Report on a page

This is our first report on information systems controls, designed to recognise the collective need across government for more focus on the security of information. This report provides:

- a summary of matters identified in our information systems audits for state entities in Queensland's public sector
- preliminary insights on legacy systems that have passed their lifespan and are no longer supported by their technology providers.

Queensland public sector entities include the 21 core departments (referred to as 'departments' in this report), statutory bodies, and government owned corporations.

IT system defences need strengthening

While entities generally have effective IT controls for finance systems, control deficiencies remain in:

- system access (controlling who can access which part of systems)
- passwords and authentication (verifying that only authorised users can access systems)
- security configuration (checking allowable and required actions to access systems)
- detective controls to identify potential incidents
- managing risks associated with third parties.

Entities are not fully tackling root causes due to competing priorities and are not checking that implemented controls are effective. A significant number of deficiencies remain unresolved from prior years, suggesting that entities are not addressing IT risks in a timely way.

Entities need greater focus on:

- strengthening IT systems defence to address control deficiencies that continue to exist
- addressing IT systems deficiencies from prior years to close security gaps.

Half of finance systems are being used beyond their lifespan

Half of the systems we audited for financial reporting purposes are legacy systems being used well beyond their expected lifespan and are no longer supported by technology providers. Entities often need to implement manual workarounds and may be unable to implement security updates. This impacts effective operation of controls and the efficiency of entities' operations, and creates security risks.

Departments, as part of their annual report to the Department of Customer Services, Open Data and Small and Family Business, reported increases in at-risk systems, which require attention. The accuracy, quality, and completeness of data reported about at-risk systems suggest there is not a complete understanding of the extent of these legacy systems, the cost to replace those systems, and IT asset management practices.

Departments need to continue to accurately and completely report on at-risk systems and their register of IT assets.

For entities embarking on new system implementations, we have provided key considerations for those with governance oversight responsibilities for projects and accountable officers for assessing the effectiveness of controls in Appendix D.