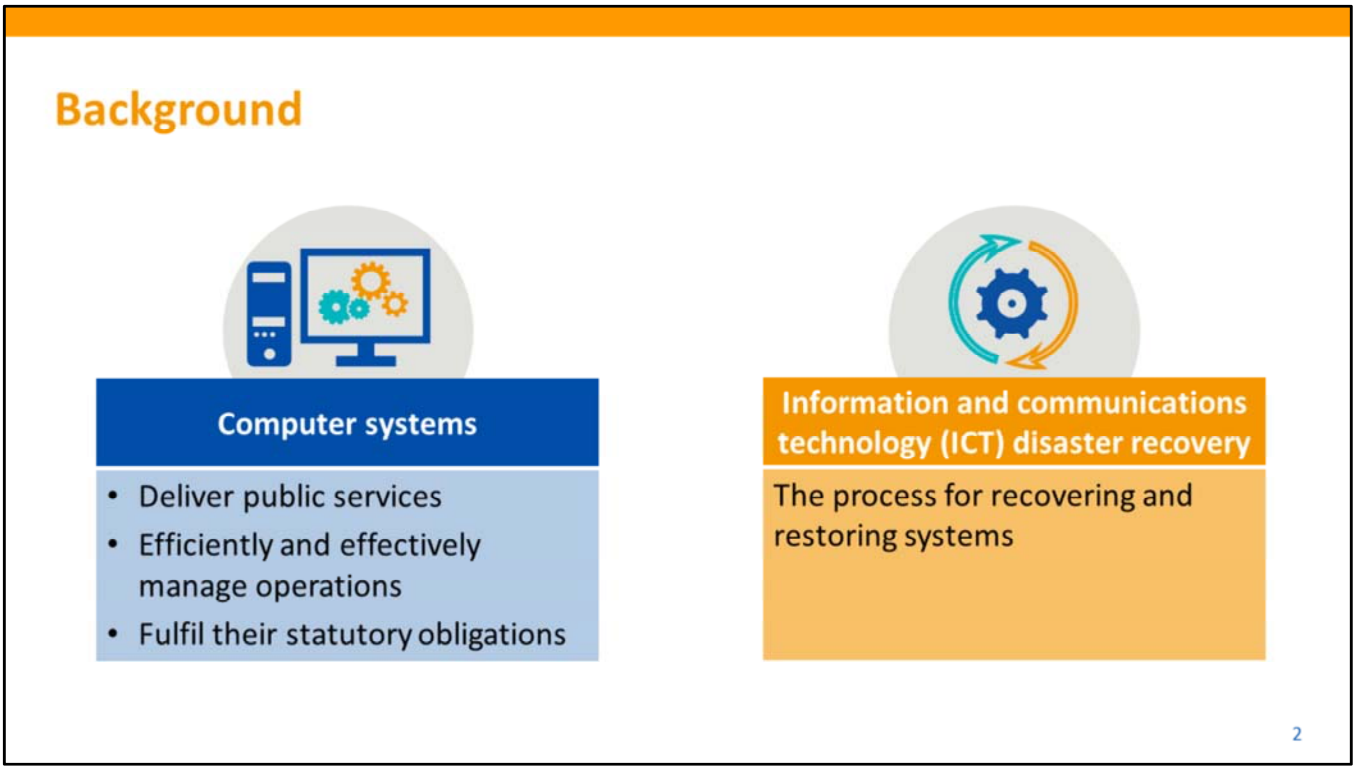
ICT Disaster Recovery Planning

Tabled 29 November 2017

VAGO

This presentation provides an overview of the Victorian Auditor-General's report on *ICT Disaster Recovery Planning*.



Background

Computer systems

- Deliver public services
- Efficiently and effectively manage operations
- Fulfil their statutory obligations

Information and communications technology (ICT) disaster recovery

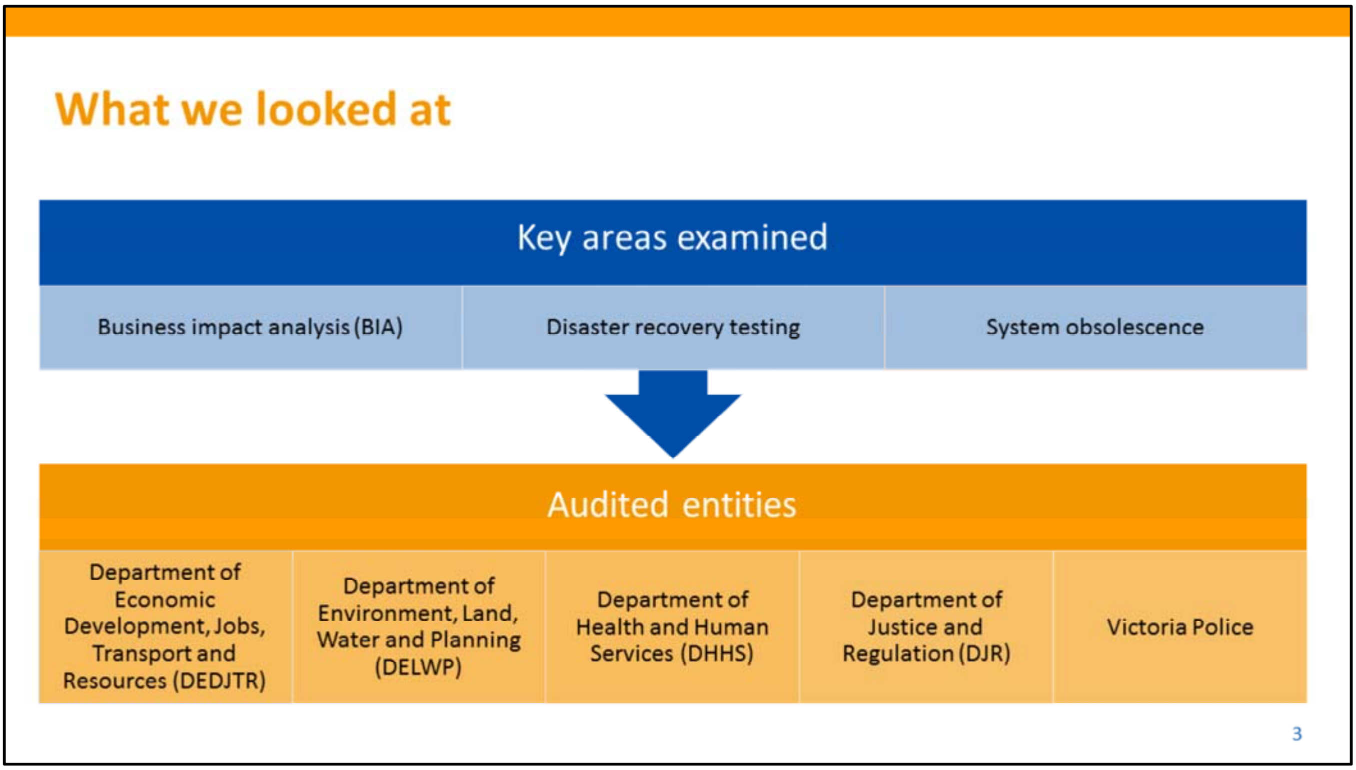
The process for recovering and restoring systems

