Appendix one – List of 2017 recommendations

The table below lists the recommendations made in this report with a rating of high ⚠, medium ➖, or low ✅ in the level of risk they pose.

1. Overall trends

1.1 New and repeat findings	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.	⚠
1.2 High risk findings	Agencies should rectify high risk internal control deficiencies as a priority.	⚠
1.3 Common findings	Agencies should coordinate actions and resources to help rectify common IT control and governance deficiencies.	➖

2. Information technology

2.1 IT security	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 access to necessary functions and data • monitor privileged user account activity on a regular basis.	⚠
	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.	⚠
	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 passwords remembered) • maximum and minimum password ages.	➖
2.2 Cyber security	The Department of Finance, Services and Innovation should revisit its existing framework to develop a shared cyber security terminology and strengthen the current reporting requirements for cyber incidents.	⚠

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. ❗

Agencies should ensure they adequately resource staff dedicated to cyber security. ❗

2.4 Other IT systems
Agencies should consistently perform user acceptance testing before system upgrades and changes. They should also properly approve and document changes to IT systems. ❗

Agencies should complete business impact analyses to strengthen disaster recovery plans, then regularly test and update their plans. ❗

3. Asset management

3.1 Capital investment
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. ➖

3.3 Asset disposals
Agencies should have formal processes for disposing of surplus properties. ➖

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. ➖

5. Ethics and conduct

5.1 Ethical framework
Agencies should regularly review their code-of-conduct policies and ensure they keep their codes of conduct up-to-date. ➖

5.2 Potential conflicts of interest
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. ❗

Agencies should improve the way they manage gifts and benefits by promptly updating registers and providing annual training to staff. ❗

Key	✅ Low risk	➖ Moderate risk	❗ High risk