[P.P.4ZD

Government
of South Australia

# Report

of the

# Auditor-General

Supplementary Report

for the

year ended 30 June 2017

---

Tabled in the House of Assembly and ordered to be published, 28 November 2017

Second Session, Fifty-Third Parliament

## Disaster recovery planning: November 2017

By authority: Sinead O'Brien, Government Printer, South Australia

2017

General enquiries to:

Auditor-General
Auditor-General's Department
Level 9
State Administration Centre
200 Victoria Square
Adelaide SA 5000

www.audit.sa.gov.au

ISSN 0815-9157

Government of South Australia
Auditor-General's Department

Level 9
State Administration Centre
200 Victoria Square
Adelaide SA 5000
DX 56208
Victoria Square
Tel +618 8226 9640
Fax +618 8226 9688
ABN 53 327 061 410
audgensa@audit.sa.gov.au
www.audit.sa.gov.au

27 November 2017

The Hon R P Wortley MLC
President
Legislative Council
Parliament House
ADELAIDE SA 5000

The Hon M J Atkinson MP
Speaker
House of Assembly
Parliament House
ADELAIDE SA 5000

Dear President and Speaker

**Report of the Auditor-General: Supplementary Report for the year ended 30 June 2017 'Disaster recovery planning: November 2017'**

As required by the *Public Finance and Audit Act 1987*, I present to each of you the Auditor-General's Supplementary Report for the year ended 30 June 2017 'Disaster recovery planning: November 2017'.

**Content of the Report**

Part A of the Auditor-General's Annual Report for the year ended 30 June 2017 referred to audit work that would be subject to supplementary reporting to Parliament.

This Supplementary Report provides detailed commentary and audit observations on a review to determine whether SA Government agencies have implemented sufficient processes and controls to recover their key information assets following a disaster or significant business disruption.

**Acknowledgements**

The audit team for this report was Andrew Corrigan, James Baker, Brenton Borgman and Tyson Hancock.

We also appreciate the cooperation and assistance given by staff of the agencies we reviewed.

Yours sincerely

Ian McGlen
**Acting Auditor-General**

# Contents

# 1 Executive summary

## 1.1 Introduction

IT disaster recovery planning ensures that organisations can maintain or recover their important IT systems in the event of interruption. For SA Government agencies, these systems often support essential community services or public administration.

Effective disaster recovery planning helps agencies to recover important IT systems within expected time frames. How quickly these systems need to be recovered depends on the business processes they support.

The objective of this review was to determine whether SA Government agencies have implemented sufficient processes and controls to recover their key information assets following a disaster or significant business disruption.

To assess this, we reviewed the disaster recovery arrangements of 19 agencies, each differing in size and in the complexity of their operations.

## 1.2 Conclusion

Implementing disaster recovery controls has an associated cost. As with all areas of activity, agencies have to decide their IT operational and risk management priorities and where to focus their limited financial and human resources.

Within these constraints, agencies need to apply appropriate disaster recovery controls relative to their risks, especially for their key business systems. This is just as important for agencies that outsource components of their IT infrastructure and support.

Our review identified that most SA Government agencies have implemented some disaster recovery controls, including secondary data centre sites to maintain operations for their key IT systems in a disaster. A number of agencies we reviewed were strengthening their recovery arrangements following SA's state-wide power outage in September 2016.

However, based on our overall findings, we concluded that many of the agencies we reviewed had not implemented sufficient processes and controls to mitigate their key disaster recovery risks.

Without sufficient controls in place, agencies may not be able to recover their key business systems within expected time frames. This increases the risk of disruption to important public services.

## 1.3 What we found

**Figure 1.1: Summary of our findings for the 19 agencies reviewed**

**Plans and procedures**
Section 4

- Six agencies did not have a disaster recovery plan for some or all of their systems, with plans at a further 10 agencies in draft or needing review
- Nine agencies did not have detailed recovery procedures for all systems, or the procedures were insufficient

**Recovery arrangements**
Section 5

- 12 agencies did not have recovery time and point objectives* defined for some or all of their systems
- Eight agencies did not define maximum allowable outage times for some or all of their key business processes
- Three agencies had not implemented sufficient secondary site arrangements

**Disaster recovery testing**
Section 6

- 14 agencies did not maintain formal disaster recovery testing schedules for all key business systems
- Only one agency conducted full disaster recovery testing for its key systems, with 16 agencies partially testing their recovery arrangements
- Two agencies did not conduct any disaster recovery testing

**Skillsets and risk assessments**
Section 7

- 10 agencies could not demonstrate they had sufficient IT resources to effectively conduct disaster recovery activities
- Six agencies had not conducted a recent disaster recovery plan risk assessment to identify potential threats to data, hardware and supporting environments

* Refer section 2.2 for an explanation of recovery time and point objectives.

## 1.4 What we recommended

Our recommendations to agencies, depending on their particular circumstances, included:

- developing, approving and implementing disaster recovery plans for all key business systems
- regularly reviewing these plans to ensure that they reflect the current operating environment
- developing detailed recovery procedures
- defining recovery time objectives and recovery point objectives for key business systems
- scheduling disaster recovery tests for key business systems regularly, in line with their importance

- documenting results and recommendations from disaster recovery tests
- assessing the availability and skillsets of the resources needed to respond to a major disaster recovery event
- upskilling IT resources through disaster recovery testing or formal training
- conducting a risk assessment of disaster recovery plans for key business systems
- documenting disaster recovery risks in agency risk registers, along with controls and treatment plans.

## 1.5 Response to our recommendations

We considered the views of all 19 agencies during our review. Most agencies responded positively to our findings, providing details of how they plan to remediate the issues we identified and/or any remediation activities already completed. In some cases, approved funding and certain prerequisite activities are required to address the findings. One agency in particular cited underfunding and a lack of resourcing as the reasons for their control deficiencies.

Some agencies confirmed their arrangements with specific service providers who assist them with aspects of disaster recovery. They also reiterated reasons for their existing disaster recovery arrangements and mitigating controls.

In particular, one agency stressed that it was prudent to consider the level of resources, appropriate controls and ongoing activity that can reasonably be applied by smaller agencies. Despite agreeing with our findings, another agency responded that its business continuity and disaster recovery systems and processes are consistent with the nature and extent of its functions.

Not all agencies responded with clear target dates for remediation. However, where provided, they expected to remediate most issues by the end of 2018.

We thank the 19 agencies reviewed for their cooperation during the review.

# 2 Background

## 2.1 What is disaster recovery planning?

IT disaster recovery planning is a key element of an organisation's internal control system. It ensures that important IT systems and services are available in the event of interruption, or helps to restore these services when required.

Examples of interruption may include losing access to a key IT system, network connections or important data. A disaster recovery event may also involve losing access to an entire building or data centre.

It is vital that SA Government agencies can access and process their data promptly to avoid disruption to important community services, as well as financial loss or reputational risks. Therefore, planning for disasters is an important part of the risk management process.

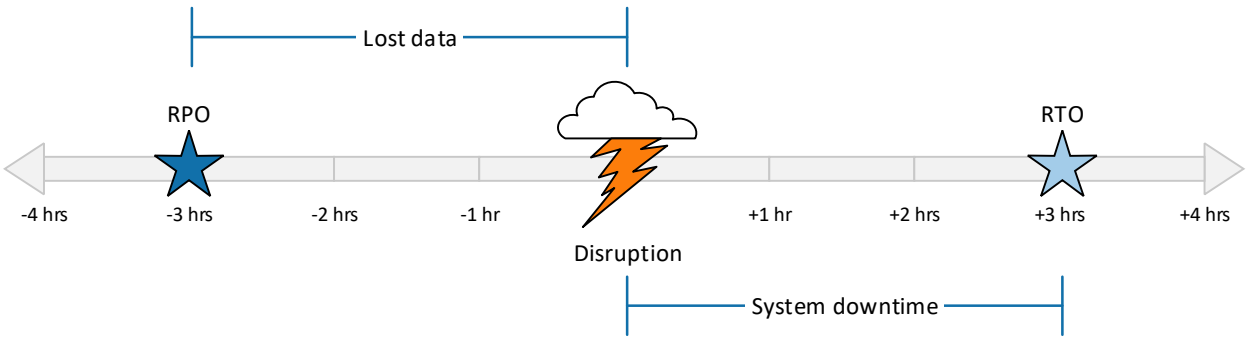
The question of whether individual applications or IT services need to remain available depends on the importance of the business processes they support.

## 2.2 Key disaster recovery concepts

### Recovery time and point objectives

Individual IT systems should be assigned recovery time objectives (RTOs) and recovery point objectives (RPOs), as shown in figure 2.1. This helps to set expectations about the required time to restore a key business system and the potential extent of lost data.

