D. Status of prior recommendations

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

Figure D1
Status of recommendations from Education 2023 (Report 13: 2023–24)

Strengthen information system controls (All entities)		Further action needs to be taken
2023 – REC 1	With the evolving security threats, we recommend that all education entities: • limit information system access to only those employees and third-party users (for example, contractors) who require this to perform their jobs • monitor activities performed by employees and third-party users who have access to sensitive data and can make changes within the system • update security settings in line with updated risk assessments, security policies, and better practices. Ensure third-party users comply with these.	While entities have taken appropriate actions to resolve the issues we have reported to them each year, we continue to identify similar internal control deficiencies. Entities should continue to improve their processes for managing cyber security risks associated with services provided by third parties. This remains a recommendation.
Assess employment agreements and historical pay practices to identify potential wage underpayments (All entities)		**Further action needs to be taken**
2023 – REC 3	All education entities should: • assess the risk of underpayment of staff based on the complexity of their enterprise agreements, how they were paid historically, and the number of casual staff they employ • based on their assessed risk of underpayment, perform a detailed review of employment contracts and enterprise agreements, ensuring they match the payroll system set up for different wage types. Assess whether specialised external support is needed to assist with the review • establish and maintain adequate measures and controls to identify shortfalls in payment • provide training to key staff on how to interpret the different awards and employee entitlements in enterprise agreements • consider the need to invest in contemporary payroll and timekeeping systems to ensure accurate and thorough record-keeping practices. As part of their decision-making process, entities will need to perform an analysis of costs and benefits before making any investments.	Universities are continuing to assess the extent of any historical underpayments of staff wages and entitlements, and they are taking steps to address issues they have identified. They should continue to focus on managing the risk of wage underpayments. This remains a recommendation for universities. Other education entities have assessed the risk of wage underpayments and reviewed their systems and practices appropriately.

Source: Queensland Audit Office.

Figure D2
Status of recommendations from Education 2021 (Report 19: 2021–22)

Understand the cost of service delivery to make informed decisions about future services and efficiencies in operations (TAFE Queensland)		**Partially implemented**
2021 – REC 1	In order to remain sustainable in the longer term, TAFE Queensland needs to continue to develop its understanding of the value of its services and the costs of delivering them. It should use this understanding to decide whether to invest in training that is more efficient or of greater value to students, to standardise processes, and to continue to implement strategies for increasing its student revenue and market share. TAFE Queensland should continue to work alongside the Department of Trade, Employment and Training and Queensland Treasury to design and implement strategies to support its broader financial sustainability.	TAFE Queensland is still working on projects and initiatives to better understand its costs for service delivery, aimed at improving its longer-term financial sustainability. This remains a recommendation.
Complete regular and timely assessments of the condition of assets (Department of Education and Department of Trade, Employment and Training)		**Fully implemented**
2021 – REC 2	Both departments should ensure that condition assessments for their buildings are completed as soon as possible. The information from these assessments should be used to inform their maintenance budgets and long-term asset management strategies, which should consider both physical assets and digital infrastructure. These assessments should be undertaken regularly to ensure existing assets continue to be fit for purpose, and to address changing learning styles.	Both departments, as reported in Chapter 5 – *Asset management in education entities* – have completed their asset condition assessments for buildings and intend to continue these regularly, with the next assessment already planned.

Source: Queensland Audit Office.

Figure D3
Status of recommendations from Education 2020 (Report 18: 2020–21)

Strengthen the security of information systems (All entities)		Further action needs to be taken
2020 – REC 1	All entities should 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. These practices must also be aware of other users, such as students, to ensure all networks are as secure as possible. 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 modify information) 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 taken appropriate actions to resolve the issues we have reported to them each year, we continue to identify similar internal control deficiencies across multiple systems. Entities should continue to monitor how they manage these risks. This remains a recommendation.

Source: Queensland Audit Office.

Where a recommendation is specific to an entity, we have reported on the action that entity has taken and whether we consider the issue 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 government or the agency 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.