Western Australia Financial Management Act 2006, 2022.*
Department of Justice, *Western Australia Government Financial Responsibility Act 2000, 2021.*
Department of Justice, *Western Australia Procurement Act 2020*, 2021.
Department of Justice, *Western Australia Public Interest Disclosure Act 2003*, 2017.
Department of Justice, *Western Australia Public Sector Management Act 1994*, 2022.
Department of Treasury, Treasurer's Instructions – specifically TI 825 *Risk Management and* TI 304 *Authorisation of Payments,* 2022.
Enacting legislation for GTEs and other government bodies
Office of the Auditor General Western Australia, *Forensic Audit Report – Establishment Phase,* November 2021.
Office of the Auditor General Western Australia, *Fraud Prevention and Detection in the Public Sector*, June 2013.
Public Sector Commission WA, *Integrity Strategy for WA Public Authorities,* 2019.
Standards Australia, AS 8001:2021 – *Fraud and corruption control,* June 2021.
Standards Australia, AS ISO 37001:2019 *Anti-bribery management system,* 2019.
Standards Australia, AS ISO 31000:2018 *Risk management – Guidelines* Risk Assessment, 2018.
Standards Australia, SA SNZ HB 436-2013 *Risk Management Guidelines* (companion to AS ISO 31000:2018), 2013.

Appendix 3: Fraud control system benchmarking tool

An important component of the periodic assessment of the efficacy of an entity's FCS is to determine whether an entity's FCS aligns with the requirements and guidance set out in the standard, in effect, a benchmarking of the entity's fraud control program against the requirements and guidance of the standard. An organisation's performance against each element of the standard can be assessed in accordance with a 5-element rating scheme as set out below.

Alignment with AS 8001:2021 – *Fraud and corruption control* best practice model	Rating
Meeting better practice	5
Approaching better practice	4
Minimum acceptable level	3
Inadequate but some progress made towards better practice	2
Inadequate - no progress towards achieving better practice	1

The following are the relevant steps required to prepare and deliver an FCS benchmarking project:

Step 1	Consult and collaborate across the entity in a consideration of the FCS benchmarking model and determine which, if any, elements of the model are not relevant to the entity's own circumstances, make necessary adjustments to the model in preparation for analysis.[15]
Step 2	Gather all entity documentation pertaining to the control of fraud risk within the entity – this would include: • current FCS documentation • current governing body charter • most recent fraud risk assessment • the entity's disciplinary procedures • recent analysis of awareness raising activities within the entity • most recent external environmental scan analysis

[15] e.g. requirements and guidance of AS 8001:2021 Section 3.6 *Performance Based Targets* may not be relevant to public sector entities and could therefore be removed from the model.

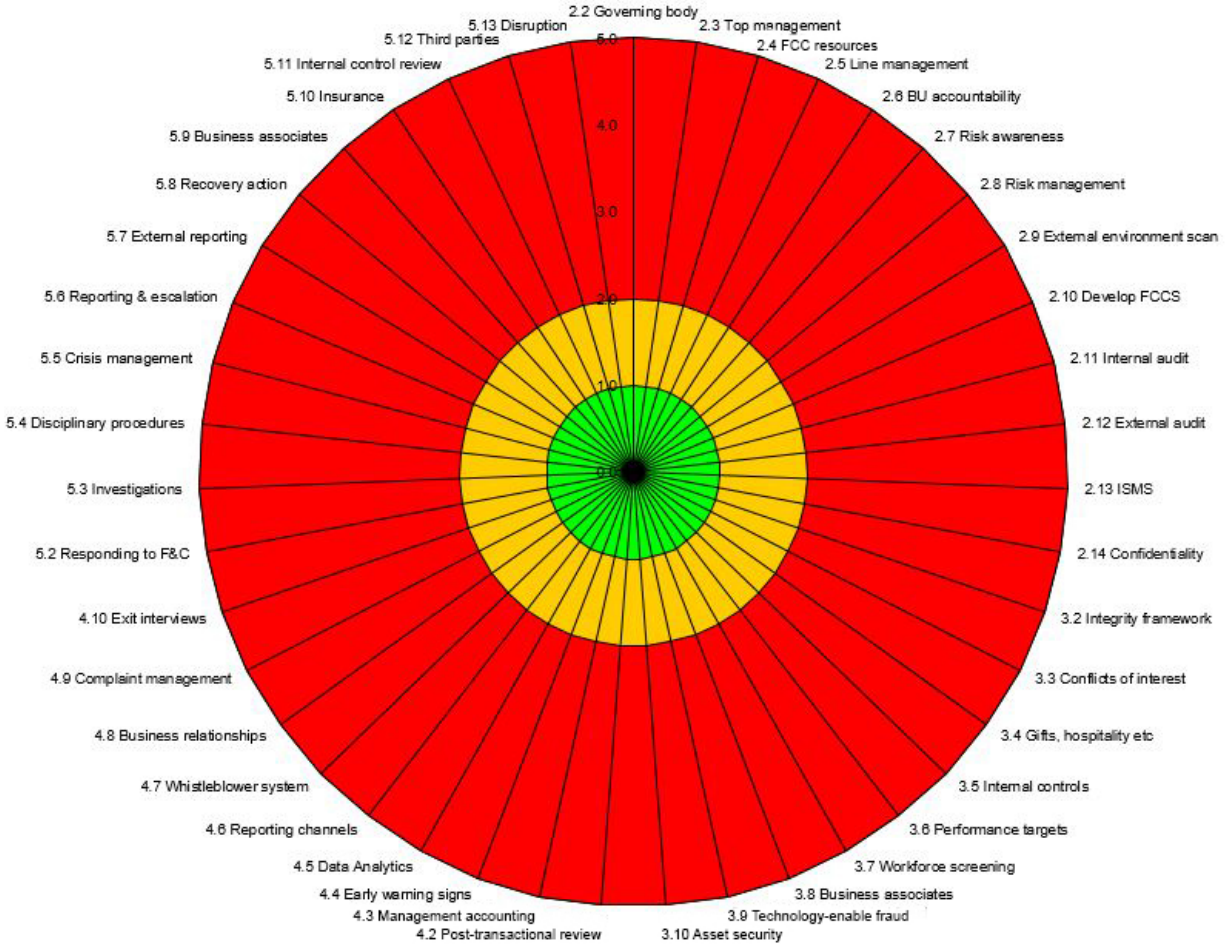
	• internal audit charter • any recent internal audit reports in relation to fraud risk management • all integrity related documentation • current workforce screening policy • current cybersecurity / information system management policies • a summary of the last 5 years fraud incidents covering results could provide insight into common activities, themes and weaknesses. Details such as number of events per year, fraud theme (procurement, CC etc), quantum, fraud substantiated Y/N, vulnerability identified, how vulnerability treated, date vulnerability treated • reports of analysis of internal control efficacy including pressure testing transactions.
Step 3	Consult broadly across the entity to arrive at a realistic and reliable assessment of the entity's current performance against each relevant element of AS8001:2021. Consultation would include: • if a relevant policy or procedure is currently in place or is proposed • the frequency of review of all relevant policies and procedures • if there is adequate resourcing to ensure that the FCS is properly and effectively administered • the culture within the entity in terms of adherence to the key elements of the FCS.
Step 4	Collaborate with relevant system and process owners to arrive at a rating on a scale of 1 to 5 for each element of the FCS being assessed in terms of its current alignment with AS 8001:2021.
Step 5	Consult broadly within the organisation in relation to initiatives currently in train for implementation in the future, collaborate with relevant system and process owners to arrive at a rating on a scale of 1 to 5 for each element of the FCS being assessed in terms of its future alignment with AS 8001:2021 on the assumption that the initiative is fully implemented.
Step 6	Enter scores into the model and review the output chart.
Step 7	Present to the relevant oversight committee within the entity.
Step 8	Implement remedial action required for the entity to better align with the better practice model per AS 8001:2021.
Step 9	Monitor the ongoing efficacy of the FCS in light of this analysis over time.

Presentation of the benchmarking analysis

The outcome of this analysis can be usefully presented in a variety of tabular or graphical formats. The way in which the benchmarking analysis results are presented will depend on the needs of the entity. One particularly visual way of presenting the outcomes of the benchmarking analysis is by way of a ‘spider-web’ diagram as shown below.

A Microsoft Excel tool is provided on our website with detailed instructions to assist in the preparation of this analysis and production of the spider web diagram is detailed below.

The spider web diagram is particularly useful for presenting current and future state alignment of an entity’s FCS with AS 8001:2021 and for showing improvement over time. For example, if a spider web diagram depicting the current and anticipated alignment of the entity’s FCS with AS 8001:2021 is presented to each meeting of the relevant oversighting committee (e.g. an audit committee) the committee would be able to efficiently monitor progress against action items initiated to address identified gaps.



The green area	Represents the entity's current alignment with the requirements and guidance of AS 8001:2021.
The amber area	Represents the entity's anticipated future alignment with the requirements and guidance of AS 8001:2021 once initiatives currently in train are fully implemented. Theoretically, the amber area should progressively turn to green over the projected implementation timeframe.
The red area	Represents the current 'gap' between either the current alignment (green) or anticipated future alignment (amber) with the requirements and guidance of AS 8001:2021.

(Appendix AAR: 8.1D)

Appendix 4: External threat assessment tool

Assessment of external threats using the PESTLE model requires a rigorous 7-step process as follows:

Step 1: Consult and collaborate across the entity, make necessary adjustments to the worksheet in preparation for analysis.

Step 2: Gather all documentation pertaining to external threats in the environment in which the entity operates or is considering operations.

Step 3: Consider the most recent fraud risk assessment conducted in relation to the entity's operation.

Step 4: In collaboration with risk and process owners, consider the six PESTLE factors that could impact the entity's fraud risks.

Step 5: Identify external factors that need to be addressed by the entity to more effectively control fraud risks.

Step 6: Develop risk treatments for risks that need to be further mitigated and adjust in fraud risk assessment and fraud control system.

Step 7: Review external threats periodically.

The following is an example worksheet for assessing external threats against an entity using the PESTLE model.

