Appendix one – List of 2023 recommendations

The table below lists the recommendations made in this report.

2. Financial reporting

2.1 Common accounting issues	• Universities should prioritise remediation of wage underpayments to affected employees. • Universities should ensure controlled entities comply with the GSF Act reporting obligations.

3. Internal controls and governance

3.1 Internal controls trends	Universities should ensure repeat findings on internal control deficiencies are addressed in a timely manner, particularly those that have been repeat findings for a number of years.
3.2 Code of ethics and conduct	Universities should ensure: • all staff annually attest to the Code of Conduct • all new staff acknowledge they understand the requirements of the Code of Conduct upon commencement of employment • the Code of Conduct is reviewed regularly • all key elements are included in the Code of Conduct • the Code of Conduct extends to contractors and third-party vendors.
3.3 Conflicts of interest	Universities should maintain a centralised conflict of interest register for all staff. Registers should be updated when conflicts are identified and on an annual basis. Conflict of interest registers should be referred to during procurement activity to ensure that any perceived or actual conflicts of interest risk are identified and appropriately addressed.
3.4 Risk management	All universities should ensure: • mandatory annual risk management awareness training is provided to all staff • emerging risks are considered in their risk register • the effectiveness of risk mitigating controls are documented • risk maturity reviews are performed regularly and action plans to address gaps are implemented.
3.5 Internal audit function	Universities should ensure: • their internal audit functions are independently evaluated • internal audit recommendations are implemented on a timely basis • controlled entities are considered and incorporated on a risk basis in their internal audit plans.

5. Cyber security

5.1 Cyber security risks in the university sector	Universities should ensure proactive processes exist across all faculties and divisions to identify, monitor and comply with the requirements of the *Security of Critical Infrastructure Act 2018*.	
5.2 Identifying and responding to cyber security risk	Consistent with their individual risk management frameworks or acceptance criteria, universities should identify and manage risks that exceed their risk appetite.	
	All universities should track and annually assess their cyber security maturity.	
	All universities should develop, monitor, and re-evaluate their cyber security uplift programs as they progressively achieve their targets.	
5.3 Cyber resilience	Universities should ensure cyber security event monitoring and coverage extends across systems, functions, and operations.	
	Universities should develop and finalise multiple playbooks to formalise and streamline responses to common and frequent cyber security incidents.	
	Universities should formally document the outcome of their Cyber Incident Response Plan testing to make sure that lessons from the exercise are learned.	

Key  **Low risk**  **Medium risk**  **High risk**