Computer systems are critical for agencies to:

- deliver public services
- efficiently and effectively manage their operations; and
- fulfil their statutory obligations.

To ensure systems remain available and continue to operate reliably, agencies must be able to recover and restore them in the event of a disruption or disaster.

Information and communications technology (ICT) disaster recovery is the process for recovering and restoring systems.



What we looked at

Key areas examined

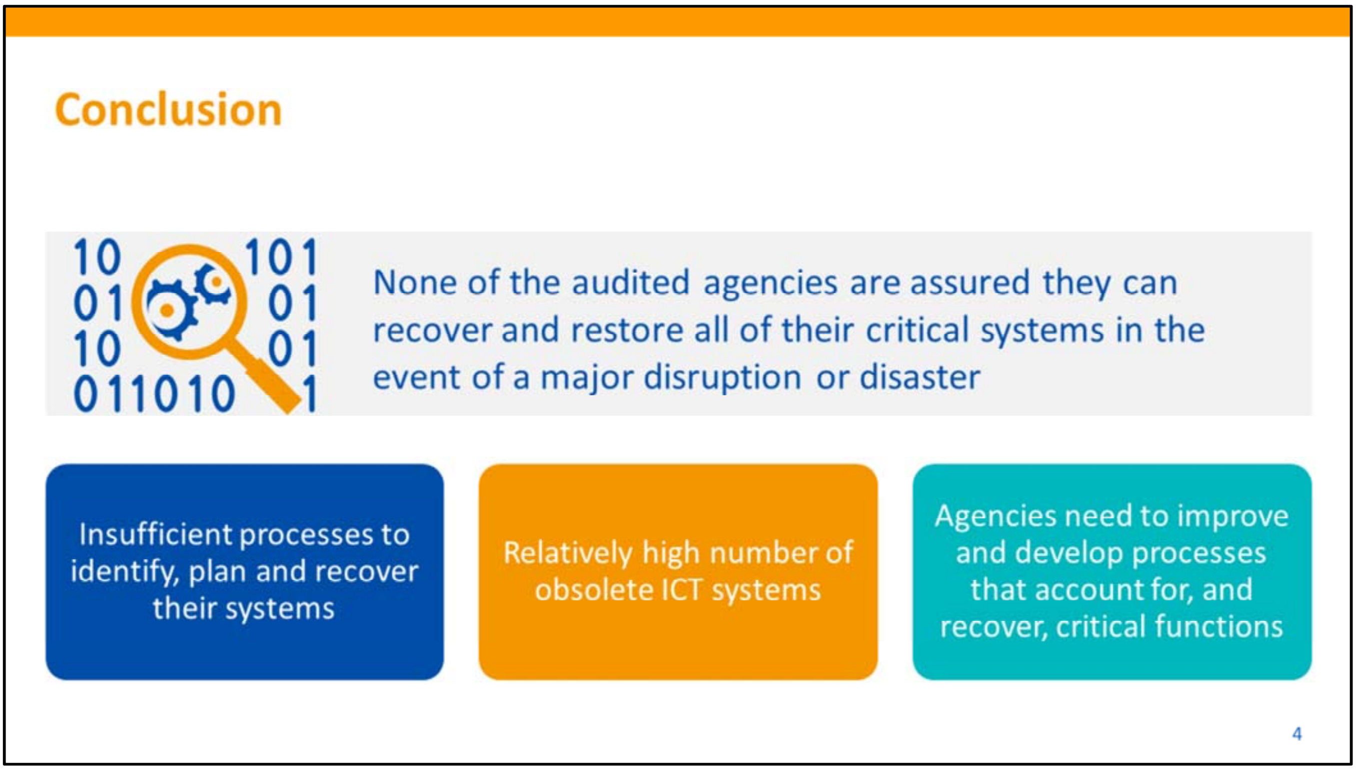
- Business impact analysis (BIA)
- Disaster recovery testing
- System obsolescence

Audited entities

- Department of Economic Development, Jobs, Transport and Resources (DEDJTR)
- Department of Environment, Land, Water and Planning (DELWP)
- Department of Health and Human Services (DHHS)
- Department of Justice and Regulation (DJR)
- Victoria Police

In this audit, we assessed whether sampled agencies' ICT disaster recovery processes are likely to be effective in the event of a disruption.

