D. Status of recommendations from prior reports

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

Figure D1
Status of recommendations for councils from our report *Local government 2020* (Report 17: 2020–21)

Improve financial reporting by strengthening month-end and year-end financial reporting processes		**Further action needs to be taken***
REC 1	Councils should strengthen their month-end and year-end processes to assist with timely and accurate monthly internal financial reporting and their annual financial statements. We recommend all councils use their recent financial statement preparation experiences to perform an initial self-assessment against the maturity model available on our website.	We continue to find that month-end processes in councils appear to be ineffective. This year, we identified 73 deficiencies across 60 councils where improvements were required to ensure timely and reliable month-end and year-end reporting. We continue to recommend that councils improve their month-end processes.
Improve valuation and asset management practices		**Further action needs to be taken**
REC 2	• Councils need to engage with asset valuers early to complete the valuation of assets well before year end. • Councils need to use accurate information in their long-term asset management strategies and budget decisions. • Councils need to regularly match the asset data in their financial records to the asset data in their engineering/geographic information systems to ensure it is complete and reliable.	We continue to identify issues with the asset management policies and practices of councils. Councils still need to improve processes for asset valuations. We observed several councils who did not meet their legislative deadline because of errors and delays in asset valuations. In line with these findings, we continue to recommend that councils strengthen their asset management policies and practices.

Strengthen security of information systems		**Further action needs to be taken**
REC 3	We recommend all councils strengthen the security of their information systems. Councils rely heavily on technology, and increasingly, they need to be prepared for cyber attacks. Any unauthorised access could result in fraud or error, and significant reputational damage. Councils' workplace culture, through their people and processes, must emphasise strong security practices to provide a foundation for the security of information systems. All entities across the local government sector 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. Councils 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 find deficiencies in information systems, particularly regarding user access permissions. This year, we identified 67 new internal control issues in information systems across 31 councils and observed that 28 internal control issues were unresolved from prior years. We also identified that 20 councils have not provided cyber security training to their staff, which is an important tool in managing cyber security risks. The recommendation to strengthen the security of information systems remains.

Improve risk management processes		**Further action needs to be taken**
REC 4	Councils should have a complete and up-to-date risk management framework including: • comprehensive risk registers that identify risks (including the risk of fraud) and appropriate risk mitigation strategies • current and relevant business continuity and disaster recovery plans. These plans are tested periodically.	We have observed an improvement in the number of councils having adequate risk management processes. This year, 22 councils did not have adequate risk management processes in place – this is down from 29 councils in 2019–20. Although this is an improvement, it still represents over a quarter of the sector. This recommendation will remain.
Enhance procurement and contract management practices		**Further action needs to be taken**
REC 5	• Councils need to ensure they obtain value for money for the goods and services they procure and that they have the appropriate approvals to procure the goods and services. • To effectively manage their contractual obligations, councils should ensure their contract registers are complete and contain up-to-date information.	We have identified issues relating to procurement and contract management practices at 29 councils this year. This is only a small improvement when compared to the 31 councils in 2019–20 who had these issues. In line with these findings, we continue to recommend that councils strengthen their procurement and contract management practices.

Note: *Refer to Recommendation status definitions later in this appendix.

Source: Queensland Audit Office.

Figure D2
Status of recommendations for councils from our report
***Local government entities: 2018–19 results of financial audits* (Report 13: 2019–20)**