**Figure 2.1: Recovery time and point objectives**



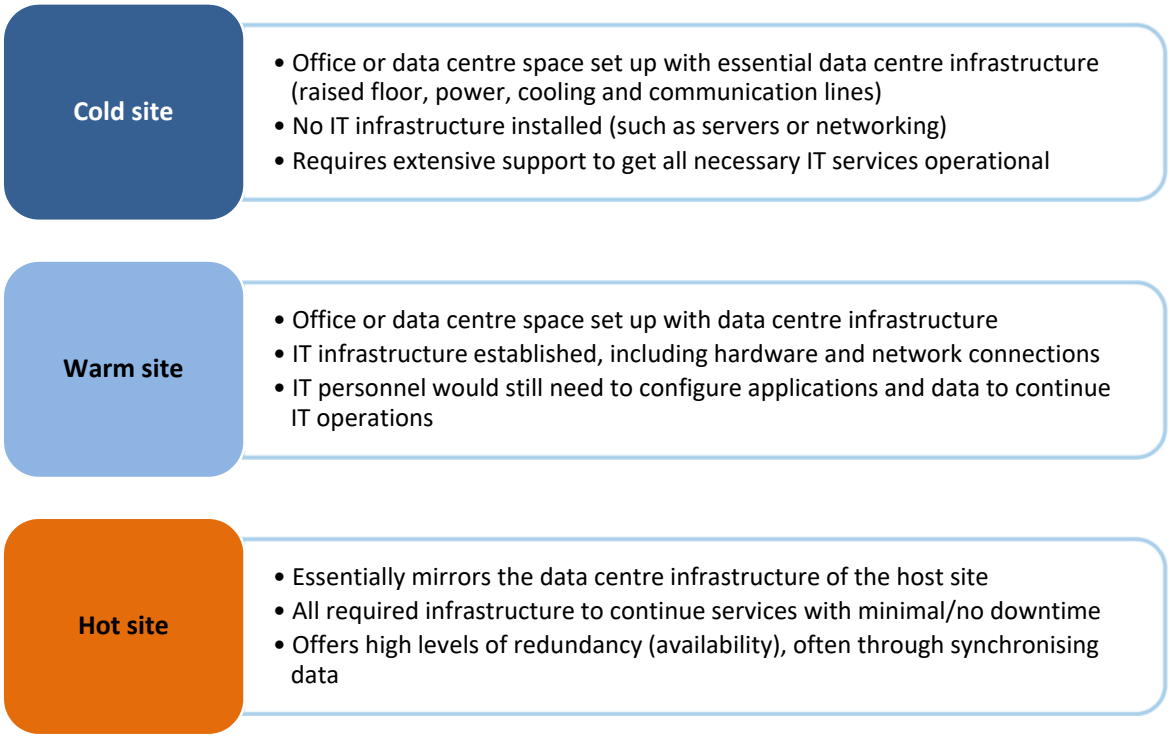

**RPO** – the amount of data that could potentially be lost during a disaster

**RTO** – the length of time it will take to restore a key business system after a failure or disaster occurs

### Secondary site arrangements

If an agency's primary data centre becomes unavailable, it may use alternative facilities at a secondary site to maintain key IT services. These secondary sites are typically categorised as shown in figure 2.2.

**Figure 2.2: Typical categories of secondary sites**




Typically, the lower the established RTOs and RPOs, the greater the ongoing cost is to an agency. This is because of additional IT infrastructure requirements for a hot secondary site to provide minimal or no loss of data and system functionality.

Therefore, agencies need to consider the benefits of increased redundancy against the increased costs, as well as the importance of the business process that the IT service supports.

## 2.3 Disaster recovery and business continuity

Whereas disaster recovery planning focuses on IT services, business continuity planning focuses on business processes. It enables agencies to continue offering services in the event of a disruption by maintaining their important business processes.

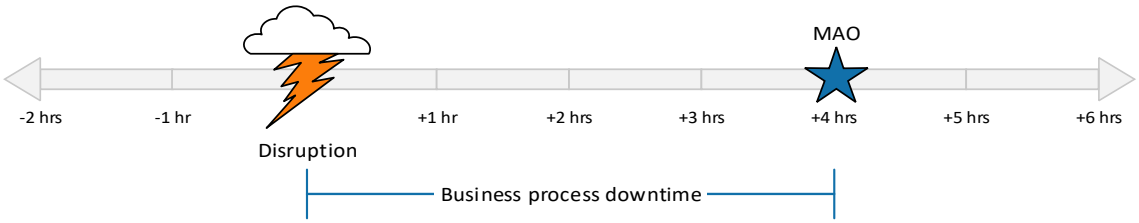
Key differences between IT disaster recovery and business continuity planning are highlighted in figure 2.3.

**Figure 2.3: Differences between disaster recovery and business continuity planning**

| Attribute | Disaster recovery planning | Business continuity planning |
|---|---|---|
| **Typical owner** | ICT | Business units |
| **Focus** | Recovering IT systems in a disaster | Maintaining important business functions |
| **Key metrics** | RTO – time to restore a key system<br>RPO – potential data loss | Maximum allowable outage time |
| **Plan informed by** | Business requirements, as outlined in the business continuity plan<br>IT risk assessment | Business impact assessment |

Given that most business processes heavily rely on IT systems, it is important that there is consistency between business continuity and disaster recovery arrangements. Specifically, the business continuity plan should identify important business functions and the maximum allowance outage time for each function. The maximum allowable outage time is the maximum time that an agency can tolerate the disruption of an important business function before there is a significant impact on its operations.

**Figure 2.4: Maximum allowable outage time**




**MAO** – maximum allowable outage: the maximum length of time that can elapse before a business process outage is considered unacceptable or intolerable.

The MAO time should be greater than the RTO (refer to figure 2.1).

The RTOs specified in the IT system disaster recovery plan should align with maximum allowance outage times. This ensures that IT systems can be recovered within acceptable business time frames.

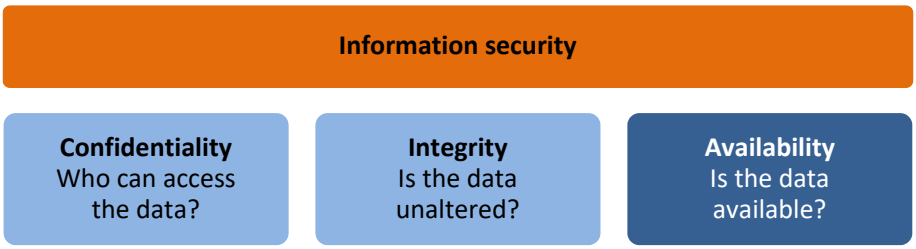
## 2.4 Information security concepts and standards

### General concepts

Information security refers to processes and methodologies designed and implemented to protect any form of confidential, private and sensitive information from unauthorised access, use, disclosure, disruption, modification or destruction.

Accordingly, disaster recovery planning is a key component in ensuring the availability of systems and data, as shown in figure 2.5.

**Figure 2.5: Overview of key information security components**




## ISO 27001

ISO 27001[1] is an international specification detailing best practice requirements for establishing, implementing, maintaining and continually improving an information security management system.

An information security management system aims to preserve the confidentiality, integrity and availability of information by applying a risk management process. Implementing one gives stakeholders confidence that organisations adequately manage risks and fully understand agency assets/systems. Stakeholders may also gain confidence through certification processes.

ISO 27001 includes requirements for implementing disaster recovery controls as part of information security continuity. It requires that information security continuity is integrated into an organisation's business continuity management system. This includes the control objectives shown in figure 2.6.

**Figure 2.6: Key ISO 27001 control objectives related to disaster recovery planning**

| | |
|---|---|
| **Planning** | • Determine requirements for information security and the continuity of information security management in adverse situations, such as a crisis or disaster |
| **Implementation** | • Establish, document, implement and maintain processes, procedures and controls to ensure the required level of continuity for information security during an adverse situation |
| **Verification** | • Verify, review and evaluate information security continuity controls at regular intervals in order to ensure that they are valid and effective during adverse situations |
| **Availability** | • Implement sufficient redundancy to meet availability requirements for information processing facilities |

[1] International Organization for Standardization 2016, ISO/IEC 27001 Information Security Management, viewed 11 October 2017, <http://www.iso.org/iso/home/standards/management-standards/iso27001.htm>.

### Information Security Management Framework

The mandatory SA Government Information Security Management Framework is a Cabinet-approved document that describes 40 policies and 140 standards in support of contemporary industry practices for the security of information stored, processed, transmitted or otherwise manipulated using ICT. It requires agencies to implement whatever control measures are necessary to provide adequate protection for their information and associated assets.

Standard 122 states that agencies must establish a process to maintain business continuity and disaster recovery. This should incorporate information security considerations, and the allocation of responsibilities and resources, to appropriately support the business continuity management processes.

The Information Security Management Framework also requires agencies to protect against external and environmental threats, particularly with respect to data backup, disaster recovery activities and restoration capabilities.

## 2.5 Recent developments

On 28 September 2016, South Australia experienced an extreme weather event, triggering a state-wide power outage. Although power was restored to Adelaide within several hours, large areas of the State remained without power for several days.

After this event, the SA Government commissioned an independent review[2] of the emergency management response, led by former South Australia Police Commissioner Gary Burns.

This review identified that many business continuity plans within government departments, including emergency services, proved to be inadequate. This is because the plans lacked contingencies for backup power, or the planned contingencies failed. The review identified that government agency responses to the blackout were quite varied, as was their ability to function and continue providing essential services. In some cases, staff did not know what was required or have an understanding of the documented plans they should have followed.

Findings from this review reiterated the need for agencies to implement effective disaster recovery arrangements for important IT systems, as part of a broader approach for managing agency business continuity.

## 2.6 Responsibilities for disaster recovery

Generally, individual SA Government agencies are responsible for their own disaster recovery arrangements. However, in some cases, responsibilities are shared with another

[2] Burns, G, Adams, L & Buckley, G 2017, *Independent review of the extreme weather event: South Australia 28 September – 5 October 2016*, Government of South Australia, accessed 28 September 2017, <http://www.dpc.sa.gov.au/__data/assets/pdf_file/0003/15195/Independent-Review-of-Extreme-Weather-complete.pdf>.

agency or an external vendor:

- **Distributed Computing Support Services (DCSS) arrangements** – most agencies have servers under the DCSS arrangements. Servers are maintained by an external vendor and are hosted at data centres, such as the central data centre at Glenside. As part of the service contract, the vendor is responsible for aspects of disaster recovery planning, particularly at the network and operating system level. Individual agencies remain responsible for recovering applications.
- **SA Government mainframe** – a number of agencies use Masterpiece for financial and general ledger functions, hosted on the SA Government mainframe. Masterpiece is managed centrally by Shared Services SA for most agencies, with an external vendor providing disaster recovery support.
- **Justice Technology Services** – some systems used by agencies in the Justice portfolio are managed centrally by Justice Technology Services. Justice Technology Services manages disaster recovery for these systems.
- **Cloud providers** – in instances where agencies use applications hosted by a cloud provider, they will generally rely on the provider to manage aspects of disaster recovery arrangements.