We examined disaster recovery at Victoria Police and four departments that provide essential government services—the Department of Economic Development, Jobs, Transport and Resources, the Department of Environment, Land, Water and Planning, the Department of Health and Human Services, and the Department of Justice and Regulation.



Conclusion

None of the audited agencies are assured they can recover and restore all of their critical systems in the event of a major disruption or disaster

Insufficient processes to identify, plan and recover their systems

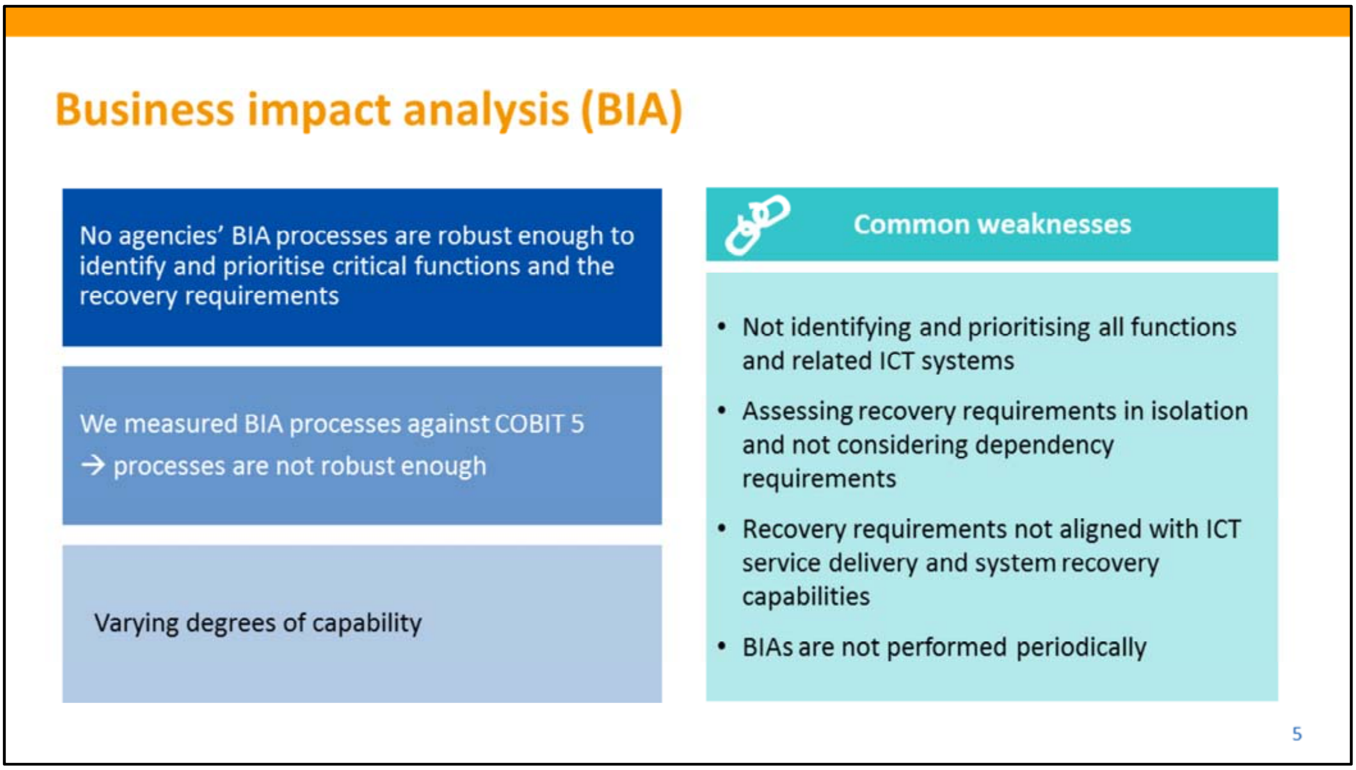
Relatively high number of obsolete ICT systems

Agencies need to improve and develop processes that account for, and recover, critical functions

None of the audited agencies have sufficient assurance that they can recover and restore all of their critical systems to meet business requirements in the event of a disruption.

Agencies do not have sufficient and necessary processes to identify, plan and recover their systems. Compounding this is the relatively high number of obsolete ICT systems agencies are still using to deliver some of their critical business functions.

Agencies need to significantly improve and develop well-resourced and established processes that can recover their critical business functions following a disruption.



Business impact analysis (BIA)

No agencies' BIA processes are robust enough to identify and prioritise critical functions and the recovery requirements