PESTLE factor	Example questions to consider	External threat assessment	Action to be taken (risk assessment, risk treatments, fraud control system)
Political			
To identify the political situation of the country in which the organisation operates, including the stability and leadership of the government, whether there is a budget deficit or surplus, lobbying interests and international political pressure.	1. Has there been a recent change in government (at local, state or federal level)? 2. Is there any anticipated change in government funding foreshadowed? How will a change in funding impact the entity's fraud exposure (e.g. an increase in funding for grants or a decrease in funding for administration)? 3. Is there any legislative change anticipated in relation to employment law that may impact the entity's ability to manage its fraud exposure?	Insert text	Insert text

(Appendix AAR: 8.1D)

115

PESTLE factor	Example questions to consider	External threat assessment	Action to be taken (risk assessment, risk treatments, fraud control system)
	4. Is there a likely increase or reduction in government mandated regulation? 5. If yes, will that give rise to an increase in the entity's fraud exposure (either internally or externally initiated fraud)? 6. Are there any other political factors the entity should consider?		
Economic			
To determine the economic factors that could have an impact on the organisation, including interest rates, inflation, unemployment rates, foreign exchange rates and monetary or fiscal policies.	1. Are all economies in which the entity operates currently stable? 2. If there are indications of instability in an economy in which the entity operates, to what degree will this impact the risk of fraud within or against the entity? 3. Are there any key economic decisions (either recently implemented or in contemplation) likely to have an impact on the entity's fraud exposure (e.g. rising interest rates, a change in taxation rates)? 4. Is there currently significant pressure on wages and salaries that could act to reduce disposable income of the general population and to what degree could that impact on the entity's fraud exposure? 5. Is there likely to be a change in employment levels in the economy in the next three to five years?	Insert text	Insert text

(Appendix AAR: 8.1D)

116

PESTLE factor	Example questions to consider	External threat assessment	Action to be taken (risk assessment, risk treatments, fraud control system)
	6. Is there likely to be a change in working arrangements that may increase the risk of fraud within the entity (e.g. remote working, flexible working arrangements)? 7. Are there any other economic factors the entity should consider?		
Social			
To identify the expectations of society by analysing factors such as consumer demographics, significant world events, integrity issues, cultural, ethnic and religious factors, and consumer opinions.	1. Has there been a marked decline in integrity standards within the broader community or is this anticipated going forward? How could these changes impact the entity's fraud exposures in the future? 2. Is it likely that the entity will only be able to attract adequate human resource is by offering work arrangements that are not sustainable for the entity? 3. Are there any other social factors they should consider?	Insert text	Insert text
Technological			
To identify how technology, including technological advancements, social media platforms and the role of the internet more broadly, is affecting or could affect the organisation.	1. Does the entity have a heavy reliance on technology internally? 2. Does the entity have a heavy reliance on technology to interact with external parties including business associates, customers, clients	Insert text	Insert text

(Appendix AAR: 8.1D)

PESTLE factor	Example questions to consider	External threat assessment	Action to be taken (risk assessment, risk treatments, fraud control system)
	and the general public? 3. Does the entity embrace leading edge cyber-security? 4. Does the entity have strict policies governing the use of its IT equipment by the workforce for personal purposes? 5. Does the entity have strong controls over the use of technology in the course of remote working? 6. Does the entity closely monitor developments in technology-enabled fraud? 7. Are there any other technological factors that the entity should consider?		
Legal			
To identify how specific legislation, including industry specific regulations, and case law are affecting or could affect the organisation's future operations.	1. Does the entity have a strong compliance function? 2. Does the entity have a strong sense of its own duties of integrity when interacting with external parties (i.e. is there a risk of the entity itself being accused of fraudulent or other illegal conduct)? 3. Are there indicators of significant change in the regulatory landscape affecting the entity? 4. Is the entity aware of its vicarious liabilities in relation to the conduct of members of its own		

PESTLE factor	Example questions to consider	External threat assessment	Action to be taken (risk assessment, risk treatments, fraud control system)
	workforce? 5. Are there any other legal factors that the entity should consider?		
Environmental			
To identify how local, national and international environmental issues are affecting or could affect the organisation.	1. Does the entity operate in circumstances where there is a likelihood of a high environmental impact? 2. If so, does this give rise to any raised risk of manipulation of financial or non-financial reporting? 3. Are there any other environmental factors that the entity should consider?		

(Appendix AAR: 8.1D)

Appendix 5: Tools to support the fraud risk management process

A5.1 Communication and consultation tool

Fraud risk owners can sometimes encounter problems with those responsible for developing, implementing and maintaining fraud controls relating to their risks. This may be because a control owner is experiencing staffing or funding constraints or they lack the requisite expertise. In these circumstances the person tasked with performing the fraud risk program can assist through:

- requesting progressive pieces of work
- fostering productive linkages between parties responsible for fraud control
- providing expert advice to stakeholders
- seeking strategic support from the senior staff to formulate solutions to impediments at the operational or program level.

The table below describes some methods for communication and consultation across an entity.

Structured one-on-one discussion with the process / risk owners	Speak with relevant business units – the people who work with the systems and processes every day. Meet one-on-one to facilitate an enhanced understanding of relevant risk and control issues.
Convene focus groups with process and risk owners and stakeholders	Facilitate detailed discussion of fraud risks with focus groups along with one-on-one meetings as an effective way to identify risks, internal controls that should mitigate those risks, whether they are operating as intended (think like a fraudster), assessing risks and developing effective risk treatments.
Seek input on fraud risk matters from across the entity	Invite the entire workforce to provide their input in relation to the entity's fraud exposures in an online survey.
Regular reporting to the project management committee	A project to manage fraud risk should be subject to a rigorous program of two-way communication between the oversight committee and the practitioner/team tasked with the project.
External communication and consultation	The project committee and the team responsible for delivering the project should consider the benefits of communication and consultation with parties external to the entity such as regulators, subject matter experts and peer organisations.
Reporting to the audit and risk committee	It is important for an audit and risk committee to be informed of developments in relation to fraud risks because they are responsible for overseeing the entity's risk management and internal controls.

A5.2 Scope context and criteria tool

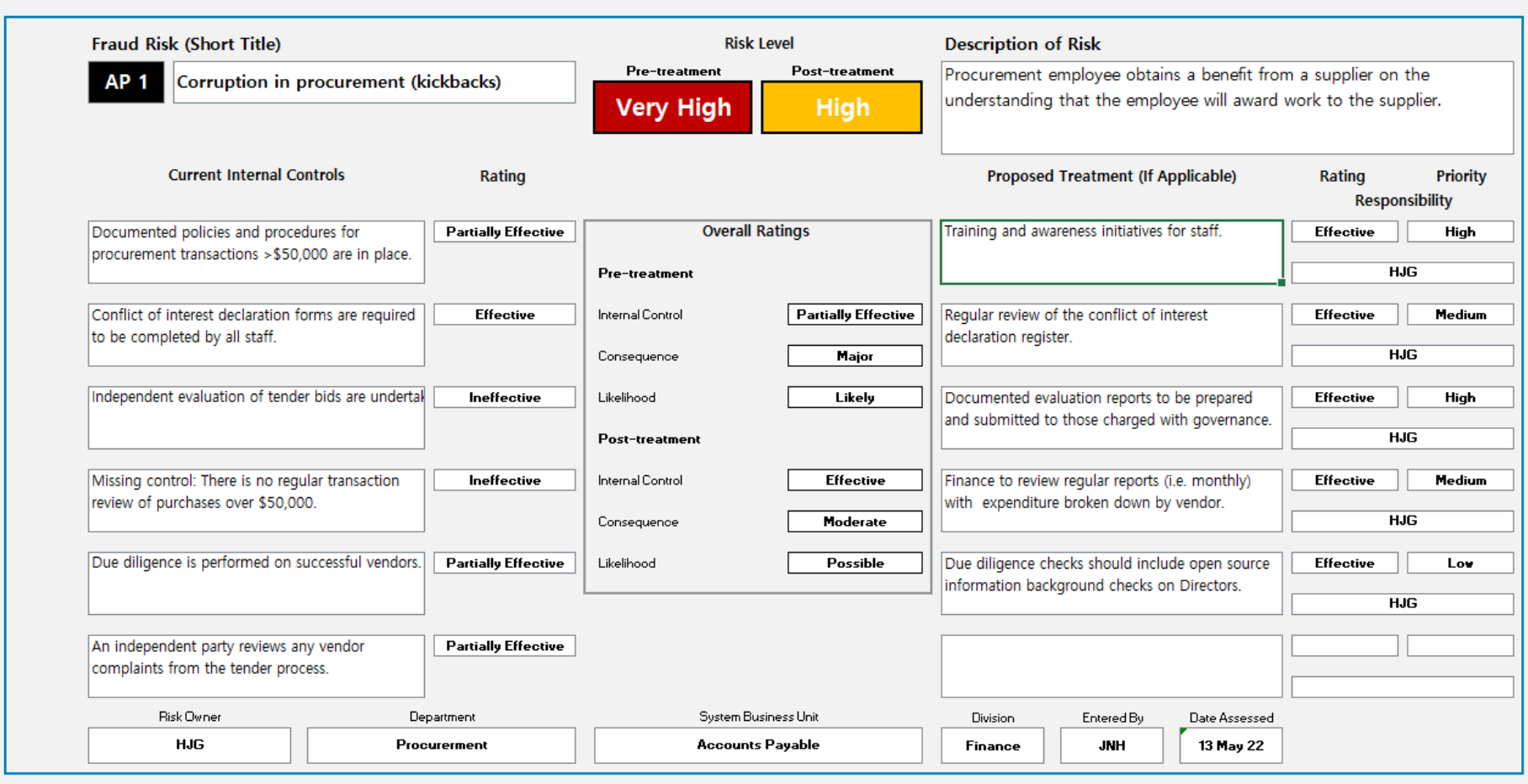
Factor	Definition	Fraud risk assessment "XX Process"
Scope	The boundaries within which the fraud risk assessment will take place.	• The specific parts of the XX process to be assessed for fraud risks. • The business units and operational teams involved in the processes to be assessed. • Tools to be used in the fraud risk assessment. • Logistical considerations, milestones and timelines for completing the fraud risk assessment.
Context	The internal and external factors influencing the environment the entity operates in.	Internal factors may include: • The strategic objectives of the entity and how this influences the XX process. • The existing employee level in the XX process and their experience, as well as their level of training in identifying indicators of potential fraud. External factors include: • Increasing fraud trends targeting XX process. • Recent known scams in the public domain that have been uncovered.
Criteria	Likelihood and consequence criteria aligned to an entity's existing risk framework that can be used to rate fraud risks identified in the fraud risk assessment.	• Likelihood criteria is a rating scale (i.e Extremely unlikely to Almost certain) set by the entity to identify the expected frequency of a fraud risk in the XX process being realised, both with no internal controls in place (inherent) and existing controls in place (residual). • Consequence criteria is a rating scale (Low – Catastrophic) across a number of defined loss factors (i.e. financial damage, reputational damage, legal damage), to identify the expected impact of a fraud risk in the XX process being realised both with no internal controls in place (inherent) and existing controls in place (residual). • What is acceptable frequency / consequence.

(Appendix AAR: 8.1D)

A5.3 Risk assessment tools

A5.3.1 Example fraud risk assessment worksheet

A fraud risk assessment worksheet can be used to document all relevant information for each risk identified and assessed. Having applied the worksheet for this purpose it can also then be used as a risk register (alternatively, identified and assessed fraud risks could be included in the entity's enterprise risk register).



Fraud Risk (Short Title)		Risk Level: Pre-treatment	Risk Level: Post-treatment	Description of Risk
AP 1	Corruption in procurement (kickbacks)	Very High	High	Procurement employee obtains a benefit from a supplier on the understanding that the employee will award work to the supplier.

