C. Status of prior recommendations

Our report, *Transport 2020* (Report 10: 2020–21), identified the following recommendations for transport sector entities. Although some corrective actions have addressed parts of the recommendations, further action needs to be taken for all three recommendations.

Figure C1
Status of recommendations from prior year's report

Improve procurement processes (all entities)		Further action needs to be taken*
REC 1	All entities should: • assess their compliance with conflict of interest processes • ensure supplier information and payments are appropriately authorised and independently reviewed.	The entity with the significant deficiency has updated procurement checklists to ensure the conflicts of interest declarations are completed prior to being appointed as a panel member. However, we continue to identify other control deficiencies relating to officers not completing independence declarations before participating on tender panels. Further action is needed to improve these processes. Entities have undertaken appropriate corrective action to ensure the integrity of supplier information and payments. No new issues have been identified that indicate an ongoing, underlying risk.

Strengthen the security of information systems (all entities)		Further action needs to be taken*
REC 2	We recommend all public sector entities strengthen the security of their information systems. They rely heavily on technology, and increasingly, they have to 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. All entities across the public sector 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.	We continue to identify several control deficiencies relating to information systems. Cyber attacks continue to be a significant risk, with ongoing changes in entities' working environments due to COVID-19. Entities have undertaken the following to strengthen the security of information systems: • implemented security monitoring systems to detect and report on potential security threats and events • enabled multi-factor authentication on all external systems available to the public • implemented strong password practices in line with the state's recommendations (for example, a minimum of eight-character passwords) • implemented mandatory cyber security awareness training • implemented policies and processes to identify critical security vulnerabilities. We recommend all transport entities continue implementing policies and processes to strengthen the security of information systems.

Strengthen payroll processes and controls (all entities)		Further action needs to be taken*
REC 3	All entities should ensure employee information, timesheets, and payments are recorded accurately, appropriately authorised, and independently reviewed.	Transport entities have: • reconciled fortnightly payment summaries to bank statements and the general ledger • updated processes for changes to employee information to ensure they are adequately documented, appropriately authorised, and accurately entered in the system • matched employee pay rates set up in payroll systems to employment contracts. We continue to identify several control deficiencies relating to the completion and review of manual timesheets. Given the high volume of employees still using some form of paper-based timesheets, there is an increased risk of errors that require correcting in a subsequent pay run. These adjustments take significant time and resources, which could be reduced using electronic timesheet systems. We recommend that all transport entities ensure timesheet processes are followed and consider a technology solution to automate timesheets.

Notes: *Refer to 'Recommendation status definitions'.

Source: Queensland Audit Office.

Recommendation status definitions

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 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.