C. Status of recommendations made in *Energy 2020* (Report 11: 2020–21)

Our report, *Energy 2020* (Report 11: 2020–21), identified the following recommendation for energy sector entities. These entities have taken appropriate action for the recommendation to resolve prior year issues. However, we continue to identify significant control weaknesses in the security of information systems, and this remains a recommendation for energy entities in 2021.

Figure C1
Status of the recommendation from last year's report

Strengthen the security of information systems (all entities)		Further action needs to be taken
REC 1	We recommend all 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. 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), in particular 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 our report—*Managing cyber security risks* (Report 3: 2019–20)—to ensure their systems are appropriately secured.	We continue to identify control deficiencies relating to assigning and monitoring user access. Entities have undertaken the following to strengthen the security of information systems: • regularly reviewing user access to ensure it remains appropriate • implementing strong password practices in line with the state's recommendations (for example, a minimum of eight-character passwords) • monitoring and reviewing the actions of users with privileged access • implementing policies and processes to identify critical security vulnerabilities. Although the entities have undertaken the above actions, we continue to identify control deficiencies in relation to information systems. We recommend all energy entities continue practising and implementing policies and processes to strengthen the security of their information systems.

Source: Queensland Audit Office.

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.