# 3 Audit mandate, objective and scope

## 3.1 Our mandate

The Auditor-General has the authority to conduct this review under section 36(1)(a)(iii) of the *Public Finance and Audit Act 1987*.

## 3.2 Our objective

The objective of this review was to determine whether SA Government agencies have implemented sufficient processes and controls to recover their key information assets following a disaster or significant business disruption.

To do this, we assessed whether:

- agencies have implemented disaster recovery plans and detailed recovery procedures for all key business systems, including documented roles and responsibilities and clear communication plans
- suitable recovery arrangements have been implemented for key business systems, such as secondary sites
- recovery arrangements are based on defined recovery objectives, as well as linkage with relevant business continuity plans
- agencies regularly test disaster recovery arrangements for key systems, with testing outcomes documented
- agencies have assessed their IT skillsets to effectively conduct disaster recovery activities
- agencies have identified, assessed and treated disaster recovery-related risks.

## 3.3 What we reviewed and how

Key information assets are part of an agency's important infrastructure. This includes systems, services and functions that are fundamental to the ongoing functioning and survivability of an organisation.[3]

In 2016 we sent a questionnaire to the following agencies requesting details of their disaster recovery processes and controls for their key information assets:

- Attorney-General's Department (AGD)
- Courts Administration Authority (CAA)
- Department for Communities and Social Inclusion (DCSI)
- Department for Correctional Services (DCS)

[3] Government of South Australia 2017, *Information Security Management Framework*, version 3.3, accessed 28 September 2017, <https://digital.sa.gov.au/sites/default/files/content_files/policy/ISMF-v3.3.pdf>.

- Department for Education and Child Development (DECD)
- Department for Health and Ageing (SA Health)
- Department of Environment, Water and Natural Resources (DEWNR)
- Department of Planning, Transport and Infrastructure (DPTI)
- Department of Primary Industries and Regions (PIRSA)
- Department of State Development (DSD)
- Department of the Premier and Cabinet (DPC)
- Department of Treasury and Finance (DTF)
- Legal Services Commission (LSC)
- Public Trustee (PT)
- SACE Board of South Australia (SACE Board)
- South Australia Police (SAPOL)
- South Australian Fire and Emergency Services Commission (SAFECOM)
- South Australian Tourism Commission (SATC)
- South Australian Water Corporation (SA Water).

These 19 agencies were selected to include both large and small agencies, ensuring we capture a reasonable cross-section of the SA Government.

In 2017 we validated the information agencies provided by reviewing relevant documentation and meeting with nominated agency staff.

For DPTI, we focused our assessment on the following systems, which were managed by separate business units:

- computerised train control system
- heavy rail and light rail traction supervisory control and data acquisition (SCADA)[4] systems
- traffic management systems
- Transport Regulation User Management Processing System (TRUMPS)
- South Australian Integrated Land Information System (SAILIS).

For DPC, we focused on Masterpiece (accounts payable, accounts receivable and general ledger), e-Procurement (purchase management and invoice processing) and Chris21 (payroll).

## 3.4 What we did not review

Given that the focus of our review was on disaster recovery planning, we did not review agency business continuity plans in detail. However, where agencies did not have business continuity plans or they did not link sufficiently with disaster recovery plans, we have included this in our findings.

[4] SCADA – Supervisory control and data acquisition. SCADA systems are used to monitor and control a plant or equipment in industries such as telecommunications, water, energy and transportation. These systems tend to be classified as important to government to provide essential services to the community.

During our review, we requested that agencies provide us with lists of their key information assets. This informed our testing approach, however we did not review whether these asset lists were complete.

As previously mentioned, our reviews at DPC and DPTI were limited to specific information systems.

When presenting our findings, we did not attempt to rank agencies' disaster recovery maturity. This was due to the differences in each agency's size and resourcing, business requirements, and the complexity and importance of their IT environments.

# 4 Plans and procedures

### What we found

- Some agencies did not have a disaster recovery plan.
- Some disaster recovery plans did not include all key business systems.
- Some disaster recovery plans were in draft or required updating.
- Some agencies had insufficient disaster recovery procedures.

### What we recommended

- Agencies should develop, approve and implement disaster recovery plans for all key business systems. They should regularly review these plans to reflect the current operating environment.
- Disaster recovery plans should include key information assets, defined responsibilities and clear communication plans.
- Agencies should develop detailed recovery procedures for all key business systems, including details about how to recover or failover business systems to the disaster recovery site if required. Procedures should cover the application itself, as well as supporting infrastructure, databases and networks.

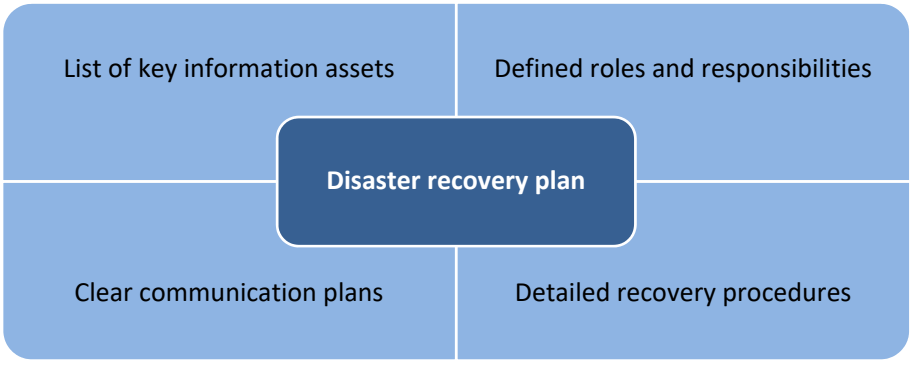
## 4.1 Introduction

Agencies need to formally document their disaster recovery arrangements in a disaster recovery plan. This ensures that staff are fully aware of how to recover key systems in a disaster. It also assists with retaining disaster recovery process expertise should key staff leave the agency.

Disaster recovery plans should be current, incorporate all key systems and be reviewed at least annually. Agencies should review their plans more frequently where they are implementing new systems, data centres and/or IT staff reorganisations.

Disaster recovery plans should include several key components, as shown in figure 4.1.

**Figure 4.1: Key components of a disaster recovery plan**



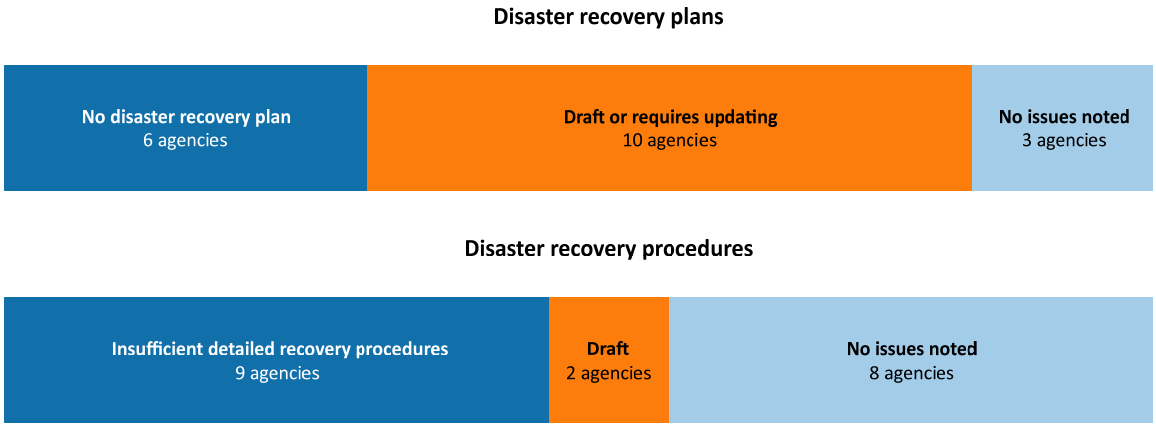
Communication plans should include details about notifying affected staff in the event of a disaster, as well as a clear escalation process. The disaster recovery plan should also outline roles and responsibilities in the event of a disaster. Staff should be made aware of their disaster recovery responsibilities through regular training sessions and regular disaster recovery testing (refer section 5).

Agencies also need to document detailed recovery procedures for all key business systems, whether as part of the overall disaster recovery plan or in separate documents. These documents should include step-by-step procedures about how to recover or failover business systems to the disaster recovery site if required. Procedures should cover the application itself, as well as supporting infrastructure, databases and networks.

## 4.2 Findings

### 4.2.1 Overview

**Figure 4.2: Overview of testing results for disaster recovery plans and procedures**




### 4.2.2 No disaster recovery plan exists or the plan does not incorporate all key business systems

#### Affected agencies

DCS, DECD, DEWNR, DPTI, DTF and SAFECOM.

#### Recommendation

Agencies should develop, approve and implement disaster recovery plans for all key business systems.

Plans should include key information assets, defined responsibilities, detailed recovery procedures and clear communication plans.

#### Finding

Six of the 19 agencies we reviewed did not have a disaster recovery plan implemented for some or all of their systems. Results for these agencies are summarised in figure 4.3.

Where agencies do not have documented disaster recovery plans for all key business systems, there is a risk that agencies cannot recover these systems within maximum allowable outage times in the event of a disaster or system failure.