We measured BIA processes against COBIT 5
→ processes are not robust enough

Varying degrees of capability

Common weaknesses

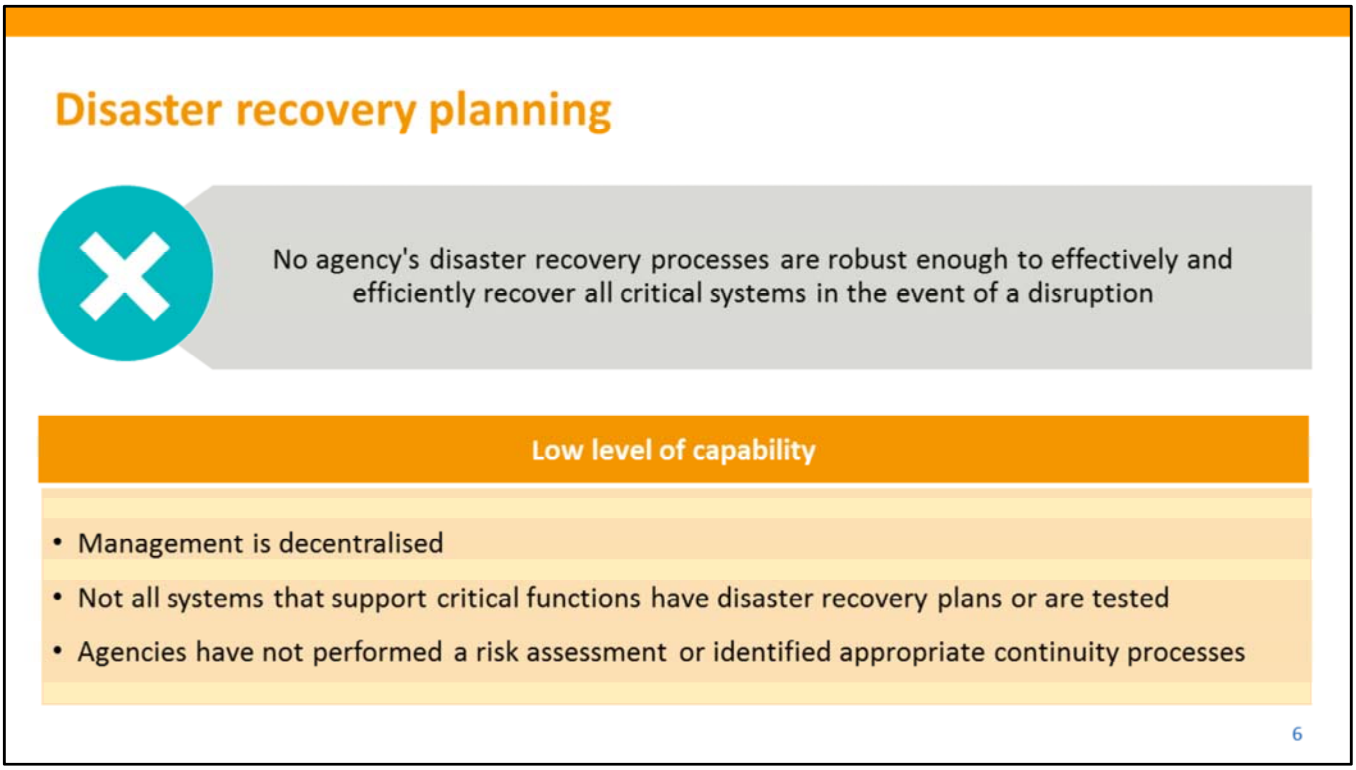
- Not identifying and prioritising all functions and related ICT systems
- Assessing recovery requirements in isolation and not considering dependency requirements
- Recovery requirements not aligned with ICT service delivery and system recovery capabilities
- BIAs are not performed periodically

A business impact analysis (BIA) identifies what business functions are critical to the daily operations of an agency and the required resources it needs to operate (e.g. systems). The BIA identifies how much time business functions have to return to full or the acceptable degraded level of operation following a disruption.

We measured agencies' BIA processes against COBIT 5, a globally accepted processes assessment model and found their processes are not robust enough to identify and prioritise their critical business functions and the recovery requirements for related systems.

Their processes have varying degrees of capability with several common weaknesses including:

- not identifying and prioritising all business functions and related ICT systems
- assessing recovery requirements in isolation and not identifying and considering system dependency requirements
- not aligning systems' recovery requirements with ICT service delivery and system recovery capabilities; and
- not performing BIAs periodically.



Disaster recovery planning

✖ No agency's disaster recovery processes are robust enough to effectively and efficiently recover all critical systems in the event of a disruption

