E. Status of prior recommendations

In *Health 2022* (Report 10: 2021–22), we identified the following recommendation for hospital and health services (HHSs) and the Department of Health (the department). These entities need to take further action to address this recommendation. We continue to identify significant control weaknesses in the security of information systems, and this remains a recommendation for health entities in 2023.

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 4 new deficiencies in information system controls in 2022–23. Of the issues raised in prior years, 3 are yet to be resolved.

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

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.	There has been improvement, with some of the previously reported procurement deficiencies being resolved during prior years. However, as noted in Chapter 3, we identified 4 new deficiencies in procurement controls in 2022–23. This highlights that more work is needed in this area.
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, 6 issues raised in prior years (2018–2022) are yet to be resolved.

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.	We continued to identify weaknesses in system security. We made a new recommendation in our *Health 2022* report – Recommendation 1.
Approve service agreements for shared services		**Fully implemented**
2020 – REC 4	The Department of Health and the hospital and health services should work together to approve and sign service level agreements with each other for the purchasing and payroll services the department performs on behalf of the HHSs. The agreements should clearly identify the roles and responsibilities of each party, including the quality and scope of services and the respective costs.	Service agreements between the department and each HHS now include service schedules outlining roles and responsibilities for services provided by the department to HHSs.
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 anticipated maintenance.	The anticipated maintenance of assets has increased by $351 million in 2022–23. Chapter 5 of this report includes a new recommendation to address inconsistencies in calculating anticipated maintenance of assets.

Where a recommendation is specific to an entity, we have reported on the action that entity has taken and whether the issue is considered to be *fully implemented*, *partially implemented, not implemented* or *no longer applicable*.

Status	Definition	
Fully implemented	Recommendation has been implemented, or alternative action has been taken that addresses the underlying issues, and no further action is required. Any further actions are business as usual.	
Partially implemented	Significant progress has been made in implementing the recommendation or taking alternative action, but further work is required before it can be considered business as usual. This also includes where the action taken was less extensive than recommended, as it only addressed some of the underlying issues that led to the recommendation.	
Not implemented	**Recommendation accepted**	No or minimal actions have been taken to implement the recommendation, or the action taken does not address the underlying issues that led to the recommendation.
	Recommendation not accepted	The government or the agency did not accept the recommendation.
No longer applicable	Circumstances have fundamentally changed, making the recommendation no longer applicable. For example, a change in government policy or program has meant the recommendation is no longer relevant.	

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.