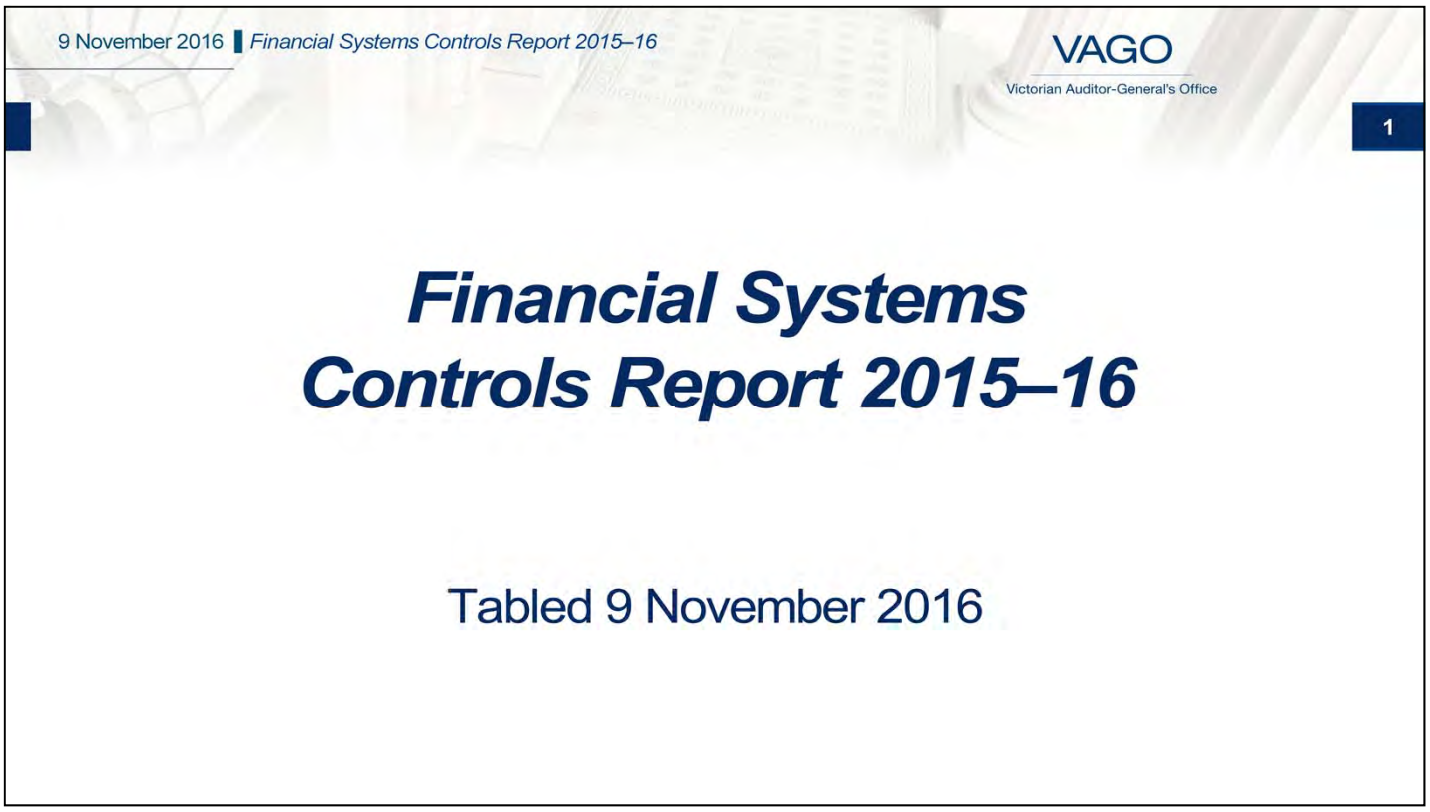
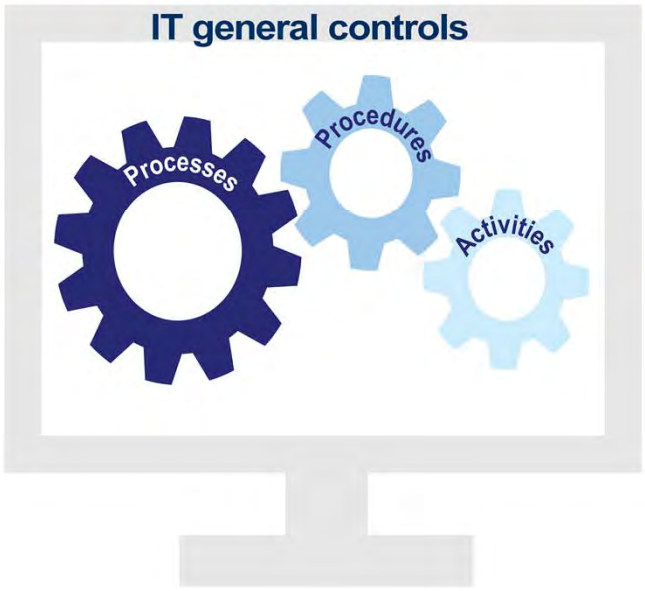