Current Internal Controls	Rating	Proposed Treatment (If Applicable)	Rating	Priority / Responsibility
Documented policies and procedures for procurement transactions >$50,000 are in place.	Partially Effective	Training and awareness initiatives for staff.	Effective	High / HJG
Conflict of interest declaration forms are required to be completed by all staff.	Effective	Regular review of the conflict of interest declaration register.	Effective	Medium / HJG
Independent evaluation of tender bids are undertal	Ineffective	Documented evaluation reports to be prepared and submitted to those charged with governance.	Effective	High / HJG
Missing control: There is no regular transaction review of purchases over $50,000.	Ineffective	Finance to review regular reports (i.e. monthly) with expenditure broken down by vendor.	Effective	Medium / HJG
Due diligence is performed on successful vendors.	Partially Effective	Due diligence checks should include open source information background checks on Directors.	Effective	Low / HJG
An independent party reviews any vendor complaints from the tender process.	Partially Effective			

Overall Ratings	
Pre-treatment	
Internal Control	Partially Effective
Consequence	Major
Likelihood	Likely
Post-treatment	
Internal Control	Effective
Consequence	Moderate
Likelihood	Possible

Risk Owner	Department	System Business Unit	Division	Entered By	Date Assessed
HJG	Procurement	Accounts Payable	Finance	JNH	13 May 22

(Appendix AAR: 8.1D)

The following is a short summary of the information that would be recorded on each risk assessment sheet (note that much of the information referred to in the following table will not have been prepared in the risk identification stage when the fraud risk worksheet is first created. The worksheet is intended to build over time as the entity works its way through the identification, analysis, evaluation and treatment development phases).

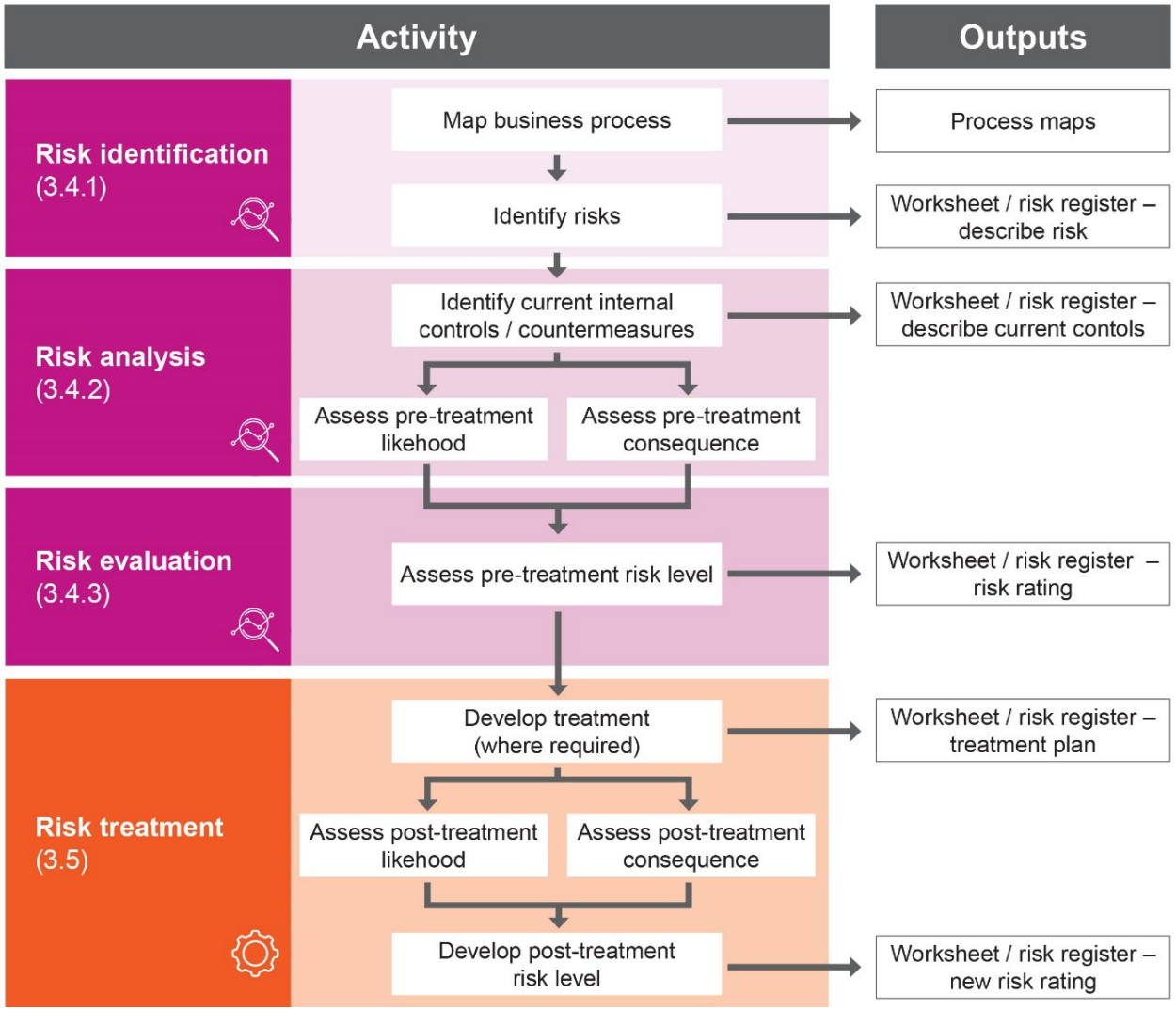
As noted above, each identified risk should be recorded on a separate risk assessment worksheet. The risk assessment worksheet can then be used as the entity's register of fraud risks. Alternatively, identified and assessed fraud risks can be recorded in the entity's enterprise risk register.

Data field	Information to be recorded (for each risk)
Fraud Risk Number	A reference number unique to each risk – the risk number is used in all outputs of the risk assessment process.
Fraud Risk (Short Title)	Short description of the risk that is generally used to identify the risk being discussed in relevant outputs.
Description of Risk	A more detailed outline of the risk consistent with the short title.
Risk Owner	The individual or position within the business unit who has primary responsibility for the business systems relevant to the identified fraud risk.
Department	The department to which the business unit belongs (see below).
System Business Unit	The business unit that has most control of the business systems and processes relevant to the identified risk.
Entered By	The individual or position who entered the fraud risk particulars into the risk assessment worksheet.
Date Assessed	The date on which the worksheet was populated.
Current Internal Controls	A short active title / description of each existing internal control (e.g. "System controls only allow limited authorised users to change bank accounts") and a short statement as to how the internal control mitigates the risk.
Current Internal Controls Rating	A rating on an appropriate scale (i.e. "Ineffective", "Partially Effective" or "Effective") of the effectiveness of each internal control on mitigating the risk.
Proposed Treatment (If Applicable)	Treatments the entity proposes to take to strengthen the existing internal control framework and reduce the risk rating to an acceptable level.
Proposed Treatment (If Applicable) Rating	A rating on an appropriate scale (i.e. "Ineffective", "Partially Effective" or "Effective") of the effectiveness of each treatment on mitigating the risk.
Proposed Treatment Priority	The proposed priority of the treatment.
Overall Ratings – Pre-treatment Internal Control	A rating on an appropriate scale (i.e. "Ineffective", "Partially Effective" or "Effective") of the overall effectiveness of the existing internal control framework on mitigating the risk.

Data field	Information to be recorded (for each risk)
Overall Ratings – Pre-treatment Likelihood	A rating on an appropriate scale (i.e. “Almost Certain” to “Rare”) of the likelihood of a risk being realised with the existing internal control framework.
Overall Ratings – Pre-treatment Consequence	A rating on an appropriate scale (i.e. “Extreme” to “Negligible”) of the consequence of a risk being realised with the existing internal control framework.
Overall Ratings – Post-treatment Internal Control	A rating on an appropriate scale (i.e. “Ineffective”, “Partially Effective” or “Effective”) of the overall effectiveness of the post-treatment internal control framework on mitigating the risk.
Overall Ratings – Post-treatment Likelihood	A rating on an appropriate scale (i.e. “Almost Certain” to “Rare”) of the likelihood of a risk being realised with the post-treatment internal control framework.
Overall Ratings – Post-treatment Consequence	A rating on an appropriate scale (i.e. “Extreme” to “Negligible”) of the consequence of a risk being realised with the post-treatment internal control framework.
Overall Risk Rating Pre-treatment	A rating on an appropriate scale (i.e. “Very High” to “Low”) of the fraud risk level by reference to the risk matrix (taking into account the assessed effectiveness of pre-existing internal controls).
Overall Risk Rating Post-treatment	A rating on an appropriate scale (i.e. “Very High” to “Low”) of the fraud risk level by reference to the risk matrix taking into account the assessed effectiveness of the post-treatment internal control framework.

(Appendix AAR: 8.1D)

A5.3.2 Risk assessment and treatment process overview



Source: OAG based on AS ISO 31000:2018 *Risk management - Guidelines* Clause 6.4 and 6.5

(Appendix AAR: 8.1D)

A5.3.3 Key fraud risk identification questions

Some key questions to ask when trying to identify fraud risks are listed below.

Key questions that need to be asked in identifying fraud risks
If I wanted to steal from this entity, knowing what I know about the current business systems process and internal controls, how would I do it?
If I wanted to get some sort of improper financial or non-financial advantage out of my position, how would I do it?
What do I know about this process that nobody else knows or checks?
Who has sole control over specific systems or processes that nobody else has visibility over?
What forms of payment does this process have – is it cash, card, EFT etc?
How can this process be made easier for the process owner at the expense of the entity?

A5.3.4 Commonwealth Fraud Prevention Centre's 'Actor, Action, Outcome' method of describing fraud risks[16]

An effective method for describing fraud risk is to consider the actor, action and outcome. The level of detail is important when describing fraud risks. Without sufficient detail it becomes difficult to consider the factors (i.e. actors and actions) that contribute to the fraud risk and how fraud controls will specifically address these contributing factors.

An example of a poorly defined fraud risk from the invoice payment process provided would be "Fraud in the invoice payment process".

The following are more accurately defined fraud risks from the same example:

- "a service provider (Actor) submits a falsified invoice (Action) to receive a payment for services not provided (Outcome)"
- "a service provider (Actor) coerces an official to approve and/or process a falsified invoice (Action) to receive a payment for services not provided (Outcome)"
- "an official (Actor) manipulates the finance system (Action) to divert an invoice payment to their own bank account (Outcome)".

Judgement should be applied in striking a balance between capturing sufficient detail and documenting a manageable number of fraud risks. This could be achieved by combining similar risks and clearly documenting the various contributing factors (actors and actions).

[16] Commonwealth Fraud Prevention Centre '*Fraud Risk Assessment – Leading Practice Guide'.*

The description can help with an entity's assessment of its fraud risks and how it considers ways in which to control it. Some of these controls may already exist and some may be new.

For example, an entity might limit the opportunity for an accounts payable officer to submit and processes a fictitious invoice that pays into an employee's account by:

- splitting the authorising powers (submit and process)
    - segregation of duties between invoice entry and payment authority
- validating the invoice details (fictitious invoice)
    - third party verification of goods/services being received
    - check supplier details in your supplier master file are an exact match to public records (e.g. Australian Business Register)
- cross-checking internal records (employee account)
    - compare bank accounts in supplier payment file against employee bank accounts.

