# C. Status of prior recommendations

Our report, *Water 2020* (Report 9: 2020–21), identified the following recommendations for water sector entities. These entities have taken appropriate action for two of the three recommendations. However, we continue to identify significant control weaknesses in the security of information systems. This is a critical issue for water sector entities and must be addressed as soon as possible.

**Figure C1**
**Status of recommendations from prior year's report**

| **Strengthen the security of information systems (all entities)** | | **Further action needs to be taken*** |
|---|---|---|
| **REC 1** | We recommend all public sector 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.<br>Their workplace culture, through their people and processes, must emphasise strong security practices to provide a foundation for the security of information systems.<br>All entities across the public sector should:<br>• provide security training for employees so they understand the importance of maintaining strong information systems, and their roles in keeping them secure<br>• 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<br>• regularly review user access to ensure it remains appropriate<br>• 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<br>• implement strong password practices and multi-factor authentication (for example, a username and password, plus a code sent to a mobile), particularly for systems that record sensitive information<br>• encrypt sensitive information to protect it<br>• 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.<br>Entities 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 identify several control deficiencies relating to information systems. Cyber attacks continue to be a significant risk, with ongoing changes in entities' working environments due to COVID-19.<br>Entities have undertaken the following to strengthen the security of information systems:<br>• implemented security monitoring systems to detect and report on potential security threats and events<br>• enabled multi-factor authentication on all external systems available to the public<br>• implemented strong password practices in line with the state's recommendations (for example, a minimum of eight-character passwords)<br>• implemented mandatory cyber security awareness training<br>• implemented policies and processes to identify critical security vulnerabilities.<br>We recommend all water entities continue implementing policies and processes to strengthen the security of information systems. |

| **Improve timely recognition of donated assets (distributor-retailers)** | | **Fully implemented*** |
|---|---|---|
| **REC 2** | Distributor-retailers (Urban Utilities and Unitywater) need to:<br>• engage more closely with developers to determine whether assets themselves are complete<br>• obtain engineering drawings and other information in a timely manner<br>• closely monitor development application registers for completeness of recorded assets<br>• identify and address causes of delays in processing engineering drawings. | Distributor-retailers have undertaken the following activities to improve timely recognition of donated assets (charges paid by developers, either in cash or in assets such as water and sewerage infrastructure):<br>• performed independent reviews to amend data inconsistencies<br>• performed weekly compliance checks of all donated assets to ensure completeness and accuracy of data<br>• monitored adherence to new processes to ensure controls are operating effectively.<br>Legacy issues may happen throughout the year, due to the time lag between building applications and the recognition of developer contributions. However, no new issues have been identified that indicate an ongoing, underlying risk. |
| **Understand complex employee arrangements (all entities)** | | **Appropriate action has been taken*** |
| **REC 3** | As part of the negotiation process for enterprise agreements, entities should ensure they understand how these arrangements interact with employee contracts. | Water entities have undertaken the following to help in understanding complex employee arrangements:<br>• engaged external experts to advise on the development of enterprise agreements<br>• reviewed compliance obligations (for example, annualised salaries and hours of work in accordance with employee contracts)<br>• updated payroll and human resource policies and procedures to ensure practices are compliant and understood<br>• undertaken periodic reconciliations of individual employment contracts to ensure the entity is compliant with all employee obligations<br>• conducted internal reviews in collaboration with external experts to obtain assurance that employees are being paid in accordance with their specific employment arrangements.<br>No new issues have been identified across the sector that indicate an ongoing, underlying risk that requires reporting to parliament. |

Note: *Refer to ‘Recommendation status definitions’.

*Source: Compiled by the Queensland Audit Office from Water 2020 (Report 9: 2020–21) and responses received from each water sector entity.*

# Recommendation status definitions

If a recommendation is specific to an entity or particular entities, 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*.

<table>
<tr><th>Status</th><th colspan="2">Definition</th></tr>
<tr><td><b>Fully implemented</b></td><td colspan="2">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.</td></tr>
<tr><td><b>Partially implemented</b></td><td colspan="2">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.</td></tr>
<tr><td rowspan="2"><b>Not implemented</b></td><td><b>Recommendation accepted</b></td><td>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.</td></tr>
<tr><td><b>Recommendation not accepted</b></td><td>The entity did not accept the recommendation.</td></tr>
<tr><td><b>No longer applicable</b></td><td colspan="2">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.</td></tr>
</table>

If 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 decided 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. |