This presentation provides an overview of the Victorian Auditor-General's report *Financial Systems Controls Report 2015–16.*

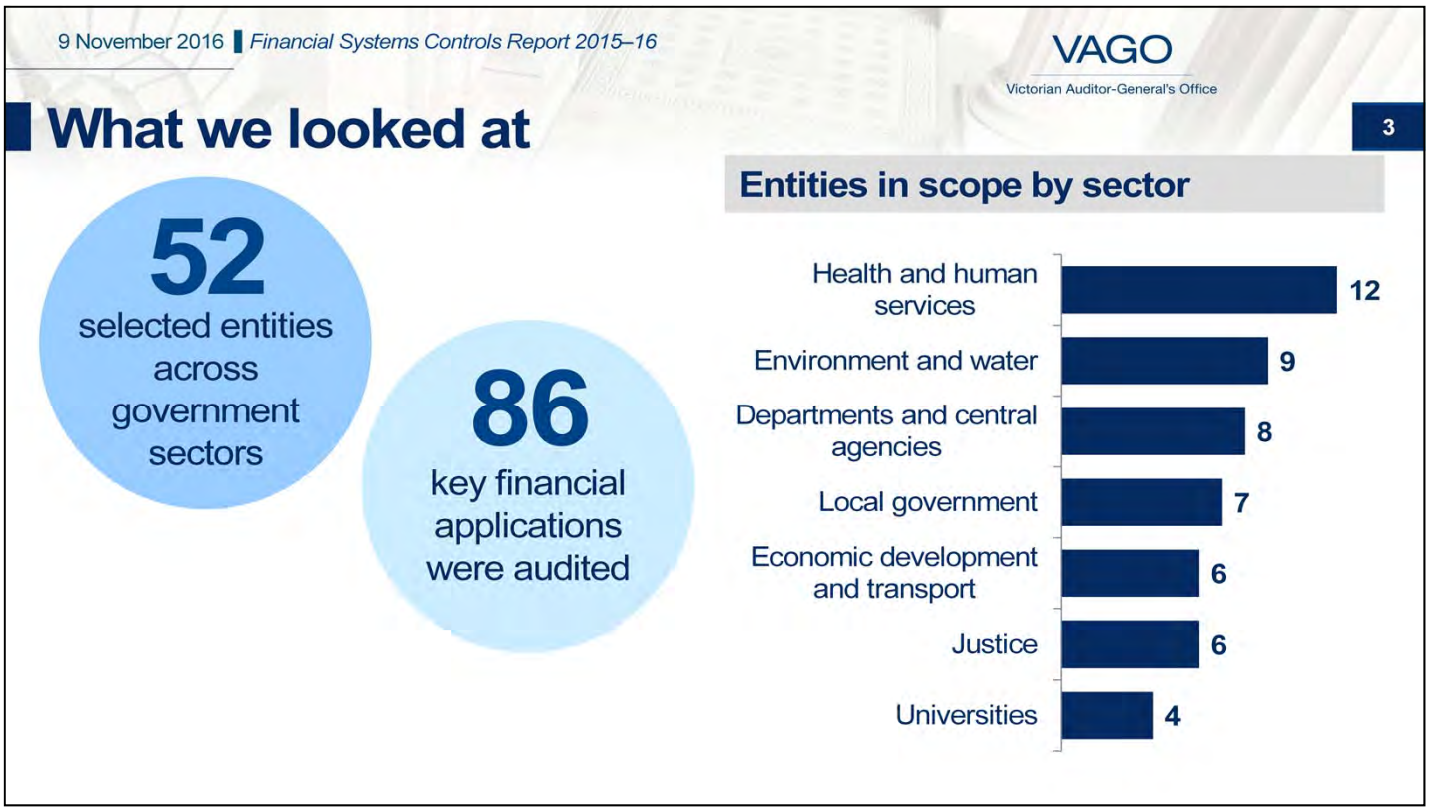
About financial systems controls



This report provides an overview of the strength of the IT controls that protect financial information at public sector entities.