**Figure 4.3: Results summary – agencies with no disaster recovery plan for some or all key business systems**

| Agency | Disaster recovery plans | | Comments |
|---|---|---|---|
| | Documented for key systems | Work underway to develop | |
| DCS | ✘ | – | • Most systems managed by third-party service providers.<br>• These systems have certain disaster recovery resilience capabilities built into external hosting environments. |
| DECD | ✘ | ✓ | • Disaster recovery plan development will be assisted by business continuity planning program work and recent indicative pricing for cloud-based disaster recovery services.<br>• DECD advised that most IT infrastructure is outsourced to SA Government IT service contracts. |
| DEWNR | ✘ | ✓ | • No overarching plan but some disaster recovery documentation and site failover plans exist.<br>• Improvements to its business continuity planning are being made by implementing a resilience management framework. |
| DPTI | ✘ | ✓ | • No disaster recovery plan for the computerised train control or rail traction SCADA systems.<br>• Plan being drafted for computerised train control system as part of Information Security Management Framework compliance work. |
| DTF | ✘ | ✓ | • Disaster recovery plan for IT network infrastructure maintained. However, documented and approved disaster recovery plans did not exist for all key business systems.<br>• Subsequent to our review, DTF advised us that it plans to update the disaster recovery plan in 2017-18 to include important business processes and systems. |
| SAFECOM | ✘ | – | • Responsible for conducting certain disaster recovery activities, including where business systems are managed by another SA Government agency or an external provider.<br>• No disaster recovery plan maintained. |

### 4.2.3 Disaster recovery plans in draft, outdated or needing review

#### Affected agencies

AGD, CAA, DPC, DPTI, DSD, LSC, PT, SACE Board, SAPOL, SATC and SA Water.

#### Recommendation

Agencies should approve and regularly review disaster recovery plans for all key business systems. These plans should reflect the current operating environment at each agency.

#### Finding

In addition to finding 4.2.2, the disaster recovery plans for a further 10 agencies were in draft, outdated or needed reviewing. Further, although one agency's plan included all systems and sufficient details, we noted that this plan had not been formally approved by management.

Results for these agencies are summarised in figure 4.4.

Where agencies do not have approved and regularly reviewed disaster recovery plans for all key business systems, there is a risk that they cannot recover these systems within maximum allowable outage times in the event of a disaster or system failure. Without formally documenting disaster recovery arrangements there is also a greater risk of knowledge loss if key IT staff leave the agency.

**Figure 4.4: Results summary – agencies with disaster recovery plans that require updating**

| Agency | Disaster recovery plans | | Comments |
|---|---|---|---|
| | Approved and reviewed | Include all systems and sufficient details | |
| AGD | ✘ | ✘ | • Some important processes and systems listed in AGD's business continuity plan not included in the disaster recovery plan.<br>• AGD is remediating a number of disaster recovery-related activities identified by an internal audit completed in March 2017. |
| CAA | ✘ | ✘ | • Disaster recovery plans for a number of key business systems still in draft. After our review, plans were developed for a number of these systems. |
| DPC | ✘ | ✓ | • Disaster recovery plans in place for mainframe and Chris21.<br>• Disaster recovery plan for e-Procurement systems in draft. |

| Agency | Disaster recovery plans | | Comments |
|---|---|---|---|
| | Approved and reviewed | Include all systems and sufficient details | |
| DPTI | ✘ | ✓ | • At the time of our review we could not obtain evidence that key stakeholders had formally reviewed and approved the TRUMPS disaster recovery plan. DPTI has since advised, however, that disaster recovery is now a standing agenda item in its TRUMPS Governance Committee meetings.<br>• The SAILIS disaster recovery plan was last updated in April 2015 and was being updated to provide further clarification. |
| DSD | ✘ | ✘ | • DSD implemented a new secondary warm site in 2017 after the separation of the DSD and TAFE SA production environments. Our review of disaster recovery commenced prior to the full implementation of this program of work.<br>• Disaster recovery plan needs to be updated to reflect these recent changes in secondary site arrangements and how systems will be recovered. |
| LSC | ✘ | ✘ | • Disaster recovery plan not updated since November 2012.<br>• LSC engaged an external service provider to develop a disaster recovery plan. Plan yet to be updated to reflect service provider recommendations. |
| PT | ✓ | ✘ | • Disaster recovery plan was quite brief in nature and needed to be enhanced to provide a clearer representation of the current approach. This includes details of specific systems. |
| SACE Board | ✓ | ✘ | • A disaster recovery plan exists, with detailed recovery testing procedures for its key online business systems.<br>• However, the document did not include plans for recovering several other key business systems. |

| Agency | Disaster recovery plans | | Comments |
|---|---|---|---|
| | Approved and reviewed | Include all systems and sufficient details | |
| SAPOL | ❶ | ✘ | • ❶ SAPOL places strong emphasis on its business continuity planning framework and command and control approach to respond to a disaster recovery event or system failure. It advised that its business continuity plans contain details of the process to recover failed IT infrastructure.<br>• In SAPOL's assessment, the above controls negated the need for an overarching disaster recovery plan. However, our review of SAPOL's business unit continuity plans noted they do not contain sufficient information to cover all aspects of an IT disaster recovery plan. Examples include documenting what events would invoke IT disaster recovery procedures, communication protocols and management structures, RTOs or RPOs applied to key business systems and reference to technical recovery procedures. |
| SATC | ✓ | ✘ | • Support for most of SATC's systems is managed by DPC and external service providers.<br>• Disaster recovery and business continuity plans maintained, which contain general information on SATC's current environment.<br>• However, the plan does not identify key business systems or document plans for recovery. |
| SA Water | ✘ | – | • Coordination plan for IT continuity planning is in draft. |

### 4.2.4 Insufficient disaster recovery procedures

#### Affected agencies

AGD, CAA, DPC, DPTI, DSD, PIRSA, SACE Board, SAFECOM, SAPOL, SATC and SA Water.

#### Recommendation

Agencies should develop detailed recovery procedures for all key business systems.

These documents should include step-by-step procedures about how to recover or failover business systems to the disaster recovery site if required. Procedures should cover the application itself, as well as supporting infrastructure, databases and networks.

## Finding

Nine of the 19 agencies we reviewed did not have detailed recovery procedures in place for all key business systems, or the procedures were insufficient.

A further two agencies reviewed had not formally completed and approved their detailed recovery procedures.

Results for these agencies are summarised in figure 4.5.

Where agencies do not have detailed recovery procedures for all key business systems, there is a risk that they cannot recover these systems within agreed recovery objectives in the event of a disaster or system failure. Without formally documenting disaster recovery arrangements, there is also a greater risk of knowledge loss if key IT staff leave the agency.

**Figure 4.5: Results summary – agencies with insufficient disaster recovery procedures**

| Agency | Detailed recovery procedures | | Comments |
|---|---|---|---|
| | Exist for key systems | Reviewed and approved | |
| AGD | ✘ | – | • Detailed recovery procedures not fully documented.<br>• Although the disaster recovery plan includes some procedures relating to tape and disk restore procedures, the recovery steps listed are only high-level and not system specific.<br>• AGD is remediating a number of disaster recovery-related activities identified by an internal audit completed in March 2017. |
| CAA | ✓ | ✘ | • Some procedures developed in 2015 but still in draft. |
| DPC | ✘ | – | • No detailed recovery procedures for e-Procurement systems. |
| DPTI | ✘ | ✘ | • No detailed recovery procedures for the computerised train control system or environment.<br>• DPTI is developing suitable procedures as part of information security management systems compliance work.<br>• At the time of our review, the rail traction SCADA system recovery procedures had not been reviewed since 2014. DPTI has since advised that there are current work instructions operators may refer to for maintenance purposes. |

| Agency | Detailed recovery procedures | | Comments |
|---|---|---|---|
| | Exist for key systems | Reviewed and approved | |
| DSD | ✘ | – | • Procedures did not include recovery phase processes for end users to validate the effective operation of business systems (eg verifying the application is available). |
| PIRSA | ✓ | ✘ | • Procedures were in draft at the time of our review. In response, PIRSA advised that these draft procedures accurately reflected the current operating environment and have since been approved. |
| SACE Board | ✘ | – | • Detailed recovery testing procedures exist for its key online business systems.<br>• However, no detailed recovery procedures maintained for several other key business systems. Manual process is currently required to restore these systems in a disaster. |
| SAFECOM | ✘ | – | • Detailed recovery procedures not documented where SAFECOM is responsible for recovery activities. |
| SAPOL | ✘ | – | • Recovery requires certain manual system tasks to be carried out.<br>• Detailed recovery procedures not documented in a central repository. |
| SATC | ✘ | – | • SATC maintains a priority server listing, resumption schedule and some informally documented recovery information.<br>• SATC is jointly responsible for recovering some other key business systems. However, no references to these other systems were included in the documents we reviewed.<br>• No indication of tasks to be conducted to confirm successful recovery. |
| SA Water | ✘ | – | • 78 out of 128 key business systems do not have detailed recovery procedures.<br>• SA Water is developing these procedures on an ongoing basis as part of business-as-usual testing and systems implementation projects. |

# 5 Recovery arrangements

### What we found

- Deficiencies with agency recovery objectives and outage times.
- No disaster recovery secondary site at some agencies.
- Current secondary site arrangements are insufficient or have limitations at some agencies.

### What we recommended

- Recovery time and point objectives should be specified in agency disaster recovery plans for all key business systems.
- Recovery time and point objectives will need to be within business-defined maximum allowable outage times outlined in agency business continuity plans.
- Some agencies should explore options and/or proceed with current plans regarding possible alternative hosting and secondary site arrangements.

## 5.1 Introduction

Agencies need to implement sufficient IT recovery arrangements to meet their expected recovery time and point objectives (RTOs and RPOs). As noted in section 2.2, agencies may use secondary sites to recover or maintain key IT services in the event of a disaster. Figure 5.1 provides examples of potential recovery arrangements to meet set objectives.

