Appendix two – Status of 2017 recommendations

Recommendation	Current status	
Overall trends		
Agencies should focus on emerging information technology (IT) risks, but also manage new IT risks, reduce existing IT control deficiencies, and address repeat internal control deficiencies on a more timely basis.	The number of new and repeat IT control deficiencies increased this year. Refer to section 2.3 for further details.	❗
Agencies should rectify high risk internal control deficiencies as a priority.	All but one of the high risk internal control deficiencies identified last year have been rectified.	➖
Agencies should coordinate actions and resources to help rectify common IT control and governance deficiencies.	There has been a small reduction in the proportion of repeat internal control deficiencies. Refer to section 2.3 for further details.	➖
Information technology		
Agencies should tighten privileged user access to protect their information systems and reduce the risks of data misuse and fraud. Agencies should ensure they: • only grant privileged access in line with the responsibilities of a position • review the level of access regularly • limit privileged user access to necessary functions and data • monitor privileged user account activity on a regular basis.	The use and monitoring of privileged users remains an issue at agencies. Refer to section 3.2 for further details.	❗
Agencies should strengthen user access administration to prevent inappropriate access to sensitive systems. Agencies should: • establish and enforce clear policies and procedures • review user access regularly • remove user access for terminated staff promptly • change user access for transferred staff promptly.	User access administration remains an issue at agencies. Refer to section 3.2 for further details.	❗
Agencies should review and enforce password controls to strengthen security over sensitive systems. As a minimum, password parameters should include: • minimum password lengths and complexity requirements • limits on the number of failed log-in attempts • password history (such as the number of password remembered) • maximum and minimum password ages.	Password controls remains an issue at agencies. Refer to section 3.2 for further details.	❗

Recommendation	Current status	
The Department of Finance, Services and Innovation (DFSI) should revisit its existing framework to develop shared cyber security terminology and strengthen the current reporting requirements for cyber incidents.	Cyber security terminology is in the process of being developed with input from other jurisdictions and key stakeholders. The current incident reporting process is not mandatory. DFSI is investigating options to make this reporting mandatory to overcome the current intermittent nature of reporting from agencies.	➖
The Department of Finance, Services and Innovation should: • mandate minimum standards and require agencies to regularly assess and report on how well they mitigate cyber security risks against these standards • develop a framework that provides for cyber security training.	A draft version of minimum standards is being developed. DFSI is working with clusters to understand current training already in place and leverage this information to develop training.	➖
Agencies should consistently perform user acceptance testing before system upgrades and changes. They should also properly approve and document changes to IT systems.	Program change controls remains an issue at agencies. Refer to section 3.2 for further details.	➖
Agencies should complete business impact analyses to strengthen disaster recovery plans, then regularly test and update their plans.	Absence of a disaster recovery or business continuity plan and/or testing during the year was identified at four agencies.	➖
Asset management		
Agencies with high capital asset investment ratios should ensure their project management and delivery functions have the capacity to deliver their current and forward work programs.	Relevant agencies continue to monitor this recommendation. Agencies reported: • a reduction in their capital program, which reduces the risk of insufficient capacity to deliver the program • that project risk management and delivery controls are in place to address this risk.	➖
Agencies should have formal processes for disposing of surplus properties.	Relevant agencies have developed a policy for disposal of surplus property or assessed that a policy is not required, as surplus property is rarely held.	✅
Agencies should use Property NSW to manage real property sales unless, as in the case for State owned corporations, they have been granted an exemption.	This exception did not arise during the audits of agencies. The relevant agencies have addressed this recommendation.	✅
Ethics and conduct		
Agencies should regularly review their code-of-conduct policies and ensure they keep their codes of conduct up-to-date.	Agencies have updated their code of conduct or advised that the code of conduct will be updated in 2018–19.	➖

Recommendation	Current status	
Agencies should improve the way they manage conflicts of interest, particularly by: • requiring senior executives to make a conflict-of-interest declaration at least annually • implementing processes to identify and address outstanding declarations • providing annual training to staff • maintaining current registers of conflicts of interest.	All agencies have a process that requires senior executives to make a conflict of interest declaration annually and update the conflict of interest register. Some agencies are still implementing processes to identify and address outstanding declarations and provide training to staff.	⊖
Agencies should improve the way they manage gifts and benefits by promptly updating registers and providing annual training to staff.	Some agencies have not updated their policies to require immediate updating of the gifts and benefits register or provide annual training to staff.	⊖

✓ Fully addressed	⊖ Partially addressed	! Not addressed