E. Status of recommendations made in prior reports

The following tables provide the current status of the issues raised in our prior reports.

Figure E1
Status of recommendations from *State entities 2023* (Report 11: 2023–24)

Manage the cyber security risks associated with services provided by third parties. (All entities)		**Further action needs to be taken**
REC 1	We recommend that all entities implement a process to manage the security risks relating to third-party services for information systems and technologies, and introduce procedures that will: • identify how they use third-party services, the extent to which they use them, and the associated security risks • establish due diligence (vetting and continuous monitoring) processes when engaging new third parties or continuing with third-party services • define security standards and the appropriate contractual agreements to manage security risks • establish a process to continually assess how well each third party manages its security risks and responds to and recovers from security incidents.	This year we identified 28 new deficiencies within state entities regarding how they manage cyber security risks associated with services provided by third parties. This is in addition to the 7 deficiencies from prior years that are still being actioned as of 30 June 2024. We recommend entities continue to monitor how they manage these risks. We are also planning a performance audit in 2025–26 to assess in more detail how effectively public sector entities manage third-party cyber security risks.
Implement robust policies and procedures to ensure special payments are appropriate, defensible, and transparent. (All entities)		**Further action needs to be taken**
REC 2	We recommend that all entities implement robust policies and procedures that specify when a special payment is appropriate and how it should be made. Guidance should outline who is authorised to approve special payments and what constitutes appropriate documentation to support: • the reason and nature of the payment • the approving officer • the amount, including supporting calculations.	This year, total special payments across the state sector increased by 5.9 per cent to $84.279 million. We also reported 14 new deficiencies (8 of which were significant and required immediate action). In line with these findings, we continue to recommend that entities strengthen their policies and procedures related to making special payments.
Improve awareness and understanding of guidance material available for special payments, including ex-gratia payments. (Queensland Treasury)		**Further action needs to be taken**
REC 3	We recommend that Queensland Treasury improves the awareness and understanding that all state entities have of guidance material available for special payments, including ex-gratia payments. This should include: • expectations for internal governance • required documentation, including supporting calculations, to support special payments • reporting requirements.	We continue to recommend that Queensland Treasury improves awareness and develops guidance material for special payments.

Source: Queensland Audit Office.

Figure E2
Status of recommendations from *State entities 2022* (Report 11: 2022–23)

Audit committees to actively monitor the implementation of audit recommendations (including internal audit recommendations) and encourage the timely resolution of outstanding internal control weaknesses. (Audit committees of all entities)		**Further action needs to be taken**
REC 1	We recommend that audit committees of public sector entities actively monitor the implementation of audit recommendations and encourage the timely resolution of outstanding internal control weaknesses. This should ensure the agreed recommendations address the underlying cause of the issue and issues are resolved in accordance with agreed timelines. Audit committees play an integral role in ensuring effective internal controls, including holding management to account so that identified weaknesses are resolved appropriately and in a timely manner.	We continue to see issues that remain outstanding beyond agreed timelines. We also note that for 2 core departments, we continue to raise deficiencies over audit committee governance in 2023–24. Of the issues we raised with core departments in 2021–22, 11 per cent have not been resolved this year, and some issues are still outstanding from 2018–19.

Source: Queensland Audit Office.

Figure E3
Status of recommendations from *State entities 2021* (Report 14: 2021–22)

Advise on machinery of government changes, set performance measures, and monitor costs. (Central agencies)		**Appropriate action has been taken**
REC 1	We recommend the Department of the Premier and Cabinet and Queensland Treasury take the following actions for future government restructures: • Provide advice to the incoming or returning government on potential impacts of restructures, including the key risks to be managed and estimated costs to implement, drawing on lessons learnt from past machinery of government changes. • Require departments to articulate, measure, and report on the benefits to be achieved from the machinery of government change and the cost to implement the restructure. This should include guidance on how to measure and report benefits and costs.	The Public Service Commission published the *Machinery of Government handbook* in October 2024. The handbook provides information and guidance to agencies about: • how machinery of government (MoG) changes are effected • time frames • governance • people management • financial management • corporate services • shared service arrangements • records management. Agencies are expected to implement MoG changes in accordance with the handbook.

