C. Status of recommendations made in prior reports

The following table provides 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)		Status
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.	We consider the recommendations as closed as: • we have reported our observations to state entities that we audited • our report *Managing third-party cyber security risks* (Report 13: 2025–26) has also highlighted better practice approaches for identifying, assessing, monitoring, and managing third-party risks.

Source: Queensland Audit Office.