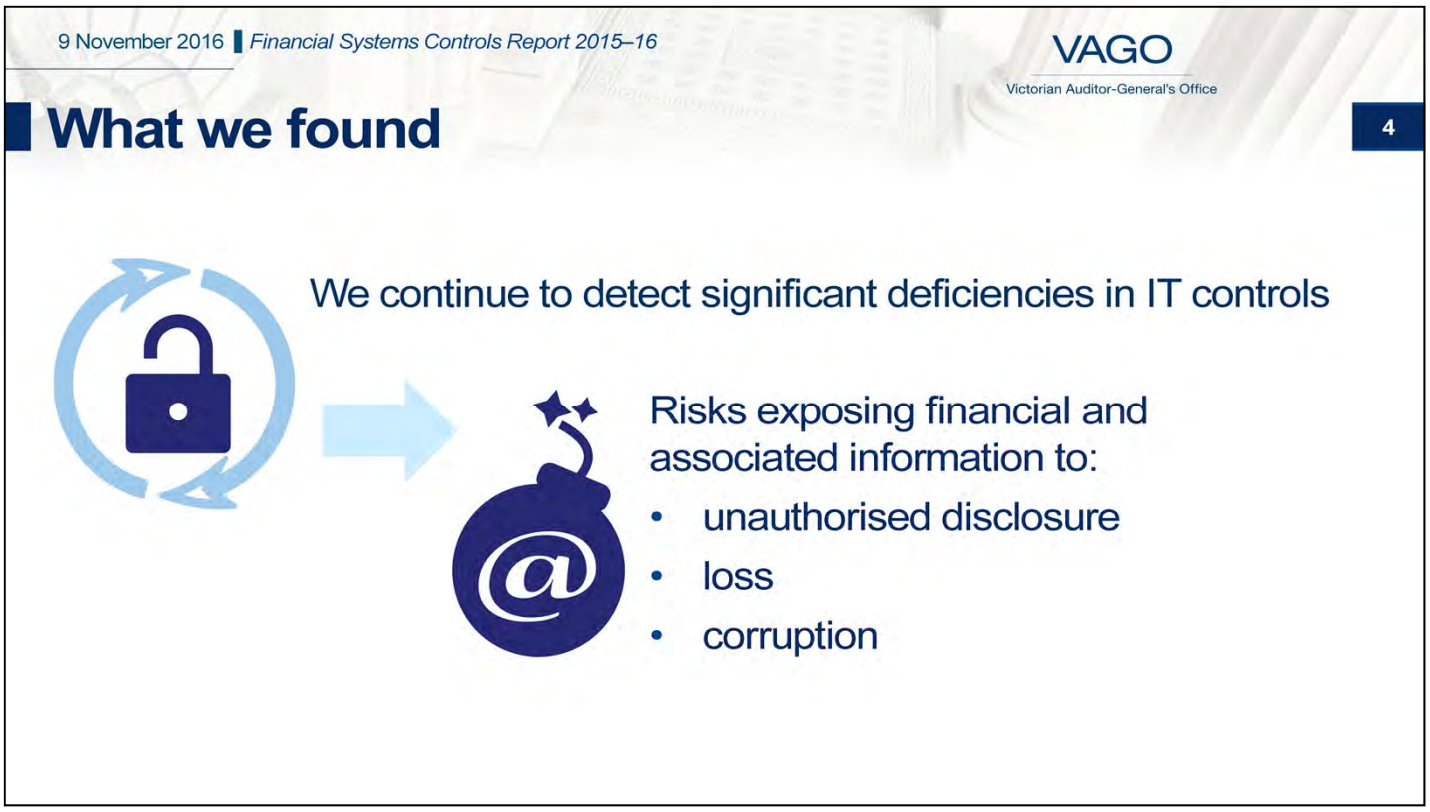
IT general controls are the policies, procedures and activities put in place by an entity to ensure the confidentiality, integrity and availability of its IT systems and data. Ineffective IT general controls may affect the reliability of the system's underlying financial data and programs.