Entities can link each of the above controls back to distinct parts (actor, action, outcome) of the fraud description.

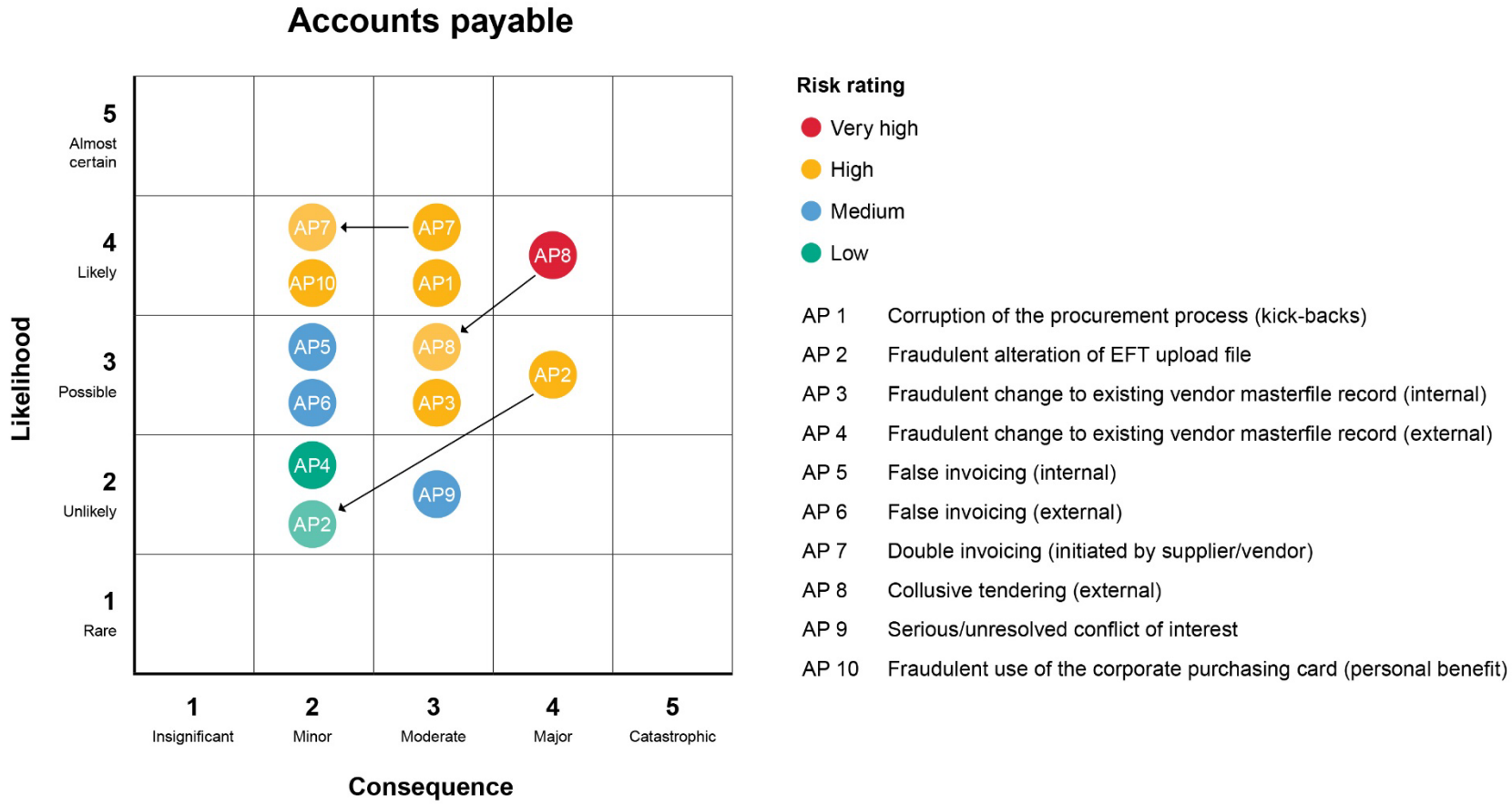
(Appendix AAR: 8.1D)

127

A5.3.5 Example diagrammatic presentation of assessed fraud risks

It can be useful to present identified and assist fraud risks in diagrammatic form.

The following example shows the relative ratings of likelihood and consequence and the resulting overall risk rating for ten accounts payable related fraud risks. Diagrammatic analysis is also useful to show the projected change in risk rating as a result of implementation of a treatment plan introducing new or revised internal controls / fraud controls. The change in rating in relation to risk PR-1 is due to the introduction of new or revised internal controls that will reduce the consequence of the risk if it did occur (although in this example the likelihood remains unchanged).



A5.3.6 Example public sector fraud risks

The following is a short summary of fraud risks that are commonly found in the public sector environment. This summary is not intended to be an exhaustive list, but it can be used as a 'thought provoker' in the identification of operational risks types facing the entity being assessed.

Accounts payable fraud	
False invoicing (creation of a fictitious vendor)	A fictitious vendor is created in the finance system to which payments for false invoices are made for goods/services not ordered and not delivered (typically fraud of this type involves personnel within the entity but it can be perpetrated at times by external parties acting alone or by external parties operating in collusion with a member of the target entity's workforce)
Fraudulent change to vendor master file	Fraudulent change to the entity's vendor master file (i.e. change of bank details to divert legitimate vendor payments to an account controlled by the perpetrator) – this can be done by a person internal to the entity, a person external to the entity or by collusion between internal and external persons
Online banking fraud	Manipulation of vendor or other payments in the online banking system immediately prior to execution of the payment file in the entity's online banking system – the fraudulent manipulation of the online payment file is concealed by making false entries in the entity's accounting records
False invoicing (existing vendor)	Manipulation and processing of fraudulent payments for invoices apparently rendered by a legitimate vendor but, in fact, fraudulently generated and issued by the perpetrator who is generally a member of the entity's own workforce
Duplicate payments for the invoices already settled	More than one payment is made for the same invoice – this can be initiated inadvertently by a vendor who issues the same invoice twice in error but the vendor then fails to report the double receipt and fraudulently converts the duplicate payment

Procurement and tendering	
Corruption of the procurement process (involving personnel within the entity)	Corruption involving an employee of the entity and a vendor in the selection of a winning bid or tender often involving bribery / kickbacks but often motivated by personal or family association between the bidder and the entity's employee without direct financial reward – corruption can involve provision of a confidential bid price, contract details or other sensitive information to gain an advantage for one tenderer over other tenderers
Bid rigging (excluding personnel within the entity)	Collusive tendering between multiple bidders for the same contract for mutual advantage (no involvement of the entity's personnel)

Procurement and tendering	
Conflicts of interest	Undeclared association between an employee of an entity and a tenderer giving rise to an actual or perceived bias in awarding of a contract
Improperly receiving hospitality, gifts and benefits	An employee receiving or soliciting hospitality, gifts or benefits from a vendor or potential vendor hoping to gain a commercial advantage in doing so – depending on the circumstances, this behaviour may constitute fraud

Falsification and manipulation of claims for work-related expenditure	
Use of the entity's funds for personal expenditure	Claiming employee expenses for business-related expenditure not incurred or incurred for personal use or benefit (supported by false or inflated receipts / invoices)
Double-dipping	Claiming multiple reimbursements for the same expenses or claiming for expenses paid personally using receipts for purchases already made via another of the entity's reimbursement systems

Diversion of incoming funds	
Accounts receivable fraud	Redirection of incoming receipts to a spurious account followed by write-off of accounts receivable balance
Unauthorised discounts	Processing unauthorised discounts for early payment of invoices where the discount value is fraudulently transferred to the employee's own bank account
An authorised application of unknown receipts	Funds can be received by an entity where the source of the funds is unknown and the funds are allocated to a suspense account pending rectification – a possible fraud involves the transfer of part of the balance of the suspense account to an employee's own benefit with a manipulation of the accounting system to conceal the theft
Inflating invoice value	Inflating the value of an invoice raised by the entity with receipts in payment of the invoice directed to a spurious account controlled by the staff member concerned who then redirects the correct (reduced) value of the invoice to the entity's correct account
Vendor overpayment	Deliberately overpay a vendor in payment of an invoice for goods or services validly received, claim a refund for the overpayment and then direct the remittance to a spurious bank account
Theft of cash all funds received	Fraudulently failing to record receipt of cash received and then misappropriate for own benefit

Payroll	
Timesheet fraud	Fraudulent submission of falsified timesheets for casual employees who did not work with diversion of resulting remuneration generated to own account
Fraudulent alteration of remuneration rates	Alteration of remuneration rates (salaries or hourly rates) in the payroll system in relation to the employee making the change or for another employee in exchange for personal benefit
Ghost employee fraud	Fabrication of fictitious employees on the payroll with remuneration paid to own account
Fraudulently failing to record personal leave	An employee taking personal leave (annual, long-service, sick or carer's leave) without recording the leave in the HR system
Worker's compensation fraud	Worker's compensation fraud – fraudulent claims for injuries not sustained

Assets and Inventory	
Asset theft	Theft of the entity's assets, including computers and other IT related assets
Information theft	Theft or abuse of proprietary or confidential information (customer information, intellectual property, pricing schedules, business plans, etc)
Unauthorised private use of employer property	Use of employer property for personal use or benefit
Cash theft	Theft of petty cash

Manipulation of financial reporting	
Fraudulent manipulation of an entity's financial reporting	Fraudulent manipulation of financial reports in order to make it appear that a business entity has performed better (in financial or non-financial terms) than it has actually performed – this can be motivated by a need to demonstrate a certain level of personal performance in order to secure a performance bonus but may also be driven in the public sector by the need to meet political expectations

Cyber-borne attack	
Business email compromise	Emails impersonating vendors or an executive instructing payment to be made to a spurious bank account or a change to existing bank details
Phishing emails	Emails designed to dupe employees into providing personal information (i.e. by clicking on a link or opening an attachment)
Malware	Installing malware onto a computer or computer system within the entity which then issues fraudulent instructions (e.g. to change the bank account of a vendor in the vendor masterfile or change the payroll bank account of one or more employees)

A5.4 Risk treatment tools

A5.4.1 SMART principle for co-designing fraud controls[17]

Think about the fraud risk you have described and ways in which you might be able to prevent, monitor or detect the exploitation.

The following table outlines the 'SMART' principle which can be applied to help co-design controls with key risk stakeholders.

Specific	The control should have a clear and concise objective. They should also be well defined and clear to anyone with a basic knowledge of the work. Consider: who, what, where, when and why.
Measurable	The control and its progress should be measurable. Consider: • What does the completed control look like? • What are the benefits of the control and when they will be achieved? • The cost of the control (both financial and staffing resources).
Achievable	The control should be practical, reasonable and credible and should also consider the available resources. Consider: • Is the control achievable with available resources? • Does the control comply with policy and legislation?
Relevant	The control should be relevant to the risk. Consider: • Does the control modify the level of risk (through impacting the causes and consequences)? • Is the control compatible with the entity's objectives and priorities?
Timed	The control should specify timeframes for completion and when benefits are expected to be achieved.

