C. Status of recommendations made in *State entities 2020* (Report 13: 2020–21)

In our report, *State entities 2020* (Report 13: 2020–21), we identified the following recommendations for Queensland state public sector entities. Entities need to take further action to resolve all of these recommendations.

Use recent financial statement preparation experiences, including responses to the COVID-19 pandemic, to identify improvements and plan for the year ahead (all entities)		**Further action needs to be 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. 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.	While some entities reassessed their processes, some that were impacted by machinery of government changes decided to undertake the assessment once employee and system changes had been finalised in 2021–22.
Improve timeliness of financial statements being made publicly available (relevant ministers and central agencies)		**Further action needs to be taken**
REC 2	We continue to encourage relevant ministers and central agencies to explore opportunities for releasing the audited financial statements of public sector entities in a more timely way. This could be by specifying the maximum number of days between financial statement certification and tabling (as has been done for Queensland local governments, with one month to table their annual report in council), or by allowing entities to publish financial statements on their websites prior to the tabling of their annual reports in parliament.	No change has been made to the requirements for publishing financial statements. The timeliness of publishing annual reports with audited financial statements has deteriorated over the last 2 years.

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 have mostly resolved the specific issues we reported to them, ongoing changes in people and systems means new control weaknesses continue to be identified. Entities need to be vigilant to maintain effective internal controls and protect systems from attack.
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 continue to identify significant control deficiencies in some entities that have not used independently sourced information to verify changes to supplier bank account details. We recommend all entities continue verifying changes to supplier bank account details using independently sourced information, including when responsibility for the check is shared between the entity and a shared service provider. A clear understanding of the role and responsibilities between the entity and the shared service provider should be documented and communicated to all employees.

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 continue to identify entities that have not reviewed payroll reports (at all or in a timely manner), particularly reports identifying exceptions and overtime anomalies.
Automate financial approvals and monitoring of internal controls (all entities)		**Further action needs to be 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.	Entities with specific issues last year have enhanced the financial approval process, including using exception reports to identify transactions that are approved by an individual above their delegation limit. However, we continue to identify some entities where grant expenditure has been approved above financial delegation limits. We recommend entities ensure staff understand the assigned financial delegations and that sufficient monitoring controls are in place to prevent grants being approved by staff who do not hold delegations with high enough financial limits.
Ongoing compliance with financial accountability requirements following a machinery of government change (departments)		**Further action needs to be taken**
REC 7	When a machinery of government change occurs and functions move between departments, departments should promptly conduct a review to ensure consistency of fundamental processes (such as approvals) and compliance with the *Financial Accountability Act 2009* and the *Financial Accountability Handbook*.	Departments have resolved most immediate impacts of the machinery of government changes announced in November 2020. The review of fundamental processes has been identified by most as an activity that will be performed in 2022.

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.