In this report, we provide an overview of the strength of the IT controls that protect financial information at public sector entities.



As part of our 2015–16 financial audits, we tested the effectiveness of selected IT controls at 52 entities to determine whether they are operating as intended and are effectively mitigating risk.

This is the third report of its kind and it aims to provide further insight into our IT audit findings and identify wider trends.



We are concerned that we continue to detect significant deficiencies in IT controls, many in systems that have been in place for a number of years. The weaknesses we continue to observe each year unnecessarily expose financial and associated information held by the affected entities to higher risks of unauthorised disclosure, loss or corruption.

Accountable officers and the governing bodies of these entities need to pay greater attention to mitigating risks to their information systems.

VAGO
Victorian Auditor-General's Office

Key theme: Addressing underlying risks or issues

60%

of our findings from previous reports remain open or were raised again

In the course of this audit we identified three key themes.

First, while entities are gradually addressing IT audit findings, they are not tackling the underlying risks or issues.

Sixty per cent of our findings from previous reports remain open or have been raised again.

VAGO
Victorian Auditor-General's Office

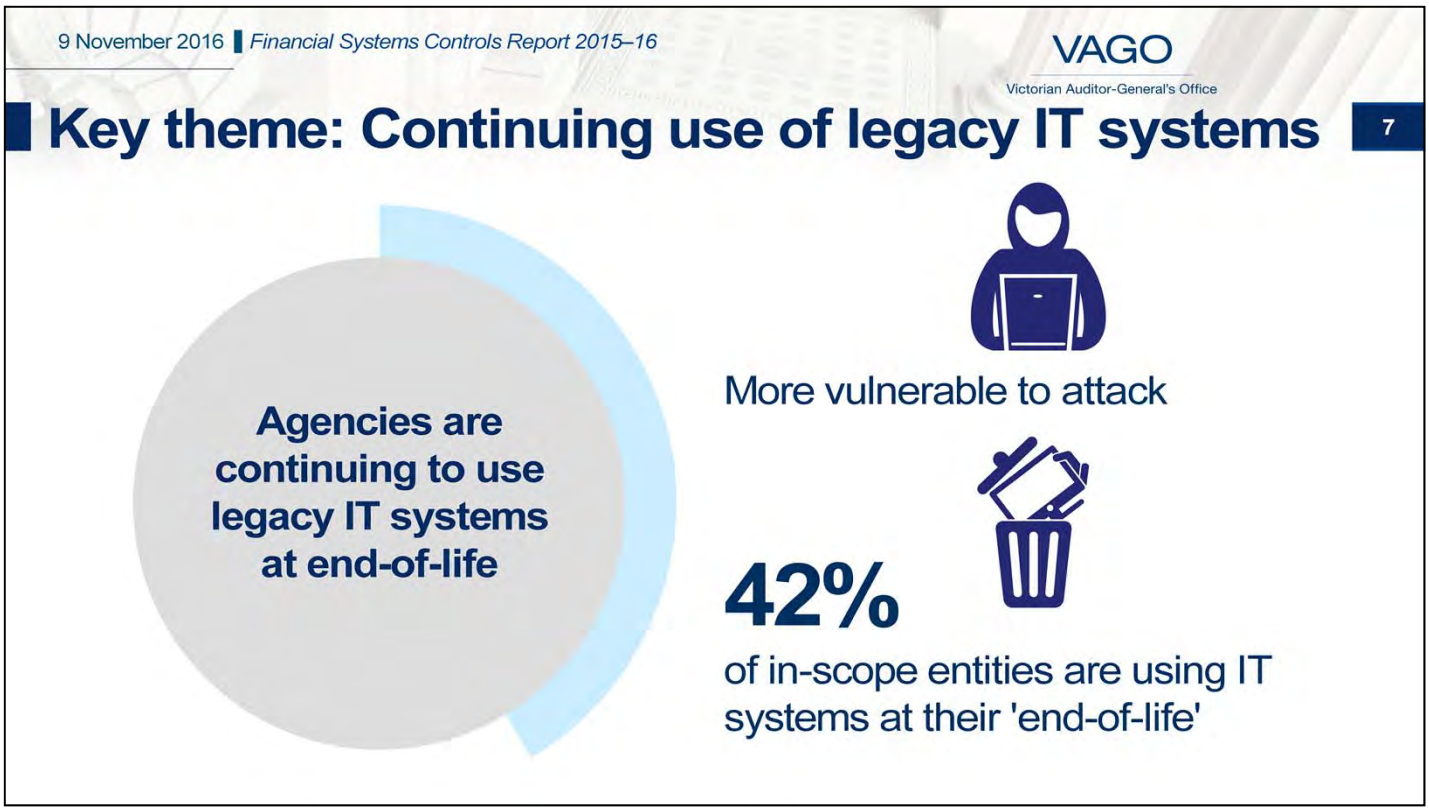
Key theme: Outsourced IT environments not effectively managed

Controls in outsourced IT environments are not being effectively managed

Entities still do not obtain any substantive assurance that outsourced providers are operating and managing controls effectively.

Second, while some entities outsource their IT environments, this does not absolve them from maintaining effective controls.

More public sector entities are seeking assurance about the IT controls used by their outsourced providers, usually in the form of a service assurance report. But we continue to find entities that do not seek any substantive assurance that the controls implemented and managed by their outsourced providers are operating effectively.



Third, some entities continue to use IT systems and applications after vendor support ceases—for example, older versions of software. This can cause critical business systems to become unstable and less reliable, increases the cost of maintenance and support while making them more vulnerable to attack by exploiting their security weaknesses.

This year we reported 31 matters about IT systems passing their 'end-of-life', across 42 per cent of the entities we looked at.

VAGO
Victorian Auditor-General's Office

Areas of focus

We surveyed **43** entities about their:

- wireless security
- strategies to mitigate targeted cyber intrusions

This year, we also considered two areas of focus. We surveyed 43 entities about their wireless security and strategies to mitigate targeted cyber intrusions.