Improve timeliness of financial statements being made publicly available. (Departments and relevant ministers)		**Partially implemented**
REC 2	Departments and their ministers should explore opportunities for releasing the audited financial statements of public sector entities in a more timely way. This could involve departments progressively providing annual reports to the minister, instead of waiting to provide all annual reports in the portfolio at the same time. Queensland Treasury should consider legislative change to specify the maximum number of days between financial statement certification and tabling. This is the case for Queensland local governments, which must table their annual reports in council within one month of certifying their financial statements. Alternatively, the annual reports for abolished state government entities must be tabled within 14 days of being provided to the minister.	In its response to this recommendation, Queensland Treasury undertook to encourage tabling at the earliest opportunity but did not accept the recommendation to consider legislative change. We observed improvement in the timeliness of annual report tabling. Entities tabled their annual reports (including financial information), on average, one week earlier than last year.
Ensure consistent payroll processes are implemented. (All entities)		**Further action needs to be taken**
REC 5	In addition to our recommendation from 2020–21 to promptly review payroll reports, we also recommend entities: • provide staff with internal policies and manuals that outline payroll processes • ensure staff consistently comply with these, particularly for processes such as employee terminations and approval of employee overtime.	We continue to identify departments that have not reviewed payroll reports in a timely manner or at all and have inconsistencies in the completion of payroll processes. In 2023–24, we identified the following deficiencies in payroll processes at state entities: • core departments – 9 new deficiencies • other state entities – 20 new deficiencies (2 significant).
Review procurement policies and manuals. (All entities)		**Further action needs to be taken**
REC 7	Entities should review their procurement policies and manuals to ensure they give clear guidance for staff to follow when making procurement decisions. The policies and manuals should also specify what documentation staff should maintain to record the process and decisions.	We continue to identify deficiencies relating to procurement and contract management processes at: • core departments – 7 new deficiencies (one significant) • other state entities – 22 new deficiencies (6 significant). Entities need to take further action to enhance their procurement practices.

Source: Queensland Audit Office.

Figure E4
Status of recommendations from *State entities 2020* (Report 13: 2020–21)

Use recent financial statement preparation experiences, including responses to the COVID-19 pandemic, to identify improvements and plan for the year ahead. (All entities)		**Appropriate action has been taken**
REC 1	We recommend all entities use their recent financial statement preparation experiences to update their initial self-assessment against the maturity model – available on our website at: www.qao.qld.gov.au/reports-resources/better-practice/financial-statement-preparation-maturity-model-self-assessment. This should include reflection on the process changes made in response to the COVID-19 pandemic, and planning early for the 2020–21 financial statements, given the uncertainty about what challenges the year ahead might bring. Where areas for improvement are identified, each entity should establish an implementation plan, with oversight by its audit committee. Where a machinery of government change has resulted in functions moving between departments, departments should conduct a review to align their financial statement preparation processes within the new department and reassess the maturity of those processes.	The majority of departments revisited their financial statement maturity self-assessments in 2023–24. We recommend that this practice continue. Departments should consider whether their assessments remain current and put action plans in place to address areas requiring improvement.

