




L. Information system controls – guide for audit and risk committees

We encourage the audit and risk committees of public sector entities to consider the following questions regarding the security of their information systems.

This guide complements our previous reports – *Managing cyber security risks* (Report 3: 2019–20) and *Responding to and recovering from cyber attacks* (Report 12: 2023–24). It is designed to assist committees in assessing the effectiveness of their information system controls.

Figure L1
Guide on information system security controls for audit and risk committees

Area	Questions
 <p>Governance and oversight</p>	<ul style="list-style-type: none"> • How does the committee monitor the effectiveness of the entity's information system security controls and cyber security measures? • What steps does the committee take to oversee how the entity adapts its cyber security strategies and information system security controls to evolving threats?
 <p>Access management and security configuration</p>	<ul style="list-style-type: none"> • What is the entity's strategy to control unrestricted access to sensitive systems for internal staff and contractors, and how does it ensure these controls are operating effectively? • How does management monitor the activities of users of information systems that have extensive permissions within systems and in detecting unauthorised actions? • Are the entity's password policies and access management practices aligned with recommendations from the Australian Cyber Security Centre website and software vendors?
 <p>Best practices</p>	<ul style="list-style-type: none"> • Is there a framework in place to document and share lessons learnt from cyber security incidents and from control issues that arise in relation to information systems? • How does management of the entity conduct root cause analysis to identify recurring issues with its information systems? • What processes are in place to ensure control deficiencies identified in one system are assessed and addressed across all systems in the entity? • How frequently does management update the entity's security settings based on new or elevated risks and policies? • What specific controls are in place to manage the risks associated with using unsupported older legacy systems?

Source: Queensland Audit Office.