[17] Commonwealth Fraud Prevention Centre '*Fraud Risk Assessment – Leading Practice Guide'.*

A5.4.2 Example internal controls that may be effective in controlling fraud risks

The following is a short summary of internal controls that experience has shown may be effective in controlling fraud risks in each of the categories contemplated in A5.3.6 above.

Once again, this is not intended as an exhaustive list and is intended to promote consideration of current and possible internal controls within each WA public sector entity when undertaking a targeted fraud risk assessment. It is anticipated that these internal controls may be effective in controlling fraud by:

- preventing a fraudulent transaction from being processed
- quickly detecting a fraudulent transaction after it has been processed thereby preventing any further transactions and minimising loss
- assisting an entity to respond to fraud incidents that have been detected.

The internal controls set out below can be used to:

- identify internal controls already in place during the risk analysis phase of the risk assessment
- identify internal controls that may be useful in further mitigating fraud risk in the risk evaluation phase of the risk assessment.

Accounts payable fraud
• Separate procurement and payment functions
• Separate handling (receipt and deposit) functions from record keeping functions (recording transactions and reconciling accounts)
• Require reconciliation to be completed by an independent person who does not have record keeping responsibilities
• Monitor the entity's financial activity, compare actual to budgeted revenues and expenses
• Require procurement and accounts payable employees to take leave of a minimum duration (e.g. two weeks at a time) with another member of the team performing their role in their absence
• If the entity is so small that duties cannot be separated, require an independent check of work being done supplemented by appropriate and effective data analytics and other reviews appropriate to the entity's situation

Procurement and tendering
• Implement a tendering / contracting panel made up of independent personnel (i.e. unconnected to the procurement processes), to oversight the awarding of contracts
• Standard contract conditions and specifications to be used with variations to be approved by senior management
• Use evaluation criteria as agreed by the contract panel prior to tendering
• Contract terms and conditions should be those of the purchasing department and not subject to change without the written approval of senior management
• Clear audit trails with written records including formal authorisation of changes to original documentation
• Independent post-transactional review of a substantial sample of tendering and contracting transactions with a particular focus on high-risk transaction types
• Splitting of contacts should not be permitted unless authorised by senior management
• Management reviews of the reasonableness and competitiveness of prices
• Ensure contractors with a poor performance record are removed from the approved supplier's list

Falsification and manipulation of claims for work-related expenditure
• Limit the number of entity issued purchasing cards and users
• Set account limits with purchasing card providers (value, items that can be purchased etc.)
• Require employees with entity issued purchasing cards to submit itemised, original receipts for all purchases followed by lodgement of hard copy supporting documentation
• Independent rigorous examination of credit card transactions each month including detailed review of relevant receipts, invoices and other supporting documentation

Falsification and manipulation of claims for work-related expenditure
• Periodic review of a sample of hardcopy supporting documentation
• Monitor the entity's financial activity, compare actual to budgeted revenues and expenses
• Require an explanation of significant variations from budget

Diversion of incoming receipts
• Send official notification to all regular providers / suppliers with particulars of the entity's bank account with statement that this is the only account to which refunds should be remitted
• Independent post-transactional view of a sample of invoices rendered to identify any manipulations
• Independent post-transactional review of emails between accounts payable / accounts receivable personnel within the entity and customers / clients to determine if there is any indication of manipulation of invoices raised or payments made

Payroll
• Payroll system procedures and training
• Segregation of duties preventing payroll batch file payments or payroll master file changes without two approvers
• Limited system administrator access to the payroll system
• System controls to prevent changes to pay rates or salaries without approval
• Changes to payroll masterfile (e.g. particularly for bank account numbers) only available to employees via an HR 'kiosk' in the HR system – system unable to process a change of bank account number outside of the HR kiosk
• HR system to automatically generate a confirmation email to the employee where there has been a change of masterful data
• Rigorous approval process for creation of new employees in the payroll system

Payroll
• Timely notification process from HR to Payroll of employees due to resign from the entity
• Periodic review of payroll system audit logs
• Management review of variance reports from previous payroll run to confirm reasons for significant differences
• Employee background checks for new hires with access to the payroll system – this should include criminal record screening and specific questions about any previous integrity concerns / disciplinary findings etc.
• Mandatory password changes for those with access to the payroll system to a suitable strength and complexity
• Physical security of computers used by payroll staff with direct system access
• Electronic timesheet systems and approval process for overtime

Assets and inventory
• Physical security of desirable assets (i.e. laptops, IT equipment)
• Password protection and remote wiping capability in the case a laptop is lost or stolen
• Regular stocktakes of assets and inventory and updating asset registers
• Security of cash (i.e. petty cash) and gift vouchers in locked tins or a safe
• Tracking systems for assets and approval process for transfer of location
• Maintain vehicle logs, listing the dates, times, mileage or odometer readings, purpose of the trip, and name of the employee using the vehicle

Manipulation of financial reporting
• Active engagement with entity's external auditor in relation to the annual audit (i.e. working collaboratively with the auditor to identify any manipulation of the financial reporting)
• Analysis to identify unusual activity
• Detailed review of journal and other adjustments to the general Ledger with a focus, as a minimum, on high value transactions

Cyber-borne attack
• BitLocker protection of all IT assets to ensure security of data
• Access to databases/systems require unique user logon identification and password authentication
• Document authorisation that is needed to establish accountability and issue, alter, or revoke user access
• Prohibit shared user logon IDs and passwords, and user logon IDs and passwords
• Set database user access permissions that are based on the principles of privilege and separation of duties
• Restrict access to servers and office locations which contain sensitive and confidential data by physical security to authorised personnel
• Access to databases/systems require unique user logon identification and password authentication

This page is intentionally left blank

Auditor General's 2021-22 reports

Number	Title	Date tabled
19	Forensic Audit – Construction Training Fund	22 June 2022
18	Opinion on Ministerial Notification – FPC Sawmill Volumes	20 June 2022
17	2022 Transparency Report – Major Projects	17 June 2022
16	Staff Rostering in Corrective Services	18 May 2022
15	COVID-19 Contact Tracing System – Application Audit	18 May 2022
14	Audit Results Report – Annual 2020-21 Financial Audits of State Government Entities Part 2: COVID-19 Impacts	9 May 2022
13	Information Systems Audit Report 2022 – State Government Entities	31 March 2022
12	Viable Cycling in the Perth Area	9 December 2021
11	Forensic Audit Report – Establishment Phase	8 December 2021
10	Audit Results Report – Annual 2020-21 Financial Audits of State Government Entities	24 November 2021
9	Cyber Security in Local Government	24 November 2021
8	WA's COVID-19 Vaccine Roll-out	18 November 2021
7	Water Corporation: Management of Water Pipes – Follow-Up	17 November 2021
6	Roll-out of State COVID-19 Stimulus Initiatives: July 2020 – March 2021	20 October 2021
5	Local Government COVID-19 Financial Hardship Support	15 October 2021
4	Public Building Maintenance	24 August 2021
3	Staff Exit Controls	5 August 2021
2	SafeWA – Application Audit	2 August 2021
1	Opinion on Ministerial Notification – FPC Arbitration Outcome	29 July 2021

Office of the Auditor General
Serving the Public Interest

Office of the Auditor General
Western Australia

7th Floor Albert Facey House
469 Wellington Street, Perth

Perth BC, PO Box 8489
PERTH WA 6849

T: 08 6557 7500
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

(Appendix AAR: 8.1E)

Western Australian
Auditor General's Report

Information Systems Audit Report 2022 – Local Government Entities

Report 22: 2021-22
28 June 2022

Office of the Auditor General
Western Australia

Audit team:
Aloha Morrissey
Kamran Aslam
Svetla Alphonso
Ben Goodwin
Khubaib Gondal
Michael Chumak
Sayem Chowdhury
Reshma Vikas
Sooraj Suresh
Tuck Owyong
Karen Telford
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.

(Appendix AAR: 8.1E)

WESTERN AUSTRALIAN AUDITOR GENERAL'S REPORT

Information Systems Audit Report 2022 – Local Government Entities

Report 22: 2021-22
June 2022

This page is intentionally left blank

(Appendix AAR: 8.1E)

THE PRESIDENT
LEGISLATIVE COUNCIL

THE SPEAKER
LEGISLATIVE ASSEMBLY

INFORMATION SYSTEM AUDIT REPORT 2022 – LOCAL GOVERNMENT ENTITIES

This report has been prepared for submission to Parliament under the provisions of section 24 of the *Auditor General Act 2006*.

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

This is the third local government annual information systems audit report by my Office. The report summarises the results of our 2021 annual cycle of information systems audits across a selection of 45 local government entities.

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

CAROLINE SPENCER
AUDITOR GENERAL
28 June 2022

Contents

Auditor General's overview

This report summarises important findings and recommendations from our 2020-21 annual cycle of information systems audits at 45 local government entities (entities).

Entities rely on information systems to operate and deliver services to their communities. In doing so, they collect and store vast amounts of information about their residents and operations. As information and cyber security threats continue to evolve, it is increasingly important that entities implement appropriate controls to protect their valuable information and systems. My November 2021 audit report[1] on cyber security highlighted the need for entities to improve their management of cyber security risks and this year's general computer controls (GCC) audits at entities show that information security remains a significant area of concern.

Like last year, none of the 12 entities where we performed capability maturity assessments met our benchmark for information security and none of the entities met our expectations across all 6 control categories. While we saw some improvements in the management of IT risks, physical security and IT operations, change control showed the most progress.

Included in this report are case studies which highlight how weak controls can potentially compromise entities and result in system breaches, loss of sensitive and confidential information and financial loss. Entities need to continuously review and improve their practices to establish robust safeguards and enhance their resilience against cyber threats. Complex networks and systems require smaller entities to also dedicate resources to manage their information and cyber security.

Entities should use the recommendations in this report to address weaknesses in their information systems controls and improve their capability maturity. Given the nature of findings this year, I have chosen again not to identify the audited entities.

[1] Auditor General for Western Australia, *Cyber Security in Local Government*, Report 9: 2021-22, November 2021.

Introduction

Local government entities (entities) rely on information systems to prepare their financial statements and to deliver a wide range of services to their communities. Our general computer controls (GCC) audits assess if entities have effective system controls in place to support the confidentiality, integrity and availability of their IT systems and financial reporting. These audits are performed as an integral part of, and inform, our financial audit program.

This report summarises the GCC audit findings reported to 45 entities for 2020-21. For 12 of these entities, generally medium to large, we also performed capability maturity assessments. A GCC audit with a capability maturity assessment is the most comprehensive information systems audit we undertake. We use these findings to inform our financial audit risk assessment and work program for the sector.