Audit committees	**Further action needs to be taken***
• All councils should have an audit committee with an independent chair. • All audit committee members must understand their roles and responsibilities and the risks the committee needs to monitor. • Audit committees must hold management accountable for ensuring timely remedial actions are taken on audit issues. All extensions of agreed time frames for remedial action requires consideration by the audit committee, including management's risk mitigation strategies, until remedial action is completed.	We continue to find councils that do not have audit committees. As at 30 June 2021, there were 15 councils (30 June 2020: 16 councils) that did not have an audit committee. We continue to recommend to all these councils that they establish an independent audit committee with appropriately qualified committee members. Councils without an effective audit committee have 47 significant deficiencies that have been unresolved for more than 12 months (55% of the sector).
Internal audit	**Further action needs to be taken**
• All councils must establish and maintain an effective and efficient internal audit function, as required by the *Local Government Act 2009*.	We continue to find councils that do not have an internal audit function. As at 30 June 2021, there were 6 councils (30 June 2020: 7 councils) that did not have an internal audit function. In addition to that, 6 councils that had an internal audit function established at 30 June 2021 did not have any audit activity during the 2020–21 financial year. We continue to recommend to all these councils that they establish an internal audit function as required by the *Local Government Act 2009*.
Secure employee and supplier information	**Further action needs to be taken**
• Councils must verify changes to employee and supplier bank account details through sources independent of the change request. • Councils need to ensure information systems are secure to prevent unauthorised access that may result in fraud or error. Security measures could include encryption of information, restriction of user access, regular monitoring by management, and appropriate segregation of duties.	We continue to find deficiencies at councils with regards to securing employee and supplier information. Similarly, we continue to find weaknesses with information systems security. We have expanded on this recommendation and have included this as a part of REC 3 in Figure D1 above.

Conduct mandatory cyber security awareness training	Further action needs to be taken
Councils need to develop and implement mandatory cyber security awareness training for all staff, to be completed during induction and at regular periods during employment. This should include: • delivering targeted training to higher-risk user groups, such as senior management, staff who have access to sensitive data, software developers, system administrators, and third-party providers • recording and monitoring whether all staff have completed their required cyber security awareness training • conducting campaigns to test the adequacy of staff vigilance to risks, such as phishing (fraudulent emails) and tailgating (following a person into an office), so entities can assess and improve their awareness programs.	As at 30 June 2021, 20 councils had not provided cyber security awareness training to their employees. We continue to recommend that all councils provide cyber security awareness training to their new and current employees.

Note: *Refer to Recommendation status definitions later in this appendix.

Source: Queensland Audit Office.

Figure D3
Status of recommendations for the department from our report *Local government 2020* (Report 17: 2020–21)

Require all councils to establish audit committees		**Not implemented – Recommendation accepted***
REC 6	We continue to recommend the department requires all councils to establish an audit committee and ensure that each chairperson of the committee is independent of council and management. In light of the difficulties some councils have faced with internal control weaknesses, fraud, ransomware, and achieving financial sustainability, this is more important now than ever.	The proposal continues to be considered by the department but has not as yet been progressed.
Makes changes to sustainability ratios		**Partially implemented**
REC 7	We recommend the department develops new financial sustainability ratios for Queensland councils. In developing these ratios and associated targets, we recommend the department considers the different sizes, services, and circumstances of the various councils. We also recommend that new financial sustainability ratios be established in time for the year ending 30 June 2022.	The department has developed a new framework that is currently in the consultation phase. The new framework is expected to be implemented for the 2023–24 financial year.
Provide greater certainty over long-term funding		**Partially implemented**
REC 8	We recommend the department reviews its current funding model to identify opportunities to provide funding certainty to councils beyond one financial year. A 3- to 5-year funding model would assist councils, especially those heavily reliant on grants, to develop and implement more sustainable medium- to long-term plans.	The department has partially implemented this, and some grants in the 2020–21 year were multi-year grants. The department is undertaking a review of its grants program and will consider other grants in the 2022–23 financial year for future funding programs.
Provide training to councillors and senior leadership teams around financial governance		**Partially implemented**
REC 9	We recommend the department provides periodic training to councillors and senior leadership teams for councils that are highly reliant on grants. The training should focus on helping these councils: • establish strong leadership and governance • enhance internal controls and oversight • improve financial sustainability in the long term.	The department is in the process of developing training in financial governance and basic financial management for councillors. Some pilot sessions have already been delivered, and additional sessions are planned to be rolled out.

Note: *Refer to Recommendation status definitions later in this appendix.

Source: Queensland Audit Office.

Recommendation status definitions

If 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 entity 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.	

If a general recommendation has been made for all entities to consider, we assess 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.