C. Status of recommendations made in prior reports

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

Figure C1
Status of recommendations from *State entities 2023* (Report 11: 2023–24)

Manage the cyber security risks associated with services provided by third parties (all entities)		Further action needs to be taken
REC 1	We recommend that all entities implement a process to manage the security risks relating to third-party services for information systems and technologies, and introduce procedures that will: • identify how they use third-party services, the extent to which they use them, and the associated security risks • establish due diligence (vetting and continuous monitoring) processes when engaging new third parties or continuing with third-party services • define security standards and the appropriate contractual agreements to manage security risks • establish a process to continually assess how well each third party manages its security risks and responds to and recovers from security incidents.	This year we identified 5 new deficiencies within state entities regarding how they manage cyber security risks associated with services provided by third parties. This is in addition to the 9 deficiencies from prior years still being actioned as of 30 June 2025. We recommend entities continue to monitor how they manage these risks. Our performance audit on managing third-party cyber security risks for tabling in 2025–26 will assess in more detail how effectively public sector entities manage third-party cyber security risks.

Source: Queensland Audit Office.

Figure C2
Status of recommendations from *State entities 2020* (Report 13: 2020–21)

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. Entities 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 resolved some of the issues we reported to them, we continue to identify new control weaknesses with the security of their information systems. Entities need to maintain effective internal controls and protect systems from attack. We encourage all entities to regularly self-assess the strengths of their information systems against the recommendations we made to all entities in: • *Managing cyber security risks* (Report 3: 2019–20) • *Responding to and recovering from cyber attacks* (Report 12: 2023–24).

Source: Queensland Audit Office.