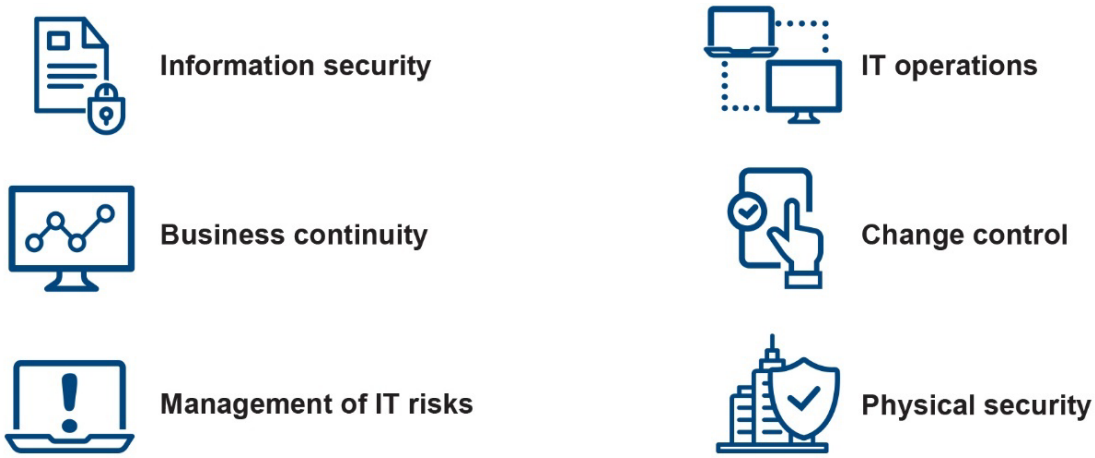
For our capability maturity assessments, we asked the 12 entities to self-assess against the provided capability maturity model. We then compared their results to ours (which were based on the results of our GCC audits). These assessments are a way to see how well-developed and capable entities' established IT controls are.

For the remaining 33 entities, our contract audit firms or our financial audit teams examined the GCCs but did not undertake capability maturity assessments. Information system findings identified during these audits are included in this report.

The methodology we have developed for our GCC audits is based on accepted industry good practice. Our assessment is also influenced by various factors including:

- business objectives of the entity
- level of dependence on IT
- technological sophistication of computer systems
- value of information managed by the entity.

We focused on the following 6 categories (Figure 1) for both our GCCs and capability maturity assessments.



Source: OAG

Figure 1: GCC categories

Throughout the report we have included case studies that illustrate the significant impact poor controls can have on entities.

Conclusion

We reported 358 control weaknesses to 45 entities this year, compared to 328 weaknesses at 50 entities last year. Ten percent (37) of this year's weaknesses were rated as significant and 71% (254) as moderate. These weaknesses represent a considerable risk to the confidentiality, integrity and availability of entities' information systems and need prompt resolution.

Fifty-six percent (202) of the findings were unresolved issues from last year. Entities need to address these weaknesses to reduce the risk of their systems and information being compromised.

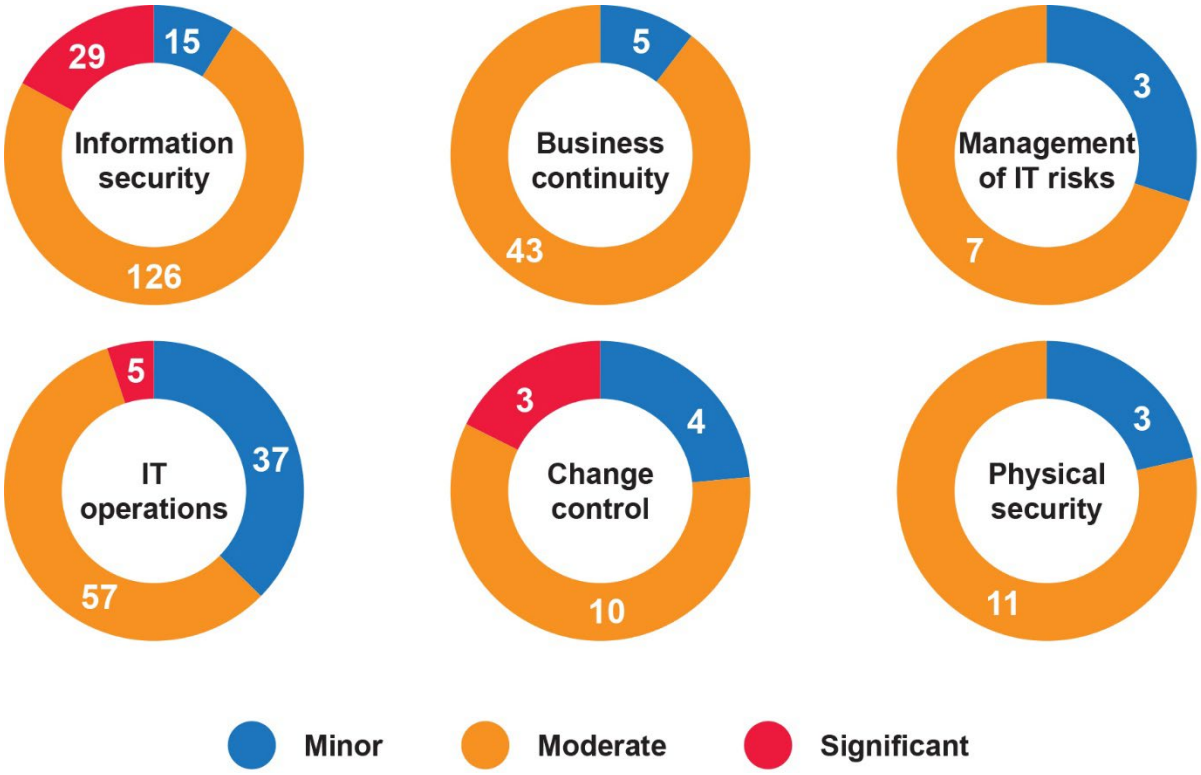
None of the 12 entities that had capability maturity assessments met our expectations across all 6 control categories, a similar finding to last year. Information security remains a significant risk again this year and needs urgent attention. Compared to 2019-20, there have been some improvements in change control, management of IT risks, physical security and IT operations. However, entities need to improve in all 6 control categories.

What we found: General computer controls

In 2020-21, we reported 358 findings to the 45 entities we audited. We reported the weaknesses we found to each entity in a management letter. As management letters are often made public, we removed any sensitive technical details which could increase an entity's risk of cyber attacks. To assist entities to address weaknesses we reported these sensitive details to them in separate confidential letters. Entities generally agreed to implement our recommendations.

Figure 2 summarises the distribution and significance of our findings across the 6 control categories.

Like last year, we rated most of our findings as moderate. Entities that fail to address these moderate risks can, over time, become more exposed to vulnerabilities. We have included in this report specific case studies to highlight how weak controls can potentially compromise entities' systems.



Source: OAG

Figure 2: Distribution and significance of GCC findings in each control category

What we found: Capability assessments

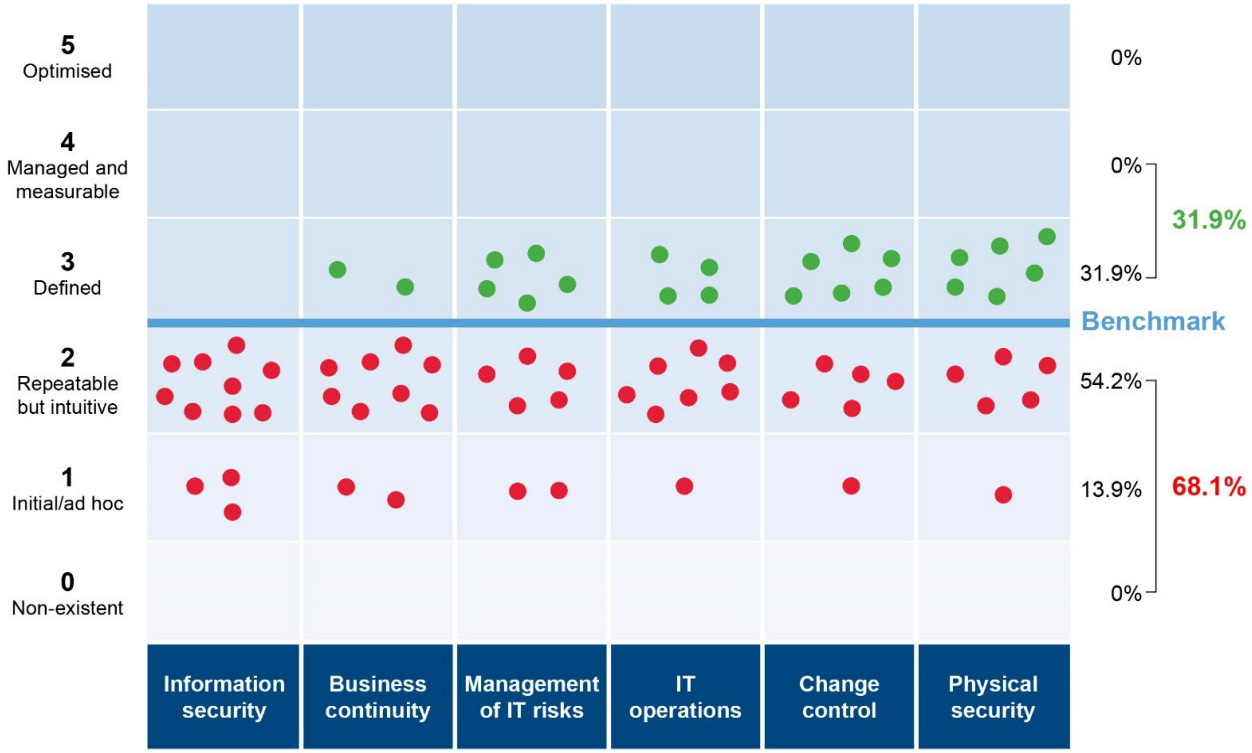
We conducted in-depth capability maturity assessments at 12 entities. We used a 0 to 5 rating scale[2] (Figure 3) to evaluate each entity's capability maturity in each of the 6 GCC categories. Our model allows us to compare entity results from year to year. We expect entities to achieve a level 3 (Defined) rating or better across all 6 categories.

Source: OAG

Figure 3: Rating scale and criteria

Figure 4 shows the results of our capability assessments across all 6 control categories for the 12 entities we assessed in 2020-21.

[2] The information within this maturity model assessment is derived from the criteria defined within COBIT 4.1, released in 2007 by ISACA.



Source: OAG

Figure 4: 2020-21 capability maturity model assessment results

The percentage of entities rated level 3 or above for individual categories was as follows:

Category	2020-21 %		2019-20 %
Information security	0	–	0
Business continuity	17	↓	18
Management of IT risks	42	↑	27
IT operations	33	↑	18
Change control	50	↑	18
Physical security	50	↑	45

Source: OAG

Table 1: Percentage of entities rated level 3 or above

None of the 12 entities met our expected benchmark (level 3 Defined) across all control categories.

There were some improvements in the management of IT risks, IT operations, change control and physical security, however, most entities still fell below our benchmark. Information security remains a significant concern, with all entities below our benchmark and not able to demonstrate adequate controls. A lack of robust controls can expose entities and impact critical services provided to the public.