**Figure 5.1: Examples of recovery arrangements based on recovery time/point objectives**

| Recovery time objective | Recovery point objective | Potential recovery arrangements |
|---|---|---|
| 1 hour | Minimal data loss | Hot site with data synchronised in near real-time |
| 3 hours | 1 hour | Warm site with some data synchronised |
| 1 day | 1 day | Warm site with disk backups |
| 5 days | 1 day | Cold site with disk backups |

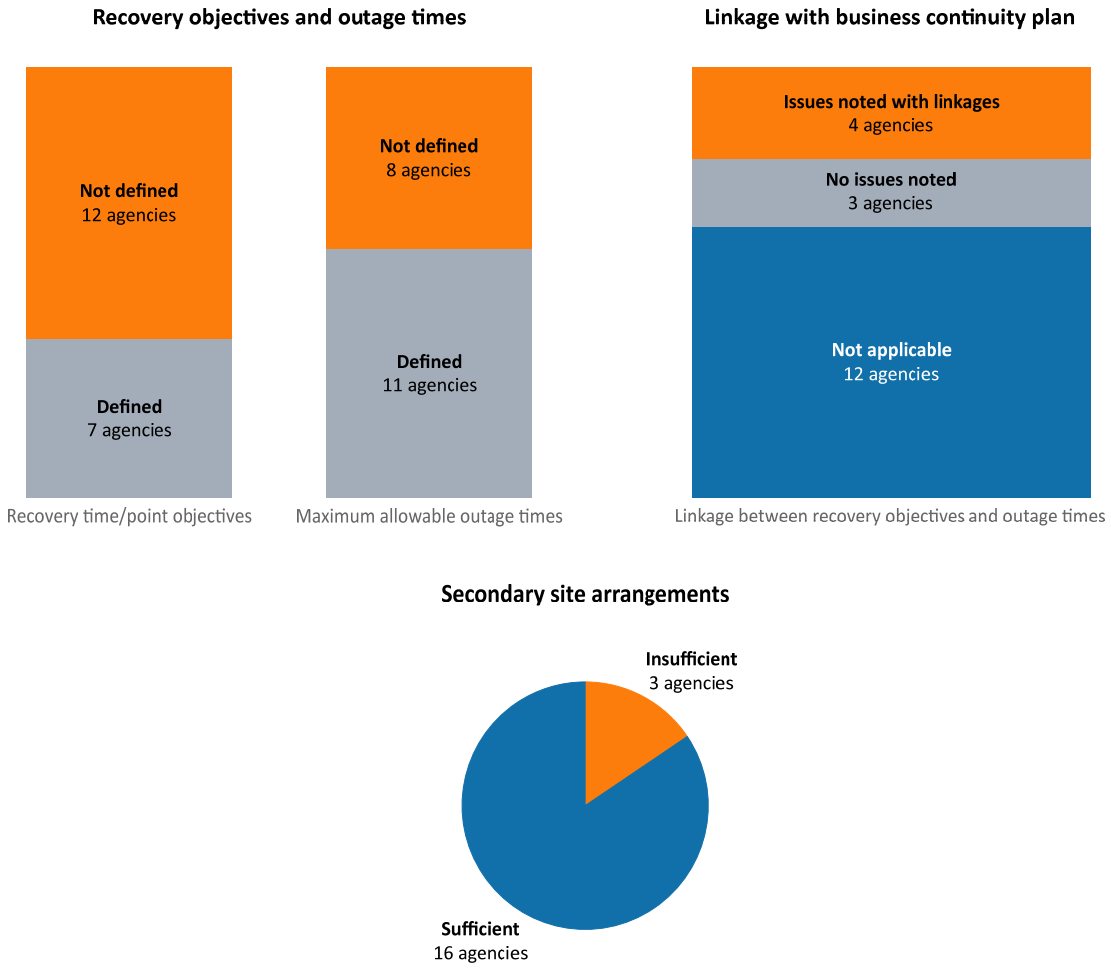
We assessed whether agencies aligned these IT recovery arrangements with business expectations. To do this, we reviewed agency business continuity plans and compared RTOs/RPOs with the maximum allowable outage times in the plan.

Maximum allowable outage times should be equal to or greater than RTOs. This ensures that agencies can recover an IT service within the time the agency expects to continue its business processing.

## 5.2 Findings

### 5.2.1 Overview

**Figure 5.2: Overview of testing results for recovery arrangements**




### 5.2.2 Deficiencies with agency recovery objectives and outage times

#### Affected agencies

AGD, CAA, DCS, DECD, DEWNR, DPC, DPTI, DTF, LSC, PIRSA, SACE Board, SA Health and SA Water.

#### Recommendation

Recovery time and point objectives should be specified in agency disaster recovery plans for all key business systems.

Recovery time and point objectives will need to be within business-defined maximum allowable outage times outlined in agency business continuity plans.

## Finding

12 of the 19 agencies we reviewed did not have RTOs and/or RPOs defined for some or all of their systems. For another agency, although they were defined, there was no formal process conducted to determine these metrics.

For eight of the 19 agencies we reviewed, the maximum allowable outage times were not defined for some or all key business processes.

Where key disaster recovery and business continuity metrics have not been clearly specified, there is a risk that agencies may not be able to restore key business systems within business accepted time frames.

Results for these agencies are summarised in figure 5.3.

**Figure 5.3: Results summary – instances of deficiencies with RTO, RPO and maximum allowable outage times for key business systems**

| Agency | RTOs and RPOs are defined | Maximum allowable outage times are defined | Comments |
|---|---|---|---|
| AGD | ✘ | ✓ | • AGD is remediating a number of disaster recovery-related activities identified by an internal audit completed in March 2017. |
| CAA | ✓ | ✘ | • CAA maintains documentation listing all key business systems, including their desired and achievable RTO and RPOs.<br>• However, maximum allowable outage times were not identified for two systems and a number of RTOs do not meet desirable outage times.<br>• An internal risk analysis identified certain positive disaster recovery controls, including a redundant data centre and resilient processing platforms. |
| DCS | ✘ | ✘ | • RTOs and RPOs not defined for two business systems.<br>• DCS advised that these systems are managed by service providers and have certain disaster recovery resilience capabilities built in. |
| DECD | ✘ | ✘ | • DECD advised that it was progressing its disaster recovery plan and business unit continuity plans through its Business Continuity Management Program. |

| Agency | RTOs and RPOs are defined | Maximum allowable outage times are defined | Comments |
|---|---|---|---|
| DEWNR | ✘ | ✘ | • DEWNR is making improvements to its business continuity and disaster recovery plans by implementing a Business Continuity Management Framework. This includes developing an overarching disaster recovery plan and improving the strategic alignment of the business and the IT support teams. |
| DPC | ✘ | ✓ | • No documented and approved disaster recovery plan for e-Procurement systems.<br>• RTOs and RPOs are defined for Chris21 and mainframe. |
| DPTI | ✘ | ✘ | • No specified and approved RTO and RPO for the computerised train control system.<br>• Maximum allowable outage times not identified for rail operations.<br>• DPTI advised that it was drafting a disaster recovery plan and updated business continuity plan as part of information security management system compliance work. |
| DTF | ✘ | ✓ | • RTOs and RPOs not defined for all important business systems at the time of our review.<br>• After we completed our review, DTF advised us that it has developed an ICT business continuity plan that includes RTOs and RPOs for core ICT and common SA Government services. |
| PIRSA | ✘ | ✘ | • An internal audit of business continuity plans was completed in June 2017 with remediation expected in 2017-18. |
| SACE Board | ✘ | ✘ | • SACE Board has mainly focused on the recovery of its online business systems used to provide students with their SACE results.<br>• However, RTO, RPO and maximum allowable outage times were not identified for four other key business systems. Examples include its financial management system and electronic document and records management system. |
| SAFECOM | ✘ | ✓ | • RTOs and RPOs are not defined for key business systems. |

| Agency | RTOs and RPOs are defined | Maximum allowable outage times are defined | Comments |
|---|---|---|---|
| SAPOL | ✘ | ✓ | • SAPOL's business unit business continuity plans do not contain sufficient information to cover all aspects of an IT disaster recovery plan. This includes RTOs or RPOs applied to key business systems for disaster recovery purposes. |
| SATC | ✘ | ✓ | • RTOs and RPOs are not defined for key business systems. |
| SA Water | ❶ | ✘ | • ❶ No formal process was conducted to determine disaster recovery metrics including RTOs and RPOs. These metrics were developed by business owners based on perceived impact of interruption, however they were not appropriately validated by the Information Technology group. |

Additionally, for three of the 19 agencies we reviewed, RTOs exceeded the maximum allowable outage times for some key business systems.

There is an increased risk that these agencies will not be able to recover their systems within required business time frames.

Results for these agencies are summarised in figure 5.4.

**Figure 5.4: Results summary – agencies where RTO times exceed maximum allowable outage times**

| Agency | RTOs within maximum allowable outage times | Comments |
|---|---|---|
| CAA | ✘ | • CAA maintains documentation listing all key business systems, including their desired and achievable RTOs and RPOs.<br>• However, maximum allowable outage times were not identified for two systems and a number of RTOs do not meet desirable outage times. |
| LSC | ✘ | • A number of RTOs do not meet desirable maximum allowable outage times. |
| SA Water | ❷ | • ❷ Our single sample of an SA Water service impact analysis[5] identified the business system RTO exceeded the defined maximum allowable outage time. This assessment recommended the business unit consider business continuity strategies to avoid significant impacts to SA Water. Other business units may have similar shortfalls. |

[5] SA Water's service impact analysis focused on business processes directly impacted by an IT service.

Finally, we noted that SA Health maintains a business impact assessment of key services and IT service resumption plans for all key business systems. However, we identified that documentation conflicts exist between business continuity plans and disaster recovery metrics, including maximum allowable outage times, RTOs and RPOs for four business systems.

### 5.2.3 No disaster recovery secondary site or insufficient/limitations with current arrangements

#### Affected agencies

DECD, DPC and DPTI.

#### Recommendation

Some agencies should explore options and/or proceed with current plans regarding possible alternative hosting and secondary site arrangements.