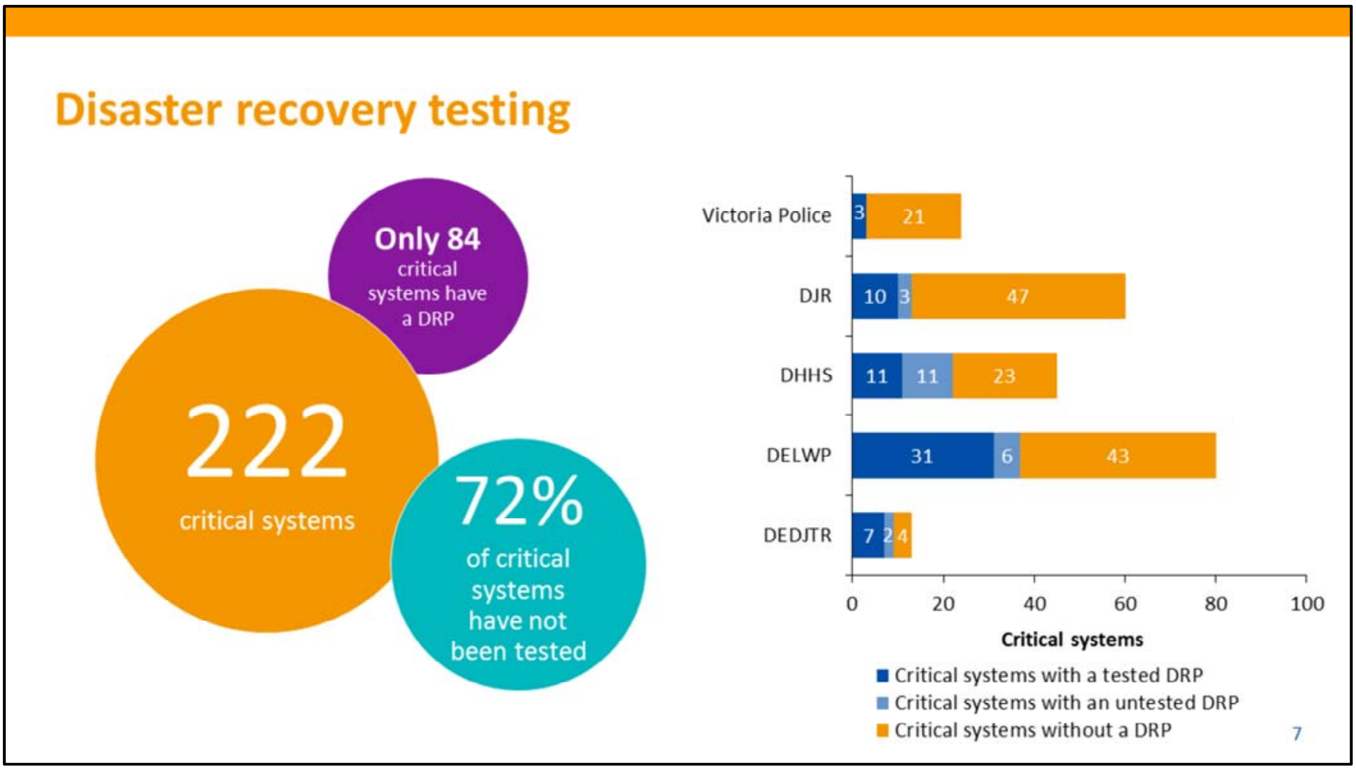
Low level of capability

- Management is decentralised
- Not all systems that support critical functions have disaster recovery plans or are tested
- Agencies have not performed a risk assessment or identified appropriate continuity processes

We also measured agencies' disaster recovery processes against COBIT 5 and found their processes are not robust enough to effectively and efficiently recover all critical systems in the event of a disruption.

The disaster recovery processes show low levels of capability. For example:

- management of ICT disaster recovery planning is decentralised and managed by individual divisions
- not all systems that support critical functions have disaster recovery plans or are tested; and
- agencies have not performed a risk assessment to determine which critical systems need a disaster recovery plan, or identified appropriate continuity processes for when systems are unavailable.



Disaster recovery testing

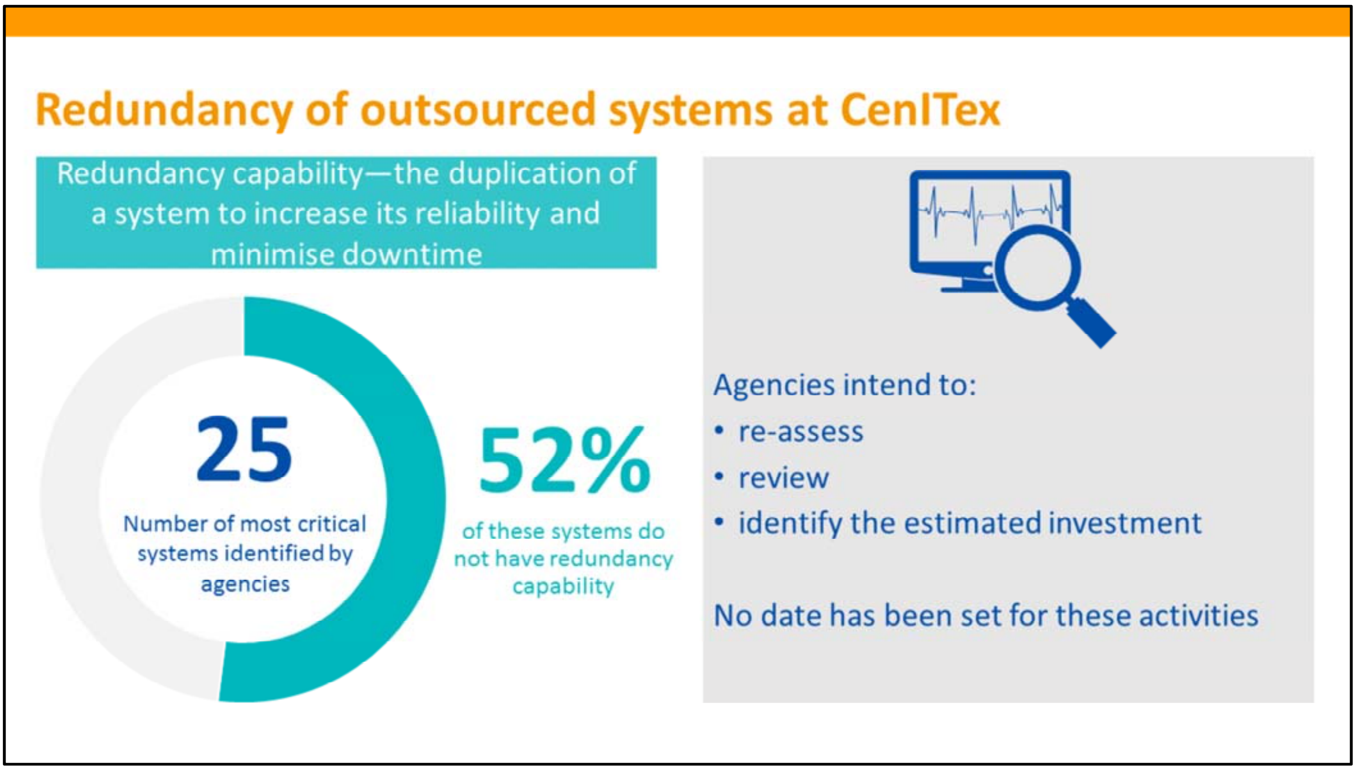
Only 84 critical systems have a DRP

222 critical systems

72% of critical systems have not been tested

None of the audited agencies have performed disaster recovery testing for all systems that support critical business functions. For agencies that do conduct testing, they are performed for selected systems and are not tested consistently.