Strengthen the security of information systems. (All entities)		Further action needs to be taken
REC 3	We recommend all entities strengthen the security of their information systems. They rely heavily on technology, and increasingly, they must be prepared for cyber attacks. Any unauthorised access could result in fraud or error, and significant reputational damage. Their workplace culture, through their people and processes, must emphasise strong security practices to provide a foundation for the security of information systems. Entities should: • provide security training for employees so they understand the importance of maintaining strong information systems, and their roles in keeping them secure • assign employees only the minimum access required to perform their job, and ensure important stages of each process are not performed by the same person • regularly review user access to ensure it remains appropriate • monitor activities performed by employees with privileged access (allowing them to access sensitive data and create and configure within the system) to ensure they are appropriately approved • implement strong password practices and multifactor authentication (for example, a username and password, plus a code sent to a mobile), particularly for systems that record sensitive information • encrypt sensitive information to protect it • patch vulnerabilities in systems in a timely manner, as upgrades and solutions are made available by software providers to address known security weaknesses that could be exploited by external parties. Entities should also self-assess against all of the recommendations in *Managing cyber security risks* (Report 3: 2019–20) to ensure their systems are appropriately secured.	While entities successfully resolved the issues we report to them, we continue to identify new control weaknesses with the security of their information systems. Entities need to be vigilant to maintain effective internal controls and protect systems from attack. We encourage all entities to regularly self-assess the strengths of their information systems against the recommendations we made to all entities in: • *Managing cyber security risks* (Report 3: 2019–20) • *Responding to and recovering from cyber attacks* (Report 12: 2023–24). We have also included in Appendix L a list of questions audit and risk committees can consider in assessing the effectiveness of entities' controls in relation to the security of information systems.
Verify changes to supplier and employee information to prevent fraud. (All entities)		**Further action needs to be taken**
REC 4	We recommend all entities ensure requests to change employee and supplier bank account details are verified using independently sourced information and reviewed by a person who is not involved in processing the change.	We continued to identify deficiencies relating to bank account detail processes at: • core departments – one new significant deficiency • other state entities – 5 new deficiencies. Entities need to take further action to enhance their bank detail amendment practices.

Promptly review employee payments. (All entities)		Further action needs to be taken
REC 5	All entities need to ensure managers have ready access to payroll reports that are easy to use and contain all required information; understand the importance of reviewing these reports in a timely manner each fortnight; and have a consistent and efficient process for documenting their review.	We continued to identify deficiencies relating to payroll processes at: • core departments – pay run processes – 15 new deficiencies (one significant) – over/underpayments – 4 deficiencies (2 significant) • other state entities – pay run processes – 21 new deficiencies (2 significant) – over/underpayments – 4 deficiencies (2 significant). Entities need to take further action to enhance their payment amendment practices.
Automate financial approvals and monitoring of internal controls. (All entities)		**Appropriate action has been taken**
REC 6	All entities need to ensure their systems and processes (internal controls) are set up so financial approval occurs correctly in the financial system. They also need to invest in tools that will promptly detect breakdowns in internal controls.	No new systemic issues have been identified across the sector that indicate an ongoing underlying risk to the sector that requires reporting to parliament. Only one other state entity had a deficiency relating to effective financial delegations required for approval.

Source: Queensland Audit Office.

Recommendation status definitions

Where a recommendation is specific to an entity, we have reported on the action that the entity has taken and whether the issue is considered to be *fully implemented*, *partially implemented, not implemented*, or *no longer applicable*.

Status		Definition
Fully implemented		Recommendation has been implemented, or alternative action has been taken that addresses the underlying issues and no further action is required. Any further actions are business as usual.
Partially implemented		Significant progress has been made in implementing the recommendation or taking alternative action, but further work is required before it can be considered business as usual. This also includes where the action taken was less extensive than recommended, as it only addressed some of the underlying issues that led to the recommendation.
Not implemented	**Recommendation accepted**	No or minimal actions have been taken to implement the recommendation, or the action taken does not address the underlying issues that led to the recommendation.
	Recommendation not accepted	The entity (or entities) did not accept the recommendation.
No longer applicable		Circumstances have fundamentally changed, making the recommendation no longer applicable. For example, a change in government policy or program has meant the recommendation is no longer relevant.

Where a general recommendation has been made for all entities to consider, we have assessed action on issues reported to specific entities in the prior year, as well as any further issues identified in the current year. On this basis, we have concluded whether *appropriate action has been taken* across the sector, or if *further action needs to be taken* to address the risk identified.

Status	Definition
Appropriate action has been taken	Recommendations made to individual entities have been implemented, or alternative action has been taken that addresses the underlying issues, and no further action is required. No new issues have been identified across the sector that indicate an ongoing underlying risk to the sector that requires reporting to parliament.
Further action needs to be taken	Recommendations made to individual entities have not been fully implemented, and/or new recommendations have been made to individual entities, indicating further action is required by entities in the sector to address the underlying risk.