For example, as part of developing and implementing a disaster recovery testing schedule, some agencies need to review whether existing secondary site arrangements are sufficient to meet business requirements. Where gaps are identified, these agencies should consider increasing the level of redundancy (availability) for important business systems at the application level.

#### Finding

For three of the 19 agencies we reviewed, we noted no disaster recovery secondary site or insufficient/limitations with current arrangements.

In the event of a disaster or system failure at the primary site, there is a risk that key business systems will not be recoverable within required time frames.

Results for affected agencies are summarised in figure 5.5.

**Figure 5.5: Results summary – no disaster recovery secondary site or insufficient/limitations with current arrangements**

| Agency | Comments |
|---|---|
| DECD | • We identified that DECD does not maintain a secondary site for all of its key business systems.<br>• To reduce this risk, DECD advised us that its current IT infrastructure includes multiple physical servers, with network failover capabilities and storage devices. DECD also advised that it proactively monitors production activities and performs service management reviews and risks assessments as necessary.<br>• We were also advised that DECD has sought pricing for secondary hosting arrangements. This is being considered within the proposed disaster recovery plan informed by the business continuity program. |

| Agency | Comments |
|---|---|
| DPC | • e-Procurement systems managed by DPC have multiple failover functions. However, all components of these systems are hosted in a single data centre. DPC confirmed that it does not maintain a secondary site arrangement for e-Procurement systems, in the event of a disaster at the primary site.<br>• To partially mitigate this risk, DPC advised us that a major incident impacting the SA Government data centre would invoke a state-wide disaster recovery process. In this case, e-Procurement systems would be a lower priority than a number of other key systems across government. This process would dictate recovery time frames for e-Procurement systems. |
| DPTI | For the computerised train control system:<br>• DPTI does not maintain a secondary site.<br>• We note that this system is only one component of the rail signalling network. Currently, the Operations Control Centre (OCC) building houses the central signalling system interlocks. DPTI advised us that it plans to implement a full secondary site, including redundant signalling interlocks, as part of relocating its OCC to Dry Creek. It expects to complete this relocation by September 2018. To partially mitigate this risk, technical staff cover multiple disciplines of the signalling and control networks. Changes proposed for the signal maintenance and engineering team structures as part of the OCC relocation include consideration of appropriate skillsets.<br><br>For SAILIS:<br>• The current secondary site arrangement is limited to a read-only capacity. In the event of extended outages, DPTI relies on certain paper-based processes, documented in business continuity plans. |

# 6 Disaster recovery testing

### What we found

- Most agencies did not maintain a formal disaster recovery testing schedule.
- Most agencies did not sufficiently test their disaster recovery arrangements.

### What we recommended

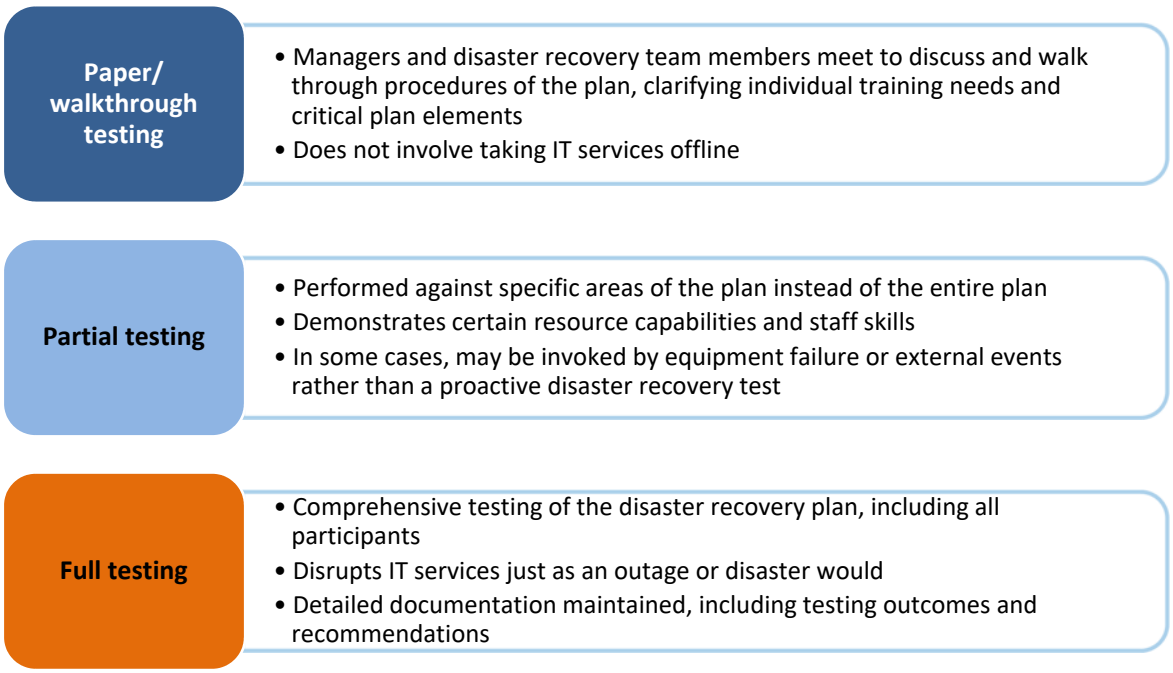
- Agencies should develop and implement disaster recovery testing schedules for all key business systems .
- Agencies should schedule disaster recovery tests for these systems regularly in line with their importance.
- Agencies should regularly test all key business systems. This is to confirm that agencies can recover key systems within expected time frames. Test results and recommendations should be documented.

## 6.1 Introduction

Agencies need to establish formal disaster recovery testing schedules for their key business systems. They should test disaster recovery arrangements regularly for these systems. This ensures that they can recover key systems within defined RTOs and RPOs, as well as maximum allowable outage times defined in business continuity plans.

We have classified disaster recovery tests as either paper/walkthrough, partial or full tests, based on the criteria listed in figure 6.1.

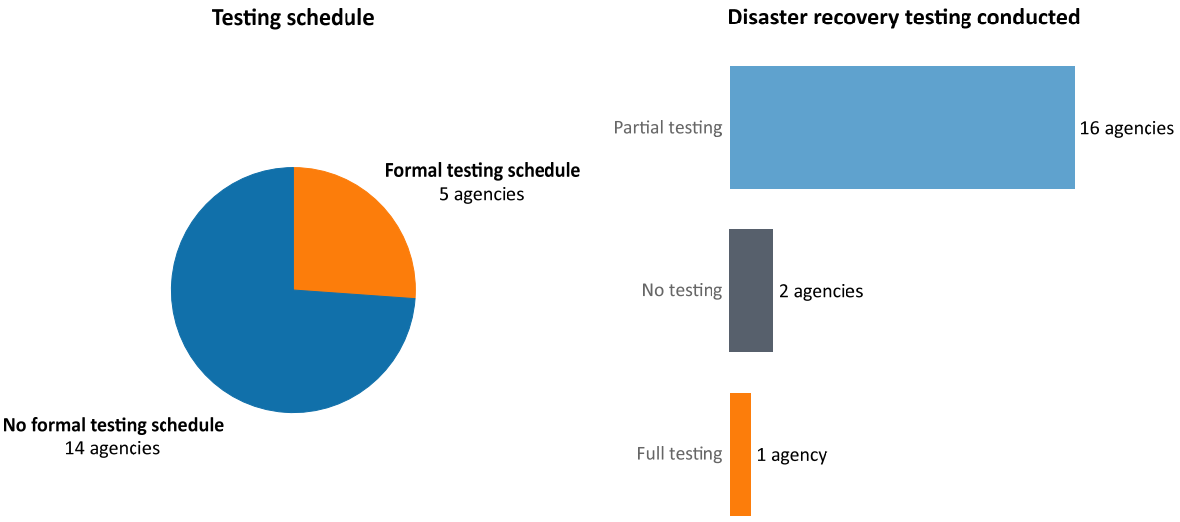
**Figure 6.1: Disaster recovery testing approaches**



## 6.2 Findings

### 6.2.1 Overview

**Figure 6.2: Overview of testing results for disaster recovery testing schedules and tests conducted**




### 6.2.2 No formal disaster recovery testing schedule

#### Affected agencies

AGD, CAA, DCSI, DECD, DEWNR, DPC, DPTI, DSD, DTF, LSC, PIRSA, SAFECOM, SAPOL and SATC.

#### Recommendation

Agencies should develop and implement disaster recovery testing schedules for all key business systems.

They should schedule tests for these systems regularly in line with their importance.

#### Finding

14 of the 19 agencies we reviewed did not maintain a formal disaster recovery testing schedule for some or all of their key business systems.

At the time of our review, AGD, DSD and DTF advised us that they were preparing disaster recovery testing schedules.

Although DPC had regularly tested disaster recovery arrangements for Masterpiece and Chris21, it did not have a formal testing schedule in place for e-Procurement systems.

Without a formal disaster recovery testing schedule, key business systems may not be regularly tested. This increases the risk that agencies cannot restore key business systems within maximum allowable outage times.

### 6.2.3 Insufficient disaster recovery testing

#### Affected agencies

AGD, CAA, DCSI, DCS, DECD, DEWNR, DPC, DPTI, DSD, DTF, LSC, PIRSA, SACE Board, SAFECOM, SA Health, SAPOL, SATC and SA Water.

#### Recommendation

Agencies should regularly test (at least annually) all key business systems. This is to confirm that agencies can recover key systems within expected time frames. They should document test results and recommendations.

#### Finding

18 of the 19 agencies we reviewed did not fully test disaster recovery arrangements for all of their key business systems within the last two years. However, 16 of these agencies did partially test aspects of their disaster recovery arrangements. Results for these agencies are summarised in figure 6.3.

Several agencies advised us that they classified the state-wide power outage in September 2016 as a partial disaster recovery test. This is because agencies needed to perform a shutdown and reboot routine or fail over to backup power sources. However, in most cases this did not involve formally invoking the disaster recovery plan or recovering business systems at a secondary site. Additionally, most agencies did not maintain documentation of their partial tests.