Based on the analysis of data gathered from audited agencies—222 critical systems have been identified, but only 84 critical systems have a disaster recovery plan and only 62 have been tested. The results are shown on the graph on this slide.



Redundancy of outsourced systems at CenITex

Redundancy capability—the duplication of a system to increase its reliability and minimise downtime

25

Number of most critical systems identified by agencies

52%

of these systems do not have redundancy capability

Agencies intend to:

- re-assess
- review
- identify the estimated investment

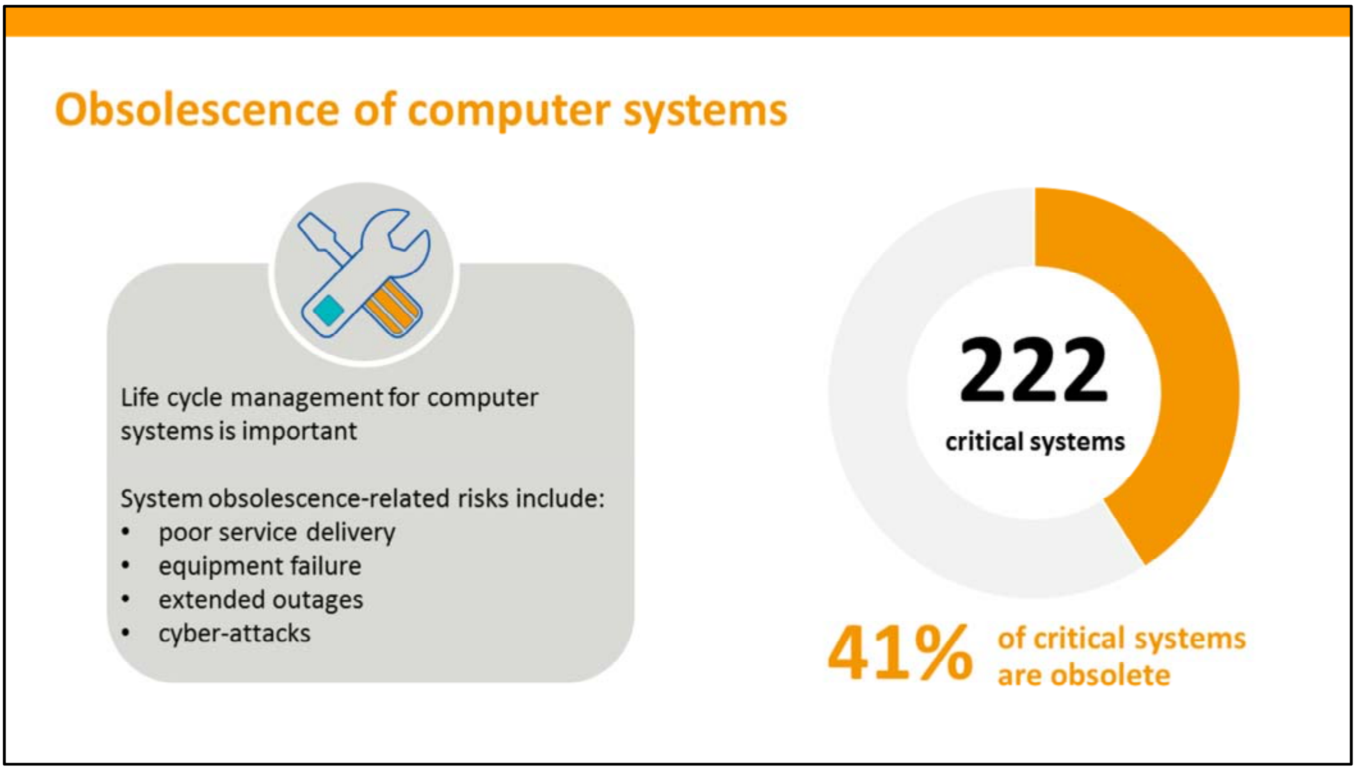
No date has been set for these activities

Six of the seven departments outsource the hosting of majority of their systems to CenITex.

CenITex reported that:

- only nine out of the 25 most important systems identified by agencies hosted at CenITex have secondary stand-by systems to provide a full and rapid recovery; and
- thirteen systems have no redundancy capability—including systems that provide services for criminal justice, marine safety and bushfire management.

Agencies intend to reassess 25 of their most important systems, review their order of priority, and identify the estimated investment required to establish and maintain an appropriate level of redundancy. No date has been set for this activity to occur.