VAGO
Victorian Auditor-General's Office

Area of focus: Wireless security

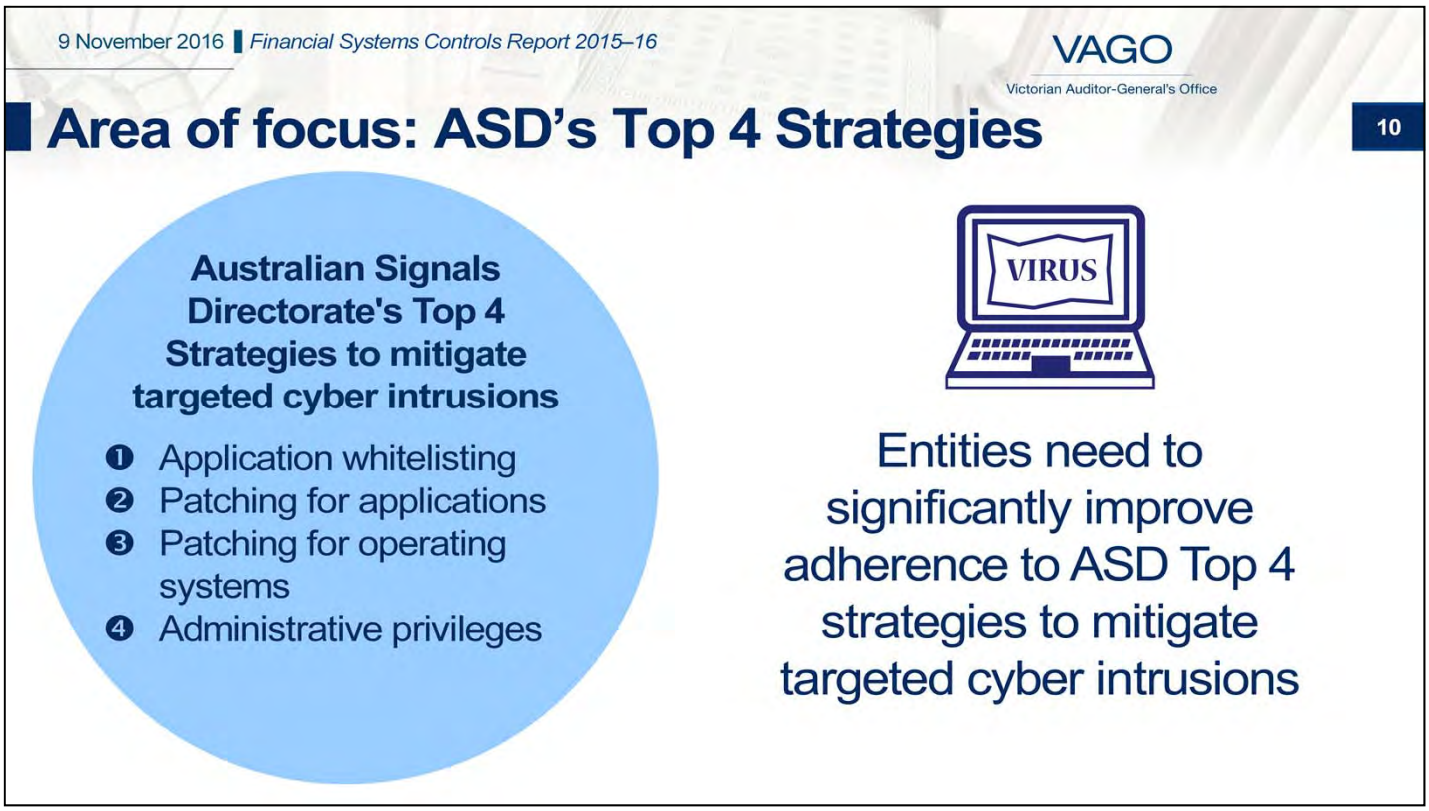
Wireless security aims to prevent unauthorised access to systems using wireless networks.

Wireless security is generally well-managed

BUT Entities need to improve:

- policies
- monitoring.