Without conducting comprehensive formal disaster recovery testing for all key business systems, there is a risk that agencies will not be able to restore these systems within maximum allowable outage times.

**Figure 6.3: Results summary – Disaster recovery testing status for agency key business systems**

| Agency | Disaster recovery testing | | Comments |
|---|---|---|---|
| | Full tests conducted | Partial tests conducted | |
| AGD | ✘ | ✓ | • Testing limited to responding to business-as-usual events.<br>• No testing performed to ensure multiple systems and data could be effectively restored.<br>• AGD remediating a number of disaster recovery-related activities identified by an internal audit completed in March 2017. |

| Agency | Disaster recovery testing | | Comments |
|---|---|---|---|
| | Full tests conducted | Partial tests conducted | |
| CAA | ✘ | ✓ | • CAA advised that the state-wide power outage demonstrated its IT environment resilience.<br>• Disaster recovery testing over the SA Government mainframe in September 2016. |
| DCSI | ✘ | ✓ | • Partially tested disaster recovery through successful restores from power shutdowns and business-as-usual events.<br>• No testing performed to ensure multiple systems and data could be effectively restored. |
| DCS | ✘ | ✓ | • Offender Management System tested in September 2016.<br>• Other systems not tested.<br>• Staff rostering system (Microster) and prisoner electronic monitoring system (Cronos) have disaster recovery resilience capabilities. |
| DECD | ✘ | ✘ | • DECD has not conducted any form of disaster recovery testing for key business systems.<br>• DECD to seek funding for disaster recovery testing as part of its business continuity management program. |
| DEWNR | ✘ | ✓ | • Tested aspects of recovery, mostly failover capabilities.<br>• Secondary site failover tested during September 2016 state-wide power outage.<br>• Testing outcomes not documented. |
| DPC | ✘ | ✓ | • e-Procurement disaster recovery plan tested for one environment in September 2016.<br>• No recent e-Procurement disaster recovery test for general SA Government environment.<br>• Chris21 and mainframe disaster recovery plans recently tested. |
| DPTI | ✘ | ✓ | • No disaster recovery testing for computerised train control system.<br>• Limited testing for rail traction SCADA systems.<br>• TRUMPS disaster recovery plan not tested since 2014. DPTI has since advised that a test is scheduled to be completed by the end of November 2017.<br>• Full disaster recovery testing for traffic management and SAILIS systems. |

| Agency | Disaster recovery testing | | Comments |
|---|---|---|---|
| | Full tests conducted | Partial tests conducted | |
| DSD | ✘ | ✓ | • DSD advised us that it maintains robust system infrastructure.<br>• Still implementing a new secondary site and had not formally tested full production environment at this site. |
| DTF | ✘ | ✓ | • DTF uses 60+ business systems managed either internally or by external providers.<br>• DTF advised us that its disaster recovery testing focuses on ICT infrastructure and 14 important DTF managed systems, based on important business processes outlined in a business impact assessment. These systems include certain interfaces and data stores.<br>• Only two of these 14 systems have been tested in the last two years.<br>• We were also advised that DTF intends to include the remaining important systems in a rolling test schedule to be finalised in 2017-18. |
| LSC | ✘ | ✓ | • Advised that it is able to recover from unplanned events, such as the state-wide power outage.<br>• No formal disaster recovery testing by LSC or external service providers.<br>• However, LSC recently tested its ability to continue operations via remote access, which we were advised was successful. |
| PIRSA | ✘ | ✓ | • Partial testing conducted in response to state-wide power outage and certain equipment malfunctions. |
| SACE Board | ✘ | ✓ | • Recovery has been focused on the online business systems used to provide students with their SACE results. However, no disaster recovery testing has been conducted to restore its other key business systems, including the financial management system and electronic document and records management system.<br>• SACE Board advised that these systems are maintained in a highly-available environment with automatic recovery for single equipment failures. |

| Agency | Disaster recovery testing | | Comments |
|---|---|---|---|
| | Full tests conducted | Partial tests conducted | |
| SAFECOM | ✘ | ✘ | • SAFECOM advised us that key business systems are on highly-available platforms, including failover capabilities. These failover capabilities, however, have not been formally tested for key business systems.<br>• Working towards migrating systems to a cloud environment to rectify disaster recovery limitations. |
| SA Health | ✘ | ✓ | • Testing generally limited to individual systems.<br>• No testing to restore multiple systems and data across various data centres.<br>• Several systems not subject to formally scheduled disaster recovery testing. However, some of these systems were expected to be replaced. |
| SAPOL | ✘ | ✓ | • Tested aspects of disaster recovery, including the state-wide power outage, a business continuity plan test exercise, mainframe disaster recovery testing and a planned power shutdown.<br>• Once a system was in production, however, SAPOL generally did not conduct disaster recovery testing. |
| SATC | ✘ | ✓ | • DPC is responsible for testing SATC's key financial systems.<br>• No formal disaster recovery testing for systems where SATC is responsible for recovery.<br>• Partial testing as a result of the state-wide power outage. |
| SA Water | ✘ | ✓ | • 61% of key business systems either have not been tested or have not been tested since system implementation.<br>• SA Water advised us that it is actively progressing its disaster recovery testing activities and has committed itself to developing IT service continuity skills with its staff through direct involvement in test planning, developing recovery procedures and testing activities. |

# 7 Skillsets and risk assessments

### What we found

- Some agencies could not demonstrate they had sufficient IT resources to effectively conduct disaster recovery activities.
- No recent risk assessment of disaster recovery arrangements by some agencies.
- Disaster recovery risks not incorporated into some agency risk registers with mitigation plans and time frames for resolution.

### What we recommended

- Agencies should assess the availability and skillsets of required resources to respond to a major disaster recovery event.
- If skillset gaps are identified, upskilling should be conducted through either involvement in disaster recovery testing or formal training. This is to ensure all ICT resources maintain an acceptable level of disaster recovery skills to effectively conduct disaster recovery activities.
- Agencies should conduct a risk assessment of its current plans for recovery of its key business systems.
- Identified disaster recovery risks should be documented in the agency risk register, with identified controls and treatment plans. These risks should be formally assigned to an owner and tracked accordingly.

## 7.1 Introduction

Agencies need to maintain their current IT skillset to effectively conduct the disaster recovery activities they are responsible for. Agencies should therefore formally assess their current IT skillset to ensure they can effectively recover key systems in the event of a disaster.

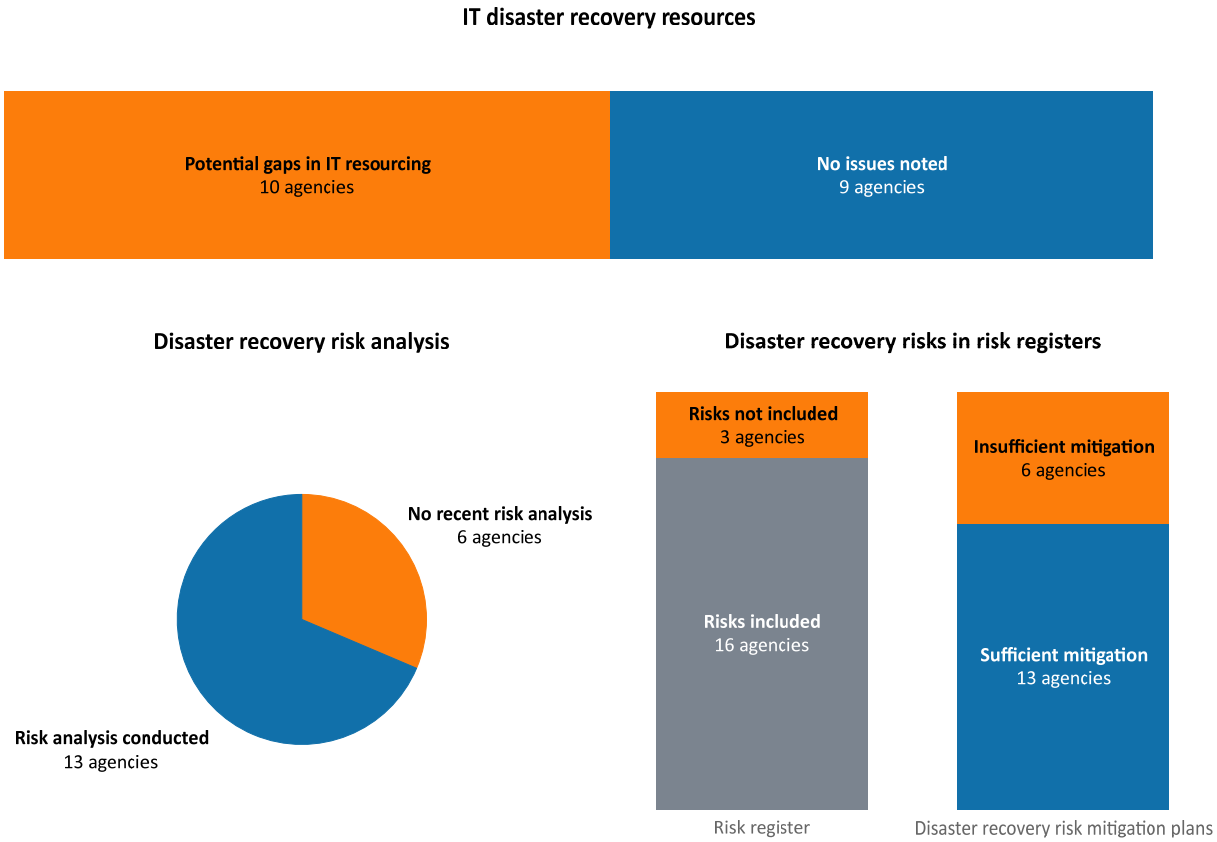
In addition, agencies' current disaster recovery arrangements may be presented with a number of potential threats to data, hardware and operating environments. Formally assessing risks with current disaster recovery plans and associated practices will help to identify these threats and reduce the likelihood of adverse impacts on an agency's ability to recover key business systems if a disaster occurs.

