C. Status of prior recommendations

In *Education 2020* (Report 18: 2020–21), we identified the following recommendations for education sector entities.

We continue to identify control weaknesses in the security of information systems. This is a critical issue for education sector entities and must be addressed as soon as possible. The entities have made progress on the other 2 recommendations, but some still need to take further action. As a result, we have made separate recommendations for individual entities.

Figure C1
Status of recommendations from last year's report

Strengthen the security of information systems (all entities)		**Further action needs to be taken***
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.	This year, we identified 55 control deficiencies in entities' systems and processes (internal controls) relating to information systems. Cyber attacks continue to be a significant risk, given ongoing changes in entities' working environments (such as employees working from home) due to COVID-19. Entities have done the following to strengthen the security of information systems. They have: • enabled multi-factor authentication on all external systems available to the public (for example, a username and password, plus a code sent to a mobile) • implemented strong password practices in line with the state's recommendations (for example, a minimum of 8-character passwords) • implemented software that helps detect fraudulent emails • refreshed cyber security strategies to address identified risk • performed assessments of their cyber security to determine how effective it is. We recommend all education entities continue implementing policies and processes to strengthen the security of information systems.

Understand the cost of service delivery in order to make informed decisions about future services and efficiencies in operations (all education entities except the departments)		Further action needs to be taken*
REC 2	In order to remain sustainable in the longer term, education entities need to continue to develop their understanding of the value of their services and the cost of delivering them. They should use this understanding to decide whether to offer the same services in the future or invest in others that are more efficient or of greater value to customers.	Universities and grammar schools have undertaken appropriate action to address this recommendation through various forms of operational restructuring and cost savings. TAFE Queensland is still working on understanding its costs for service delivery, and it needs to develop a longer-term strategy to address its financial sustainability issues. We have made a separate recommendation for TAFE Queensland to address this risk. Refer to REC 1.
Improve asset condition assessments (all entities)		**Further action needs to be taken***
REC 3	All entities need to regularly review the condition of their assets to ensure they understand current and future maintenance requirements. Entities need to use accurate information about the condition of their assets to inform their long-term asset management strategies, which should consider both physical assets and digital infrastructure.	Universities and grammar schools have undertaken appropriate action to address this recommendation by reviewing their asset management plans and future capital projects, and completing comprehensive valuations. We have made a new recommendation for the Department of Education and the Department of Employment, Small Business and Training regarding further action required in relation to the completion of their assessments of the condition of their assets. Refer to REC 2.

Note: * Refer to 'Recommendation status definitions'.

Source: Compiled by the Queensland Audit Office.

Recommendation status definitions

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 to address the underlying risk.