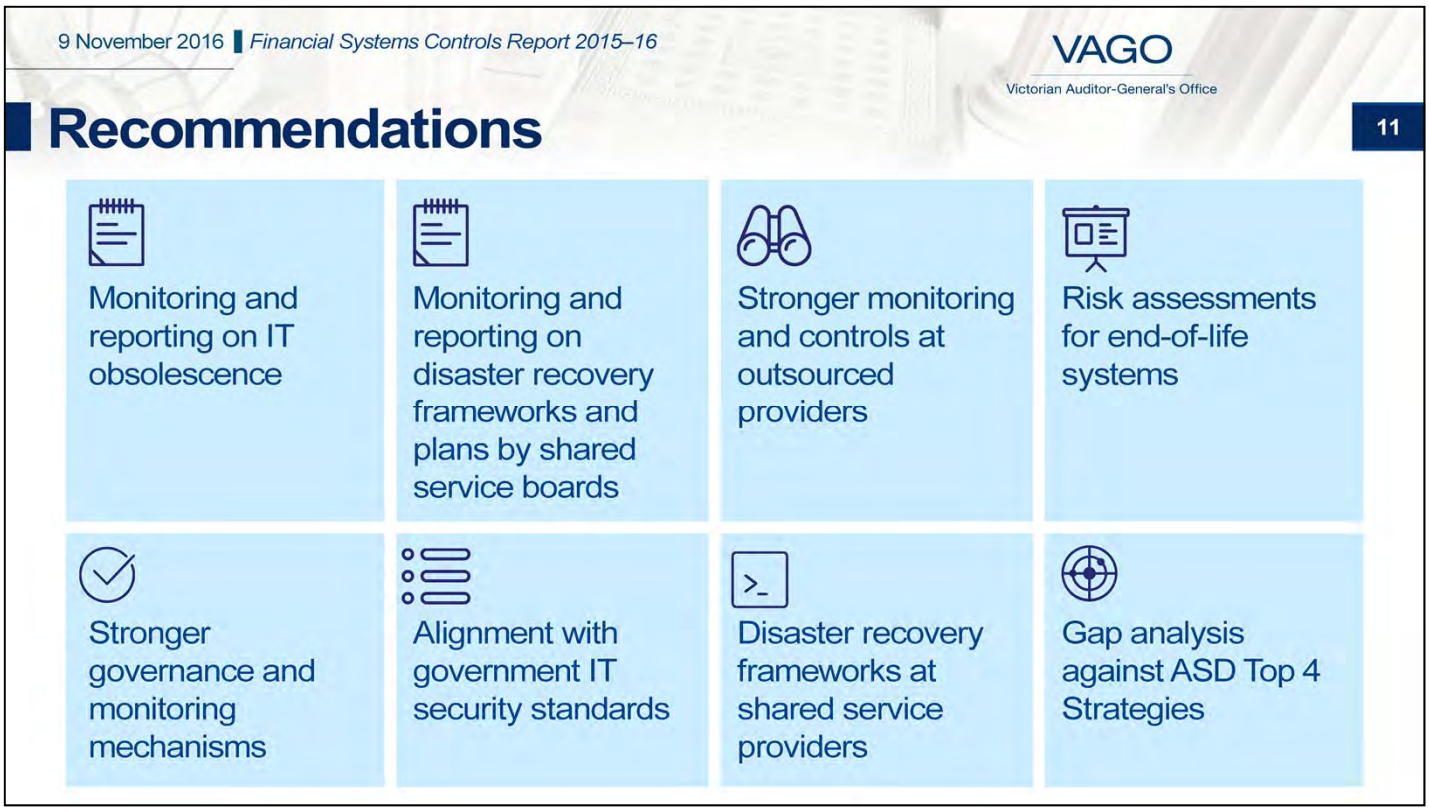
Wireless security aims to prevent unauthorised access to systems using wireless networks. Across public sector entities, wireless security is generally well controlled, however, opportunities exist to improve policies and monitoring.



The Australian Signals Directorate (ASD) has developed 35 strategies for mitigating targeted cyber intrusions. We focused on how entities are addressing the Top 4 strategies—application whitelisting , patching for applications, patching for operating systems, and administrative privileges.

Application whitelisting is a security technique in which only a limited set of approved programs are allowed to run on an entity's systems, while all other programs are blocked.

Entities need to significantly improve their adherence to the ASD Top 4 Strategies, particularly application whitelisting.



We made eight recommendations in this audit.

Two recommendations were directed to the Department of Premier & Cabinet, and six recommendations were directed to public sector entities.

The entities have accepted our recommendations. We will continue to monitor the implementation of the recommendations during future audits.

For further information, please view the full report on our website: www.audit.vic.gov.au

For further information, please see the full report of this audit on our website, www.audit.vic.gov.au.