Formally documenting disaster recovery-related risks in agencies' risk registers will help track and manage each risk until resolution, through identified controls and treatment plans.

## 7.2 Findings

### 7.2.1 Overview

**Figure 7.1: Overview of testing results for skillsets and risk assessments**




### 7.2.2 Inability to demonstrate sufficient IT resources to effectively conduct disaster recovery activities

#### Affected agencies

AGD, CAA, DCSI, DPC, DPTI, DTF, LSC, PIRSA, SAFECOM and SAPOL.

#### Recommendation

Agencies should assess the availability and skillsets of the resources needed to respond to a major disaster recovery event.

If skillset gaps are identified, upskilling should be conducted through either involvement in disaster recovery testing or formal training. This is to ensure all ICT resources maintain an acceptable level of skills to effectively conduct disaster recovery activities.

#### Finding

10 of the 19 agencies could not demonstrate they had sufficient IT resources to effectively conduct disaster recovery activities.

This increases the risk that staff may not be able to effectively recover key business systems in the event of a disaster or system failure.

Results for affected agencies are summarised in figure 7.2.

**Figure 7.2: Results summary – IT resource capability to effectively conduct disaster recovery activities**

| Agency | Comments |
|---|---|
| AGD | • We noted gaps in AGD's disaster recovery plan and associated restoration procedures. Therefore, AGD's December 2016 informal assessment of required resources and skillsets was potentially incomplete.<br>• AGD is remediating a number of disaster recovery-related activities identified in an internal audit completed in March 2017. |
| CAA | • CAA had not recently formally assessed its current IT skillset to effectively conduct disaster recovery activities. However, it had initiated a review of the CAA IT (digital) organisation. As part of this review, it will conduct a skillset assessment. |
| DCSI | • DCSI had not recently conducted a formal assessment of IT skillsets for disaster recovery activities. Additionally, it had not formally conducted disaster recovery testing to confirm its ability to restore multiple systems.<br>• DCSI advised us that the ability to restore services is a central skill maintained within the department and from an infrastructure perspective, reliance is placed on the whole-of-government service provider. |
| DPC | • DPC has not formally assessed its current skillset to effectively conduct disaster recovery activities for e-Procurement systems. Further, DPC has not sufficiently tested these systems to ensure it maintains sufficient IT skillsets for restoration activities. |
| DPTI | For the computerised control train system:<br>• There has not been any formal assessment of current its IT skillset to effectively conduct disaster recovery activities.<br>• To partially mitigate this risk, technical staff cover multiple disciplines of the signalling and control networks. Changes proposed for the signal maintenance and engineering team structures as part of the OCC relocation include consideration of appropriate skillsets.<br><br>For the rail traction SCADA systems:<br>• DPTI has not formally assessed its current IT skillset to effectively conduct disaster recovery activities for these systems.<br>• DPTI advised operational staff have specific skills relating to the SCADA systems, and have received relevant training such as operating and monitoring the SCADA equipment and responding to technical enquiries.<br><br>For TRUMPS:<br>• DPTI has not formally assessed its current IT skillset to effectively conduct disaster recovery activities. DPTI planned to do this as part of the scheduled disaster recovery test for May 2017, which has been delayed. |

| Agency | Comments |
|---|---|
| DTF | • DTF has not formally assessed its current skillset to effectively conduct disaster recovery activities for important business systems. Additionally, it has not formalised disaster recovery roles and responsibilities, or conducted recent disaster recovery training sessions.<br>• DTF advised that specific staff within DTF ICT have been assigned key disaster recovery roles and would be able to assist in a disaster.<br>• After completing our review, we were advised that DTF plans to conduct a disaster recovery training session in early 2018. |
| LSC | • LSC has not conducted any formal disaster recovery training with relevant staff for a significant period of time. LSC has not conducted any recent assessment of its current IT skillset to effectively conduct disaster recovery activities.<br>• LSC advised us that it is currently reviewing the ICT strategic plan, which includes ICT skillsets. |
| PIRSA | • PIRSA's disaster recovery plan advises that pre-testing involves ensuring all involved understand their roles and responsibilities on an annual basis, however no active formal disaster recovery testing has been conducted to confirm this understanding.<br>• PIRSA advised that disaster recovery roles and responsibilities have been considered as part of performance development conversations and in developing ICT workforce plans. |
| SAFECOM | • SAFECOM advised that four staff members within one of its support teams provide operational support for emergency incidents impacting key business systems. Staff are formally assigned to ICT incident management roles, providing on-call support on a rostered basis.<br>• However, SAFECOM has not recently assessed its current IT skillset to effectively conduct disaster recovery activities, and no formal disaster recovery testing has been conducted to confirm the required knowledge. |
| SAPOL | • SAPOL has not conducted a formal assessment of its current IT skillset to effectively conduct disaster recovery activities over its key business systems, other than its mainframe systems. |

### 7.2.3 No recent risk assessment of disaster recovery arrangements

#### Affected agencies

DPC, DPTI, PIRSA, SACE Board, SAFECOM and SA Water.

#### Recommendation

Agencies should conduct a risk assessment of their current plans for recovery of key business systems.

#### Finding

Six of the 19 agencies we reviewed did not conduct a recent disaster recovery risk assessment to identify potential threats to data, hardware and supporting environments.

Where the disaster recovery plan has not been subject to a formal risk assessment, potential threats to data, hardware and operating environments may not have been fully identified. This may adversely affect an agency's ability to recover key business systems in the event of a disaster or system failure.

Results for affected agencies are summarised in figure 7.3.

**Figure 7.3: Results summary – No recent risk assessment of disaster recovery arrangements**

| Agency | Comments |
|---|---|
| DPC | • DPC has not recently conducted a risk assessment of its disaster recovery plan for key business systems. |
| DPTI | • DPTI has not recently conducted a formal risk assessment for the TRUMPS disaster recovery plan.<br>• Following our review, DPTI advised that it would add a 'risk' section to the TRUMPS disaster recovery plan to address risks associated with the plan itself. |
| PIRSA | • PIRSA has not conducted a risk assessment of its current disaster recovery plan and associated practices. |
| SACE Board | • The SACE Board advised that it conducted a business impact assessment of its key business processes in November 2015. However, it has not conducted a risk assessment of its current disaster recovery plan for its key business system to identify potential threats to data, hardware and the supporting environment. |
| SAFECOM | • SAFECOM advised that it has not conducted a risk assessment of its current disaster recovery arrangements for its key business systems.<br>• SAFECOM is jointly responsible for recovering the SACFS Incident Management System (CRIIMSON) and SASES incident management system (WEBEOC). It also relies on other government agencies and third party providers to restore its key business systems. |
| SA Water | • SA Water advised that it has not conducted a risk assessment of its current IT service continuity arrangements for its key business systems.<br>• SA Water advised that a more structured risk assessments approach would be beneficial. This includes current data centres and other facilities. |

### 7.2.4 Disaster recovery risks have not been incorporated into agency risk registers with mitigation plans and time frames for resolution

#### Affected agencies

AGD, DEWNR, DPTI, DTF, SACE Board, SAFECOM and SA Health.

#### Recommendation

Identified disaster recovery risks should be documented in the agency risk register, with identified controls and treatment plans. These risks should be formally assigned to an owner and tracked accordingly.

## Finding

Three of the 19 agencies we reviewed had not incorporated disaster recovery risks into their risk registers.

Six of the 19 agencies we reviewed had not documented or actioned appropriate mitigation plans within time frames for resolution to resolve identified disaster recovery risks.

Without identifying and formally documenting agency disaster recovery-related risks, current treatments implemented may be insufficient to fully mitigate risks in the event that a disaster occurs.

Results for affected agencies are summarised in figure 7.4.

**Figure 7.4: Results summary – Disaster recovery risks not incorporated into agency risk registers with mitigation plans and time frames for resolution**

| Agency | Disaster recovery risks incorporated into agency risk register | Mitigation plans and resolution time frames have been documented or actioned | Comments |
|---|---|---|---|
| AGD | ✘ | ✓ | • Mitigation plans and time frames for resolution were included in the March 2017 AGD disaster recovery internal audit. |
| DEWNR | ✓ | ✘ | • DEWNR recently engaged its internal auditor to conduct certain reviews. This included reviews of crisis management and IT risk and maturity.<br>• However, for crisis management there were no documented agreed actions or time frames.<br>• For the IT risk and maturity review, although treatments have been identified in a risk register, there are no documented time frames for resolution. |
| DPTI | ✓ | ✘ | • For the rail traction SCADA systems DPTI maintained disaster recovery-related risk treatment plans. However, these plans did not address key disaster recovery aspects to mitigate risks. |

| Agency | Disaster recovery risks incorporated into agency risk register | Mitigation plans and resolution time frames have been documented or actioned | Comments |
|---|---|---|---|
| DTF | ✓ | ✘ | • DTF's consolidated risk register included several disaster recovery-related risks.<br>• However, treatment plans do not address key disaster recovery aspects to mitigate risks. |
| SACE Board | ✘ | ✘ | • Although SACE Board's risk register acknowledges the risk of IT infrastructure failure, it does not contain key disaster recovery risk details and associated controls and treatment plans to reduce the exposed level of risk. |
| SAFECOM | ✘ | ✘ | • SAFECOM advised that it is not the system owner of its key business systems. Despite this, it is jointly responsible for recovering certain systems. |
| SA Health | ✓ | ✘ | • Certain disaster recovery-related SA Heath internal audit actions were due to be addressed by December 2016.<br>• At the time of our review, SA Health advised of some progress, however the initial target completion date has since been revised to December 2018. |