Obsolescence of computer systems

Life cycle management for computer systems is important

System obsolescence-related risks include:

- poor service delivery
- equipment failure
- extended outages
- cyber-attacks

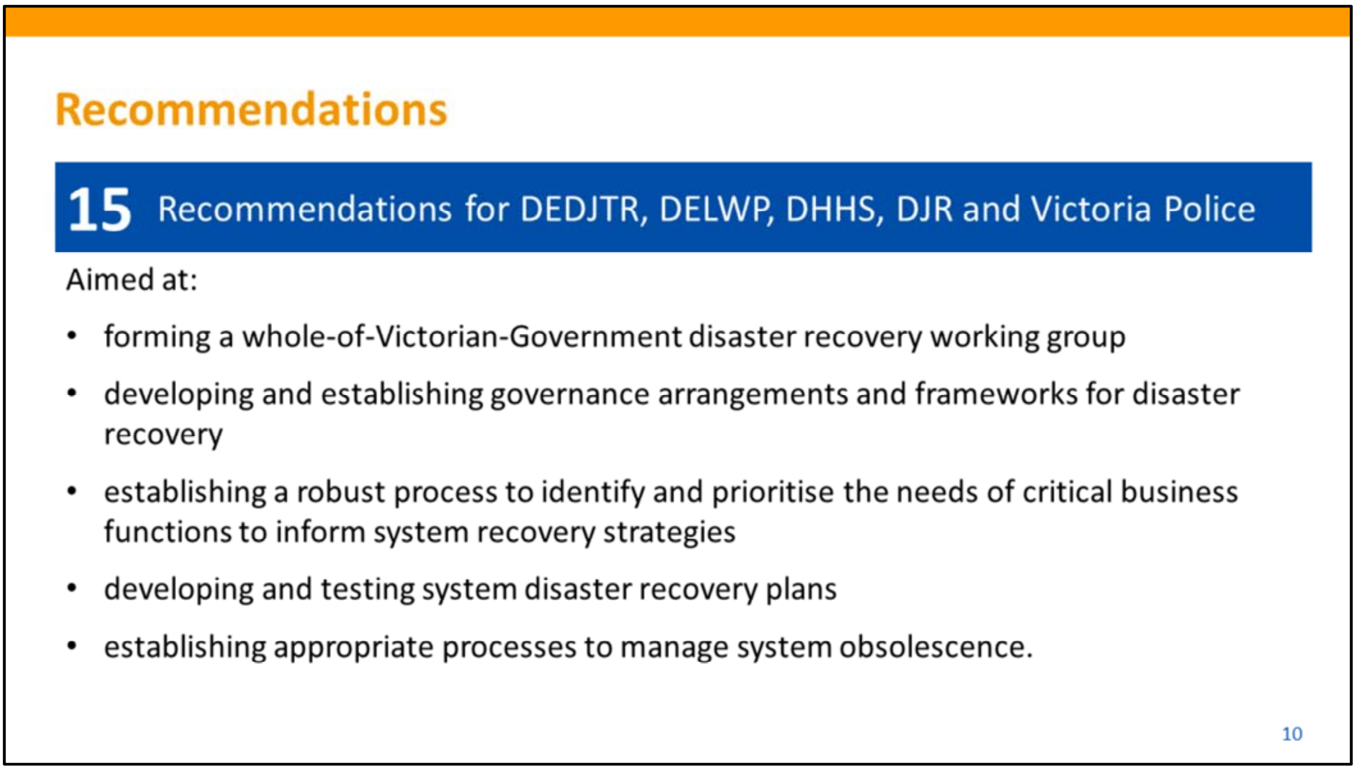
222

critical systems

41% of critical systems are obsolete

Life cycle management for computer systems is important due to the high speed of innovation and relatively short life spans. They can quickly become obsolete if not managed carefully, potentially leading to poor service delivery, equipment failure, extended outages or cyber-attacks.

Based on the analysis of data gathered from audited agencies, 41% of systems that support critical business functions are obsolete.



Recommendations

15 Recommendations for DEDJTR, DELWP, DHHS, DJR and Victoria Police

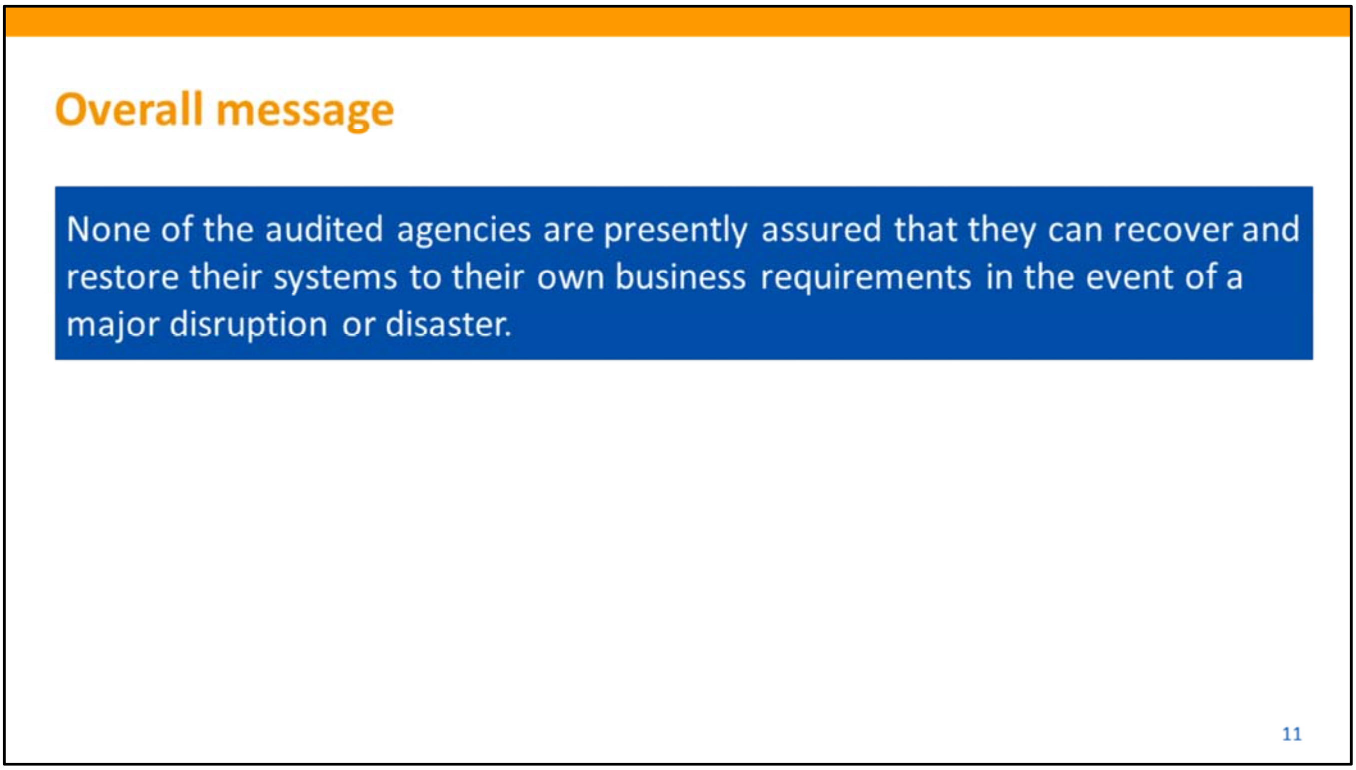
Aimed at:

