E. Status of prior recommendations

Our report, *Health 2023* (Report 6: 2023–24), identified the following 2 recommendations for health sector entities. These entities need to take further action on both recommendations. We continue to identify deficiencies we have made recommendations about in previous years. In particular, we continue to find control weaknesses in the security of information systems. We made a recommendation about this in 2020, and it still needs to be addressed.

Improve controls over rostering and overtime		**Further action needs to be taken**
2023 – REC 1	The department and 16 HHSs should: • develop a sector-wide policy for the timely submission of pay variation forms • reassess more effective and efficient ways to – control the approval of and recording of overtime approvals – monitor unplanned and planned overtime • develop a policy that defines the appropriate level of detail required by an employee to justify overtime hours worked and document the reasons for overtime worked • finalise the rollout of an electronic rostering system for nursing and midwifery staff as soon as practicable, and establish a plan and timetable to roll it out for other medical staff.	The parts of this recommendation that require further action relate to approving overtime and extending the scope of the electronic rostering system. We identified one hospital and health service (HHS) this year where there was a deficiency in relation to the approval of overtime. The department and HHSs made significant progress in rolling out the electronic rostering system to nursing and midwifery staff during 2023–24. The department plans to extend the electronic rostering system to other occupational groups, with funding allocated for this over the next 4 years.
Address inconsistencies in calculating deferred maintenance of assets		**Further action needs to be taken**
2023 – REC 2	The department and 16 HHSs should: • standardise the process for assessing anticipated maintenance of assets to ensure reliability in reporting and strategic asset management planning across the department and HHSs • ensure asset data, including data on the condition of assets, is up to date.	HHSs continue to have inconsistent approaches to calculating their maintenance needs, which increased by $580 million during 2023–24. This report includes 2 new recommendations relating to defining and separately reporting values for deferred maintenance, postponed capital maintenance, and forecast life cycle replacement, renewals, and refurbishments.

In *Health 2023* (Report 6: 2023–24) we identified that the following recommendations from our *Health 2022* (Report 10: 2022–23), *Health 2021* (Report 12: 2021–22), and *Health 2020* (Report 12: 2020–21) reports remained outstanding. An update on the status of these issues is included below.

Strengthening of information system and cyber security controls		Further action needs to be taken
2022 – REC 1	The 16 HHSs should: • review the dashboard of active users regularly to ensure access to the department's network is limited to authorised users only, and promptly notify the department of any changes required. The Department of Health should: • progress the Identity and Access Management Maturity and Service Uplift Project • update insecure settings in relation to passwords and default accounts.	We continue to identify significant control weaknesses in the security of information systems. As noted in Chapter 3, we identified 2 significant deficiencies (1 new, 1 re-raised) and 11 deficiencies (10 new, 1 re-raised) in information system controls in 2023–24. This remains a recommendation.
Procurement and contracting controls need to be strengthened		**Further action needs to be taken**
2021 – REC 1	The Department of Health and 16 HHSs should: • ensure they have appropriate contract management and procurement systems in place • provide training in procurement processes and procedures • maintain complete and up-to-date contract registers • ensure all documents relating to contracts are kept in a central location.	No significant deficiencies were identified in procurement practices. However, we did identify non-compliance with the requirement to publish information on awarded contracts on open data at 3 health entities. This remains a recommendation.
Resolve outstanding audit issues		**Further action needs to be taken**
2020 – REC 2	Queensland Health entities and their audit committees should continue to regularly review the status of outstanding audit issues and ensure they are resolved in a timely manner.	As noted in Chapter 3, internal controls are generally effective. However, 8 issues raised in prior years (2018–23) are yet to be resolved. Therefore, this remains a recommendation.

Strengthen the security of information systems		Further action needs to be taken
2020 – REC 3	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), 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 reported 13 deficiencies in information systems controls, 2 of which we considered to be significant deficiencies. The deficiencies that we identify in Chapter 3 show that the department needs to do more to strengthen controls over system access. This remains a recommendation.
Address backlog of asset maintenance		**Further action needs to be taken**
2020 – REC 5	Queensland Health entities should continue to prioritise high-risk maintenance. The hospital and health services should work with the department to find ways to mitigate the operational, clinical, and financial risks associated with deferred maintenance.	HHSs reported a $580 million increase in deferred maintenance this year. Further action is required to ensure that deferred maintenance, including high and very high-risk maintenance, is correctly identified, reported, and appropriately managed.

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.