Information security

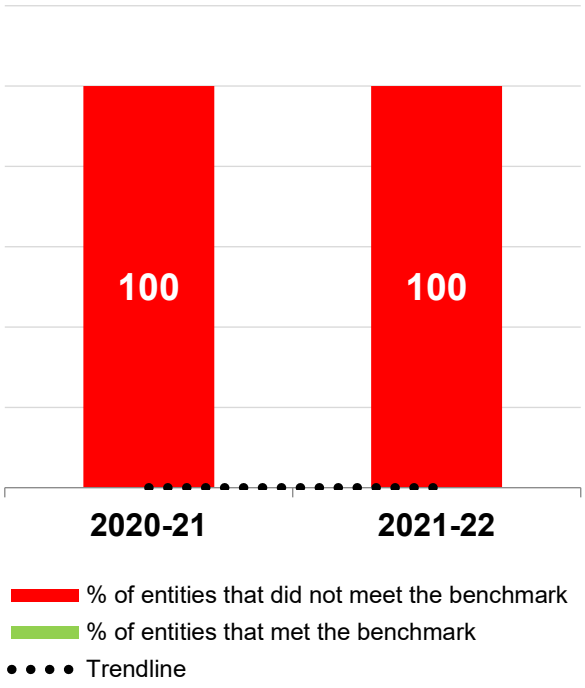
Cyber intrusions are becoming more sophisticated and frequent. Transitioning to digital services to achieve efficiencies increases the risk profile of many entities. Protection of sensitive and critical information that entities hold within their financial and operational systems should be managed with the highest priority using better practice information security controls to mitigate risks.

Our GCC audits and capability maturity assessments assess against better practice controls for information and cyber security. Figure 5 lists some of these controls.

Source: OAG

Figure 5: Information security – Better practice controls

None of the 12 entities met our benchmark for information security either because they did not have documented policies, processes and controls or they were not effective (Figure 6). Entities have a responsibility to implement adequate and robust controls to protect key systems and information.



Source: OAG

Figure 6: Information security – percentage of entities that met/did not meet our benchmark

Common weaknesses we found included:

- **Inadequate information and cyber security policies** – policies did not sufficiently cover key areas of information and cyber security or were out of date.
- **Multifactor authentication not used** – a number of systems did not have multifactor authentication to strengthen access.
- **Administrator privileges not managed well** – administrators did not have separate unprivileged accounts for normal day to day tasks. Limiting privileges and separating administrative accounts are important mitigations against network and system compromise.
- **Vulnerability management is not effective** – entities did not have appropriate processes to identify and address vulnerabilities, which increases the risk of compromise.
- **Network segregation not appropriate** – networks were not segregated to limit and contain the impact of a compromise. Partitioning the network into smaller zones and limiting the communication between these zones is an important control.
- **Unauthorised device connectivity** – there are a lack of controls to detect or prevent unauthorised devices from connecting to entity internal networks. These devices can serve as an attack point and spread malware or listen in on network traffic.
- **Emails not protected** – entities did not have controls to ensure the integrity and authenticity of emails to reduce the likelihood of successful phishing attacks. Controls such as domain-based message authentication reporting and conformance (DMARC), sender policy framework (SPF) and domain keys identified mail (DKIM) were not implemented to prevent email impersonation.

- **Lack of data loss prevention controls** – no processes to detect or block unauthorised transfers of sensitive data outside of the entities.

The importance and potential impact of common information and cyber security weaknesses are illustrated in the following case studies.

Case study 1: No policy to manage information and cyber security

Information security policy

One entity did not have a policy to manage cyber and information security. This means, systems or services may not meet security expectations of senior management and the entity may fail to achieve its objectives.

Adequate and clear policies are needed to ensure the security of information systems.

Case study 2: Weak password results in a network compromise

Password

One entity experienced a security breach when a cybercriminal was able to guess a weak password on an account used to access a public facing server through remote desktop protocol (RDP). A lack of network segregation allowed the attacker to access other parts of the network, gain privileged access to the domain controller and maliciously encrypt servers and information.

The use of strong password/passphrases, network segregation and multi-factor authentication reduce the risk of compromise.

Case study 3: No controls to mitigate malware infections

Malware protection

One entity had anti-malware protection installed on some servers but not others. It did not have application whitelisting and blocking in place or only allow trusted macros. These controls prevent delivery and execution of malicious programs.

Without appropriate controls to protect systems against malware, there is an increased risk of compromise to the confidentiality, integrity and availability of entity information or data.

Case study 4: Default domain administrator account is not controlled

Limit admin privilege

One entity shared the highly privileged default domain administrator account with individuals in different business units and had not changed the account password since 2005. The account was also heavily used for day to day operations and services, instead of using separate dedicated service accounts.

Inappropriate management of the account increases the risk that the entity will not be able to hold individuals to account for unauthorised modifications to its systems and information.

Case study 5: Poor management of technical vulnerabilities

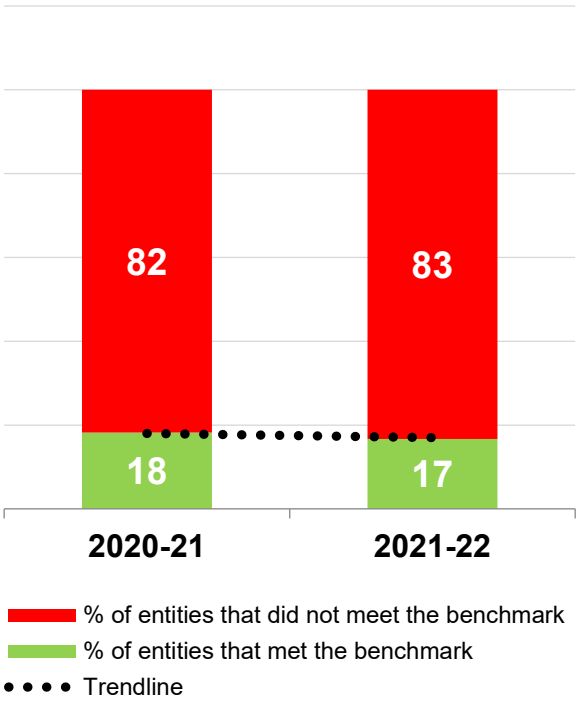
Vulnerability management

An audited entity did not have a process to manage technical vulnerabilities and system currency. It had not tested the adequacy of its external network controls to detect and prevent cyber attacks. Its process to apply software patches was also not operating well as we identified critical and high severity vulnerabilities dating back to 2013 that had not been patched.

Without effective procedures and processes to manage technical vulnerabilities in a timely manner, entities leave their IT systems exposed to malicious attackers. This could result in unauthorised access and system compromise.

Business continuity

There was no material change from last year with only 2 of the 12 entities (17%) meeting our benchmark in this category (Figure 7). Business continuity and disaster recovery plans help entities to promptly restore key business functions and processes during or after an unplanned disruption. Without these plans, entities could suffer extended outages and disruption to the delivery of important services to their communities.



Source: OAG

Figure 7: Business continuity – percentage of entities that met/did not meet our benchmark

Common weaknesses we found included:

- **Lack of business continuity and disaster recovery plans** – entities did not have appropriate business continuity and disaster recovery plans, or they were out-of-date.
- **Disaster recovery plans not tested** – without appropriate testing of disaster recovery plans, entities cannot be certain the plan will work when needed.

Documented up-to-date business continuity and disaster recovery plans help entities to promptly recover critical information systems in the event of an unplanned disruption to their operations and services. The plans should identify critical business functions and IT systems along with their recovery time objectives.

The effectiveness of these plans should be periodically tested to identify improvements where required. Tests can also be used to check that key staff are familiar with the plans and their specific roles and responsibilities in a disaster situation.

The following case study illustrates common weaknesses in recovery procedures.

Case study 6: Configuration backups are not performed

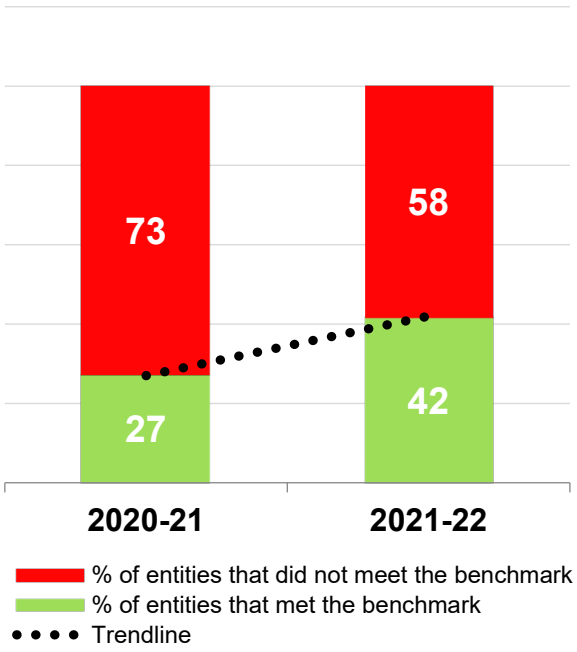
Configuration backups

An audited entity did not backup the configuration of its firewall which protects its network from cyber attacks. In the event of an emergency, the entity may not be able to recover its firewall in a timely manner, which will impact delivery of services and security of its network.

Management of IT risks

Forty-two percent of entities met our benchmark for this category in 2020-21, compared to 27% last year (Figure 8).

Entities should be aware of information and cyber security risks associated with IT including operational, strategic and project risks. All entities should have risk management policies and processes to assess, prioritise, address and monitor the risks that affect key business objectives.



Source: OAG

Figure 8: Management of IT risks – percentage of entities that met/did not meet our benchmark

Common weaknesses we found included:

- **Out-of-date policies and processes to identify, assess and treat IT risks** – without appropriate policies and processes entities cannot effectively manage their IT risks.
- **Inadequate risk registers** – risk registers did not record controls and treatment action plans and risk ratings were not appropriately assessed.

Without IT risk management policies and practices to identify, mitigate and manage threats within reasonable timeframes, entities may not meet their business objectives to deliver key services to their communities.

The following case study illustrates that entities need processes to identify their risks.

Case study 7: Entity is not aware of its information and cyber risks

Information and cyber security risk management

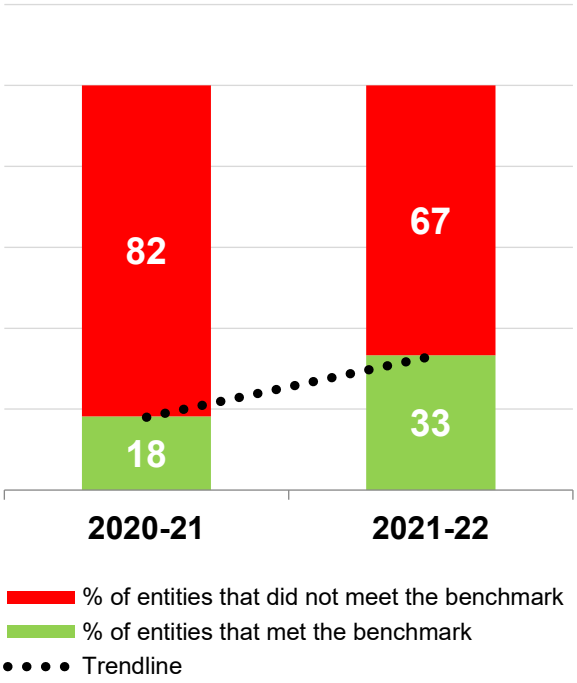
An audited entity maintained other corporate and financial risks, but it did not have a process to identify and address its cyber security risks.