- forming a whole-of-Victorian-Government disaster recovery working group
- developing and establishing governance arrangements and frameworks for disaster recovery
- establishing a robust process to identify and prioritise the needs of critical business functions to inform system recovery strategies
- developing and testing system disaster recovery plans
- establishing appropriate processes to manage system obsolescence.

We made 15 recommendations aimed at:

- forming a whole-of-Victorian-Government disaster recovery working group
- developing and establishing governance arrangements and frameworks for disaster recovery
- establishing a robust process to identify and prioritise the needs of critical business functions to inform system recovery strategies
- developing and testing system disaster recovery plans
- establishing appropriate processes to manage system obsolescence.

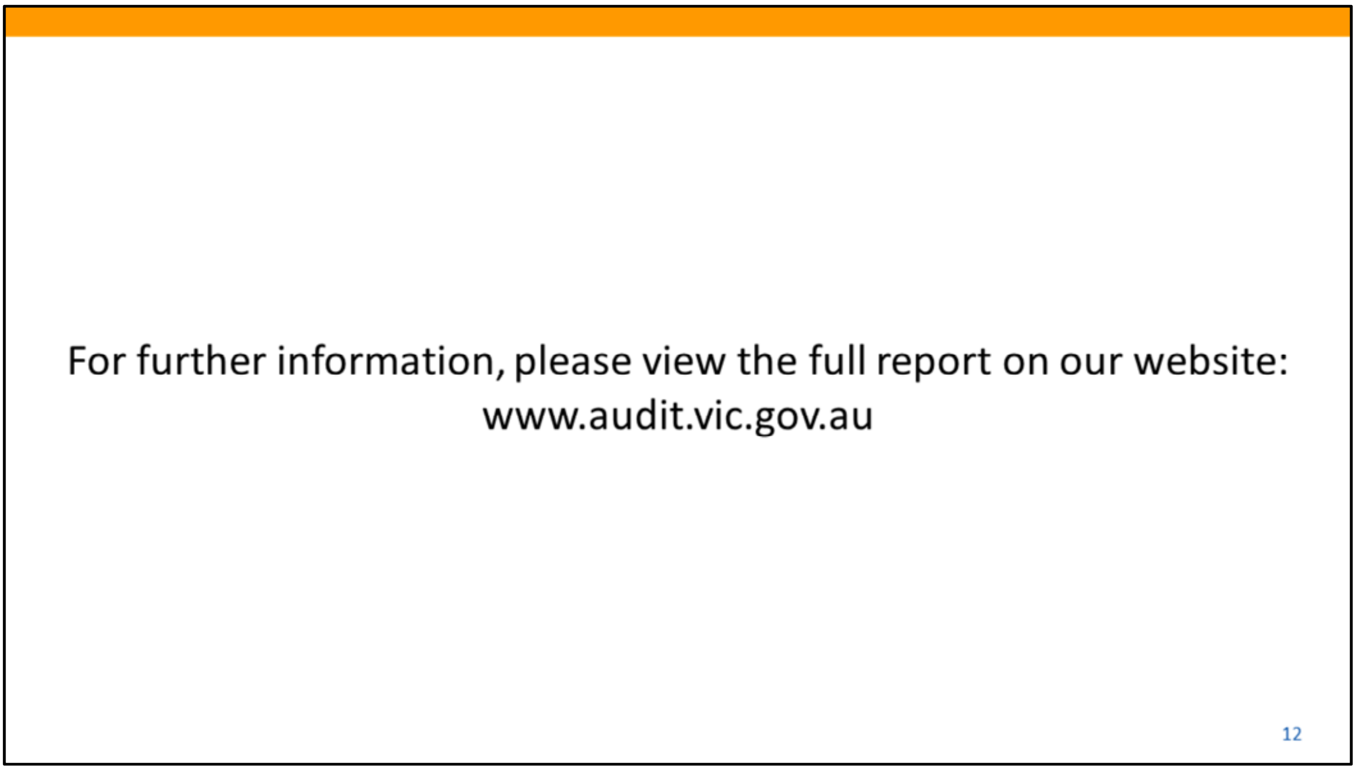
The audited agencies have provided detailed action plans and have started to address our recommendations.



Overall message

None of the audited agencies are presently assured that they can recover and restore their systems to their own business requirements in the event of a major disruption or disaster.

In summary, none of the audited agencies are presently assured that they can recover and restore their systems to their own business requirements, in the event of a major disruption or disaster.



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.