The entity is at an increased risk of information and cyber security breaches.

IT operations

Entities improved in this category with 33% meeting our benchmark in 2020-21 (Figure 9). However, we identified similar weaknesses to those highlighted in last year's report.

IT operations maintain and support the delivery of entity services. Clearly defined and effectively managed IT operations support IT infrastructure that can withstand and recover from errors and failures.



Source: OAG

Figure 9: IT operations – percentage of entities that met/did not meet our benchmark

Common weaknesses we found included:

- **Processes are not defined** – a lack of or out of date procedures to support day to day operations, such as incident and problem management.
- **Inadequate monitoring of events** – entities did not have policies and procedures to monitor event logs. System logs provide an opportunity to detect suspicious or malicious behaviour in key business applications.
- **Supplier performance not monitored** – supplier performance was not reviewed to identify and manage instances of non-compliance with agreed service levels.
- **Background checks for new starters were not performed** – staff in privileged IT positions did not go through background checks (e.g. police clearance).
- **Access was not reviewed** – regular checks were not done to validate users had the level of access to systems applicable to their role or function, and revoke user access upon termination.

The following case study illustrates a common weakness in IT operations.

Case study 8: Contractor access was not revoked in a timely manner

User account management

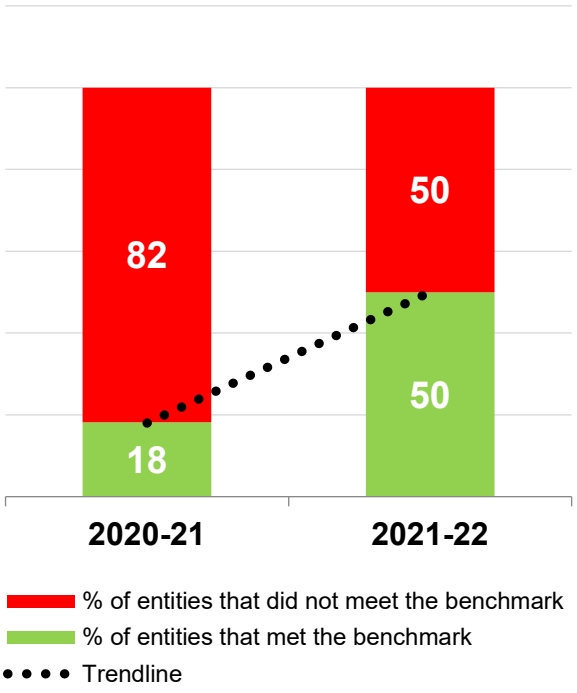
One entity did not have a central record of contract staff and therefore could not easily assess if their network access was appropriate. We sampled 13 active accounts and found that 8 belonged to terminated contract staff who no longer worked with the entity.

Poor processes to manage contract staff increases the risk of unauthorised access to the entity's IT systems and information.

Change control

Fifty percent of entities met our benchmark in 2020-21 (Figure 10), the largest improvement across the 6 control categories. This is 1 of the 2 categories where at least half of the entities met the benchmark and it is pleasing to see significant year on year improvement.

We reviewed entities' approaches to managing IT changes to minimise the risks and impacts to stakeholders. We covered change authorisation, testing, implementation and outcomes. An overarching change control framework ensures changes are made consistently and reliably.



Source: OAG

Figure 10: Change control – percentage of entities that met/did not meet our benchmark

Common weaknesses we found included:

- **Change processes not followed** – changes to critical systems did not follow change procedures. If formal procedures are not followed, there is a risk changes may be applied inconsistently resulting in unplanned system downtime and interruption to critical services.

- **Change management processes not documented** – without documented processes, changes made to IT infrastructure can adversely affect entities' operations leading to unplanned or excessive system downtime.
- **Changes were not assessed prior to implementation** – allowing significant changes without appropriate scrutiny or approval increases the risk of system outages.

Without appropriate change control, entities risk compromising the integrity of their systems and information. This can lead to excessive outages and downtime to key systems and impact their delivery of services.

The following case study illustrates the risks when IT changes are not controlled and monitored.

Case study 9: Poor change management practices could result in financial system instability

Change management

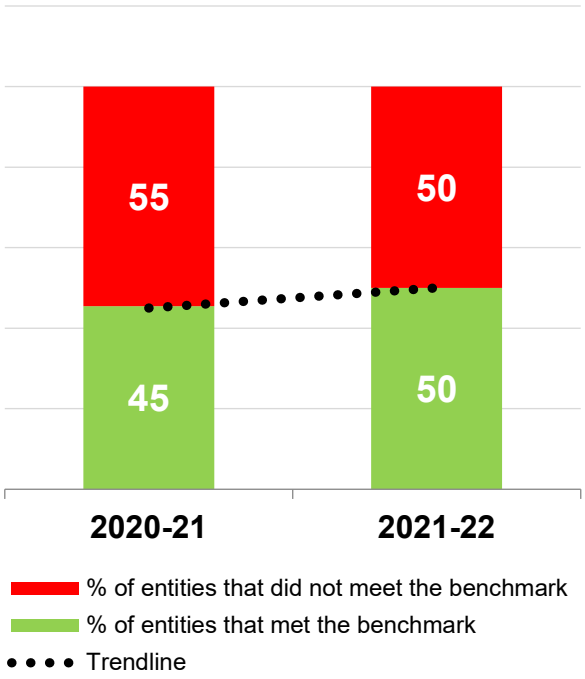
One entity made changes to its financial system without testing the impact on system integrity and availability in an independent test environment. Uncontrolled changes can have significant unintended consequences to systems and the delivery of key services.

These changes were also not recorded, contrary to the entity's change management policy. Failure to record changes increases the effort required to respond, recover and restore business as usual operations.

Physical security

There was a small improvement in physical security with half the entities meeting our benchmark this year (Figure 11).

IT systems are housed in purpose-built server rooms, which must have restricted access and adequate cooling and power. We reviewed if IT systems were protected against potential environmental hazards and tested access restrictions to ensure only authorised individuals could access the server rooms.



Source: OAG

Figure 11: Physical security – percentage of entities that met/did not meet our benchmark

Common weaknesses we found included:

- **Combustible and non-essential items were stored in server rooms** – the risk of outages is higher if server rooms are not appropriately maintained.
- **Unnecessary access to server rooms** – staff and contractors were assigned access to server rooms that they did not require and visitor access to server rooms was not logged. Lack of controlled access increases the risk of system outages and compromise from unauthorised access.
- **Fire suppression systems were not installed** – without appropriate fire suppression systems, IT infrastructure is likely to be damaged in the event of a fire.

The following case study illustrates the risk of server room outages if not protected against physical and environmental hazards.

Case study 10: Poor management of server rooms

Physical security

One entity stored combustible materials such as furniture and cardboard boxes in their server room. In addition, an excessive number (114) of people had access to the server room and a visitor log was not maintained.

There is an increased risk of accidental or deliberate damage and unauthorised access to systems.

Recommendations

1. Information security

a. Senior executives should implement appropriate policies and procedures to ensure the security of information systems and support their entity business objectives.

b. Management should ensure good security policies and practices are implemented and continuously monitored for control areas identified in Figure 5, including:

i) patching and vulnerability management

ii) application hardening and control

iii) implement technical controls to prevent impersonation and detect/prevent phishing emails

iv) strong passphrases/passwords and multi-factor authentication

v) limit and control administrator privileges

vi) segregate network and prevent unauthorised devices

vii) secure cloud infrastructure, databases, email and storage, and know clearly 'who' they are handing entity and citizen data to through their use of cloud services

viii) cyber security monitoring, intrusion detection and protection from malware.

2. Business continuity

Entities should have appropriate business continuity, disaster recovery and incident response plans to protect critical systems from disruptive events. These plans should be periodically tested.

3. Management of IT risks

Entities should:

a. understand their information assets and apply controls based on their value

b. ensure IT risks are identified, assessed and treated within appropriate timeframes. Senior executives should have oversight of information and cyber security risks.

4. IT operations

Entities should implement policies and procedures to guide key areas of IT operations such as incident management and supplier performance monitoring.

5. Change control

Approved change control processes should be consistently applied when making changes to IT systems. All changes should go through planning and impact assessment to minimise the occurrence of problems. Change control documentation should be current and approved changes formally tracked.

6. Physical security

Entities should develop and implement physical and environmental control mechanisms to prevent unauthorised access, or accidental or environmental damage to IT infrastructure and systems.

Under section 7.12A of the *Local Government Act 1995*, the 45 audited entities are required to prepare an action plan to address significant matters relevant to their entity for submission to the Minister for Local Government within 3 months of this report being tabled in Parliament, and for publication on the entity's website. This action plan should address the points above, to the extent that they are relevant to their entity.

This page is intentionally left blank

This page is intentionally left blank

Auditor General's 2021-22 reports

Number	Title	Date tabled
21	Delivering School Psychology Services	23 June 2022
20	Fraud Risk Management - Better Practice Guide	22 June 2022
19	Forensic Audit – Construction Training Fund	22 June 2022
18	Opinion on Ministerial Notification – FPC Sawmill Volumes	20 June 2022
17	2022 Transparency Report Major Projects	17 June 2022
16	Staff Rostering in Corrective Services	18 May 2022
15	COVID-19 Contact Tracing System – Application Audit	18 May 2022
14	Audit Results Report – Annual 2020-21 Financial Audits of State Government Entities Part 2: COVID-19 Impact	9 May 2022
13	Information Systems Audit Report 2022 – State Government Entities	31 March 2022
12	Viable Cycling in the Perth Area	9 December 2021
11	Forensic Audit Report – Establishment Phase	8 December 2021
10	Audit Results Report – Annual 2020-21 Financial Audits of State Government Entities	24 November 2021
9	Cyber Security in Local Government	24 November 2021
8	WA's COVID-19 Vaccine Roll-out	18 November 2021
7	Water Corporation: Management of Water Pipes – Follow-Up	17 November 2021
6	Roll-out of State COVID-19 Stimulus Initiatives: July 2020 – March 2021	20 October 2021
5	Local Government COVID-19 Financial Hardship Support	15 October 2021
4	Public Building Maintenance	24 August 2021
3	Staff Exit Controls	5 August 2021
2	SafeWA – Application Audit	2 August 2021
1	Opinion on Ministerial Notification – FPC Arbitration Outcome	29 July 2021

(Appendix AAR: 8.1E)

Office of the Auditor General
Serving the Public Interest

Office of the Auditor General
Western Australia

7th Floor Albert Facey House
469 Wellington Street, Perth

Perth BC, PO Box 8489
PERTH WA 6849

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

@OAG_WA

Office of the Auditor General for
Western Australia